



Stellungnahme

des Deutschen Anwaltvereins durch die Ausschüsse Gefahrenabwehrrecht und Verfassungsrecht

zu der Verfassungsbeschwerde zum Gesetz
über die öffentliche Sicherheit und Ordnung
in Mecklenburg-Vorpommern (Sicherheits-
und Ordnungsgesetz – SOG M-V)
– 1 BvR 1345/21 BVerfG –

Stellungnahme Nr.: 33/2022

Berlin, im Juni 2022

Mitglieder des Ausschusses Gefahrenabwehrrecht

- Rechtsanwältin Lea Voigt, Bremen (Vorsitzende, Berichterstatterin)
- Rechtsanwalt Wilhelm Achelpöhler, Münster (Berichterstatter)
- Rechtsanwalt Dr. David Albrecht, Berlin
- Rechtsanwalt Dr. Eren Basar, Düsseldorf
- Prof. Dr. Annika Dießner, Berlin (ständiges Gastmitglied im Ausschuss)
- Rechtsanwalt Dr. Nikolaos Gazeas, LL.M., Köln
- Rechtsanwalt Dr. Andreas Grözing, Köln
- Rechtsanwalt Dr. Mayeul Hiéramente, Hamburg (Berichterstatter)
- Rechtsanwalt Dr. Saleh Ihwas, Frankfurt am Main
- Rechtsanwalt Prof. Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt
- Rechtsanwältin Dr. Vivien Veit, Mönchengladbach
- Prof. Dr. Mark A. Zöller, München (ständiges Gastmitglied im Ausschuss)

Deutscher Anwaltverein

Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel

Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwalt Max Gröning
- Rechtsanwältin Uta Katharina Schmidt

Mitglieder des Ausschusses Verfassungsrecht

- Rechtsanwalt Prof. Dr. Christian Winterhoff, Hamburg
(Vorsitzender)
- Rechtsanwältin Dr. Antje Wittmann, Münster
(Stellvertretende Vorsitzende)
- Rechtsanwältin Mechtild Düsing, Münster
- Rechtsanwalt Dr. Rainard Menke, Stuttgart
- Rechtsanwalt Dr. Sebastian Schmuck, Leipzig
- Rechtsanwältin Dr. Inga Schwertner, Köln
- Rechtsanwalt Stefan von Raumer, Berlin
- Rechtsanwalt Dr. Roya Sangi, Berlin
- Rechtsanwältin Dr. Maria Marquard, Stuttgart
(Berichterstatteerin)

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwalt Dr. Nicolas Lührig, Berlin

Verteiler

- Bundesverfassungsgericht
- An die Mitglieder des Rechtsausschusses des Deutschen Bundestages
- Ausschuss für Inneres und Heimat des Deutschen Bundestages
- Arbeitsgruppe Recht und Verbraucherschutz der im Deutschen Bundestag vertretenen Parteien
- Arbeitsgruppe Inneres der im Deutschen Bundestag vertretenen Parteien
- Rechts- und Innenausschüsse der Landtage
- Bundesministerium der Justiz
- Bundesministerium des Innern und für Heimat
- An die Justizministerien und Justizverwaltungen der Bundesländer
- Bundesrechtsanwaltskammer
- Landesministerien und Senatsverwaltungen des Innern
- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Landesdatenschutzbeauftragte
- Deutscher Richterbund
- Bundesverband der Freien Berufe
- Deutsches Institut für Menschenrechte
- Gesellschaft für Freiheitsrechte
- An die Mitglieder des Vorstandes des Deutschen Anwaltvereins
- An die Vorsitzenden der Landesverbände des Deutschen Anwaltvereins
- An die Vorsitzenden der Gesetzgebungsausschüsse des Deutschen Anwaltvereins
- Forum Junge Anwaltschaft

Presse

- Redaktion NJW
- Frankfurter Allgemeine Zeitung
- Süddeutsche Zeitung
- Berliner Verlag GmbH
- Hamburger Abendblatt
- Der Tagesspiegel
- Der Spiegel
- Juris Newsletter

- JurPC
- Netzpolitik.org
- Heise
- LTO

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt mehr als 61.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 253 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene. Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

Kurzzusammenfassung

Der Deutsche Anwaltverein hält die vorliegende Verfassungsbeschwerde weitgehend für begründet. Das angefochtene SOG M-V bleibt vielfach hinter den verfassungsrechtlichen Vorgaben zurück. Dies gilt insbesondere für die in dem Gesetz vorgesehene Ausweitung von Eingriffsbefugnissen im Vorfeld konkreter Gefahren, die Regelungen zum Kernbereichsschutz und die Ausgestaltung von sog. Quellen-Telekommunikationsüberwachung und Online-Durchsuchung.

Die Stellungnahme behandelt im Allgemeinen Teil unter A. zunächst die beiden Themen Eingriffsschwelle und Kernbereichsschutz während dann unter B. die einzelnen Maßnahmen Wohnraumüberwachung, Online-Durchsuchung, Quellen-TKÜ, Rasterfahndung und Schutzpflichten für die IT-Sicherheit (Ausnutzung und Aufrechterhaltung von technischen Lücken) behandelt werden.

A. Allgemeiner Teil

I. Eingriffsschwelle (konkrete und drohende Gefahr)

Aus dem Grundsatz der Verhältnismäßigkeit im engeren Sinne ergeben sich Anforderungen an die tatbestandlichen Voraussetzungen polizeilicher Eingriffe. Diese hängen vom jeweiligen Eingriffsgewicht der Maßnahme ab (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 152, juris).

Anknüpfungspunkt für polizeiliches Handeln ist die konkrete Gefahr, also eine Sachlage, bei der im Einzelfall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für die öffentliche Sicherheit und Ordnung eintreten kann, § 3 Abs. 3 Nr. 1 SOG M-V. Eine konkrete Gefahr liegt vor, wenn die Prognose eines konkreten Gefahrenereignisses getroffen werden kann. Bestehen lediglich Anhaltspunkte für eine konkrete Gefahr im Sinne eines Gefahrenverdachts, dürfen allenfalls Eingriffe erfolgen, um die fehlenden Informationen zu beschaffen (vgl. Bäcker in: Lisken/Denniger Handbuch des Polizeirechts 7. Auflage S. 267). Ein Gefahrenverdacht legitimiert nur Maßnahmen der *Gefahrerforschung*.

Für bestimmte Bereiche kann der Gesetzgeber mit dem Ziel der Straftatenverhütung weitere polizeiliche Maßnahmen auch im Vorfeld einer konkreten Gefahr gestatten, indem er die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378 (LT 1-3), Rn. 112).

Diese Rechtsprechung des BVerfG hat der Landesgesetzgeber mit der Einführung der elektronischen Aufenthaltsüberwachung in § 67a SOG M-V aufgegriffen. Diese Maßnahme ist nach § 67a Abs. 1 SOG M-V nicht von einer konkreten Gefahr abhängig, sondern davon, dass entweder Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat nach § 67c SOG M-V begehen oder an dieser teilnehmen wird, oder das individuelle Verhalten dieser Person die konkrete Wahrscheinlichkeit dafür begründet, dass sie innerhalb eines überschaubaren Zeitraums eine terroristische Straftat nach § 67c SOG M-V begehen oder an dieser teilnehmen wird.

In der Begründung des Gesetzentwurfs zur Einführung des § 67a SOG M-V mit dem Sechsten Gesetz zur Änderung des Sicherheits- und Ordnungsgesetzes Drucksache 7/1320 S. 17 führte der Gesetzgeber explizit aus, mit § 67 a SOG M-V sollten Eingriffsbefugnisse im Vorfeld einer konkreten Gefahr geschaffen

werden. Hinsichtlich des Wortlauts des § 67a SOG M-V orientierte sich der Gesetzgeber ausdrücklich an jenen Passagen des Urteils des Bundesverfassungsgerichts zum BKA-Gesetz, in denen die Voraussetzungen beschrieben werden, unter denen der Gesetzgeber polizeiliche Maßnahmen im Vorfeld einer konkreten Gefahr gestatten kann (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378 (LT 1-3), Rn. 112).

Nunmehr sollen unter den Voraussetzungen des § 67a Abs. 1 SOG M-V auch Maßnahmen wie die Wohnraumüberwachung, § 33b Abs. 1 Satz 2 SOG M-V, der Einsatz technischer Mittel zum Eingriff in informationstechnische Systeme, § 33c Abs. 1 S. 2 SOG M-V, der Einsatz technischer Mittel zur Überwachung der Telekommunikation, § 33d Abs. 1 S.1 Nr. 2-4 SOG M-V, und die Rasterfahndung, § 44 Abs. 1 Nr. 1 SOG M-V, gestattet werden.

Diese Ausweitung von Eingriffsbefugnissen im Vorfeld der konkreten Gefahr wird von den Beschwerdeführern zu Recht gerügt, was wir im Einzelnen unter B. darlegen werden.

II. Kernbereichsschutz

§ 26a SOG M-V enthält allgemeine Regelungen zum Schutz des **Kernbereichs** privater Lebensgestaltung. Die Norm gilt für alle Maßnahmen der Datenerhebung. Sie ist daher systematisch den konkreten Regelungen zur Datenerhebung vorangestellt.

1. Allgemeine Maßstäbe des Bundesverfassungsgerichts

Der verfassungsrechtliche Schutz des Kernbereichs privater Lebensgestaltung gewährleistet dem Individuum einen Bereich höchstpersönlicher Privatheit gegenüber staatlicher Überwachung. Er wurzelt in den von den jeweiligen Überwachungsmaßnahmen betroffenen Grundrechten in Verbindung mit Art. 1 Abs. 1 GG und sichert einen dem Staat nicht verfügbaren Menschenwürdekern grundrechtlichen Schutzes gegenüber solchen Maßnahmen (BVerfGE 141, 220-

378, juris Rn. 120; Urteil vom 26. April 2022 – 1 BvR 1619/17 -, juris Rn. 275; BVerfGE 120, 274-350, juris Rn. 271).

Der Schutz des Kernbereichs privater Lebensgestaltung ist strikt und darf nicht durch Abwägung mit den Sicherheitsinteressen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes relativiert werden (BVerfGE 141, 220-378, juris Rn. 122, 124; Urteil vom 26. April 2022 – 1 BvR 1619/17 –, juris Rn. 277). Selbst überragende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Bereich privater Lebensgestaltung nicht rechtfertigen (BVerfGE 141, 220-378, juris Rn. 120; BVerfGE 120, 274-350, juris Rn. 271). Nach der Rechtsprechung des Bundesverfassungsgerichts bedeutet dies nicht, dass jede tatsächliche Erfassung von höchstpersönlichen Informationen stets einen Verfassungsverstoß oder gar eine Menschenwürdeverletzung begründet (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, juris Rn. 277).

Ein heimliches Vorgehen des Staates führt an sich noch nicht zu einer Verletzung des absolut geschützten Achtungsanspruchs. Wird jemand zum Objekt einer Beobachtung, geht damit nicht zwingend eine Missachtung seines Wertes als Mensch einher (BVerfGE 109, 279-391, juris Rn. 122). Absolut ausgeschlossen ist daher nur ein gezielter Zugriff auf den Kernbereich privater Lebensgestaltung (BVerfGE 141, 220-378, juris Rn. 125).

