

Prof. Dr. Tobias Singelnstein • Theodor-W.-Adorno-Platz 4
• 60323 Frankfurt a.M.







Prof. Dr. Tobias Singelnstein

An das
Bundesverfassungsgericht
Schlossbezirk 3
76131 Karlsruhe



Berlin, den 21. Juni 2024

Verfassungsbeschwerde

1. 
2. 
3. 
4. 
5. 
6. 

– Beschwerdeführer*innen –

Bevollmächtigter: Prof. Dr. Tobias Singelnstein, Goethe-Universität, Fachbereich
Rechtswissenschaft, Theodor-W.-Adorno-Platz 4, 60323 Frankfurt a.M.

gegen

1. § 25a Abs. 2 Satz 1 Nr. 1 i.V.m. § 25a Abs. 1 Satz 2-5, Abs. 2 Satz 2-4, Abs. 3, Abs. 4 Satz 6, Abs. 5
Satz 2 HSOG,

2. § 25a Abs. 2 Satz 1 Nr. 2 i.V.m. § 25a Abs. 1 Satz 2-5, Abs. 2 Satz 2-4, Abs. 3, Abs. 4 Satz 6, Abs. 5 Satz 2 HSOG,

3. § 25a Abs. 2 Satz 1 Nr. 3 i.V.m. § 25a Abs. 1 Satz 2-5, Abs. 2 Satz 2-4, Abs. 3, Abs. 4 Satz 6, Abs. 5 Satz 2 HSOG

des Hessischen Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung der Bekanntmachung vom 14. Januar 2005 (GVBl. I S. 14), zuletzt geändert durch Art. 2, Art. 4 des Gesetzes vom 29. Juni 2023 (GVBl. S. 456).

Namens und in Vollmacht der Beschwerdeführer*innen erhebe ich Verfassungsbeschwerde und rüge die Verletzung von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 Abs. 1 und Art. 19 Abs. 4 GG.

Gliederung des Schriftsatzes

A. Vorbemerkung.....	7
B. Gegenstand der Verfassungsbeschwerde.....	9
I. Erläuterung der angegriffenen Vorschrift.....	9
II. Die Beschwerdeführer*innen.....	11
1. Beschwerdeführerin zu 1.....	11
2. Beschwerdeführer zu 2.....	13
3. Beschwerdeführer zu 3.....	15
4. Beschwerdeführer zu 4.....	17
5. Beschwerdeführerin zu 5.....	17
6. Beschwerdeführerin zu 6.....	18
C. Zulässigkeit.....	19
I. Beschwerdebefugnis.....	19
1. Verfassungsrechtliche Rügen	19
2. Eigene und gegenwärtige Betroffenheit	19
a) Als Zielperson	20
b) Als Drittbetroffene	22
(1) Aufgrund der Streubreite	23
(2) Als Kontaktpersonen	23
(a) Beschwerdeführer*innen zu 1 bis 3	24
(b) Beschwerdeführer*innen zu 5 und 6	26
(3) Beschwerdeführer*innen mit nachweislich vorhandenen Daten	27

3.	Unmittelbare Betroffenheit.....	28
II.	Subsidiarität	29
1.	Vorbeugender Rechtsschutz.....	30
2.	Vorgehen gegen Verwaltungsvorschriften	31
3.	Nachträglicher Rechtsschutz	32
III.	Beschwerdefrist.....	32
D.	<i>Begründetheit der Verfassungsbeschwerde</i>	33
I.	Schwerwiegender Eingriff mangels wirksamer Reduzierung des Eingriffsgewichts	33
1.	Maßstab.....	33
a)	Kriterien für die Bestimmung des Eingriffsgewichts.....	34
b)	Wesentlichkeit, Bestimmtheit, Normenklarheit.....	35
(1)	Generelle Grundsätze.....	36
(a)	Wesentlichkeitstheorie.....	36
(b)	Bestimmtheit	41
(c)	Normenklarheit.....	43
(2)	Konkret im Hinblick auf Datenanalyse	44
2.	Keine Reduzierung des Eingriffsgewichts durch den Gesetzgeber	46
a)	Unzureichende Einschränkungen hinsichtlich Art und Umfang der einbezogenen Daten.....	46
(1)	Keine Beschränkung hinsichtlich Herkunft der Daten	47
(2)	Keine Einschränkungen hinsichtlich der Menge	52
(3)	Keine Beschränkung auf bestimmte Datenarten	53

(4)	Unzureichender Ausschluss der Daten „Unbeteiligter“	54
(a)	Vorgangsdaten.....	54
(b)	Verkehrsdaten	56
(c)	Sonstige Datenbestände.....	56
(5)	Keine Gewährleistung der Zweckbindung	60
(a)	Grundlegende Aspekte	60
(b)	Keine Anwendbarkeit der Kennzeichnungspflicht nach § 20a HSOG.....	63
(c)	Defizite der in § 25a HSOG vorgesehenen Konzepte	66
(aa)	Übergreifende Defizite	66
(bb)	Rollen- und Rechtekonzept	68
(aaa)	Normenklarheit	68
(bbb)	Gesetzesvorbehalt und Bestimmtheit	69
(cc)	Konzept der Kategorisierung und Kennzeichnung	72
(aaa)	Normenklarheit	72
(bbb)	Gesetzesvorbehalt und Bestimmtheit	73
b)	Unzureichende Einschränkung der Methoden der Datenanalyse.....	76
(1)	Keine Beschränkung der zugelassenen Methode	76
(2)	Kein Ausschluss von Künstlicher Intelligenz.....	80
(3)	Keine Vorkehrungen zur Vermeidung von Diskriminierung	83
II.	Nichtbeachtung der korrespondierenden Eingriffs-voraussetzungen	87
1.	Eingriffsschwellen und zu schützende Rechtsgüter des § 25a Abs. 2 Satz 1 Nr. 2 und Nr. 3 HSOG 87	
a)	Bei hoher Eingriffsintensität	87

(1)	§ 25a Abs. 2 Satz 1 Nr. 2 HSOG	88
(a)	Zu schützende Rechtsgüter	88
(b)	Eingriffsschwelle	91
(2)	§ 25a Abs. 2 Satz 1 Nr. 3 HSOG	92
(a)	Zu schützende Rechtsgüter	92
(b)	Eingriffsschwelle	93
b)	Bei reduziertem Eingriffsgewicht (hilfsweise)	93
2.	Defizitäre datenschutzrechtliche Kontrolle hinsichtlich aller Tatbestandsvarianten	94
a)	Maßstab	94
b)	Kein ausreichendes Kontrollkonzept in § 25a HSOG	95
c)	Keine Sicherungen in anderen Bestimmungen des geltenden Rechts	96
d)	Keine Vorkehrungen gegen Fehleranfälligkeit.....	97

A. Vorbemerkung

Die Verfassungsbeschwerde rügt einen Großteil der Regelungen der reformierten Ermächtigungsgrundlage zur automatisierten Anwendung zur Datenanalyse in § 25a des Hessischen Gesetz über die öffentliche Sicherheit und Ordnung (HSOG).

Nachdem das angerufene Gericht die alte Fassung der Norm sowie eine vergleichbare Vorschrift im Hamburgischen Gesetz über die Datenverarbeitung der Polizei in seinem Urteil vom 16. Februar 2023 – 1 BvR 1547/19 und 1 BvR 2634/20 zur automatisierten Datenanalyse (im Folgenden „Datenanalyse-Urteil“) für teilweise verfassungswidrig erklärt hat,

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

fasste der Gesetzgeber die Vorschrift neu.

Nach Ansicht der Beschwerdeführer*innen genügt aber auch die Neufassung der Ermächtigungsgrundlage nicht den verfassungsrechtlichen Vorschriften. Vielmehr handelt es sich bei den Änderungen lediglich um eine „wortreiche Scheinbeschränkung“,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 60.

Das angerufene Gericht hat im Datenanalyse-Urteil festgestellt, dass die Anforderungen an die Rechtfertigung variieren, da sich das Eingriffsgewicht von Befugnissen zur Datenanalyse nicht pauschal bestimmen lässt. Dieses hängt davon ab, inwieweit der Gesetzgeber beschränkende Regelungen zu Art und Umfang der Daten sowie zur Begrenzung der Auswertungsmethode vorgenommen hat,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 72 ff.

Das angerufene Gericht hat dem Gesetzgeber im Datenanalyse-Urteil dafür einige Beschränkungsmöglichkeiten aufgezeigt,

vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 78 ff.

Ausgehend davon rügen die Beschwerdeführer*innen, dass der Gesetzgeber in der neuen Fassung des § 25a HSOG keine ausreichenden Beschränkungen vorgesehen hat, um das potenziell sehr hohe Eingriffsgewicht von Datenanalysen zu reduzieren. § 25a HSOG ist nach wie vor daten- und methodenoffen konzipiert. Folglich sind auch die vorgesehenen Eingriffsvoraussetzungen, also Eingriffsschwelle und Gewicht der zu schützenden Rechtsgüter nicht verhältnismäßig ausgestaltet.

Hervorzuheben ist insbesondere, dass der Gesetzgeber die Reichweite des Vorbehalts des Gesetzes und die Wesentlichkeitstheorie verkennt, indem er die vom angerufenen Gericht im Datenanalyse-Urteil eröffnete Möglichkeit einer Regelung durch Verwaltungsvorschrift mit der Neufassung des § 25a HSOG überstrapaziert. Gerade im Hinblick auf künftige Gesetzgebungsverfahren in anderen Bundesländern benötigt es hierzu einer Klarstellung durch das angerufene Gericht.

Derzeit ist ein weiteres Verfahren gegen eine Befugnisnorm in Nordrhein-Westfalen anhängig, die ebenfalls den Einsatz von Analysesoftware zum „Data Mining“ erlaubt (Az. 1 BvR 1908/22).

B. Gegenstand der Verfassungsbeschwerde

I. Erläuterung der angegriffenen Vorschrift

§ 25a HOSG wurde mit dem Gesetz zur Änderung sicherheitsrechtlicher Vorschriften und zur Umorganisation der hessischen Bereitschaftspolizei vom 29. Juni 2023 als Reaktion auf das Datenanalyse-Urteil des angerufenen Gerichts reformiert und ist in seiner neuen Fassung, die Gegenstand dieser Verfassungsbeschwerde ist, am 12. Juli 2023 in Kraft getreten.

Durch die Neuregelung soll die weitere Nutzung der Analysesoftware hessenDATA sichergestellt werden,

vgl. LT-Drs. 20/11235, S. 5.

Das Gesetz sieht bei der Verwendung von Analysesoftware durch die hessische Polizei zwei Schritte vor: Erstens werden Daten auf einer Analyseplattform zusammengeführt (§ 25a Abs. 1 Satz 1 HSOG). Daran schließt die vom Gesetzgeber in § 25a Abs. 1 Satz 2 HSOG legal definierte automatisierte Anwendung zur Datenanalyse an, die aus einer Verknüpfung, Aufbereitung, Auswertung sowie Anwendung für statistische Zwecke bestehen kann. Dadurch wurde die noch in der alten Fassung enthaltene Beschreibung der Weiterverarbeitung ersetzt. Darin hieß es, dass durch die automatisierte Anwendung zur Datenanalyse 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 (§ 25a Abs. 2 HSOG a.F.).

Eine Anbindung an das Internet ist explizit ausgeschlossen (§ 25a Abs. 1 Satz 6 HSOG); Datensätze aus Internetquellen können aber händisch einbezogen werden (§ 25a Abs. 2 Satz 3 HSOG).

Im Vergleich zur alten Fassung umfasst die Vorschrift nunmehr drei Tatbestandsalternativen (§ 25a Abs. 2 Satz 1 Nr. 1 bis Nr. 3 HSOG) mit unterschiedlichen Eingriffsschwellen. Während die Vorgängernorm bereits zu einem Einsatz sowohl zur vorbeugenden Bekämpfung von Straftaten als auch beim Vorliegen einer konkreten Gefahr ermächtigte (§ 25a Abs. 1 HSOG a.F.), trat mit der Reform die Eingriffsschwelle der konkretisierten Gefahr hinzu. Diese setzt voraus, dass tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraumes auf eine zumindest ihrer Art nach konkretisierte Weise Straftaten [...] begangen werden (§ 25a Abs. 2 Satz 1 Nr. 2).

Anders als in der alten Fassung werden nun auch verschiedene Datenbestände aufgelistet (§ 25a Abs. 2 Satz 2 HSOG), die für sich aber wiederum jeweils verschiedene Arten von Daten erfassen können.

Daten aus Wohnraumüberwachung und Online-Durchsuchung sind nunmehr vollkommen ausgeschlossen (§ 25a Abs. 3 Nr. 2 lit. b Satz 3 HSOG), Verkehrsdaten hingegen nur für eine Tatbestandsvariante (§ 25a Abs. 2 Satz 4 HSOG). Auch werden Vorgangsdaten sogenannter „Unbeteiligter“ dem Wortlaut nach nicht in die Analyse einbezogen (vgl. § 25a Abs. 3 Nr. 2 lit. a Satz 4 HSOG).

Die alte Fassung verwies hinsichtlich der vorbeugenden Bekämpfung von Straftaten auf die in § 100a Abs. 2 Strafprozessordnung (StPO) genannten schweren Straftaten. Die Neufassung nimmt nicht mehr auf § 100a Abs. 2 StPO Bezug, sondern stellt auf das Gewicht der zu verhütenden Straftaten ab, nämlich Straftaten mit erheblicher Bedeutung (§ 25a Abs. 2 Satz 1 Nr. 2 HSOG) und schwere oder besonders schwere Straftaten (§ 25a Abs. 2 Satz 1 Nr. 3 HSOG). Straftaten mit erheblicher Bedeutung werden in § 13 Abs. 3 Satz 1 HSOG definiert, der einen breit angelegten Straftatenkatalog enthält.

§ 25a Abs. 4 HSOG regelt Zugriffskontrollen, die aus Protokollierungs- und Begründungspflichten bestehen.

Hervorzuheben ist, dass der Gesetzgeber in besonders großem Ausmaß von der vom Bundesverfassungsgericht vorgezeichneten Möglichkeit, technische und organisatorische Einzelheiten in Verwaltungsvorschriften zu regeln, Gebrauch gemacht hat. Der untergesetzliche Normgeber wird umfassend zum Erlass von Regelungen in einer Verwaltungsvorschrift ermächtigt (vgl. § 25a Abs. 3, Abs. 4 Satz 5 HSOG). Dies soll, ganz allgemein, die Zweckbindung sicherstellen (§ 25a Abs. 3 Satz 2 HSOG). Außerdem beinhaltet sie ein Rollen- und Rechtekonzept sowie ein Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten (§ 25a Abs. 3 Satz 3, Abs. 3 Nr. 1 und Nr. 2 HSOG) und soll die Einzelheiten der Zugriffskontrolle und des notwendigen Inhalts der Begründung durch Anwender*innen regeln (§ 25a Abs. 4 Satz 5 HSOG).

Die bereits in der alten Fassung (§ 25a Abs. 3 Satz 2 HSOG a.F.) enthaltene Pflicht zur Anhörung des*der Hessischen Datenschutzbeauftragten vor der Errichtung oder wesentlichen Änderung einer automatisierten Anwendung zur Datenanalyse (§ 25a Abs. 5 Satz 2 HSOG), wird in der neuen Fassung um die Klarstellung ergänzt, dass seine*ihre Aufgaben und Befugnisse im Übrigen unberührt bleiben (§ 25a Abs. 5 Satz 3 HSOG). Darüber hinaus ist nun auch der*die behördliche Datenschutzbeauftragte zu stichprobenartigen Kontrollen berechtigt (§ 25a Abs. 4 Satz 6 HSOG).

II. Die Beschwerdeführer*innen

1. Beschwerdeführerin zu 1

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2. Beschwerdeführer zu 2

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

3. Beschwerdeführer zu 3

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4. Beschwerdeführer zu 4

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

5. Beschwerdeführerin zu 5

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

6. Beschwerdeführerin zu 6

[REDACTED]

[REDACTED]

[REDACTED]

C. Zulässigkeit

Die Verfassungsbeschwerde ist zulässig.

I. Beschwerdebefugnis

Die Beschwerdeführer*innen sind im Sinne von § 90 Abs. 1 Bundesverfassungsgerichtsgesetz (BVerfGG) beschwerdebefugt. Sie sind selbst, gegenwärtig und unmittelbar von den Regelungen betroffen.

1. Verfassungsrechtliche Rügen

Die Beschwerdeführer*innen rügen eine Verletzung ihres Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG aufgrund der Möglichkeit, von einer Maßnahme nach § 25a HSOG betroffen zu sein (dazu **D.**). Daneben machen sie eine Verletzung ihres Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG geltend, da gem. § 25a Abs. 2 Satz 2 HSOG auch Daten aus Telekommunikationsüberwachungen in die Datenauswertung einfließen können (dazu insbesondere **D.I.2.a)(1)**).

Da die Beschwerdeführer*innen auch verfassungsrechtliche Defizite im Kontrollkonzept rügen, sind sie auch in Art. 19 Abs. 4 GG betroffen, da sich die entsprechenden Anforderungen aus dem jeweiligen Grundrecht in Verbindung mit Art. 19 Abs. 4 GG ergeben (dazu **D.II. 2.**),

vgl. BVerfGE 141, 220 (282 Rn. 134).

2. Eigene und gegenwärtige Betroffenheit

Die Beschwerdeführer*innen sind nach § 90 Abs. 1 BVerfGG auch selbst und gegenwärtig von § 25a HSOG betroffen.

Für die Darlegung der unmittelbaren sowie der eigenen und gegenwärtigen Betroffenheit gelten bei einer Verfassungsbeschwerde gegen eine gesetzliche

Ermächtigung zu heimlichen Überwachungsmaßnahmen besondere Anforderungen,

BVerfG, Beschluss des Ersten Senats vom 09. Dezember 2022, 1 BvR 1345/21, Rn. 41.

Zur Begründung der Möglichkeit eigener und gegenwärtiger Betroffenheit durch eine gesetzliche Ermächtigung zu heimlichen Überwachungsmaßnahmen, bei der die konkrete Beeinträchtigung zwar erst durch eine Vollziehung erfolgt, die Betroffenen in der Regel aber keine Kenntnis von Vollzugsakten erlangen, reicht es aus, wenn die Beschwerdeführer*innen darlegen, mit einiger Wahrscheinlichkeit durch auf den angegriffenen Rechtsnormen beruhende Maßnahmen in eigenen Grundrechten berührt zu werden,

BVerfG, Beschluss des Ersten Senats vom 09. Dezember 2022, 1 BvR 1345/21, Rn. 43; BVerfG, Beschluss des Ersten Senats vom 28. September 2022, 1 BvR 2354/13, Rn. 87; BVerfGE 155, 119 (160 Rn. 75).

Bei der automatisierten Anwendung zur Datenanalyse handelt es sich um eine heimliche Überwachungsmaßnahme, von der Betroffene in der Regel keine Kenntnis erlangen, sodass sie lediglich darlegen müssen, mit einiger Wahrscheinlichkeit durch § 25a HSOG in eigenen Grundrechten berührt zu werden.

Diese Wahrscheinlichkeit können die Beschwerdeführer*innen darlegen. Dabei sind folgende Betroffenheitskonstellationen denkbar: als Zielperson (dazu **a**) oder als drittbetroffene Person, das heißt als Kontaktperson oder als vollkommen unbeteiligte Person (dazu **b**)).

a) Als Zielperson

In besonderem Maße betroffen sind Zielpersonen der Analyse.

Es besteht eine hohe Wahrscheinlichkeit, dass die Beschwerdeführer*innen zu 2 bis 6 als Zielpersonen einer Analyse betroffen sind.

Dies ergibt sich insbesondere daraus, dass durch die Einbeziehung von Vorfeldtatbeständen die Eingriffsschwellen von § 25a Abs. 2 Satz 1 Nr. 2 und Nr. 3 weit ins Vorfeld einer Gefahr verlagert werden (dazu **D.II.1.a)(1)(a)**).

Dadurch erweitert sich der Kreis potenzieller Zielpersonen enorm. Eine tatbestandliche Eingrenzung ist kaum mehr vorhanden.

Die Beschwerdeführer*innen [REDACTED] sind mit einiger Wahrscheinlichkeit als Zielpersonen unmittelbar von der automatisierten Anwendung zur Datenanalyse betroffen, da sie aktivistisch tätig beziehungsweise in der Fanszene aktiv sind und sie bereits in der Vergangenheit häufiger in Kontakt mit der Polizei geraten sind, sodass mit einiger Wahrscheinlichkeit zu erwarten ist, dass sie auch künftig Überwachungsmaßnahmen, wie Maßnahmen nach § 25a HSOG, ausgesetzt sein werden.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b) Als Drittbetroffene

Werden gespeicherte Datenbestände mittels einer automatisierten Anwendung zur Datenanalyse 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.

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 50.

