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

An das
Bundesverfassungsgericht
Schlossbezirk
76131 Karlsruhe

Frankfurt, den 23. September 2022

In dem Verfassungsbeschwerdeverfahren

Der Frau Silvia Gingold u.a.
– 1 BvR 1547/19 –

nehmen wir die Verfassungsbeschwerde zurück, soweit sie sich gegen gegen § 6 Satz 5, § 20 Abs. 2 Satz 3 HVSG und §§ 15b, 15c HSOG richtet. Soweit die Verfassungsbeschwerde sich gegen § 21 Abs. 2 HVSG richtet, nehmen wir die Rüge eines unzureichenden Kontrollregimes (Beschwerdeschrift S. 64, 4. Absatz) zurück. Im Übrigen wird an der Verfassungsbeschwerde festgehalten.

Wir stellen klar, dass die Verfassungsbeschwerde, soweit sie sich auf § 13 HVSG bezieht, nur gegen § 13 Abs. 1 HVSG gerichtet ist. Ebenso stellen wir klar, dass die Verfassungsbeschwerde, soweit sie sich auf § 16 HVSG bezieht, nur gegen § 16 Abs. 1 Satz 1 und Satz 2 HVSG gerichtet ist.

Des Weiteren erwidern wir auf die hier eingegangenen Stellungnahmen insbesondere der Hessischen Staatskanzlei („Stellungnahme Hessische Staatskanzlei“) und vertiefen unseren Vortrag im Hinblick auf das Urteil des Senats zum Bayerischen Verfassungsschutzgesetz vom 26. April 2022 (Az. 1 BvR 1619/17).

INHALTSVERZEICHNIS

A. VORBEMERKUNG 3

B. ZULÄSSIGKEIT 3
I. BESONDERE AUSKUNFTSERSUCHEN, § 10 ABS. 2 SATZ 1 NR. 1 HVSG 3
II. UNZUREICHENDE BESCHRÄNKUNG DER DATENVERARBEITUNG AUS WOHNRAUMÜBERWACHUNG UND ZUGRIFFEN AUF INFORMATIONSTECHNISCHE SYSTEME, §§ 16, 18 ABS. 3 HVSG 4
III. ÜBERMITTLUNGSBEFUGNIS, § 21 ABS. 2 HVSG 5
IV. FEHLENDE BZW. UNZUREICHENDE BENACHRICHTIGUNGSPFLICHTEN 5
V. UNZUREICHENDER AUSKUNFTSANSPRUCH, § 26 ABS. 1 HVSG 9
VI. AUTOMATISIERTE DATENANALYSE, § 25A HSOG 11

C. BEGRÜNDETHEIT 13
I. BESONDERE AUSKUNFTSERSUCHEN, § 10 ABS. 2 SATZ 1 NR. 1 HVSG 13
II. UNZUREICHENDE BESCHRÄNKUNG DER DATENVERARBEITUNG AUS WOHNRAUMÜBERWACHUNG UND ZUGRIFFEN AUF INFORMATIONSTECHNISCHE SYSTEME, §§ 16, 18 ABS. 3 HVSG 17
III. ÜBERMITTLUNGSBEFUGNIS, § 21 ABS. 2 HVSG 20
IV. FEHLENDE BZW. UNZUREICHENDE BENACHRICHTIGUNGSPFLICHTEN 20
V. UNZUREICHENDER AUSKUNFTSANSPRUCH, § 26 ABS. 1 HVSG 22
VI. AUTOMATISIERTE DATENANALYSE, § 25A HSOG 22
1. VERFASSUNGSRECHTLICHER MASSSTAB 22
2. UMFANG DES DATENANALYSE 23
3. ANFORDERUNGEN AN „DATA MINING“ NICHT ERFÜLLT 27
4. UNZULÄSSIGE DYNAMISCHE VERWEISUNG 30
5. GRUNDSATZ DER ZWECKÄNDERUNG 31
6. UNZUREICHENDE VERFAHRENSSICHERUNGEN 32

A. VORBEMERKUNG

Die Beschwerdeführenden nehmen zur Kenntnis, dass auch die Staatskanzlei von der Begründetheit der Verfassungsbeschwerde in Bezug auf die Befugnisnormen zur Mobilfunkortung (§ 9 HVSG), zum Einsatz von verdeckten Mitarbeiter*innen (§ 12 Abs. 1 HVSG), zum Einsatz von Vertrauensleuten (§ 13 HVSG) und verschiedener Übermittlungsbefugnisse (§ 20 Abs. 1 und Abs. 2 Satz 1 Nr. 2 HVSG) ausgeht. Obwohl damit auch die Staatskanzlei von der Verfassungswidrigkeit zentraler Teile des HVSG ausgeht und dieses Gesetz derzeit reformiert wird, sind bisher offenbar keine substantiellen Änderungen dieser Vorschriften geplant. So soll in § 9 HVSG lediglich ein Redaktionsversehen bereinigt werden, § 12 HVSG und § 13 HVSG sollen überhaupt nicht geändert werden und in § 20 Abs. 2 HVSG soll lediglich der Verweis auf das Bundespolizeigesetz aktualisiert werden,

LT-Drucksache 20/8129, S. 3 ff.

Auch die anderen geplanten Änderungen aus dem Gesetzentwurf ändern nichts an der Zulässigkeit und Begründetheit der Verfassungsbeschwerde.

B. ZULÄSSIGKEIT

Die Verfassungsbeschwerde ist, soweit sie nicht zurückgenommen wurde, zulässig.

I. BESONDERE AUSKUNFTSERSUCHEN, § 10 ABS. 2 SATZ 1 NR. 1 HVSG

Die von der Staatskanzlei geäußerten Zweifel an der Zulässigkeit,

Stellungnahme Hessische Staatskanzlei, S. 37 f.,

sind nicht begründet.

In der Beschwerdeschrift wurde ausdrücklich darauf hingewiesen, dass die Beschwerdeführenden zu 1 und 2 Verkehrsunternehmen im Sinne von § 10 Abs. 2 Satz 1 Nr. 1 HVSG in Anspruch nehmen.

Beschwerdeschrift, S. 16, 17,

Hinsichtlich der anderen Beschwerdeführenden ergibt sich dies aus dem Umstand, dass die Nutzung von Verkehrsunternehmen (zur Weite des Begriffs unter C.I.) in Deutschland üblich ist und die Beschwerdeführenden die Norm gerügt haben.

Die Zweifel der Staatskanzlei daran, dass die Norm eine Auskunftsverpflichtung begründet,

Stellungnahme Hessische Staatskanzlei, S. 37 f., 40,

sind nicht nachvollziehbar. Eine Verpflichtung ist zwar nicht ausdrücklich geregelt, ergibt sich aber aus dem Regelungszusammenhang. Bereits der Wortlaut von § 10 Abs. 2 Satz 1 HVSG, der das Landesamt ermächtigt, Auskünfte einzuholen, legt eine entsprechende Verpflichtung nahe. Jedenfalls ergibt sich diese aus § 10 Abs. 6 Satz 3 und 4, Abs. 7 Satz 2, Abs. 9 Satz 1 HVSG, in denen jeweils von „Verpflichteten“ die Rede ist. § 10 Abs. 9 Satz 2 spricht zudem von einer „Anordnung“, mit der ein Benachteiligungsverbot zu verbinden ist.

Letztlich kommt es auf die Verpflichtung jedoch nicht an. Ein Grundrechtseingriff liegt auch vor, wenn die in § 10 Abs. 2 Satz 1 Nr. 1 HVSG genannten Unternehmen die Auskünfte freiwillig erteilen. Es kann auch – eine fehlende Verpflichtung unterstellt – nicht mit hinreichender Gewissheit davon ausgegangen werden, dass sämtliche Unternehmen die Kooperation mit dem Landesamt verweigern.

II. UNZUREICHENDE BESCHRÄNKUNG DER DATENVERARBEITUNG AUS WOHNRAUMÜBERWACHUNG UND ZUGRIFFEN AUF INFORMATIONSTECHNISCHE SYSTEME, §§ 16, 18 ABS. 3 HVSG

Die Staatskanzlei meint, dass keine eigene und gegenwärtige Betroffenheit ausreichend dargelegt wurde, da die Beschwerdeführenden keine Umstände angegeben hätten, die es plausibel erscheinen lassen, dass Gefahrenabwehr- oder Strafverfolgungsbehörden bei ihnen Daten aus einer Online-Durchsuchung oder Wohnraumüberwachung erheben würden, die anschließend an das Landesamt für Verfassungsschutz übermittelt werden könnten,

Stellungnahme Hessische Staatskanzlei, S. 49, 56 f.

Hierauf ist zu entgegnen, dass mit der vorliegenden Verfassungsbeschwerde nicht die Rechtsgrundlagen im Polizeigesetz bzw. der Strafprozessordnung zur Datenerhebung angegriffen werden, sondern allein zur Datenweiterverarbeitung durch den Verfassungsschutz. Dass der Verfassungsschutz ein gesteigertes Interesse an den Daten der Beschwerdeführenden hat, wurde hinreichend dargelegt. Woher und aus welchen geheimen Maßnahmen diese Daten stammen, können die Beschwerdeführenden nicht wissen. Es ist zudem auch hinreichend wahrscheinlich, dass die Beschwerdeführenden Ziel von Online-Durchsuchung oder Wohnraumüberwachung nach Polizei- oder Strafprozessrecht sind. Ein Vortrag, für sicherheitsgefährdende oder nachrichtendienstlich relevante Aktivitäten verantwortlich zu sein, ist zum Beleg der Selbstbetroffenheit grundsätzlich ebenso wenig erforderlich wie Darlegungen, durch die sich Beschwerdeführende selbst einer Straftat bezichtigen müssten.

BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 97.

Jedenfalls die Beschwerdeführenden zu 3 bis 5 haben zudem – überobligatorisch – Anhaltspunkte dafür dargelegt, von polizeilichen und/oder strafprozessualen Überwachungsmaßnahmen betroffen zu sein,

Beschwerdeschrift, S. 17 ff.

III. ÜBERMITTLUNGSBEFUGNIS, § 21 ABS. 2 HVSG

Die Verfassungsbeschwerde ist, soweit sie nicht zurückgenommen wurde, zulässig. Dass die Beschwerdeschrift sich nicht näher mit § 21 Abs. 3 und § 23 HVSG auseinandersetzt, mag zwar zur Unzulässigkeit der – nunmehr zurückgenommenen (s.o.) – Rüge eines unzureichenden Kontrollregimes führen,

vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 129.

Die Rüge der Übermittlungsvoraussetzungen bleibt davon jedoch unberührt,

vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 128.

Hinsichtlich dieser Rüge entspricht die Verfassungsbeschwerde inhaltlich dem Vortrag der Verfassungsbeschwerde gegen Art. 25 Abs. 3 Satz 1 Nr. 2 BayVSG, wobei der hiesige Vortrag zu § 21 Abs. 2 HVSG sogar deutlich ausführlicher ist. Sie ist mithin hinreichend begründet.

IV. FEHLENDE BZW. UNZUREICHENDE BENACHRICHTIGUNGSPFLICHTEN

Soweit die Verfassungsbeschwerde rügt, dass hinsichtlich bestimmter Eingriffsbefugnisse (§ 9, § 12 und § 13 HVSG) gar keine Benachrichtigungspflichten vorgesehen sind, genügt sie den Substantiierungsanforderungen.