Überwachungsmaßnahmen können jedoch auch zu einem unbeabsichtigten Eindringen in den Kernbereich privater Lebensgestaltung führen. In diesem Fall muss dem Kernbereichsschutz bei der Durchführung von Überwachungsmaßnahmen auf zwei Ebenen Rechnung getragen werden:

- Zum einen sind auf der Ebene der **Datenerhebung** Vorkehrungen zu treffen, die eine unbeabsichtigte Miterfassung von Kernbereichsinformationen nach Möglichkeit ausschließen (BVerfGE 141, 220-378, juris Rn. 126; Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, juris Rn. 277; BVerfGE 120, 274-350, juris Rn. 277). Es ist durch eine vorgelagerte Prüfung sicherzustellen, dass die Erfassung von kernbereichsrelevanten Situationen oder Gesprächen jedenfalls insoweit ausgeschlossen ist, als sich diese mit praktisch zu bewältigendem

Aufwand im Vorfeld vermeiden lässt. In jedem Fall ist der Abbruch der Maßnahme vorzusehen, wenn erkennbar wird, dass eine Überwachung in den Kernbereich privater Lebensgestaltung eindringt (BVerfGE 141, 220-378, juris Rn. 128).

- Zum anderen sind auf der Ebene der nachgelagerten **Auswertung und Verwertung** die Folgen eines dennoch nicht vermiedenen Eindringens in den Kernbereich privater Lebensgestaltung strikt zu minimieren (BVerfGE 141, 220-378, juris Rn. 126; Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, juris Rn. 277). Entscheidende Bedeutung für den Schutz hat insoweit die Durchsicht der erhobenen Daten auf kernbereichsrelevante Inhalte, für die ein geeignetes Verfahren vorzusehen ist, das den Belangen des Betroffenen hinreichend Rechnung trägt (BVerfGE 120, 274-350, juris Rn. 283).

2. Ausnahme in § 26a Abs. 3 Satz 1 Hs. 2 SOG M-V

Die Beschwerdeführer rügen die Ausnahme in § 26a Abs. 3 Satz 1 Hs. 2 SOG M-V. Sie machen geltend, dass der Schutz des Kernbereichs privater Lebensgestaltung einer unzulässigen Abwägung zugeführt werde.

a) Wortlaut und Auslegung

Grundsätzlich ist nach § 26a Abs. 3 Satz 1 SOG M-V eine zulässige Datenerhebung abubrechen, wenn während der Erhebung Tatsachen die Annahme rechtfertigen, dass Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erfasst werden. Von diesem Grundsatz werden in § 26a Abs. 3 Satz 1 Hs. 2 SOG M-V zwei Ausnahmen zugelassen: Ein Abbruch ist nicht vorzunehmen, sofern mit dem Abbruch der Maßnahme entweder eine Gefährdung der eingesetzten Polizeibeamten oder Vertrauenspersonen oder ihrer weiteren Verwendung verbunden wäre.

Es ist nicht ohne Weiteres ersichtlich, welche Konstellationen der Gesetzgeber bei den Ausnahmen vom Abbruch der Datenerhebung zugunsten der

eingesetzten, ermittelnden Personen vor Augen hatte. Die Gesetzesbegründung äußert sich dazu nicht (vgl. LT-Drs. 7/3694, S. 158). § 100d StPO, auf den die Gesetzesbegründung (S. 157) verweist, enthält keine vergleichbare Regelung. Eine vergleichbare Regelung findet sich in § 45 Abs. 7 Satz 2 BKAG. § 45 BKAG regelt die besonderen Mittel der Datenerhebung zur Abwehr von Gefahren des internationalen Terrorismus. Mit dieser Regelung sollte der ehemalige § 20g BKAG (a.F.) an die Vorgaben des Bundesverfassungsgerichts in seinem Urteil vom 20. April 2016 zum BKA-Gesetz (BVerfGE 141, 220-378) angepasst werden (BT-Drs. 18/11163, S. 113 und 115). Besondere Mittel der Datenerhebung sind z.B. der Einsatz von Vertrauenspersonen und verdeckten Ermittlern (§ 45 Abs. 2 Nr. 4 und 5 BKAG). Nach § 45 Abs. 7 Satz 2 BKAG ist die Maßnahme zu unterbrechen, wenn sich Anhaltspunkte für eine Kernbereichsrelevanz ergeben, „sobald dies ohne Gefährdung der beauftragten Person möglich ist“. Hier geht es offenbar um den Schutz von verdeckten Ermittlern und Vertrauenspersonen.

Es ist anzunehmen, dass der Gesetzgeber bei der Ausnahme in § 26a Abs. 3 Satz 1 Hs. 2 SOG M-V ebenfalls den Schutz verdeckter Ermittler und Vertrauenspersonen vor Augen hatte. Der Einsatz von verdeckten Ermittlern und Vertrauenspersonen ist in § 33 SOG M-V geregelt, auf den § 26a SOG M-V Anwendung findet. Vertrauenspersonen sind in der Ausnahme in § 26a Abs. 3 Satz 1 Hs. 2 SOG M-V ausdrücklich genannt. Dabei handelt es sich um Personen, deren Zusammenarbeit mit der Polizei den Betroffenen und Dritten nicht bekannt ist (§ 33 Abs. 1 Nr. 3 SOG M-V). Verdeckte Ermittler sind Polizeivollzugsbeamte, die unter einer ihnen verliehenen, auf Dauer angelegten, veränderten Identität eingesetzt werden (§ 33 Abs. 1 Nr. 4 SOG M-V). Soweit § 26a Abs. 3 Satz 1 Hs. 2 SOG M-V eine Ausnahme vom Maßnahmenabbruch im Falle einer „Gefährdung der eingesetzten Polizeibeamtinnen und Polizeibeamten“ vorsieht, sind hiermit verdeckte Ermittler gemeint. Es ist durchaus denkbar, dass ein (sofortiger) Abzug eines verdeckten Ermittlers oder einer Vertrauensperson dazu führt, dass der Betroffene die wahre Identität der Person erkennt oder zumindest vermutet. Dies kann die eingesetzte Person in Gefahr bringen und/oder ihre weitere Verwendung unmöglich machen. Dem wollte der Gesetzgeber offenbar entgegenwirken.

Dies wird durch einen Vergleich mit den Regelungen in anderen Bundesländern bestätigt. So ist nach Art. 8a Abs. 1 Satz 2 BayVSG die Anwendung eines nachrichtendienstlichen Mittels bei Anhaltspunkten für Kernbereichsrelevanz zu unterbrechen, „sobald dies ohne Gefährdung oder Enttarnung eingesetzter Personen möglich ist“. Die Verwendung des Begriffs Enttarnung macht ebenfalls deutlich, dass es hier um den Schutz von verdeckt eingesetzten Personen geht. In Baden-Württemberg wurde in § 49 Abs. 8 Satz 2 PolG die Regelung des § 45 Abs. 7 Satz 2 BKAG (s.o.) wörtlich übernommen. § 16 Abs. 2 Satz 1 Hs. 2 PolG NRW macht eine Ausnahme vom Grundsatz des Abbruchs der Datenerhebung, wenn die Erhebung aus zwingenden ermittlungstechnischen Gründen nicht unterbleiben kann. Nach der Gesetzesbegründung handelt es sich bei den „ermittlungstechnischen Gründen“ um gegenwärtige Gefahren für Leib und Leben verdeckt eingesetzter Personen (NRW LT-Drs. 14/10089, S. 28).

All diese Regelungen zielen darauf ab, verdeckt eingesetzte Personen vor Gefahren zu schützen bzw. ihre weitere Verwendungsmöglichkeit sicherzustellen. Zu diesem Zweck darf nach den o.g. Regelungen eine Maßnahme weitergeführt werden, selbst wenn sich im Laufe der Datenerhebung die Kernbereichsrelevanz herausstellt. Dies wird von den Beschwerdeführern beanstandet.

b) Unvereinbarkeit mit absolutem Schutz des Kernbereichs (Art. 1 Abs. 1 GG)

Die Ausnahmen in § 26 Abs. 3 Satz 1 Hs. 2 SOG M-V sind verfassungswidrig. Sie sind mit dem durch Art. 1 Abs. 1 GG geschützten unantastbaren Kernbereich privater Lebensgestaltung unvereinbar.

aa) Der Schutz des Kernbereichs privater Lebensgestaltung ist Ausfluss der Menschenwürdegarantie aus Art. 1 Abs. 1 GG. Er gilt absolut und darf weder mit Sicherheitsinteressen des Staates noch mit anderen überragenden Interessen der Allgemeinheit abgewogen werden (BVerfGE 141, 220-378, juris Rn. 120, 122; Urteil vom 26. April 2022 – 1 BvR 1619/17 –, juris Rn. 277; Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, juris Rn. 271).

Soweit die Ausnahme in § 26a Abs. 3 Satz 1 Hs. 2 Var. 2 SOG M-V das Erfassen von Erkenntnissen aus dem Kernbereich privater Lebensgestaltung zulässt, wenn mit dem Abbruch der Maßnahme eine Gefährdung der weiteren Verwendung von verdeckten Ermittlern oder Vertrauenspersonen verbunden wäre, hat der Gesetzgeber eine unzulässige Abwägung zwischen Kernbereichsschutz und staatlichem Interesse an einer erfolgreichen Ermittlung vorgenommen. Dabei hat er sich für den Vorrang des Ermittlungserfolgs entschieden. Der weiteren Verwendung der verdeckt eingesetzten Person – sei es im konkreten Fall oder in Zukunft – wird ein höheres Gewicht beigemessen als dem Kernbereichsschutz des Betroffenen. Dies ist mit den verfassungsrechtlichen Maßgaben des Kernbereichsschutzes i.V.m. Art. 1 Abs. 1 GG unvereinbar.

Gleiches gilt für die Ausnahme bei einer Gefährdung der verdeckt eingesetzten Person (§ 26a Abs. 3 Satz 1 Hs. 2 Var. 1 SOG M-V). § 26 Abs. 3 Satz 1 Hs. 2 SOG M-V enthält keine Konkretisierung, um welche Art von Gefährdung es sich handeln muss. Gemeint dürfte eine Gefahr für hochrangige Individualrechtsgüter wie Leib oder Leben sein. Bei diesem Normverständnis hat der Gesetzgeber hier eine Abwägung zwischen Kernbereichsschutz aus Art. 1 Abs. 1 GG und dem Grundrecht auf Leben und körperliche Unversehrtheit aus Art. 2 Abs. 2 Satz 1 GG vorgenommen. Das Abwägungsverbot gilt jedoch nicht nur für „schwerwiegende Interessen der Allgemeinheit“ (vgl. BVerfG, NJW 2012, 907 Rn. 99). Die Unantastbarkeit der Menschenwürde lässt für eine Abwägung generell keinen Raum. Nimmt man den Schutz des Kernbereichs der privaten Lebensgestaltung als Ausfluss der Menschenwürdegarantie ernst, lässt sich ein Eingriff auch nicht mit dem Schutz des Lebens anderer – hier der verdeckt eingesetzten Personen – rechtfertigen (BVerfGE 115, 118-166, juris Rn. 129 ff.). Auch insoweit ist die Ausnahme in § 26b Abs. 3 Satz 1 Hs. 2 SOG M-V verfassungswidrig.

bb) Aus der bisherigen Rechtsprechung des Bundesverfassungsgerichts zum Schutz des Kernbereichs privater Lebensgestaltung ergibt sich nichts anderes.

In der jüngsten Entscheidung zum Bayerischen Verfassungsschutzgesetz hat sich der Senat mit der Ausnahme vom Abbruchserfordernis bei einer möglichen Gefährdung oder Enttarnung eingesetzter Personen nach Art. 8a Abs. 1 Satz 2 BayVSG nicht befasst. Die Regelung genügt bereits aus anderen Gründen nicht den verfassungsrechtlichen Anforderungen an den Kernbereichsschutz (vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, juris Rn. 305 f. und 315).

