BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 33
Juli 2022

zur Verfassungsbeschwerde gegen Bestimmungen des neuen Sicherheits- und Ordnungsgesetzes Mecklenburg-Vorpommern v. 27.04.2020

- 1 BvR 1345/21-

Mitglieder des Verfassungsrechtsauschusses

RA Prof. Dr. Christian Kirchberg, Vorsitzender
RA Dr. Christian-Dietrich Bracher
RA Prof. Dr. Dr. Karsten Fehn
RA Dr. Markus Groß
RAuN Prof. Dr. Wolfgang Kuhla
RA Prof. Dr. Christofer Lenz
RA Dr. Michael Moeskes (Berichterstatter)
RA Dr. jur. h.c. Gerhard Strate
RA Prof. Dr. Michael Uechtritz
RAin Dr. jur. Katharina Wild

RA Michael Then, Schatzmeister Bundesrechtsanwaltskammer
RA Frank Johnigk, Bundesrechtsanwaltskammer

Anlage: Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern (Sicherheits- und Ordnungsgesetz - SOG M-V) vom 27. April 2020

Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern (Sicherheits- und Ordnungsgesetz - SOG M-V) Vom 27. April 2020

§ 26a

Schutz des Kernbereiches privater Lebensgestaltung

(1) Rechtfertigen Tatsachen die Annahme, dass durch eine Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist diese unzulässig.

(2) Werden durch eine Maßnahme auch Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt, dürfen diese nicht verwertet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen und die Tatsache ihrer Erlangung und Löschung ist gemäß § 46d zu dokumentieren; für die Protokollierung gilt § 46e. Die Dokumentation und entsprechende Protokollierung dürfen ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden; sie sind frühestens nach Abschluss der Datenschutzkontrolle gemäß § 48b Absatz 6 und spätestens nach vierundzwanzig Monaten zu löschen.

(3) Dürfen Daten nach diesem Gesetz erhoben werden und rechtfertigen während der Erhebung Tatsachen die Annahme, dass Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erfasst werden, ist die Maßnahme abzubrechen; dies gilt nicht, sofern mit dem Abbruch der Maßnahme eine Gefährdung der eingesetzten Polizeibeamtinnen und Polizeibeamten oder Vertrauenspersonen oder ihrer weiteren Verwendung verbunden wäre. Soweit Daten aufgezeichnet werden, ist der Aufzeichnungsvorgang, soweit dies technisch möglich ist, unverzüglich zu unterbrechen. Nach einer Unterbrechung darf die Datenerhebung und -aufzeichnung nur fortgesetzt werden, wenn aufgrund geänderter Umstände davon ausgegangen werden kann, dass die Gründe, die zur Unterbrechung geführt haben, nicht mehr vorliegen. Die Tatsache der Unterbrechung und der Fortsetzung ist zu dokumentieren oder zu protokollieren; Absatz 2 Satz 3 gilt entsprechend.

(4) Soweit in diesem Gesetz nichts Besonderes geregelt ist, ist vor einer Verwendung von Daten in oder aus Wohn- oder Geschäftsräumen oder in oder von befriedetem Besitztum die Rechtmäßigkeit dieser Datenerhebung zuvor richterlich festzustellen. Bei Gefahr im Verzug entscheidet über die Verwendung die Behördenleitung oder eine von ihr besonders beauftragte Beamtin oder ein von ihr besonders beauftragter Beamter; eine richterliche

Entscheidung ist unverzüglich nachzuholen. Sind in den Fällen des Satzes 2 Daten an andere Stellen übermittelt worden und wurde die Rechtmäßigkeit dieser Datenerhebung nicht richterlich bestätigt, ist § 45 Absatz 5 zu beachten.

(5) Soweit in diesem Gesetz nichts Besonderes geregelt ist, sind vor einer Verwendung von Daten in Fällen einer Unterbrechung nach Absatz 3, die nicht bereits von Absatz 4 erfasst werden, die erhobenen Daten der oder dem behördlichen Datenschutzbeauftragten zur Auswertung und Entscheidung über die Rechtmäßigkeit dieser Datenerhebung vorzulegen. Absatz 4 Satz 2 gilt entsprechend. Sind in den Fällen des Satzes 2 Daten an andere Stellen übermittelt worden und wurde die Rechtmäßigkeit dieser Datenerhebung nicht von der oder dem behördlichen Datenschutzbeauftragten festgestellt, ist § 45 Absatz 5 zu beachten.

§ 33
Besondere Mittel der Datenerhebung

(1) Besondere Mittel der Datenerhebung sind

1. die planmäßig angelegte Beobachtung, die durchgehend länger als 24 Stunden dauert oder an mehr als zwei Tagen stattfinden soll (längerfristige Observation),

2. der verdeckte Einsatz technischer Mittel, insbesondere solcher zur Bild- und Tonaufnahme oder Bild- und Tonaufzeichnung,

3. der Einsatz von Personen, deren Zusammenarbeit mit der Polizei den Betroffenen und Dritten (§ 3 Absatz 4 Nummer 2) nicht bekannt ist (Vertrauenspersonen),

4. der Einsatz von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten unter einer ihnen verliehenen, auf Dauer angelegten, veränderten Identität (verdeckt Ermittelnde).

(2) Mittel des Absatzes 1 können nur angewandt werden, wenn Tatsachen die Annahme der Begehung von Straftaten von erheblicher Bedeutung (§ 49) rechtfertigen und die Aufklärung des Sachverhaltes zum Zwecke der Verhütung solcher Straftaten oder ihrer möglichen Verfolgung ansonsten unmöglich oder wesentlich erschwert wäre. In diesem Fall kann die Polizei mit den Mitteln des Absatzes 1 Daten erheben über

1. Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie eine Straftat nach Satz 1 begehen oder sich an einer solchen beteiligen werden oder

2. Personen nach § 27 Absatz 3 Nummer 2.

Mittel nach Absatz 1 können bei Vorliegen der Voraussetzungen des § 67a Absatz 1 auch gegenüber den dort genannten Personen sowie Personen nach § 27 Absatz 3 Nummer 2 eingesetzt werden, wenn die Aufklärung des Sachverhaltes zum Zwecke der Verhütung terroristischer Straftaten (§ 67c) oder ihrer möglichen Verfolgung ansonsten unmöglich oder wesentlich erschwert wäre. Brief-, Post- und Fernmeldegeheimnis bleiben unberührt.

(3) Abweichend von Absatz 2 können Mittel nach Absatz 1 Nummer 2 eingesetzt werden, wenn dies ausschließlich dem Schutz der bei einem polizeilichen Einsatz tätigen Personen dient.

(4) Die Maßnahmen nach Absatz 1 und 3 dürfen auch durchgeführt werden, wenn Dritte (§ 3 Absatz 4 Nummer 2) unvermeidbar betroffen sind.

(5) Verdeckt Ermittelnde dürfen unter der Legende mit Einverständnis der berechtigten Person deren Wohnung betreten. Im Übrigen richten sich die Befugnisse verdeckt Ermittelnder nach diesem Gesetz oder anderen Rechtsvorschriften.

(6) Soweit es für den Aufbau und zur Aufrechterhaltung der Legende verdeckt Ermittelnder unerlässlich ist, können entsprechende Urkunden hergestellt, verändert und gebraucht werden. Die Unerlässlichkeit stellt die Behörde fest, die die verdeckt Ermittelnden einsetzt. Verdeckt Ermittelnde dürfen unter der Legende zur Erfüllung ihres Auftrages am Rechtsverkehr teilnehmen.

§ 33 b
Einsatz technischer Mittel zur Wohnraumüberwachung

(1) Die Polizei kann zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt, durch den verdeckten Einsatz technischer Mittel in oder aus der Wohnung einer Person, die für diese Gefahr verantwortlich ist, deren nichtöffentlich gesprochenes Wort abhören und aufzeichnen sowie von ihr Lichtbilder und Bildaufzeichnungen herstellen, soweit die Abwehr der Gefahr ansonsten unmöglich oder wesentlich erschwert wäre. Diese Maßnahmen dürfen auch unter den Voraussetzungen des § 67a Absatz 1 gegen die dort

genannten Personen durchgeführt werden, soweit die Abwehr der dort bezeichneten Gefahr ansonsten unmöglich oder wesentlich erschwert wäre.

(2) In Wohnungen anderer Personen ist die Maßnahme nur zulässig, wenn Tatsachen die Annahme rechtfertigen, dass

1. sich eine Person im Sinne des Absatzes 1 dort aufhält und

2. die Maßnahme in der Wohnung dieser Person allein nicht zur Abwehr der Gefahr oder zur Verhütung einer Straftat nach Absatz 1 führen wird.

(3) Die Maßnahmen nach Absatz 1 und 2 dürfen auch durchgeführt werden, wenn Dritte (§ 3 Absatz 4 Nummer 2) unvermeidbar betroffen sind. Bei der Beurteilung nach § 26a Absatz 1 ist insbesondere auf die Art der zu überwachenden Räumlichkeiten und das Verhältnis der dort anwesenden Personen zueinander abzustellen.

(4) Die Maßnahmen nach Absatz 1 und 2 bedürfen der richterlichen Anordnung auf Antrag der Leitung der zuständigen Polizeibehörde. Bei Gefahr im Verzug kann die Leitung der zuständigen Polizeibehörde die Maßnahme anordnen; eine richterliche Entscheidung ist unverzüglich nachzuholen. Soweit die Anordnung nach Satz 2 nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(5) Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,

2. die zu überwachende Wohnung oder die zu überwachenden Wohnräume,

3. Art, Umfang und Dauer der Maßnahme,

4. der Sachverhalt sowie

5. eine Begründung.

(6) Die Anordnung ergeht schriftlich; in Fällen von Gefahr im Verzug ist sie unverzüglich nachträglich zu dokumentieren. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,

2. die zu überwachende Wohnung oder die zu überwachenden Wohnräume,

3. Art, Umfang und Dauer der Maßnahme sowie

4. die Gründe.

Die Anordnung ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die aufgrund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(7) Das anordnende Gericht ist über den Verlauf und die Ergebnisse zu unterrichten; es entscheidet unverzüglich über die Rechtmäßigkeit der Datenverarbeitung. Sofern die Voraussetzungen der Anordnung nicht mehr vorliegen, ordnet es die Beendigung der Maßnahme an, soweit diese nicht bereits durch die Leitung der zuständigen Polizeibehörde veranlasst wurde.

(8) Bei Gefahr im Verzug entscheidet über die Verwendung erhobener Daten die Leitung der zuständigen Polizeibehörde; eine richterliche Entscheidung nach Absatz 7 Satz 1 ist unverzüglich nachzuholen. Bei der Sichtung der erhobenen Daten kann sie sich der technischen Unterstützung von zwei weiteren Bediensteten der Behörde bedienen. Die Bediensteten sind zur Verschwiegenheit über die ihnen bekannt gewordenen Erkenntnisse, die nicht verwertet werden dürfen, verpflichtet. Sind Daten an andere Stellen übermittelt worden und wurde die Rechtmäßigkeit dieser Datenerhebung nicht richterlich bestätigt, ist § 45 Absatz 5 zu beachten.

(9) § 33 Absatz 3 und § 33a Absatz 5 gelten entsprechend.

§ 33 c

Einsatz technischer Mittel zum Eingriff in informationstechnische Systeme

(1) Die Polizei darf durch den verdeckten Einsatz technischer Mittel in von der betroffenen Person genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben, wenn Tatsachen die Annahme rechtfertigen, dass eine Gefahr vorliegt für

1. Leib, Leben oder Freiheit einer Person oder

2. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt.

Eine Maßnahme nach Satz 1 ist auch zulässig, wenn die Voraussetzungen des § 67a Absatz 1 vorliegen. Die Maßnahme darf sich nur gegen eine Person richten, die für eine Gefahr verantwortlich ist. In informationstechnische Systeme anderer Personen darf die Maßnahme nur eingreifen, wenn Tatsachen die Annahme rechtfertigen, dass eine nach Satz 1 oder 2 betroffene Person dort ermittlungsrelevante Informationen speichert.

(2) Die Maßnahme darf nur durchgeführt werden, wenn die Abwehr der Gefahr ansonsten aussichtslos oder wesentlich erschwert wäre. Sie darf auch durchgeführt werden, wenn Dritte (§ 3 Absatz 4 Nummer 2) unvermeidbar betroffen sind. § 26a gilt mit der zusätzlichen Maßgabe, dass, soweit möglich, technisch sicherzustellen ist, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.

(3) Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.
Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(4) Unter den Voraussetzungen des Absatzes 1 dürfen technische Mittel eingesetzt werden, um zur Vorbereitung einer Maßnahme nach Absatz 1 die erforderlichen Daten, wie insbesondere spezifische Kennungen, sowie den Standort eines informationstechnischen Systems zu ermitteln. Personenbezogene Daten Dritter (§ 3 Absatz 4 Nummer 2) dürfen dabei nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist.

(5) Das verdeckte Durchsuchen von Sachen sowie das verdeckte Betreten und Durchsuchen von Räumlichkeiten der betroffenen Personen sind zulässig, soweit dies zur Durchführung von Maßnahmen nach Absatz 1 und 4 erforderlich ist.

(6) Die Maßnahmen nach Absatz 1 und 4, auch soweit ein Fall des Absatzes 5 vorliegt, bedürfen der richterlichen Anordnung auf Antrag der Leitung der zuständigen Polizeibehörde.

(7) Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,

2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,

3. in Fällen des Absatzes 5, soweit möglich, auch eine Bezeichnung der Sachen und die Anschrift der Räumlichkeiten der betroffenen Personen,

4. Art, Umfang und Dauer der Maßnahme,

5. der Sachverhalt sowie

6. eine Begründung.

(8) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:
1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,

2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,

3. in Fällen des Absatzes 5, soweit möglich, auch eine Bezeichnung der Sachen und die Anschrift der Räumlichkeiten der betroffenen Personen,

4. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie

5. die Gründe.

Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Anordnungsvoraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die aufgrund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(9) Das anordnende Gericht ist über den Verlauf und die Ergebnisse zu unterrichten; es entscheidet unverzüglich über die Rechtmäßigkeit der Datenverarbeitung. Sofern die Voraussetzungen der Anordnung nicht mehr vorliegen, ordnet es die Beendigung der

Maßnahme an, soweit diese nicht bereits durch die Leitung der zuständigen Polizeibehörde veranlasst wurde.

(10) Bei Gefahr im Verzug entscheidet über die Verwendung erhobener Daten die Leitung der zuständigen Polizeibehörde; eine richterliche Entscheidung nach Absatz 9 Satz 1 ist unverzüglich nachzuholen. Bei der Sichtung der erhobenen Daten kann sie sich der technischen Unterstützung von zwei weiteren Bediensteten der Behörde bedienen. Die Bediensteten sind zur Verschwiegenheit über die ihnen bekannt gewordenen Erkenntnisse, die nicht verwertet werden dürfen, verpflichtet. Sind Daten an andere Stellen übermittelt worden und wurde die Rechtmäßigkeit dieser Datenerhebung nicht richterlich bestätigt, ist § 45 Absatz 5 zu beachten.

§ 33d
Einsatz technischer Mittel zur Überwachung der Telekommunikation

(1) Die Polizei kann ohne Wissen der betroffenen Person personenbezogene Daten durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation erheben über

1. die für eine Gefahr Verantwortlichen, wenn dies zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt, erforderlich ist oder

2. Verantwortliche für eine Gefahr nach § 67a Absatz 1 oder

3. Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie für eine Person nach Nummer 1 oder 2 bestimmte oder von dieser herrührende Mitteilungen entgegennehmen oder weitergeben oder

4. Personen, bei denen Tatsachen die Annahme rechtfertigen, dass eine Person nach Nummer 1 oder 2 deren Telekommunikationsanschluss oder Endgerät benutzen wird oder

5. Personen, deren Leben oder Gesundheit gefährdet ist.

Datenerhebungen nach Satz 1 dürfen nur durchgeführt werden, wenn die Erfüllung der polizeilichen Aufgabe auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Maßnahme darf auch durchgeführt werden, wenn Dritte (§ 3 Absatz 4 Nummer 2) unvermeidbar betroffen sind.

(2) Eine Datenerhebung nach Absatz 1 kann sich auf

a) die Inhalte und Umstände der Telekommunikation oder

b) Verkehrs- und Standortdaten im Sinne des Telekommunikationsgesetzes
beziehen. Unter den Voraussetzungen des Absatzes 1 kann die Polizei auch Auskunft über die Verkehrs- und Standortdaten in einem zurückliegenden Zeitraum verlangen. Die Erhebung aller in einer Funkzelle angefallenen Verkehrsdaten (Funkzellenabfrage) ist nicht zulässig.

(3) Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass verdeckt mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird und

2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

Auf dem informationstechnischen System der betroffenen Person gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können. § 33c Absatz 3 und 5 gilt entsprechend. § 33c bleibt im Übrigen unberührt.

(4) Die Maßnahmen bedürfen der richterlichen Anordnung auf Antrag der Leitung der zuständigen Polizeibehörde. Bei Gefahr im Verzug für Leib, Leben oder Freiheit einer Person kann die Leitung der zuständigen Polizeibehörde oder eine von ihr besonders beauftragte Beamtin oder ein von ihr besonders beauftragter Beamter die Maßnahme anordnen; eine richterliche Entscheidung ist unverzüglich nachzuholen. Soweit die Anordnung nach Satz 2 nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(5) Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,

2. soweit möglich die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgeräts, sofern nicht Tatsachen die Annahme rechtfertigen, dass diese Rufnummer oder andere Kennung zugleich einem anderen Endgerät zugeordnet ist,

3. Art, Umfang und Dauer der Maßnahme,

4. im Falle des Absatzes 3 auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll, und in den Fällen der entsprechenden Anwendung des § 33c Absatz 5, soweit möglich, auch eine Bezeichnung der Sachen und die Anschrift der Räumlichkeiten der betroffenen Person,

5. der Sachverhalt sowie

6. eine Begründung.

(6) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,

2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgeräts, sofern nicht Tatsachen die Annahme rechtfertigen, dass diese Rufnummer oder andere Kennung zugleich einem anderen Endgerät zugeordnet ist,

3. Art, Umfang und Dauer der Maßnahme einschließlich der Uhrzeit der Anordnung,

4. im Falle des Absatzes 3 auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll, und in den Fällen der entsprechenden Anwendung des § 33c Absatz 5, soweit möglich, auch eine Bezeichnung der Sachen und die Anschrift der Räumlichkeiten der betroffenen Person sowie

5. die Gründe.