Nach der ständigen Rechtsprechung des Senats sind Ausnahmen von den Benachrichtigungspflichten auf das unbedingt Erforderliche zu beschränken,

BVerfGE 141, 220 <282 f.>.

Das gilt auch für Nachrichtendienste,

BVerfGE 154, 152 <287>.

Zwar ist richtig, dass die Offenlegung von Überwachungsmaßnahmen im Bereich des Verfassungsschutzes Schwierigkeiten aufwerfen kann. Dies kann auch ein abgestuftes Regelungskonzept erfordern,

vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 135.

Weitgehende Einschränkungen der Benachrichtigungspflicht dürften insbesondere beim Einsatz von Verdeckten Mitarbeitern und Vertrauensleuten gerechtfertigt sein. Auch bei der Ortung von Mobilfunkendgeräten kann im Einzelfall ein überwiegendes Geheimhaltungsinteresse bestehen. Insofern unterscheidet sich die Situation jedoch nicht grundlegend von dem Einsatz dieser Ermittlungsmethoden im polizeilichen Bereich, für den etwa § 74 BKAG eine abgestufte Regelung trifft.

Vgl. BVerfGE 141, 220 <319 f.>.

Im nachrichtendienstlichen Bereich mögen Geheimhaltungsgründe im Einzelfall ein stärkeres Gewicht haben, was sich auch in abweichenden gesetzlichen Vorschriften niederschlagen kann. Ein pauschaler Ausschluss der Benachrichtigung bei ist jedoch auch im Bereich des Verfassungsschutzes offensichtlich nicht auf das „unbedingt Erforderliche“ beschränkt, sodass es einer vertieften Auseinandersetzung mit entgegenstehenden Belangen in der Verfassungsbeschwerde nicht bedurfte.

Hinsichtlich der unzureichenden Benachrichtigungspflichten in den nunmehr noch angegriffenen Vorschriften der § 8 Abs. 4, § 10 Abs. 6 und § 11 Abs. 9 HVSG ist die Verfassungsbeschwerde zulässig und scheitert nicht am Grundsatz der Subsidiarität. Der Senat hat eine im Ansatz ähnlich gelagerte Rüge gegen die Beschränkungen der Benachrichtigungspflicht im Bayerischen Verfassungsschutzgesetz für unzulässig gehalten. Zur Begründung hat der Senat ausgeführt, nach dem Subsidiaritätsgrundsatz hätten die dortigen Beschwerdeführer

„zunächst versuchen müssen, die Reichweite der Benachrichtigungspflichten und ihrer Beschränkungen im fachgerichtlichen Verfahren zu klären“,

BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 136.

Diese Ausführungen sollten nicht auf das vorliegende Verfahren übertragen werden, denn sie überspannen den Subsidiaritätsgrundsatz.

Ein fachgerichtliches Rechtsschutzverfahren, das die gesetzliche Beschränkung einer grundsätzlichen Pflicht zur Benachrichtigung der betroffenen Person über eine verdeckte Datenerhebungsmaßnahme zum Gegenstand hat, kann zwangsläufig nur von einer Person eingeleitet werden, die 1. von einer solchen Maßnahme betroffen wurde und 2. über diese Maßnahme nicht benachrichtigt wurde. Hat keine Datenerhebung stattgefunden, so wurde die grundsätzliche Benachrichtigungspflicht von vornherein nicht ausgelöst, sodass deren gesetzliche Beschränkung nicht streitentscheidend ist. Hat die Datenerhebung stattgefunden und ist eine Benachrichtigung erfolgt, so ist die von der Datenerhebung betroffene Person hinsichtlich der Benachrichtigungspflicht nicht beschwert. Sie kann sich gegen die Datenerhebungsmaßnahme wenden, nicht aber gegen die

Benachrichtigung. Eine fachgerichtliche Klärung der Rechtsfrage, wie weit die gesetzliche Benachrichtigungspflicht reichen müsste und welche Beschränkungen verfassungsrechtlich noch hinnehmbar sind, lässt sich im Rahmen des am Schutz subjektiver Rechte im Einzelfall orientierten deutschen Verwaltungsprozessrechts nicht erlangen. Insbesondere setzt eine verwaltungsgerichtliche Feststellungsklage, die in vielen Fallkonstellationen einen weitreichenden mittelbaren Rechtsschutz gegen verfassungswidrige gesetzliche Regelungen eröffnen mag,

> vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 101,

ein feststellungsfähiges konkretes Rechtsverhältnis voraus. Gefordert wird,

> *„dass das Feststellungsbegehren auf einen hinreichend bestimmten, bereits überschaubaren, d.h. nicht nur gedachten und als möglich vorgestellten Sachverhalt bezogen ist“,*
>
> Möstl, in: BeckOK VwGO, § 43 Rn. 5, m.w.N.

Ein solcher hinreichend bestimmter Sachverhalt fehlte, wenn eine Feststellungsklage sich allgemein auf die Reichweite der Benachrichtigungspflicht bezöge, ohne von einer konkreten Datenerhebungsmaßnahme auszugehen. Eine solche Feststellungsklage hätte nicht ein konkretes Rechtsverhältnis, sondern eine gerade nicht feststellungsfähige abstrakte Rechtsfrage zum Gegenstand,

> vgl. zur Unzulässigkeit derartiger Feststellungsklagen beispielhaft für die gefestigte ständige Rechtsprechung BVerwG, Urteil vom 23. August 2007 – 7 C 13.06 –, Rn. 31; BVerwG, Urteil vom 28. Januar 2010 – 8 C 38.09 –, Rn. 32; BVerwG, Urteil vom 28. Mai 2014 – 6 A 1.13 –, Rn. 20 f.; BVerwG, Urteil vom 12. September 2019 – 3 C 3.18 –, Rn. 23.

Wer hingegen von einer verdeckten Datenerhebungsmaßnahme betroffen war, aber nicht benachrichtigt wurde, weiß nichts von der Maßnahme. Eine solche Person hat keinen Anlass, gegen eine unterbliebene Benachrichtigung gerichtlich vorzugehen, ebenso wie sie keinen Anlass hat, gegen die Maßnahme selbst vorzugehen. Von ihr unter Subsidiaritätsgesichtspunkten ein derartiges Vorgehen zu erwarten, liefe darauf hinaus, der Person einen anlasslosen Rechtsschutz anzusinnen. Sie müsste „ins Blaue hinein“ vorbringen, dass sie möglicherweise durch eine verdeckte Datenerhebungsmaßnahme betroffen worden sei, von der sie in verfassungswidriger Weise nicht benachrichtigt worden sei. Ob ein solcher Rechtsbehelf, der die beanstandete hoheitliche Maßnahme nicht näher eingrenzen könnte, überhaupt zulässig wäre, erscheint sehr zweifelhaft. Nahe läge die Bewertung, dass es an einem hinreichend konkreten Streitgegenstand fehlte und die Klage stattdessen auf die gerade nicht statthafte Klärung einer abstrakten Rechtsfrage abzielte. Denkbar wäre auch, dem Klageantrag als „Ausforschungsantrag“ das Rechtsschutzbedürfnis zu versagen. Jedenfalls

wäre eine solche Klage für den Kläger oder die Klägerin mit einem extremen, für ihn oder sie kaum einschätzbaren Prozessrisiko verbunden, da sie nur Erfolg haben könnte, wenn es wirklich zu einer Datenerhebung gekommen sein sollte. Ansonsten wäre die Klage unbegründet, ohne dass es auf die Verfassungskonformität der gesetzlichen Benachrichtigungsregelung und ihrer Beschränkungen ankäme.

Die möglicherweise von einer verdeckten Datenerhebungsmaßnahme des Verfassungsschutzes betroffene Person hätte in der Regel auch keine realistische Möglichkeit, durch einen Auskunftsantrag nach § 26 Abs. 1 Satz 1 HVSG von der Datenerhebungsmaßnahme zu erfahren und dann gegebenenfalls gegen ihre unterbliebene Benachrichtigung vorzugehen. Grund hierfür sind die Einschränkungen des gesetzlichen Auskunftsanspruchs in § 26 Abs. 2 HVSG, die weitgehend gleichlautend sind mit den Beschränkungen der Benachrichtigungspflicht in §§ 8 Abs. 4 Satz 2, 11Abs. 9 Satz 2, 11 Abs. 9 Satz 2 HVSG, sowie in § 12 Abs. 1 Satz 2 G 10 iVm § 10 Abs. 6 Satz 1 HVSG,

> vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 107.

Der Rechtsschutz gegen eine unterbliebene Benachrichtigung wäre insgesamt sogar mit noch höheren prozessualen Hürden verbunden als ein Rechtsschutz gegen eine möglicherweise drohende verdeckte Datenerhebungsmaßnahme, den der Senat den Beschwerdeführenden mit guten Gründen grundsätzlich gerade nicht zumutet,

> vgl. zuletzt BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 106 ff., wo der Subsidiaritätsgrundsatz nicht einmal erwähnt wird.

Personen, die befürchten, durch eine Sicherheitsbehörde zukünftig einmal überwacht zu werden, können gegen die drohende Überwachung immerhin möglicherweise mit einer verwaltungsgerichtlichen (vorbeugenden) Unterlassungsklage vorgehen,

> vgl. für die Zulässigkeit einer solchen Klage – wenngleich es sich möglicherweise wegen des ständigen Betriebs und der großen Streubreite der in Rede stehenden Überwachungseinrichtung eher um einen Sonderfall oder auch um eine „Ausreißerentscheidung“ handelte – BVerwG, Urteil vom 22. Oktober 2014 – 6 C 7.13 –, Rn. 15 ff.

Eine solche Klagemöglichkeit scheidet mit Blick auf das drohende Unterlassen einer Benachrichtigung aus. Bei der Benachrichtigung handelt es sich um eine behördliche positive Leistung, die durch eine vorangehende Eingriffsmaßnahme bedingt ist. Eine vorbeugende Klage auf eine möglicherweise zukünftig geschuldete, rechtlich bedingte Leistung ist dem Verwaltungsprozessrecht unbekannt.

Der Unterzeichner möchte daher respektvoll an den Senat appellieren, zu seiner bisherigen Rechtsprechung zurückzukehren, nach der zusammen mit einer Ermächtigung zu verdeckten Datenerhebungsmaßnahmen auch die Regelung über die Benachrichtigung der betroffenen Person und ihre Einschränkungen zulässigerweise unmittelbar mit einer Rechtssatzverfassungsbeschwerde angegriffen werden können,

> vgl. BVerfGE 100, 313 (354 ff., 397 ff.); 109, 279 (305 ff., 363 ff.); 125, 260 (304 ff., 353 f.); 141, 220 (260 ff., 319 f.); 155, 119 (159 ff.; 226 f.), jeweils ohne Thematisierung des Subsidiaritätsgrundsatzes im Zusammenhang mit den Beschränkungen der Benachrichtigungspflicht.

Der im Urteil zum Bayerischen Verfassungsschutzgesetz aufgezeigte Weg über einen fachgerichtlichen Rechtsschutz ist praktisch aussichtslos, zumindest aber für die betroffenen Personen mit einem außerordentlichen Prozessrisiko verbunden, dem kein auch nur annähernd gleichgewichtiger Ertrag in Form eines wirksamen Grundrechtsschutzes oder einer Aufbereitung der fachrechtlichen Rechtslage gegenübersteht. Es handelte sich um eine unzumutbare und sinnlose Anrufung der Fachgerichte, die der Subsidiaritätsgrundsatz nicht gebietet.