Gleiches gilt für Eingriffe in Art. 10 Abs. 1 GG, sofern Daten aus Telekommunikationsüberwachung und Verkehrsdaten einbezogen werden.

Für eine Betroffenheit ist es daher ausreichend, dass die eigenen Daten mit einiger Wahrscheinlichkeit in die Analyse einbezogen werden.

Betroffene müssen also selbst nicht unmittelbar Zielperson sein. Denn im Rahmen der Analyse dürfen die zusammengeführten Daten, auch gemeinsam mit weiteren rechtmäßig erhobenen personenbezogenen Daten, verknüpft, aufbereitet und ausgewertet sowie für statistische Zwecke angewendet werden (§ 25a Abs. 1 Satz 2 HSOG).

(1) Aufgrund der Streubreite

Für die Wahrscheinlichkeit eigener Betroffenheit der Beschwerdeführer*innen spricht schon die große Streubreite des § 25a HSOG. Eine solche ist gegeben, wenn die Maßnahme nicht auf einen tatbestandlich eng umgrenzten Personenkreis zielt, insbesondere wenn sie auch Dritte in großer Zahl zufällig erfassen kann,

vgl. BVerfG, Beschluss des Ersten Senats vom 09. Dezember 2022, 1 BvR 1345/21, Rn. 44.

Von einer großen Streubreite ist bei § 25a HSOG deshalb auszugehen, weil eine Vielzahl personenbezogener Daten Unbeteiligter, die nicht zwangsläufig Kontaktperson sind oder Anlass zur Überwachung gegeben haben, einbezogen werden (dazu ausführlich **D.I.2.a)(4)**). Die teilweise Beschränkung der Analyse durch § 25a Abs. 3 Nr. 2 lit. a Satz 4 HSOG hinsichtlich der einbezieharen Vorgangsdaten reicht nicht aus, um diese Beschwer entfallen zu lassen. Die Analyse von Verkehrsdaten ist lediglich hinsichtlich einer Tatbestandsvariante ausgeschlossen. Weitere Datenbestände – die ebenfalls Daten Unbeteiligter enthalten, wie beispielweise Daten aus Asservaten – sind hingegen gar nicht von der Analyse ausgeschlossen.

(2) Als Kontaktpersonen

Während damit bereits eine allgemein sehr hohe Chance besteht, als drittbetroffene Person von einer automatisierten Datenanalyse erfasst zu werden, ist diese Wahrscheinlichkeit hinsichtlich der Beschwerdeführer*innen zu [REDACTED] sogar noch weiter erhöht, da diese Kontaktpersonen von wahrscheinlichen Zielpersonen sind.

Das angerufene Gericht erkennt in seiner Rechtsprechung an, dass eine Verbindung zu Zielpersonen – sei sie politisch, beruflich oder privat – eine eigene Betroffenheit ergeben kann. Nicht erforderlich ist dabei der Vortrag von Informationen, die von einem Zeugnisverweigerungsrecht etwa nach §§ 52, 53, 53a StPO umfasst sind,

vgl. BVerfG, Beschluss des Ersten Senats vom 09. Dezember 2022, 1 BvR 1345/21, Rn. 44.

(a) Beschwerdeführer*innen zu 1 bis 3

Die Beschwerdeführerin zu 1 und der Beschwerdeführer zu 2 sind vor allem beruflich mit potenziellen Zielpersonen verbunden, da sie als Strafverteidiger*innen in Kontakt mit Personen stehen, deren Daten in verschiedenen Polizeidatenbanken gespeichert sind. Die Mandant*innen der Beschwerdeführerin zu 1 gelten für Sicherheitsbehörden zum Teil als sogenannte Gefährder*innen oder als Mitglieder terroristischer Vereinigungen. Auch der Beschwerdeführer zu 2 vertritt Personen, denen eine Beteiligung in ausländischen terroristischen Vereinigungen vorgeworfen wird, sowie viele Personen aus dem linken, insbesondere antifaschistischen Spektrum. Deshalb ist es wahrscheinlich, dass im Zuge einer Datenauswertung einer Zielperson auch die Daten der Beschwerdeführerin zu 1 und des Beschwerdeführers zu 2 als Beifang angezeigt werden. Dafür reicht unter Umständen schon eine Mailkommunikation mit der Zielperson, der Besuch der gleichen Veranstaltung oder die Nummer im Mobiltelefon der Zielperson. Da gerade in Ermittlungsverfahren zu §§ 129 ff. StGB umfangreiche und vor allem auch besonders intensive Überwachungsbefugnisse bestehen, die auch Art. 10 GG betreffen, ist es wahrscheinlich, dass auch Telekommunikationsdaten der Beschwerdeführer*innen betroffen sind.

Auch der Beschwerdeführer zu 3 ist als Kontaktperson zu qualifizieren. Sowohl im Rahmen seiner journalistischen Berichterstattung als auch seines privaten politischen Engagements hat er Kontakt mit vertraulichen Quellen und politischen Aktivist*innen. Auch für ihn besteht deshalb die erhöhte Wahrscheinlichkeit, dass er Beifang einer Datenanalyse nach § 25a HSOG wird. Angesichts dessen, dass der Beschwerdeführer fast ausschließlich per Mail oder Telefon kommuniziert, ist es wahrscheinlich, dass auch Telekommunikationsdaten einbezogen werden.

Zwar adressiert § 12a HSOG den Schutz zeugnisverweigerungsberechtigter Berufsheimnisträger*innen, zu denen die Beschwerdeführer*innen zu 1, 2,

und 3 gehören. Dieser ist aber nicht ausreichend, um Datenverarbeitungsmaßnahmen und somit die Betroffenheit der Beschwerdeführer*innen auszuschließen.

Die Beschwerdeführer*innen zu 1 und 2 sind als Strafverteidiger*innen nach § 53 Abs. 1 Satz 2 Nr. 2 StPO vom „absoluten“ Schutz des § 12a Abs. 1 HSOG erfasst; der Beschwerdeführer zu 3 als Journalist nach § 53 Abs. 1 Satz 2 Nr. 5 genießt „relativen“, also einer Abwägung zugänglichen Schutz gem. § 12a Abs. 2 HSOG. § 12a HSOG erfasst schon nicht § 25a HSOG, sondern lediglich die in § 12a Abs. 1 Satz 1 HSOG gelisteten Datenerhebungsmaßnahmen. Aber auch für die darin enthaltenen Erhebungsmaßnahmen ist nicht sichergestellt, dass im Ergebnis nicht doch Daten von Berufsheimnisträger*innen erhoben und somit in die Datenanalyse eingeführt werden können. Denn oft werden die Betroffenen eines Datenverarbeitungsvorgangs nicht oder nicht rechtzeitig als Berufsheimnisträger*innen identifiziert. Insbesondere, wenn Berufsheimnisträger*innen sich privat politaktivistisch engagieren, liegt es nahe, dass eine Unterscheidung zwischen beruflichen Kontexten und privaten Kontexten aus Sicht von Polizeibehörden nur schwer zu treffen ist. Beispielsweise beteiligt sich der Beschwerdeführer zu 2 selbst an zahlreichen Demonstrationen. Auch der Beschwerdeführer zu 3 hält zum Teil auch außerhalb seiner journalistischen Tätigkeit Kontakt zu Aktivist*innen, die Überwachungsmaßnahmen ausgesetzt sind.

Aber sogar für den Fall, dass Betroffene als Berufsheimnisträger*innen identifiziert werden, ist die Datenerhebung nicht vollkommen ausgeschlossen. Denn § 12a Abs. 1 HSOG verbietet die Erhebung nicht generell, sondern setzt voraus, dass die Maßnahme voraussichtlich Erkenntnisse erbringen würde, über die diese Person das Zeugnis verweigern dürfte.

Außerdem lassen auch das Verwertungsverbot gem. § 12a Abs. 1 Satz 2 HSOG und die Löschpflicht gem. § 12a Abs. 1 Satz 3 HSOG die Betroffenheit der Beschwerdeführer*innen zu 1 und 2 (Strafverteidiger*innen) nicht entfallen, da sie erst nachgelagert eingreifen und einen Missbrauch nicht sicher ausschließen können. Darüber hinaus erlaubt § 12a Abs. 4 HSOG für beide

Gruppen eine Ausnahme von den Schutzvorschriften, wenn Tatsachen die Annahme rechtfertigen, dass die zeugnisverweigerungsberechtigte Person die Gefahr verursacht hat. Vor dem Hintergrund des weiten Verständnisses des polizeirechtlichen Verursacherbegriffs, der auch Anscheinsstörer*innen erfasst oder lediglich einen Gefahrenverdacht ausreichen lassen kann, kann der Schutz von Berufsgeheimnisträger*innen mithin leicht unterlaufen werden,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 12a Rn. 36.

Dieselben Erwägungen gelten für Daten, die aus Strafverfahren stammen, sofern die fast gleichlautende Vorschrift des § 160a StPO einschlägig ist. Sofern § 160a Abs. 5 StPO andere Vorschriften unberührt lässt, erfasst insbesondere § 100g Abs. 4 StPO nur die Erhebung von nach § 176 Telekommunikationsgesetz (TKG) gespeicherten Daten. Außerdem verweist § 100g Abs. 4 Satz 6 StPO unter anderem auf § 160a Abs. 4 StPO, der eine Ausnahme bei möglicher Verstrickung vorsieht. Hingegen kann aus § 97 StPO ein geringeres Schutzniveau folgen,

Sackreuther, in: BeckOK StPO, 51. Ed. 1.1.2024, StPO § 160a Rn. 21 m.w.N.

(b) Beschwerdeführer*innen zu 5 und 6

Der Beschwerdeführer zu 5 und die Beschwerdeführerin zu 6 stehen privat in Kontakt mit Personen, die Ziel von Überwachungsmaßnahmen sind. Das zeigt sich für den Beschwerdeführer zu 5 insbesondere daran, dass er bereits Drittbetroffener verdeckter Überwachungsmaßnahmen war. Die Beschwerdeführerin zu 6 steht in Verbindung mit vielen Menschen aus der Fanszene, die im Visier von Polizeibehörden stehen. Es besteht daher eine erhöhte Wahrscheinlichkeit, dass sie nicht nur Ziel, sondern jedenfalls auch Beifang einer Datenanalyse nach § 25a HSOG sind. Da der Beschwerdeführer zu 5 bereits von Telekommunikationsüberwachungsmaßnahmen betroffen war, ist es wahrscheinlich, dass auch diese Daten in die Analyse einbezogen werden.

(3) Beschwerdeführer*innen mit nachweislich vorhandenen Daten

Da von den Beschwerdeführer*innen [REDACTED] nachweislich Daten vorhanden sind, ist es für sie nicht nur wahrscheinlich, sondern sogar sicher, dass sie von Datenanalysen betroffen sind beziehungsweise sein werden, da insbesondere ComVor, POLAS-HE und Crime-St gem. § 25a Abs. 2 Satz 2 HSOG einbezogen werden,

vgl. LT-Drs. 20/11235, S. 12 f.

Da im Bereich von Staatsschutzdelikten polizeiliche Befugnisse häufig Eingriffe in Art. 10 GG erlauben, ist es wahrscheinlich, dass auch Telekommunikationsdaten des Beschwerdeführers [REDACTED], der eine Eintragung in CRIME-St hat, vorliegen oder vorliegen werden, die in die Analyse einbezogen werden.

Teilweise reichen die Sachverhalte der Datenspeicherung zwar bereits einige Jahre zurück, allerdings sieht § 27 Abs. 2 Satz 1 Nr. 1 HSOG vor, dass eine Löschung erst erfolgt, wenn festgestellt wird, dass ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist oder gem. § 27 Abs. 2 Satz 1 Nr. 2 Hs. 1 HSOG die durch eine verdeckte Datenerhebung gewonnenen Daten für den der Anordnung zugrunde liegenden Zweck, zur Strafverfolgung oder zur Strafvollstreckung oder für eine etwaige gerichtliche Kontrolle nicht mehr erforderlich sind, soweit keine zulässige Weiterverarbeitung erfolgt. Es ist sehr wahrscheinlich, dass die Daten über die Aussonderungsprüffristen hinaus gespeichert werden. Denn Aussonderungsprüffristen stellen kein gesetztes Löschedatum dar, sondern gebieten lediglich eine Prüfung der Voraussetzungen einer weiteren Speicherung.

Weitere Darlegungen sind den Beschwerdeführer*innen weder möglich noch zumutbar. Insbesondere kann zum Beleg der eigenen gegenwärtigen Betroffenheit nicht verlangt werden, dass sich die Beschwerdeführer*innen selbst einer Straftat oder als mögliche Verursacher*innen einer Gefahr für die öffentliche Sicherheit bezichtigen,

vgl. BVerfG, Beschluss des Ersten Senats vom 09. Dezember 2022, 1 BvR 1345/21, Rn. 43; BVerfG, Beschluss des Ersten Senats vom 28. September 2022, 1 BvR 2354/13, Rn. 87; BVerfGE 133, 277 (312 f. Rn. 86).

3. Unmittelbare Betroffenheit

Die angegriffenen Vorschriften betreffen die Beschwerdeführer*innen auch unmittelbar.

Von einer unmittelbaren Betroffenheit durch ein vollziehungsbedürftiges Gesetz ist, obwohl dieses erst der Umsetzung durch Vollzugsakte bedarf, im Falle heimlicher Überwachungsmaßnahmen dennoch auszugehen, wenn Beschwerdeführer*innen den Rechtsweg nicht beschreiten können, weil sie keine Kenntnis von der Maßnahme erlangen oder wenn eine nachträgliche Bekanntgabe zwar vorgesehen ist, von ihr aber aufgrund weitreichender Ausnahmetatbestände auch langfristig abgesehen werden kann,

BVerfG, Beschluss des Ersten Senats vom 09. Dezember 2022, 1 BvR 1345/21, Rn. 42; BVerfG, Beschluss des Ersten Senats vom 28. September 2022, 1 BvR 2354/13, Rn. 85; BVerfG, Urteil des Ersten Senats vom 26. April 2022, 1 BvR 1619/17, Rn. 99; BVerfGE 155, 119 (159 Rn. 73).

Die Datenanalyse erfolgt ohne Kenntnis der Betroffenen. Eine spätere Kenntniserlangung ist auch nicht durch aktive Benachrichtigungspflichten sichergestellt. § 29 Abs. 1 HSOG verweist für Benachrichtigungen auf § 51 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDSIG), der wiederum in Absatz 1 voraussetzt, dass die Benachrichtigung in speziellen Rechtsvorschriften, insbesondere bei verdeckten Maßnahmen, vorgesehen oder angeordnet ist. In diesem Sinne sieht § 29 Abs. 5 Satz 1 HSOG Benachrichtigungen für die in § 28 Abs. 2 HSOG genannten Maßnahmen vor. § 25a HSOG ist dort aber nicht aufgelistet. Im Übrigen bestehen weitreichende Zurückstellungsmöglichkeiten und Ausnahmen nach § 29 Abs. 6 und Abs. 7 HSOG.

Falls für § 25a HSOG überhaupt ein Auskunftsanspruch gem. § 29 Abs. 1 i.V.m. § 52 Abs. 1 HDSIG besteht, gewährt er jedenfalls keine Möglichkeit, mit Gewissheit über eine Datenanalyse informiert zu werden, da er gem. § 29 Abs. 1 HSOG i.V.m. § 52 Abs. 4 HDSIG i.V.m. § 51 Abs. 2 HDSIG weitreichende Möglichkeiten vorsieht, von der Auskunft abzusehen oder sie einzuschränken. Die Auskunft hätte mithin nur begrenzte Aussagekraft. Betroffene müssen auch nicht zwangsläufig darüber unterrichtet werden, dass von der Auskunft abgesehen oder die Auskunft eingeschränkt wurde (vgl. § 52 Abs. 6 Satz 2 HDSIG). Darüber hinaus ist es für potenziell Betroffene nicht zumutbar, fortlaufend Auskunftersuchen zu initiieren, um im Falle einer positiven Auskunft Rechtsschutz zu suchen.

II. Subsidiarität

Gegen formelle Gesetze ist ein Rechtsweg nicht gegeben, weshalb § 90 Abs. 2 Satz 1 BVerfGG der Verfassungsbeschwerde nicht entgegensteht. Auch der Grundsatz der Subsidiarität steht der Zulässigkeit nicht entgegen. Dieser erfordert grundsätzlich vor Einlegung einer Verfassungsbeschwerde alle zur Verfügung stehenden prozessualen Möglichkeiten zu ergreifen, um eine Korrektur der geltend gemachten Verfassungsverletzung zu erwirken oder eine Grundrechtsverletzung zu verhindern. Das gilt auch, wenn zweifelhaft ist, ob ein entsprechender Rechtsbehelf statthaft ist und er im konkreten Fall in zulässiger Weise eingelegt werden kann,

BVerfG, Beschluss des Ersten Senats vom 09. Dezember 2022, 1 BvR 1345/21, Rn. 45.

Ausnahmen bestehen unter anderem, soweit die Beurteilung einer Norm allein spezifisch verfassungsrechtliche Fragen aufwirft, die das Bundesverfassungsgericht zu beantworten hat, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung verbesserte Entscheidungsgrundlagen zu erwarten wären oder wenn die Anrufung der Fachgerichte offensichtlich sinn- und aussichtslos wäre oder sie sonst nicht zumutbar ist,

BVerfG, Beschluss des Ersten Senats vom 09. Dezember 2022, 1 BvR 1345/21, Rn. 47.

Diese beiden Ausnahmen sind vorliegend gegeben.

1. Vorbeugender Rechtsschutz

Eine Anrufung der Fachgerichte im vorbeugenden Rechtsschutz wäre sinn- und aussichtslos, da eine vorbeugende Unterlassungs- oder Feststellungsklage unzulässig wäre. Diese würde vielmehr erfordern, dass die Beschwerdeführer*innen ein konkretes behördliches Verfahren bezeichnen können,

vgl. zur vorbeugenden Unterlassungsklage BVerwG, Urteil vom 19. März 1974 – 1 C 7.73; Beschluss vom 30. September 1981 – 3 B 39.81; Urteil vom 13. Dezember 2017 – 6 A 6.16 Rn. 12; Urteil vom 25. Januar 2023 – 6 A 1/22; Urteil vom 9. November 2023 – 10 A 3/23; *Pietzcker/Marsch*, in: Schoch/Schneider, VwGO, 44. EL März 2023, § 42 Abs. 1 Rn. 163;

vgl. zur Feststellungsklage BVerwG, Urteil vom 17. Januar 1980 – 7 C 63.77; Urteil vom 7. Mai 1987 – 3 C 53/85; Urteil vom 30. Mai 2018 – 6 A 3/16, juris Rn. 53; *Marsch*, in: Schoch/Schneider, VwGO, 44. EL März 2023, § 43 Rn. 17 ff.

Eine Klage „ins Blaue hinein“ ist hingegen unzulässig.

Kenntnis von einem laufenden Verfahren können die Betroffenen bezüglich der Datenanalyse frühestens erlangen, wenn die Hessische Polizei offene Gefahrenabwehrmaßnahmen durchführt oder das Verfahren in ein offenes strafrechtliches Ermittlungsverfahren überleitet. Dies wird allerdings keineswegs in jedem Fall geschehen. Zudem wird die Datenanalyse zu diesem Zeitpunkt bereits abgeschlossen sein, sodass ein vorbeugender Rechtsschutz zu spät käme.

Außerdem wirft die Beurteilung der Norm allein spezifisch verfassungsrechtliche Fragen auf, die das Bundesverfassungsgericht zu

beantwortet hat, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung verbesserte Entscheidungsgrundlagen zu erwarten wären.

Denn die Beschwerdeführer*innen rügen neben der Verletzung von Grundrechten insbesondere einen Verstoß gegen den Gesetzesvorbehalt sowie den Grundsatz der Normenklarheit und Bestimmtheit. Dabei handelt es sich um rein verfassungsrechtliche Fragestellungen, die das Bundesverfassungsgericht zu beantworten hat. Die verfassungsrechtliche Beurteilung hängt nicht von der Klärung von Tatsachen oder der fachrechtlichen Auslegung der einzelnen Tatbestandsmerkmale der angegriffenen Befugnisse ab, sondern maßgeblich von deren hinreichender gesetzlicher Begrenzung, Anleitung und Bestimmtheit.

2. Vorgehen gegen Verwaltungsvorschriften

Abgesehen davon, dass ein fachgerichtliches Vorgehen gegen Verwaltungsvorschriften im Wege von § 47 Abs. 1 Nr. 2 VwGO nur in absoluten Ausnahmefällen möglich ist,

Giesberts, in: BeckOK VwGO, 69. Ed. 1.4.2024, VwGO § 47 Rn. 29 m.w.N.;

Panzer/Schoch, in: Schoch/Schneider, 44. EL März 2023, VwGO § 47 Rn. 25 ff.,

ist es unter Subsidiaritätsgesichtspunkten auch nicht geboten, zunächst fachgerichtlich gegen die Verwaltungsvorschrift zur Ausführung des § 25a des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (VV § 25a HSOG) vorzugehen, da es allein um die bereits genannten spezifisch verfassungsrechtlichen Fragestellungen geht. Ein fachgerichtlicher Rechtsschutz in Form einer Normenkontrolle könnte zu dieser Klärung nicht beitragen.