Bei Gefahr im Verzug kann die Angabe der Gründe unterbleiben; sie ist unverzüglich nachzuholen. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die aufgrund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(7) Aufgrund der Anordnung hat jeder Diensteanbieter im Sinne des Telekommunikationsgesetzes der Polizei nach Maßgabe des Telekommunikationsgesetzes und der Telekommunikations-Überwachungsverordnung die Maßnahmen unverzüglich zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Die in Anspruch genommenen Diensteanbieter werden entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes entschädigt.

(8) Über die Rechtmäßigkeit erhobener Daten, die im Wege einer automatischen Aufzeichnung ohne zeitgleiche Prüfung, ob der Kernbereich privater Lebensgestaltung berührt ist, erlangt wurden, entscheidet die oder der behördliche Datenschutzbeauftragte. Satz 1 gilt entsprechend, wenn sich bei zeitgleicher Prüfung Tatsachen ergeben, die die Annahme rechtfertigen, dass Erkenntnisse aus dem Kernbereich erfasst werden. Bei Gefahr im Verzug entscheidet über die Verwendung erhobener Daten die Leitung der zuständigen Polizeibehörde oder eine von ihr besonders beauftragte Beamtin oder ein von ihr besonders beauftragter Beamter; eine Entscheidung der oder des behördlichen Datenschutzbeauftragten ist unverzüglich nachzuholen. Soweit personenbezogene Daten Dritter (§ 3 Absatz 4 Nummer 2) erhoben worden sind, sind diese unverzüglich nach der Entscheidung zur Datenweiterverarbeitung zu löschen, soweit dies technisch möglich ist. Sind in den Fällen des Satzes 3 Daten an andere Stellen übermittelt worden und wurde die Rechtmäßigkeit dieser Datenerhebung nicht von der oder dem behördlichen Datenschutzbeauftragten festgestellt, ist § 45 Absatz 5 anzuwenden.

§ 34
Einsatz unbemannter Luftfahrtsysteme

Bei den nachfolgenden Maßnahmen dürfen unter Beachtung der dort bestehenden Regelungen Daten auch durch den Einsatz unbemannter Luftfahrtsysteme erhoben werden:

1. offene Bild- und Tonaufnahmen oder Bild- und Tonaufzeichnungen nach § 32 Absatz 1,3,4 und 10,
2. Einsatz besonderer Mittel der Datenerhebung nach § 33,

3. Einsatz technischer Mittel in Wohnungen nach § 33b,

4. Einsatz technischer Mittel zum Eingriff in informationstechnische Systeme nach § 33c,

5. Einsatz technischer Mittel zur Telekommunikationsüberwachung nach den §§ 33d, 33f und 33g.

Eine Datenerhebung mittels unbemannter Luftfahrtsysteme durch eine Vertrauensperson ist unzulässig.

§ 35
Ausschreibung zur polizeilichen Beobachtung und gezielten Kontrolle

(1) Rechtfertigen Tatsachen die Annahme dafür, dass bestimmte Personen Straftaten von erheblicher Bedeutung (§ 49) oder terroristische Straftaten (§ 67c) begehen werden, kann die Polizei zur Verhütung oder zur vorbeugenden Bekämpfung solcher Straftaten personenbezogene Daten, insbesondere die Personalien dieser Personen oder die amtlichen Kennzeichen, die Identifizierungsnummern oder die äußeren Kennzeichnungen der von solchen Personen benutzten oder eingesetzten Kraftfahrzeuge, Wasserfahrzeuge, Luftfahrzeuge oder Container, in einem Dateisystem speichern, damit andere Polizeibehörden Erkenntnisse über das Antreffen sowie über Personen nach § 27 Absatz 3 Nummer 2 bei Gelegenheit einer Überprüfung aus anderem Anlass übermitteln (Ausschreibung zur polizeilichen Beobachtung). Die Maßnahme kann auch durchgeführt werden, wenn die Voraussetzungen des § 67a Absatz 1 vorliegen.

(2) Unter den Voraussetzungen des Absatzes 1 ist auch die Ausschreibung zur gezielten Kontrolle zulässig. Unbeschadet anderer Vorschriften kann die Polizei im Rahmen der gezielten Kontrolle

1. die Identität von Personen feststellen, die sich in einem zur gezielten Kontrolle ausgeschriebenen Fahrzeug oder Container befinden,

2. das zur gezielten Kontrolle ausgeschriebene Fahrzeug oder den Container sowie die darin befindlichen Sachen durchsuchen sowie

3. die zur gezielten Kontrolle ausgeschriebene Person durchsuchen
und die daraus gewonnenen Erkenntnisse an die ausschreibende Polizeibehörde übermitteln.

Die für die Identitätsfeststellung sowie die Durchsuchung von Personen und Sachen geltenden Vorschriften sind im Übrigen anzuwenden.

(3) Die Maßnahmen nach Absatz 1 und 2 bedürfen der Anordnung durch die Leitung der zuständigen Polizeibehörde.

(4) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,

2. sonstige Angaben nach Absatz 1,

3. Art, Umfang und Dauer der Maßnahme sowie

4. die Gründe.

(5) Die Anordnung ist auf höchstens sechs Monate zu befristen. Liegen die Voraussetzungen für die Anordnung nicht mehr vor oder ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, ist die Ausschreibung unverzüglich zu löschen. Eine Verlängerung um jeweils nicht mehr als sechs weitere Monate ist zulässig, soweit die Voraussetzungen der Anordnung fortbestehen. Eine Verlängerung bedarf der gerichtlichen Anordnung nach Maßgabe des Absatzes 4 auf Antrag der Leitung der zuständigen Polizeibehörde; der Antrag muss die Angaben nach Absatz 4 Satz 2 Nummer 1 bis 3 sowie den Sachverhalt und eine Begründung enthalten.

§ 44
Rasterfahndung

(1) Die Polizei kann von Behörden, anderen öffentlichen Stellen und von Stellen außerhalb der öffentlichen Verwaltung

1. unter den Voraussetzungen des § 67a Absatz 1 oder

2. zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist,

die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateisystemen zum Zweck des Abgleichs mit anderen Datenbeständen verlangen (Rasterfahndung), wenn Tatsachen die Annahme rechtfertigen, dass dies zur Abwehr der Gefahr erforderlich ist. Von den Verfassungsschutzbehörden des Bundes oder der Länder, dem Bundesnachrichtendienst sowie dem Militärischen Abschirmdienst kann die Übermittlung nach Satz 1 nicht verlangt werden.

(2) Das Übermittlungsersuchen ist auf Namen, Anschrift, Tag und Ort der Geburt sowie auf im einzelnen Falle festzulegende Merkmale zu beschränken; es darf sich nicht auf personenbezogene Daten erstrecken, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Von Übermittlungsersuchen nicht erfasste personenbezogene Daten dürfen übermittelt werden, wenn wegen erheblicher technischer Schwierigkeiten oder wegen eines unangemessenen Zeit- oder Kostenaufwands eine Beschränkung auf die angeforderten Daten nicht möglich ist; diese Daten dürfen nicht verwendet werden.

(3) Die Maßnahme bedarf der richterlichen Anordnung auf Antrag der Leitung der zuständigen Polizeibehörde. Bei Gefahr im Verzug kann die Leitung der zuständigen Polizeibehörde die Maßnahme anordnen; eine richterliche Entscheidung ist unverzüglich nachzuholen. Soweit die Anordnung nach Satz 2 nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(4) Im Antrag sind anzugeben:

1. soweit möglich die Angaben nach Absatz 2 Satz 1,

2. die zur Übermittlung zu Verpflichtenden,

3. der Sachverhalt,

4. eine Begründung.

(5) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. soweit möglich die Angaben nach Absatz 2 Satz 1,

2. die zur Übermittlung Verpflichteten,

3. der Sachverhalt,

4. die Gründe.

(6) Die oder der Landesbeauftragte für den Datenschutz ist unverzüglich über die Maßnahme zu unterrichten.

(7) Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen personenbezogenen Daten auf dem Datenträger zu löschen und die Unterlagen zurückzugeben oder zu vernichten, soweit sie nicht zur Abwehr einer anderen Gefahr im Sinne des Absatzes 1 Satz 1 oder für ein mit dem Sachverhalt zusammenhängendes Strafverfahren erforderlich sind.

§ 46a
Benachrichtigungspflichten bei verdeckten und eingriffsintensiven Maßnahmen

(1) Bei folgenden Maßnahmen sind die dort jeweils benannten Personen durch die durchführende Stelle zu benachrichtigen:

1. bei Feststellung der Identität von Personen auf Übersichtsaufzeichnungen nach § 32 Absatz 1 Satz 1 Nummer 2 Satz 2 die Adressaten der Maßnahme,

2. bei Einsatz besonderer Mittel der Datenerhebung nach § 33 Absatz 1

a) die Adressaten der Maßnahme,

b) diejenigen, deren personenbezogene Daten verarbeitet wurden und

c) diejenigen, deren nicht allgemein zugängliche Wohnung betreten wurde,

3. bei Einsatz technischer Mittel in Wohnungen nach § 33b die von der Maßnahme betroffenen Personen, auch wenn die Maßnahme nach § 33b Absatz 9 als Personenschutzmaßnahme erfolgt ist,

4. bei verdecktem Zugriff auf informationstechnische Systeme nach § 33c, Eingriffen in den Telekommunikationsbereich nach § 33d oder Inanspruchnahme von Diensteanbietern nach den §§ 33e bis 33g und § 33h Absatz 1 Satz 2 und Absatz 2

a) die Adressaten der Maßnahme und

b) diejenigen, deren personenbezogene Daten im Rahmen einer solchen Maßnahme verarbeitet wurden,

5. bei Ausschreibung zur polizeilichen Beobachtung oder gezielten Kontrolle nach § 35

a) die Adressaten der Maßnahme und

b) diejenigen, deren personenbezogene Daten verarbeitet wurden,

6. bei Rasterfahndung nach § 44 die Personen, gegen die nach Auswertung der Daten weitere Maßnahmen durchgeführt wurden,

7. bei elektronischer Aufenthaltsüberwachung nach § 67a die Adressaten der Maßnahme, wenn Bewegungsbilder erstellt wurden, wobei die Benachrichtigung spätestens zwei Monate nach deren Beendigung zu erfolgen hat.

Erfolgen Maßnahmen mit Mitteln des § 33d Absatz 3, sind die in Satz 1 Nummer 4 genannten Personen auch darüber zu unterrichten, dass mit technischen Mitteln verdeckt auf informationstechnische Systeme zugegriffen wurde. Die Benachrichtigung unterbleibt, soweit überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen. Zudem kann die Benachrichtigung einer in Satz 1 Nummer 2, 4 und 5 bezeichneten Person, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen wurde. Nachforschungen zur Feststellung der Identität oder des Aufenthaltsortes einer in Satz 1 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des

Aufwands für die Feststellung sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist. Bezieht sich die Benachrichtigung auf Daten, die an oder von Verfassungsschutzbehörden des Bundes oder der Länder oder die an den oder von dem Bundesnachrichtendienst oder Militärischen Abschirmdienst übermittelt wurden, ist sie nur nach Zustimmung dieser Stellen zulässig.

(2) Die Benachrichtigung erfolgt, sobald dies ohne Gefährdung des Zwecks der Maßnahme, der eingesetzten Polizeibeamtinnen und Polizeibeamten oder Vertrauenspersonen oder der in der jeweiligen Befugnisnorm genannten Rechtsgüter geschehen kann. In den Fällen des Absatzes 1 Satz 1 Nummer 2 und bei Maßnahmen nach § 33b Absatz 9 ist auch eine Gefährdung der weiteren Verwendung von Vertrauenspersonen und verdeckt Ermittelnden als bedeutender Belang zu berücksichtigen. Ist wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen die betroffene Person eingeleitet worden, ist die Benachrichtigung in Abstimmung mit der Staatsanwaltschaft zurückzustellen, solange der Stand des Ermittlungsverfahrens eine Benachrichtigung nicht zulässt.

(3) Die Benachrichtigung hat zumindest zu enthalten:

1. die Angaben nach § 46 Absatz 1,

2. die Rechtsgrundlage der Datenerhebung und gegebenenfalls der weiteren Verarbeitung,

3. Informationen über die mutmaßliche Dauer der Datenspeicherung oder, falls diese Angabe nicht möglich ist, Kriterien hierfür sowie

4. gegebenenfalls über die Kategorien der Empfänger der Daten.

(4) Wird die Benachrichtigung aus einem der in Absatz 2 genannten Gründe zurückgestellt, bedarf die weitere Zurückstellung der richterlichen Zustimmung, wenn sie nicht innerhalb des folgenden Zeitraums erfolgt:

1. sechs Monate nach Beendigung des Einsatzes technischer Mittel in Wohnungen nach § 33b oder des verdeckten Zugriffs auf informationstechnische Systeme nach § 33c oder § 33d Absatz 3 oder

2. ein Jahr nach Beendigung einer der übrigen in Absatz 1 Satz 1 Nummer 1 bis 6 bezeichneten Maßnahmen.

Sind mehrere Maßnahmen in einem engen zeitlichen Zusammenhang durchgeführt worden, so beginnt die in Satz 1 genannte Frist mit der Beendigung der letzten Maßnahme. Die richterliche Entscheidung ist vorbehaltlich einer anderen richterlichen Anordnung jeweils nach einem Jahr erneut einzuholen. Eine Benachrichtigung kann mit richterlicher Zustimmung frühestens nach dem Ablauf von fünf Jahren auf Dauer unterbleiben, wenn

1. überwiegende Interessen einer betroffenen Person entgegenstehen oder

2. die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden

und eine Verwendung der Daten gegen die betroffene Person ausgeschlossen ist. In diesem Fall sind die Daten zu löschen.

§ 48b
Aufsicht durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz über die Datenverarbeitung

(1) Unbeschadet anderer Regelungen dieses Gesetzes nimmt die oder der Landesbeauftragte für den Datenschutz im Rahmen der Aufsicht über die Datenverarbeitung zu Zwecken der Richtlinie (EU) 2016/680 die Aufgaben entsprechend Artikel 57 Absatz 1 Buchstabe a bis i und t der Verordnung (EU) 2016/679 wahr und übt die Befugnisse entsprechend Artikel 58 Absatz 1, Absatz 2 Buchstabe a und b sowie Absatz 3 Buchstabe a und b dieser Verordnung aus.

(2) Weitergehende Maßnahmen darf die oder der Landesbeauftragte für den Datenschutz im Anwendungsbereich der Richtlinie (EU) 2016/680 nur anordnen, wenn dies zur Abwendung einer nach Ausübung der Befugnisse nach Absatz 1 fortbestehenden wesentlichen Verletzung datenschutzrechtlicher Vorschriften erforderlich ist und die Aufgabenwahrnehmung durch die verantwortliche Stelle dadurch nicht wesentlich beeinträchtigt wird. Eine Löschung von personenbezogenen Daten darf nicht angeordnet werden.

(3) Unbeschadet der Bestimmungen in Absatz 1 und 2 kann die oder der Landesbeauftragte für den Datenschutz festgestellte Verstöße gegen Vorschriften über den Datenschutz im Anwendungsbereich der Richtlinie (EU) 2016/680 beanstanden und ihre Behebung in angemessener Frist fordern. Sie oder er kann die Rechts- und Fachaufsichtsbehörde hierüber

verständigen. Werden die beanstandeten Verstöße nicht behoben, kann sie oder er von den in Satz 2 genannten Stellen binnen angemessener Frist geeignete Maßnahmen fordern. Nach fruchtlosem Fristablauf kann die oder der Landesbeauftragte für den Datenschutz den Landtag und die Landesregierung verständigen.

(4) Übt die oder der Landesbeauftragte für den Datenschutz für die betroffene Person deren Rechte im Anwendungsbereich der Richtlinie (EU) 2016/680 aus, hat sie oder er die Rechtmäßigkeit der Verarbeitung zu überprüfen und die betroffene Person innerhalb einer angemessenen Frist über das Ergebnis dieser Überprüfung zu unterrichten oder ihr die Gründe mitzuteilen, aus denen die Überprüfung nicht vorgenommen werden kann. Hierbei ist die betroffene Person auf die Rechtsschutzmöglichkeiten gegen die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz hinzuweisen. Die Mitteilung an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese Stelle nicht einer weitergehenden Auskunft zustimmt. Die oder der Landesbeauftragte für den Datenschutz hat eine bei ihr oder ihm eingelegte Beschwerde über eine Verarbeitung, die in die Zuständigkeit einer Aufsichtsbehörde des Bundes, eines anderen Landes oder in einem anderen Mitgliedstaat der Europäischen Union fällt, unverzüglich an die zuständige Aufsichtsbehörde weiterzuleiten. Sie oder er hat in diesem Fall die betroffene Person über die Weiterleitung zu unterrichten und ihr auf deren Ersuchen weitere Unterstützung zu leisten.

(5) Die Aufsicht durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz im Anwendungsbereich der Richtlinie (EU) 2016/680 erstreckt sich nicht auf eine Datenverarbeitung, die gerichtlich überprüft wurde.

(6) Die oder der Landesbeauftragte für den Datenschutz führt zu den in § 46f Absatz 2 genannten Maßnahmen und zu Datenübermittlungen an Drittstaaten und weitere zwischen- und überstaatliche Stellen nach den §§ 39d bis 39h im Abstand von längstens zwei Jahren zumindest stichprobenartig Kontrollen durch. Dies gilt auch für Datenübermittlungen an Drittstaaten und weitere zwischen- und überstaatliche Stellen nach der Verordnung (EU) 2016/679.

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit etwa 166.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Stellungnahme

Die von mehreren Beschwerdeführern erhobene Verfassungsbeschwerde richtet sich unmittelbar gegen einfachgesetzliche Bestimmungen, die §§ 33 Abs. 2 S. 1, 3 i.V.m. 26a, 46a; 33c, 33d; 34; 35; 44; 48b SOG M-V.

Die angegriffenen Normen ermöglichen die verdeckte Ermittlung im öffentlichen Raum durch Aufnahmen, Ermittlungspersonal und Vertrauensleute sowie die verdeckte Überwachung von Wohnraum, Telekommunikation und informationstechnischen Systemen, ferner die offene Ermittlung durch unbemannte Flugobjekte, Ausschreibung und Rasterfahndung und regeln dahingehend den Schutz des Kernbereichs privater Lebensführung, die Befugnisse des/der Landesdatenschutzbeauftragten.