V. UNZUREICHENDER AUSKUNFTSANSPRUCH, § 26 ABS. 1 HVSG

Soweit sich die Verfassungsbeschwerde gegen die Beschränkung des Auskunftsanspruchs durch das Erfordernis eines besonderen Auskunftsinteresses in § 26 Abs. 1 Satz 1 HVSG richtet, genügt sie dem Grundsatz der Subsidiarität.

Der Senat hat diesbezüglich jedoch ebenfalls eine im Ansatz ähnlich gelagerte Rüge gegen die Beschränkungen des Auskunftsanspruchs im Bayerischen Verfassungsschutzgesetz für unzulässig gehalten. Zur Begründung hat der Senat ausgeführt, dass die Möglichkeit bestanden hätte,

> *„einen Antrag auf Auskunft […] zu stellen und im Falle einer Ablehnung des Antrags in einem gerichtlichen Verfahren klären zu lassen, was einfachrechtlich unter einem besonderen Interesse an der Auskunft im Sinne des Art. 23 Abs. 1 Satz 1 BayVSG zu verstehen ist“,*
>
> BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 137.

Ähnlich wie bei den Benachrichtigungspflichten stellt diese Subsidiaritätsanforderung eine Neuerung in der Rechtsprechung des Senats dar. Bisher prüfte der Senat, ob die Auskunftsrechte den Anforderungen an Transparenz und Rechtsschutz genügen, ohne dass er im Rahmen der Zulässigkeit auf den Subsidiaritätsgrundsatz eingegangen ist,

vgl. BVerfGE 133, 277 <367 f.>; 141, 220 <319 f.>; 154, 152 <287; 308 f.>.

Dogmatisch ist ein solches Vorgehen auch vorzugswürdig. Nach der ständigen Rechtsprechung des Senats entstammen Auskunftsansprüche (und Benachrichtigungspflichten) der verhältnismäßigen Ausgestaltung von heimlichen Überwachungsmaßnahmen, da

> *„der Verhältnismäßigkeitsgrundsatz […] auch Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle [stellt]. […] Zur Flankierung von informationsbezogenen Eingriffen, deren Vornahme oder Umfang die Betroffenen nicht sicher abschätzen können, hat der Gesetzgeber überdies Auskunftsrechte vorzusehen.“*
>
> BVerfGE 141, 220 <282 f.>.

Die Prüfung einer ausreichenden Flankierung von Überwachungsmaßnahmen erfolgt damit im Rahmen der Prüfung der Verhältnismäßigkeit im engeren Sinne der angegriffenen Rechtsgrundlage.

> BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 132.

Im Rahmen dieser Verhältnismäßigkeitsprüfung ist daher der Gesamtkomplex der Regelung in den Blick zu nehmen. Folglich sind zwingend auch die ausgestaltenden Rechte und Pflichten zu prüfen. Dass die Beschwerdeführenden die unzureichende Norm des § 26 Abs. 1 HVSG ausdrücklich auch als Beschwerdegegenstand angegriffen haben, kann ihnen nicht zum Nachteil gereichen.

Darüber hinaus ist das Beschreiten des fachgerichtlichen Rechtswegs in Bezug auf die Rüge unzureichender Auskunftspflichten weder zielführend noch zumutbar. Zwar ist bei einer abgelehnten Auskunft die Verpflichtungsklage statthaft. Eine Klärung der Interpretation des Merkmals des besonderen Interesses ist jedoch ausgeschlossen, wenn die Auskunft erteilt wird, was insbesondere dann geschieht, wenn zum Zeitpunkt der Antragstellung keine oder nur vergleichsweise unverfängliche Daten gespeichert sind. So kommt es inzwischen regelmäßig vor, dass Nachrichtendienste auch bei nicht dargelegtem besonderen Interesse nach Ermessen Auskunft erteilen (vgl. § 26 Abs. 1 Satz 2 HVSG). Damit ist aber nicht sichergestellt, dass auch in Zukunft Auskunft erteilt wird. Dies wäre jedoch erforderlich, um die Datenerhebungsbefugnisse als verhältnismäßig im engeren Sinne ansehen zu können.

Schließlich wirft das Kriterium des besonderen Interesses in § 26 Abs. 1 Satz 1 HVSG allein spezifisch verfassungsrechtliche Fragen auf, die das Bundesverfassungsgericht zu beantworten hat, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung verbesserte Entscheidungsgrundlagen zu erwarten wären. Die Verfassungsbeschwerde macht geltend, dass sich ein grundrechtlich anerkanntes Auskunftsinteresse bereits daraus ergibt, dass der

Auskunftbegehrende möglicherweise Betroffener von Eingriffen in sein Recht auf informationelle Selbstbestimmung ist.

> Beschwerdeschrift, S. 55.

Dieses Auskunftsinteresse kann jedoch nicht identisch sein mit dem „besonderen Auskunftsinteresse“, da dieses Merkmal ansonsten jegliche Funktion verlieren würde.

Soweit die Verfassungsbeschwerde rügt, dass der Auskunftsanspruch sich von vornherein nicht auf die Herkunft personenbezogener Daten und die Empfänger von Übermittlungen erstreckt,

> Beschwerdeschrift, S. 55,

genügt sie den Substantiierungsanforderungen. Zwar gibt es tatsächlich naheliegende Gründen für eine Ausschlussregelung,

> vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 138.

Auf diese ist die Verfassungsbeschwerde auch eingegangen. Einer vertieften Auseinandersetzung bedurfte es jedoch nicht, da die im Einzelfall entgegenstehende Ausforschungsgefahr und andere Geheimhaltungsgründe jedenfalls keinen pauschalen Ausschluss rechtfertigen können.

Dasselbe gilt für Daten, die nicht strukturiert in automatisierten Dateien gespeichert sind. Einer vertieften Auseinandersetzung mit den Erwägungen des Gesetzgebers,

> vgl. LT-Drs. 19/5412, S. 52 f.,

bedurfte es nicht. Denn eine automatisierte Suche ist jedenfalls nicht in jedem Fall unmöglich bzw. unzulässig, sodass ein pauschaler Ausschluss offensichtlich nicht gerechtfertigt ist. Auch der Subsidiaritätsgrundsatz steht aus den oben genannten Gründen der Zulässigkeit nicht entgegen.

VI. AUTOMATISIERTE DATENANALYSE, § 25A HSOG

Die Verfassungsbeschwerde erfüllt die Anforderungen des Subsidiaritätsgrundsatzes. Es ist den Betroffenen nicht möglich oder zumindest nicht zumutbar, gegen den Vollzug der angegriffenen Norm vorzugehen und sich so einen indirekten Rechtsschutz gegen die Regelung zu verschaffen. Maßgeblich ist, dass die Beschwerdeführenden von der verdeckt durchgeführten automatisierten Zusammenführung und Analyse ihrer personenbezogenen Daten keine Kenntnis erlangen.

Vgl. Beschwerdeschrift, S. 31.

§ 29 Abs. 1 HSOG verweist zwar auch auf § 51 HDSIG, der die Benachrichtigung betroffener Personen regelt. Diese Norm setzt jedoch voraus, dass die Benachrichtigung „in speziellen Rechtsvorschriften, insbesondere bei verdeckten Maßnahmen, vorgesehen oder angeordnet“ ist. Dies ist in § 29 Abs. 5 HSOG nur für Maßnahmen nach § 28 Abs. 2 HSOG der Fall, wozu nicht die automatisierte Datenanalyse nach § 25a HSOG gehört.

Vgl. Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, S. 17.

Den Beschwerdeführenden ist es auch nicht möglich und zumutbar, sich durch wiederholte Auskunftsanträge Kenntnis von der Maßnahme zu verschaffen. Dabei kann dahinstehen, ob überhaupt eine Auskunft über die Maßnahme erteilt werden muss (dazu unten C.VI.). Denn der Auskunftsanspruch unterliegt jedenfalls gemäß § 29 Abs. 1 HSOG i. V. m. § 52 Abs. 4 HDSIG i. V. m. § 51 Abs. 2 HDSIG weitgehenden Einschränkungen. Würde eine Auskunft erteilt, hätte sie wegen dieser Einschränkungen nur begrenzte Aussagekraft und könnte nicht zuverlässig belegen, ob die Beschwerdeführenden von einer Maßnahme nach § 25a HSOG betroffen sind oder nicht.

Vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 - , Rn. 107.

Im Übrigen besteht auch keine vorbeugender Rechtschutzmöglichkeit. Insoweit wird auf die Ausführungen zu den unzureichenden Benachrichtigungspflichten im Hessischen Verfassungsschutzgesetz verwiesen (oben IV.), die entsprechend gelten. Auch bei der automatisierten Datenanalyse wäre für die Erhebung einer vorbeugenden Unterlassungs- oder Feststellungsklage die Bezeichnung eines konkreten Rechtsverhältnisses notwendig. Eine konkrete Bestimmung der von der Polizei durchgeführten Datenanalyse ist den Beschwerdeführenden jedoch nicht möglich.

Vgl. Beschwerdeschrift S. 38 ff.

Auch hinsichtlich der Rüge fehlender Benachrichtigung selbst ist der Subsidiaritätsgrundsatz gewahrt. Insofern wird ebenfalls auf die Ausführungen zu den unzureichenden Benachrichtigungspflichten im Hessischen Verfassungsschutzgesetz (oben IV.) verwiesen. Die Verfassungsbeschwerde ist insoweit auch hinreichend substantiiert. Im Unterschied zum Hessischen Verfassungsschutzgesetz und zum Bayerischen Verfassungsschutzgesetz handelt es sich bei der automatisierten Datenerhebung nach § 25a HSOG um eine polizeiliche Maßnahme. Sofern der Senat dem Umstand, dass „die Offenlegung von Überwachungsmaßnahmen im Bereich des Verfassungsschutzes Schwierigkeiten aufwerfen kann“,

vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 107; dazu oben unter IV.,

entscheidende Bedeutung beimisst, gilt dies jedenfalls nicht für die Benachrichtigung über Maßnahmen nach § 25a HSOG.

Hinsichtlich der Rüge eines unzureichenden Auskunftsanspruchs wird auf die diesbezüglichen Ausführungen zur Auskunft nach § 26 Abs. 1 HVSG (oben V.) verwiesen. Auch hinsichtlich der Auskunft über die automatisierte Datenanalyse ist das Beschreiten des fachgerichtlichen Rechtswegs weder zielführend noch zumutbar.

C. BEGRÜNDETHEIT

I. BESONDERE AUSKUNFTSERSUCHEN, § 10 ABS. 2 SATZ 1 NR. 1 HVSG

Die Verfassungsbeschwerde gegen die Norm ist weiterhin begründet. Auch die geplanten Änderungen durch das Gesetz zur Änderung sicherheitsrechtlicher Vorschriften und zur Umorganisation der hessischen Bereitschaftspolizei,

LT-Drs. 20/8129, S. 3 f.,

ändern hieran nichts. Zwar ist es im Hinblick auf die Normenklarheit positiv zu bewerten, dass vor dem Wort „einholen“ das Wort „Auskünfte“ eingefügt werden soll und das Gesetz anschließend einen grammatikalisch vollständigen deutschen Satz enthält. Auch die Klarstellung bezüglich des Geltungsbereiches in § 10 Abs. 10 HVSG-E ist zu begrüßen. Jedoch sollen ansonsten keine substanziellen Änderungen erfolgen, die Maßnahmen greifen weiterhin erheblich in das Recht auf informationelle Selbstbestimmung ein und sind auch mit den Maßstäben, die im Urteil zum Bayerisches Verfassungsschutzgesetz aufgestellt wurden, nicht vereinbar.