3. Nachträglicher Rechtsschutz

Mangels Benachrichtigungspflicht und hinreichender Auskunftsmöglichkeiten ist auch kein nachträglicher Rechtsschutz gegen die automatisierte Anwendung zur Datenanalyse möglich oder zumutbar (siehe oben **C.I.3.**).

III. Beschwerdefrist

Die Jahresfrist des § 93 Abs. 3 BVerfGG ist gewahrt. Das HSOG, zuletzt geändert durch Art. 2, Art. 4 des Gesetzes zur Änderung sicherheitsrechtlicher Vorschriften und zur Umorganisation der hessischen Bereitschaftspolizei vom 29. Juni 2023 (GVBl. S. 456), ist hinsichtlich der anzugreifenden Regelung gem. Artikel 9 des Änderungsgesetzes am Tag nach der Verkündung und damit am 12. Juli 2023 in Kraft getreten. Die Jahresfrist endet folglich mit dem 11. Juli 2024.

D. Begründetheit der Verfassungsbeschwerde

Die Verfassungsbeschwerde ist begründet.

Bei § 25a Abs. 2 Satz 1 Nr. 1 bis Nr. 3 HSOG handelt es sich um schwerwiegende Eingriffe in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sowie in Art. 10 GG (**D.I.**), die den hier geltenden strengen Anforderungen des Gebots der Verhältnismäßigkeit, wie sie das angerufene Gericht im Datenanalyse-Urteil näher konturiert hat, nicht genügen (**D.II.**) und die Beschwerdeführer*innen deshalb in ihren Grundrechten verletzen.

I. Schwerwiegender Eingriff mangels wirksamer Reduzierung des Eingriffsgewichts

Unter Berücksichtigung des Maßstabs für die Beurteilung der Eingriffsintensität (**1.a**) und unter Berücksichtigung der Wesentlichkeitstheorie sowie den Grundsätzen der Bestimmtheit und Normenklarheit (**1.b**) enthält § 25a HSOG keine ausreichenden Einschränkungen (**2.**), die dazu führen, dass die Möglichkeiten der Erkenntnisgewinnung so eingegrenzt sind, dass kein besonders schwerer eigenständiger Eingriff in die informationelle Selbstbestimmung der Betroffenen erfolgen kann. Vielmehr handelt es sich bei allen Tatbestandsvarianten des § 25a Abs. 2 Satz 1 HSOG um schwere Eingriffe in die informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sowie in Art. 10 Abs. 1 GG und Art. 19 Abs. 4 GG.

1. Maßstab

§ 25a HSOG ist an den im Datenanalyse-Urteil präzisierten Kriterien für die Bestimmung des Eingriffsgewichts (**a**) sowie an der Wesentlichkeitstheorie sowie den Grundsätzen der Bestimmtheit und Normenklarheit zu messen (**b**).

a) Kriterien für die Bestimmung des Eingriffsgewichts

Das Eingriffsgewicht ergibt sich erstens aus dem Gewicht der zusammenführenden Weiterverwendung vormals getrennter Daten und zweitens daraus, dass Anwendungen zur automatisierten Datenanalyse ein potenzielles Eigengewicht haben, wenn dadurch neue Erkenntnisse über Personen gewonnen werden können,

vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 50,

da somit neue Belastungseffekte entstehen, wodurch sich das Gewicht der individuellen Beeinträchtigung bedeutend erhöhen kann,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 66 ff.

Das Eingriffsgewicht hängt von verschiedenen Faktoren ab und kann demgemäß vom Gesetzgeber durch unterschiedliche Vorkehrungen und Kombinationen von Schutzmechanismen beeinflusst werden,

vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 75.

Wie schwer das Eigengewicht der automatisierten Anwendung zur Datenanalyse im Einzelfall wiegt, lässt sich anhand bestimmter Kriterien bestimmen, die das angerufene Gericht näher beschrieben hat: Das Eingriffsgewicht wird vor allem durch Art und Umfang der verarbeitbaren Daten sowie die zugelassene Methode der Datenanalyse bestimmt. 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,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 78.

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,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 78.

Besonderes Eingriffsgewicht kann der Einsatz komplexer Formen des Datenabgleichs haben,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 90.

Insgesamt ist die Methode automatisierter Datenanalyse oder -auswertung umso eingriffintensiver, 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,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 90.

Durch Begrenzungen der Art und des Umfangs der verarbeitbaren Daten sowie der Methoden kann der Gesetzgeber die Eingriffsintensität mithin steuern.

b) Wesentlichkeit, Bestimmtheit, Normenklarheit

Derartige Beschränkungen sind aber nur dann wirksam, wenn sie unter Wahrung des Gesetzesvorbehalts normenklar und hinreichend bestimmt sind,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 110 ff.

Diese allgemeingültigen Grundsätze **((1))** muss der Gesetzgeber einhalten, um eine verfassungskonforme Regelung zu gewährleisten. Im Hinblick auf die Befugnis zum Einsatz automatisierter Anwendungen zur Datenanalyse hat das angerufene Gericht diese Grundsätze konkretisiert **((2))**.

(1) Generelle Grundsätze

(a) Wesentlichkeitstheorie

In ständiger Rechtsprechung hat das Bundesverfassungsgericht aus grundrechtlichen Gesetzesvorbehalten und dem Rechtsstaatsprinzip (Art. 20 Abs. 3 GG) sowie dem Demokratieprinzip (Art. 20 Abs. 1 und 2 GG) die Verpflichtung des Gesetzgebers abgeleitet, in allen grundlegenden normativen Bereichen die wesentlichen Entscheidungen selbst zu treffen,

z.B. BVerfGE 150, 1 (96 Rn. 191 m.w.N.); grundlegend schon BVerfGE 33, 125 (159 ff., insb. 163); BVerfGE 40, 237 (248 f. Rn. 45); BVerfGE 49, 89 (126 Rn. 76); *Denninger*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Auflage 2021, B. Rn. 58; zur historischen Entwicklung in der Rechtsprechung des BVerfG eingehend *Lassahn*, Rechtsprechung und Parlamentsgesetz, 2017, S. 77 ff.

Die rechtsstaatliche Anbindung des Vorbehalts des Gesetzes stellt auf Transparenz, Vorhersehbarkeit und Kontrollierbarkeit ab. Die demokratische Rückkopplung gewährleistet, dass die grundlegenden Entscheidungen vom Parlament als einzig unmittelbar demokratisch legitimiertes Staatsorgan getroffen werden,

vgl. *Gärditz*, in: Friauf/Höfling, GG, 42. EL Dezember 2023, Art. 20 (6. Teil) Rn. 130 ff.; *Rux*, in: BeckOK GG, 57. Ed. 15.1.2024, Art. 20 Rn. 173.

Die Wesentlichkeitstheorie bestimmt nicht nur, dass eine parlamentarische Regelung notwendig ist, sondern gleichzeitig auch deren Reichweite.

Denn die Qualifikation einer Regelung als „wesentlich“ hat typischerweise ein Verbot der Normdelegation und ein Gebot größerer Regelungsdichte durch den parlamentarischen Gesetzgeber zur Folge,

BVerfGE 150, 1 (97 f. Rn. 195).

Wann es einer Regelung durch den parlamentarischen Gesetzgeber bedarf, lässt sich nur mit Blick auf den jeweiligen Sachbereich und auf die Eigenart des betroffenen Regelungsgegenstandes beurteilen. Die verfassungsrechtlichen

Wertungskriterien sind dabei den tragenden Prinzipien des Grundgesetzes, insbesondere den darin verbürgten Grundrechten, zu entnehmen,

BVerfGE 150, 1 (97 Rn. 193); BVerfGE 139, 19 (45 Rn. 52); BVerfGE 108, 282 (311 f. Rn. 68); BVerfGE 98, 218 (251 Rn. 137).

Wesentlich im grundrechtsrelevanten Bereich bedeutet nach der Rechtsprechung des angerufenen Gerichts „wesentlich für die Verwirklichung der Grundrechte“,

BVerfGE 150, 1 (97 Rn. 194); BVerfGE 139, 19 (45 Rn. 52); BVerfGE 98, 218 (251 Rn. 137); BVerfGE 47, 46 (79 Rn. 117).

Als wesentlich sind also Regelungen zu verstehen, die für die Verwirklichung von Grundrechten erhebliche Bedeutung haben und sie besonders intensiv betreffen,

BVerfGE 139, 19 (45 Rn. 52 m.w.N.).

Darüber hinaus stellt das angerufene Gericht auch auf staatsorganisationsrechtliche prozedurale Gründe ab, die für eine Regelung durch das Parlament sprechen: Damit soll gewährleistet werden, dass Entscheidungen von besonderer Tragweite aus einem Verfahren hervorgehen, das der Öffentlichkeit Gelegenheit bietet, ihre Auffassungen auszubilden und zu vertreten und das die Volksvertretung dazu anhält, Notwendigkeit und Ausmaß von Grundrechtseingriffen in öffentlicher Debatte zu klären. Geboten ist ein Verfahren, das sich durch Transparenz auszeichnet und die Beteiligung der parlamentarischen Opposition gewährleistet,

BVerfGE 150, 1 (96 f. Rn. 192); BVerfGE 139, 19 (46 Rn. 53); BVerfGE 108, 282 (312 Rn. 68); BVerfGE 85, 386 (403 f. Rn. 66).

Hingegen ist ein umfassender Parlamentsvorbehalt aber abzulehnen, weil der Grundsatz der Gewaltenteilung auch darauf zielt, dass staatliche Entscheidungen möglichst richtig, das heißt von den Organen getroffen werden, die dafür nach ihrer Organisation, Zusammensetzung, Funktion und Verfahrensweise über die besten Voraussetzungen verfügen,

BVerfGE 150, 1 (99 Rn. 197); BVerfGE 98, 218 (251 f. Rn. 137).

Mithin bezieht das angerufene Gericht auch funktionale Erwägungen mit ein, um zu beurteilen, ob es eines Parlamentsgesetzes bedarf,

vgl. *Lassahn*, Rechtsprechung und Parlamentsgesetz, 2017, S. 85 f.

Für die Bedeutung untergesetzlicher Normen folgert das angerufene Gericht, dass grundsätzlich zwar auch Gesetze, die zu (ergänzenden) Rechtsverordnungen und Satzungen ermächtigen, den Voraussetzungen des Gesetzesvorbehalts genügen können, die wesentlichen Entscheidungen aber durch den parlamentarischen Gesetzgeber selbst erfolgen müssen,

BVerfGE 150, 1 (98 Rn. 195); BVerfGE 139, 19 (47 Rn. 54).

Die Wesentlichkeitsdoktrin wird in der Literatur zum Teil dahingehend kritisiert, dass es sich um ein vages Abgrenzungskriterium handele,

Sachs, in: ders., GG, 9. Aufl. 2021, Art. 20 Rn. 116; *Kotzur*, in: v. Münch/Kunig, GG, 7. Aufl. 2021, Art. 20 Rn. 158; *Leisner*, in: Sodan, GG, 4. Aufl. 2018, Art. 20 Rn. 50; *Schulze-Fielitz*, in: Dreier, GG, 3. Aufl. 2015, Bd. 2, Art. 20 (Rechtsstaat) Rn. 113: „nicht eindeutig“.

Sie erfährt aber grundsätzlich Zustimmung,

Gärditz, in: Friauf/Höfling, GG, 42. EL Dezember 2023, Art. 20 (6. Teil) Rn. 144; *Rux*, in: BeckOK GG, 57. Ed. 15.1.2024, Art. 20 Rn. 176.1; vgl. *Sommermann*, in: Huber/Voßkuhle, GG, 8. Aufl. 2024, Art. 20 Rn. 273 ff.; vgl. *Jarass*, in: ders./Pieroth, GG, 18. Aufl. 2024, Art. 20 Rn. 71.

Während der Wesentlichkeitsbegriff teilweise lediglich paraphrasiert und mit dem Begriff der Wichtigkeit gleichgesetzt wird, wozu sehr intensive grundrechtliche Eingriffe und die Harmonisierung miteinander kollidierender Grundrechte gehörten,

Mann, in: Sachs, GG, 9. Aufl. 2021, Art. 80 Rn. 22,

kommt vor allem funktionalen Erwägungen besondere Bedeutung zu.

Da materielle Gesetzgebung auf abstrakt-generelle Regelungen ziele, setze eine Regelung durch den Gesetzgeber voraus, dass der potenzielle Regelungsgegenstand überhaupt einer sachgerechten Abstrahierung und Generalisierung zugänglich sei,

vgl. *Gärditz*, in: Friauf/Höfling, GG, 42. EL Dezember 2023, Art. 20 (6. Teil) Rn. 151.

Geboten sei eine Präzisierung der Wesentlichkeitsdoktrin durch funktionsadäquate Abgrenzungskriterien,

Gärditz, in: Friauf/Höfling, GG, 42. EL Dezember 2023, Art. 20 (6. Teil) Rn. 144.

Dies ermögliche eine sachgerechte funktionale Zuordnung von Regelungsbedürfnissen zu Regelungsebenen,

vgl. *Gärditz*, in: Friauf/Höfling, GG, 42. EL Dezember 2023, Art. 20 (6. Teil) Rn. 144; *Grzeszick*, in: Dürig/Herzog/Scholz, GG, 103. EL Januar 2024, Art. 20 VI Rn. 87.

Zum Teil werden konkrete Kriterien benannt: Unter anderem die Grundrechtsrelevanz, die Größe des Adressat*innenkreises, die Langfristigkeit einer Festlegung, gravierende finanzielle Auswirkungen, erhebliche Auswirkungen auf das Staatsgefüge, Konkretisierungen offenen Verfassungsrechts sowie, im Gegensatz zur Ansicht des angerufenen Gerichts,

BVerfGE 139, 19 (45 f. Rn. 52); BVerfGE 49, 89 (126 Rn. 73); BVerfGE 98, 218 (251 Rn. 137); BVerfGE 108, 282 (312 Rn. 68); BVerfGE 150, 1 (97 Rn. 194)

möglicherweise die politische Wichtigkeit oder Umstrittenheit sprächen für die Wesentlichkeit einer Angelegenheit. Gegen die Wesentlichkeit einer Frage sprächen hingegen unter anderem die Erforderlichkeit flexibler Regelungen, das Vorliegen entwicklungsöffener Sachverhalte, die Entlastung des Parlaments, das Bedürfnis nach dezentraler Regelung und bundesstaatlicher Koordinierung, das Einräumen von Beteiligungsrechten für die von der

Regelung Betroffenen sowie – möglicherweise – die Grenzen des Sachverstands des Parlaments,

Grzeszick, in: Dürig/Herzog/Scholz, GG, 103. EL Januar 2024, Art. 20 VI Rn. 107 m.w.N.; *Kalscheuer/Jacobsen*, DÖV 2018, 523 (525 f.).

Zum Teil wird die Wesentlichkeitstheorie als Abwägungstheorie verstanden: Die Grundrechtsrelevanz im Sinne der Eingriffsintensität sei nur ein Kriterium unter vielen, die abgewogen werden müssten, und sei deshalb nicht mit der Wesentlichkeit per se gleichzusetzen,

Kalscheuer/Jacobsen, DÖV 2018, 523 (528), vgl. *Grzeszick*, in: Dürig/Herzog/Scholz, GG, 103. EL Januar 2024, Art. 20 VI Rn. 109.

Es sei eine Gesamtbewertung erforderlich. In Grenzfällen könnten „Defizite“ hinsichtlich des Grads der Betroffenheit durch einen „Überschuss“ in Bezug auf die Bedeutung der Rechtsgüter ausgeglichen werden,

Sommermann, in: Huber/Voßkuhle, GG, 8. Aufl. 2024, Art. 20 Rn. 279.

Technische Detailfragen, die sich bereits ihrem Gegenstand nach nicht sinnvoll in Gesetzesform gießen ließen, bedürften keiner spezifizierten gesetzlichen Grundlage. Das parlamentarische Gesetzgebungsverfahren könne keinen sinnvollen Beitrag leisten, im weiteren Sinne unpolitische, technische Detailfragen sachgerecht zu erfassen und zu entscheiden,

Gärditz, in: Friauf/Höfling, GG, 42. EL Dezember 2023, Art. 20 (6. Teil) Rn. 152.

Wenn Regelungen auf fortwährende Aktualität angewiesen seien, genüge aus funktionalen Gründen eine untergesetzliche Regelung durch den Verordnungsgeber,

Gärditz, in: Friauf/Höfling, GG, 42. EL Dezember 2023, Art. 20 (6. Teil) Rn. 142.

Gerade auch bei Sachverhalten, die sich rasch änderten, könne dies im Sinne eines dynamischen Grundrechtsschutzes liegen,

Rux, in: BeckOK GG, 57. Ed. 15.1.2024, Art. 20 Rn. 180.

Denn der Verordnungsgeber könne die Regelungen rascher und einfacher auf dem neusten Stand halten,

BVerfGE 150, 1 (102 Rn. 204).

(b) Bestimmtheit

Die Wesentlichkeitsdoktrin beantwortet nicht nur die Frage, ob überhaupt ein bestimmter Gegenstand gesetzlich zu regeln ist. Sie ist vielmehr auch dafür maßgeblich, wie genau diese Regelungen im Einzelnen sein müssen,

BVerfGE 139, 19 (47 Rn. 54); BVerfGE 150, 1 (98 Rn. 196).

Denn der parlamentarische Gesetzgeber darf sich seiner Regelungsverantwortung nicht entziehen, indem er zwar ein Gesetz beschließt, dieses aber inhaltlich so vage fasst, dass die sachliche Entscheidung letztlich den gesetzesanwendenden Gewalten obliegt,

Rux, in: BeckOK GG, 57. Ed. 15.1.2024, Art. 20 Rn. 179.

Das Erfordernis der hinreichenden Bestimmtheit der Ermächtigungsgrundlage bei Delegation einer Entscheidung stellt insoweit eine notwendige Ergänzung und Konkretisierung des Gesetzesvorbehalts und des Grundsatzes der Gesetzmäßigkeit der Verwaltung dar,

BVerfGE 139, 19 (47 Rn. 54).

Das soll bei Grundrechtseingriffen die Rechte des demokratisch gewählten Parlaments sichern, der Exekutive begrenzende Handlungsmaßstäbe liefern, den Gerichten eine wirksame Rechtskontrolle ermöglichen und dem Bürger erlauben, sich auf belastende Maßnahmen einzustellen,

Jarass, in: ders./Pieroth, GG, 18. Aufl. 2024, Art. 20 Rn. 79; *Gärditz*, in: Friauf/Höfling, GG, 42. EL Dezember 2023, Art. 20 (6. Teil), Rn. 137.

Die durch den Vorbehalt des Gesetzes vorgegebene Bestimmtheit des förmlichen Gesetzes überschneidet sich in weitem Umfang mit dem allgemeinen rechtsstaatlichen Bestimmtheitsgebot,

Jarass, in: ders./Pieroth, GG, 18. Aufl. 2024, Art. 20 Rn. 78; vgl. *Rux*, in: BeckOK GG, 57. Ed. 15.1.2024, Art. 20 Rn. 182;

kann aber darüber hinausgehen,

Grzeszick, in: Dürig/Herzog/Scholz, 103. EL Januar 2024, Art. 20 VI Rn. 75.

Der Grad der verfassungsrechtlich gebotenen Bestimmtheit hängt dabei von den Besonderheiten des in Rede stehenden Sachbereichs und von den Umständen ab, die zu der gesetzlichen Regelung geführt haben.

BVerfGE 150, 1 (98 Rn. 196).

Die Bestimmtheit der Ermächtigungsnorm muss insbesondere der Grundrechtsrelevanz der Regelung entsprechen, zu der ermächtigt wird: Je erheblicher diese in die Rechtsstellung des Betroffenen eingreift, desto höhere Anforderungen müssen an den Bestimmtheitsgrad der Ermächtigung gestellt werden.

BVerfGE 139, 19 (47 Rn. 55); vgl. *Hopfauf*, in: Schmidt-Bleibtreu/Hofmann/Henneke, GG, 15. Aufl. 2021, Einleitung Rn. 280; *Kotzur*, in: v. Münch/Kunig, GG, 7. Aufl. 2021, Art. 20 Rn. 155.

Darüber hinaus sind die Bedeutung des Regelungsgegenstandes und die Intensität der durch die Regelung oder aufgrund der Regelung erfolgenden Grundrechtseingriffe ebenso zu berücksichtigen wie der Kreis der Anwender*innen und Betroffenen der Norm sowie deren konkretes Bedürfnis, sich auf die Normanwendung einstellen zu können,

BVerfGE 150, 1 (98 Rn. 196 m.w.N.).