In seiner Entscheidung zur Online-Durchsuchung formuliert der Senat für den Kernbereichsschutz auf Erhebungsebene, die gesetzliche Regelung habe darauf hinzuwirken, dass die Erhebung kernbereichsrelevanter Daten „soweit wie informationstechnisch und ermittlungstechnisch möglich“ unterbleibt (BVerfGE 120, 274-350, juris Rn. 281). Aus dieser Formulierung könnte man schlussfolgern, der Senat akzeptiere Fälle, in denen eine bewusste Erhebung kernbereichsrelevanter Daten zulässig ist – z.B., wenn es aus ermittlungstechnischen Gründen erforderlich ist (so § 16 Abs. 2 Satz 1 Hs. 2 PolG NRW, wobei „ermittlungstechnische Gründe“ bei einer gegenwärtigen Gefahr für Leib und Leben verdeckt eingesetzter Personen vorliegen sollen, vgl. NRW LT-Drs. 14/10089, S. 28). Dies liefe auf eine Abwägung des Kernbereichsschutzes mit den staatlichen Ermittlungsinteressen hinaus.

Eine solche Abwägung lässt sich der Entscheidung zur Online-Durchsuchung jedoch nicht entnehmen. Das o.g. Zitat des Senats bezieht sich nur auf den heimlichen Zugriff auf informationstechnische Systeme (BVerfGE 120, 274, juris Rn. 278). Dieser erfolgt in der Regel automatisiert, was das „Herausfiltern“ von Daten mit Kernbereichsbezug im Vorfeld der Erhebung erschwert. Dies erkennt der Senat an. Dennoch ist auf Erhebungsebene darauf hinzuwirken, dass kernbereichsrelevante Daten „soweit wie informationstechnisch und ermittlungstechnisch möglich“ nicht erhoben werden. Insbesondere sind verfügbare informationstechnische Sicherungssysteme einzusetzen (BVerfGE 120, 274, juris Rn. 281). Der Senat befasst sich hier nicht mit dem Abbruch oder der Unterbrechung einer bereits begonnenen Datenerhebung, sondern mit dem Kernbereichsschutz im Vorfeld der Maßnahme. Mit seiner einschränkenden Formulierung „soweit [...] möglich“ trägt er dem Umstand Rechnung, dass es bei

Online-Durchsuchungen in der Regel technisch schwierig ist, die Kernbereichsrelevanz vor der Datenerhebung abzuschätzen.

Für den in § 26a Abs. 3 Satz 1 SOG M-V geregelten Fall, dass sich während der Datenerhebung konkrete Anhaltspunkte für eine Kernbereichsrelevanz ergeben, trifft der Senat keine Aussage. Insbesondere befasst er sich nicht mit dem Maßnahmenabbruch beim Einsatz von verdeckten Ermittlern oder Vertrauenspersonen. Es gibt keine Anhaltspunkte, dass der Senat in diesem Fall eine Abwägung zwischen Kernbereichsschutz und dem Schutz der eingesetzten Personen für verfassungsgemäß hält (so auch Sachs, Schriftliche Stellungnahme 14/3027 zum Entwurf zur Änderung des PolG NRW (14/10089), S.8). Im Gegenteil heißt es in der Entscheidung zum BKA-Gesetz ausdrücklich, „in jedem Fall“ sei der Abbruch der Maßnahme vorzusehen, wenn erkennbar wird, dass eine Überwachung in den Kernbereich privater Lebensgestaltung eindringt (BVerfGE 141, 220-378, juris Rn. 128).

Diese Anforderungen erfüllt § 26a Abs. 3 Satz 1 SOG M-V nicht.

cc) Dieses Ergebnis kann dazu führen, dass das Leben von verdeckt eingesetzten Personen riskiert werden muss, um den sofortigen Abbruch der Maßnahme und damit den umfassenden Schutz des Kernbereichs privater Lebensgestaltung des Betroffenen zu gewährleisten. Dies erscheint hart. Das Leben der unschuldigen, verdeckt eingesetzten Personen wird den meisten gewichtiger erscheinen als die Wahrung der menschlichen Würde des Beschuldigten. Eine solche Wertung ist dem Staat jedoch durch Art. 1 Abs. 1, Art. 79 Abs. 3 GG verwehrt (BVerfGE 109, 279-391, juris Rn. 125).

Allerdings ist zu bemerken, dass kaum praktische Anwendungsfälle denkbar sind, in denen der Abbruch einer verdeckten Ermittlung zum Schutz des Kernbereichs privater Lebensgestaltung mit einer Gefahr für das Leben der verdeckt eingesetzten Person verbunden ist. Denn zum einen ist die Verletzung des Kernbereichs privater Lebensgestaltung, d.h. eine Menschenwürdeverletzung nur in Ausnahmefällen anzunehmen. Nicht jede tatsächliche Erfassung von höchstpersönlichen Informationen begründet stets eine Menschenwürdeverletzung (BVerfG, Urteil vom 26. April 2022 –

1 BvR 1619/17 –, juris Rn. 277). Auch Tagebücher oder ähnliche private Aufzeichnungen sind nicht in jedem Fall dem Kernbereich privater Lebensgestaltung zuzuordnen (BVerfGE 80, 367, Rn. 20). Eine Menschenwürdeverletzung liegt nur vor, wenn mit der Datenerhebungsmaßnahme eine Missachtung des Wertes des Betroffenen als Mensch einhergeht und er zum Objekt der staatlichen Verbrechensbekämpfung gemacht wird (vgl. BVerfGE 109, 279, juris Rn. 120 ff.). Eine Verletzung der Menschenwürde wird z.B. bei der Beobachtung von Äußerungen innerster Gefühle gegenüber Vertrauenspersonen oder von Ausdrucksformen der Sexualität angenommen (BVerfGE 109, 279, juris Rn. 127).

§ 26a Abs. 3 SOG M-V definiert zudem nicht, wie der Maßnahmenabbruch zu erfolgen hat. Es ist nicht erforderlich, dass die verdeckt eingesetzte Person ihre wahre Identität offenlegt. Hier besteht ein gewisser Spielraum. Die Datenerhebung wird auch dann unterbrochen, wenn sich die verdeckt eingesetzte Person vom Betroffenen entfernt. Belauscht eine verdeckt eingesetzte Person ein Gespräch über innerste Gefühle oder beobachtet sie sexuelle Handlungen, kann sie sich abwenden und entfernen. Eine Lebensgefahr dürfte damit in aller Regel nicht verbunden sein.

3. Sichtung der Daten nach § 26a Abs. 5 Satz 1 SOG M-V

Die Beschwerdeführer rügen die in § 26a Abs. 5 Satz 1 SOG M-V geregelte Sichtung der Daten durch den behördlichen Datenschutzbeauftragten im Falle eines Maßnahmenabbruchs.

a) Wortlaut und Auslegung

Nach § 26a Abs. 5 Satz 1 SOG M-V sind vor einer Verwendung von Daten in Fällen einer Unterbrechung nach Absatz 3 – die nicht bereits von Absatz 4 erfasst werden – die erhobenen Daten dem behördlichen Datenschutzbeauftragten zur Auswertung und Entscheidung über die Rechtmäßigkeit dieser Datenerhebung vorzulegen. § 26a Abs. 5 Satz 1 SOG M-V knüpft an Absatz 4 an. Dieser betrifft die Verwendung von Daten in/aus

Wohn- und Geschäftsräumen und dem befriedeten Besitztum. Wegen der besonderen Kernbereichsrelevanz dieser Daten ist vor ihrer Verwendung die Rechtmäßigkeit der Erhebung von einem Richter oder einer Richterin festzustellen. Das schließt Unterbrechungsfälle nach § 26a Abs. 3 SOG M-V in Wohn- und Geschäftsräumen und dem befriedeten Besitztum mit ein (LT-Drs. 7/3694, S. 159). Für die Sichtung von Daten aus Online-Durchsuchungen enthält § 33c Abs. 9 SOG M-V einen speziellen Richtervorbehalt. Diese Regelung geht nach § 26a Abs. 5 Satz 1 SOG M-V vor (vgl. dazu ausführlich unter II.1).

§ 26a Abs. 5 Satz 1 SOG M-V betrifft folglich alle Fälle, in denen die Datenerhebung außerhalb von Wohn- und Geschäftsräumen oder dem befriedeten Besitztum stattgefunden hat und es sich nicht um eine Online-Durchsuchung handelt. Das sind im Wesentlichen die in § 33 Abs. 1 SOG M-V genannten besonderen Mittel der Datenerhebung: längerfristige Observation, verdeckter Einsatz technischer Mittel, insbesondere solcher zur Bild- und Tonaufnahme oder Bild- und Tonaufzeichnung sowie Einsatz von Vertrauenspersonen und verdeckten Ermittlern. Diese Maßnahmen finden regelmäßig außerhalb der Wohnung statt.

Für die Sichtung der Daten aus der Telekommunikationsüberwachung enthält § 33d Abs. 8 SOG M-V eine Sonderregelung. Danach ist ebenfalls der behördliche Datenschutzbeauftragte zuständig (vgl. dazu ausführlich unter III.1).

b) Maßstäbe des Bundesverfassungsgerichts

Das Bundesverfassungsgericht hat die verfassungsrechtlichen Anforderungen an den Kernbereichsschutz bei der Sichtung von erhobenen Daten für drei Fälle erörtert: die Wohnraumüberwachung, die Online-Durchsuchung und die Telekommunikationsüberwachung.

Besonders strenge Anforderungen an den Kernbereichsschutz auf der Auswertungs- und Verwertungsebene stellt das Bundesverfassungsgericht bei der Wohnraumüberwachung und der Online-Durchsuchung. Beide Maßnahmen dringen besonders tief in die Privatsphäre ein (BVerfGE 141, 220-378, Rn. 192).

Die Online-Durchsuchung trägt zudem typischerweise die Gefahr einer Erfassung auch höchstvertraulicher Daten in sich (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, juris Rn. 284). Für diese Maßnahmen verlangt das Bundesverfassungsgericht die Sichtung durch eine unabhängige Stelle.