Anders als die Staatskanzlei meint, erlaubt die Rechtsgrundlage die Erhebung von qualitativ hochwertigen Informationen, die eine umfangreiche Erfassung der Persönlichkeit ermöglichen. Sie ist mit einer Ortung des Mobiltelefons vergleichbar. Daher kann die Maßnahme

> *„nur zugelassen werden, wenn dies zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten ist. Dabei kommt es auf die konkrete Relevanz der hierdurch zu gewinnenden Erkenntnisse für die weitere Aufklärung verfassungsfeindlicher Bestrebungen an. Da die Maßnahme regelmäßig gezielt gegen bestimmte Personen gerichtet sein dürfte, muss die Überwachung gerade dieser Personen zur Aufklärung beitragen. Darüber hinaus muss die Nutzung der Befugnis wegen des potenziell hohen Eingriffsgewichts von einem gesteigerten Beobachtungsbedarf abhängig gemacht werden“*

BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 107

Eine gesteigerte Beobachtungsbedürftigkeit kann sich etwa daraus ergeben, dass die Bestrebung darauf gerichtet ist, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten oder dass sie volksverhetzend tätig wird,

vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 194 ff. auch zu weiteren Anhaltspunkten.

§ 10 Abs. 2 Satz 1 Nr. 1 HVSG setzt demgegenüber lediglich tatsächliche Anhaltspunkte für Bestrebungen und Tätigkeiten nach § 2 Abs. 2 HVSG voraus und erfüllt damit nicht die Eingriffsschwelle einer gesteigerten Beobachtungsbedürftigkeit.

Die Argumentation der Staatskanzlei, dass Abfragen bei Verkehrsdienstleistern im Vergleich zur Ortung von Mobilfunkanbietern einen erheblich geringfügigeren Eingriff darstellen,

Stellungnahme Hessische Staatskanzlei, S. 42,

überzeugt nicht.

Zunächst ist der Behauptung zu widersprechen, die Auskunftsersuchen seien nicht durch Auskunftsverpflichtungen der Befragten abgesichert. Die Auskunftsverpflichtung ergibt sich vielmehr aus dem Regelungszusammenhang (siehe bereits oben unter B. I.).

Unzutreffend ist auch die Behauptung der Staatskanzlei, dass die Verfassungsmäßigkeit des § 10 Abs. 2 Satz 1 Nr. 2 HVSG außer Streit stehe. Diese Norm ist lediglich nicht Gegenstand der Verfassungsbeschwerde. Auf die Verfassungsmäßigkeit kommt auch im vorliegenden Zusammenhang nicht an. Entscheidend ist, dass die Maßnahme eine Zuordnung von Daten ermöglicht, die nach § 10 Abs. 2 Satz 1 Nr. 1 HVSG erhoben werden, und damit die Intensität dieses Eingriffs steigert.

Das Argument, eine Überwachung mittels Auskunftsersuchen würde „am Hauptbahnhof enden“, ist heutzutage nicht mehr richtig. Es mag vor 20 Jahren der Fall gewesen sein, dass für die Weiterreise von zentralen Mobilitätsknoten nur anonyme Reisemittel zur Verfügung standen, sei es der öffentliche Nahverkehr, Taxi oder auch die Fortbewegung zu Fuß. Heutzutage bestehen hingegen zahlreiche Mobilitätsangebote über digitale Plattformen, die ein anonymes Reisen immer unwahrscheinlicher machen. Zu nennen sind hier Leihräder oder -roller, Carsharing, digitale Mitfahrzentralen, Uber, Taxi-Apps, etc. Auch im öffentlichen Nahverkehr ist eine Nachverfolgung der Reiseroute inzwischen möglich, wenn eine digitale Stempelkarte benutzt wird. All diese digitalen Mobilitätsdienstleister können unproblematisch unter „Verkehrsunternehmen“ subsumiert werden. Dafür

spricht auch die Gesetzesbegründung, nach dem der Begriff der Verkehrsunternehmen „ausdrücklich weit gefasst“ ist und „den volatilen Bedingungen eines globalisierten Fernreisemarkts“ Rechnung tragen soll. Fernbus- und Eisenbahntransportunternehmen werden lediglich als Beispiele genannt,

> LT-Drs. 19/5412, S. 39.

Es ist naheliegend, jedenfalls nicht auszuschließen, dass diese Dienste auch Daten über den genauen Routenverlauf der vergangenen Nutzungen speichern, da diese Daten auch als Grundlage der Abrechnung dienen. Nach der derzeitigen Ausgestaltung der Norm erlaubt sie dem Verfassungsschutz auch den Abruf dieser Daten, denn abgefragt werden können auch Daten zur „Inanspruchnahme und Umständen von Transportleistungen“. Der Begriff der „Umstände“ ist denkbar weit und lässt keine Einschränkungen erkennen. Unproblematisch kann hierunter auch eine konkrete Reiseroute subsumiert werden,

> vgl. auch Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 24.06.2022, S. 35.

In ihrer Stellungnahme argumentiert die Staatskanzlei, dass eine solche Überwachung vermieden werden kann und weiterhin anonymes Reisen möglich ist. Das ist insoweit richtig, als Mobilität durch das eigene Fahrrad oder die Fortbewegung zu Fuß weiterhin anonym möglich ist. Auch ist es richtig, dass Fahrkarten überwiegend immer noch am Schalter oder am Automaten gekauft werden können. Jedoch trägt das Argument nicht weit, denn de facto wird heutzutage ein großer Teil der Mobilität digital abgewickelt. So werden derzeit 70 % der 140 Millionen verkauften Fernverkehrstickets der Bahn digital verkauft. Zudem ist eine weitere Reduzierung des Automatenbestandes geplant,

> vgl. https://www.tagesspiegel.de/wirtschaft/konzern-setzt-ganz-auf-digitale-fahrkarten-bahn-will-fernticket-verkauf-an-automaten-weiter-reduzieren/23795940.html, zuletzt aufgerufen am 17.08.2022.

Moderne digitalisierte Mobilitätsformen sind nichts Besonderes mehr, sondern werden allgemein genutzt und stellen den neuen „Normalfall“ der Fortbewegung dar. Es ist gerade dieser Umstand, der eine Eingriffsbefugnis wie in § 10 Abs. 2 Satz 1 Nr. 1 HVSG für den Verfassungsschutz interessant macht. Würden Personen heute noch wie vor 20 Jahren reisen, gäbe es kaum einen Anwendungsfall für diese Norm.

Das Argument der Vermeidbarkeit bzw. Umgehbarkeit der Überwachungsmaßnahmen überzeugt auch deswegen nicht, da viele Überwachungsmaßnahmen durch eine entsprechend vorsichtige Lebensgestaltung vermeidbar sind. So können Bürger*innen eine Mobilfunkortung vermeiden, indem sie kein Mobiltelefon nutzen oder dieses stets ausschalten. Die Überwachung des Briefverkehrs oder der Telekommunikation können sie vermeiden, indem sie keine Briefe schreiben oder nicht telefonieren. Die Möglichkeit eines Kontaktes mit

Vertrauensleuten oder verdeckten Mitarbeiter*innen können sie erheblich reduzieren, indem sie keinen sozialen Umgang pflegen. Dennoch stellen all diese Maßnahmen unstreitig erhebliche Eingriffe in die Freiheitssphäre von Bürger*innen dar. Die Frage der Vermeidbarkeit ist daher nicht entscheidend, vielmehr dienen Grundrechte gerade dem Schutz dieser Freiheitsbetätigungen. Der staatliche Eingriff muss sich an den Freiheitssphären messen lassen, nicht die Freiheitssphäre am Eingriff. Insbesondere ist es nicht haltbar, dass die Eingriffsintensität davon abhängt, ob Bürger*innen auf bestimmte Sphären des Schutzbereiches ihrer Grundrechte verzichten können oder nicht.

Die Staatskanzlei erwehrt sich in ihrer Stellungnahme eines Vergleichs des besonderen Auskunftsersuchens mit der Mobilfunkortung mit dem Argument, dass eine Abfrage nach § 10 Abs. 2 S. 1 Nr. 1 HVSG nur ein fragmentarisches Bild liefern könne, während die Mobilfunkortung eine genaue Ortung zulasse,

> Stellungnahme Hessische Staatskanzlei, S. 41 f.

Dieses Argument ist aus mehreren Gründen nicht richtig. Zum einen erlaubt auch eine Mobilfunkortung durch eine „stille SMS“ stets immer nur die Zuordnung zu einer bestimmten Funkzelle. Die Exaktheit der Ortung hängt damit von der Größe der einzelnen Funkzellen ab. Zum anderen gilt das Argument der Staatskanzlei gerade nicht für neuere digitale Verkehrsdienstleister, da diese den Verlauf der Bewegung präzise erfassen und somit auch ein lückenloses Bewegungsprofil erstellt werden kann (s.o.).

Die Staatskanzlei erwidert in ihrer Stellungnahme, dass eine Abfrage von sämtlichen Verkehrsunternehmen zudem nicht zu befürchten sei, da dies aus praktischen Gründen ausscheide,

> Stellungnahme Hessische Staatskanzlei, S. 41.

Jedoch stellte der Senat in seiner Entscheidung zum Bayerisches Verfassungsschutzgesetz bereits klar, dass sich die Schwere des Grundrechtseingriffs nach den tatsächlichen und rechtlichen Nutzungsmöglichkeiten richtet,

> vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 320.

Zwar mag eine solche breite Abfrage nicht der derzeitigen Praxis des Verfassungsschutzes entsprechen, jedoch ist sie ohne Weiteres gesetzlich möglich. Insbesondere ist hierbei an (teil-)automatisierte Verfahren zu denken, die den Verwaltungsaufwand erheblich reduzieren würden.

II. UNZUREICHENDE BESCHRÄNKUNG DER DATENVERARBEITUNG AUS WOHNRAUMÜBERWACHUNG UND ZUGRIFFEN AUF INFORMATIONSTECHNISCHE SYSTEME, §§ 16, 18 ABS. 3 HVSG

Die Beschwerdeführenden gehen weiterhin von der Verfassungswidrigkeit der angegriffenen Normen aus. Auch das Urteil zum Bayerisches Verfassungsschutzgesetz ändert nach Ansicht der Beschwerdeführenden hieran nichts, da in dem Urteil die materiellen Anforderungen an einen Datenaustausch zwischen Behörden jedenfalls nicht abgesenkt wurden. Es dürfte im Gegenteil zweifelhaft sein, ob nach dem Urteil überhaupt noch Daten aus Online-Durchsuchung und Wohnraumüberwachung an Nachrichtendienste übermittelt bzw. von diesen abgerufen und genutzt werden dürfen. Der Senat hat klargestellt, dass sowohl Maßnahmen der Online-Durchsuchung als auch der Wohnraumüberwachung nur bei Vorliegen einer konkretisierten bzw. dringenden Gefahr zulässig sind und im Verhältnis zu polizeilichen Befugnissen subsidiär ausgestaltet sein müssen.

> BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 168 f. und Rn. 175 ff.

Daraus ergibt sich, dass eine Übermittlung solcher Daten durch Gefahrenabwehrbehörden an andere Behörden, die nicht der Gefahrenabwehr oder Strafverfolgung dienen, unzulässig ist. Zu letzteren gehören grundsätzlich auch die Nachrichtendienste, denn diesen kommt nur eine subsidiäre Gefahrenabwehrfunktion zu. Diese subsidiäre Zuständigkeit ist aber denknotwendig immer dann ausgeschlossen, wenn die Daten schon durch die originär zuständigen Gefahrenabwehrbehörden erhoben wurden.