Auch nach dem allgemeinen Bestimmtheitsgrundsatz müsse sichergestellt bleiben, dass das Handeln der Verwaltung messbar und in gewissem Ausmaße für Bürger*innen voraussehbar und berechenbar sei sowie, dass eine Gerichtskontrolle ermöglicht werde,

Rux, in: BeckOK GG, 57. Ed. 15.1.2024, Art. 20 Rn. 182 m.w.N.; *Schulze-Fielitz*, in: Dreier, GG, 3. Aufl. 2015, Bd. 2, Art. 20 (Rechtsstaat) Rn. 129.

Er soll gewährleisten, dass die Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinde und dass die Gerichte eine wirksame Rechtskontrolle durchführen können,

BVerfGE 150, 1 (98 Rn. 196); *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Henneke, GG, 15. Aufl. 2021, Art. 20 Rn. 89; vgl. *Lassahn*, Rechtsprechung und Parlamentsgesetz, 2017, S. 88 f.

Schon aus der parlamentarischen Leitentscheidung der Ermächtigung müsse erkennbar und vorhersehbar sein, was dem Bürger gegenüber zulässig sein soll,

BVerfGE 139, 19 (47 Rn. 55).

Bei komplexen Risiko- und Abwägungsentscheidungen genüge es, dass der Gesetzgeber die inhaltlichen Grundlinien der Rechtsgüterabwägungen vorentscheide, Entscheidungsfreiräume der Verwaltung präzisiere und im Übrigen die Mindestvoraussetzungen für eine geordnete Entscheidungsfindung im Verwaltungsverfahren gesetzlich anordne und organisatorische Voraussetzungen für eine hinreichend transparente Beteiligung von Sachverständigengremien schaffe. An die Stelle einer spezifischen einzelnen Eingriffsermächtigung trete dann ein abgestimmtes System aus Abwägungsdirektiven, Organisations- und Verfahrensvorschriften. Beispielhaft dafür sei das Umweltrecht: Dort werde Wesentliches, wie immissionsrechtliche Grenzwerte, nicht im Gesetz, sondern in exekutiven Normen geregelt. Dies kehre die Wesentlichkeitsdoktrin gewissermaßen um, um auf einen unsicheren oder sich rasch verändernden Kenntnisstand flexibel und schnell reagieren zu können,

Grzeszick, in: Kahl/Ludwigs, Handbuch des Verwaltungsrechts Band III, 1. Aufl. 2022, § 72 Rn. 30; *ders.*, in: Dürig/Herzog/Scholz, GG, 103. EL Januar 2024, Art. 20 VI Rn. 115 f.

(c) Normenklarheit

Eng mit dem Bestimmtheitsgrundsatz zusammen hängt auch das Gebot der Normenklarheit. Nach der jüngeren Rechtsprechung des Bundesverfassungsgerichts steht bei dem Gebot der Normenklarheit die

inhaltliche Verständlichkeit einer Regelung im Vordergrund, insbesondere damit Bürger*innen sich auf mögliche belastende Maßnahmen einstellen könnten,

BVerfG, Beschluss vom 28. September 2022, 1 BvR 2354/13, Rn. 110;
Hofmann, in: Schmidt-Bleibtreu/Hofmann/Henneke, GG, 15. Aufl. 2021,
Art. 20 Rn. 89, 91; vgl. *Sommermann*, in: Huber/Voßkuhle, GG, 8. Aufl.
2024, Art. 20 Rn. 289.

Hierin unterscheidet es sich von dem Bestimmtheitsgrundsatz, der sich auf die Perspektive von Regierung, Verwaltung und Gerichten bezieht. Bei der heimlichen Datenerhebung und -verarbeitung, die tief in die Privatsphäre einwirken können, ergeben sich aus dem Gebot der Normenklarheit besonders strenge Anforderungen. Da die Handhabung hierauf bezogener Ermächtigungen von den Betroffenen weitgehend nicht wahrgenommen und angegriffen werden kann, kann ihr Gehalt nur sehr eingeschränkt im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden,

eingehend BVerfG, Beschluss vom 28. September 2022, 1 BvR 2354/13,
Rn. 110 ff.

Somit sind Gesetzesvorbehalt, Bestimmtheitsgrundsatz und der Grundsatz der Normenklarheit eng miteinander verzahnt.

(2) Konkret im Hinblick auf Datenanalyse

Ausgehend von diesen, der Rechtsprechung des angerufenen Gerichts entwachsenen Grundsätzen findet im Datenanalyse-Urteil zum Teil eine Konkretisierung statt.

Der Gesetzgeber müsse die wesentlichen Grundlagen zur Begrenzung von Art und Umfang der Daten und der Verarbeitungsmethoden selbst durch Gesetz vorgeben,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 112.

Wegen der besonderen Technizität und der raschen Fortentwicklungsbedürftigkeit der hier zur Milderung des Eingriffs benötigten Regelungen könne er, soweit eine tiefere gesetzliche Normierung nicht praktikabel erscheine, die Verwaltung zur näheren Regelung organisatorischer und technischer Einzelheiten ermächtigen. Er müsse 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 seien,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 112.

Somit ist eine Delegation der Regelungsaufgabe an die Verwaltung grundsätzlich möglich. Dennoch steht eine solche unter der Prämisse der Wahrung oben genannter Grundsätze, insbesondere des Vorbehalts des Gesetzes, worauf das angerufene Gericht im Datenanalyse-Urteil an mehreren Stellen explizit hinweist,

vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR
1547/19, 1 BvR 2634/20, Rn. 110, 112, 113 f., 165.

Unter Einbeziehung auch oben genannter genereller verfassungsrechtlicher Grundsätze verdichtet sich der auf den untergesetzlichen Normgeber übertragbare Regelungsbereich mithin auf organisatorische und technische Einzelheiten. Diese kommen in Betracht, um gesetzgeberisch angeleitete Maßstäbe zu konkretisieren und standardisieren. Dies betrifft aus funktionalen Erwägungen vor allem die technischen und organisatorischen Einzelheiten, da diese dafür geeignet sind, das Gesetz in die praktischen Abläufe zu integrieren. Insbesondere die technischen Details können sich je nach eingesetzter Software und damit verbundener Updates kurzfristig ändern, sodass es aus funktionalen Gründen sachgerecht erscheint, der Verwaltung dafür die Regelungskompetenz einzuräumen. Diese Regelungskompetenz reicht aber gerade nur soweit es nicht praktikabel wäre, derartige Einzelheiten im Gesetz selbst zu regeln.

Geht es hingegen darum, die Grenzen der Eingriffsbefugnis festzulegen, ist ausschließlich der parlamentarische Gesetzgeber selbst zur Regelung befugt.

Für eine hohe Regelungsdichte des parlamentarischen Gesetzes spricht zunächst die Grundrechtsrelevanz. § 25a HSOG ist eine hohe Eingriffsintensität beizumessen, da die automatisierte Anwendung zur Datenanalyse potenziell schwerwiegend in Grundrechte eingreift. Aber auch im Hinblick darauf, dass Rechtsschutz gegen heimliche Überwachungsmaßnahmen faktisch ausgeschlossen ist, ist es für die Verwirklichung der Grundrechte wesentlich, dass der Gesetzgeber selbst in hinreichend bestimmter und normenklarer Weise die Grenzen des Eingriffs festlegt. Aus denselben Gründen ist es gerade bei schwerwiegenden heimlichen Grundrechtseingriffen essentiell, Notwendigkeit und Ausmaß von Grundrechtseingriffen in öffentlicher Debatte zu klären.

2. Keine Reduzierung des Eingriffsgewichts durch den Gesetzgeber

Die gesetzgeberische Ausgestaltung des § 25a HSOG gewährleistet unter Beachtung dieser Maßstäbe keine ausreichende Eingriffsreduzierung, weder durch eine Beschränkung hinsichtlich Art und Umfang der verarbeitbaren Daten **(a)**), noch hinsichtlich der Methoden der Analyse **(b)**). Insbesondere genügen die vom Gesetzgeber beabsichtigten Einschränkungen weder dem Vorbehalt des Gesetzes, noch ist für Rechtsanwender*innen oder betroffene Personen klar und vorhersehbar, welche Eingriffe mit der Regelung verbunden sind.

a) Unzureichende Einschränkungen hinsichtlich Art und Umfang der einbezogenen Daten

§ 25a HSOG enthält kaum Beschränkungen der Art und des Umfangs der verarbeitbaren Daten. Zu den einzubeziehenden Datenbeständen gehören gem. § 25a Abs. 2 Satz 2 HSOG Vorgangsdaten, Falldaten, Daten aus den polizeilichen

Auskunftssystemen, Verkehrsdaten, Telekommunikationsdaten, Daten aus Asservaten und Daten aus dem polizeilichen Informationsaustausch. Es ist gem. § 25a Abs. 2 Satz 3 HSOG auch möglich, Datensätze aus gezielten Abfragen in gesondert geführten staatlichen Registern sowie einzelne gesondert gespeicherte Datensätze aus Internetquellen ergänzend einzubeziehen. Laut der Gesetzesbegründung sollen dazu beispielsweise Daten aus dem Melderegister, dem Zentralen Verkehrsinformationssystem (ZEVIS) oder dem Waffenregister gehören, welche über die Analyseplattform auf direktem Weg abgefragt werden können,

LT-Drs. 20/11235, S. 14.

Daten aus Internetquellen sind beispielsweise Datensätze aus sozialen Netzwerken,

LT-Drs. 20/11235, S. 14.

(1) Keine Beschränkung hinsichtlich Herkunft der Daten

Eine Möglichkeit, das Eingriffsgewicht zu reduzieren, besteht darin, die verarbeitbaren Daten hinsichtlich ihrer Herkunft zu beschränken,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 79.

§ 25a Abs. 2 Satz 2 HSOG zählt zwar (abschließend) Datenbestände auf, die automatisiert in die Analyse einbezogen werden sollen. Diese Aufzählung ist aber nicht als Begrenzung auf Daten bestimmter Herkunft zu verstehen.

Denn die Regelung setzt weder voraus, dass es sich um originär von der Polizei erhobene Daten handelt, noch sind Daten aus anderen Bundesländern, aus dem Zuständigkeitsbereich des Bundes oder aus anderen Staaten ausgeschlossen. Die Daten könnten vielmehr originär auch von anderen, nicht polizeilichen Behörden oder auch von nicht-öffentlichen Stellen stammen.

Die Regelung schließt auch nicht aus, dass ursprünglich von Nachrichtendiensten erhobene Daten, die an die Polizei – unter

einschränkenden Voraussetzungen – übermittelt werden, einbezogen werden. Die übermittelten Daten sind dann in polizeilichen Datenbanken gespeichert, obwohl sie ursprünglich nicht von Polizeibehörden erhoben wurden.

Dadurch, dass Daten aus polizeilichen Auskunfts- und Informationssystemen einbezogen sind, werden gerade auch Daten einbezogen, die nicht von der hessischen Landespolizei erhoben wurden. Auch INPOL ist ein polizeiliches Auskunfts- und Informationssystem. Sofern die Gesetzesbegründung lediglich auf POLAS-HE und EPOST 810 verweist,

LT-Drs. 20/11235, S. 12 ff,

ist diese Beschränkung nicht im Wortlaut des § 25a Abs. 2 Satz 2 HSOG angelegt.

Auch eine herkunftsbezogene Eingrenzung der Daten derart, dass nur Daten in die automatisierte Anwendung einbezogen werden, die bei der Wahrnehmung bestimmter polizeilicher Aufgaben angefallen sind, wie sie beispielsweise § 2 Satz 1 Hs. 1 ATDG beinhaltet (nur Daten aus der Terrorismusbekämpfung),

vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 82,

ist in § 25a HSOG nicht vorgesehen.

Insbesondere die Einbeziehung von Daten aus der Vorgangsverwaltung in die Datenanalyse (§§ 20 Abs. 9 Satz 3, 25a Abs. 2 Satz 2 HSOG) stellt sich als besonders intensiv dar. Die Vorgangsverwaltung dient der formalen Begleitung eines Vorgangs, also dazu, die bei einer Dienststelle anfallenden Informationen, wie etwa Anfragen oder Anzeigen in geordneter Form aufzubewahren und ein Wiederauffinden zu ermöglichen,

Müller/Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 832 m.w.N.

Ihr kommt somit lediglich eine Hilfsfunktion zu,

Müller/Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 833.

Bei Neueingängen in Vorgangsbearbeitungssystem werden nicht selten recht großzügig personenbezogene Daten von Beteiligten im weiteren Sinne aufgenommen, wobei eine Verifizierung, zuverlässige Kategorisierung und Kennzeichnung oftmals (noch) nicht gegeben ist,

vgl. *Bäuerle*, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 20 Rn. 153.

Aufgenommen werden beispielweise Daten aus Ermittlungsvorgängen, wie Anzeigen, Ermittlungsberichte, Vermerke oder auch bei Verkehrsunfällen aufgenommene Daten. Darüber hinaus enthalten sie aber auch Daten zu Anzeigerstatter*innen, Zeug*innen, Hinweisgeber*innen, Unfallbeteiligten und anderen Personen, die nicht Verdächtige oder Beschuldigte im Sinne des Strafprozessrechts oder Verantwortliche im Sinne des Polizeirechts sind,

Arzt, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 1184 m.w.N.

Es handelt sich also um Daten, für die eine abschließende Sachverhaltsbeurteilung noch aussteht. Aus diesem Grund werden Vorgangsdaten in der Regel nicht in polizeiliche Ermittlungen einbezogen und auch bei Auskunftersuchen gesondert ausgewiesen.

Ausgeschlossen sind nun zwar die personenbezogenen Vorgangsdaten Unbeteiligter gem. § 25a Abs. 3 Nr. 2 lit. a Satz 4 HSOG. Dieser Ausschluss stellt sich in der konkreten Umsetzung aber als zu unbestimmt dar (siehe **D.I.2.a)(4)**).

Ein zweiter Ausschluss betrifft gem. § 25a Abs. 3 Nr. 2 lit. b Satz 3 HSOG Daten aus Wohnraumüberwachung und Online-Durchsuchung. Praktisch wurden in Hessen in den letzten Jahren aber keine Daten aus Wohnraumüberwachung und Online-Durchsuchung erhoben,

zur Wohnraumüberwachung: BT-Drs. 20/8568; LT-Drs. 20/11766; LT-Drs. 20/9197; zur Online-Durchsuchung: *Bundesamt für Justiz*, Stand Juli 2023, abrufbar unter https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Justizstatistiken/Uebersicht_Online_Durchsuchung_2021.pdf?__blob=publicationFile&v=4,

sodass die Auswirkung des Ausschlusses in praktischer Hinsicht auch künftig gering sein wird,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 49 f.,

und keine nennenswerte Eingrenzung darstellt.

Daten aus anderen schwerwiegenden Grundrechtseingriffen sind hingegen nicht ausgeschlossen:

Der Gesetzgeber hat sich insbesondere explizit dazu entschlossen, auch Daten aus Telekommunikationsüberwachung einzubeziehen, die aus Maßnahmen nach § 100a StPO und § 15a HSOG stammen können,

LT-Drs. 20/11235, S. 13.

Als besonders privat, und damit für die Beurteilung der Eingriffsintensität relevant, stellen sich die bei Telekommunikationsüberwachungsmaßnahmen neben den Verkehrsdaten anfallenden Inhaltsdaten dar, die gleichermaßen nicht nur die überwachte Person betreffen, sondern auch Gesprächspartner*innen. Deren Weiterverarbeitung stellt gleichzeitig einen Eingriff in Art. 10 Abs. 1 GG dar. In der Gesetzesbegründung wird dazu ausgeführt, dass Kommunikationsinhalte selbst in einem Freitextfeld gespeichert würden, dessen Inhalt im Rahmen der automatisierten Datenanalyse per extra Mausklick zwar angezeigt werde, aber ohne vorherige gesonderte polizeiliche Bewertung und technische Aufbereitung nicht automatisiert weiterverarbeitet würden,

LT-Drs. 20/11235, S. 13.

Diese Einschränkung findet aber an keiner Stelle des Gesetzestexts Niederschlag, sodass § 25a HSOG die (automatisierte) Einbeziehung von Kommunikationsinhalten vielmehr zulässt.

Neben den Daten aus Telekommunikationsüberwachung können auch Daten, die aus dem Einsatz verdeckter Ermittler (§ 16 HSOG; § 110a StPO), längerfristiger Observationen, oder dem Einsatz technischer Mittel außerhalb von Wohnungen (§ 15 HSOG; §§ 100f, 163f StPO) stammen, sowie Nutzungsdaten (§ 100k StPO) einbezogen werden.

Auch Verkehrsdaten, die in der Regel aus schwerwiegenden Grundrechtseingriffen stammen und dem Schutz des Art. 10 Abs. 1 GG unterstellt sind,

Ogorek, in: BeckOK GG, 57. Ed. 15.1.2024, Art. 10 Rn. 38,

sind gem. § 25a Abs. 2 Satz 4 HSOG lediglich für eine Tatbestandsvariante, nämlich zur vorbeugenden Bekämpfung von Straftaten nach § 25a Abs. 2 Satz 1 Nr. 3 HSOG ausgeschlossen. Liegt hingegen eine konkretisierte Gefahr im Sinne von § 25a Abs. 2 Satz 1 Nr. 2 HSOG vor, dürfen Verkehrsdaten einbezogen werden. Da diese Tatbestandsvariante Bezug auf einen breit angelegten Straftatenkatalog nimmt, der eine Vielzahl von Vorfeldstraftatbeständen einbezieht (dazu **D.II.1.a)(1)(a)**), dürfte die Überwindung der Eingriffsschwelle für Polizeibehörden im Einzelfall einfach zu argumentieren sein, um die Einbeziehung von Verkehrsdaten zu rechtfertigen,

vgl. *Bäuerle*, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 51.

Damit verbleiben Verkehrsdaten für einen vermutlich beachtlichen Teil der Anwendungsfälle im Datenpool,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 52.

Im Kern können damit sämtliche Daten, auf die die Polizeibehörden Zugriff haben, einbezogen werden. Lediglich eine direkte Anbindung an das Internet ist ausgeschlossen. Daten aus dem Internet können jedoch indirekt einbezogen

werden, indem sie zunächst in eine der vorhandenen Datenbanken eingespeist werden.

(2) Keine Einschränkungen hinsichtlich der Menge

Auch die Datenmenge ist nicht beschränkt.

Weder begrenzt § 25a HSOG die Menge der verarbeitbaren Daten dadurch, dass nur solche Daten in die Analyse einbezogen werden dürfen, die für die Bekämpfung näher eingegrenzter Straftaten erforderlich ist,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 83,

noch erfolgt eine rein händische Hinzuziehung der Daten,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 88.

Vielmehr werden die in § 25a Abs. 2 Satz 2 HSOG gelisteten Datenbestände gem. § 25a Abs. 1 Satz 1 HSOG automatisiert zusammengeführt, was das Eingriffsgewicht erhöht.

Auch die in § 25a Abs. 3 Nr. 1 HSOG vorgesehene Zugriffsbeschränkung stellt keine ausreichende Beschränkung dar.

Zugriffsbeschränkungen können zwar grundsätzlich zu einer Beschränkung führen, allerdings nur, wenn dadurch die Menge der verarbeiteten Daten reduziert wird. 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,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 89.

Dieses Ziel wird indessen konterkariert, wenn die wenigen umfassend Zugriffsberechtigten Analyse- und Auswertestellen zugeordnet werden, wie es in Nr. 2.2.2 und 4.1 Abs. 2 VV § 25a HSOG vorgesehen ist, deren Aufgabe

offensichtlich darin besteht, den Organisationseinheiten mittels Durchführung automatisierter Analysen zuzuarbeiten. Auf diesem Weg wird nicht die Zahl der Analysevorgänge reduziert, sondern ihre Durchführung zentralisiert, sodass letztlich auch das aus der automatisierten Datenanalyse gewonnene „neue Wissen“ über die wenigen umfassend Zugriffsberechtigten hinaus Verbreitung und Anwendung in den Polizeibehörden findet,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 59.

(3) Keine Beschränkung auf bestimmte Datenarten

Eine Beschränkung auf bestimmte Datenarten,

vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 87,

sieht § 25a HSOG ebenfalls nicht vor.

Die Aufzählung in § 25a Abs. 2 Satz 2 HSOG zählt zwar (abschließend) Datenbestände auf, die automatisiert in die Analyse einbezogen werden sollen. Diese Aufzählung ist aber nicht als Begrenzung der zugelassenen Datenarten zu verstehen, wie sie beispielweise in § 3 Abs. 1 ATDG oder § 29 Abs. 2a Satz 3 Geldwäschegesetz (GwG) vorgesehen ist. Denn die in Datenbeständen enthaltenen Daten können ganz unterschiedlicher Art sein. So können beispielsweise allein Falldaten unterschiedliche Datenarten enthalten: Adressen, Namen, Familienstand, besuchte Orte, Zugehörigkeit zu Organisationen usw. Insbesondere biometrische Daten sind von § 25a HSOG nicht ausgeschlossen.