Zur Telekommunikationsüberwachung hat das Bundesverfassungsgericht bislang noch keine abschließende Klärung vorgenommen, allerdings einen Verzicht auf einen Rekurs auf eine unabhängige Stelle dann für zulässig erachtet, wenn die Erfassung kernbereichsrelevanter Gespräche bereits auf Ebene der Erhebung vermieden wird (vgl. dazu ausführlich unter A.3.c) cc)).

c) Kein hinreichender Kernbereichsschutz bei der Datensichtung

Danach ist der Kernbereichsschutz bei der Sichtung von Daten im Sinne von § 26a Abs. 5 Satz 1 SOG M-V nicht hinreichend gesichert.

aa) § 26a Abs. 5 Satz 1 SOG M-V sieht die Sichtung der Daten bei einem Maßnahmenabbruch durch den behördlichen Datenschutzbeauftragten vor. Bei diesem handelt es sich nicht um eine unabhängige Stelle. Die unabhängige Sichtung dient sowohl der Rechtmäßigkeitskontrolle als auch dem Herausfiltern höchstvertraulicher Daten, sodass diese nach Möglichkeit der überwachenden Behörde gegenüber nicht offenbar werden (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, juris Rn. 282, 286; BVerfGE 141, 220-378, Rn. 200, 220, 224). Die Sichtung durch eine unabhängige Stelle setzt daher voraus, dass die Kontrolle im Wesentlichen von externen, nicht mit Sicherheitsaufgaben betrauten Personen wahrgenommen wird. Die Sichtung durch den behördeninternen Datenschutzbeauftragten genügt diesen Anforderungen nicht (so ausdrücklich BVerfGE 141, 220-378, Rn. 225).

bb) § 26a Abs. 5 Satz 1 SOG M-V betrifft vor allem längerfristige Observationen sowie den verdeckten Einsatz von Vertrauenspersonen, verdeckten Ermittlern und technischen Mitteln zur Bild-/Tonaufnahme bzw. -aufzeichnung, soweit die Maßnahmen außerhalb von Wohn- und Geschäftsräumen stattfinden. Diese Maßnahmen greifen nicht in gleicher Weise in die Privatsphäre des Betroffenen

ein wie die Wohnraumüberwachung oder die Online-Durchsuchung. Im Gegensatz zur Wohnraumüberwachung ist kein besonders privater Rückzugsraum betroffen, dem zur Wahrung der Menschenwürde besonderes Gewicht zukommt. Die Online-Durchsuchung erfasst Informationen aus dem informationstechnischen System des Betroffenen, die ggf. über lange Zeit angesammelt wurden. Das gesamte Nutzungsverhalten kann nach- und mitverfolgt werden, was sich angesichts des heute üblichen Nutzungsverhaltens zur Erfassung eines umfassenden Persönlichkeitsprofils verdichten kann. Damit sind längerfristige Observationen (auch durch Bild- und Tonaufnahmen) sowie der verdeckte Einsatz bestimmter Personen nicht ohne Weiteres mit Wohnraumüberwachung und Online-Durchsuchung vergleichbar. Diese Maßnahmen betreffen unmittelbar stattfindende Tätigkeiten und Handlungen außerhalb von Privaträumen, z.B. Bewegungen oder Gespräche auf offener Straße, in öffentlich zugänglichen Gebäuden sowie Restaurantbesuche oder Freizeitaktivitäten. Bei diesen Maßnahmen ist stets mit einer Beobachtung durch Dritte zu rechnen. Die Kernbereichsrelevanz dieser Maßnahmen besteht vor allem darin, dass auch der höchstpersönliche Austausch zwischen Vertrauenspersonen umfasst sein kann.

cc) Danach ist die Sichtung der Daten nach dem Abbruch einer Maßnahme im Sinne von § 33 Abs. 1 SOG M-V nicht in jedem Fall erforderlich. Es ist danach zu unterscheiden, ob die Erfassung kernbereichsrelevanter Gespräche bereits auf der Ebene der Datenerhebung ausgeschlossen wird. Nur wenn dies der Fall ist, bedarf es keiner Sichtung durch eine unabhängige Stelle.

§ 26a Abs. 5 Satz 1 SOG M-V betrifft den Fall, dass es zu einer Unterbrechung der Datenerhebung kam, weil sich während der Erhebung Anhaltspunkte ergeben, dass Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung erfasst werden (Abs. 3). Die Regelung setzt mithin voraus, dass die Erfassung kernbereichsrelevanter Daten nicht bereits auf Erhebungsebene ausgeschlossen wurde. Andernfalls wäre eine Unterbrechung nach § 26a Abs. 3 Satz 1 SOG M-V nicht erforderlich. Regelmäßig lässt sich auch nicht im Vorfeld der Maßnahme klären, ob es zur Erfassung eines Gesprächs zwischen zwei Personen des höchstpersönlichen Vertrauens kommt. Die in § 33 Abs. 1 SOG M-V genannten

besonderen Mittel der Datenerhebung sind gerade darauf ausgerichtet, den Betroffenen über einen längeren Zeitraum zu beobachten. Welche Gespräche er in dieser Zeit führt, ist in der Regel nicht bzw. nicht sicher vorhersehbar.

Daraus folgt, dass bei einem Maßnahmenabbruch wegen Kernbereichsrelevanz im Sinne von § 26a Abs. 3 Satz 1 SOG M-V die Rechtmäßigkeit der Datenerhebung von einer unabhängigen Stelle zu prüfen ist. Diesen Anforderungen genügt § 26a Abs. 5 Satz 1 SOG M-V nicht (vgl. BVerfGE 141, 220-378, Rn. 245 zur Verfassungsmäßigkeit von § 20I Abs. 6 BKAG a.F. wegen der vorgelagerten Sichtung durch ein Gericht).

B. Besonderer Teil

I. Wohnraumüberwachung, § 33 b Abs. 1 Satz 2 SOG

Nach § 33 b Abs. 1 Satz 2 SOG M-V kann die Polizei durch den verdeckten Einsatz technischer Mittel in oder aus der Wohnung einer Person deren nicht öffentlich gesprochenes Wort abhören und aufzeichnen sowie von ihr Lichtbilder und Bildaufzeichnungen herstellen, wenn die Voraussetzungen des § 67a Abs. 1 SOG M-V vorliegen, die Maßnahmen gegen die dort genannten Personen gerichtet sind und die Abwehr der dort bezeichneten Gefahr ansonsten unmöglich oder wesentlich erschwert wäre.

Anders als nach § 33b Abs. 1 Satz 1 SOG M-V ist der Einsatz technischer Mittel zur Wohnraumüberwachung damit nicht an die Voraussetzungen der Abwehr einer gegenwärtigen Gefahr geknüpft.

Die Eingriffsschwelle für eine Wohnüberwachung ergibt sich aus Art. 13 Abs. 4 GG. Der in der Wohnraumüberwachung liegende besonders tief in die Privatsphäre eindringende Eingriff ist demnach nur zur Abwehr einer dringenden Gefahr zulässig, an deren Vorliegen strenge Anforderungen zu stellen sind und die über eine konkrete Gefahr noch hinausgehen. Dies gilt insbesondere für die Wahrscheinlichkeit eines Schadens (vgl. BVerfG, Urteil vom 26. April 2022 – 1 BVR 1619/17 –, Rn. 177).

Die Befugnis der Wohnraumüberwachung nach § 33b Abs. 1 Satz 2 i.V.m. § 67a Abs. 1 SOG M-V knüpft indessen gerade nicht wie § 33b Abs. 1 Satz 1 SOG M-V an eine konkrete Gefahr an, sondern lässt die Wohnraumüberwachung bereits im Vorfeld einer solchen konkreten Gefahr zu. Denn die Voraussetzungen des § 67a Abs. 1 SOG M-V beschreiben Umstände im Vorfeld einer konkreten Gefahr, bei denen der Eintritt eines Schadens nicht in gleicher Weise wahrscheinlich ist wie bei einer konkreten Gefahr.

Im Unterschied zur Bestimmung des § 20h BKAG ist also nach § 33b Abs. 1 Satz 2 SOG M-V weder eine dringende Gefahr noch eine konkrete Gefahr für diese Eingriffe in das Grundrecht aus Art. 13 GG erforderlich. § 33b Abs. 1 Satz 2 SOG gestattet Maßnahmen der Wohnraumüberwachung im Vorfeld einer konkreten Gefahr, statt wie es Art. 13 Abs. 4 GG verlangt, über die konkrete Gefahr hinausgehende Anforderungen an die Zulässigkeit von Maßnahmen der Wohnraumüberwachung zu knüpfen.

Die gesetzlichen Eingriffsvoraussetzungen werden daher dem grundrechtlichen Maßstab des Art. 13 Abs. 4 GG für Eingriffe in das Grundrecht aus Art. 13 Abs. 1 GG nicht gerecht.

Die Verfassungsbeschwerde ist insoweit begründet.

II. Online-Durchsuchung

1. Regelung des § 33c Abs. 1 S. 2 SOG M-V (Terroristische Straftaten)

Die Beschwerdeführer rügen ein Verstoß gegen das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme (S. 43 ff.). Die Ausweitung des Anwendungsbereichs der sog. Online-Durchsuchung auf die in § 67a Abs. 1 SOG M-V genannten terroristischen Taten sei unverhältnismäßig.

a) Wortlaut und Auslegung

Der Verweis von § 33c Abs. 1 S. 2 SOG M-V auf § 67a Abs. 1 SOG M-V ist so zu verstehen, dass entweder die Voraussetzungen des § 67a Abs. 1 Nr. 1 SOG M-V oder des § 67a Abs. 1 Nr. 2 SOG M-V vorliegen müssen. Die weiteren Tatbestandsmerkmale des § 67a Abs. 1 SOG M-V dürften hier unbeachtlich sein, da diese ausschließlich die Ausgestaltung der elektronischen Aufenthaltsüberwachung betreffen. Sowohl § 67a Abs. 1 Nr. 1 SOG M-V als auch § 67a Abs. 1 Nr. 2 SOG M-V nehmen Bezug auf die Legaldefinition der terroristischen Straftat nach § 67c SOG M-V.

Der dortige Katalog orientiert sich am Straftatenkatalog des § 129a Abs. 1, 2 StGB. Der Landesgesetzgeber hat insoweit, anders als der Bundesgesetzgeber, der die Verhütung von Straftaten i.S.d. § 129a Abs. 1, 2 StGB nur im Rahmen der Telekommunikationsüberwachung als zulässig erachtet (vgl. § 51 Abs. 1 S. 1 Nr. 2, 3 i.V.m. § 5 Abs. 1 S. 2 BKAG n.F.), auch für die Online-Durchsuchung die Verhütung von Straftaten im größeren Umfang als zulässigen Zweck erachtet.

Darüber hinaus hat der Landesgesetzgeber u.a. auch Straftaten nach §§ 224, 227 StGB – unter den in § 67c SOG M-V genannten Bedingungen – als erfasst angesehen, die nicht in § 129a StGB gelistet sind und daher keine terroristischen Straftaten i.S.d. BKAG darstellen.

b) Verfassungsrechtliche Vorgaben

Der 1. Senat hat klargestellt, dass für die Online-Durchsuchung mindestens eine konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut erforderlich ist (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 310). Dies ergebe sich zwar nicht unmittelbar aus dem Wortlaut des Grundgesetzes, sei aber verfassungsrechtlich geboten (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 311). An anderer Stelle heißt es, es müsse eine konkrete Gefahr für ein „überragend wichtiges Rechtsgut“ vorliegen (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 212; BVerfG, Urteil vom 27.

Februar 2008 – 1 BvR 370/07, 1 BvR 595/07 –, Rn. 247 f.). Der 1. Senat führt dazu aus (Hervorhebung nicht im Original):

*„Ein derartiger Eingriff darf nur vorgesehen werden, wenn die Eingriffsermächtigung ihn davon abhängig macht, dass tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen. Überragend wichtig sind zunächst **Leib, Leben und Freiheit der Person**. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu zählt etwa auch die **Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen**.*

Zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine existentielle Bedrohungslage nicht besteht, ist eine staatliche Maßnahme grundsätzlich nicht angemessen, durch die – wie hier – die Persönlichkeit des Betroffenen einer weitgehenden Ausspähung durch die Ermittlungsbehörde preisgegeben wird. Zum Schutz solcher Rechtsgüter hat sich der Staat auf andere Ermittlungsbefugnisse zu beschränken, die ihm das jeweils anwendbare Fachrecht im präventiven Bereich einräumt.“

Ein allgemeiner Sachwertschutz wird nicht für ausreichend erachtet (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 108). Das Bundesverfassungsgericht hat ferner festgestellt, dass § 3 G 10-Gesetz a.F. nicht ausreichend gewesen sei, weil der dortige Straftatenkatalog kein Konzept zum Schutz überragend wichtiger Rechtsgüter erkennen lasse (BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07 –, Rn. 266).