Das Hessische Ministerium des Innern und für Sport argumentiert, es sei ausreichend, dass nur bei der Übermittlung eine entsprechende Nutzungsschwelle beachtet werde. Zwar bedürfe es nach dem Doppeltürmodell sowohl auf Seiten der abrufenden, als auch der übermittelnden Behörde einer Rechtsgrundlage, jedoch müssten nicht auf beiden Seiten der „Doppeltür“ dieselben hohen Anforderungen an die Zweckänderung erfüllt sein, vielmehr genüge dies auf Seiten der übermittelnden Behörde,

> vgl. Stellungnahme Hessische Staatskanzlei, S. 54.

Die maßgebliche Zweckänderung sei in der Übermittlung selbst zu sehen, so dass auch nur für diese eine entsprechende Übermittlungsschwelle erforderlich sei. Werden solche übermittelten Daten dann durch die empfangende Behörde weiterverwendet, so stelle dies keine (weitere) Zweckänderung dar,

> vgl. Stellungnahme Hessische Staatskanzlei, S. 53.

Die Rechtsansicht des Hessischen Ministeriums des Innern und für Sport ist nicht haltbar und mit den vom Senat aufgestellten Prinzipien zur

Datenübermittlung und Zweckänderung nicht vereinbar. Das Ministerium meint aus dem Umstand, dass der Senat in seinem Urteil zum Bayerisches Verfassungsschutzgesetz umfangreiche Übermittlungsvoraussetzungen für den Verfassungsschutz statuiert hat, schließen zu können, dass der Senat

> *„die zu erfüllende Eingriffsschwelle also offenbar aufseiten der übermittelnden Behörde [verortet], nicht aufseiten der die übermittelnden Informationen nutzenden Behörde.“*
>
> Stellungnahme Hessische Staatskanzlei, S. 50.

Dies stellt einen logisch unzulässigen Umkehrschluss dar. Nur weil es (auch) umfangreicher Übermittlungsvoraussetzungen bedarf, ist die Nutzung der übermittelten Daten im Anschluss nicht voraussetzungsfrei zulässig. In der hierzu zitierten Passage des Urteils zum Bayerisches Verfassungsschutzgesetz äußert sich der Senat überhaupt nicht zu den Voraussetzungen einer weiteren Nutzung nach erfolgter Übermittlung,

> vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 170 ff.

Das Hessische Ministerium des Innern und für Sport verkennt, dass es in dem zitierten Urteil um eine völlig andere Konstellation geht, da dort Daten von einem Nachrichtendienst an eine operativ tätige Behörde übermittelt werden sollen. Daher ist für diesen Fall das informationelle Trennungsprinzip besonders zu beachten. Im Falle der angegriffenen Normen des §§ 16 und 18 Abs. 3 HVSG geht es hingegen um die umgekehrte Konstellation: Es sollen Daten, die von einer operativen Behörde erhoben wurden, an einen Nachrichtendienst übermittelt werden. Das informationelle Trennungsprinzip ist hierfür weniger relevant, da eine Umgehung der niedrigeren nachrichtendienstlichen Erhebungsschwellen nicht droht, vielmehr geht es um allgemeine Grundsätze der Zweckbindung und Zweckänderung von Daten. Hierzu hat der Senat in seinem Urteil zum Bayerischen Verfassungsschutzgesetz festgehalten:

> *„Weiter reicht die Zweckbindung allerdings für Daten aus Wohnraumüberwachungen und Online-Durchsuchungen. Hier ist jede weitere Nutzung der Daten in einem neuen Verfahren nur dann zweckentsprechend, wenn sie auch aufgrund einer den Erhebungsvoraussetzungen entsprechend dringenden beziehungsweise zumindest konkretisierten Gefahr erforderlich ist. Das außerordentliche Eingriffsgewicht solcher Datenerhebungen spiegelt sich hier auch in einer besonders engen Bindung jeder weiteren Nutzung der gewonnenen Daten an die Voraussetzungen und Zwecke der Datenerhebung. Eine Nutzung der Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz unabhängig von einer dringenden oder zumindest konkretisierten Gefahr kommt hier nicht in Betracht“*

BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 228.

Zum verfassungswidrigen § 20v Abs. 4 Satz 2 Nr. 1 BKAG, der voraussetzungsfrei auch die Verwendung von Daten aus Online-Durchsuchung und Wohnraumüberwachung erlaubte, führte der Senat aus:

„Für Informationen aus diesen besonders intensiven Überwachungsmaßnahmen bedarf jede über das ursprüngliche Ermittlungsverfahren hinausgehende Nutzung jeweils erneut des Vorliegens aller Eingriffsvoraussetzungen, wie es für eine Datenneuerhebung mit diesen Mitteln verfassungsrechtlich geboten wäre.“

BVerfGE 141, 220 <333>.

Den offenen Widerspruch der angegriffenen Normen hierzu versucht das Hessische Ministerium des Innern dadurch zu kaschieren, dass die Übermittlung als einzige Zweckänderung angesehen wird. Dieses Argument kann schon mit der Überlegung entkräftet werden, dass die übermittelten Daten vom Verfassungsschutz mehrfach, für unterschiedliche Zwecke und über einen langen Zeitraum immer wieder verwendet werden können. Selbstverständlich stellt jede dieser Nutzungen eine eigene Zweckänderung dar und muss sich an den hierfür geltenden Anforderungen messen lassen. Es ist abwegig anzunehmen, dass jede Nutzung der übermittelten Daten, auch Jahre nach der Übermittlung, sich noch innerhalb eines Übermittlungs-Nutzungszweckes „Verwendung durch eine andere Behörde“ oder „Verwendung zu anderen Zwecken“ bewege,

vgl. Stellungnahme Hessische Staatskanzlei, S. 53.

Als Beleg für diese Rechtsansicht führt das Ministerium die Rechtsprechung des Senats an, dass jede Übermittlung von Daten an eine andere Behörde eine Zweckänderung darstellt,

vgl. Stellungnahme Hessische Staatskanzlei, S. 55.

Wie bereits zuvor wird aus dieser Aussage ein logisch unzulässiger Umkehrschluss gezogen, nämlich dass die Zweckänderung im Rahmen der Übermittlung die einzige relevante Zweckänderung darstelle und nach Übermittlung keine weiteren erfolgen würden bzw. könnten. Aus dieser Ansicht ergäben sich in der Folge nicht mehr erklärbare Widersprüche. Denn sollte der Verfassungsschutz selbst in zulässiger Weise Daten aus einer Online-Durchsuchung oder Wohnraumüberwachung erhoben haben, so muss er gem. § 8 Abs. 6 HVSG bei jeder Zweckänderung die dort aufgestellten, engen Kriterien beachten. Wurden die Daten jedoch von einer anderen Behörde übermittelt, so dürfte der Verfassungsschutz mit diesen nach Belieben verfahren. Ein Grund für eine solche unterschiedliche Behandlung ist nicht ersichtlich und wird auch vom Ministerium nicht genannt.

III. ÜBERMITTLUNGSBEFUGNIS, § 21 ABS. 2 HVSG

Die Verfassungsbeschwerde ist begründet. Dies steht spätestens fest mit der Entscheidung des Senats zum weitgehend wortlautgleichen Art. 25 Abs. 3 Satz 1 Nr. 2 BayVSG.

> BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 380.

Auch § 21 Abs. 2 HVSG sieht keine ausreichende Übermittlungsschwelle vor. Wie in der Parallelvorschrift aus dem Bayerischen Verfassungsschutzgesetz genügt es, „wenn die Übermittlung zur Wahrung erheblicher Sicherheitsinteressen des Empfängers erforderlich ist.“ Im Unterschied zum Bayerisches Verfassungsschutzgesetz müssen nach § 21 Abs. 2 HVSG für ein solches erhebliches Interesse noch nicht einmal tatsächliche Anhaltspunkte vorliegen. Die Voraussetzungen für eine Übermittlung sind damit noch geringer und die Vorschrift ist daher erst recht nicht mit dem Grundgesetz vereinbar.

IV. FEHLENDE BZW. UNZUREICHENDE BENACHRICHTIGUNGSPFLICHTEN

Hinsichtlich der Begründetheit der Verfassungsbeschwerde wegen unzureichender und fehlender Benachrichtigungspflichten wird an den Ausführungen in der Verfassungsbeschwerde festgehalten. Die Staatskanzlei argumentiert in der Sache verfehlt, wenn sie vorträgt, dass die hohen materiellen Anforderungen des § 7 Abs. 1 HVSG und der Richtervorbehalt gem. § 8 Abs. 1 HVSG es rechtfertigen würden, dass eine Benachrichtigungspflicht gem. § 8 Abs. 4 Satz 2 HVSG eingeschränkt werden kann,

> vgl. Stellungnahme Hessische Staatskanzlei, S. 34.

Die Anforderungen des § 7 Abs. 1 und § 8 Abs. 1 HVSG dienen dem Schutz von Grundrechtsträger*innen vor erheblichen und tiefen Eingriffen des Staates und leiten sich unmittelbar aus dem Grundgesetz ab. Die Benachrichtigungspflichten sollen bei verdeckten Eingriffen des Staates effektiven Rechtsschutz gemäß Art. 19 Abs. 4 GG ermöglichen. Der Senat hat bereits klargestellt, dass zu den Anforderungen an eine verhältnismäßige Ausgestaltung geheimer Eingriffsmaßnahmen eine gesetzliche Anordnung von Benachrichtigungspflichten gehört und Ausnahmen auf das unbedingt Erforderliche zu beschränken sind,

> BVerfGE 141, 220 <281 f.>.

Aus dem Grundgesetz folgt damit ein klares Regel-Ausnahme-Verhältnis, das nicht durch einen Richtervorbehalt außer Kraft gesetzt wird. Zwar stellt ein Richtervorbehalt eine weitere verfahrensrechtliche Anforderung dar, jedoch können und sollen dadurch andere verfahrensrechtliche Sicherung nicht ersetzt werden.

Entsprechendes gilt für die Benachrichtigungspflicht in § 11 Abs. 9 HVSG, wobei hier bereits kein Richtervorbehalt besteht. Das Hessische Ministerium des Innern und für Sport argumentiert, dass das besondere Aufgabenprofil des Verfassungsschutzes eine Ausnahme von der Benachrichtigung rechtfertige, solange eine „Gefährdung des Zweckes der Beschränkung nicht ausgeschlossen werden kann“,

Stellungnahme Hessische Staatskanzlei, S. 45.