Auch hinsichtlich der zugelassenen Dateiformate,

vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 87,

finden sich in § 25a HSOG keine Einschränkungen. Gerade die Einbeziehung von Asservaten wird regelmäßig auch Video-, Bild- und Audioaufnahmen beinhalten. Da es sich dabei um zum Großteil unstrukturierte Daten handelt,

LT-Drs. 20/11235, S. 14,

können sich darin zum Beispiel auch Screenshots von Chats befinden, die besonders sensible Kommunikationsinhalte betreffen und von Art. 10 Abs. 1 GG geschützt sind.

Die unzureichende Beschränkung der Art der zu verwendenden Daten führt erstens dazu, dass die Menge der Daten als besonders hoch zu qualifizieren ist, und zweitens dazu, dass auch besonders persönlichkeitsrelevante Informationen einfließen können. Daraus ergibt sich ein hohes Eingriffsgewicht.

(4) Unzureichender Ausschluss der Daten „Unbeteiligter“

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,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 84.

Eine solche Begrenzung ist durch § 25a HSOG nicht gewährleistet.

(a) Vorgangsdaten

Zwar stellt die Neuregelung auf den ersten Blick eine Verbesserung dar, da die Vorgangsdaten Unbeteiligter nicht in die Analyse einbezogen werden dürfen (§ 25a Abs. 3 Nr. 2 lit. a Satz 4 HSOG).

Allerdings hat der Gesetzgeber nicht hinreichend normenklar und bestimmt genug geregelt, wie sich Unbeteiligte von Kontaktpersonen abgrenzen und zu welchem Zeitpunkt und nach welchen Kriterien sich die Einstufung bemisst.

Lediglich die Gesetzesbegründung liefert Hinweise darauf, was der Gesetzgeber unter „Unbeteiligten“ versteht: Unbeteiligte sollen demnach Personen sein, die

mit einem polizeilich relevanten Sachverhalt nur zufällig in Berührung stehen oder standen,

LT-Drs. 20/11235, S. 16.

Es ist unklar, wann von einer Zufälligkeit auszugehen ist. So stehen zum Beispiel Anzeigenerstatter*innen nicht zufällig in Berührung mit einem polizeilich relevanten Sachverhalt und sind dennoch Unbeteiligte in dem Sinne, dass sie grundsätzlich nicht in Straftaten verfangen sind oder Kontaktperson solcher Personen sind.

Zwar steht der Begriff „Unbeteiligte“ neben und in Abgrenzung zu anderen Kategorien (verurteilte, beschuldigte, verdächtige Personen und sonstigen Anlasspersonen sowie deren Kontaktpersonen, vgl. § 25a Abs. 3 Nr. 2 lit. b HSOG), allerdings sieht das Gesetz auch für diese Kategorien keine Definitionen vor.

Keine Kontaktpersonen dürften jedenfalls Personen sein, die nur flüchtig oder zufällig in Kontakt mit Personen stehen, bezüglich derer die Polizei tatsächliche Anhaltspunkte besitzt, dass diese selbst in (hinreichend gewichtige) Straftaten verfangen sind (vgl. z.B. § 18 Abs. 1 Satz 1 Nr. 3 BKAG). Das geht aber weder aus § 25a HSOG hervor, noch enthalten die Regelungen des HSOG Legaldefinitionen für diese Personenkategorien. Sofern zum Beispiel § 13 Abs. 2 Nr. 2 HSOG maßgeblich für die Einordnung als Kontaktperson sein soll, geht das nicht hinreichend normenklar aus § 25a HSOG oder aus § 13 Abs. 2 Nr. 2 HSOG hervor.

Das Hessische Ministerium des Inneren und für Sport gab im Verfahren, das dem Datenanalyse-Urteil zugrunde lag, an, dass man polizeilich keine Unbeteiligten kenne, denn alle Personen, zu denen im Vorgangssystem etwas dokumentiert sei, seien hierdurch Beteiligte,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 136.

Abgesehen davon, dass Defizite in Bezug auf Normenklarheit und Wesentlichkeit dazu führen, dass kein wirksamer Ausschluss garantiert ist,

geht wohl auch der Gesetzgeber davon aus, dass die Regelung nur begrenzt wirksam ist, wenn er in der Gesetzesbegründung ausführt, dass der „Prozess der abgestuften Erkenntnisgewinnung **tendenziell** [Hervorhebung nicht im Original] darauf gerichtet ist, ihre [Unbeteiligte] personenbezogenen Daten auszufiltern, bevor weitere Verarbeitungsschritte ergriffen werden“,

LT-Drs. 20/11235, S. 16.

(b) Verkehrsdaten

Ferner enthalten auch Verkehrsdaten, insbesondere solche, die aus Funkzellenabfragen gem. § 100g Abs. 3 StPO oder aus Telekommunikationsüberwachungsmaßnahmen stammen, aufgrund ihrer Streubreite typischerweise eine Vielzahl von Daten Unbeteiligter. Diese sind aber lediglich für eine Tatbestandsvariante ausgeschlossen (siehe oben **D.I.2.a)(1)**). Um einen ausreichenden Schutz zu gewährleisten, müssten Verkehrsdaten aber auch für die Eingriffsschwelle einer konkretisierten Gefahr (§ 25a Abs. 2 Satz 1 Nr. 2 HSOG) ausgeschlossen werden.

(c) Sonstige Datenbestände

Darüber hinaus erfassen auch andere verarbeitbare Datenbestände eine Vielzahl von Daten unbeteiligter Personen. Der Ausschluss der darin enthaltenen Daten Unbeteiligter ist nicht gewährleistet.

Falldaten sind die in Fallbearbeitungssystemen enthaltenen Daten. Ein Fallbearbeitungssystem gehe insofern über die reine Verwaltung von Vorgangsdaten hinaus, als es Anwender*innen ein benutzerfreundliches, speziell auf die Aufhellung von Strukturen hin ausgerichtetes Werkzeug zur Verfügung stelle, das weniger personenbezogen als vielmehr ereignisbezogen ausgerichtet sei und vor allem Beziehungen zwischen Personen, Institutionen, Objekten und Sachen abbildet und sowohl zu präventiven als auch repressiven Zwecken eingesetzt werden könne,

LT-Drs. 20/11235, S. 12 unter Verweis auf *Arzt*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 1289 ff.

Somit werden Daten Unbeteiligter immer dann im Fallbearbeitungssystem aufgenommen und so der Analyse zugänglich gemacht, wenn aus einem Vorgang ein Fall wird.

Darüber hinaus können polizeiliche Sachbearbeiter*innen nachträglich die Einstufung der Person auch im Vorgangsdatensystem jederzeit ändern,

LT-Drs. 20/11235, S. 16.

Auch Asservate, beispielsweise Datenträger wie USB-Sticks, Festplatten, Smartphones und Laptops, können große Mengen personenbezogener Daten Unbeteiligter, insbesondere von Freund*innen, Familienangehörigen oder Bekannten enthalten. § 94 StPO erlaubt im Strafverfahren auch die Sicherstellung und Beschlagnahme nicht körperlicher Gegenstände, wie elektronisch (digital) gespeicherte Informationen und Kommunikationsdaten auf Mobiltelefonen, Computern oder sonstigen Datenträgern,

Hauschild, in: MüKo StPO, Bd. 1, 2. Aufl. 2023, § 94 Rn. 13; *Greven*, in: KK-StPO, 9. Aufl. 2023, § 94 Rn. 4.

Das Auslesen dieser Datenträger ist ohne weitere Anordnung möglich,

Greven, in: KK-StPO, 9. Aufl. 2023, StPO § 94 Rn. 4.

Begrenzungen hinsichtlich des Umfangs der sicherzustellenden beziehungsweise zu beschlagnahmenden Daten erfolgen über den Verhältnismäßigkeitsgrundsatz,

BVerfGE 113, 29 (55 ff. Rn. 113 ff.).

Die weitere Speicherung und Verarbeitung der Daten richten sich nach §§ 483 ff. StPO. Diese Vorschriften stellen aber keine hinreichende Aussonderung bestimmter Daten sicher, sodass die Inhalte der Datenträger, also beispielsweise auf Datenträgern gespeicherte Adressen, Telefonnummern,

Fotos und Videos, die unbeteiligte Personen betreffen, weiterhin vorhanden sind und mithin analysiert werden können.

Ferner enthalten Daten aus Telekommunikationsüberwachung regelmäßig Daten unbeteiligter Gesprächspartner*innen, da lediglich der Kernbereich privater Lebensgestaltung ausgeschlossen wird (§ 100d StPO; § 15a Abs. 1 Satz 4 i.V.m. § 15 Abs. 4 Satz 4-6 HSOG).

Auch die in § 20 Abs. 6 Satz 1 HSOG enthaltene Beschränkung hinsichtlich der Weiterverarbeitung von aus im Rahmen der Strafverfolgung erhobenen Daten bewirkt keinen Schutz unbeteiligter Personen. Gem. § 20 Abs. 6 Satz 1 HSOG ist eine Weiterverarbeitung personenbezogener Daten, die Polizeibehörden im Rahmen der Strafverfolgung gewonnen haben, zulässig, soweit dies zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Hinsichtlich der Daten von Personen, die verdächtig sind, eine Straftat begangen zu haben, ist die Weiterverarbeitung nur zulässig, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass zukünftig Strafverfahren gegen die betroffenen Personen zu führen sein werden (§ 20 Abs. 6 Satz 2 Hs. 1 HSOG). Damit ist nun eine Negativprognose nötig.

Erstens ist aber zumindest nicht hinreichend bestimmt klargestellt, dass § 20 Abs. 6 HSOG auf eine Weiterverarbeitung nach § 25a HSOG anwendbar ist. Denn 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 Bürger*innen hinreichend deutlich erkennbar sein, und es muss auch hinreichend klar sein, was daraus für die praktische Ausgestaltung gerade der Datenanalyse oder -auswertungsbefugnis folgt,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 114.

Zweitens betrifft die Negativprognose und die damit verbundene Löschung nur die personenbezogenen Daten der ehemals verdächtigen Person, nicht aber die Daten unbeteiligter Zeug*innen, Geschädigter oder Anzeigenerstatter*innen,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 20 Rn. 123.

Deren Weiterverarbeitung ist lediglich an die Erforderlichkeit zu den oben genannten Zwecken geknüpft. Bei der in der Polizeipraxis nicht ungewöhnlichen großzügigen Auslegung des Prinzips der Erforderlichkeit der Weiterbearbeitung zu den genannten Zwecken würde der Datenbestand somit zwar um die Daten der Personen ohne Negativprognose reduziert, nicht jedoch um die der Unbeteiligten, deren Daten im Rahmen des Strafverfahrens erhoben worden waren,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 20 Rn. 124.

Insofern in der Literatur eine verfassungskonforme Interpretation dahingehend angeregt wird, dass auch Daten Unbeteiligter auszuschließen sind,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 20 Rn. 126,

ist dem entgegenzusetzen, dass Einschränkungen zur Begrenzung des Eingriffsgewichts besondere Anforderungen an Bestimmtheit und Normenklarheit erfordern, die eine solche Auslegung nur in sehr begrenztem Umfang erlauben. Gerade der Schutz Unbeteiligter muss bereits durch den Gesetzgeber selbst hinreichend klar und deutlich festgelegt werden und darf nicht erst durch Einschränkungen mittels kaum erzielbarer Gerichtsurteile erfolgen.

Insgesamt lässt § 25a HSOG somit nach wie vor eine breite Einbeziehung von Daten Unbeteiligter zu. Für objektiv Unbeteiligte besteht also ein erhöhtes Risiko, Ziel weiterer polizeilicher Aufklärungsmaßnahmen zu werden.

(5) Keine Gewährleistung der Zweckbindung

Die Einhaltung der Grundsätze der Zweckbindung ist insbesondere für Daten aus schwerwiegenden Grundrechtseingriffen nicht sichergestellt.

(a) Grundlegende Aspekte

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,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 138.

Insbesondere Regelungen zur Sicherung der Zweckbindung 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,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 80.

So müsste bei § 25a HSOG technisch und organisatorisch sichergestellt sein, dass bei einer Datenanalyse je nachdem, welche Tatbestandsalternative des § 25a Abs. 2 Satz 1 HSOG im Einzelfall vorliegt, jeweils nur Daten einfließen, die zu vergleichbar gewichtigen Zwecken, also zum Schutz vergleichbar gewichtiger Rechtsgüter hätten erhoben werden dürfen. Falls also der Zweck

der Analyse auf die Verhinderung einer Straftat von lediglich erheblicher Bedeutung zielt, dürfen nach dem Grundsatz der hypothetischen Datenenerhebung keine Daten einbezogen werden, die nur im Hinblick auf schwere oder besonders schwere Straftaten erhoben werden dürfen.

Der Gesetzgeber geht hinsichtlich der Analyse von Daten aus Telekommunikationsüberwachung davon aus, dass die Voraussetzungen der Zweckänderung in jeder Tatbestandsalternative des § 25a Abs. 2 Satz 1 HSOG erfüllt seien,

LT-Drs. 20/11235, S. 9.

Vergleicht man aber den Katalog der vom Gesetzgeber als „erheblich“ bewerteten Straftaten in § 13 Abs. 3 Satz 1 HSOG mit dem Katalog des § 100a Abs. 2 StPO, sind diese nicht deckungsgleich. Der Katalog des § 13 Abs. 3 Satz 1 HSOG geht sogar über § 100a Abs. 2 StPO hinaus und ist noch weiter „nach unten“ geöffnet,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 13 Rn. 123.

§ 13 Abs. 3 Satz 1 HSOG enthält keine abschließende Aufzählung von Straftatbeständen, sondern erfasst erstens alle Verbrechen. Zweitens knüpft die Vorschrift für Vergehen an abstrakte Merkmale an (siehe dazu **D.II.1.a)(1)(a)**), die die einbezogenen Straftatbestände erfüllen müssen und verlangt zusätzlich, dass diese im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören. Beispielsweise enthält § 100a Abs. 2 StPO nicht § 126 StGB (Störung des öffentlichen Friedens durch Androhung von Straftaten), § 130a StGB (Anleitung zu Straftaten), einfache Körperverletzungen (§ 223 StGB) oder den Besitz von Betäubungsmitteln.

Diese Straftaten sind jedenfalls keine schweren Straftaten, sodass Daten aus Telekommunikationsüberwachungen dafür nicht verwendet werden dürften.

Zwar verweist § 25a Abs. 3 Satz 1 HSOG nun auch ausdrücklich auf § 20 Abs. 1 und 2 HSOG, sodass jedenfalls die Geltung der darin verankerten Grundsätze zur Zweckbindung und Zweckänderung klargestellt ist.

Die Anwendbarkeit weiterer speziellerer Regelungen über die Weiterverarbeitung von Daten auf § 25a HSOG ist hingegen nicht hinreichend geregelt. Dazu gehören beispielsweise § 479 Abs. 2 Satz 2 StPO oder § 12 Abs. 2 Satz 4, Abs. 4, § 14 Abs. 1 Satz 3, Abs. 2 Satz 3, Abs. 4 Satz 3, § 15 Abs. 6 Satz 4, Satz 5, Abs. 9, § 15a Abs. 1 Satz 4, § 15b Abs. 3 Satz 1, § 15c Abs. 3 Satz 2, Satz 4 HSOG,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 91, § 20 Rn. 29-33.1.

Darüber hinaus fordert das angerufene Gericht für die praktische Umsetzung der Grundsätze der Zweckbindung und Zweckänderung eine entsprechende Kennzeichnung der Daten,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 65.

Die Vorgaben des angerufenen Gerichts erfordern für die technische Umsetzung eine umfassende Mikrokategorisierung,

vgl. *Hartmann/Cipierre/Beeck*, RDV 2023, 147 (150).

Weder schreibt § 25a HSOG eine ausreichende Unterscheidung nach Herkunft und Erhebungszwecken vor, noch wird eine entsprechende Kennzeichnungspflicht im Gesetzestext explizit festgeschrieben. Um dem Vorbehalt des Gesetzes zu genügen, muss der Gesetzgeber aber selbst vorschreiben, dass eine Kennzeichnung der Daten zwingend vorgesehen werden muss. Außerdem muss er selbst vorgeben, welchen Unterscheidungskriterien die Kennzeichnung folgen muss. Denn dabei handelt es sich um wesentliche Entscheidungen, die eine Begrenzung des Datenumfangs bewirken sollen und damit die Reichweite und Grenzen der Befugnis betreffen. Die technischen Einzelheiten, also wie genau die eingesetzte Software die Kennzeichnung konkret umsetzt, könnten hingegen der Verwaltung übertragen werden.

(b) Keine Anwendbarkeit der Kennzeichnungspflicht nach § 20a HSOG

§ 20a HSOG schreibt grundsätzlich vor, dass Daten bei der Speicherung gekennzeichnet werden müssen.

Ob diese Kennzeichnung bei der Zusammenführung der Daten im Rahmen der Anwendung zur automatisierten Datenanalyse fortbestehen soll oder durch die Zuordnung zu Phänomenbereichen und/oder Regelungen des Konzepts der Kategorisierung und Kennzeichnung (dazu sogleich unter **c**)) ersetzt werden soll, ist aus § 25a HSOG zumindest nicht hinreichend bestimmt ersichtlich.

Das angerufene Gericht fordert, dass, soweit sich Maßgaben zur Eingrenzung zulässiger Datenverarbeitung bereits aus Vorschriften des allgemeinen oder des polizeilichen Datenschutzrechts ergeben, deren Anwendbarkeit auf die Datenanalyse oder -auswertungsbefugnis sowohl für die Behörde als auch für Bürger*innen hinreichend deutlich erkennbar sein muss. Auch muss hinreichend klar sein, was daraus für die praktische Ausgestaltung gerade der Datenanalyse oder -auswertungsbefugnis folgt,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 114.

§ 25a HSOG verhält sich an keiner Stelle dazu, ob § 20a HSOG bei der automatisierten Anwendung zur Datenanalyse eine Rolle spielt. *E contrario* § 25a Abs. 3 Satz 1 HSOG, der § 20 Abs. 1 und Abs. 2 HSOG ausdrücklich für anwendbar erklärt, kann vielmehr davon ausgegangen werden, dass § 20a HSOG mangels konkreter Bezugnahme im Gesetzestext keine Anwendung finden soll.

Gegen eine Anwendbarkeit spricht auch, dass § 25a Abs. 3 Nr. 2 HSOG ein eigenes Konzept der Kategorisierung und Kennzeichnung vorsieht, dessen gesetzliche Anleitung aber unzureichend ausgestaltet ist (siehe dazu **D.I.2.a)(5)(b)(cc)**). Insbesondere im Hinblick auf die Kategorisierung von Personengruppen unterscheidet sich dieses Konzept von § 20a HSOG. § 25a Abs. 3 Nr. 2 lit. a Satz 3 HSOG sieht eine Differenzierung nach einerseits verurteilten, beschuldigten, verdächtigen Personen und sonstigen

Anlasspersonen sowie deren Kontaktpersonen und andererseits unbeteiligten Personen vor. § 20a Abs. 1 Nr. 2 HSOG schreibt, sofern Grunddaten angelegt wurden, eine Kategorisierung vor, ohne aber selbst einen Katalog zu benennen. In Betracht kommen § 13 Abs. 2 HSOG und § 67 HDSIG. Beide stimmen nicht mit den oben genannten Kategorien überein,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 20a Rn. 20 ff.

Während § 67 HDSIG die europarechtliche Kategorisierung aus Art. 6 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (JI-Richtlinie) übernimmt, legt § 13 Abs. 2 HSOG eine davon und auch wiederum von § 25a Abs. 3 Nr. 2 lit. a Satz 3 HSOG abweichende Kategorisierung fest.

In der Kommentarliteratur wird vertreten, dass daraus, dass der untergesetzliche Normgeber in der Verwaltungsvorschrift zu § 25a HSOG keine Kennzeichnung geregelt habe, geschlossen werden könne, dass § 20a HSOG anwendbar sei,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 95.

Ein solcher Schluss verbietet sich aber schon aus normenhierarchischen Gesichtspunkten, da es dann der untergesetzliche Normgeber in der Hand hätte, den Willen des Gesetzgebers zu bestimmen.

Selbst wenn § 20a HSOG grundsätzlich anwendbar sein sollte, ist dennoch fraglich, ob die Kennzeichnung im Rahmen der Weiterverarbeitung mittels Datenanalyse fortbestehen soll. Denn § 20a Abs. 3 HSOG schreibt das Fortbestehen der Kennzeichnungspflicht explizit nur für die Übermittlung an eine andere Stelle vor.