Dies gilt erst recht für den Katalog des § 67c SOG M-V. Die dort genannten Straftatbestände können, auch unter Berücksichtigung der an § 129a StGB angelehnten Anforderungen an die Bestimmung und Eignung, nicht sämtlich als Tatbestände zum Schutz überragend wichtiger Rechtsgüter verstanden werden. Dies gilt erst recht angesichts der gesetzgeberischen Intention, den

Handlungsspielraum der Behörde über § 33c Abs. 1 S. 1 SOG M-V hinaus zu erweitern. Der Landesgesetzgeber geht offensichtlich davon aus, dass die Verhinderung von Straftaten mittels Online-Durchsuchung auch dann zulässig sein soll, wenn keine Gefahr für die in Satz 1 Nr. 1, 2 genannten Rechtsgüter vorliegt. Diese Entscheidung erfolgte offenbar bewusst, da der Landesgesetzgeber insoweit vom Regelungskonzept des BKAG abweicht, an das er sich jedoch an anderer Stelle angelehnt hat (LT-Drs. 7/3694, S. 182, 178).

Soweit die Beschwerdeführer rügen, dass der Anwendungsbereich der sog. Online-Durchsuchung in unverhältnismäßiger Weise ausgeweitet wird, ist die Verfassungsbeschwerde begründet.

Unklar ist zudem, ob der Zweck der Maßnahme ausreichend bestimmt ist. So fordert die bundesverfassungsgerichtliche Rechtsprechung bei der Online-Durchsuchung nicht nur die Gefahr für ein überragend wichtiges Rechtsgut, sondern auch eine Begrenzung auf ein Tätigwerden zur Abwehr der Gefahr (vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 311). § 33c Abs. 1 SOG M-V enthält, anders als § 33b Abs. 1 SOG M-V, keinen ausdrücklichen Hinweis auf ein Tätigwerden „zur Abwehr der Gefahr“. Insoweit dürfte allerdings eine verfassungskonforme Auslegung i.V.m. § 33c Abs. 2 S. 1 SOG M-V dergestalt möglich sein, dass die Online-Durchsuchung auch zum Zwecke der Abwehr der festgestellten Gefahr dienen soll.

2. Regelung des § 33c Abs. 1 S. 4 SOG M-V (Nicht-Verantwortliche)

Die Beschwerdeführer rügen zudem die Verfassungswidrigkeit des § 33c Abs. 1 S. 4 SOG M-V. Dieser verstoße gegen das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme, weil hinsichtlich dritter Personen keine Subsidiarität der Maßnahme vorgeschrieben sei (S. 45).

a) Wortlaut und Auslegung

Zutreffend weisen die Beschwerdeführer darauf hin, dass § 33c Abs. 1 S. 4 SOG M-V keine explizite Regelung enthält, die eine Subsidiarität der Maßnahme zu

Lasten eines Nicht-Verantwortlichen gegenüber einer Maßnahme gegen den Verantwortlichen normiert. Allerdings enthält § 33c Abs. 2 S. 1 SOG M-V eine allgemeine Subsidiaritätsklausel, während diese in § 33b Abs. 1 S. 1 und S. 2 SOG M-V jeweils maßnahmenspezifisch geregelt ist. Die allgemeine Subsidiaritätsvorschrift des § 33c Abs. 2 S. 1 SOG M-V findet daher auch auf Maßnahmen zu Lasten von Nicht-Verantwortlichen Anwendung.

b) Verfassungsrechtliche Anforderungen

Das Bundesverfassungsgericht fordert, dass ein Zugriff auf das informationstechnische System eines Dritten nur dann erfolgt, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Zielperson dort ermittlungsrelevante Informationen speichert **und** ein auf ihre eigenen informationstechnischen Systeme beschränkter Zugriff zur Erreichung des Ermittlungsziels nicht ausreicht (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 115). Eine solche Regelung ist in § 33c SOG M-V nicht enthalten. Unklar ist insoweit, ob aufgrund der Erfordernisse der Normbestimmtheit bei der Online-Durchsuchung (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 123) von der Verfassungswidrigkeit des § 33c Abs. 1 S. 4 SOG M-V auszugehen ist oder ob, aufgrund der Unklarheit der Gesetzesbegründung (LT-Drs. 7/3694, S. 180), eine verfassungskonforme Auslegung dergestalt stattfinden kann, dass § 33c Abs. 2 S. 1 SOG M-V so ausgelegt werden muss, dass stets ein Vorrang einer Maßnahme nach § 33c Abs. 1 S. 1 oder S. 2 SOG M-V zu prüfen ist.

3. Regelung des § 33c Abs. 5 SOG M-V (Eingriff in Art. 13 Abs. 1 GG)

§ 33c Abs. 5 SOG M-V sieht ein Recht zum „verdeckten“ Betreten und Durchsuchen von Räumlichkeiten der betroffenen Person vor. Die Beschwerdeführer rügen einen Verstoß gegen Art. 13 GG (S. 46 ff.).

a) Wortlaut und Auslegung

Die Vorschrift des § 33c Abs. 6 SOG M-V sieht einen Richtervorbehalt vor. Inhaltlich enthält § 33c Abs. 5 SOG M-V keine detaillierten Voraussetzungen für

den Erlass einer Betretens- oder Durchsuchungsanordnung. Der Gesetzgeber lässt insoweit die Erforderlichkeit zur Durchführung einer Maßnahme nach § 33c Abs. 1 oder 4 SOG M-V genügen. Implizit setzen ein Betreten und Durchsuchen daher voraus, dass die gesetzlichen Anforderungen nach Abs. 1 oder Abs. 4 im Zeitpunkt der Anordnung i.S.d. § 33c Abs. 5, 6 SOG M-V erfüllt sind. Das Betreten und Durchsuchen einer Räumlichkeit kann nicht erforderlich sein, wenn die Maßnahme selbst bereits unzulässig ist. Aus dem Tatbestandsmerkmal der Erforderlichkeit folgt ebenfalls, dass ein Durchsuchen nur mit dem Ziel erfolgen darf, das informationstechnische System, welches mittels Online-Durchsuchung überwacht werden soll, aufzuspüren.

b) Verfassungsrechtliche Vorgaben

Soweit ersichtlich, hat sich das Bundesverfassungsgericht noch nicht ausdrücklich zu der Frage verhalten, ob „heimliche“ Durchsuchungen mit Art. 13 GG in Einklang zu bringen sind.

In der Kommentarliteratur finden sich zahlreiche Stimmen, die darauf hinweisen, dass eine Rechtfertigung des Eingriffs nach **Art. 13 Abs. 2 GG** nicht in Betracht komme, da das insoweit ins Auge gefasste Leitbild der „Durchsuchung“ nur offene Ermittlungsmaßnahmen erfasse (vgl. BK-GG/Herdegen, 71. Lfg. [Oktober 1993], Art. 13 Rn. 52; Wolff, in: Hömig/ders. (Hrsg.), GG, 13. Aufl. 2022, Art. 13 Rn. 9; Gornig, in: v. Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 13 Rn. 65; Roggan, Stellungnahme vom 14. August 2019, S. 25 f., abrufbar unter: <https://sogenannte-sicherheit.org/wp-content/uploads/2019/08/SOG-Stellungnahme-Roggan.pdf>). Dem ist, soweit ersichtlich, in Rechtsprechung und Literatur nicht widersprochen worden. Dass der verfassungsrechtliche Durchsuchungsbegriff keine heimlichen Maßnahmen zulässt, dürfte sich zudem aus der Binnensystematik des Art. 13 GG ergeben. Dort sind für aufgrund ihrer Heimlichkeit besonders grundrechtsintensive Eingriffe in Art. 13 Abs. 3-5 GG qualifizierte Gesetzgebungsvorbehalte (Begrenzung auf besonders schwere Straftaten und Entscheidung eines Spruchkörpers in Art. 13 Abs. 3 GG; Abwehr dringender Gefahren in Art. 13 Abs. 4 GG) vorgesehen. Derartige qualifizierte Gesetzesvorbehalte sind in Art. 13

Abs. 2 GG nicht enthalten, was für einen restriktiven Anwendungsbereich sprechen dürfte.

Angesichts des vom Bundesverfassungsgericht an anderer Stelle betonten weitgehenden Gleichlaufs von akustischer Wohnraumüberwachung und Online-Durchsuchung (vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 311; BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 192) dürfte ein Eingriff in Art. 13 Abs. 1 GG zum Zwecke der Vorbereitung einer Online-Durchsuchung daher, wenn überhaupt, nur unter den in Art. 13 Abs. 4 GG normierten Bedingungen als verfassungsrechtlich zulässig zu erachten sein.

§ 33c SOG M-V sieht allerdings keine Beschränkung auf dringende Gefahren vor. Bereits deshalb ist die Verfassungsbeschwerde insoweit begründet. Im Übrigen ist zweifelhaft, ob Art. 13 GG überhaupt „heimliche“ Durchsuchungen zulässt (vgl. Roggan aaO).

4. Kernbereichsschutz des § 33c Abs. 9-10 SOG M-V

Die Beschwerdeführer rügen einen unzureichenden Kernbereichsschutz im Regelungskonzept des SOG M-V (S. 35 ff.), vgl. dazu allgemein die Ausführungen oben unter A. II. Dabei findet auch die Regelung zum Kernbereichsschutz bei Online-Durchsuchungen Erwähnung. Hierbei wird auf das vom Bundesverfassungsgericht aufgestellte Postulat der Notwendigkeit einer Sichtung durch unabhängige Stellen als elementarer Bestandteil des Grundrechtsschutzes rekurriert.

a) Wortlaut und Auslegung

Der Kernbereichsschutz wird im SOG M-V sowohl allgemein in § 26a SOG M-V als auch konkret für die Online-Durchsuchung in § 33c Abs. 9-10 SOG M-V geregelt. Das Gesetz äußert sich nicht ausdrücklich zum Verhältnis beider Vorschriften. Die Gesetzesbegründung geht allerdings offenbar davon aus, dass

die Datenverwendung insoweit ausschließlich nach § 33c Abs. 9-10 SOG M-V erfolgt (LT-Drs. 7/3694, S. 159).

Dort ist zunächst ausdrücklich geregelt, dass im Regelfall das anordnende Gericht über die Rechtmäßigkeit der Datenverarbeitung zu entscheiden hat (§ 33c Abs. 9 S. 1 2. HS SOG M-V). Aus der Ausnahmeregelung des § 33c Abs. 10 S. 1 SOG M-V folgt, dass mit Datenverarbeitung auch die Verwendung gemeint sein dürfte. Aus § 33c Abs. 10 S. 2 SOG M-V dürfte wiederum folgen, dass darunter auch die Sichtung fällt. Der Gesetzesbegründung ist zu entnehmen, dass sich die Regelung an § 46 Abs. 7 BKAG orientiert (LT-Drs. 7/3694, S. 182, 178) und gerade dem Schutz des Kernbereichs dienen soll. Damit soll die gerichtliche Auswertung der mittels Online-Durchsuchung erhobenen Daten im Hinblick auf kernbereichsrelevante Daten die Regel sein.