Es behauptet, dass die Regelung des § 11 Abs. 9 Satz 2 Alt. 1 HVSG inhaltlich der des § 101 Abs. 5 StPO entspreche, wonach die Benachrichtigung erfolgt, „sobald dies ohne Gefährdung des Untersuchungszweckes möglich […] ist“. Im anschließenden Satz führt es dann aber dem widersprechend aus, dass aufgrund „der Sensibilität der Tätigkeit des Verfassungsschutzes“ eine Regelung erforderlich sei, die eine Benachrichtigung erst vorsehe, wenn eine Beeinträchtigung nicht ausgeschlossen werden kann. Es geht damit erkennbar davon aus, dass ein inhaltlicher Unterschied besteht, ansonsten wäre der Hinweis auf die unterschiedlichen Aufgabenprofile und Anforderungen der Behörden nicht verständlich. Inwiefern die „Sensibilität der Tätigkeit des Verfassungsschutzes“ einen im Vergleich zur Tätigkeit der Staatsanwaltschaft weitgehenderen Benachrichtigungsausschluss erforderlich mache, wird nicht weiter begründet. Dies dürfte auch schwerfallen, denn eine Formulierung wie in § 101 Abs. 5 StPO würde die spezifische Tätigkeit des Verfassungsschutzes schon berücksichtigen, da sie den Untersuchungszweck mit in Bezug nimmt. Anders als in § 11 Abs. 9 Satz 2 HVSG werden hier jedoch die Wahrscheinlichkeitsanforderungen nicht ins Bodenlose abgesenkt, sondern es bleibt an der Behörde im konkreten Fall zu begründen, warum keine Benachrichtigung erfolgen soll.

Ergänzend wird vorgetragen, dass der Senat in seiner Entscheidung zum Bayerisches Verfassungsschutzgesetz – obgleich es die Begründetheit der Verfassungsbeschwerde gegen die Benachrichtigungspflichten nicht geprüft hat – zu Recht erhebliche Zweifel an der Verfassungsgemäßheit von Verweisungen in das G 10-Gesetz hat erkennen lassen,

BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17, Rn. 134.

Das HVSG verwendet in § 10 Abs. 6 Satz 1 HVSG dieselbe Regelungstechnik. Genau wie in den entsprechenden Vorschriften des Art. 11 Abs. 2 Satz 3, 17 Abs. 2 Satz 1 und 19a Abs. 3 Satz 4 BayVSG ist kaum zu erkennen, wo im Hessischen Verfassungsschutzgesetz Mitteilungspflichten bestehen. Wer nicht weiß, dass der in Bezug genommene § 12 Abs. 2 G 10 Benachrichtigungspflichten enthält, findet sie im Hessischen Verfassungsschutzgesetz genauso wenig wie im Bayerisches Verfassungsschutzgesetz,

vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17, Rn. 134.

§ 10 Abs. 6 Satz 1 HVSG verstößt daher auch gegen den Grundsatz der Normenklarheit und ist auch aus diesem Grund verfassungswidrig.

V. UNZUREICHENDER AUSKUNFTSANSPRUCH, § 26 ABS. 1 HVSG

Die Beschwerdeführenden haben zur Kenntnis genommen, dass der hessische Gesetzgeber die Vorschrift in § 26 Abs. 1 Satz 1 HVSG zu ändern gedenkt und Antragstellende in Zukunft voraussichtlich nicht mehr auf „einen konkreten Sachverhalt“ hinweisen müssen.

> LT-Drs. 20/8129, S. 4.

Diese Änderung ist zu begrüßen, da die Anforderungen an das Bestehen eines Auskunftsanspruchs gesenkt werden, jedoch ändert dies nichts an der Verfassungswidrigkeit der Norm. Es wird auf die Ausführungen in der Verfassungsbeschwerde verwiesen, die durch die geplante Änderung nicht tangiert werden.

VI. AUTOMATISIERTE DATENANALYSE, § 25A HSOG

1. VERFASSUNGSRECHTLICHER MASSSTAB

Insofern die Staatskanzlei eine Bezugnahme der Rasterfahndung als Verkennung der Substantiierungsobliegenheiten rügt, ist dem nicht zu folgen,

> vgl. Stellungnahme Hessische Staatskanzlei, S. 85 ff.

Vielmehr obliegt es den Beschwerdeführer*innen bei einer neuartigen Maßnahme gerade, entsprechende Anforderungen aus der bestehenden Rechtsprechung des angerufenen Gerichts herzuleiten. Als Anknüpfungspunkt können dabei notwendigerweise nur Entscheidungen zu Maßnahmen vergleichbaren Eingriffsgewichts sein. Wie in der Beschwerdeschrift ausgeführt (S. 70 ff.) war daher gerade eine Bezugnahme der Entscheidung des Senats zu Rasterfahndung geboten. § 25a HSOG geht in seiner Eingriffsintensität noch über die Rasterfahndung hinaus,

> so auch Stellungnahme des Bundesbeauftragten für den Datenschutz und Informationsfreiheit, S. 20,

sodass die vom Senat aufgestellten Anforderungen zur Rasterfahndung als Mindestmaß anzusehen sind.

Mittlerweile hatte der Senat jedoch die Möglichkeit, sich mit der erweiterten Datennutzung von Dateien in einer Verbunddatei auseinanderzusetzen.

> vgl. BVerfGE 156, 11.

Wie bereits vorgetragen, sind die hierzu entwickelten Maßstäbe auch auf § 25a HSOG zu übertragen. In diesem Zusammenhang wurde auch bereits detailliert dargelegt, dass sich keine wesentliche Einschränkung der Eingriffsintensität aus der lediglich mittelbaren Einbindung nachrichtendienstlicher Informationen ergibt. Auf diese Ausführungen wird verwiesen.

> Stellungnahme vom 10. Mai 2021; vgl. auch Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, S. 3; Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, S. 20.

Nach § 25a Abs. 2 HSOG dient die automatisierte Datenanalyse dazu, „Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen“ herzustellen und die „eingehenden Erkenntnisse zu bekannten Sachverhalten [zuzuordnen] und gespeicherte Daten statistisch auszuwerten“. Damit gleicht die Befugnis derjenigen aus § 6a ATDG, die der Entscheidung des Senats zugrunde lag. Der von der Staatskanzlei vorgebrachte Begriff des „Datamatching“ ist mithin irreführend,

> vgl. Stellungnahme Hessische Staatskanzlei, S. 81.

2. UMFANG DES DATENANALYSE

Darüber hinaus versucht die Staatskanzlei in weiten Teilen ihrer Stellungnahme darzulegen, dass sich die umfangreichen Analysemöglichkeiten zumindest nicht eindeutig aus dem Gesetz ergäben.

> Stellungnahme Hessische Staatskanzlei, S. 84 ff.

Dem ist zunächst zu entgegnen, dass es sich bei § 25a HSOG um eine eingriffsintensive Maßnahme handelt, für die hohe Bestimmtheitsanforderungen bestehen.

> Vgl. zuletzt BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 272 ff.

Im Bereich derartiger Eingriffsbefugnisse darf der Landesgesetzgeber gerade nicht uneindeutige Regelungen schaffen, deren Grenzen erst in langjährigen Verfahren durch Fachgerichte aufgezeigt werden.

> Vgl. auch Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, S. 10.

Darüber hinaus ist den Stellungnahmen der Datenschutzbeauftragten zuzustimmen, dass die Tragweite der Vorschrift durchaus klar ist.

Vgl. Stellungnahme des Bundesbeauftragten für den Datenschutz und Informationsfreiheit, S. 10; Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, S. 19.

So besteht gerade keine Beschränkung der Analyse auf polizeiliche Datenbestände. Selbst wenn eine solche Beschränkung der aktuellen Verwaltungspraxis entspräche, bleibt entscheidend, welche rechtlichen und tatsächlichen Möglichkeiten die Rechtsgrundlage bietet,

vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17, Rn. 320.

Aber selbst unter Zugrundelegung der Interpretation der Staatskanzlei sind die Datenbestände, auf die die Polizei im Rahmen einer automatisierten Datenanalyse zugreifen kann, immens und potenziell unbegrenzt. Rechtlich möglich ist auch danach nämlich, dass in die automatische Datenanalyse alle Daten einfließen können, die die Polizei legal erheben oder sich von anderen öffentlichen Stellen oder privaten Unternehmen übermitteln lassen kann (§ 13 HSOG, § 22 HDSIG).

Vgl. Beschwerdeschrift, S. 74 f.

Einerseits sind schon die polizeilichen Datenbestände der Landes- und Bundesbehörden umfassend und dürften in Zukunft weiterwachsen, wie sich aus den Stellungnahmen der Datenschutzbeauftragten ergibt,

vgl. Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, S. 11-16; Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, S 9 f.

Hinzu kommen, wie die Staatskanzlei selbst schildert, noch Datenbestände aus strafprozessualen Maßnahmen.

§ 13 HSOG stellt keine echte Begrenzung der Menge und Art der Daten dar. Insbesondere können gemäß § 13 Abs. 1 Nr. 2 Alt. 1 HSOG alle Daten aus allgemein zugänglichen Quellen entnommen werden. Eine materielle Erhebungsschwelle besteht nicht, wie sich schon aus einem Vergleich zu § 13 Abs. 1 Nr. 3 HSOG ergibt. Von der Analyse erfasst werden somit auch alle Fotos, Beiträge etc. aus sozialen Netzwerken, da diese in aller Regel öffentlich sind. Dies streitet auch die Staatskanzlei nicht ab. Dass diese Einbeziehung nicht „automatisch“ erfolgt, sondern „manuell initialisiert“ werden muss,

vgl. Stellungnahme Hessische Staatskanzlei, S. 87,

führt zu keiner maßgeblich anderen rechtlichen Bewertung, da hiermit nichts über den Umfang eines solchen „Informationsbeschaffungsprozesses“ gesagt wird.

Schließlich verharmlost die Staatskanzlei die Eingriffsintensität der ermöglichten erweiterten Datennutzung, wenn sie sie lediglich als ein Instrument bezeichnet, um unübersichtliche und große Datenmengen nachvollziehbar darzustellen,

vgl. Stellungnahme Hessische Staatskanzlei, S. 86 f.

Aus § 25a Abs. 2 HSOG wird deutlich, dass es darum geht, Beziehungen zwischen zuvor isolierten Datensätzen herzustellen und neue Informationen zu erzeugen. Denkbar ist auch, dass die Staatskanzlei selbst das Potential einer Datenanalyse durch maschinelles Lernen mit immer leistungsstärkeren Rechnern (noch) nicht erkannt hat.

Die Staatskanzlei behauptet, dass keine unbeteiligten Menschen betroffen seien. Diese seien nicht von der Analyse umfasst, da eine anlasslose Erhebung personenbezogener Daten ohnehin unzulässig wäre,

vgl. Stellungnahme Hessische Staatskanzlei, S. 87.

Dabei verkennt die Staatskanzlei, dass in die Auswertung auch Daten einfließen, die lediglich zur Vorgangsverwaltung und Dokumentation polizeilichen Handelns erhoben und gespeichert wurden. Darin sind neben den Daten von beschuldigten Personen auch Daten von Anzeigenerstatter*innen, Zeug*innen und Opfern enthalten.

Vgl. *Arzt* in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Auflage 2021, Rn. G 1184 ff.

Insbesondere im Vorgangsbearbeitungssystem ComVor finden sich in nicht unerheblichem Umfang auch Daten von Personen, die im polizeirechtlichen Sinne Nichtstörer*innen bzw. nicht Tatverdächtige sind.

Vgl. *Bäuerle* in: BeckOK PolR Hessen, 26. Ed. 01.07.2022, HSOG § 25a Rn. 24; Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, S. 13.

Bei diesen handelt es sich um Menschen, die keinen Anlass für die Speicherung ihrer Daten durch die Polizei gegeben haben. Die Staatskanzlei erweckt den Eindruck, dass die Nutzung von Daten, die lediglich zur Vorgangsverwaltung und Dokumentation polizeilichen Handelns gespeichert werden, den (gesetzlichen) Normalfall darstellt. Dies ist jedoch nicht der Fall, denn grundsätzlich sollen nur Daten von der Polizei für die Analyse genutzt werden, die auch dem konkreten polizeilichen Zweck der Gefahrenabwehr oder der Vorbeugung von Straftaten dienen.