Darüber hinaus sieht § 20a Abs. 4 HSOG eine Ausnahme von der Kennzeichnungspflicht vor, soweit eine Kennzeichnung entweder nicht

möglich ist (Satz 1) oder solange eine Kennzeichnung technisch nicht möglich ist oder einen unverhältnismäßigen Aufwand erfordern würde (Satz 2). Satz 1 soll die tatsächliche Unmöglichkeit einer Kennzeichnung betreffen, etwa, wenn nicht bekannt oder feststellbar ist, wer die Daten erhoben hat oder zu welchem Zweck sie ursprünglich erhoben wurden.

LT-Drs. 19/5728, S. 189.

Für Satz 2 bleibt unklar, aus welchen konkreten Umständen sich die Unmöglichkeit ergeben soll,

Bauerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 20a Rn. 40.

Damit legt die Vorschrift weitreichende Ausnahmen von der Kennzeichnungspflicht fest. Zu befürchten ist vor allem, dass es im Rahmen von Vorgangsdaten zu keiner hinreichenden Kennzeichnung kommt. Vorgangsdatenbanken erfassen sehr viele verschiedene Vorgänge und damit auch Daten einer Großzahl von Personen, sodass eine Kennzeichnung schnell einen großen Aufwand hervorrufen kann.

Damit zeigt sich ein generelles Problem der Vorschrift: Solange keine Kennzeichnung möglich ist oder diese großen Aufwand bedeutet, werden Daten weiter in die Analyse eingezogen. Damit wird ein Anreiz gesetzt, keine Kennzeichnungsmöglichkeiten zu schaffen, beziehungsweise keine solchen, die den Aufwand der Kennzeichnung minimieren. Hinzu kommt, dass dies gerade auch Daten aus schwerwiegenden Grundrechtseingriffen umfasst, die andernfalls vielfach nicht in eine Analyse einbezogen werden dürften. Da jede Weiternutzung von bereits erhobenen Daten einen weiteren Grundrechtseingriff darstellt,

vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 55 ff. m.w.N.,

wäre eine Weiternutzung zu nicht vergleichbar gewichtigen Zwecken verfassungsrechtlich unzulässig. Vielmehr sollte daher der gegenteilige – grundrechtsschonendere – Ansatz verfolgt werden: Solange keine

Kennzeichnung möglich ist, dürfen Daten auch nicht in die Analyse einbezogen werden.

(c) Defizite der in § 25a HSOG vorgesehenen Konzepte

(aa) Übergreifende Defizite

Gem. § 25a Abs. 3 Satz 2 HSOG wird die Geltung von § 20 Abs. 1 und Abs. 2 HSOG durch eine Verwaltungsvorschrift sichergestellt. Die Verwaltungsvorschrift beinhaltet gem. § 25a Abs. 3 Satz 3, Abs. 3 Nr. 1 und Nr. 2 HSOG ein Rollen- und Rechtekonzept sowie ein Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten.

Die Möglichkeit, Regelungen in Verwaltungsvorschriften zu treffen, steht dem Gesetzgeber nach der Rechtsprechung des angerufenen Gerichts in gewissem Umfang zur Verfügung. Jedoch wahrt § 25a Abs. 3 Satz 2 HSOG nicht die vorgegebenen Grenzen.

Der Gesetzgeber hat 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,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 113.

Schon auf formaler Ebene genügt § 25a Abs. 3 Satz 2 HSOG diesen Anforderungen nicht, da der Gesetzgeber die Art und Weise der Veröffentlichung der Verwaltungsvorschrift nicht normiert hat.

Die Verwaltungsvorschrift kann darüber hinaus eine Sicherung der Zweckbindung nicht gewährleisten, da die gesetzliche Grundlage nicht normenklar formuliert ist, den Gesetzesvorbehalt missachtet und zu unbestimmt ist. Mithin sind auch die Festlegung und die verlässliche Dokumentation der Vorgaben und Kriterien nicht gewährleistet.

Gem. § 25a Abs. 3 Satz 4 HSOG gilt für beide Konzepte gleichermaßen, dass sie sich unter Berücksichtigung der in Abs. 2 Satz 1 nach Schutzgütern und Eingriffsschwellen unterschiedenen Lagebilder an dem übergeordneten Ziel der Reduzierung des jeweils zu analysierenden Datenvolumens, der Angemessenheit der jeweils angewandten Analysemethode und des größtmöglichen Schutzes Unbeteiligter (funktionale Reduzierung der Eingriffsintensität) orientieren. Da eine „Orientierung“ keinerlei rechtliche Verpflichtung beinhaltet, die Norm lediglich in unbestimmter Weise die aus dem Verhältnismäßigkeitsgrundsatz folgenden abstrakten Anforderungen an eine wirksame Einschränkung wiedergibt, ist die Angabe als rechtliches Nullum zu bewerten. Dass die darin enthaltenen Angaben den verfassungsrechtlichen Maßstab für die einfachgesetzliche Ausgestaltung des Gesetzgebers darstellen sollen, steht außer Frage. Diesen übergeordneten Maßstab derart im Gesetzestext zu verankern, führt aber lediglich dazu, den Maßstab ohne nähere Konturierung an die Verwaltung durchzureichen. Eine solche Gesetzgebungspraxis verstößt gegen den Vorbehalt des Gesetzes. Dieser verlangt, dass der Gesetzgeber die sich aus dem Verhältnismäßigkeitsprinzip ergebenden Anforderungen selbst regelt und die anspruchsvollen Abwägungen nicht der Rechtsanwendung überlässt,

vgl. *Gärditz*, in: Friauf/Höfling, GG, 42. EL Dezember 2023, Art. 20 (6. Teil)
Rn. 133.

Hierdurch werden Verwaltungsentscheidungen versachlicht, da die gesetzliche Begriffsbildung die für die Verwaltung zu bewältigende Komplexität reduziert, Maßstäbe verdichtet und Entscheidungen vorstrukturiert,

Gärditz, in: Friauf/Höfling, GG, 42. EL Dezember 2023, Art. 20 (6. Teil)
Rn. 133.

Diese dem Wesentlichkeitsvorbehalt nicht genügende Delegation unter Wiederholung abstrakter Verhältnismäßigkeitsanforderungen führt sich in den weiteren Regelungen zu den Konzepten fort.

(bb) Rollen- und Rechtekonzept

§ 25a Abs. 3 Satz 3, Satz 4, Abs. 3 Nr.1 HSOG sieht ein Rollen- und Rechtekonzept vor. Laut Gesetzesbegründung soll dieses Konzept festlegen, welche Personen innerhalb der Polizeiorganisation Zugriff auf welche Daten erlangen können, und mit welchen Rechten und Pflichten der Zugriff für die jeweilige Person verbunden ist,

LT-Drs. 20/11235, S. 15.

Dadurch sollen Anwender*innen Phänomenbereiche mit jeweils abgeschotteten Datenkammern zugewiesen werden,

vgl. LT-Drs. 20/11235, S. 15.

Zunächst ist es grundsätzlich positiv zu bewerten, dass der Gesetzgeber ein Rechte- und Rollenkonzept vorsieht. Allerdings ist die gesetzgeberische Ausgestaltung des Konzepts in mehrerlei Hinsicht verfassungsrechtlich defizitär und kann deshalb auch nicht sicherstellen, dass Daten den Grundsätzen der Zweckbindung und Zweckänderung entsprechend weiterverarbeitet werden.

(aaa) Normenklarheit

Die Regelung genügt nicht dem Maßstab der Normenklarheit (siehe dazu **D.I.1.b)(1)(c)**).

Gem. § 25a Abs. 3 Nr.1 Satz 1 HSOG regelt das Rollen- und Rechtekonzept die zweckabhängige Verteilung sachlich eingeschränkter Zugriffsrechte anhand von Phänomenbereichen.

Dass Zugriffsrechte an Phänomenbereiche geknüpft werden sollen, dürfte für Bürger*innen noch nachvollziehbar sein.

Maßstab für das Konzept sind das Gewicht der zu schützenden Rechtsgüter und der Grad der Dringlichkeit des polizeilichen Einschreitens (§ 25a Abs. 3 Nr. 1 Satz 2 HSOG). Aus der Perspektive von Bürger*innen ist dieser Teil der Regelung absolut unverständlich. Dies beruht erstens darauf, dass der Regelung

ein enormes Maß an Abstraktheit attestiert werden kann, zweitens auf den unklaren Begrifflichkeiten, an die die Norm anknüpft. Schon der Begriff der „Dringlichkeit“ ist unbestimmt und unklar. Offen bleibt, nach welchen Kriterien sich die Dringlichkeit beurteilt, welche Abstufungen damit verbunden sind, wie sich diese zu den Eingriffsschwellen verhält und wie sie sich letztlich auf die zweckabhängige Verteilung von Zugriffsrechten auswirkt. Auch das Verhältnis zum zweiten maßstabsbildenden Faktor „Gewicht der zu schützenden Rechtsgüter“ bleibt offen. Damit sind die Bedeutung und Auswirkung dieses Maßstabs für Bürger*innen nicht erkennbar.

(bbb) Gesetzesvorbehalt und Bestimmtheit

Darüber hinaus verstoßen die Regelungen zum Rechte- und Rollenkonzept auch gegen den Vorbehalt des Gesetzes und den Bestimmtheitsgrundsatz.

Denn der hessische Gesetzgeber gibt für das Rechte- und Rollenkonzept lediglich einen Maßstab, ein Prinzip und Mindestanforderungen vor. Diese wenigen Vorgaben sind wiederum so unbestimmt, dass eine hinreichende, dem Grundsatz der Wesentlichkeit genügende gesetzgeberische Anleitung der Verwaltung für die Ausarbeitung von Konkretisierungen und Standardisierungen fehlt. Vielmehr handelt es sich dabei wiederum um abstrakte Kriterien, die für die gesetzgeberische Tätigkeit im Rahmen der Schaffung einer verhältnismäßigen Rechtsgrundlage maßstabsbildend sein können. Diese Kriterien unter Beibehaltung ihrer Abstraktheit in Gesetzesform zu gießen, führt dazu, die eigentlich dem parlamentarischen Gesetzgeber obliegende Entscheidung ohne eine nähere, hinreichend bestimmte Anleitung auf die Exekutive zu übertragen und verstößt somit gegen den Vorbehalt des Gesetzes.

Als Maßstab für das Rechte- und Rollenkonzept gibt der Gesetzgeber das Gewicht der zu schützenden Rechtsgüter und den Grad der Dringlichkeit des polizeilichen Einschreitens vor (§ 25a Abs. 3 Nr. 1 Satz 2 HSOG). Auch aus der Sicht von Rechtsanwender*innen – die der Bestimmtheitsgrundsatz in Abgrenzung zum Grundsatz der Normenklarheit adressiert – bleibt unklar, wie

dieser abstrakte Maßstab umgesetzt werden soll. Insofern ergeben sich für diese Perspektive keine Unterschiede zu den im Rahmen der Normenklarheit festgestellten Defiziten.

In § 25a Abs. 3 Nr. 1 Satz 4 HSOG heißt es, dass im Rechte- und Rollenkonzept mindestens die einzelnen Phänomenbereiche, ihre Gewichtung und ihr Verhältnis zueinander umschrieben und die dienstrechtliche Stellung der Berechtigten, ihre Funktion und ihre spezifische Qualifizierung bezogen auf den Umfang der jeweiligen Berechtigung festgelegt werden.

Es ist unklar, was genau der Gesetzgeber unter „Phänomenbereichen“ versteht.

Die Gesetzesbegründung ergänzt den Begriff um ein weiteres Wort und will darunter kriminologische Phänomenbereiche verstanden wissen,

LT-Drs. 20/235, S. 15,

Auch dadurch erhält der Begriff keine schärfere Konturierung. So sind sehr unterschiedliche Einteilungen denkbar,

siehe z.B. *Bundeskriminalamt*, Deliktsbereiche, abrufbar unter https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/deliktsbereiche_node.html; *Landeskriminalamt Sachsen*, Polizeiliche Kriminalstatistik 2022, S. 84 ff., abrufbar unter <https://www.polizei.sachsen.de/de/102744.htm>.

§ 25a Abs. 3 Nr. 1 HSOG trifft aber keine Aussage darüber, wie kleinteilig die Einteilung in Phänomenbereiche erfolgen soll, also wie viele es mindestens geben muss, und ob sie die einzelnen polizeilichen Zuständigkeitsbereiche widerspiegeln sollen. Ob der Begriff mit dem der „Rolle“ gleichzusetzen ist oder eine Rolle mehrere Phänomenbereiche erfassen soll, ist nicht ersichtlich.

Weder wird dem untergesetzlichen Normgeber verpflichtend aufgegeben, Datenbestände Phänomenbereichen zuzuordnen, noch ist geregelt, zu welchem Zeitpunkt und nach welchen Kriterien dies erfolgen muss.

Diese Aspekte sind aber wesentlich, wenn der Gesetzgeber eine wirksame Einschränkung über Phänomenbereiche schaffen will. Will er die

Phänomenbereiche nicht selbst bestimmen, muss er immerhin Vorgaben dazu machen, an welches Kriterium die Bestimmung von Phänomenbereichen anknüpfen soll, um dem Vorbehalt des Gesetzes zu genügen.

Nach der Regelung wäre auch eine Einteilung in lediglich zwei Phänomenbereiche denkbar, die sich zum Großteil überschneiden. Eine solche Umsetzung würde nur eine minimale Einschränkung bedeuten und stellt keine „funktionsbedingte[...] Reduzierung des Umfangs der jeweils zu verarbeitenden Daten und damit [...] strategischen Verringerung der Eingriffsintensität“,

LT-Drs. 20/11235, S. 15,

dar. Die mangelhafte gesetzgeberische Anleitung spiegelt sich auch in der praktischen Umsetzung: In Ziffer 2.1. der Verwaltungsvorschrift zur Ausführung des § 25a des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (VV § 25a HSOG) sind lediglich drei Phänomenbereiche gelistet: Schwere Kriminalität (SK), Organisierte Kriminalität (OK) und Staatsschutzkriminalität (ST). Diese ermöglichen aber keine hinreichende Abgrenzung verschiedener Delikte. Der Phänomenbereich „OK“ ist ein kriminologisch umstrittenes Konstrukt, das aufgrund seines starken Bezugs auf die Person des Beschuldigten kaum eine inhaltliche Abgrenzung bezüglich bestimmter Taten ermöglicht. Bei „schwerer Kriminalität“ handelt es sich um einen umfassenden Auffangbereich. Denn schwere Kriminalität erstreckt sich auf verschiedene polizeiliche Zuständigkeitsbereiche und führt damit im Ergebnis nicht wirklich zu einer Einschränkung.

Das Rechte- und Rollenkonzept kann in Anbetracht seiner verfassungsrechtlichen Defizite nicht gewährleisten, dass die Grundsätze der Zweckbindung und Zweckänderung eingehalten werden. Zwar soll die Verteilung zweckabhängig anhand von Phänomenbereichen erfolgen. Dabei wird aber nicht klar, ob und inwieweit die ursprünglichen Erhebungszwecke bei der Verteilung eine Rolle spielen müssen, ob die Phänomenbereiche daran anknüpfen und wie dies technisch umgesetzt wird. Auch das in § 25a Abs. 3 Nr. 1 Satz 3 HSOG verankerte Prinzip, wonach mehr Berechtigte Zugriff auf weniger und wenige Berechtigte Zugriff auf mehr der in der Analyseplattform

zusammengeführten Daten haben dürfen, ändert nichts an diesem Befund. Denn was „mehr“ Daten sind beziehungsweise ob damit Daten aus schwerwiegenden Grundrechtseingriffen gemeint sind, ergibt sich daraus gerade nicht,

vgl. *Bäuerle*, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 58.

Zudem ergibt sich dieses Prinzip bereits aus dem Grundsatz der Verhältnismäßigkeit. Insofern verlagert der Gesetzgeber auch an dieser Stelle die von ihm selbst zu treffende Abwägungsentscheidung wiederum auf den untergesetzlichen Normgeber.

Für eine wirksame Ausgestaltung des Konzepts müsste – entweder durch den Gesetzgeber selbst oder mittels ausreichend angeleiteter, hinreichend bestimmter und normenklarer Delegation – in einem ersten Schritt eine eindeutige und abschließende Zuordnung von Delikten oder Rechtsgütern zu den einzelnen Phänomenbereichen erfolgen. In einem zweiten Schritt müsste für jeden Phänomenbereich eine Zuordnung von Datenbeständen unter Berücksichtigung der ursprünglichen Erhebungszwecke zu den drei Tatbestandsalternativen des § 25a Abs. 2 Satz 1 HSOG sichergestellt werden.

(cc) Konzept der Kategorisierung und Kennzeichnung

Auch das Konzept der Kategorisierung und Kennzeichnung stellt die Wahrung der Grundsätze der Zweckbindung in seiner derzeitigen Ausgestaltung nicht sicher, da es schon nicht den Anforderungen an Normenklarheit, Gesetzesvorbehalt und Bestimmtheit genügt.

(aaa) Normenklarheit

Gem. § 25a Abs. 3 Nr. 2 lit. b Satz 2 HSOG müssen abstrakte Regelungen getroffen werden, die der eingeschränkten Verwendbarkeit von Daten aus schwerwiegenden Grundrechtseingriffen Rechnung tragen.

Die „eingeschränkte Verwendbarkeit“ gibt nicht in normenklarer Weise die Voraussetzungen einer Zweckänderung bei Datenerhebungen aus

schwerwiegenden Grundrechtseingriffen wieder. Eine solche Regelungsweise ist verfassungsrechtlich nicht haltbar, da für Bürger*innen nicht ansatzweise erkennbar ist, was damit gemeint ist. Vielmehr müssten Bürger*innen die einschlägige Rechtsprechung des angerufenen Gerichts und den Grundsatz der hypothetischen Datenneuerhebung kennen, um die Norm richtig verstehen zu können beziehungsweise deren Auswirkungen zu erkennen.

(bbb) Gesetzesvorbehalt und Bestimmtheit

Vor allem aber sind der Vorbehalt des Gesetzes und der Grundsatz der Bestimmtheit verletzt.

Gemäß § 25a Abs. 3 Nr. 2 HSOG regelt das Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten anhand der Maßstäbe des Veranlassungszusammenhangs und der Grundrechtsrelevanz, welche personenbezogenen Daten in welcher Weise in die automatisierte Analyse einbezogen werden dürfen.

Gem. § 25a Abs. 3 Nr. 2 lit. a Satz 1 HSOG ist der Veranlassungszusammenhang der sachliche Bezug der von der Analyse betroffenen Personen zum jeweiligen Phänomenbereich (siehe zur Unbestimmtheit etc. oben **D.I.2.a)(5)(c)(bb)(bbb)**). Diese Kategorisierung nach einerseits verurteilten, beschuldigten, verdächtigen Personen und sonstigen Anlasspersonen sowie deren Kontaktpersonen und andererseits unbeteiligten Personen (§ 25a Abs. 3 Nr. 2 lit. a Satz 3 HSOG) ist im Rahmen der Weiterverwendung nach dem Grundsatz der hypothetischen Datenneuerhebung aber nicht allein maßgeblich und sichert mithin auch nicht die Einhaltung der Grundsätze der Zweckbindung.

Auch der Maßstab der Grundrechtsrelevanz vermag an diesem Ergebnis nichts zu ändern. Darunter versteht der Gesetzgeber die Kategorisierung personenbezogener Daten nach der Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung bei ihrer Erhebung (§ 25a Abs. 3 Nr. 2 lit. b Satz 1 HSOG). Abgesehen vom Ausschluss von Daten aus Wohnraumüberwachung und Onlinedurchsuchung trifft der Gesetzgeber selbst

aber keine näheren Vorgaben. Vielmehr muss die Verwaltung abstrakte Regelungen treffen, die der „eingeschränkten Verwendbarkeit“ von Daten aus schwerwiegenden Grundrechtseingriffen Rechnung tragen, und es muss durch technisch-organisatorische Vorkehrungen sichergestellt werden, dass diese Regelungen praktisch wirksam werden (§ 25a Abs. 3 Nr. 2 lit. b Satz 2 HSOG).

Dies verstößt gegen den Gesetzesvorbehalt. Denn der Gesetzgeber muss selbst regeln, dass bei Daten aus anderen schwerwiegenden Grundrechtseingriffen eine weitere Verwendung inhaltlich auf Konstellationen zu begrenzen ist, 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,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 118.