Eine Ausnahme für Gefahr im Verzug ist in § 33c Abs. 10 S. 1 SOG M-V geregelt. Diese Regelung befugt die Behördenleitung zur Auswertung. Diese kann die Aufgabe nach § 33c Abs. 10 S. 2 SOG M-V an zwei Bedienstete delegieren. Diese Bediensteten sind nach § 33c Abs. 10 S. 3 SOG M-V zur Verschwiegenheit verpflichtet.

b) Verfassungsrechtliche Vorgaben

Das Bundesverfassungsgericht hat bereits in der Vergangenheit festgestellt, dass bei der Sichtung der erfassten Daten einer Online-Durchsuchung eine unabhängige Stelle einzubinden ist (vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 286). Dies schließt nach der Rechtsprechung des Bundesverfassungsgerichts die „Hinzuziehung“ von Bediensteten, sofern diese zur Verschwiegenheit verpflichtet sind, nicht aus (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 315; BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 224). Der 1. Senat hat allerdings klargestellt, dass die tatsächliche Durchführung und Entscheidungsverantwortung in den Händen einer gegenüber der Behörde [BKA] unabhängigen Person liegen muss (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 224). Auch eine etwaige bloße „Sachleitung“ des Gerichts ist unzureichend (BVerfG, Urteil vom

20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 225). Der 1. Senat hat allerdings anerkannt, dass der Gesetzgeber die Möglichkeit hat, die notwendigen Regelungen zu treffen, um den Ermittlungsbehörden für Ausnahmefälle bei Gefahr im Verzug auch kurzfristig erste Handlungsmöglichkeiten einzuräumen (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 129). Der Senat hat insoweit offengelassen, welche Regelungen mit dem Erfordernis eines effektiven Kernbereichsschutzes vereinbar sind. Der Senat hat allerdings auf die besondere Bedeutung der Normenklarheit hingewiesen (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 123).

Es bestehen insoweit gewichtige Zweifel daran, dass die Ausgestaltung in § 33c Abs. 10 SOG M-V verfassungskonform ist. So lässt die Vorschrift vollständig offen, für welche Rechtsgüter eine Gefahr bestehen muss. Insbesondere wird nicht klargestellt, dass auch eine Gefahr für die nach Absatz 1 geschützten Rechtsgüter notwendig ist.

Darüber hinaus ist der reine Verweis auf eine „Gefahr im Verzug“ zu unbestimmt, da bereits die Durchführung einer Online-Durchsuchung das Vorliegen einer **Gefahr** für Rechtsgüter verlangt. Der Begriff der Gefahr im Verzug wird auch nicht im SOG M-V legaldefiniert (vgl. § 3 Abs. 3 SOG M-V). Wenn aber der gesetzliche Regelfall bereits eine Gefahr für die in Rede stehenden Rechtsgüter verlangt, ist der Gesetzgeber verfassungsrechtlich gehalten, den Ausnahmefall unter Rückgriff auf normenklare Begriffe zu definieren. Ansonsten bestünde im Hinblick auf die Bedeutung des Kernbereichsschutzes die nicht hinnehmbare Gefahr, dass sich die Annahme von Gefahr im Verzug zum Regelfall verkehrt. Unverhältnismäßig ist zudem, dass der Gesetzgeber in § 33c Abs. 10 S. 1 SOG M-V nicht nur die – ggfs. zeitaufwendige – Sichtung der Daten in die Hände der eigentlich von der unabhängigen Stelle zu kontrollierenden Exekutive legt, sondern dieser sogar das Recht einräumt, die Entscheidung, ob Gefahr im Verzug vorliegt, zu treffen. Für eine derartige Verlagerung der Entscheidungsbefugnis ist indes angesichts des Gewichts eines (möglichen) Eingriffs in den Kernbereich mangels Erforderlichkeit regelmäßig kein Raum. Das Bundesverfassungsgericht hat wiederholt festgestellt, dass zur verfahrensrechtlichen Absicherung besonders eingriffsintensiver Maßnahmen ein

richterlicher Eildienst zu schaffen sein kann (BVerfG, Beschluss vom 12. März 2019 – 2 BvR 675/14 –). Diese Wertungen sind übertragbar.

Im Interesse der Vermeidung von (regelhaften) Ausnahmekonstellationen dürfte zudem geboten sein, dass die in § 33c Abs. 9 S. 1 SOG M-V normierte **Unterrichtungspflicht** konkretisiert wird, damit nicht erst nach einer mehrmonatigen Überwachung (vgl. § 33c Abs. 8 SOG M-V) eine Einbindung des Gerichts erfolgt und so eine Eilbedürftigkeit entsteht, wenn die Sichtungskapazitäten des Gerichts unzureichend sind.

III. Quellen-TKÜ

1. Regelung des § 33d Abs. 1 S.1 Nr. 2-4 SOG M-V (Verweis auf § 67a Abs. 1 SOG M-V)

Die Beschwerdeführer rügen, dass der Verweis in § 33d Abs. 1 S. 1 Nr. 2-4 SOG M-V auf § 67a Abs. 2 SOG M-V mit dem Bestimmtheitsgrundsatz und dem Verhältnismäßigkeitsgrundsatz nicht in Einklang zu bringen sei (S. 58 f.).

a) Wortlaut und Auslegung

§ 33d Abs. 1 S. 1 Nr. 2-4 SOG M-V verweisen auf § 67a Abs. 1 SOG M-V, der wiederum auf § 67c SOG M-V rekurriert. Die Natur der Taten wird dabei in § 67c SOG M-V benannt, die Umschreibung der einer konkreten Gefahr vorgelagerten Fallkonstellationen ist in § 67a Abs. 1 SOG M-V erfasst.

b) Verfassungsrechtliche Anforderungen

Die verfassungsrechtlichen Anforderungen an eine Anknüpfung an Verhaltensweisen, die noch nicht die Schwelle zur konkreten Gefahr erreichen, hat der 1. Senat in der BKA-Entscheidung präzisiert (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 165, 232). Soweit ersichtlich orientiert sich die Formulierung des § 67a Abs. 1 SOG M-V an den dortigen

Ausführungen in Rn. 165. Dies dürfte verfassungsrechtlich nicht zu beanstanden sein.

Die Regelung des § 33d Abs. 1 S. 1 Nr. 2-4 SOG M-V ist allerdings dennoch verfassungswidrig. So enthalten diese Eingriffsgrundlagen, anders als § 33d Abs. 1 S. 1 Nr. 1 SOG M-V, keine Vorgabe, dass das Handeln der Behörde zum Zwecke der Abwehr einer Gefahr i.S.d. § 33d Abs. 1 S. 1 Nr. 1, 2 SOG M-V erfolgen muss. Anders als § 33c Abs. 2 S. 1 SOG M-V (und u.a. § 51 Abs. 1 BKAG) verlangt § 33d Abs. 1 S. 2 SOG M-V ausschließlich, dass die Maßnahmen nur durchgeführt werden, wenn die „**Erfüllung der polizeilichen Aufgabe**“ auf andere Weise aussichtslos oder wesentlich erschwert wäre. Damit ist eine (verfassungskonforme) Auslegung der Vorschrift des § 33d Abs. 1 S. 1 Nr. 2-4 SOG M-V dergestalt, dass eine Beschränkung auf Maßnahmen zur Abwehr der konkret genannten Gefahr zu erfolgen hat, nicht möglich.

Der 1. Senat des Bundesverfassungsgerichts hat zur Online-Durchsuchung klargestellt, dass eine Begrenzung auf ein Tätigwerden zur Abwehr der Gefahr erforderlich ist (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 311). Dies wird damit begründet, dass ansonsten die besondere Eingriffsschwelle einer Gefahr im polizeilichen Sinne ihre verfassungsrechtlich gebotene Begrenzungsfunktion verlöre. Auch wenn die für die Online- Durchsuchung entwickelten Maßstäbe nicht stets eins zu eins auf die (Quellen-)Telekommunikationsüberwachung übertragbar sind, so sind für die heimliche und eingriffsintensive Maßnahme der Telekommunikationsüberwachung ebenfalls verfassungsrechtliche Grenzen hinsichtlich der zu schützenden Rechtsgüter und des Grades der Konkretisierung der Gefährdungssituation zu ziehen (vgl. BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94 u.a. –). Auch hier erfordert das Bestimmtheitsgebot eine klare Definition des Zwecks (vgl. zur Strafverfolgung BVerfG, Beschluss vom 12. Oktober 2011, 2 BvR 236/08 u.a. –, Rn. 205). Da dies unterblieben ist, sind die Regelungen verfassungswidrig.

2. § 33d Abs. 3 SOG M-V (Quellen-TKÜ)

Die Beschwerdeführer rügen, dass § 33d Abs. 3 S. 2 SOG M-V einen verfassungsrechtlich unzulässigen Zugriff auf gespeicherte Daten erlaube und die Quellen-TKÜ so zur „kleinen Online-Durchsuchung“ werde (S. 59 ff.). Zutreffend weisen sie darauf hin, dass anders als bei der strafprozessualen Quellen-TKÜ keine explizite Beschränkung auf Kommunikationsinhalte ab Anordnungszeitpunkt aufgenommen worden sei. Insoweit dürfte allerdings eine verfassungskonforme Auslegung möglich sein.

Verfassungsrechtlich bedenklich ist allerdings, dass § 33d SOG M-V keine eigenständige Regelung zur Ausgestaltung der eingesetzten Mittel enthält (vgl. auch Roggan, aaO, S. 29 f.). So stellt der Verweis in § 33d Abs. 3 S. 3 SOG M-V auf § 33c Abs. 3 SOG M-V anders als § 100a Abs. 5 S. 1 StPO nicht sicher, dass die eingesetzte Technik eine Beschränkung auf die zulässigerweise nach § 33d Abs. 3 S. 1, 2 SOG M-V zu erhebenden Daten gewährleistet. Dies ist verfassungsrechtlich problematisch, da der Gesetzgeber nicht ausreichend sicherstellt, dass den mit der Überwachung betrauten Mitarbeiterinnen und Mitarbeitern nur Kommunikationsdaten zur Kenntnis gelangen (vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 234).

3. § 33d Abs. 3 i.V.m. § 33c Abs. 5 SOG M-V (Eingriff in Art. 13 Abs. 1 GG)

Die Beschwerdeführer rügen auch insoweit einen Verstoß gegen Art. 13 GG (S. 61). Es wird auf die obigen Ausführungen verwiesen (vgl. unter B. I).

4. Kernbereichsschutz bei § 33d SOG M-V

Die Beschwerdeführer rügen einen unzureichenden Kernbereichsschutz im Regelungskonzept des SOG M-V (S. 35 ff.), vgl. dazu allgemein die Ausführungen oben unter A. II. Dabei findet, wenn auch am Rande, die Thematik des Kernbereichsschutzes bei der Telekommunikationsüberwachung Erwähnung. Insoweit bestehen Zweifel an der Verfassungskonformität der Vorschrift des § 33d Abs. 8 SOG M-V.

a) Wortlaut und Auslegung

Der Schutz des Kernbereichs bei der Auswertung von Daten aus einer Telekommunikationsüberwachung wird in § 33d Abs. 8 SOG M-V geregelt. Zudem enthält § 26a Abs. 5 SOG M-V allgemeine Vorgaben. Das Verhältnis der Vorschriften zueinander wird im Gesetz nicht klargestellt. Nach der Gesetzesbegründung sollen beide Vorschriften nebeneinander Anwendung finden (LT-Drs. 7/3694, S. 187). An anderer Stelle wird indes ein Vorrang des § 33d Abs. 8 SOG M-V suggeriert (LT-Drs. 7/3694, S. 159). Eine kumulative Anwendung der Vorschriften dürfte im Ergebnis jedoch der Intention des Gesetzgebers entsprechen. Dementsprechend erfolgt im Grundsatz eine Prüfung durch den behördlichen Datenschutzbeauftragten in folgenden Fallkonstellationen:

- Automatische Aufzeichnung ohne zeitgleiche Prüfung, § 33d Abs. 8 S. 1 SOG M-V.
- Automatische Aufzeichnung mit zeitgleicher Prüfung, wenn sich Tatsachen ergeben, die die Annahme rechtfertigen, dass Erkenntnisse aus dem Kernbereich erfasst werden, § 33d Abs. 9 S. 2 SOG M-V.
- Unterbrechung der Datenerhebung, § 26a Abs. 5 SOG M-V.