Dieses Problem besteht auch in Bezug auf soziale Medien, selbst wenn kein direkter Zugriff des Systems auf das Internet besteht. Werden Daten aus sozialen Medien erhoben, enthalten diese regelmäßig auch Informationen, über

Freund*innen, Familie und Bekannte einer Zielperson, die sodann von der Analyse umfasst sind.

Der Aussage der Staatskanzlei, dass keine Möglichkeit bestehe, durch die automatisierte Datenanalyse Persönlichkeitsprofile zu erstellen, wird entgegengetreten. Die Staatskanzlei verweist darauf, dass keine neuen Daten erhoben, sondern nur bestehende Daten miteinander verknüpft würden. Zudem könne auch von einer Überwachung über einen längeren Zeitraum, bei der umfassend nahezu alle Bewegungen und Lebensäußerungen registriert werden, keine Rede sein,

vgl. Stellungnahme Hessische Staatskanzlei, S. 99 f.

Die Staatskanzlei verkennt damit die weitreichenden Möglichkeiten der eigenen Maßnahme.

Zunächst wird die Intensität des Grundrechtseingriffs nicht dadurch gemindert, dass die Analyse nach § 25a HSOG auf Daten beruht, die zuvor auf Grundlage anderer Befugnisse erhoben wurden. Einige Daten waren zwar bereits in den vormals getrennten polizeilichen Datenbeständen vorhanden, allerdings können diese auf Grundlage der neuen Befugnis untereinander zusammengeführt werden. Die anschließende gemeinsame Auswertung der Daten ist aufgrund des damit verbundenen Informationsgewinns jedoch ein eigener Grundrechtseingriff von erheblicher Qualität. Durch die komplexen Verarbeitungs- und Verknüpfungsmöglichkeiten, die moderne Software-Tools zur Datenanalyse bieten, gewinnen zuvor möglicherweise belanglose Informationen einen neuen Gehalt.

BVerfGE 156, 11 <109>.

Auf diese Weise werden Zusammenhänge zwischen in zuvor unterschiedlichen Quellen „verstreut“ gespeicherten Daten sichtbar, die wiederum Anlass für Folgemaßnahmen der Polizei geben können. Bei der Beurteilung von § 25a HSOG darf gerade diese Möglichkeit von nachfolgenden operativen polizeilichen Maßnahmen nicht außer Betracht bleiben. Denn oftmals erfolgen diese nicht nur auf Grundlage von ursprünglich erhobenen (belanglosen) Daten aus Befragungen, Observationen oder Telekommunikationsüberwachungen, sondern vielmehr werden Folgemaßnahmen erst durch Information möglich, die aufgrund der automatisierten Analyse gewonnen wurden und somit einen neuen Gehalt erlangten.

Darüber hinaus kann das Argument der Staatskanzlei, dass keine langfristige Überwachung vorliege, nicht überzeugen. Zwar handelt es sich bei der Durchführung der automatisierten Datenanalyse um eine punktuelle Maßnahme, jedoch bezieht sich diese unter Umständen auf eine großen, weit in die Vergangenheit zurückreichenden Datenbestand.

Vgl. Beschwerdeschrift, S. 11 ff.

In Bezug auf die jeweiligen Zielpersonen der polizeilichen Analyse kann die Kombination aus Daten aus den Informationssystemen der Polizei, der Telekommunikationsüberwachung und aus übermittelten Daten etwa vom Einwohnermeldeamt teilweise schon nahezu lückenlose Einblicke in die Persönlichkeit und private Lebensführung dieser Personen bieten. Darüber hinaus können die Inhalte polizeilicher Datenbanken über die Erhebung und Speicherung von Informationen aus sozialen Medien und anderen öffentlichen Quellen angereichert werden und damit einen weitreichenden Einblick in das Leben, die Beziehungen und Netzwerke betroffener Personen gewähren. Insbesondere der Zugriff auf soziale Netzwerke birgt eine große Gefahr. Wie bei Messenger-Diensten und Dating-Apps liegt auch bei sozialen Netzwerken der Kern der Anwendungen im Bereich der sozialen Interaktion. Bereits die Überwachung allein dieser Anwendungen ermöglicht erhebliche Aufschlüsse über die Persönlichkeit von Nutzer*innen. Aus verfassungsrechtlicher Sicht ist eine mögliche etwaige Beschränkung in der Praxis zwar zu begrüßen, jedoch keinesfalls ausreichend. Vielmehr bedürfte es bereits einer Einschränkung in § 25a HSOG selbst, an der es aber fehlt.

Schließlich sind auch aktuelle Entwicklungen der polizeilichen (und allgemein sicherheitsbehördlichen) Informationsordnung zu betrachten, welche die Verknüpfbarkeit vorhandener Datenbestände verbessern sollen. Je mehr Datenbestände immer leichter zugänglich und immer besser verknüpft werden können, desto umfassender sind die Einblicke in die private Lebensführung der Betroffenen und desto höher wird die Gefahr einer Erstellung von umfassenden Persönlichkeitsprofilen.

So soll im Rahmen des Programmes „Polizei 20/20“ ein neues Datenhaus der Polizei geschaffen werden, in dem Daten nicht mehr in getrennten Dateien, sondern gemeinsam thematisch geordnet werden. Im Ergebnis soll das polizeiliche Informationswesen harmonisiert werden, sodass die circa 320.000 Polizeibeschäftigten jederzeit und überall Zugriff auf die Informationen haben. Zentrale Ziele der Umstellung sind die Verbesserung der Verfügbarkeit und Verknüpfbarkeit polizeilicher Informationen. An diese strukturellen Änderungen der Informationsordnung sollen alle 20 deutschen Polizeibehörden beteiligt sein, neben dem Bundeskriminalamt nehmen die 16 Landespolizeibehörden, die Bundespolizei, das Zollkriminalamt und die Polizei beim Deutschen Bundestag teil.

Vgl. Bundesministerium des Inneren, Polizei 2020 - White Paper, S. 8 ff.

3. ANFORDERUNGEN AN „DATA MINING“ NICHT ERFÜLLT

Anders als die Staatskanzlei meint,

Stellungnahme Hessische Staatskanzlei, S. 96,

hält § 25a HSOG den strengen verfassungsrechtlichen Anforderungen nicht stand.

So auch Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, S. 4 ff; Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, S. 25 ff.

Um Wiederholungen zu vermeiden, wird auf die Ausführungen zur nicht hinreichend qualifizierten Eingriffsschwelle verwiesen.

Vgl. Beschwerdeschrift, S. 76 ff.; Stellungnahme vom 10. Mai 2021, S. 5 f.

Weder die von der Staatskanzlei angeführte Aufgabenzuweisung (§ 1 Abs. 4 HSOG) noch der Verhältnismäßigkeitsgrundsatz führen zu einem anderen Ergebnis. Vielmehr bedarf es einer bestimmten und normenklaren Regelung der Eingriffsschwellen einer intensiven Eingriffsermächtigung durch den Gesetzgeber selbst.

Vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17, Rn. 199 ff.

Die erweiterte Datennutzung muss auf spezifische Ziele begrenzt sein. Der Senat unterscheidet zwischen drei verschiedenen Zwecken des „Data Mining“ und fordert diesbezüglich unterschiedlich hohe Eingriffsschwellen.

Für die erweiterte Nutzung zur Gefahrenabwehr muss eine wenigstens hinreichend konkretisierte Gefahr in dem Sinne gegeben sein, dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für hochrangige Rechtsgüter vorliegen.

Vgl. BVerfGE 156, 11 <Leitsatz 3.b., Rn. 118>.

Mit der Bezugnahme auf § 100a Abs. 2 StPO verlagert § 25a HSOG die Eingriffsschwelle derart weit in das Vorfeld einer konkreten Gefahr, dass nach dem Wortlaut nicht einmal auf Tatsachen gestützte Anhaltspunkte für bestimmte Straftaten vorliegen müssen.

So auch Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, S. 5f.

Anders als die Staatskanzlei meint, kann diese extrem niedrige Anforderung an die Gefahrenprognose nicht dadurch kompensiert werden, dass § 25a HSOG ausschließlich besonders gewichtige Rechtsgüter wie Leib, Leben, Freiheit der Person, Bestand oder Sicherheit des Bundes oder eines Landes schütze,

vgl. Stellungnahme Hessische Staatskanzlei, S. 97.

Vielmehr enthält § 100a Abs. 2 StPO auch Straftaten, deren Schutzgüter keineswegs äquivalent zu den in § 25a HSOG genannten Schutzgütern sind.

Vgl. Beschwerdeschrift, S. 77.

Darüber hinaus wird nicht in Abrede gestellt, dass für die Verwendung von personenbezogenen Daten, die durch besonders invasive Ermittlungsmethoden wie nach §§ 100b, 100c und 100g StPO gewonnen wurden, besondere Eingriffsschwellen bestehen, auf welche § 20 Abs. 6 HSOG i.V.m. § 479 Abs. 2 StPO verweisen.

Allerdings ändert dies nichts an den zu niedrigen Eingriffsschwellen des § 25a HSOG selbst, welcher einen eigenen Grundrechtseingriff darstellt. Vielmehr verdeutlicht dies nur erneut die hohe Eingriffsintensität des § 25a HSOG, denn aufgrund der Verwendung personenbezogener Daten aus besonders invasiven Ermittlungsarten, können auch höchstpersönliche Daten aus einer Online-Durchsuchung oder Wohnraumüberwachung in die Datenanalyse einbezogen werden. Die Gefahr der Bildung eines umfassenden Persönlichkeitsprofils nimmt dadurch erheblich zu, zu denken ist hier an die Möglichkeiten einer Sprachanalyse von aufgezeichneten Unterhaltungen. Aufgrund leistungsstarker Rechner und selbstlernender Algorithmen können auf diese Weise sogar Nebensächlichkeiten Bedeutung erlangen. So könnte z.B. aus einer belegten Stimme, Husten, Nießen etc. auf den Gesundheitszustand geschlossen werden. Ob die eingesetzte Software dies technisch heute schon kann, ist unklar. Wie zahlreiche „Digital Health“-Anwendungen zeigen, wäre dies schon heute alles andere als Zukunftsmusik, rechtlich möglich wäre es jedenfalls.

Auch die Ausführungen der Staatskanzlei hinsichtlich der Verhältnismäßigkeit des geschützten Rechtsguts der Sachen von bedeutendem Wert überzeugen nicht.

Vgl. Stellungnahme Hessische Staatskanzlei, S. 98 f.

Die Argumentation stützt sich auf einen Verweis auf andere Normen, die ebenfalls dieses Schutzgut enthalten und angeblich als verfassungskonform zu betrachten seien. Es muss jedoch vom Gesetzgeber präzise und bestimmt im Wortlaut deutlich gemacht werden, dass angesichts der Schwere des mit der Datenanalyse verbundenen Grundrechtseingriffs die in § 25a Abs. 1 HSOG normierten Sachen von bedeutendem Wert im Sinne des Urteils zum BKA-Gesetz nur wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen sein können.

Gleiches gilt für die Ausführungen zur Staatskanzlei bezüglich des Rechtsguts der gleichgewichtigen Schäden für die Umwelt.

Vgl. Stellungnahme Hessische Staatskanzlei, S. 99.