Auch dadurch, dass der Gesetzgeber lediglich von „eingeschränkter Verwendbarkeit“ spricht, wird er den verfassungsrechtlichen Anforderungen des Gesetzesvorbehalts nicht gerecht, da dies nicht nur nicht ausreichend normenklar, sondern darüber hinaus vor dem Hintergrund der Schwere des Grundrechtseingriffs, auch mit Blick auf die Heimlichkeit der Maßnahme, zu unbestimmt ist. Indem die Verwaltung dafür abstrakte Regelungen treffen soll, delegiert der Gesetzgeber eine wesentliche Entscheidung, die er nach der Wesentlichkeitstheorie selbst treffen muss, an die Exekutive. Aber gerade bei grundrechtsintensiven Maßnahmen wie der automatisierten Anwendung zur Datenanalyse, erfordert der Gesetzesvorbehalt eine erhöhte Regelungsdichte (siehe oben **D.I.1.b**)).

Der Gesetzgeber entzieht sich mithin seiner verfassungsrechtlichen Verantwortung, selbst festzulegen oder jedenfalls hinreichend konkrete Vorgaben zu machen, unter welchen Voraussetzungen ein schwerwiegender Grundrechtseingriff vorliegt. Dies könnte normativ beispielsweise in Form einer Auflistung von Erhebungstatbeständen erfolgen.

Der Gesetzgeber muss im Wesentlichen auch selbst bestimmen, welche Datensätze welcher Tatbestandsalternative des § 25a Abs. 2 Nr. 1 bis Nr. 3 HSOG zugeordnet werden: So müsste er sicherstellen, dass bei Nr. 2 (konkretisierte Gefahr für die Begehung einer Straftat von lediglich erheblicher Bedeutung), um den Grundsatz der Zweckbindung zu wahren, keine Daten einbezogen werden dürfen, die nur bei schweren oder besonders schweren Straftaten erhoben werden dürfen.

Bei diesen Maßgaben handelt es sich weder um technische oder organisatorische Details noch um eine Regelung von Gegebenheiten, die einem sich schnell verändernden Kenntnisstand unterliegen, und darum durch den untergesetzlichen Normgeber geregelt werden dürfen. Vielmehr verschiebt der Gesetzgeber die Definition erforderlicher Entscheidungsmaßstäbe in den Bereich der Exekutive.

Der Gesetzgeber muss zudem regeln, dass die Einschränkung durch entsprechende technische und organisatorische Vorkehrungen wirksam gesichert wird. Insbesondere müssen Informationen aus eingriffsintensiver Datenerhebung vorab gekennzeichnet oder abgetrennt werden,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1
BvR 2634/20, Rn. 118.

Der Gesetzgeber gibt hingegen lediglich vor, dass der untergesetzliche Normgeber nach Schwere des Grundrechtseingriffs bei der Erhebung kategorisieren muss. Ob damit eine entsprechende Kennzeichnung oder Trennung der zusammengeführten Datenbestände vorab verbunden sein soll, geht aus der Norm nicht klar hervor, zumal auch das Verhältnis zu § 20a HSOG unklar ist **(D.I.2.a)(5)(b))**. Lediglich der Begriff des Konzepts der Kategorisierung und Kennzeichnung lässt darauf schließen, dass der Gesetzgeber wahrscheinlich eine Kennzeichnung der Daten vor Augen hatte. Eine entsprechende Pflicht findet sich in der Norm aber nicht.

Zwar kann der Gesetzgeber die konkrete Ausgestaltung entsprechender Schutzmaßgaben der Verwaltung überlassen,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 118,

allerdings sind damit organisatorische und technische Einzelheiten gemeint,

vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR
1547/19, 1 BvR 2634/20, Rn. 112,

also konkret, wie eine Kennzeichnung technisch und organisatorisch
umzusetzen ist, nicht aber die Normierung einer Kennzeichnungspflicht im
Sinne der Entscheidung für ein bestimmtes Schutzkonzept an sich.

b) Unzureichende Einschränkung der Methoden der Datenanalyse

Auch die zugelassene Methode beeinflusst die Eingriffsintensität,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 90 ff.

Da diese nicht beschränkt ist, sondern vielmehr komplexe Analysen zulässt, den
Einsatz von Künstlicher Intelligenz (KI) nicht hinreichend klar ausschließt und
der Gesetzgeber keine Vorkehrungen zur Verhinderung der Realisierung von
Diskriminierungsrisiken getroffen hat, handelt es sich auch unter diesem
Gesichtspunkt um einen schwerwiegenden Eingriff.

(1) Keine Beschränkung der zugelassenen Methode

§ 25a HSOG bietet die Möglichkeit komplexer Analysen, da die Zahl der
Ableichschritte nicht von vorherein begrenzt ist. Die Norm eröffnet
weitreichende Möglichkeiten einer Datenanalyse.

Gem. § 25a Abs. 1 Satz 2 HSOG dürfen Polizeibehörden die zusammengeführten
Daten, auch gemeinsam mit weiteren rechtmäßig erhobenen
personenbezogenen Daten, verknüpfen, aufbereiten und auswerten sowie für
statistische Zwecke anwenden.

Diese Legaldefinition der automatisierten Anwendung zur Datenanalyse lässt kaum erkennen, dass es sich in der Sache um eine von Algorithmen gesteuerte Datei-, Format- und datenbankübergreifende Recherche und Analyse von personenbezogenen Daten zur Generierung neuen Wissens und neuer Erkenntnisse handelt, die in sehr großen Datenbeständen unter regelmäßiger Durchbrechung der datenschutzrechtlichen Zweckbindung erfolgt,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 25.

Das Ausmaß des Eingriffs ist für betroffene Personen somit kaum nachvollziehbar, sodass die Regelung schon aus Gründen der Normenklarheit verfassungswidrig ist.

Mit der Formulierung sind den Abgleichschritten und der maschinellen Erstellung von Verknüpfungen keine Grenzen gesetzt. Die Leistung und Charakteristik der für das Data-Mining verwendeten Algorithmen wird dadurch in keiner Weise eingeschränkt,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 42.

Allein der Vorgang des Auswertens kann alle technischen Möglichkeiten einer Datenanalyse erfassen.

Die in § 25a Abs. 1 Satz 3 HSOG enthaltene Beschreibung der Anwendung zur automatisierten Datenanalyse als lediglich technisches Hilfsmittel der Polizei, das es den Polizeibehörden ermöglichen soll, ihre Bewertungen, Prognosen und Entscheidungen auf der Grundlage möglichst verlässlicher Tatsachenfeststellungen zu treffen, verschleiert erstens das Ausmaß des Eingriffs. Solche Software ist kein bloßes Hilfsmittel, wie beispielsweise ein Textverarbeitungsprogramm, sondern dient dazu, neues grundrechtsrelevantes Wissen zu generieren, bis hin zur Erstellung umfassender Persönlichkeitsprofile. Zweitens ist keinesfalls sichergestellt, dass der Einsatz zu verlässlichen Tatsachenfeststellungen führt, vielmehr hängt die Verlässlichkeit von der Ausgestaltung des Programms, unter anderem dessen Fehleranfälligkeit, der Datenqualität und davon ab, ob Vorkehrungen gegen die Verstärkung von Diskriminierungsrisiken getroffen wurden,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 82 ff.

Die Anwendung der zusammengeführten Daten für statistische Zwecke ermöglicht es, eine Datenanalyse durchzuführen, um allein statistische Auffälligkeiten in den Datenmengen zu entdecken, aus denen dann, möglicherweise auch mit Hilfe weiterer automatisierter Anwendungen, weitere Schlüsse gezogen werden.

Auch die Art der Suchergebnisse ist vom Gesetzgeber nicht beschränkt worden. Vielmehr sind neue personenbezogene Erkenntnisse und maschinelle Sachverhaltsbewertungen möglich.

Ferner ist die Verwendung der durch die Analyse neu erlangten Informationen nicht an spezifische Voraussetzungen geknüpft, die die Folgen für Betroffene absehbar machen.

Daraus ergibt sich eine hohe Eingriffsintensität,

vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 98 f.

Gem. § 25a Abs. 1 Satz 4 HSOG erfolgt die automatisierte Anwendung zur Datenanalyse immer anhand anlassbezogener und zielgerichteter Suchkriterien. Weder finden sich in der Norm selbst nähere Vorgaben zu möglichen Suchkriterien, noch gibt der Gesetzgeber der Verwaltung die Festlegung solcher Kriterien auf. Somit ist der normative Gehalt des § 25a Abs. 1 Satz 4 HSOG denkbar gering. Offene Suchvorgänge werden durch die Voraussetzung, dass die automatisierte Anwendung zur Datenanalyse immer anhand zielgerichteter Suchkriterien erfolgt, gerade nicht ausgeschlossen. Denn diese Suchkriterien werden in § 25a HSOG nicht näher spezifiziert oder eingegrenzt, sondern können selbst entsprechend offen formuliert sein.

Dass ein polizeilicher Informationseingriff nicht anlass- oder ziellos erfolgen darf, ist auch ohne die Regelung eine rechtsstaatliche Selbstverständlichkeit,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 42.

Das hat auch das angerufene Gericht betont: 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,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 95.

Gem. § 25a Abs. 3 Satz 4 HSOG orientieren sich die Konzepte unter anderem an der Angemessenheit der jeweils angewandten Analysemethode. Abgesehen davon, dass vollkommen unklar ist, was daraus konkret für die Ausgestaltung solcher Konzepte folgen soll (**D.I.2.a)(5)(c)**), können daraus jedenfalls keine Rückschlüsse auf Einschränkungen der zulässigen Analysemethoden gezogen werden.

Die Komplexität der automatisierten Datenanalyse soll aber auch darüber hinaus vom untergesetzlichen Normgeber aufgegriffen werden: Gem. § 25a Abs. 3 Nr. 2 lit. a Satz 2 HSOG folgt das Konzept der Kategorisierung und Kennzeichnung dem Prinzip, wonach eine automatisierte Datenanalyse umso komplexer sein darf, je gewichtiger der Veranlassungszusammenhang ist, und dass sie umso einfacher sein muss, je weniger gewichtig der Veranlassungszusammenhang ist.

Damit normiert der Gesetzgeber erneut lediglich den Grundsatz der Verhältnismäßigkeit. Darüber hinaus kann das Prinzip schon aus Gründen der Normenklarheit und des Bestimmtheitsgrundsatzes keine wirksame Einschränkung der Methoden darstellen,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 43.

Es ist vollkommen unklar, wie sich das Gewicht des Veranlassungszusammenhangs konkret auf die angewandte Methode auswirken soll. Erstens sind im Rahmen der Analyse Daten von Personen mit ganz unterschiedlichen Veranlassungszusammenhängen betroffen, zweitens

ist der Analysevorgang als ein Gesamtvorgang zu betrachten, sodass nicht einleuchtet, inwiefern sich die Methode dann aber pro angewandtes Datum in einem einzigen Vorgang unterscheiden soll.

Ferner wird nicht geregelt, wodurch sich eine „komplexe“ von einer „einfachen“ Analyse unterscheidet oder welche Komplexitätsabstufungen überhaupt denkbar sind.

§ 25a Abs. 3 Nr. 2 lit. a Satz 2 HSOG missachtet auch den Vorbehalt des Gesetzes, da dem untergesetzlichen Normgeber ohne hinreichend normenklare und bestimmte Vorgaben, nicht einmal als Pflicht, vielmehr als Prinzip, aufgegeben wird, je nach Veranlassungszusammenhang Beschränkungen der Komplexität des Analysevorgangs vorzunehmen.

Der Gesetzgeber muss aber 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 Abgleichsschritte zur Verknüpfung der Abgleichergebnisse mit weiteren Datenbeständen erfolgen. Eine Beschränkung der Abgleichmöglichkeiten müsste vielmehr im Gesetz selbst angelegt sein,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 121.

Eine solche Beschränkung findet sich in § 25a HSOG aber gerade nicht.

(2) Kein Ausschluss von Künstlicher Intelligenz

Als besonders eingriffsintensiv stellt sich § 25a HSOG auch deshalb dar, weil der Einsatz Künstlicher Intelligenz nicht ausgeschlossen ist.

Gem. § 25a Abs. 1 Satz 5 HSOG wird die automatisierte Anwendung zur Datenanalyse manuell ausgelöst und läuft regelbasiert auf einer von Menschen

definierten Abfolge von Analyse- und Verarbeitungsschritten ab (§ 25a Abs. 1 Satz 5 HSOG).

Der Gesetzgeber beabsichtigt, den Einsatz selbstlernender Systeme auszuschließen, indem er versucht, den exklusiven Einsatz deterministischer Systeme zu beschreiben,

LT-Drs. 20/11235, S. 7.

Das angerufene Gericht versteht – in Abgrenzung zu KI – unter deterministischen Systemen solche, deren Analysefunktion sich nicht eigenständig verändern kann, sondern in der Software unveränderlich vorprogrammiert ist,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 101.

Dass nur deterministische Systeme in diesem Sinne zur Anwendung kommen dürfen, geht aber aus dem Wortlaut nicht hinreichend deutlich hervor, sodass die Norm gegen den Bestimmtheitsgrundsatz verstößt.

Denn „regelbasiert“ trifft keine Aussage darüber, von wem und zu welchem Zeitpunkt die Regeln des Systems definiert werden,

vgl. *Bäuerle*, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a
Rn. 27 f.

Zwar muss die „Abfolge der Analyse- und Verarbeitungsschritte“ von Menschen definiert sein. Der Wortlaut legt den Schluss nahe, dass zwischen den „Regeln“ des Systems und der „Abfolge“ der Analyse- und Verarbeitungsschritte ein Unterschied besteht, die Regeln also nicht unbedingt von Menschen definiert sein müssen.

Selbst wenn die Abfolge der Analyse- und Verarbeitungsschritte eines Systems von Menschen definiert ist, können diese, ohne gegen § 25a Abs. 1 Satz 5 HSOG zu verstoßen, in der Durchführung der Schritte mit selbstlernenden Systemen arbeiten, die die Regeln (Wenn-dann-Muster) für den jeweiligen Schritt erzeugen.

Dies gilt insbesondere für den Einsatz sogenannter schwacher KI-Systeme, die von Menschen programmiert, manuell ausgelöst und insoweit regelbasiert ablaufen, als sie eine Abfolge von Analyse- und Verarbeitungsschritten vornehmen. Der Unterschied zu Programmen mit starr deterministischen („wenn-dann“) Algorithmen besteht lediglich darin, dass sich die hier verwendeten Algorithmen im Rahmen der Verarbeitungsschritte anhand der analysierten Daten durch das Erkennen von Varianten und Mustern optimieren (können),

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 27.1, 85.

Jedenfalls der Einsatz von KI bei der Vorprogrammierung der Regeln entsprechender Systeme ist nicht ausgeschlossen.

Grundsätzlich gliedert sich der Lernzyklus eines selbstlernenden Systems in die Phase der Datenerhebung und des Aufbereitens, die Phase der Modellableitung und des Lernvorgangs sowie die Anwendungsphase.

Hüger, Künstliche Intelligenz und Diskriminierung, 2023, S. 55 ff. m.w.N.

Während einige Trainingsmethoden mit Abschluss der Trainingsphase ein finales, starres Modell erzeugen, ermöglichen andere Trainingstechniken eine stetige Selbstanpassung des Systems auf Grundlage einer sich ständig verändernden Fallbasis, sodass eine klare Trennung in Trainings- und Anwendungsphase nicht mehr möglich ist,

Hüger, Künstliche Intelligenz und Diskriminierung, 2023, S. 61 m.w.N.

Auch wenn eine Selbstanpassung des Systems in der Anwendungsphase ausgeschlossen wäre, würden sich die Gefahren des Einsatzes lernfähiger Systeme dann lediglich in den Bereich der Vorprogrammierung verlagern. Auch hier können sich diskriminierende Muster herausbilden, die dann in der Anwendung fortwirken.

Denn die zentralen technischen Ursachen algorithmenbasierter Diskriminierungen sind auf der Ebene der Trainingsdaten zu verorten,

Hüger, Künstliche Intelligenz und Diskriminierung, 2023, S. 113 m.w.N.

Aber auch der Lernvorgang birgt Diskriminierungsrisiken, etwa bei der Bestimmung der Zielvariablen für den Modellierungsprozess. Im Modellierungsprozess selbst verstärken sich die im Trainingssatz vorhandenen diskriminierenden Verzerrungen. In der Anwendungsphase kommt es dann zu Bestätigungsverzerrungen durch Feedback-Schleifen,

vgl. Hüger, Künstliche Intelligenz und Diskriminierung, 2023, S. 120 ff. m.w.N.

Vor diesem Hintergrund ist es zwar als positiv zu bewerten, dass die Software mit den Polizeidaten nicht weiterlernen darf. Trotzdem kann dieser Ausschluss das Eingriffsgewicht nicht reduzieren, wenn der Einsatz selbstlernender Systeme in der Vorprogrammierung nicht ausgeschlossen ist.

(3) Keine Vorkehrungen zur Vermeidung von Diskriminierung

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,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 95.

Da die Anwendung auch zu statistischen Zwecken erfolgen darf, muss der Gesetzgeber entsprechende Vorkehrungen treffen.

Auch die Möglichkeit des Einsatzes von KI erfordert besondere verfahrensrechtliche Vorkehrungen, die trotz der eingeschränkten Nachvollziehbarkeit ein hinreichendes Schutzniveau sichern, um die Herausbildung und Verwendung diskriminierender Algorithmen zu verhindern,

vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.

Dafür kommt eine Reihe von technisch-organisatorischen Maßnahmen in Betracht, die zum Teil bereits vor der Anwendungsphase stattfinden, wie etwa die Nutzung ausgewogener Trainingsdaten,

Hüger, Künstliche Intelligenz und Diskriminierung, 2023, S. 158 ff. m.w.N.

Dies kann aber nur wirksam umgesetzt werden, wenn der Staat selbst maßgeblichen Einfluss auf die Entwicklung entsprechender Software hat.

Aber auch Maßnahmen zur Transparenzerhöhung kommen in Betracht, wie etwa Tests und Audits, um die Funktionsweise der eingesetzten Software zu rekonstruieren. Insbesondere Begründungen im Sinne einer *Explainable AI* können dazu beitragen, später Anhaltspunkte für Diskriminierungen zu erhalten,

Hüger, Künstliche Intelligenz und Diskriminierung, 2023, S. 153 ff. m.w.N.

Auch der EuGH weist darauf hin, dass gerade im Hinblick auf die Gewährleistung von effektivem Rechtsschutz und Kontrolle transparent und nachvollziehbar sein muss, wie eine Software zu dem jeweiligen Ergebnis im Einzelfall kommt,

vgl. EuGH, Urteil v. 21. Juni 2022, C-817/19, Rn. 195.

Derartige Vorkehrungen sind aber an keiner Stelle vorgesehen.

Insofern die KI-Verordnung der Europäischen Union darauf abzielt, zukünftig Risiken, die mit dem Einsatz von KI verbunden sind, zu identifizieren und diesen entgegenzuwirken, entfaltet diese jedenfalls noch keine Wirkung. Schutzvorkehrungen, die Hoch-Risiko-Systeme betreffen, zu denen hessenDATA gehören wird, treten voraussichtlich erst im Juli 2027 in Kraft.

Auch Vorkehrungen zur Entdeckung und Korrektur von Fehlern der eingesetzten Datenauswertungstechnologie,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 102,

hat der Gesetzgeber nicht getroffen,

so auch *Bäuerle*, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a
Rn. 65 a.E.

Auch im landesrechtlichen Datenschutzrecht finden sich keine ausreichenden
Schutzvorkehrungen.

Insbesondere § 68 HDSIG, auf den auch § 20 Abs. 12 Satz 2 HSOG verweist,
schreibt zur Qualitätssicherung zwar eine Unterscheidung zwischen Tatsachen
und persönlichen Einschätzungen vor, eine Rechtsfolge bei Nichteinhaltung ist
daran aber nicht geknüpft,

Johannes, in: Roßnagel, Hessisches Datenschutz- und
Informationsfreiheitsgesetz, 1. Auflage 2021, § 68 Rn. 16 f.

§ 66 HDSIG stellt zwar grundsätzliche Anforderungen an die
datenschutzgerechte Gestaltung von Datenverarbeitungssystemen (Privacy by
Design) und die Implementierung datenschutzfreundlicher Voreinstellungen
(Privacy by Default),

Johannes, in: Roßnagel, Hessisches Datenschutz- und
Informationsfreiheitsgesetz, 1. Auflage 2021, § 66 Rn. 1.

Die technischen und organisatorischen Maßnahmen dienen dazu, die
allgemeinen Grundsätze nach § 42 HDSIG umzusetzen,

Roßnagel in: ders., Hessisches Datenschutz- und
Informationsfreiheitsgesetz, 1. Auflage 2021, § 42 Rn. 15.

Ob und in welchem Umfang daraus verpflichtende Maßnahmen zur
Vermeidung von Diskriminierung im Rahmen von § 25a HSOG folgen, bleibt
aber unklar. Insbesondere im Hinblick darauf, dass die Auswahl der
Maßnahmen einer Abwägung zugänglich ist,

Johannes, in: Roßnagel, Hessisches Datenschutz- und
Informationsfreiheitsgesetz, 1. Auflage 2021, § 66 Rn. 18 ff.,

dürfte die Wirksamkeit dieser Regelung im Hinblick auf schwere Grundrechtseingriffe nach § 25a HSOG mindestens zweifelhaft sein. Sie zielt außerdem schon nicht explizit auf die Vermeidung von Diskriminierung.