Die hier genannten einfachgesetzlichen Bestimmungen sind in der Anlage zu diesem Votum wiedergegeben.

Gerügt werden die Verletzungen folgender Grundrechte:

- Das Grundrecht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

- Das Grundrecht auf Sicherheit und Integrität informationstechnischer Systeme, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

- Das Grundrecht auf Unverletzlichkeit der Wohnung, Art. 13 Abs. 1 GG.

- Das Fernmeldegeheimnis, Art. 10 Abs. 1 GG.

Die Bundesrechtsanwaltskammer ist der Auffassung:

Soweit die Verletzung des Grundrechts auf Sicherheit und Integrität informationstechnischer Systeme gerügt wird, ist die Beschwerde unzulässig. Im Übrigen ist sie zulässig. Hierzu nachfolgend A.

Die Beschwerde ist teilweise begründet. Die Normen

- § 33 Abs. 2 S. 1 SOG M-V

- § 33 Abs. 2 S. 1, S. 3 i.V.m. § 67a Abs. 1 Nr. 1, § 67c Nr. 2 SOG M-V, soweit darin auf Vorfeldstraftaten verwiesen wird

- § 26a SOG M-V

- § 46a Abs. 2 S. 1 SOG M-V
- § 33b Abs. 1 S. 2 SOG M-V
- § 33c Abs. 1 S. 2, S. 4 und Abs. 5 SOG M-V
- § 33d Abs. 1 Nr. 2 und Abs. 3 S. 3 i.V.m. § 33c Abs. 5 SOG M-VSOG M-V
- § 34 Nr. 1, Nr. 2-5 i.V.m. § 32 Abs. 6 S. 1 SOG M-V
- § 35 Abs. 1 S. 1 HS 1, HS 2 Alt. 2, S. 2 SOG M-V
- § 44 Abs. 1 Nr. 1 SOG M-V

sind verfassungswidrig. Hierzu nachfolgend B.

Begründung:

Inhalt:

A. Zulässigkeit

I. Möglichkeit einer Grundrechtsverletzung gegeben

1. Informationelle Selbstbestimmung (Datenschutz)

Das Grundrecht auf informationelle Selbstbestimmung gewährleistet, dass Grundrechtsträger über die Erhebung, Speicherung und Verwendung personenbezogener Daten selbst entscheiden können.[1]. Durch jede polizeiliche Ermittlung werden Informationen über die jeweiligen Personen gesammelt und gespeichert, sodass eine Verletzung der Anforderungen an die Rechtfertigung eines Eingriffs durch die angegriffenen Normen §§ 33, 33b bis 33d, 34, 35 und 44 SOG M-V i.V.m. den jeweiligen Schutzvorschriften jedenfalls nicht ausgeschlossen werden kann.

2. Sicherheit und Integrität informationstechnischer Systeme

Durch die online-Überwachung, § 33c, sowie durch die Quellen-TKÜ, § 33d SOG M-V, soweit dabei die Nutzung persönlicher informationstechnischer Systeme gestattet wird, wird durch Hoheitsträger auf vernetzte Datenträger zugegriffen, die der Erzeugung, Speicherung und Verarbeitung von Daten dienen.[2] Damit ist jedenfalls nicht ausgeschlossen, dass das Grundrecht auf Sicherheit und Integrität informationstechnischer Systeme verletzt ist.

3. Unverletzlichkeit der Wohnung

§ 33b SOG M-V sowie die §§ 33c Abs. 5, 33d Abs. 3 S.3 i.V.m. 33c Abs. 5 SOG M-V wird das Betreten privater Wohnräumlichkeiten gestattet, sodass eine Verletzung des Grundrechts auf Unverletzlichkeit der Wohnung jedenfalls möglich erscheint.

4. Fernmeldegeheimnis

Soweit § 33d SOG M-V die Überwachung laufender Telekommunikation (TKÜ) gestattet, ist die Verletzung des Fernmeldegeheimnis aus Art. 10 Abs. 1 GG nicht schlechthin ausgeschlossen.[3]

II. Unmittelbare und gegenwärtige Selbstbetroffenheit

Zulässigkeitsfragen stellen sich bei der hier unmittelbar gegen ein Gesetz gerichteten Verfassungsbeschwerde sodann allenfalls im Hinblick auf das Merkmal der Unmittelbarkeit. Diese ist allerdings im Ergebnis unproblematisch gegeben:

Eine unmittelbare Betroffenheit liegt vor, wenn die angegriffene Maßnahme selbst ohne weiteren Durchführungsakt auf die Rechtsposition der Betroffenen einwirkt.[4] Es müssen durch das Gesetz selbst konkrete Rechtspositionen erlöschen oder Verpflichtungen begründet werden.[5] Eine Überprüfung gesetzlicher Vorschriften, die *eines* exekutiven Vollzugsakts bedürfen, ist nur zulässig, soweit der

[1] BVerfGE 78, 77 (84)
[2] BVerfG, 27.02.2008, NJW 2008, 822 (824f).
[3] BVerfG, 27.02.2008, NJW 2008, 822 (825, 835).
[4] vgl. BVerfGE 1, 97 (102f).
[5] BVerfGE 53, 366 (389).

Rechtsweg faktisch nicht offensteht oder der Verweis auf den Rechtsweg nach Umsetzung der Maßnahme nicht korrigierbare Grundrechtseingriffe mit sich brächte.[6] Bei größerer Streubreite der Maßnahmen steigt durch die Möglichkeit der zufälligen Miterfassung auch die Wahrscheinlichkeit der Betroffenheit für alle Bürger.[7]

1. Überwachungsmaßnahmen gem. §§ 33, 33b, 33c, 33d SOG M-V

Eine unmittelbare Betroffenheit liegt jedenfalls bei heimlich durchgeführten Überwachungsmaßnahmen schon dann vor, wenn eine zeitnahe Benachrichtigung der Betroffenen von der Durchführung der Maßnahme nicht zwingend erfolgt, und daher der Rechtsweg nicht, jedenfalls nicht zeitnah beschritten werden kann.[8] So liegt es im Wesentlichen -mit einigen Einschränkungen- hier.

Die Beschwerdeführenden legen überdies im Einzelnen im Wesentlichen dar, wenngleich mit Einschränkungen, von der angegriffenen Maßnahme mit einiger Wahrscheinlichkeit berührt zu werden:

a) Unmittelbare Betroffenheit in der Eingriffsdimension der gerügten Grundrechte

Die Beschwerdeführende zu 1 ist eine Anwältin, die berufsmäßig in Kontakt mit Personen steht, gegen die Strafverfahren und Ermittlungen wegen Verdacht der Begehung von Straftaten gem. § 67c SOG M-V (insb. § 89a StGB) geführt werden und bei der insb. die tatsachengestützte Annahme der Kenntnis von solchen Straftaten nach § 27a Abs. 3 Nr. 2 lit. a SOG M-V in Betracht kommt, sodass sie mit gegenüber der Gesamtbevölkerung signifikant erhöhter Wahrscheinlichkeit als Zielperson von Überwachungsmaßnahmen in Betracht kommt oder bei der Überwachung einer Zielperson miterfasst wird. Dabei sind sowohl die Überwachung nach § 33 Abs. 1 als auch die Überwachung der Kommunikation und Speichermedien im Arbeitsumfeld gem. §§ 33c und 33d SOG M-V realistischerweise denkbar. Auch die Miterfassung durch technische Wohnraumüberwachung gem. § 33b SOG M-V bei Treffen in privaten Räumen der Mandanten ist aufgrund des hohen persönlichen Kontakts wahrscheinlich.

Der Beschwerdeführer zu 2 steht als Journalist in vergleichbarem beruflichem Kontakt zu Personen, die dem extremen Spektrum zugeordnet werden können und ist damit mit der gleichen Wahrscheinlichkeit wie die Beschwerdeführerin zu 1 von heimlichen Ermittlungsmaßnamen betroffen.

Die Beschwerdeführerin zu 3 ist exponierte politische Aktivistin und bewegt sich bei der Organisation von Demonstrationen und politischen Protestaktionen typischerweise im Vorfeld möglicher Gefahren, die bei Versammlungen und Protestaktionen entstehen können. Für die Organisation politischer Aktionen ist ebenfalls breit gestreute Kommunikation und Vernetzung typisch. Damit bewegt sie sich jedenfalls in einem Umfeld, in dem Gefahrprävention realistischerweise eingreift. Zwar legt die Beschwerde nicht im Einzelnen dar, inwiefern die Beschwerdeführerin Zielperson von Maßnahmen werden könnte oder als Kontaktperson miterfasst werden könnte. Jedenfalls der Einsatz von V-Leuten und die Überwachung von Wohnraum und Telekommunikation in der betreffenden Szene erfassen faktisch alle Personen, die mit solchen Personen, die als extremistisch eingeschätzt werden, auf irgendeine Art in Kontakt stehen, und weisen somit eine hohe Streubreite auf, sodass von einer gesteigerten Wahrscheinlichkeit eines heimlichen Grundrechtseingriffs auszugehen ist.

Dahingegen ist die online-Durchsuchung typischerweise zielgenau auf ein informationstechnisches System beschränkt und erfasst ohne große Streubreite eine einzelne Person. Die Beschwerdeführerin

[6] BVerfGE 53, 366 (390).
[7] BVerfGE 125, 260 (305).
[8] BVerfGE 150, 309 (326); 141, 220 (261).

legt jedoch nicht dar, inwieweit sie einer dahingehend gesteigerte Wahrscheinlichkeit der Betroffenheit in Zusammenhang mit ihrem politischem Aktivismus ausgesetzt ist. Darlegungen der Selbstbezichtigung einer Straftat sind grundsätzlich nicht zu verlangen.[9]

Bei online-Durchsuchungen ist das Feld der Zielpersonen naturgemäß klein. Allerdings stehen den Betroffenen auch kaum Möglichkeiten zu Verfügung, ihre Betroffenheit anders geltend zu machen, als dadurch, dass sie durch soziale Kontakte und ein gewisses berufliches oder privates Umfeld in das Visier der Gefahrenabwehrbehörden kommen könnten. Personen, die nicht berufsmäßig mit möglichen Straftätern in Kontakt stehen und entsprechende Informationen speichern, müssten eigene Straftaten darlegen. Dieses Erfordernis ist nach der bisherigen Rechtsprechung des BVerfG jedoch ausgeschlossen.[10] Es ist hier jedenfalls aufgrund des Umfelds und der weit ins Vorfeld einer konkreten Gefahr verlagerten Möglichkeit des Eingriffs, und angesichts der auf effektiven Rechtsschutz angelegten Rechtsschutzgarantie gem. Art. 19 Abs. 4 GG eine unmittelbare Betroffenheit. Vorbeugender Rechtsschutz kommt mangels konkreter Maßnahme, der vorgebeugt werden soll, und im Einzelfall häufig schon wegen des fehlenden Wissens um die eigene bevorstehende Betroffenheit regelmäßig nicht in Betracht.

Die Beschwerdeführer zu 4 und 5 berufen sich auf ihre Kontakte in der Fußballszene. Wie die Szene des politischen Aktivismus ist das organisierte Fantum durch die im Zusammenhang mit Ausschreitungen und Straftaten auffällige Hooligan-Szene jedenfalls in Teilen ein realistisch denkbares Zielobjekt für polizeiliche Überwachungsmaßnahmen, sodass jedenfalls heimliche Maßnahmen mit großer Streubreite die Beschwerdeführenden zufällig miterfassen können. Für die Überwachung informationstechnischer Systeme gilt für Personen, die weiten Kontakt und Unterstützung für gewalttätig auffällige Fans pflegen, das oben gesagte. Eine unmittelbare Betroffenheit besteht hinsichtlich des Eingriffs in das IT-Grundrecht bei unzureichender Eingriffsschwelle.

b) Eingriff in das Grundrecht auf Sicherheit und Integrität informationstechnischer Systeme durch Verletzung einer Schutzpflicht

Die Beschwerdeführenden rügen darüber hinaus einen Eingriff in das sogenannte „IT-Grundrecht“ durch Verletzung einer staatlichen Schutzpflicht durch das Nutzen und Aufrechterhalten von Sicherheitslücken in der privat genutzten Software. Trotz dahingehendem besonderen Schutzbedürfnisses habe der mecklenburg-vorpommerische Gesetzgeber in Ermangelung eines ausreichenden Schwachstellenmanagements das Untermaßverbot verletzt.

Durch das Nutzen von Schwachstellen für die Infiltration technischer Systeme konkretisiert sich die allgemeine, den Grundrechten als objektiv-rechtliche Grundordnung innewohnende Verpflichtung zum Schutz der grundrechtlichen Freiheitsräume. Bürgerinnen und Bürger sind gegen Angriffe Dritter auf staatlich festgestellte und genutzte Schwachstellen zu schützen. Hierfür ist der Gesetzgeber gehalten, im Rahmen des Untermaßverbots zumindest eine geeignete Regelung zu schaffen, die den Zielkonflikt zwischen der Ermöglichung und Durchführung von online-Durchsuchungen zur Gefahrenabwehr und dem allgemeinen Schutzbedürfnis der Bevölkerung auflöst.[11] Dabei kommt es nicht auf eine über die grundsätzliche Betroffenheit als Opfer von Angriffen hinausgehende Individualisierung an. Die Beschwerdeführende sind ist bereits als Inhaber und Nutzer informationstechnischer Systeme betroffen.

[9] BVerfGE 109, 279 (308).
[10] BVerfGE 109, 279 (308).
[11] BVerfG, 08.06.2021, NVwZ 1361 (1364).

Eine Schutzpflicht ist erst dann verletzt, wenn der Gesetzgeber keine Regelung getroffen hat, oder die getroffene Regelung offensichtlich unzureichend ist und es dadurch zu einer unverhältnismäßigen Belastung kommt. Es kommt nicht auf das von der Beschwerde dargelegte besondere Schutzbedürfnis, sondern vielmehr auf das Fehlen oder die Untauglichkeit von schützenden Maßnahmen an.

Die Unmittelbarkeit ergibt sich nicht aus einem besonderen Schutzbedürfnis, das sich sich auf die besondere Betroffenheit der Überwachung durch ausländische Geheimdienste stützt. Die Unmittelbarkeit einer Beschwer ist grundsätzlich auch dann gegeben, wenn die Verletzung durch ausländische Staatsgewalt erfolgt, sodass im Inland kein Rechtsschutz gegeben ist.[12] Die maßgebliche Entscheidung des BVerfG bezieht sich jedoch auf ausländische Vollzugsakte. Das mögliche Ausnutzen von Schutzlücken durch internationale Geheimdienste erfolgt nicht im Vollzug eines internationalen Abkommens, sondern steht in dieser Hinsicht dem Handeln Privater gleich. Die Ausführungen können nicht die vertiefte, spezifische Auseinandersetzung mit dem zum Schutz getroffenen Regelungskomplex ersetzen.

Die Beschwerde nimmt eine solche Auseinandersetzung, die auch die Umsetzung der unionsrechtlichen Vorgaben der DSGVO und der JI-RL abhandeln müsste, im Rahmen der Zulässigkeit jedoch ebenso wenig vor wie bei der Feststellung des angeblich unzureichenden Schutzniveaus im Rahmen der Begründetheit. Zwar widmet sich die Beschwerde den Befugnissen des Landesdatenschutzbeauftragten und in diesem Rahmen auch der Umsetzung des einschlägigen Unionsrechts an anderer Stelle. Sie setzt sich jedoch nicht damit auseinander, inwiefern der Verarbeitungsvorgang, auf den sich die Verordnung 2016/679 bezieht, sowie das unionsrechtliche Regime der Folgenabschätzung nach Art. 27 der JI-RL (2016/680) eine Auslegung der §§ 48b ff SOG M-V gebietet, die ein ausreichendes Schutzniveau ergibt.[13]

Nicht zuletzt fehlt es an einer Auseinandersetzung mit anderen gesetzlichen Schutzbestimmungen wie des IT-Staatsvertrags und sonstigen landesrechtlichen und untergesetzlichen Regelungen. Zudem sind nach dem Grundsatz der Subsidiarität der Verfassungsbeschwerde Auslegungsfragen des einfachen Rechts zunächst vor den Fachgerichten zu klären. Im vorliegenden Fall erscheint es nicht aussichtslos, durch eine entsprechende Leistungsklage ein Urteil zu erwirken, das die Datenschutzpflichten und dahingehenden Befugnisse des / der Landesdatenschutzbeauftragten ausspricht.[14]

Eine unmittelbare Betroffenheit durch Verletzung einer Schutzpflicht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG hinsichtlich § 33c SOG M-V ist demnach nicht gegeben.

Somit ist die Beschwerde in dieser Hinsicht bereits nicht zulässig.

2. Sonstige Maßnahmen (§§34, 35, 44 SOG M-V) und Überwachung durch unbemannte Flugobjekte (Drohnen), § 34 SOG M-V, Ausschreibung zur polizeilichen Beobachtung und zur gezielten Kontrolle, § 35 SOG M-V, Rasterfahndung, § 44 SOG M-V

Schon die dauerhafte Möglichkeit, im öffentlichen Raum ohne besondere Ankündigung einer Überwachung ausgesetzt zu sein, der sich nicht entzogen werden kann, stellt eine unmittelbare Betroffenheit dar, derer es keine weiteren Vollzugsakte bedarf. Sie ergibt sich direkt aus dem Gesetz, das die Betroffenen – nämlich alle Personen, die sich im öffentlichen Raum aufhalten – zwingt, mit der dauerhaften Möglichkeit eines Eingriffs zu rechnen, dessen Vollzugsakt nicht von sonstigen Drohnen

[12] BVerfGE 6, 290 (295).
[13] BVerfG vom 08.06.2021, NVwZ 2021, 1361 (1366).
[14] vgl. dazu BVerfG, 08.06.2021, NVwZ 1361 (1368).

unterscheidbar und aufgrund der Unauffälligkeit der Fluggeräte ohnehin kaum wahrnehmbar erfolgt. Eine unmittelbare Beschwer liegt somit vor.