Eine Einbindung des behördlichen Datenschutzbeauftragten ist mithin nicht vorgesehen, wenn bei einer vom Polizeibeamten begleiteten Maßnahme (aus Sicht der eingesetzten Beamten) keine Tatsachen festgestellt werden, die eine Einbindung des Datenschutzbeauftragten rechtfertigen.

Bei Gefahr in Verzug sieht das Gesetz die Möglichkeit einer Handlung durch die Behördenleitung oder einen Beamten, der allerdings anders als bei § 33c Abs. 10 nicht zur Verschwiegenheit verpflichtet sein muss, vor (§ 33d Abs. 8 S. 3 SOG M-V).

b) Verfassungsrechtliche Anforderungen

Für den Fall, dass das Bundesverfassungsgericht eine Sichtung durch eine unabhängige Stelle für notwendig erachtet, hat es klargestellt, dass dies eine Vorlage sämtlicher Daten erfordert und nicht nur die Vorlage in Zweifelsfällen (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 306, 315). Zudem hat das Bundesverfassungsgericht klargestellt, dass der behördliche Datenschutzbeauftragte keine unabhängige Stelle darstellt (vgl. dazu bereits A. II. 3.c) aa)). Wäre eine solche Vorlagepflicht gegeben, würden die Regelungen der §§ 33d Abs. 8, 26a Abs. 5 SOG M-V nicht mit dem Grundgesetz im Einklang stehen.

In der Entscheidung zum BKA-Gesetz vom 20. April 2016 hat der 1. Senat des Bundesverfassungsgerichts klargestellt, dass jenseits der Online-Durchsuchung bei der Telekommunikationsüberwachung keine kategorische Pflicht zur Prüfung durch eine unabhängige Stelle bestehe (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 240; vgl. bereits BVerfG, Beschluss vom 12. Oktober 2011 – 2 BvR 236/08 u.a. –, Rn. 224). Allerdings hat der 1. Senat offenbar vor allem die Überwachung einzelner Akte unmittelbarer (mündlicher) Kommunikation (mit Vertrauenspersonen) im Blick gehabt (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 238, 241). Insoweit hat der 1. Senat eine Möglichkeit gesehen, dass bereits auf der Erhebungsstufe eine Prüfung erfolgt, die die Erfassung höchstprivater **Gespräche** verhindert (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 239). Zudem hat der 1. Senat eindeutig Folgendes erklärt:

„Erlaubt der Gesetzgeber in dieser Weise auch die Erhebung von Informationen, für die Zweifel bestehen können, ob sie dem Kernbereich privater Lebensgestaltung unterfallen, bedarf es für solche Aufzeichnungen dann aber auch der Sichtung durch eine unabhängige Stelle.“

(BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 241).

Seit dem Urteil des 1. Senats aus April 2016 haben sich die Rahmenbedingungen signifikant verändert. So hat u.a. die 3. Kammer des 2. Senats des Bundesverfassungsgerichts im Juli 2016 die fachgerichtliche Entscheidung des LG Ellwangen, dass vom Telekommunikationsbegriff des § 100a StPO auch das Surfen im Internet bzw. das Verwenden einer Suchmaschine („Googlen“) erfasst sei, als verfassungsrechtlich vertretbar eingestuft (BVerfG, Beschluss vom 6. Juli 2016 – 2 BvR 1454/13 –). In Anwendung dieser Rechtsprechung kann eine Telekommunikationsüberwachung neben dem klassischen Telefonat, dem Mitlesen von E-Mails und privaten Chats auch eine vollständige Überwachung der privaten oder gar intimen Internetnutzung erfassen. Die moderne Telekommunikationsüberwachung dient nur zum Teil der Überwachung (mündlichen) Kommunikationsverhaltens, sondern wird in der Praxis regelmäßig auch zur Überwachung des Datenstroms von Mobiltelefonen und Computern eingesetzt. Damit erfasst die Telekommunikationsüberwachung im Wesentlichen gerade die besonders sensiblen Verhaltensweisen, die der 1. Senat noch im April 2016 als für die Online-Durchsuchung typusprägend eingestuft hat („Nach- oder Mitverfolgen der Bewegungen im Internet, Erschließen von geheim gehaltenen Schwächen und Neigungen; vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 238.). Hinzu kommt, dass bei der Überwachung derartiger Datenströme ein effektiver Kernbereichsschutz auf Ebene der Erhebung regelmäßig ausgeschlossen ist.

Die Überwachung des Surfverhaltens des modernen Internetnutzers kann tiefgehende Einblicke in den (psychischen) Gesundheitszustand, die politischen und sexuellen Vorlieben und die berufliche Tätigkeit ermöglichen. Eine kürzlich von der ARD ausgestrahlte Dokumentation (Made to Measure: Eine digitale Spurensuche, 1. September 2021, abrufbar unter: <https://www.ardmediathek.de/video/wdr-dok/made-to-measure-eine-digitale-spurensuche/wdr/Y3JpZDovL3dkci5kZS9CZWl0cmFnLWYwZGQwNTgwLWMyNDUtNGlwZC1iNjE5LTljY2YwNDM5NmVhMQ>) veranschaulicht, dass allein über die Rekonstruktion von Google-Suchen einer Person intime Erkenntnisse über Suizidgedanken, Abtreibungen und Essstörungen ermittelt werden konnten. Hierbei handelte es sich um Erkenntnisse, die die betroffene Person nicht mit

Dritten geteilt haben muss. Beispiele sind u.a. der Besuch anonymer Foren, z.B. für Opfer von Gewalt- und Sexualverbrechen, Recherchen zu medizinischen Symptomen (66 Prozent der Deutschen haben im Jahr 2019 derartige Recherchen zu eigenen Symptomen angestellt, vgl.

<https://de.statista.com/infografik/8497/nutzung-des-internets-fuer-gesundheitsinformationen/>) oder die Nutzung pornographischer Angebote im Internet (ca. 14 Mio. Deutsche sind regelmäßige Nutzer, vgl.

<https://de.statista.com/infografik/8869/pornografie-im-internet/>). Angesichts einer durchschnittlichen Internet-Nutzungsdauer von 269 Minuten/Tag in der Altersgruppe 14-29 (vgl.

<https://de.statista.com/statistik/daten/studie/1073613/umfrage/taegliche-nutzungsdauer-des-medialen-internets-nach-altersgruppen-in-deutschland/>)

ermöglicht die Überwachung von Datenströmen eine umfassende Überwachung von Interessen und Neigungen der Bürgerinnen und Bürger.

Die Gefahr des Zugriffs der Behörden auf einen umfangreichen Datenbestand, der auch Daten enthält, die den Kernbereich betreffen können, wird durch eine vom Bundesgerichtshof tolerierte (BGH, Beschluss vom 14. Oktober 2020 – 5 StR 229/19 –, NStZ 2021, 355 m. Anm. Grözinger) Rechtspraxis erhöht, über eine Anordnung der Telekommunikationsüberwachung – konkret im repressiven Bereich – auch auf Datenbestände zurückzugreifen, die bereits vor Anordnung der Telekommunikation existierten. Die Zugriffsmöglichkeit auf retrograde Kommunikationsdaten führt damit im kernbereichsrelevanten Bereich der E-Mail-Kommunikation und Internetnutzung zu einer Gefahrenlage, die mit der Online-Durchsuchung vergleichbar ist. Die Einschränkung der Gesetzesbegründung (LT-Drs. 7/3694, S. 186) ist insoweit unzureichend, da diese – wie die Entscheidung des Bundesgerichtshofs zeigt (vgl. Grözinger, NStZ 2021, 358, 359 mit Verweis auf BT-Drs. 18/12785, S. 50) – keine Gewährleistung für eine restriktive Auslegung in der Praxis bietet.

Diese neuen bzw. gerichtlich neu eingeräumten Möglichkeiten der Auslegung der Vorschriften zur Telekommunikationsüberwachung führen dazu, dass die vom 1. Senat geschilderte Situation eingetreten ist (insb. keine Möglichkeit der Prüfung der Kernbereichsrelevanz auf Erhebungsebene) und eine Sichtung durch eine

unabhängige Stelle geboten ist. Dem DAV ist bewusst, dass das Erfordernis der Einbindung einer unabhängigen Stelle im Bereich der (präventiven und repressiven) Telekommunikationsüberwachung mit signifikanten praktischen Hürden für Polizei- und Strafverfolgungsbehörden einhergehen würde. Angesichts der signifikanten Ausweitung behördlicher Befugnisse im Bereich der Telekommunikationsüberwachung ist eine verfassungsrechtliche Einhegung indes, wie der 1. Senat bereits im Grundsatz festgestellt hat, geboten. Die Einbindung einer unabhängigen Stelle ist zumindest dann verfassungsrechtlich zwingend, sofern im Rahmen einer Telekommunikationsüberwachung nicht nur das mündlich gesprochene Wort überwacht wird. Hier ist ein Kernbereichsschutz auf Erhebungsebene regelmäßig nicht umsetzbar.

Darüber hinaus gelten die oben (vgl. B.II.4 b)) zur Frage der Gefahr im Verzug dargestellten verfassungsrechtlichen Bedenken auch hinsichtlich der Regelung des § 33d Abs. 8 S. 3 SOG M-V, zumal die mit der Entscheidung beauftragten Beamten und Beamtinnen nicht zur Verschwiegenheit verpflichtet sind.

IV. Rasterfahndung

Die Verfassungsbeschwerde wendet sich gegen § 44 Abs. 1 Nr. 1 SOG M-V, wonach eine Rasterfahndung auch unter den Voraussetzungen des § 67 a Abs. 1 SOG M-V gestattet ist.

Durch die Bezugnahme auf die Voraussetzungen des § 67 a Abs. 1 SOG M-V ist eine Rasterfahndung gestattet, wenn Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat nach § 67c SOG M-V begehen oder an dieser teilnehmen wird oder das individuelle Verhalten dieser Person die konkrete Wahrscheinlichkeit dafür begründet, dass sie innerhalb eines überschaubaren Zeitraums eine terroristische Straftat nach § 67c M-V begehen oder an dieser teilnehmen wird.

Die Voraussetzungen des § 67a Abs. 1 SOG M-V beschreiben Umstände im Vorfeld einer konkreten Gefahr, bei denen der Eintritt eines Schadens nicht in gleicher Weise wahrscheinlich ist wie bei einer konkreten Gefahr.

Indem der Gesetzgeber die Zulässigkeit der Rasterfahndung mit § 44 Abs. 1 Nr. 1 SOG M-V im Vorfeld einer konkreten Gefahr gestattet, verfehlt er den vom Bundesverfassungsgericht in seiner Entscheidung vom 4. April 2006 – 1 BvR 518/02 –, BVerfG 115, 320 entwickelten Maßstab. Danach muss die Zulässigkeit einer präventiven polizeilichen Rasterfahndung vom Vorliegen einer konkreten Gefahr für hochrangige Rechtsgüter, wie den Bestand und die Sicherheit des Bundes oder eines Landes oder für Leben oder Freiheit einer Person, abhängig gemacht werden. Im Vorfeld der Abwehr einer konkreten Gefahr ist eine Rasterfahndung unzulässig. Sie ist mit Eingriffen in das Recht auf informationelle Selbstbestimmung von erheblichem Gewicht verbunden, weil sie zu vollständig verdachtslos und mit hoher Streubreite erfolgenden Grundrechtseingriffen führt, die Informationen mit intensivem Persönlichkeitsbezug erfassen können, BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 –, BVerfGE 115, 320-381, Rn. 138. Die von einer Rasterfahndung Betroffenen stehen regelmäßig in keiner tatsächengestützten Verbindung zu einer konkreten Bedrohungssituation.