Gerade wenn der Staat auf kommerzielle Anbieter zurückgreift, kann er maximal über Ausschreibungen Einfluss auf die Technikgestaltung nehmen,

Johannes, in: Roßnagel, Hessisches Datenschutz- und Informationsfreiheitsgesetz, 1. Auflage 2021, § 66 Rn. 14.

Das ist aber bei derart schweren Grundrechtseingriffen mittels einer Analyse mit unbegrenzt vielen Abgleichsschritten nicht ausreichend.

§ 59 HDSIG enthält Anforderungen an die Sicherheit der Datenverarbeitung, betrifft damit die Integrität und Vertraulichkeit nach § 42 Nr. 6 HDSIG,

Johannes, in: Roßnagel, Hessisches Datenschutz- und Informationsfreiheitsgesetz, 1. Auflage 2021, § 68 Rn. 5,

und zielt mithin nicht auf die Verhinderung von Diskriminierungen.

Auch die defizitär ausgestaltete datenschutzrechtliche Kontrolle vermag keine geeignete Sicherung darzustellen (siehe dazu **D.II.2.**). Von der Protokollierungspflicht gem. § 28 Abs. 2 HSOG ist § 25a HSOG nicht erfasst.

II. Nichtbeachtung der korrespondierenden Eingriffsvoraussetzungen

Die Tatbestandsalternativen des § 25a Abs. 2 Satz 1 Nr. 2 und Nr. 3 HSOG genügen nicht den verfassungsrechtlichen Rechtfertigungsanforderungen, die der Grundsatz der Verhältnismäßigkeit an derart intensive Grundrechtseingriffe stellt **(1.)**. Ferner genügt § 25a HSOG insgesamt nicht den verfassungsrechtlichen Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle **(2.)**.

1. Eingriffsschwellen und zu schützende Rechtsgüter des § 25a Abs. 2 Satz 1 Nr. 2 und Nr. 3 HSOG

Die Tatbestandsalternativen des § 25a Abs. 2 Satz 1 Nr. 2 und Nr. 3 HSOG genügen nicht den verfassungsrechtlichen Anforderungen an Eingriffsschwelle und Rechtsgüterschutz für eingriffsintensive heimliche Überwachungsmaßnahmen **(a)**). Auch bei § 25a Abs. 1 Satz 1 Nr. 1 HSOG handelt es sich um einen schwerwiegenden Grundrechtseingriff. Jedenfalls die darin vorgesehene Eingriffs- und Rechtsgüterschwelle genügt aber im Gegensatz zu den anderen beiden Tatbestandsvarianten den verfassungsrechtlichen Anforderungen.

Selbst wenn das Gericht zu der Auffassung gelangen sollte, dass der Gesetzgeber ausreichend Einschränkungen getroffen habe, um das Eingriffsgewicht zu reduzieren, wären auch in diesem Fall die verfassungsrechtlichen Anforderungen nicht erfüllt **(b)**).

a) Bei hoher Eingriffsintensität

Heimliche Überwachungsmaßnahmen, die tief in das Privatleben hineinreichen, sind nur zum Schutz besonders gewichtiger Rechtsgüter zulässig, zu denen vor allem Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes zählen,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 105.

Der Gesetzgeber muss die Rechtsgüter nicht unmittelbar benennen, sondern kann auch an entsprechende Straftaten anknüpfen, deren Verhütung er mit der Befugnis bezweckt,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 105 a.E.

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,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1
BvR 2634/20, Rn. 106.

Weder § 25a Abs. 2 Satz 1 Nr. 2 **((1))** noch Nr. 3 **((2))** HSOG erfüllen diese Voraussetzungen.

(1) § 25a Abs. 2 Satz 1 Nr. 2 HSOG

§ 25a Abs. 2 Satz 1 Nr. 2 HSOG genügt diesen verfassungsrechtlichen Anforderungen an Rechtsgüterschutz und Eingriffsschwelle nicht, da die Tatbestandsvariante schon die Verhinderung von Straftaten mit lediglich erheblicher Bedeutung ausreichen lässt **((a))** und einen Eingriff unterhalb der konkretisierten Gefahr im Gefahrenvorfeld zulässt **((b))**,

so auch *Bäuerle*, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a
Rn. 62 f. hinsichtlich der Anforderungen an die zu schützenden
Rechtsgüter.

(a) Zu schützende Rechtsgüter

Unter erheblichen Straftaten versteht der Gesetzgeber die in § 13 Abs. 3 Satz 1 HSOG enthaltenen Straftaten,

LT-Drs. 20/11235, S. 11.

Die Bezugnahme auf § 13 Abs. 3 Satz 1 HSOG ist unter mehreren Gesichtspunkten verfassungsrechtlich problematisch.

Erstens erfasst § 13 Abs. 3 Satz 1 Nr. 2 HSOG Straftatbestände, die bloße Vergehen darstellen, unter der Einschränkung, dass die Vergehen im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören.

Unter den in § 13 Abs. 3 Satz 1 Nr. 2 lit. a und lit. c HSOG genannten Straftaten finden sich vor allem auch solche, die nicht dem Schutz besonders gewichtiger Rechtsgüter dienen. Dies gilt insbesondere für die dort genannten Delikte gegen bedeutende Sach- oder Vermögenswerte und die gewerbs-, gewohnheits-, serien- oder bandenmäßig oder sonst organisiert begangenen Straftaten,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 36.

Zweitens sieht sich die Regelung insgesamt Kritik hinsichtlich ihrer Bestimmtheit ausgesetzt,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 13 Rn. 121 f., § 25a Rn. 35,

zumal keine abschließende Aufzählung von Delikten erfolgt.

Im Hinblick darauf, dass es sich bei § 25a HSOG um schwerwiegende heimliche Grundrechtseingriffe handelt und deshalb besondere verfassungsrechtliche Anforderungen an die Bestimmtheit zu stellen sind, ist § 25a Abs. 2 Satz 1 Nr. 2 HSOG i.V.m. § 13 Abs. 3 Satz 1 HSOG zu unbestimmt. Für Rechtsanwender*innen ist nicht hinreichend klar, welche Tatbestände im Ergebnis darunter zu fassen sind, sodass die Gefahr besteht, dass § 25a Abs. 2 Satz 1 Nr. 2 HSOG bereits bei Bagatelldelikten, wie einfachen Körperverletzungen oder dem Besitz von Betäubungsmitteln Anwendung findet.

Drittens fallen unter § 13 Abs. 3 Satz 1 HSOG auch sogenannte Vorfeldstraftaten.

Vorfeldstraftaten sind solche Straftatbestände, die auch Verhaltensweisen erfassen, die vom Gesetzgeber als generell gefährlich für gewichtige

Individualrechtsgüter (vor allem Leben, Leib und Freiheit) und gewichtige Kollektivrechtsgüter (etwa die äußere und innere Sicherheit des Staates) bewertet werden, aber als einzelne Handlungen in räumlicher oder zeitlicher Hinsicht noch vor einer konkreten Gefährdung oder gar Verletzung solcher Rechtsgüter liegen können,

vgl. BVerfG, Beschluss des Ersten Senats vom 09. Dezember 2022, 1 BvR 1345/21, Rn. 50.

§ 13 Abs. 3 Satz 1 Nr. 2 lit. b HSOG umfasst beispielsweise § 149 StGB. Aber auch die §§ 89a bis 89c StGB (gem. § 13 Abs. 3 Satz 1 Nr. 2 lit. b HSOG i.Vm. § 74a Abs. 1 Nr. 2 GVG) sowie §§ 129a, 129b StGB (gem. § 13 Abs. 3 Satz 1 Nr. 2 lit. b HSOG i.Vm. § 120 Abs. 1 Nr. 6 GVG) sind davon erfasst. Außerdem wurden nun auch die §§ 86a, 126, 130, 130a StGB (gem. § 13 Abs. 3 Satz 1 Nr. 2 lit. b HSOG) explizit aufgenommen.

Will der Gesetzgeber an solche Vorfeldstraftaten anknüpfen, muss er aber sicherstellen, dass in jedem Einzelfall eine konkrete oder konkretisierte Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegt. Er muss also zusätzlich fordern, dass damit bereits eine konkretisierte Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegt,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 170; BVerfG, Beschluss des Ersten Senats vom 28. September 2022, 1 BvR 2354/13, Rn. 134.

Der Gesetzgeber hat aber keine derartigen sicherstellenden Vorgaben getroffen,

so auch *Bäuerle*, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 36.

Weiterhin knüpft § 13 Abs. 3 Satz 1 Nr. 2 lit. b HSOG an § 74a und § 120 GVG an. Der schlichte Verweis auf § 120 GVG ist zu unbestimmt, wie das angerufene Gericht im Urteil zum Bundesverfassungsschutzgesetz (BVerfSchG) ausgeführt hat. Denn § 120 Abs. 2 Nr. 1-4 GVG setzt insbesondere voraus, dass der Generalbundesanwalt die Verfolgung übernimmt,

BVerfG, Beschluss des Ersten Senats vom 28. September 2022, 1 BvR 2354/13, Rn. 144.

Es ist auch vorliegend nicht klar, ob und wie diese zusätzliche Tatbestandsvoraussetzung geprüft werden muss.

(b) Eingriffsschwelle

Außerdem genügt die Eingriffsschwelle nicht den verfassungsrechtlichen Anforderungen. Denn die Definition der konkretisierten Gefahr in § 25a Abs. 2 Satz 1 Nr. 2 HSOG deckt sich nicht mit den Anforderungen, die das angerufene Gericht an eine konkretisierte Gefahr stellt. 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 erstens den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zweitens darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 106 m.w.N.

Der hessische Gesetzgeber lässt für die konkretisierte Gefahr in § 25a Abs. 2 Satz 1 Nr. 2 HSOG hingegen ausreichen, dass tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraumes auf eine zumindest ihrer Art nach konkretisierte Weise Straftaten [...] begangen

werden. Der zweite Aspekt, nämlich dass sich die Prognose aber auch darauf beziehen muss, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann, ist in der Definition nicht enthalten. Insofern bleibt § 25a Abs. 2 Satz 1 Nr. 2 HSOG hinter den verfassungsrechtlichen Anforderungen zurück.

(2) § 25a Abs. 2 Satz 1 Nr. 3 HSOG

Auch § 25a Abs. 2 Satz 1 Nr. 3 HSOG genügt den verfassungsrechtlichen Anforderungen an Rechtsgüterschutz **((a))** und Eingriffsschwelle **((b))** nicht.

(a) Zu schützende Rechtsgüter

Zwar zielt § 25a Abs. 2 Satz 1 Nr. 3 HSOG hinsichtlich des Rechtsgüterschutzes auf die Verhinderung schwerer oder besonders schwerer Straftaten. Allerdings erfolgt auch in dieser Tatbestandsvariante keine abschließende Aufzählung von Delikten. Laut der Gesetzesbegründung sollen schwere Straftaten solche sein, die mit einer Höchststrafe von mindestens fünf Jahren Freiheitsstrafe bedroht sind, und besonders schwere Straftaten solche, die mit einer Höchststrafe von mindestens zehn Jahren Freiheitsstrafe bedroht sind. Maßgeblicher Anknüpfungspunkt für die Einordnung sei der abstrakte Strafrahmen, wie er vom Gesetzgeber für eine bestimmte Straftat festgelegt werde. Praktisch relevant seien vor allem die Straftatenkataloge der §§ 100a Abs. 2, 100b Abs. 2 StPO,

LT-Drs. 20/11235, S. 11.

Abgesehen davon, dass sich diese Erwägungen nicht im Gesetz widerspiegeln, fallen nach der Definition der Gesetzesbegründung auch Vorfeldstraftatbestände darunter, namentlich §§ 89a, 129, 129a, 129b, 149 StGB. Dies ist insbesondere in Kombination mit der Eingriffsschwelle verfassungsrechtlich problematisch (dazu sogleich **(b))**.

(b) Eingriffsschwelle

Sachverhalte, die unter die Tatbestandsvariante des § 25a Abs. 2 Satz 1 Nr. 3 HSOG subsumiert werden können, liegen im Gefahrenvorfeld, also unterhalb der Schwelle einer konkretisierten Gefahr, was für sich schon nicht den verfassungsrechtlichen Anforderungen an schwerwiegende Grundrechtseingriffe entspricht.

Da die Tatbestandsvariante auch Vorfeldstraftatbestände beinhaltet, ist eine doppelte Vorverlagerung gegeben. Es werden gerade nicht nur Konstellationen erfasst, die darauf zielen, typische Serienstraftaten, wie Wohnungseinbruchsdiebstahl, vorherzusehen und zu verhindern,

vgl. *Löffelmann*, JR 2023, 331 (342).

Die Tatbestandsvariante kommt, soweit sie Vorfeldtatbestände einbezieht, einer anlasslosen automatisierten Auswertung personenbezogener Daten gleich, zumal der Grundsatz der Zweckbindung nicht sichergestellt ist (siehe oben **D.I.2.a)(5)**). Eine anlasslose automatisierte Auswertung personenbezogener Daten hat das angerufene Gericht als unzulässig eingestuft,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 108.

b) Bei reduziertem Eingriffsgewicht (hilfsweise)

Aber selbst wenn das angerufene Gericht entgegen der Auffassung der Beschwerdeführer*innen zu dem Ergebnis kommen sollte, dass das Eingriffsgewicht hinreichend reduziert sei, wären die verfassungsrechtlichen Anforderungen nicht erfüllt.

Während 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,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1
BvR 2634/20, Rn. 107.

§ 25a Abs. 2 Satz 1 Nr. 2 HSOG geht auf Seiten des Rechtsgüterschutzes deutlich über den Schutz besonders gewichtiger Rechtsgüter hinaus. Dann müsste mindestens die Eingriffsschwelle streng sein. Allerdings bleibt auch diese hinter den Anforderungen an eine konkretisierte Gefahr zurück (siehe oben **D.II.1. a)(1)(b)**).

§ 25a Abs. 2 Satz 1 Nr. 3 HSOG knüpft zwar an die Verhinderung schwerer oder besonders schwerer Straftaten an. Allerdings ermöglicht die Norm durch ihre doppelte Vorverlagerung im Ergebnis eine anlasslose Datenanalyse (siehe oben **D.II.1. a)(1)(b)**).

2. Defizitäre datenschutzrechtliche Kontrolle hinsichtlich aller Tatbestandsvarianten

§ 25a HSOG genügt in keiner seiner Tatbestandsvarianten (§ 25a Abs. 2 Satz 1 Nr. 1 bis Nr. 3 HSOG) den Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle,

so auch *Bäuerle*, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a
Rn. 65,

a) Maßstab

Diese folgen aus dem Verhältnismäßigkeitsgrundsatz,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 109 m.w.N.,

und ergeben sich aus dem jeweiligen Grundrecht in Verbindung mit Art. 19
Abs. 4 GG,

BVerfGE 141, 220 (282 Rn. 134).

Der Verhältnismäßigkeitsgrundsatz stellt für tief in die Privatsphäre reichende Überwachungsmaßnahmen deshalb an eine wirksame Ausgestaltung dieser Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis gesteigerte Anforderungen,

BVerfGE 141, 220 (284 Rn. 140).

Insbesondere einer sachgerechten Ausgestaltung der Kontrolle kommt große Bedeutung zu,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 109.

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,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19,
1 BvR 2634/20, Rn. 109.

b) Kein ausreichendes Kontrollkonzept in § 25a HSOG

Gem. § 25a Abs. 4 Satz 6 HSOG ist die oder der behördliche Datenschutzbeauftragte zur Durchführung stichprobenartiger Kontrollen berechtigt. Angesichts dessen, dass es sich lediglich um ein Recht und keine Pflicht handelt, ist eine Kontrolle aber nicht sichergestellt.

Auch der Hessische Beauftragte für Datenschutz und Informationsfreiheit ist vor der Einrichtung oder einer wesentlichen Änderung lediglich anzuhören (§ 25a Abs. 5 Satz 2 HSOG). Gem. § 25a Abs. 5 Satz 3 HSOG bleiben seine Aufgaben und Befugnisse unberührt. Diese ergeben sich aus §§ 13, 14 HDSIG und legen keine verpflichtende Kontrolle fest. Die Norm ist insoweit deklaratorisch,

Bäuerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 115.

Ein solches Konzept ist aus verfassungsrechtlicher Sicht nicht ausreichend.

Angesichts der Kompensationsfunktion der aufsichtlichen Kontrolle für den schwach ausgestalteten Individualrechtsschutz kommt deren regelmäßiger Durchführung besondere Bedeutung zu und sind solche Kontrollen in angemessenen Abständen – deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf – durchzuführen,

BVerfGE 141, 220 (285 Rn. 141).

Wenn durch § 25a HSOG aber im Ergebnis kein*e Datenschutzbeauftragte*r zur Kontrolle verpflichtet wird, ist keine regelmäßige Durchführung gewährleistet.

c) Keine Sicherungen in anderen Bestimmungen des geltenden Rechts

§ 29a HSOG, der zu stichprobenartigen Kontrollen verpflichtet, ist auf § 25a HSOG nicht anwendbar, da die Norm nur für § 23 HSOG und die in § 28 Abs. 2 HSOG zu protokollierenden Maßnahmen gilt.

§ 64 Abs. 1 HDSIG schreibt vor, dass der*die Verantwortliche vor der Inbetriebnahme von neu anzulegenden Dateisystemen die*den Hessische*n Datenschutzbeauftragte*n zu konsultieren hat, wenn entweder aus einer Datenschutz-Folgenabschätzung nach § 62 HDSIG hervorgeht, dass die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft (Nr. 1), oder die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat (Nr. 2). Beide Voraussetzungen dürften beim geplanten Einsatz von Analysesoftware vorliegen, sodass eine Konsultation erfolgen muss. § 64 HDSIG sichert aber keine ausreichende datenschutzrechtliche Kontrolle, sondern verfolgt eine präventive Zielrichtung vor der Inbetriebnahme, indem der*die Datenschutzbeauftragte Empfehlungen aussprechen kann (§ 64 Abs. 3 HDSIG). Auf ähnliche Weise verfolgt auch die Pflicht zur Durchführung einer Datenschutzfolgenabschätzung nach § 62 HDSIG eine präventive Zielrichtung und kann eine Kontrolle nicht ersetzen.

Dabei ist insbesondere zu Bedenken, dass die geplante Software bereits im Einsatz ist. Das in § 65 HDSIG normierte Erfordernis eines Verzeichnisses von Verarbeitungstätigkeiten dient vor allem dazu, eine wirksame Kontrolle durch den*die Hessische*n Beauftragte*n für Datenschutz und Informationsfreiheit zu ermöglichen,

Johannes, in: Roßnagel, Hessisches Datenschutz- und Informationsfreiheitsgesetz, 1. Auflage 2021, § 65 Rn. 1.

Gleiches gilt für die Protokollierung nach § 71 HDSIG. Weiterhin kann § 66 HDSIG, der grundsätzliche Anforderungen an die datenschutzgerechte Gestaltung von Datenverarbeitungssystemen (Privacy by Design) und die Implementierung datenschutzfreundlicher Voreinstellungen (Privacy by Default) stellt (siehe dazu oben **D.I.2.b)(3)**), keine Kontrolle ersetzen. § 59 HDSIG zielt auf Datensicherheit und nicht auf die Sicherstellung der Rechtmäßigkeit der Datenverarbeitung und ist folglich keine Kontrollvorschrift. Meldepflichten und -rechte (§§ 60, 71 HDSIG) stellen auch keine hinreichende Sicherung dar, da sie ein aktives Tätigwerden des Verantwortlichen voraussetzen und lediglich Einzelfälle betreffen.

d) Keine Vorkehrungen gegen Fehleranfälligkeit

Obwohl § 25a HSOG den Einsatz komplexer Methoden ermöglicht (siehe oben unter **D.I.2.b)**), hat der Gesetzgeber keine flankierenden Schutzmaßnahmen getroffen.

Das angerufene Gericht fordert aber bei komplexeren Formen des automatisierten Abgleichs von Daten, dass Vorkehrungen gegen eine hiermit spezifisch verbundene Fehleranfälligkeit getroffen werden, was auch gesetzliche Regelungen zu einem staatlichen Monitoring der Entwicklung der eingesetzten Software erfordern kann,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 109.

Gerade im Hinblick darauf, dass auf das System eines privaten Anbieters zurückgegriffen wird, wäre es geboten gewesen, ein Monitoring normativ zu verankern,

Bauerle, in: BeckOK PolR Hessen, 32. Ed. 1.3.2024, HSOG § 25a Rn. 65a.

Prof. Dr. Tobias Singelstein