Die Ausschreibung, d.h. das Abspeichern von personenbezogenen Informationen in einer polizeilichen Datenbank, erfolgt zunächst verdeckt. Die Betroffenen wissen nichts von ihrer besonderen Stellung im Datensystem. Die besondere Durchsuchung und die gezielte Identitätsfeststellung und Durchsuchung von KFZ und der sich darin befindlichen Personen hingegen erfolgt offen. Allerdings erfolgt die Verwendung der dadurch gewonnenen personenbezogenen Daten ebenfalls verdeckt. Durch ihre beruflichen Kontakte und ihr soziales Umfeld stehen alle Beschwerdeführenden jedenfalls mit Menschen in Kontakt, die Zielperson einer Maßnahme nach § 35 Abs. 2 SOG M-V sein können. Selbst, wenn die Betroffenen von der Möglichkeit der Weitergabe und Verwendung ihrer Daten wissen, kann das Einlegen eines erfolgsversprechenden Rechtsmittels nicht schneller als die Verwendung der Daten erfolgen. Somit ist die Belastung der Beschwerdeführenden durch Maßnahmen nach § 35 Abs. 2 SOG M-V wahrscheinlicher als beim Durchschnitt der Bevölkerung, ohne, dass hinreichend Rechtsschutzmöglichkeiten bestehen. Eine unmittelbare Beschwer liegt vor.

Mit der Rasterfahndung kann die Polizei die Herausgabe von Daten anderer Behörden zur eigenen Verwendung verlangen. Der gesamte Vorgang erfolgt verdeckt und ohne Benachrichtigung der Betroffenen. Die Eingriffe sind allerdings auf Fälle von bevorstehender Gefahr oder im Vorfeld der Gefahr terroristischer Straftaten beschränkt. Die Daten von Kontaktpersonen dürfen nicht herausgegeben werden. Zwar bezeichnen sich die Beschwerdeführenden eher als Kontaktpersonen als Vorbereitende einer Straftat oder Gefahr iSv § 44 Abs. 1 SOG M-V. Die Selbstbezichtigung einer Straftat darf jedoch nicht verlangt werden (s.o.). Insgesamt ist nicht völlig unwahrscheinlich, dass die Prognosen der Polizei sich auch auf die Beschwerdeführenden richtet, die sich jedenfalls im Umfeld solcher bevorstehenden Gefahren bewegen. Eine Benachrichtigung und damit Rechtsschutzmöglichkeit ist erfolgt erst gem. § 46a SOG M-V nach Beendigung der Maßnahme und auch nicht ausnahmslos, sodass die Anforderungen an zeitnahen und lückenlosen Rechtsschutz nicht gewahrt sind

Im Ergebnis liegt also eine unmittelbare, gegenwärtige Betroffenheit in eigenen Rechten bei allen geltend gemachten Vorschriften vor mit Ausnahme der geltend gemachten Schutzpflichtverletzung im Rahmen der online-Durchsuchung.

Die geltend gemachten Verletzungen spezifischen Verfassungsrechts wirken allesamt verdeckt oder zumindest faktisch verdeckt. Die Klagebefugnis ergibt sich gerade aus den nicht hinreichenden Rechtsschutzmöglichkeiten.

A. Begründetheit

I. Eingriffsbefugnisse zur heimlichen Überwachung gem. § 33 SOG M-V

1. Eingriffsschwelle

§ 33 Abs. 1 SOG M-V gestattet den Einsatz heimlicher Ermittlungsmethoden, die von der längerfristigen Observation über die verdeckte Aufnahme von Bild und Ton bis hin zum Einsatz von V-Leuten und verdeckten Ermittlungspersonen reichen. Der Einsatz ist zulässig, wenn gem. § 33 Abs. 2 S.1 SOG M-V Tatsachen die Annahmen rechtfertigen, dass eine Straftat gem. § 49 SOG M-V begangen wird oder wenn im Vorfeld die Wahrscheinlichkeit besteht, dass eine wenigstens ihrer Art nach konkretisierte, zeitlich nahestehende und auf individualisierte Personen begrenzbare terroristische Straftat gem. § 67c

SOG M-V begangen wird oder anhand des individuellen Verhaltens prognostiziert werden kann, dass eine Person eine solche Straftat begehen wird (§ 67a Abs. 1 SOG M-V).

Das BVerfG leitet aus dem Grundsatz der Verhältnismäßigkeit Anforderungen an die Eingriffsschwelle polizeilicher Maßnahmen ab. Die Eingriffsschwelle bestimmt sich grundsätzlich im Verhältnis zu der Belastung der polizeipflichtigen Person und dem Gewicht der geschützten Rechtsgüter.[15] Jedenfalls ausreichend ist eine konkrete Gefahr. Eine konkrete Gefahr ist eine Sachlage, die bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens im Einzelfall in absehbarer Zeit mit hinreichender Wahrscheinlichkeit zu einer Verletzung des polizeilichen Schutzguts führt. Dabei sinken die Anforderungen an die Wahrscheinlichkeitsprognose, je gewichtiger das geschützte Rechtsgut ist. Allerdings muss jedenfalls der prognostizierte Kausalverlauf konkret sein. Die Gefahrenabwehr noch weiter im Vorfeld einer konkreten Gefahr ist jedoch zulässig, wenn entweder die Rechtsgutsverletzung an sich bereits wenigstens der Art nach konkretisiert ist, das Geschehen zeitlich absehbar ist und die Störenden wenigstens so weit individualisiert sind, dass eine gezielte Überwachung einzelner möglich ist.[16] Somit kommt es zumindest darauf an, dass nicht der gesamte Kausalverlauf in einer Prognose vorgezeichnet werden kann, aber zumindest eine Straftat der Art nach absehbar ist, somit das Ergebnis des Kausalverlaufs mit gewisser Wahrscheinlichkeit vorhergesagt werden kann. Es kommt darauf an, dass im Einzelfall an konkrete Umstände anknüpfend ein konkretisiertes Geschehen vorhergesagt werden kann. Ferner ist der Eingriff grundsätzlich, je nach Gewicht des gefährdeten Rechtsguts und Belastung des Einzelnen, auch zulässig, wenn das individuelle Verhalten einer Person die Prognose zulässt, dass sie terroristische Straftaten begehen wird.[17] Die personenbezogene Gefahrenprognose steht als eigene Kategorie neben der konkreten bzw. der drohenden Gefahr im Vorfeld der konkreten Gefahr.[18]

2. Eingriffsschwelle § 33 Abs. 2 S. 1 SOG M-V: Tatsachen, die die Annahme der Begehung von Straftaten iSv § 49 SOG M-V rechtfertigen

Die Beschwerdeführenden bringen vor, dass die Norm verfassungswidrige Eingriffe in Grundrechte zulässt, indem sie nicht ausschließt, dass sich die Gefahrprognose allein auf allgemeine Erfahrungssätze stützt. Somit liegt nach Ansicht der Beschwerde die Eingriffsschwelle so weit im Vorfeld einer konkreten Gefahr, dass ein in keiner Weise konkretisiertes Geschehen prognostiziert werden kann. Schon seien die geschützten Rechtsgüter nicht gewichtig genug, um eine Vorverlagerung der Gefahrenprognose überhaupt zu rechtfertigen.

Grundsätzlich erfordert die durch Tatsachen gerechtfertigte Annahme eine an Tatsachen, d.h. dem Beweis zugänglich Vorgänge der Vergangenheit oder Gegenwart, gestützte Prognose, dass eine Gefahr möglich ist. Möglicherweise ist § 33 Abs. 2 S. 1 SOG M-V dahingehend auszulegen, dass der Sache nach eine konkrete Gefahr erforderlich ist. Der Begriff wurde teilweise von Literatur und Rechtsprechung auf eine Schwelle verengt, die einer konkreten Gefahr zumindest ähnelt.[19] Unstrittig wird die Schwelle jedoch zumindest unterhalb der einer konkreten Gefahr angesiedelt. Eine verfassungskonforme Auslegung der jeweiligen Eingriffsnormen könnte jedoch eine Gefahrenschwelle ergeben, die den Anforderungen des BVerfG entspricht.

[15] BVerfGE 125, 260 (330); 141, 220 (271).
[16] BVerfGE 125, 260 (330); 141, 220 (272).
[17] BVerfGE 141, 220 (272 f).
[18] Zum Ganzen vgl. auch Schneider, NVwZ 2021, 1646 (1648).
[19] vgl. nur Graulich, in Lisken / Denninger, Handbuch des Polizeirechts, 2021, Rn. 134 ff; Albrecht, BeckOK PolR NS, zu § 32 NPOG; VG Hamburg, 02.10.2012, S K 1236/11.

Allerdings legt das BVerfG selbst den Begriff so aus, dass Tatsachen (nicht nur Vermutungen) erforderlich sind, auf die allgemeine Erfahrungssätze angewandt werden.[20] Auch vor dem Hintergrund des Bestimmtheitsgebots verlangt es, dass Eingriffsnormen so gefasst sind, dass ausgeschlossen ist, dass sich eine Prognose nur auf allgemeine Erfahrungssätze stützt.[21] Die fast wortgleich abgefasste Norm § 20g Abs. 1 Nr. 2 BAKG a.F. verwarf das BVerfG aufgrund der zu niedrig angesetzten Eingriffsschwelle.

Zudem liegt bei Auslegung der Norm im Kontext des SOG M-V die Annahme einer konkreten Gefahr oder wenigstens einer sich dem annähernden Eingriffsschwelle nicht nahe. So definiert § 67a SOG M-V für terroristische Straftaten eine Eingriffsschwelle im Vorfeld der Gefahr, die den Anforderungen des BVerfG dem Wortlaut nach entspricht, und dabei einen höheren Grad an Konkretheit des bevorstehenden Schadensereignisses fordert als die bloße Begehung von Straftaten. Bei Vergleich der geschützten Rechtsgüter liegt der Schluss, dass § 33 Abs. 2 S. 1 SOG eine höhere Eingriffsschwelle definieren soll, zwar nahe. Der Wortlaut gibt jedoch auch in Abgleich mit § 44 SOG M-V, der für die Rasterfahndung explizit eine „Gefahr“ verlangt, eine entsprechende Auslegung nicht her. Selbst bei entsprechender Auslegung im Einzelfall wäre es gerade für Laien unter keinen Umständen erkenntlich, welche Anforderungen bei der jeweiligen wahrscheinlichen Rechtsgutsverletzung erfüllt sein müssten. Die Definition der Eingriffsschwelle läge somit vollumfänglich in der Hand der Exekutive, sodass eine restriktive Auslegung von § 33 Abs. 2 S. 1 SOG M-V irgendwo zwischen dem Vorfeld der konkreten Gefahr und der konkreten Gefahr zwar theoretisch möglich wäre, das Ergebnis jedoch dem Bestimmtheits- und dem Wesentlichkeitsgrundsatz widerspricht.[22]

Letztlich erfordert die Eingriffsschwelle nach ihrem Wortlaut lediglich, dass überhaupt eine Straftat iSv § 49 SOG M-V auf Basis von beweisbaren Vorgängen der Vergangenheit oder Gegenwart angenommen werden kann. Dadurch wird zwar auf ein konkretes Geschehen im Einzelfall Bezug genommen. Es werden jedoch keinerlei Anforderungen an die Konkretheit der Prognose bzw. der Straftat aufgestellt. Auch in Ansehung der Rechtsprechung des BVerfG würde damit den Bürgerinnen und Bürgern das Risiko aufgebürdet, dass die Behörden die Norm nicht in engerer Auslegung in Vereinbarkeit mit den Anforderungen des BVerfG anwenden, sondern den weiten Prognoserahmen der Begehung irgendeiner Straftat in irgendeiner Form ausschöpfen und aus allgemeiner Erfahrung und allgemeinen Korrelationen aus Tatsachen auf eine nicht näher konkretisierte Zukunft schließen.

Somit ist festzuhalten, dass schon die Eingriffsschwelle nicht den Anforderungen genügt, die das BVerfG auch für den Schutz höchster, gewichtigster Rechtsgüter aufstellt. § 33 Abs. 2 S. 1 SOG M-V ist bereits aus diesem Grund unverhältnismäßig und damit verfassungswidrig.

Die Eingriffsnorm umfasst wie § 20g BKAG a.F. ein breites Spektrum an Befugnissen, die von geringer bis starker Intensität des Grundrechtseingriffs reichen, unter Umständen die Privatsphäre jedoch auch tief betreffen. Grundsätzlich sind neben den besonders gewichtigen, aufgeführten Rechtsgütern jedoch auch der Schutz von Vermögenswerten geeignet, einen solchen Eingriff zu rechtfertigen, soweit dieser im Kontext der Terrorismusabwehr relevant ist-[23] Vorliegend wurde jedoch für die Gefahrenbekämpfung im Rahmen der Terrorismusabwehr eine eigene Eingriffsschwelle definiert, sodass die Terrorismusabwehr für Eingriffe nach § 33 Abs. 1, 2 S. 1 SOG M-V gerade keine Grundvoraussetzung darstellt.

[20] BVerfGE 110, 33 (61).
[21] BVerfGE 141, 220 (291).
[22] vgl. auch BVerfG, 27.07.2005, NJW 2005, 2603 (2607).
[23] BVerfGE 141, 220 (287 f); 133, 277 (365).

Demnach reichen die von § 49 Nr. 2, 3 SOG M-V aufgeführten Straftaten nicht aus, um die tiefen Grundrechtseingriffe zu rechtfertigen. Eine Abstufung der Schutzgüter, die geeignet sind, Eingriffe von schwerer Intensität zu rechtfertigen, sieht der Landesgesetzgeber nicht vor. Eine entsprechende restriktive Handhabe der Norm wäre zwar grundsätzlich möglich, widerspricht jedoch wie die restriktive Auslegung der Gefahrenschwelle dem Bestimmtheitsgebot. Im Einzelfall wäre nie klar geregelt, welche Straftaten in welcher Begehungsform jeweils geeignet sind, einen Eingriff zu rechtfertigen, und somit die Voraussetzungen der Überwachung von den Betroffenen, aber auch von den Gerichten nicht eindeutig einzuschätzen. Die Voraussetzungen eines Grundrechtseingriffs sind nach dem Wesentlichkeitsprinzip gerade durch das Parlament zu regeln, sodass die Bestimmung von Inhalt, Zweck und Ausmaß des Eingriffs nicht der Exekutive überlassen wird.[24]

Somit ist § 33 Abs. 2 S. 1 SOG M-V auch unter diesem Aspekt verfassungswidrig.

3. Eingriffsschwelle bei terroristischen Straftaten, § 33 Abs. 2 S. 3 SOG M-V

Die Eingriffsschwellen für terroristische Straftaten des Katalogs gem. § 67c SOG M-V richten sich zwar nach dem Wortlaut des vom BVerfG verlangten Mindestniveaus für Eingriffsvoraussetzungen.

Im Kern kommt es darauf an, wie weit die Verletzung für das geschützte Rechtsgut eines Straftatbestands konkretisiert sein muss und wie weit die tatsächliche Verletzung absehbar sein muss. Bei der Prognose im Vorfeld der konkreten Gefahr kommt es darauf an, dass ein gefährdetes Rechtsgut der Art nach konkretisiert werden kann oder das individuelle Verhalten einer Person aussagekräftig auf die künftige terroristische Aktivität schließen lässt.

Vorbereitungsstraftaten wie § 89a StGB stellen Handlungen unter Strafe, die selbst lediglich in Verbindung mit einem entsprechenden subjektiven Tatbestand die Gefahr einer Rechtsgutsverletzung begründen. Die Anwendbarkeit der Eingriffsnormen des SOG M-V wird durch § 67c Abs. 1 SOG M-V nur insoweit eingeschränkt, dass die Straftat subjektiv einen terroristischen Hintergrund haben und objektiv zur Schädigung eines Landes oder des Bundes geeignet ist. Damit sind auch Vorfeldstraftaten uneingeschränkt erfasst, die gerade aufgrund der Art ihrer Begehung ein so erhebliches Schädigungspotential enthalten, dass die Strafbarkeit verfassungsrechtlich gerechtfertigt ist. In der Vorbereitungshandlung z.B. gem. § 89a StGB muss sich gerade die staatsschädigende Absicht des Täters manifestieren. Die staatsschädigende Straftat muss sich daher der Art nach schon konkretisiert haben.[25] Demnach ist der Anwendungsbereich der Norm sogar enger gefasst als die Definition der terroristischen Straftat gem. § 67c Abs. 1 SOG M-V, der keine weiter konkretisierte Absicht einer staatsschädigenden Straftat verlangt, sondern nur die Vorstellung und objektive Eignung einer Tat zur Schädigung eines Staats, eines Landes oder einer internationalen Organisation.

a) Anforderungen an die Prognose nach §33 Abs. 2 S. 3 i.V.m. §67a Abs. 1, § 67c SOG M-V

Die Prognose muss sich auf Straftaten beziehen, die jedenfalls einen terroristischen Hintergrund haben, d.h. in subjektiver Hinsicht dazu bestimmt sind, die Bevölkerung einzuschüchtern, und in objektiver Hinsicht eine erhebliche, potentielle schädigende Auswirkung haben[26]

Die besondere Gefahr der Vorbereitungsstraftaten und deren terroristischer Hintergrund ergibt sich erst aus der subjektiven Absicht des Täters / der Täterin, mit der Handlung einen Terrorakt vorzubereiten. Ein Durchschlagen auf die Prognose, um wie dargestellt das Mindestmaß an Wahrscheinlichkeit der

[24] BVerfGE 27.07.2005, NJW 2005, 2603 (2607).
[25] (zum Ganzen: BGH, 08.05.2014, 3 StR 243/13, insb. Rn. 27ff, 37, 41.)
[26] BeckOK PolR Nds/Ullrich NPOG § 2 Rn. 151-155.

Rechtsgutsverletzung herzustellen, kann sich daher überhaupt nur ergeben, wenn die innere Einstellung des Täters in dieser Prognose mitenthalten sein muss. Der Täter muss schon bei Begehung der Vorbereitungstat fest entschlossen sein, die terroristische Tat zu begehen.[27] Erst dann ist überhaupt eine abstrakte Rechtsgutsgefährdung in dem Maße festzustellen, dass eine Strafbarkeit der objektiv sozial adäquaten Handlung verfassungsrechtlich zu rechtfertigen ist.