Zwar hat das Bundesverfassungsgericht in seinem Urteil zum BKA-Gesetz vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378 (LT 1-3), Rn. 112 ausgesprochen, der Gesetzgeber sei von Verfassungs wegen nicht von vornherein auf die Schaffung von Eingriffstatbeständen beschränkt, die dem tradierten sicherheitsrechtlichen Modell der Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren entsprechen. Er könne die Grenzen für bestimmte Bereiche mit dem Ziel schon der Straftatenverhütung auch weiter ziehen, indem er die Anforderung an die Vorhersehbarkeit des Kausalverlaufs reduziert.

Zulässig sind Maßnahmen im Vorfeld einer konkreten Gefahr aber nur, wenn Tatsachen bekannt sind, die nicht nur im Hinblick auf die abzuwehrende Gefahr den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich

absehbares Geschehen zulassen. Auch über die Identität der beteiligten Personen muss zumindest so viel bekannt sein, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf diese Personen beschränkt werden kann, so ausdrücklich BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 112.

Genau diese Begrenzung auf einen individualisierten Personenkreis ist bei einer Rasterfahndung nicht gegeben. Sie zeichnet sich im Gegenteil durch die große Streubreite der Betroffenen aus, gerade diese Streubreite des Eingriffs kennzeichnet den schwerwiegenden Grundrechtseingriff, der mit einer Rasterfahndung verbunden ist. Denn Grundrechtseingriffe, die sowohl durch Verdachtslosigkeit als auch durch eine große Streubreite gekennzeichnet sind - bei denen also zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben - weisen grundsätzlich eine hohe Eingriffsintensität auf (vgl. BVerfGE 100, 313, 376, 392; 107, 299, 320 f.; 109, 279, 353; 113, 29, 53; 113, 348, 383). Denn der Einzelne ist in seiner grundrechtlichen Freiheit umso intensiver betroffen, je weniger er selbst für einen staatlichen Eingriff Anlass gegeben hat, BVerfG, Beschluss vom 4. April 2006 – 1 BvR 518/02 –, BVerfGE 115, 320-381, Rn. 117. Im Vorfeld einer konkreten Gefahr sind Grundrechtseingriffe mit einer Streubreite wie der Rasterfahndung damit unzulässig.

Da sich die nach § 44 Abs. 1 Nr. 1 SOG M-V unter den Voraussetzungen des § 67 a Abs. 1 SOG M-V zulässigen Maßnahmen der Rasterfahndung in keiner Weise von den Maßnahmen der Rasterfahndung unterscheiden, die der Gesetzgeber mit § 44 Abs. 1 Nr. 2 SOG M-V im Einklang mit der Rechtsprechung des BVerfG von einer konkreten Gefahr abhängig gemacht hat, ist die Verfassungsbeschwerde insoweit begründet.

V. Schutzpflichten für die IT-Sicherheit (Ausnutzung und Aufrechterhaltung von technischen Lücken)

Die Beschwerdeführer rügen, dass die Befugnis zur Online-Durchsuchung die aus dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme folgende staatliche Pflicht, Grundrechtsträger vor der unberechtigten Ausnutzung staatlich bekannter IT-Sicherheitslücken zu schützen, verletze.

Sie gehen davon aus, dass diese Schutzpflicht die Geheimhaltung und Nutzung sog. Zero-Days zum Zwecke von Online-Durchsuchung und Quellen-TKÜ generell ausschließt. Zumindest müssten die Ermächtigungsgrundlagen aber Regelungen für ein behördliches Schwachstellen-Management enthalten.

1. Wortlaut und Auslegung

Das SOG M-V erlaubt unter bestimmten Voraussetzungen den verdeckten Einsatz technischer Mittel, um in informationstechnische Systeme einer Person einzugreifen und aus diesen Daten zu erheben (§ 33c Abs. 1 S. 1 SOG M-V).

Ein solcher Eingriff kann unter anderem dadurch erfolgen, dass man mit technischen Mitteln von außen zu dem informationstechnischen System Zugang erlangt, indem man eine Schwachstelle des Systems ausnutzt. Das SOG M-V trifft aber keine Regelungen über den Umgang mit IT-Sicherheitslücken durch die Polizeibehörden.

2. Verfassungsrechtliche Anforderungen

Der 1. Senat des Bundesverfassungsgerichts hat in seinem Beschluss vom 8. Juni 2021 – 1 BvR 2771/18 –, festgestellt, dass sich aus dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme eine Pflicht des Staates ergibt, dazu beizutragen, dass die Schutzgüter gegen Angriffe Dritter geschützt werden. Wisse der Staat von Sicherheitslücken, die den Herstellern und Nutzern unbekannt sind, verdichte sich sein allgemeiner Schutzauftrag zu einer konkreten Verpflichtung, die Nutzerinnen und Nutzer

informationstechnischer Systeme davor zu schützen, dass Dritte über unbekannte Sicherheitslücken die genutzten Systeme infiltrieren (BVerfG, Beschluss vom 8. Juni 2021 – 1 BvR 2771/18 –, Rn. 35).

Diese Schutzpflicht schließt zwar die Ausnutzung von Sicherheitslücken für eine Quellen-Telekommunikationsüberwachung nicht aus, verlange aber, dass der Gesetzgeber den Umgang der Polizeibehörden mit Sicherheitslücken, die den Herstellern nicht bekannt sind, regelt (BVerfG, Beschluss vom 8. Juni 2021 – 1 BvR 2771/18 –, Rn. 35, 41 ff.). Andernfalls bestünde die Gefahr, dass die Behörde im Interesse der Durchführung ihr übertragener Überwachungsbefugnisse es unterlässt, Sicherheitslücken zu melden oder sogar aktiv darauf hinwirkt, dass diese unerkannt bleiben (BVerfG, Beschluss vom 8. Juni 2021 – 1 BvR 2771/18 –, Rn. 42).

Diesen verfassungsrechtlichen Anforderungen wird das SOG M-V nicht gerecht. Es ermächtigt die Polizei, unter Ausnutzung von IT-Sicherheitslücken Daten zu erheben, trifft aber keine Regelungen über den Umgang mit diesen Sicherheitslücken.

Die Verfassungsbeschwerde ist daher auch insoweit begründet.

C. Zusammenfassung

Damit hält der Deutsche Anwaltverein die Verfassungsbeschwerde im Ergebnis weitgehend für begründet. Das Gesetz bleibt bei der vorgesehenen Ausweitung von Eingriffsbefugnissen im Vorfeld konkreter Gefahren, bei den Regelungen zum Kernbereichsschutz und auch bei den konkreten Maßnahmen hinter verfassungsrechtlichen Anforderungen zurück.

Der vom Landesgesetzgeber offenbar gegenüber dem BKAG bewusst weiter gestaltete Anwendungsbereich der extrem eingriffsintensiven sog. Quellen-TKÜ und Online-Durchsuchung (durch Verweis auf das Gefahrenvorfeld in § 67a Abs. 1 SOG M-V) ist unverhältnismäßig. Es fehlen zudem eine Subsidiaritätsklausel für Nicht-Verantwortliche und Regelungen über den Umgang mit IT-

Sicherheitslücken, die staatliche Behörden vorhalten, um Quellen-TKÜ- und Online-Durchsuchungsmaßnahmen durchführen zu können und mit deren Geheimhaltung ein Risiko für die IT-Sicherheit allgemein verbunden ist. Diesbezüglich hat das BVerfG jüngst entschieden, dass den Staat hier eine Schutzpflicht trifft und er zu deren Erfüllung gehalten ist, entsprechende Regelungen zu treffen.

Bei der Quellen-TKÜ wird außerdem zu recht gerügt, dass § 33d Abs. 3 S. 2 SOG M-V auch den Zugriff auf gespeicherte Daten erlaube und die Quellen-TKÜ so zu einer „kleinen Online-Durchsuchung“ werde. Zudem fehlt eine Regelung über die einzusetzende Technik und damit auch die gesetzgeberische Gewährleistung, dass mit der Überwachungstechnologie auch wirklich nur diejenigen Daten erhoben werden, die § 33d Abs. 3 S. 1, 2 SOG M-V zulassen.

Der in § 26a SOG M-V allgemein geregelte Kernbereichsschutz bei polizeilichen Überwachungsmaßnahmen wird mit den in Abs. 3 S. 1 vorgesehenen Ausnahmen einer Abwägung zugänglich gemacht. Dies widerspricht dem aus Art. 1 Abs. 1 GG folgenden *absoluten* Schutz der Intimsphäre vor staatlichen Eingriffen und ist deshalb verfassungswidrig.

Auch die Ausgestaltung der Datensichtung bei Vorliegen des Verdachts der Erhebung kernbereichsrelevanter Daten ist von vorne herein unzureichend. Die Sichtung soll gem. § 26a Abs. 5 S. 1 SOG M-V durch den behördlichen Datenschutzbeauftragten bzw. bei Gefahr im Verzug gem. § 33c Abs. 10 SOG M-V durch von der Behördenleitung bestimmte Bedienstete erfolgen. Erforderlich ist es aber nach der Rechtsprechung des Bundesverfassungsgerichts, hiermit eine *unabhängige* Stelle zu betrauen, die nicht Teil der Behörde ist, welche die Datenerhebung veranlasst hat. Auch die diesbezüglich erhobene Rüge ist daher begründet.

Der Deutsche Anwaltverein geht ferner davon aus, dass im Lichte der jüngeren technischen Entwicklungen eine Sichtung der erhobenen Daten durch eine unabhängige Stelle auch jenseits der Online-Durchsuchung bei Telekommunikationsüberwachungsmaßnahmen wegen der notorischen

Kernbereichsrelevanz regelmäßig erforderlich ist (anders noch das BKAG-Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –; Rn. 240).

Überwachungsgegenstände sind heute weit mehr als klassische Telefonie und textbasierte Kommunikation. Insbesondere die Überwachung des Surfverhaltens im Internet ermöglicht weitreichende Erkenntnisse über die Person, die auch die Bereiche erfasst, die bislang für die Online-Durchsuchung als prägend galten.

Die Regelung des § 33a Abs. 5 SOG M-V, wonach Räumlichkeiten betroffener Personen heimlich betreten und durchsucht werden dürfen, ist schon mangels Beschränkung auf Fälle des Vorliegens einer dringenden Gefahr verfassungswidrig. Zudem ist fraglich, ob eine heimliche Durchsuchung überhaupt mit Art. 13 GG vereinbar ist. Hierzu hat sich das Bundesverfassungsgericht bislang – soweit ersichtlich – noch nicht geäußert.

Die Ausgestaltung der Rasterfahndung in § 44 Abs. 1 Nr. 1 SOG M-V, der auf § 67a Abs. 1 SOG M-V Bezug nimmt und eine Rasterfahndung schon im Vorfeld einer konkreten Gefahr zulässt, verfehlt schließlich die in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Maßstäbe. Danach setzt eine präventivpolizeiliche Rasterfahndung das Vorliegen einer konkreten Gefahr für hochrangige Rechtsgüter voraus.