Es ändert nichts an der Unbestimmtheit der Formulierung dieses Schutzguts in § 25a HSOG, dass in der Gesetzesbegründung zum ehemaligen § 26 HSOG konkretere Ausführungen zur Auslegung getroffen wurden. Diese vermögen

nichts daran zu ändern, dass § 25a HSOG nicht den Grundsatz der Normenklarheit und Bestimmtheit erfüllt.

4. UNZULÄSSIGE DYNAMISCHE VERWEISUNG

Darüber hinaus ist dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit zuzustimmen, wenn dieser es in Betracht zieht, die Verweisung auf den Katalog des § 100a StPO als unzulässige dynamische Verweisung einzustufen,

> vgl. Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, S. 17; Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, S. 23f.

Aus dem vom Landesgesetzgeber erlassenen § 25a HSOG geht nicht hinreichend hervor, ob auf die jeweils aktuelle Fassung von § 100a Abs. 2 StPO Bezug genommen wird – eine Vorschrift, die regelmäßig vom Bundesgesetzgeber verändert wird – oder eine spezifische Fassung als Anknüpfungspunkt festgelegt sein soll.

Allerdings verlangen Regelungen, die zu einem Grundrechtseingriff ermächtigen, eine Abwägung des betroffenen Grundrechts mit entgegenstehenden Grundrechten, anderen Verfassungsbelangen oder sonstigen schützenswerten Interessen. Die grundlegende Grundrechtsabwägung muss der zum Grundrechtseingriff ermächtigende Gesetzgeber treffen, um so die Verantwortung für die Abwägungsentscheidung zu übernehmen. Dies ist aber nicht ohne Weiteres realisierbar, wenn der Landesgesetzgeber dynamisch auf Bundesrecht verweist. Dann besteht die Gefahr, dass letztlich gar kein Gesetzgeber die erforderliche Abwägungsentscheidung in voller Verantwortung trifft.

> Vgl. BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17, Rn. 385.

Bei § 100a Abs. 2 StPO handelt es sich um eine Vorschrift des Bundesgesetzgebers. Der hessische Landtag kann damit nicht beeinflussen, ob und wann die Vorschrift geändert wird. Zudem liegt der landesgesetzgeberischen Abwägung die derzeitige Fassung von § 100a Abs. 2 StPO zugrunde. Sofern eine dynamische Verweisung vorliegen soll – was bei der derzeitigen Formulierung naheliegt – führt eine Änderung von § 100a Abs. 2 StPO dazu, dass nunmehr auch Maßnahmen aus Gründen möglich sind, die der Landesgesetzgeber nicht in die notwendige Abwägung miteinbezogen hatte.

Außerdem müssen solche dynamische Verweisungen von einem Landesgesetz auf ein Bundesgesetz ein eng umrissenes Feld betreffen und den Inhalt im Wesentlichen bereits festlegen,

> vgl. BVerfGE 23, 265 <269 f.>; 26, 338 <366 f.>; 153, 310 <343 Rn. 79>.

Aufgrund der Verweisung in § 25a HSOG auf § 100a Abs. 2 StPO ist jedoch kaum ersichtlich, wie umfangreich der Anwendungsbereich tatsächlich ist. Dies verstößt gegen das Gebot der Normenklarheit.

5. GRUNDSATZ DER ZWECKÄNDERUNG

Die Staatskanzlei suggeriert in ihrer Stellungnahme, dass die Beschwerdeführenden davon ausgehen, § 20 HSOG sei nicht auf § 25a HSOG anwendbar,

> vgl. Stellungnahme Hessische Staatskanzlei, S. 89.

Dies ist nicht richtig, tatsächlich wird die Anwendbarkeit von § 20 HSOG in der Verfassungsbeschwerde sogar ausdrücklich angenommen.

> vgl. Beschwerdeschrift, S. 81.

Wie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit treffend ausführt, wird jedoch der Grundsatz der Zweckbindung nicht eingehalten. Vielmehr wird die eigentlich notwendige Trennung zwischen Aufgabenerfüllung, Vorgangsverwaltung, Dokumentation und Gefahrenvorsorge bzw. Strafverfolgungsvorsorge bei der automatisierten Analyse nach § 25a HSOG aufgehoben. In § 25a i. V. m. § 20 Abs. 9 Satz 3 HSOG ist dies ausdrücklich geregelt. Dem entspricht der weite Wortlaut, der sich wie dargelegt auf sämtliche „gespeicherte personenbezogene Daten“ bezieht. Da § 20 Abs. 9 Satz 3 HSOG insoweit eine ausdrückliche Regelung trifft, lässt der Wortlaut in Bezug auf die gebotene Zweckbindung – auch angesichts des Umfangs der betroffenen Datenbestände – keinen Spielraum für eine verfassungskonforme Auslegung.

> Vgl. Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, S. 28.

Darüber hinaus wurde in der Verfassungsbeschwerde vorgebracht, dass eine Datenverarbeitung nach § 25a HSOG keine bloße weitere Nutzung von Daten darstellt, die nur den eher geringen Anforderungen der Zweckbindung unterliegt – auch wenn bereits diese nicht von § 25a HSOG erfüllt werden. Um Wiederholungen zu vermeiden, wird auf die Beschwerdeschrift verwiesen.

> Vgl. Beschwerdeschrift, S. 71 f.

Lediglich die Anforderungen der Zweckbindung für die automatisierte Datenanalyse zu verlangen, ist unzureichend. Vielmehr sind darüber hinaus, aufgrund der neuen Qualität des Eingriffs, die weitergehenden verfassungsrechtliche Anforderungen nach dem Grundsatz der Zweckänderung und der hypothetischen Datenneuerhebung geboten.

6. UNZUREICHENDE VERFAHRENSSICHERUNGEN

§ 25a HSOG verfehlt die Anforderungen an Transparenz, Rechtsschutz und Kontrolle.

Eine Benachrichtigungspflicht ist nicht vorgesehen (s.o. unter B.VI.), wäre jedoch angesichts der Eingriffsintensität geboten.

Der Auskunftsanspruch nach § 29 HSOG i. V. m. § 52 HDSIG ist nicht ausreichend, weil nicht sichergestellt ist, dass sich der Anspruch auch auf die automatisierte Datenanalyse und die damit generierten Daten bezieht,

> vgl. Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, S. 16.

Jedenfalls wäre aber ein normenklarer, gesetzlich verankerter Anspruch auf Auskunft erforderlich,

> so auch der Hessische Beauftragte für Datenschutz und Informationsfreiheit in seiner Stellungnahme, S. 16.

Der Staatskanzlei ist auch nicht zuzustimmen, wenn sie die Protokollierungspflicht nach § 71 HDSIG als ausreichend erachtet,

> vgl. Stellungnahme Hessische Staatskanzlei, S. 102.

§ 71 Abs. 2 HDSIG trifft zwar allgemeine Protokollierungsvorgaben, fordert allerdings keine spezifische Begründung für die konkrete Nutzung der Daten. Aufgrund des intensiven Grundrechtseingriffs der automatisierten Datenanalyse nach § 25a HSOG ist jedoch zur Gewährleistung eines effektiven Rechtsschutzes eine solche konkrete Begründung zu fordern – insbesondere in Anbetracht der unbestimmten Formulierung der angegriffenen Vorschrift.

> So auch Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, S. 8.

Darüber hinaus ist § 25a HSOG auch nicht von der speziellen Protokollierungspflicht bei verdeckten und eingriffsintensiven Verfahren nach § 28 HSOG erfasst.

> So auch Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, S. 17.

Schließlich verkennt die hessische Staatskanzlei die Voraussetzungen einer wirksamen Aufsicht.

> Vgl. Stellungnahme Hessische Staatskanzlei, S. 104.

Zwar ist eine Anhörung des Hessischen Datenschutzbeauftragten in § 25a Abs. 3 Satz 2 HSOG vorgeschrieben, diese läuft in der Praxis jedoch ins Leere. Denn eine Anhörung erfolgt nur für generelle Anordnungen der Polizeibehörden, nicht jedoch für die Anwendung der automatisierten Datenanalyse im konkreten Einzelfall. Darüber hinaus mangelt es der Behörde in § 14 Abs. 3 HDSIG an der Befugnis eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen, was jedoch für eine unionsrechtskonforme Umsetzung des Art. 47 Abs. 2 lit. c) der Richtlinie (EU) 2016/680 (JI-RL) notwendig wäre.

Vgl. Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, S. 17.

Dass dies in der Praxis die aktuellen Ressourcen der hessischen Datenschutzbehörde in personeller Hinsicht überspannen würde, ändert nichts an der grundlegenden Notwendigkeit einer effektiven Kontrolle und Aufsicht für intensive Grundrechtseingriffe.

BVerfGE 65, 1 <46>; 133, 277 <370 Rn. 215>; 141, 220 <Rn. 141>.

Der Hinweis der Hessischen Staatskanzlei, dass die Datenschutzbehörde selbst eine Beanstandung verbunden mit der Aufforderung zur Stellungnahme zu den ergriffenen Maßnahmen vornehmen könne,

vgl. Stellungnahme Hessische Staatskanzlei, S. 105,

verkennt die verfassungsrechtlichen Anforderungen an eine effektive Aufsicht und Kontrolle.

Zunächst ist erforderlich, dass Zugriffe und Änderungen des Datenbestandes vollständig protokolliert werden. Angesichts der Kompensationsfunktion der aufsichtlichen Kontrolle für den schwach ausgestalteten Individualrechtsschutz kommt deren regelmäßiger Durchführung besondere Bedeutung zu. Demnach sind solche Kontrollen in angemessenen Abständen – deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf – durchzuführen. Dies ist bei der Ausstattung der Aufsichtsinstanz zu berücksichtigen.

Vgl. BVerfGE 133, 277 <370 f. Rn. 217>; 141, 220 <Rn. 141>.

Bereits eine umfassende Protokollierungspflicht lässt § 25a HSOG vermissen (s.o.).

Darüber hinaus erfüllt eine Beanstandung aus eigener Initiative des Datenschutzbeauftragten nicht die verfassungsrechtlichen Vorgaben an eine regelmäßige Durchführung der Kontrolle. Um diese mit Sicherheit zu gewährleisten, muss eine solche Kontrolle hinreichend bestimmt im Gesetz verankert werden und darf nicht zur freien Disposition der Aufsichtsbehörde gestellt werden.

Schließlich ist die Wirkung einer Warnung gem. § 14 Abs. 2 Satz 5 HDSIG,

vgl. Stellungnahme Hessische Staatskanzlei, S. 105,

nicht mit der Effektivität einer – wie vom Hessischen Datenschutzbeauftragten geforderten – endgültigen Beschränkung der Verarbeitung oder eines Verbots vergleichbar und kann keine effektive Aufsicht sicherstellen.

Um eine solche Aufsicht durch die hessische Datenschutzbehörde trotz knapper Ressourcen zu gewährleisten, schlägt der Hessische Beauftragte für Datenschutz und Informationsfreiheit vor, dass die Pflicht zur Datenschutzkontrolle in § 29a HSOG auch auf § 25a HSOG erweitert wird. Darüber hinaus sollten die Behördenleitervorbehalte nach § 25a Abs. 3 Satz 1 HSOG ausgebaut, regelmäßige Berichtspflichten eingeführt sowie Richtervorbehalte jedenfalls hinsichtlich der Nutzung von TKÜ-Daten und Funkzellendaten für die Datenanalyse normiert werden.

Vgl. Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, S. 18.

Diesem Vorschlag ist als erster konkreter Schritt hin zu einer effektiven Aufsicht und Kontrolle zur Wahrung des Rechtsschutzgebots des Art. 19 Abs. 4 GG zuzustimmen.