Die Eingriffsschwellen sind grundsätzlich verfassungskonform, wenn die jeweilige Prognose geeignet ist, einen Eingriff aufgrund der Wahrscheinlichkeit der Rechtsgutsbeeinträchtigung zu rechtfertigen.

b) Prognose einer der Art nach konkretisierten Rechtsgutsverletzung in zeitlicher Nähe durch individualisierte Personen, § 67a Abs. 1 S. 1 Nr. 1 SOG M-V

Grundsätzlich bezieht sich eine Gefahr bzw. die Beurteilung im Vorfeld einer Gefahr auf den objektiv zu erwartenden Geschehensablauf. Die innere Einstellung der betroffenen Person kann aus objektiver Perspektive naturgemäß nicht abgeschätzt werden. Im vorliegenden Fall stößt der traditionelle Gefahrbegriff und somit die Beurteilung einer absehbaren Rechtsgutsverletzung an seine Grenzen, wenn sich die Rechtsgutsverletzung nicht aus dem objektiven Geschehensablauf ergibt, sondern aus der Person des Störers selbst. Die Gefahr liegt dann nicht im ungehinderten, natürlichen Fortlauf der Dinge begründet, sondern in persönlichen Eigenschaften und Absichten und den darin begründeten Verhaltensweisen eines Menschen. Diese sind denklogisch jedoch nicht objektiv vorhersehbar, wie es beispielsweise ein Schaden nach einem Verkehrsunfall mit überhöhter Geschwindigkeit wäre.

Wie auch in der Beschwerde dargestellt, versagt die hergebrachte Methode der Gefahrermittlung durch Prognose der Kausalzusammenhänge bei der Prognose menschlichen, ideologiegetriebenen Verhaltens. Niemand kann ernsthaft prognostizieren, ob der Kauf eines bestimmten brennbaren Mittels der Anschlagsvorbereitung dient oder lediglich etwa der Gartenarbeit etc.

Diese Grenze hat auch das BVerfG gesehen und in seinem Urteil zum BKAG berücksichtigt, indem es die Prognose einer bevorstehenden terroristischen Straftat anhand des individuellen Verhaltens einer Person zulässt (s.o.). Damit sind jedoch auch die Hürden für die Prognose einer Gefahr gesetzt, die sich aus dem individuellen Verhalten einer Person ergibt: Deren Eigenschaften und Neigungen müssen über einen längeren Zeitraum beobachtet und genau beurteilt werden. Eine andere Möglichkeit, auf die gefahrbringende innere Einstellung eines Menschen zu schließen, als ihn / sie umgangssprachlich „kennen zu lernen“, ist schlicht nicht vorstellbar. Angesichts des Gewichts der durch terroristische Straftaten geschützte Rechtsgüter ist allerdings auch ausgeschlossen, polizeiliche Prognosen auf diesem Gebiet trotz deren Fehleranfälligkeit vollständig zu verbieten. Im Umkehrschluss ist dann jedoch die Prognose einer der Art nach konkretisierten Straftat in zeitlicher Nähe durch eine irgendwie individualisierte Person wie in der Beschwerde dargestellt nicht möglich und verfassungsrechtlich unzulässig. Wenn die Hürden für die Beurteilung einer Gefahr, die sich aus dem Verhalten einer Person ergibt, in der Gefährderprognose liegen, kann eine darunter angesiedelte Eingriffsschwelle bei Gefahren, die sich aus dem subjektiven Tatbestand ergeben, nicht zulässig sein.

c) Gefährderprognose aufgrund des individuellen Verhaltens einer Person, § 67a Abs. 1 S. 1 Nr. 2 SOG M-V

Hier ist entscheidend, ob das BVerfG sich bei dem Begriff „terroristische Straftaten“ auch auf Vorbereitungshandlungen oder lediglich auf tatsächliche Verletzungen des Bestands und der Sicherheit einer Gebietskörperschaft der Bundesrepublik bezieht. In Abgrenzung zur oben dargestellten Prognose ergibt sich die Rechtfertigung für das Einschreiten aus dem individuellen Verhalten einer Person, das

[27] BGH, 08.05.2014, 3 StR 243/13, NJW 2014, 3459 (3456).

auf die Begehung einer terroristischen Straftat schließen lässt. Vorbereitungsstraftaten qualifizieren sich gerade dadurch, dass die Person eine terroristische Straftat fest beabsichtigt. Damit macht es im Ergebnis keinen Unterschied, ob sich die Prognose auf die Vorbereitungsstraftat in der festen Absicht der Begehung einer terroristischen Straftat oder auf den Terrorakt selbst bezieht. Lediglich der zeitliche Aspekt trennt die Vorbereitungstat von der tatsächlichen objektiven Rechtsgutsverletzung in subjektiver Hinsicht. Auch in praktischer Hinsicht wird sich die Ermittlung auf die tatsächliche Durchführung eines Terrorakts konzentrieren. Ob ein bestimmtes, zur Durchführung geeignetes Mittel erworben wird oder eine bestimmte Vereinigung gegründet wird, legt lediglich die zeitliche Nähe und stärkere Konkretisierung eines Plans für den Terrorakt nahe, entscheidend ist jedoch die Einschätzung der inneren Einstellung zur Durchführung dieses Terrorakts. Ist diese für eine Vorbereitungsstrafbarkeit ausreichend, ist sie auch ausreichend, die Wahrscheinlichkeit der tatsächlichen Durchführung bei ungehindertem Geschehensablauf zu begründen.

d) Verstoß der Verweisungsketten gegen das Gebot der Normklarheit

Die Beschwerdeführenden machen weiterhin geltend, dass die umfangreichen Verweisungsketten in §§ 33 Abs. 2, 67a, 67c SOG M-V, die weiterhin auf Normen des StGB verweisen, welche wiederum eigene Verweisungen enthalten, aufgrund der komplexen und unübersichtlichen Regelungstechnik nicht mehr den Anforderungen an Klarheit und Verständlichkeit von Normen entsprechen.

Verweisungsketten auch von einiger Komplexität sind allerdings grundsätzlich zulässig. Sie dürfen aber nicht zu Schwierigkeiten bei der Normanwendung führen, indem auf Normen verwiesen wird, die unterschiedliche Spannungslagen bewältigen. Dadurch ergeben sich Fragestellungen, in welchem Kontext die anzuwendenden Normen zu interpretieren sind und wie sich die unterschiedliche Zielsetzung im Einzelfall auswirkt, sodass eine klare Auslegung kaum mehr möglich ist.[28]

Vorliegend könnte der Verweis einer Eingriffsnorm im Rahmen und der Zielsetzung des Gefahrenabwehr auf Normen, die Vorbereitungshandlungen unter Strafe stellen, gegen das Gebot der Normklarheit und Bestimmtheit verstoßen. Wie bereits aus den unter c) dargestellten Auslegungsschwierigkeiten ersichtlich, ergeben sich erhebliche Probleme aus dem Verweis einer Befugnis, die sich auf eine objektive Prognose stützt, auf Straftaten in der Zukunft, deren Unrechtsgehalt wiederum schwerpunktmäßig in der Absicht liegt, die sich in einer eigentlich sozial adäquaten, für sich nicht rechtsgutsverletzenden Handlung manifestiert. Eine Prognose der künftigen inneren Einstellung ist faktisch nicht möglich und würde in einer völlig wahllosen Verfolgung möglicher Gesinnungen enden.

Jedenfalls die objektive Prognose des Kausalverlaufs nach § 67a Abs. 1 Nr. 1 SOG M-V lässt sich denklogisch nicht mit der Zielsetzung der Vorfeldstraftaten in Einklang bringen. Die Strafbarkeit ergibt sich hier aus dem zweifelsfreien Beweis des entsprechenden objektiven und subjektiven Tatbestands, während die Prognose gerade eine Wahrscheinlichkeitsüberlegung darstellt. Innere Einstellungen verlaufen jedoch nicht kausal und kalkulierbar. § 67a Abs. 1 Nr. 1 SOG M-V gibt auch keine weiteren Aufschlüsse über die Anforderungen an diese Prognose, die sich schon gem. § 67c Abs. 1 HS 2 Nr. 1 SOG M-V auf subjektive Tatbestandsmerkmale beziehen muss. Damit liegt jedenfalls in der Gefahrprognose eine nicht nur unverhältnismäßige Eingriffsschwelle, sondern auch eine Verweisung auf Normen, die miteinander nicht in Einklang zu bringen sind.[29]

§ 67a Abs. 1 Nr. 2 SOG M-V bezieht sich, wie dargestellt, auf das Verhalten einer Person und lässt somit Rückschlüsse auf deren innere Einstellung grundsätzlich zu. Die Norm begegnet jedoch ebenfalls Auslegungsschwierigkeiten, welche Anforderungen an diese Prognose zu stellen sind. Es bleibt bei dem

[28] BVerfGE 154, 154 (266); 110, 33 (57f).
[29] vgl. auch BVerfGE 110, 33 (58), BVerfG vom 26.04.2022, 1 BvR 1619/17 (zum bayVSG), Rn. 272.

Verweis einer Norm der Straftatenverhütung auf Normen, die sich auf einen abgeschlossenen, beweisbaren Lebenssachverhalt beziehen.

Das BVerfG stellt fest, dass eine Prognose, die sich lediglich auf die gerechtfertigte Annahme einer Planung stützt, nicht mit den Anforderungen an Normklarheit und Bestimmtheit vereinbar ist.[30] Allerdings folgt in der darauf folgenden Rechtsprechung die Feststellung, dass eine personenbezogene Gefährderprognose aufgrund des individuellen Verhaltens grundsätzlich zulässig ist (s.o.). Wie oben dargestellt, ist damit verlangt, dass sich die innere Einstellung bereits gebildet hat. § 67a Abs. 1 Nr. 2 SOG M-V stellt damit nicht wie Nr. 1 auf eine zukünftige, sondern auf eine bereits bestehende gefestigte Einstellung ab. Zusätzlich wird eine vertretbare Prognose einer tatsächlichen terroristischen Straftat verlangt. Somit kann jedenfalls unter Heranziehung der mittlerweile gefestigten Rechtsprechung des BVerfG zur Prognose im Vorfeld einer konkreten Gefahr grundsätzlich zweifelsfrei ausgelegt werden und erfüllt jedenfalls mittlerweile die Anforderungen an Normklarheit und Bestimmtheit.

4. Ergebnis

§ 33 Abs. 2 S. 1, S. 3 i. V. m. § 67a Abs. 1 Nr. 1, § 67c Nr. 2 SOG M-V, soweit darin auf Vorfeldstraftaten verwiesen wird, verstoßen gegen den Verhältnismäßigkeitsgrundsatz und stellen somit eine Verletzung des Rechts auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1, Art. 1 Abs. 1 GG dar.

5. Kernbereichsschutz

Der Kernbereichsschutz ist in § 26a SOG M-V allgemein geregelt und muss daher den höchsten Anforderungen genügen, die das BVerfG an den Schutz bei Eingriffen stellt, die der weitestgehenden Erfassung der Persönlichkeit dienen können (z.B. online-Durchsuchungen). Jedenfalls ist ein entsprechender Kernbereichsschutz auch bei Maßnahmen erforderlich, die wie die Eingriffsbefugnisse nach § 33 Abs. 1 SOG M-V tief in die Privatsphäre eindringen können.[31]

Das beabsichtigte, geplante Eindringen in den Kernbereich intimer Lebensführung ist unbedingt zu unterlassen. Besteht schon die Wahrscheinlichkeit, dass der Kernbereich bei der Überwachung erfasst wird, ist eine Maßnahme von vornherein unzulässig. Wenn es bei der Überwachung von Situationen, die nicht dem intimsten Lebensbereich zugerechnet werden, versehentlich zu einer Erfassung kommt, ist die Aufzeichnung unverzüglich abzubrechen. Eine weitere, automatische Aufzeichnung ist lediglich bei Zweifeln über den höchstpersönlichen Charakter der Kommunikation zulässig, wenn dabei auch die Durchführung von Straftaten besprochen wird.[32]

§ 26a Abs. 3 SOG M-V regelt den Abbruch von Maßnahmen hingegen nur unter der Bedingung, dass Ermittlungspersonen selbst oder der weitere Einsatz der Ermittlungspersonen nicht gefährdet werden. Die Überwachung im Kernbereich privater Lebensführung ist gem. § 26a Abs. 1 SOG M-V zwar grundsätzlich unzulässig. Die einmal begonnene Überwachung wird jedoch nur unter einem Gefährdungs- und Verwendungsvorbehalt abgebrochen und damit im Vorbehaltsfall wissentlich weitergeführt. Es wird somit eine Folgenabwägung angestellt zum Schutz der Individualrechtsgüter der Einsatzpersonen oder des Einsatzes an sich, also eines öffentlichen Interesses. Diese Erwägungen sind jedoch nicht vereinbar mit den Anforderungen, die das BVerfG an den Kernbereichsschutz stellt. Eine beabsichtigte Erfassung nach einer Abwägung ist schon mit dem absoluten Schutz der Intimsphäre als Ausfluss der Menschenwürdegarantie unvereinbar. Vielmehr ist eine Prognose anzustellen, ob bei künftigen Maßnahmen der Kernbereich betroffen wird. Schlägt sich schon darin die bloße

[30] BVerfGE 110, 33 (58).
[31] vgl. BVerfGE 141, 220 (295); BVerfG vom 26.04.2022, 1 BvR 1619/17 (zum BayVSG), Rn. 167.
[32] vgl. BVerfGE 141, 220 (295ff); BVerfG vom 26.04.2022, 1 BvR 1619/17, Rn. 272 ff.

Wahrscheinlichkeit des Betreffens nieder, ist die Maßnahme bereits unzulässig. Das Fortführen einer automatischen Aufzeichnung ist nur zulässig, wenn über den Charakter des Erfassten Zweifel bestehen. Dementsprechend ist das Fortführen einer Maßnahme, die mit absoluter Gewissheit den Kernbereich betrifft, unter keinen Umständen mit den Anforderungen der Verfassung vereinbar.

Somit entsprechen die heimlichen Überwachungsmaßnahmen gem. §§ 33 Abs. 1, 33b – 33d SOG M-V sämtlich unter dem Aspekt des Kernbereichsschutzes in materieller Hinsicht nicht den verfassungsrechtlichen Anforderungen.

§ 26a Abs. 4, Abs. 5 SOG M-V ordnet vor Verwendung die Sichtung durch eine datenschutzbeauftragte Person der Behörde an. Daten aus Wohnraumüberwachung sind durch einen Richter/eine Richterin vorab zu prüfen.

Nach der Rechtsprechung des BVerfG sind Informationen aus der Wohnraumüberwachung, die typischerweise den Kernbereich der privaten Lebensführung betreffen, grundsätzlich durch eine unabhängige Stelle zu sichten.[33] Unabhängige Stelle meint dabei eine Einrichtung, die von der Behörde derart getrennt ist, dass diese nicht in Kontakt mit den Informationen kommt, bevor sie freigegeben sind.[34] Eine solche Vorkehrung wurde mit § 26a Abs. 4 S. 1 SOG M-V geschaffen, sodass die Anforderungen auf der Verwertungsebene in verfahrensrechtlicher Hinsicht zunächst gewahrt scheinen.

Hinsichtlich der Überwachung gem. § 33 Abs. 1 SOG M-V entspricht die Norm somit den verfassungsrechtlichen Anforderungen an die verfahrensrechtliche Ausgestaltung der Verwertung.

6. Benachrichtigung, § 46a SOG M-V

Die Betroffenen sind gem. § 46a SOG M-V von der Durchführung heimlicher Maßnahmen zu benachrichtigen. Allerdings könnte der nach § 46a Abs. 2 SOG M-V zulässige Aufschub der Benachrichtigung die Rechtsschutzgarantie gem. Art. 19 Abs. 4 GG i. V. m. den jeweils berührten Grundrechten verletzen, wenn sie die Rechtsschutzmöglichkeiten unverhältnismäßig weit in die Zukunft verschiebt.

Ein Aufschub, bis der Zweck der Maßnahme, die daran beteiligten Personen oder die durch die Maßnahme geschützten Rechtsgüter nicht mehr gefährdet ist, ist nach der bisherigen Rechtsprechung des BVerfG jedoch zulässig.[35]

Die „weitere Verwendung“ kann in Abgrenzung zu den anderen Aufschubgründen nur meinen, dass Personen erneut bei künftigen Maßnahmen eingesetzt werden. Dadurch wird nicht mehr auf die laufende Maßnahme und das dadurch geschützte Rechtsgut Bezug genommen, sondern im Prinzip die Verfügbarkeit von Einsatzpersonal in der Zukunft für nicht weiter konkretisierte Zwecke geschützt. Dadurch wird faktisch dem unendlichen Aufschub der Benachrichtigung die Tür geöffnet: Die Möglichkeit des künftigen Einsatzes besteht, solange eine Ermittlungsperson aktiv ist. Diese Verwendung kann logischerweise dadurch gefährdet werden, dass Informationen über die Person des verdeckt Ermittelnden weiter getragen werden. Zwar lässt sich die „weitere Verwendung“ restriktiv dahin auslegen, dass eine konkrete Gefahr für die weitere Verwendung bestehen muss. Dies ist jedoch mit keinem Wort im Gesetz angedeutet.

---

[33] BVerfGE 141, 220 (301); zul. BVerfG am 26.04.2022, 1 BvR 1619/17, Rn. 282.
[34] BVerfGE 141, 220 (306ff).
[35] vgl. BVerfGE 125, 260 (344); 141, 220 (282).

Zwar lässt das BVerfG den Aufschub der Benachrichtigung grundsätzlich zu. Dabei muss jedoch die realistische Chance, absehbaren und effektiven Rechtsschutz zu erlangen, gewahrt bleiben. Dem entspricht die Abwägung nach § 46a Abs. 2 S. 2 SOG M-V nicht. Zudem ist die weitere Verwendung im Begründungskatalog des BVerfG weder aufgeführt, noch entspricht sie von der Konkretheit und Wahrscheinlichkeit der Rechtsgutsverletzung den aufgezählten Gründen, die auf die bereits laufende Maßnahme und die sich aus der Benachrichtigung im konkreten Fall ergebenden Gefahren abstellen.

7. Im Ergebnis:

Die Norm ist somit insoweit verfassungswidrig aufgrund des Verstoßes gegen Art. 19 Abs. 4 i. V. m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG.

Es besteht indes entgegen der Auffassung der Beschwerdeführer kein Verstoß gegen das Prinzip der Normenklarheit. Es ist klar zu entnehmen, dass § 46a Abs. 2 S. 1 SOG M-V eine gebundene Entscheidung regelt, während es in § 46a Abs. 2 S. 2 SOG M-V um eine Abwägung geht. Die Berücksichtigung von Belangen ist für Ermessensentscheidungen typisch. Diese Normstruktur, bei der ab einer bestimmten Schwelle die Entscheidung vorgegeben ist, während darunter eine Abwägung vorzunehmen ist, ist der Rechtsordnung nicht fremd und findet sich z.B. auch in § 35 Abs. 1 GewO. Sowohl der Tatbestand (Gefahr für die weitere Verwendung von Ermittlungspersonal) als auch die Rechtsfolge (Aufschub der Benachrichtigung) findet sich in der Formulierung und kann dem Zusammenhang der Sätze 1 und 2 entnommen werden. Ein Verstoß gegen das Gebot der Normklarheit liegt dagegen vor, wenn für Normanwendende nicht klar ersichtlich ist, welche Rechtsfolgen sich unter welchen Voraussetzungen ergeben können. Vor dem Hintergrund, dass Normen soweit wie möglich zunächst verfassungskonform auszulegen sind, ist ein Verstoß gegen das Gebot der Normklarheit aufgrund „schlampiger“, aber im Kontext klar verständlicher Formulierung nicht ersichtlich.

Im Ergebnis ist § 46a Abs. 2 S. 1 SOG M-V jedoch wegen Verstoßes gegen Art. 19 Abs. 4 i. V. m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG verfassungswidrig.

II. Wohnraumüberwachung, § 33b SOG M-V

§ 33b SOG M-V ermächtigt zur optischen und akustischen Wohnraumüberwachung bei Vorliegen einer gegenwärtigen Gefahr für Leib, Leben und Freiheit einer Person oder für den Bestand und die Sicherheit eines Landes oder des Bundes oder unter den Voraussetzungen des § 67a Abs. 1 SOG M-V.

1. Anforderungen an die Eingriffsschwelle

Wohnraumüberwachungen stellen einen besonders tiefgreifenden Eingriffs in die Privatsphäre dar und sind gem. Art. 13 Abs. 4 GG nur bei Vorliegen einer dringenden Gefahr zulässig. Die Rechtsgutsschädigung muss unmittelbar bevorstehen. Anderenfalls ist sie gerade nicht dringend. Darüber hinaus entspricht es einer dringenden Gefahr iSv Art 13 Abs. 4 GG, wenn die gesicherte Kenntnis von konkreten Vorbereitungshandlungen für näher qualifizierte terroristische Straftaten besteht.[36] [37]

[36] BVerfGE 141, 220 (298).

[37] Vgl. zum Ganzen BVerfGE 141, 220 (269ff, 297f); 130, 1 (32); BeckOK GG/Kluckert GG Art. 13 Rn. 19-20; Jarass/Pieroth GG Art. 13 Rn. 29, 30; MVVerfG LKV, 345ff.

2. Verfassungsmäßigkeit von §33b SOG M-V

Jedenfalls die in § 33b Abs. 1 S. 1 definierte Eingriffsschwelle der gegenwärtigen Gefahr für die aufgezählten, allesamt bedeutenden Rechtsgüter entspricht den Anforderungen des Art. 13 Abs. 4 GG.

Die Beschwerdeführenden machen geltend, dass sich die Verfassungswidrigkeit der Eingriffsbefugnis aus dem Verweis von § 33b Abs. 1 S. 2 auf § 67a Abs. 1 SOG M-V ergibt. Dadurch würde die Eingriffsschwelle unzulässig weit ins Vorfeld der geforderten konkreten Gefahr gerückt.

Der verfassungsgebende Gesetzgeber verwendet in Art. 13 Abs. 4 S. 1 GG das Wort „Gefahrenabwehr", während für sonstige Maßnahmen gem. Art. 13 Abs. 7 GG die „Verhütung" von Gefahren ausreicht. Damit muss ersichtlich eine gegenüber der bloßen Gefahrverhütung engerer Maßstab angelegt werden. Die Gefahrenabwehr stellt nach allgemeinem Verständnis auf die Abwehr einer bereits konkretisierten, unmittelbare bevorstehenden Gefahr ab.[38] Auch wenn das Einschreiten im Vorfeld einer konkreten Gefahr zugelassen werden würde, müsste sich jedenfalls die Rechtsgutsgefährdung der Art nach so weit konkretisiert haben, dass die Behörden eine konkrete Vorstellung des Geschehens haben, dass sie abzuwehren versuchen. Dem genügt die Prognose irgendeiner zukünftigen terroristischen Straftat allerdings nicht. Somit ist auch die Eingriffsbefugnis gem. § 67a Abs. 1 Nr. 2 SOG M-V in Ansehung der Wohnraumüberwachung verfassungswidrig.

III. Online-Durchsuchung, § 33c SOG M-V

§ 33c SOG M-V gestattet die online-Durchsuchung sowie die dafür notwendigen Wohnraumbetretungsrechte. Die Beschwerdeführenden greifen die aus ihrer Sicht unzureichende Eingriffsschwelle (1), den Einsatz gegen Dritte (2) sowie die Wohnraumbetretungsrechte (3) wegen Verstoß gegen Art. 2 Abs. 1, Art. 1 Abs. 1 und Art. 13 Abs. 1 GG an. Darüber hinaus machen sie eine Schutzpflichtverletzung geltend, die jedoch mangels ausreichendem Sachvortrag zum vorhandenen Schutzniveau unzulässig ist.

§ 33c Abs. 1 SOG M-V gestattet das verdeckte Durchsuchen von informationstechnischen Systemen bei Vorliegen einer Gefahr für Leib, Leben oder Freiheit einer Person sowie für den Bestand und die Sicherheit des Bundes, eines Landes oder die Existenz der Menschen. Darüber hinaus ist die Maßnahme unter den Voraussetzungen des § 67a Abs. 1 SOG M-V zulässig.

1. Eingriffsschwelle

Der Zugriff auf informationstechnische Systeme stellt einen Eingriff in das Grundrecht auf Sicherheit und Integrität informationstechnischer Systeme dar. Dieser ist bei präventiver Zielsetzung im Rahmen der Gefahrenabwehr von vornherein nur dann gerechtfertigt, wenn bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Es braucht eine wenigstens der Art nach konkretisierte, zeitlich absehbare Schädigung eines bedeutenden Rechtsguts durch wenigstens individualisierbare Personen, sodass ein gezielte Überwachung möglich ist.[39] In Bezug auf terroristische Straftaten stellt dem das BVerfG auch die Prognose der Begehung terroristischer Straftaten anhand des individuellen Verhaltens einer Person gleich.[40]

[38] vgl. MVVerfG, LKV 2000, 345 (351).
[39] BVerfGE 120, 274 (326, 328).
[40] BVerfGE 141, 220 (272f).

§ 33c Abs. 1 SOG M-V kopiert wortgleich die Eingriffsschwelle der konkreten Gefahr für ein bedeutendes Rechtsgut und ist insoweit verfassungsgemäß. Der Verweis auf § 67a Abs. 1 SOG M-V ist jedenfalls verfassungswidrig, soweit sich § 67a Abs. 1 Nr. 1 SOG M-V auf Vorfeldstraftaten bezieht (s.o.) mangels angemessener Eingriffsschwelle. In Bezug auf § 67a Abs. 1 Nr. 2 SOG M-V gilt das oben herausgearbeitete. Wie bei heimlichen Maßnahmen gem. § 33 Abs. 1 SOG M-V kann die online-Überwachung tief in die Privatsphäre eindringen. Dieser Eingriffsintensität wird jedoch Rechnung getragen, wenn die tiefe Überzeugung und die Absicht, eine terroristische Straftat zu begehen, festgestellt werden kann.

Somit ist § 33c Abs. 1 SOG M-V verfassungswidrig, soweit § 33c Abs. 1 S. 2, § 67a Abs. 1 Nr. 1 SOG M-V auf Vorfeldstraftaten gem. § 67c Abs. 1 Nr. 2 SOG M-V Bezug nehmen.

2. Einsatz gegen Dritte

Weiter bestimmt § 33c Abs. 1 S. 4 SOG M-V, dass sich der Eingriff auch gegen Dritte richten kann, die für die jeweilige Gefahr nicht verantwortlich sind, wenn Tatsachen die Annahme rechtfertigen, dass die verantwortliche Person auf den Geräten Dritter relevante Informationen speichert. Der Zugriff auf informationstechnische Systeme von Nicht-Störern ist jedoch nur dann erforderlich und damit verhältnismäßig, wenn der Zugriff auf die eigenen Geräte des Störers nicht ausreicht.[41] Dem jedoch genügt § 33c Abs. 1 S. 4 SOG M-V ersichtlich nicht.

Somit stellt die Erstreckung der online-Durchsuchung auf die informationstechnischen Systeme Dritter einen ungerechtfertigten Eingriff in Art. 2 Abs. 1, Art. 1 Abs. 1 GG dar und ist folglich verfassungswidrig.

3. Wohnraumbetretungsrechte

§ 33c Abs. 5 SOG M-V schließlich gestattet das heimliche Betreten von Wohnungen, um Zugang zu informationstechnischen Systemen zu erhalten und Überwachungssoftware zu installieren. Damit wird eine eigene Eingriffsbefugnis geschaffen, die über den Zugriff auf das informationstechnische System selbst hinausgeht und die sich an Art. 13 GG messen lassen muss. Diese Rechtsgrundlage ist auch erforderlich, weil es sich beim Betreten von Wohnraum zur Infiltration technischer Geräte mit Spähsoftware gerade nicht um eine zulässige Annexkompetenz handelt.[42]

Es handelt sich um das heimliche Betreten von Wohnraum, um zielgerichtet auf ein informationstechnisches System zuzugreifen. Somit könnte eine Form des Durchsuchens gem. Art. 13 Abs. 2 GG vorliegen. Eine Durchsuchung ist das ziel- und zweckgerichtete Suchen staatlicher Organe nach Personen oder Sachen oder zur Ermittlung eines Sachverhalts, um etwas aufzuspüren, was der Inhaber der Wohnung von sich aus nicht offen legen will.[43] Zwar dient auch das Betreten der Wohnung zum Zugriff auf ein informationstechnisches System dem ziel- und zweckgerichteten Suchen nach etwas. Allerdings kann das heimliche Betreten nicht unter Art. 13 Abs. 2 GG gefasst werden, wenn das Durchsuchen einer Wohnung offen erfolgen muss. Insbesondere stellt ein heimlicher gegenüber einem offenen Eingriff kein rechtliches Minus dar, sondern einen intensiveren Eingriff (siehe oben).

Nach Ansicht der Beschwerdeführenden kann eine Durchsuchung nach Art. 13 Abs. 2 GG nur eine offen durchgeführte Maßnahme sein. Kennzeichnend für eine Durchsuchung ist die Offenheit der

[41] BVerfGE 141, 220 (274).
[42] vgl. Derin/Golla, NJW 2019, 1111 (1112) mwN.
[43] BVerfGE 76, 83 (89).

Maßnahme.[44] Dieser Ansicht ist vor Änderung des BayPAG auch die bayerische Datenschutzbeauftragte.[45]

Anderer Ansicht ist dagegen die ehem. bayerische Justizministerin Merk.[46]

Im Vergleich zu den heimlich durchgeführten Maßnahmen nach Art. 13 Abs. 3 und 4 GG unterliegt die Durchsuchung einer geringeren Eingriffsschwelle. Eine dringende Gefahr ist nicht verlangt. Heimliche Maßnahmen sind jedoch grundsätzlich eingriffsintensiver als offen durchgeführte Maßnahmen, gegen die sich die betroffene Person unmittelbar wehren kann.[47] Nach dem allgemeinen Verständnis des Worts „Durchsuchung“, aber auch im Vergleich zu den weit höheren Anforderungen an heimlich durchzuführende Maßnahmen, die, offen durchgeführt, offensichtlich zwecklos wären, muss die Durchsuchung ein offen durchgeführter Eingriff sein.

Das heimliche Betreten von Wohnungen ist somit nicht von Art. 13 Abs. 2 GG umfasst.

Die Maßnahme lässt sich auch nicht als „Minus“ unter Art. 13 Abs. 4 GG fassen. Das BVerfG hat schon im Jahre 2008 dargelegt, dass die online-Durchsuchung an sich nicht von Art. 13 GG umfasst ist und das Grundrecht auf Sicherheit und Integrität informationstechnischer Systeme herausgearbeitet.[48] Das Betreten einer Wohnung, um die online-Durchsuchung zielgerichtet vorzubereiten, ist nicht im heimlichen Lauschangriff enthalten, der sich auf das Ausspähen der Wohnung an sich richtet. Im Gegensatz zu Maßnahmen, die das verdeckte Abhören gem. Art. 13 Abs. 3, 4 GG vorbereiten, lässt sich die Vorbereitung der online-Durchsuchung aufgrund der Möglichkeiten, außerhalb des Wohnraums oder digital auf das Endgerät zuzugreifen, nicht als notwendige, typische Annexmaßnahme qualifizieren.

Der Zugriff stellt auch keine sonstige Maßnahme gem. Art. 13 Abs. 7 GG dar. Darunter können nämlich nur Eingriffe gefasst werden, die ihrem Typus nach nicht den Eingriffsarten gem. Art. 13 Abs. 2-5 GG entsprechen. Eine dem Typ einer Durchsuchung entsprechende, aber heimlich durchgeführte Maßnahme lässt sich demnach nicht unter Art. 13 Abs. 7 GG fassen. Jedenfalls für Maßnahmen nach Art. 13 Abs. 2-5 GG kann auch keine verfassungsimmanente Rechtfertigung gefunden werden.[49]

Demnach ist das heimliche Betreten von Wohnraum zum Zweck der Vorbereitung der online-Durchsuchung schon von vornherein nicht zulässig.

Die Betretungsbefugnis gem. § 33c Abs. 5 SOG M-V stellt somit einen nicht zu rechtfertigenden Eingriff in Art. 13 Abs. 1 GG dar und ist daher verfassungswidrig.

4. Ergebnis

§ 33c Abs. 1 SOG M-V ist verfassungswidrig, soweit § 33c Abs. 1 S. 2, § 67a Abs. 1 Nr. 1 SOG M-V auf Vorfeldstraftaten gem. § 67c Abs. 1 Nr. 2 SOG M-V Bezug nehmen.

§ 33c Abs. 1 S. 4 und Abs. 5 SOG M-V sind verfassungswidrig.

---

[44] vgl. v. Mangoldt/Klein/Starck/Gornig GG Art. 13 Rn. 65; Eisenberg, NJW 1993, 1033 (1038) mwN.; Kutscha, NJW 2007, 1169 (1169).
[45] vgl. MMR 2008, IV (PM des bayLfD).
[46] vgl. MMR 2008, IV (PM des BayLMdJ).
[47] vgl. nur BGH, 31.01.2007, NJW 2007, 930 (951) mwN.
[48] BVerfGE 120, 274 (310f).
[49] vgl. v. Mangoldt/Klein/Starck/Gornig GG Art. 13 Rn. 148.

IV. TKÜ und Quellen-TKÜ, § 33d SOG M-V

Die Beschwerdeführenden machen geltend, dass die Eingriffsbefugnis zur Telekommunikationsüberwachung (TKÜ) und Quellen-TKÜ gem. § 33d SOG M-V aufgrund unverhältnismäßiger Eingriffsschwellen gegen das Fernmeldegeheimnis gem. Art. 10 Abs. 1 GG und das Grundrecht auf Sicherheit und Integrität informationstechnischer Systeme verstoßen. Darüber hinaus seien die Wohnraumbetretungsrechte verfassungswidrig und Schutzpflichten im Hinblick auf das Ausnutzen von Sicherheitslücken verletzt.

1. Verfassungsmäßigkeit von § 33d Abs. 1 SOG M-V

Die Erfassung laufender Telekommunikation und der Zugriff auf Endgeräte zum Zweck der Erfassung der laufenden Telekommunikation stellen einen Eingriff in Art. 10 Abs. 1 GG dar.[50]

a) Anforderungen an Eingriffe durch TKÜ / Quellen-TKÜ

Die TKÜ gem. § 33d Abs. 1, Abs. 2 SOG M-V greift die Inhalte und Umstände sowie die Standortdaten der Telekommunikation ab und stellt damit einen schwerwiegenden Eingriff in das Fernmeldegeheimnis dar.[51] Neben der heimlichen Überwachung vermeintlich vertraulicher und privater Kommunikation, des Kommunikationsverhaltens und der Bewegungsmuster, die tiefe Einblicke in die Persönlichkeit bietet, wird die Freiheit der Person auch mittelbar durch die Furcht vor möglicher heimlicher Überwachung beeinträchtigt. Zudem weist der Eingriff aufgrund der Vielzahl der kontaktierten unbeteiligten Personen eine hohe Streubreite auf.

Dieser schwerwiegende Eingriff kann zum Schutz ausreichend gewichtiger Rechtsgüter gerechtfertigt werden und ist nur bei einer adäquaten Eingriffsschwelle verhältnismäßig.

Die geschützten Rechtsgüter gem. § 33d Abs. 1 Nr. 1-5 SOG M-V umfassen Leib, Leben und Freiheit der Person sowie die Sicherheit und den Bestand des Bundes, eines Landes und die Existenz der Menschen. Auf diese Rechtsgüter beziehen sich auch die terroristischen Straftaten gem. § 33d Abs. 1 Nr. 2, § 67a Abs. 1, § 67c SOG M-V, sodass hinreichend gewichtige Rechtsgüter geschützt werden.

b) Bewertung der Verfassungsmäßigkeit von § 33d Abs. 1 SOG M-V

Jedenfalls die Eingriffshürde der Gefahr für ein bedeutendes Rechtsgut ist verfassungskonform. Darüber hinaus jedoch lässt § 33d Abs. 1 Nr. 2 SOG M-V auch die Datenerhebung in Fällen des § 67a Abs. 1 SOG M-V zu. Die Schwere des Grundrechtseingriffs entspricht mindestens der der heimlichen Überwachung; angesichts der großen Streubreite der Maßnahme und der vermeintlichen besonderen Vertraulichkeit des über Telekommunikationsmittel gesprochenen Worts ist eher von einem intensiveren Grundrechtseingriff auszugehen.[52] Jedenfalls die Eingriffsschwelle gem. §§ 33 Abs. 1 Nr. 2, 67a Abs. 1 Nr. 1, 67c Abs. 1 Nr. 2 SOG M-V ist somit verfassungswidrig, soweit sie sich auf Vorfeldstraftaten bezieht.

Das BVerfG hebt die Wohnraumüberwachung und die online-Durchsuchung als besonders tiefe Eingriffe in die Privatsphäre heraus, während die Telekommunikationsüberwachung lediglich einen

[50] BVerfGE 141, 220 (309).
[51] vgl. BVerfGE 113, 348 (382f) zu § 33a Nds. SOG a.F. mit vergleichbaren Befugnissen.
[52] vgl. Schneider, NVwZ 2021, 1646 (1648); BVerfGE 141, 220 (310, 316); 113, 348 (382).

schweren Eingriff darstellt. Diese sind grundsätzlich zur Abwehr terroristischer Gefahren, also für den Bestand der Rechtsordnung und der Stabilität und des Zusammenhalts der Gesellschaft schlechthin, auch bei verhaltensbezogener Prognose einer nicht weiter konkretisierten Rechtsgutsverletzung möglich. Darüber hinaus verspricht gerade die Kommunikation einer Person, die berechtigter weise als Gefährder eingestuft werden kann, besondere Erkenntnisgewinne zur Verhütung terroristischer Straftaten, die schon aufgrund ihrer Schwere nicht alleine geplant werden können. Auch im Einzelfall muss daher die Privatsphäre einer Person, der aufgrund konkreter Tatsachen und Verhaltensweisen ein besonders hohes Potential terroristischer Aktivitäten zugesprochen wird, hinter dem Bestand der freiheitlich-demokratischen Gesellschaft an sich zurückstehen. Auch Vorfeldstraftaten weisen bereits ein hinreichendes Gefährdungspotential auf, wenn die Überzeugung der Person, einen Anschlag zu begehen, bereits aufgrund ihres Verhaltens feststellbar ist.

Somit ist die Eingriffsschwelle der individuellen Prognose verfassungsrechtlich haltbar. § 33d Abs. 1 Nr. 2 SOG M-V ist insoweit verfassungskonform.

§§ 33d Abs. 1 Nr. 2, 67a Abs. 1 Nr. 1, 67c Abs. 1 Nr. 2 SOG M-V ist jedoch verfassungswidrig, soweit sich der Eingriff auf Vorfeldstraftaten bezieht. Zwar weisen die Eingriffe eine stärkere Intensität auf als die übrigen heimlichen Überwachungsmaßnahmen. Eine mit Art. 13 Abs. 4 GG vergleichbare Intensität und damit Anforderungen an die Schranke bestehen jedoch nicht.

2. Verfassungsmäßigkeit von § 33d Abs.2 S.2 SOG M-V

Nach Ansicht der Beschwerdeführenden stellt der durch § 33d Abs. 2 S. 2 SOG M-V zugelassene Zugriff auf informationstechnische Systeme und die sich daran anschließende, umfassende Datenauswertung einen mit der online-Durchsuchung vergleichbaren Eingriff dar und verletzt Art. 2 Abs. 1, Art. 1 Abs. 1 GG.

a) Schutzbereich des Grundrechts auf Sicherheit und Integrität informationstechnischer Systeme

Soweit sich die staatliche Maßnahme darauf beschränkt, die Inhalte und Umstände der laufenden Kommunikation bzw. darauf bezogene Daten auszuwerten, ist der Eingriff an Art. 10 Abs. 1 GG zu messen. Dies gilt grundsätzlich auch dann, wenn die Auswertung durch Zugriff auf ein informationstechnisches System erfolgt. Der Schutzbereich des Grundrechts auf Sicherheit und Integrität informationstechnischer Systeme ist erst dann eröffnet, wenn der Zugriff auf das informationstechnische System auch solche Daten erfasst, die nicht bloß Inhalte und Umstände der laufenden Kommunikation sind, sondern im System gespeicherte Informationen. Es reicht, dass grundsätzlich die Möglichkeit besteht, diese Informationen auszuwerten. Diese Daten können grundsätzlich durch eine Software geschützt werden und sind somit vertraulicher als die laufende Kommunikation, befinden sich aber außerhalb des von Art. 10 Abs. 1 GG umfassten Gefährdungsbereichs und fallen daher nicht unter den Schutz des Fernmeldegeheimnisses. Greift eine TKÜ als Quellen-TKÜ auf das gesamte Endgerät zu und ist grundsätzlich geeignet, die darauf gespeicherten Daten auswerten, ist neben dem Fernmeldegeheimnis auch das IT-Grundrecht aus Art. 2 Abs. 1, Art. 1 Abs. 1 GG betroffen, weil die Gefährdungslage vom Schutz der laufenden Kommunikation nicht mehr ausreichend umfasst ist.[53]

§ 33d Abs. 3 S. 2 SOG M-V bestimmt, dass neben dem Abhören der laufenden Kommunikation durch Zugriff auf informationstechnische Systeme auch die darauf gespeicherten Daten über Inhalte und Umstände der Kommunikation ausgewertet werden dürfen, solange sichergestellt ist, dass diese auch als laufende Kommunikation hätte aufgezeichnet werden dürfen. Zwar ist es zutreffend, dass bei korrekt

[53] vgl. zum Ganzen BVerfGE 120, 274 (307f).

ausgeführter Infiltration und nach Sortierung der Information nach Zeit der Speicherung und Art der Information nur Daten abgegriffen würden, die auch als laufende Kommunikation hätten aufgezeichnet werden dürfen. Allerdings besteht jedenfalls die Gefahr, dass bei einmal erfolgter Infiltration des informationstechnischen Systems auch andere Daten ausgewertet werden. Ist das System einmal angegriffen in der Weise, dass auch auf gespeicherte Informationen zugegriffen werden kann, kann die Malware theoretisch so programmiert und aufgespielt werden, dass nur bestimmte Daten davon erfasst werden. Jedenfalls bei der Überwachung laufender Kommunikation sind Sicherheit und Integrität des informationstechnischen Systems nicht betroffen, wenn technisch sicher gestellt wird, dass das System im Übrigen nicht durchsucht wird.[54] Allerdings erlaubt § 20l BKAG a.F. nur die Überwachung laufender Kommunikation, nicht das Erfassen von Daten, die als laufende Kommunikation hätten überwacht werden dürfen, wenn zu diesem Zeitpunkt schon ein Eingriff angeordnet worden wäre. Es kommt im Ergebnis darauf an, ob es technisch möglich ist, sicher zu stellen, dass nur die Daten laufender Kommunikation rückwirkend überwacht werden.

Nach der gesetzgeberischen Konzeption ist der Zugriff auf sonstige Daten nicht zulässig. Dies technisch sicher zu stellen und ein Übergreifen auf den restlichen Datenbestand zweifelsfrei auszuschließen, bleibt eine Herausforderung der Normanwender und ist von diesen zu bewältigen. Auch das irrtümliche Auslesen von Daten mit falschem Zeitstempel muss von den Normanwendern ausgeschlossen werden, soweit Daten, die mit falschem Zeitstempel abgespeichert wurden, technisch überhaut denkbar sind.

Es trifft nicht zu, dass eine eventuelle technische Unmöglichkeit, von vorneherein nur auf bestimmte Daten zuzugreifen und diese auszuwerten, notwendigerweise zu Lasten der Betroffenen geht.[55] Darüber hinaus ist der Zugriff auf nur einen bestimmten Teil der Festplatte und einen bestimmten Dateienpfad ohne Kenntnisnahme von den restlichen Daten nicht schlechthin ausgeschlossen. Nur unter dieses Voraussetzungen kann ein Eingriff gem. § 33d Abs. 2 S.2 SOG M-V überhaupt erfolgen, denn beim Handeln aufgrund dieser Rechtsgrundlage bleibt jede Durchsuchung auf die Daten laufender Kommunikation beschränkt. Besteht die Gefahr der weitergehenden Erfassung sonstiger Daten, muss der Eingriff auf § 33c Abs. 1 SOG M-V gestützt werden. Die laufende Kommunikation unterfällt gerade dem Schutzbereich des Fernmeldegeheimnisses, sodass der Eingriff an Art 10 Abs. 1 GG zu messen ist und nicht am Recht auf Sicherheit und Integrität informationstechnischer Systeme.[56]

Darüber hinaus machen die Beschwerdeführenden eine Verletzung des Grundrechts auf Sicherheit und Integrität informationstechnischer Systeme durch Schutzpflichtverletzung wegen eines unzureichenden Schutzniveaus geltend. Dahingehend fehlt es jedoch bereits an der Beschwerdebefugnis mangels Darlegung der unmittelbarer Betroffenheit der Beschwerdeführenden.

Jedenfalls ist die Rüge nicht substantiiert. § 48b Abs. 2 S. 1 und Abs. 3 S. 1 SOG M-V beziehen sich im Rahmen der Beanstandungsbefugnis des / der Landesdatenschutzbeauftragten explizit auf die Durchsetzung der JI-RL. Art. 27 RL 2016/680 bestimmt, dass bei der Verwendung risikoreicher Technologien vorab eine Datenschutzfolgenabschätzung erfolgen muss. Dies umfasst in unionsrechtsfreundlicher Auslegung den Erhalt des von der JI-RL geforderten Schutzniveaus für alle möglicherweise betroffenen Personen.[57] Mit der, wenn auch zur Überwachungstätigkeit nach § 48b Abs. 1 SOG M-V subsidiären, eigenen Anordnungsbefugnis und der Beanstandungsbefugnis zu den Aufsichtsbehörden und, bei deren Untätigkeit, zu Landesregierung und Landesparlament, hat der

[54] BVerfGE 141, 220 (312).
[55] vgl. dazu auch BVerfGE 141, 220 (311f).
[56] so auch Graulich, Lisken/Denninger, Handbuch des Polizeirechts, Rn. 784ff., vgl. zum vergleichbaren Eingriff gem. §100a Abs. 1 S. 3 StPO im Rahmen repressiver Strafverfolgung BeckOK StPO/Graf StPO § 100a Rn. 123 f, 127.
[57] BVerfG, 08.06.2021, NVwZ 1361 (1366).

Landesgesetzgeber eine Anordnung zum Schutz der Sicherheit und Integrität informationstechnischer Systeme getroffen, die insgesamt jedenfalls nicht völlig ungeeignet erscheint.

§ 33d Abs. 2 S. 2 SOG M-V ist somit unter dem Aspekt der Schutzpflichtverletzung nicht zu beanstanden.

b) Vereinbarkeit mit Art. 10 Abs. 1 GG

Die Eingriffsbefugnis stellt hier keinen rechtswidrigen Eingriff in Art. 10 Abs. 1 GG dar, auch soweit sie die Erfassung von Kommunikationsdaten zulässt, die vor Erlass des richterlichen Beschlusses aufgezeichnet wurden. Dadurch wird der Zugriff auf die gesamte vergangene Kommunikation ermöglicht, solange feststeht, dass zum Zeitpunkt der Kommunikation die Eingriffsvoraussetzungen gem. § 33a Abs. 1 SOG M-V vorgelegen hätten. Ein richterlicher Beschluss muss zu dem Zeitpunkt, zu dem die Kommunikation stattgefunden hat, nicht vorgelegen haben, sondern lediglich zum Zeitpunkt der Maßnahme. Die Parallelvorschrift der StPO gestattet gem. § 100a Abs. 1 S. 3, Abs. 5 S. 1 Nr. 1 Lit. b StPO nur das Erfassen von Informationen über Kommunikation, die nach der richterlichen Anordnung stattgefunden hat. Eine entsprechende Vorschrift fehlt im SOG M-V. Allerdings ist in Art. 10 GG kein Richtervorbehalt normiert. Jedes Erfassen vergangener Kommunikation muss auch den Eingriffshürden entsprechen. Dadurch ist sichergestellt, dass das Auswerten vergangener laufender Kommunikation der Abwehr einer aktuellen Gefahr dient. Folglich ist jeder Zugriff auf vergangene Kommunikation im Lichte einer aktuellen Gefahr zu rechtfertigen, was ein ausuferndes Abhören vergangener Kommunikation verhindert. Für die Betroffenen macht es angesichts der Heimlichkeit der Maßnahme keinen Unterschied, ob der Eingriff vor oder nach der gelaufenen Kommunikation angeordnet wurde. Ein unverhältnismäßiger Eingriff ist somit nicht festzustellen.

c) Zwischenergebnis

§ 33d Abs. 2 S. 2 SOG M-V ist für sich genommen nicht verfassungswidrig.

V. Wohnraumbetretungsbefugnis gem. § 33d Abs. 3 S. 3 i.V.m. § 33c Abs. 5 SOG M-V

Für die Wohnraumbetretungsbefugnis gem. § 33d Abs. 3 S. 3 i.V.m. § 33c Abs. 5 SOG M-V zum Zeck des physischen Zugriffs auf ein informationstechnisches System gilt das bereits oben gesagte. Die Norm ist verfassungswidrig wegen Verstoß gegen Art. 13 Abs. 1 GG.

VI. Einsatz unbemannter Luftfahrsysteme, § 34 SOG M-V

Die Beschwerdeführenden bringen vor, dass die Befugnis zum Einsatz unbemannter Luftfahrsysteme (Drohnen) verfassungswidrig ist, soweit dadurch die verfassungswidrigen Eingriffe nach §§ 33, 33b – 33d SOG M-V ermöglicht werden. Darüber hinaus sei die Erhebung von Bild- und Tonaufnahmen an öffentlich zugänglichen Veranstaltungen und Ansammlung verfassungswidrig.

1. Drohneneinsatz zur heimlichen Überwachung

§ 34 Nr. 2–5 SOG M-V verweist u.a. auf die §§ 33, 33b-33d SOG M-V, sodass die Verfassungswidrigkeit dieser Normen auch auf den Drohneneinsatz durchschlägt, soweit sie festgestellt wurde.

2. Aufnahmen an öffentlich zugänglichen Orten

Die Aufnahmen gem. § 34 Nr. 1 SOG M-V könnten das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1, Art. 1 Abs. 1 GG verletzen. Dabei kommen ein Mangel an effektivem Rechtsschutz sowie ein Verstoß gegen den Verhältnismäßigkeitsgrundsatz in Betracht.

a) Informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung als Ausfluss des allgemeinen Persönlichkeitsrechts gewährleistet das Recht, über die Erfassung, Speicherung und Verwendung personenbezogener Daten selbst zu entscheiden. Daneben kommt bei Bildaufzeichnungen das Recht am eigenen Bild in Betracht, wobei dieses ebenfalls eine Ausprägung des allgemeinen Persönlichkeitsrechts ist, sodass eine Abgrenzung dahinstehen kann.

Durch die Bild- und Tonaufnahmen werden Menschen schwerpunktmäßig in großen Mengen und aus größerer Entfernung erfasst. Jedenfalls durch das Aufzeichnen und Speichern der Aufnahmen von Personen, deren Identität durch moderne Gesichtserkennungssoftware bestimmbar ist, werden personenbezogene Daten generiert und verwendet.[58]

Möglicherweise stellt der Einsatz von Drohnen zur bloßen Beobachtung mangels Individualisierung und personenbezogener Erfassung durch die Fluggeräte selbst gar keinen Grundrechtseingriff dar. Dagegen spricht jedoch, dass die beobachteten Personen, gerade bei stetig verbesserter technischer Qualität der Aufzeichnungen, jedenfalls bestimmbar sind. Die Drohnen können als Augen und Ohren der Sicherheitsbehörden genutzt werden, sodass die beobachteten Personen tatsächlich auch von Beamten und Beamtinnen wahrgenommen werden. Insbesondere durch moderne Gesichtserkennungssoftware ist die Anonymität der erfassten Personen nur noch eine Illusion. Somit stellt schon das bloße Beobachten und Belauschen von Menschen durch Drohnen einen Eingriff in Art. 2 Abs. 1, Art. 1 Abs. 1 GG dar. Darüber hinaus entfaltet schon die Möglichkeit, aufgezeichnet zu werden, einen gewissen Verhaltensdruck, der wenigstens mittelbar in die allgemeine Handlungsfreiheit eingreift. Allein das Gefühl, überwacht zu werden, generiert den Druck, sich in vorauseilendem Gehorsam in rechtlicher wie moralischer Hinsicht möglichst regelkonform zu verhalten.[59]

b) Verletzung informationelle Selbstbestimmung und Unverhältnismäßigkeit

Die Beschwerdeführenden machen geltend, dass die Maßnahme unverhältnismäßig ist. Sie stellt darauf ab, dass die Maßnahme aufgrund ihrer hohen Streubreite und faktischen Heimlichkeit ohne Benachrichtigung jedenfalls in Fällen des § 32 Ab. 6 S. 2 SOG M-V unangemessen tief in das Recht der Betroffenen auf informationelle Selbstbestimmung eingreift.

Wenn die heimliche Überwachung grundsätzlich zulässig ist, ist selbst bei späterer Benachrichtigung der Betroffenen dadurch die jederzeitige Möglichkeit gegeben, im öffentlichen Raum überwacht zu werden. Insbesondere der Drohneneinsatz bei Ansammlungen erfasst jede zufällige Zusammenkunft mehrerer Menschen, wie sie im Alltag häufig vorkommt. Zwar geschieht die Überwachung nicht absichtlich verdeckt, dennoch häufig nicht erkennbar.[60] Dies spiegelt sich auch in der Benachrichtigungspflicht gem. § 32 Abs. 6 S. 1 SOG M-V.

---

[58] BVerfGE 120, 378 (397ff); 122, 348 (368).
[59] vgl. dazu auch Zöller/Ihwas, NVwZ 2014, 408 (409f).
[60] vgl. Roggan, NVwZ 2011, 590 (591).

Auf der anderen Seite dient die Überwachung der Prävention von Straftaten im Allgemeinen und damit der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie dem Schutz der Individualrechtsgüter. Allerdings müsste in einem Szenario, in dem wirksam Straftaten verhindert werden, tatsächlich eine dauerhafte und weitgehend lückenlose Überwachung des öffentlichen Raums angedacht sein. Denn Szenarien, die besonders anfällig für Eskalation und Gewalttaten sind, z.B. Ansammlungen einer Vielzahl an Menschen, werden typischerweise ohnehin schon von Streifenwagen und Polizeieinsätzen begleitet. Durch die Präsenz von Polizeibeamten und -beamtinnen und die sofortige Möglichkeit zum Eingreifen wird die Begehung von Straftaten darüber hinaus auch wirkungsvoller verhindert.

Durch die jedenfalls potentielle dauerhafte Überwachung verbleibt außerhalb der eigenen Wohnung kein Raum mehr, in dem Bürgerinnen und Bürger unbefangen und ohne die Angst vor staatlicher Bewachung zusammenkommen können. Dabei geht mit der Beobachtung jedenfalls im Alltagsleben auch die Bewertung und moralische Beurteilung des eigenen Verhaltens einher. Bürgerinnen und Bürger werden nicht zwischen staatlicher, vermeintlich neutraler und automatisierter Beobachtung ohne moralische Bewertung des Verhaltens und dem Gefühl, von Mitmenschen beobachtet zu werden, unterscheiden. Es bleibt das ständige Gefühl, nicht alleine zu sein, und das entsprechende Verhalten in vorauseilendem Gehorsam aus Angst, Fehler zu begehen. Damit entfaltet die Möglichkeit der heimlichen Überwachung genau wie die offene Überwachung einen erheblichen Eingriff in das Persönlichkeitsrecht und die allgemeine Handlungsfreiheit. Wenn die unbefangene Interaktion zwischen Menschen nicht mehr möglich ist, kann das erhebliche Konsequenzen auch für Begegnungen im öffentlichen Raum und damit für das gesellschaftliche Zusammenleben insgesamt haben. Im schlimmsten Fall könnte sich die unbefangene Interaktion und das gesellschaftliche Leben vollständig in private Räume verlagern, in denen sich die Menschen unbeobachtet und daher wohler fühlen – selbst, wenn sie keine Nachteile aufgrund bestimmter politischer Einstellungen, die im Widerspruch zu aktuellen Regierung stehen, befürchten. Ein gesellschaftliches Zusammenleben und damit auch die freie politische Meinungsbildung, Austausch und Debatten über bestehende gesellschaftliche Zirkel und Schichten hinweg ist dann kaum mehr möglich. Bei ständiger Anwesenheit der staatlichen Hoheitsgewalt leidet im Ergebnis auch die Demokratie an sich.[61]

Darüber hinaus kann durch die Beobachtung von Ansammlung und öffentlichen Veranstaltungen durch die Überwachung auch ein Persönlichkeitsprofil der Personen erstellt werden, die in ihrem Bereich besonders aktiv sind und daher häufig prominent auf solchen Aktionen auftreten. Durch die Aufzeichnung von Veranstaltungen können Profile bereits erstellt werden, sobald sie einmal erfasst wurden. Dann kann eine Gesichtserkennungssoftware die jeweilige Person immer wieder identifizieren. Die Bedrohungslage, bei der die einzelnen Betroffenen nicht nachvollziehen können, ob und inwieweit sie tatsächlich betroffen sind, jedoch immer mit der Möglichkeit rechnen müssen, besteht somit nicht nur darin, dass eine einzelne Aktivität beobachtet wird, sondern vielmehr im langfristigen Überwachen und Speichern und dementsprechend auch der Auswertung ihrer Aktivitäten im öffentlichen Raum.

Dem gegenüber können zwar Straftaten wirkungsvoll durch Abschreckung mit effektiver Aufklärung und Strafdrohung verhindert werden, sodass die Maßnahme grundsätzlich geeignet ist. Allerdings muss beachtet werden, dass für den Schutz gewichtiger Rechtsgüter sonstige heimliche Überwachungsmaßnahmen möglich sind, und im Übrigen der Rechtsgüterschutz durch die persönliche Anwesenheit von Ermittlungspersonen zum größten Teil gewährleistet werden kann.

Die Überwachung ist auf Ansammlungen und öffentliche Veranstaltungen beschränkt. Der Drohneneinsatz kann schon von vornherein nur erfolgen, wenn die Einsatzpersonen von einer solchen Veranstaltung wissen und die Geräte an den entsprechenden Ort schicken. Damit unterscheidet sich

[61] vgl. Roggan, NVwZ 2011, 590 (591).

der Drohneneinsatz von der tatsächlichen physischen Polizeipräsenz nur dadurch, dass die Beamten zum Eingreifen erst noch an den Ort des Geschehens gelangen müssen. Die Situationen können zwar besser erfasst und überblickt werden. Mangels physischer Anwesenheit von Einsatzkräften besteht die Verhinderung von Straftaten jedoch lediglich in der Abschreckungswirkung der Aufnahmegeräte. Daher ist schon zweifelhaft, ob die Maßnahme überhaupt effektiver als das mildere Mittel Polizeipräsenz und damit erforderlich ist.

Jedenfalls ist sie unverhältnismäßig. Das mögliche Verhindern einzelner Rechtsgutsverletzungen kann nicht die massenhafte und dauerhafte Überwachung des öffentlichen Raums durch die Staatsgewalt rechtfertigen. Damit ist § 34 Nr. 1 SOG M-V insgesamt unverhältnismäßig und somit verfassungswidrig.

c) Verletzung des Rechts auf effektiven Rechtsschutz, Art. 19 Abs. 4 i.V.m. § Art. 2 Abs. 1, Art. 1 Abs. 1 GG

Das Recht auf effektiven Rechtsschutz ist verletzt, wenn es keine Möglichkeit für Betroffene gibt, den Grundrechtseingriff effektiv gerichtlich zu verfolgen. Die Grundrechtseingriffe müssen offen erfolgen; die Betroffenen müssen wenigstens zeitnah von heimlichen Maßnahmen unterrichtet werden (siehe oben).

Die Überwachung durch Drohnen soll gem. § 32 Abs. 1 SOG M-V offen erfolgen. Eine Benachrichtigung der betroffenen Personen ist schon aufgrund der extremen Streubreite faktisch wenig aussichtsreich. Die Bürgerinnen und Bürger sind demnach darauf angewiesen, dass sie die Maßnahme auch wahrnehmen. Bei lebensnaher Betrachtung ist dies jedoch häufig kaum möglich, wenn Fluggeräte der Polizei nicht explizit und für die Betroffenen mit bloßem Auge wahrnehmbar sind. Folglich kann jedoch der Schluss gezogen werden, dass bei verfassungskonformer Auslegung die „offene“ Überwachung gem. § 32 Abs. 1 SOG M-V so gestaltet sein muss, dass die Betroffenen die Maßnahme auf jeden Fall erkennen können. Dann sind jedoch auch die Anforderungen an einen effektiven Rechtsschutz gewahrt.

Allerdings könnte § 32 Abs. 6 S. 2 SOG M-V verfassungswidrig sein, soweit dieser die nicht offenkundige Erfassung von Personen vorsieht. Dadurch wird der Einsatz von Drohnen zugelassen, die nicht sofort als polizeiliche Fluggeräte erkennbar sind. Um die Benachrichtigung nachzuholen, müssten alle Personen, bei größeren Menschenansammlungen unter Umständen eine immense Zahl, identifiziert und benachrichtigt werden. Das wiederum setzt voraus, dass die Behörden über die ladungsfähige Anschrift sämtlicher erfasster Personen verfügen. Die Personen können jedoch überhaupt nur erfasst und identifiziert werden, wenn sie bereits in einem Datensystem der Polizei hinterlegt sind, was nicht gewährleistet werden kann und für sich einen extremen Grundrechtseingriff darstellen würde. Eine Benachrichtigung wird in vielen Fällen faktisch nicht möglich sein.

Somit verstößt § 32 Abs. 6 S. 2 SOG M-V gegen Art. 19 Abs. 4 GG.

d) Ergebnis

§ 34 Nr. 1 SOG M-V ist insgesamt verfassungswidrig.

§ 34 Nr. 2-5 SOG M-V ist damit ebenfalls verfassungswidrig, soweit auf verfassungswidrige Befugnisse verwiesen wird.

VII. Ausschreibung zur gezielten polizeilichen Kontrolle, § 35 SOG M-V

Die Ausschreibung zur gezielten polizeilichen Kontrolle besteht darin, dass personenbezogene Daten wie z.B. Kennzeichen in einem zentralen Datensystem abgespeichert werden. Trifft eine zufällige

polizeiliche Kontrolle auf eine im Speicher erfasste Person, wird dies abgespeichert, § 35 Abs. 1 S. 2 SOG M-V. Darüber hinaus werden Eingriffsbefugnisse gem. § 35 Abs. 2 SOG M-V (im Wesentlichen Identitätsfeststellung und Durchsuchung) aktiviert. Die ermittelten Informationen werden wiederum in dem Speichersystem hinterlegt. Es können auch Informationen über Begleitpersonen nach § 27 Abs. 3 Nr. 2 SOG M-V erfasst und abgespeichert werden.

1. Keine Gesetzgebungskompetenz

Vorliegend kommt mit der Ausgestaltung des gerichtlichen Verfahrens eine konkurrierende Bundeskompetenz gem. Art. 74 Abs. 1 Nr. 1 GG in Betracht. Dafür müsste die vom SOG M-V erwähnte Strafverfolgungsvorsorge tatsächlich auf den Gerichtsprozess abzielen (1) und der Bund von seiner Kompetenz im Rahmen der polizeilichen Ausschreibung nicht abschließend Gebrauch gemacht haben (2).

Es handelt sich um eine Regelung des Strafprozesses, wenn eine Maßnahme nicht mehr präventiv auf das Verhüten von Unrecht, sondern auf die Durchführung des auf das Unrecht folgenden Prozesses gerichtet ist. Es kommt auf die Zielsetzung der Norm an, wie sie sich in objektiver Hinsicht darstellt.[62]

Dabei kann es sich auch um eine zukünftige Straftat handeln. Die Gefahrenabwehr hingegen ist präventiv auf den Rechtsgüterschutz ausgerichtet. Davon ist auch die Verhütung von Straftaten erfasst. Nicht erfasst sind jedoch alle Maßnahmen, die sich mit der Straftat gleichermaßen „abfinden“ und den Prozess vorbereiten.

§ 35 Abs. 1 S. 1 SOG M-V richtet sich neben der Verhütung auch auf die „vorbeugende Bekämpfung solcher Straftaten“. Die vorbeugende Bekämpfung meint gem. § 7 Abs. 1 Nr. 4 SOG M-V die Vorsorge für die Verfolgung künftiger Straftaten. Der Wortlaut bezieht sich somit explizit auf den der begangenen Straftat folgenden Strafprozess. Dafür spricht auch die Systematik mit der expliziten Formulierung in Abgrenzung zur Verhütung von Straftaten. Nach allgemeinem Sprachverständnis meint die Verhütung“, dass Straftaten gar nicht erst stattfinden sollen. Zwar wird die Vorsorge für die Verfolgung im Rahmen der Gefahrenabwehr aufgezählt. Das schließt aber nicht aus, dass sich der Gesetzgeber hier auf die Strafverfolgungsvorsorge bezieht, die gleichermaßen „bei Gelegenheit“ der Gefahrenabwehr stattfinden soll.

Der Bund hat mit § 163e StPO eine Norm für die Ausschreibung zur Beobachtung bei polizeilichen Kontrollen geschaffen. § 163e Abs. 1 StPO regelt, dass Personen bei ausreichenden Anhaltspunkten in Bezug auf die Begehung erheblicher Straftaten ausgeschrieben werden können und dadurch polizeilich beobachtet werden, sollten sie im Rahmen irgendeiner Maßnahme polizeilich kontrolliert werden. Des Weiteren können gem. § 163e Abs. 2 StPO auch Kennzeichen und sonstige personenbezogene Daten ausgeschrieben werden. § 163e Abs. 3 StPO regelt die Datenerfassung und -übermittlung im Falle des Antreffens der jeweiligen Person. § 163e Abs. 4 StPO enthält Verfahrensvorschriften.

Somit umfasst § 163e StPO die grundsätzliche Ausschreibung zur Beobachtung bei polizeilicher Kontrolle und die sich an das Antreffen anschließenden Maßnahmen. Somit verbleibt hier kein Raum für Regelungen, die bei Antreffen der ausgeschriebenen Person weitere Befugnisse beinhalten. Die Regelung des § 163e StPO ist insoweit abschließend. Damit ist der Landesgesetzgeber gem. Art. 72 GG für den Erlass eigener Vorschriften gesperrt.

[62] BVerfGE 150, 244 (273).

Somit handelte das Land Mecklenburg-Vorpommern beim Erlass des § 35 Abs. 1 HS 2 Alt. 2, § 7 Abs. 1 Nr. 4 Var. 2 SOG M-V ohne Gesetzgebungskompetenz. Die Norm ist bereits deshalb insoweit verfassungswidrig.

2. Hilfsweise: Materielle Verfassungswidrigkeit

Für die Anforderungen an die Eingriffsschwelle kommt es auf die Schwere des Grundrechtseingriffs an. Die Ausschreibung betrifft durch das Erfassen, Speichern und Verarbeiten von Daten das Recht auf informationelle Selbstbestimmung. Ein Eingriff wiegt umso schwerer, je tiefer er in die Privatsphäre eindringt, je mehr Personen er erfasst (Streubreite), je länger und umfassender die Datenerfassung erfolgt und ob sie heimlich oder offen durchgeführt wird.[63]

Durch die erstmalige Ausschreibung werden zwar nur einzelne, personenbezogene Daten verarbeitet. Allerdings wird im Fortgang der Maßnahme über bis zu sechs Monate bei jeder zufälligen polizeilichen Kontrolle der Ort der Kontrolle erfasst, sodass ein Bewegungsprofil erstellt werden kann. Durch das Erfassen der Kontaktpersonen gem. § 27 Abs. 3 S. 2 SOG M-V, was Personen aus dem gesamten Lebensumfeld betreffen kann, kann auch ein Sozialprofil erstellt werden. Darüber hinaus weist die Maßnahme dadurch auch eine hohe Streubreite auf. Abgesehen davon, dass gerade bei Kontrollen im Fahrzeug nicht sicher erkannt werden kann, ob die mitfahrende Person doch nur flüchtigen oder zufälligen Kontakt zur Zielperson der Maßnahme hat, umfasst der Kreis der Personen mit nicht nur flüchtigem Kontakt einen erheblichen Kreis an Menschen.[64] Somit weist die Maßnahme im Ergebnis eine hohe Eingriffsintensität auf.

Solche Maßnahmen können durch Gefahren für gewichtige Rechtsgüter oder bei terroristischer Bedrohung im Vorfeld einer Gefahr bei ausreichend konkretisierter Gefahr ergriffen werden (siehe oben).

Vorliegend reicht für das Ausschreiten die durch Tatsachen gerechtfertigte Annahme des Begehung einer erheblichen oder terroristischen Straftat aus. Die durch Tatsachen gerechtfertigte Annahme liegt jedoch weit unterhalb der Gefahr und fordert kein in irgendeiner Art konkretisiertes Gefahrenszenario oder eine gefährliche Person. Eine einengende Auslegung würde dem Gebot der Normklarheit widersprechen. Wie auch für die heimlichen Befugnisse gem. § 33 Abs. 1 SOG M-V reicht diese Eingriffshürde nicht aus, um den Grundrechtseingriff zu rechtfertigen.

Zudem braucht es ein gewichtiges Rechtsgut, um den Eingriff zu rechtfertigen. Als solche kommen Leib, Leben und Freiheit der Person sowie der Bestand und die Sicherheit eines Landes, des Bundes oder der Menschheit insgesamt in Betracht. Die erheblichen Straftaten gem. § 35 Abs. 1 S. 1 Alt. 1 § 49 SOG M-V genügen diesen Anforderungen nicht in Gänze (siehe oben A) I. 2. b)).

Darüber hinaus verweist § 35 Abs. 1 S. 2 SOG M-V auf § 67a Abs. 1 SOG M-V. Die Eingriffsintensität ist mindestens mit § 33 Abs. 1 SOG M-V vergleichbar. Auch dahingehend kann auf die obigen Ausführungen verwiesen werden. Somit ist § 35 Abs. 1 S. 2 ebenfalls verfassungswidrig, soweit er mit §§ 67a Abs. 1 Nr. 1, 67c Abs. 1 Nr. 2 SOG M-V auf Vorfeldstraftaten verweist.

§ 35 Abs. 1 S. 1 SOG M-V ist somit nicht verhältnismäßig und damit verfassungswidrig.

§§ 35 Abs. 1 S. 2, 67a Abs. 1 Nr. 1, 67c Abs. Nr. 2 SOG MV sind somit ebenfalls verfassungswidrig.

---

[63] vgl. Schneider, NVwZ 2021, 1646 (1647f.), BVerfGE 141, 220 (287).
[64] BVerfGE 133, 277 (349).

3. Spezielle Befugnisse gem. § 35 Abs. 2 S. 1 Nr. 2, Nr. 3 SOG M-V

Darüber hinaus sind auch die speziellen Eingriffsbefugnisse gem. § 35 Abs. 2 SOG M-V für sich genommen selbst bei verfassungsmäßiger Ausschreibung verfassungswidrig.

§ 35 Abs. 2 S. 1 Nr. 2 und 3 SOG M-V gestatten die Identitätsfeststellung und Durchsuchung der Sache oder der Person bei Gelegenheit der zufälligen Kontrolle. Hinsichtlich der Verfassungsmäßigkeit der Eingriffsnormen kommt es auf die Eingriffshürde an.

§ 35 Abs. 2 S. 2 SOG M-V verweist auf die übrigen Voraussetzungen der Durchsuchung. Nach Ansicht der Beschwerdeführenden ist damit lediglich auf Verfahrensvorschriften, nicht jedoch auf materielle Eingriffsschwellen Bezug genommen. Dafür spricht, dass, würde § 35 Abs. 2 S. 1 SOG M-V als Rechtsgrundverweisung verstanden, die Norm gegenstandslos wäre. Ein entsprechender Eingriff könnte einfach auf die Rechtsgrundlage zur Durchsuchung gestützt werden. Zudem wird nur bei der Durchsuchung weitergehend verwiesen, hinsichtlich der Identitätsfeststellung findet sich kein Hinweis auf weitere Voraussetzungen, wobei die Voraussetzungen in materieller Hinsicht in § 29 SOG M-V detailliert geregelt sind. Das spricht dafür, dass lediglich das gem. § 53 Abs. 5 SOG M-V anzuwendende Verfahren eingehalten werden soll, es aber nicht auf die tatbestandlichen Voraussetzungen ankommen soll und die Norm damit als Rechtsfolgenverweisung zu verstehen ist.

Damit erschöpft sich die Eingriffsvoraussetzung gem. § 35 Abs. 2 S. 1 Nr. 2 und 3 SOG M-V in der Ausschreibung zur gezielten polizeilichen Kontrolle, die lediglich auf die Voraussetzungen der Ausschreibung zur polizeilichen Kontrolle verweist (s.o.) Diese sind schon als Eingriffshürden der Ausschreibung zur polizeilichen Kontrolle ungeeignet und daher teilweise verfassungswidrig. Erst recht kann dadurch somit nicht die Ausschreibung zur gezielten polizeilichen Kontrolle gerechtfertigt werden. Die Eingriffe müssen sich daher auf die dafür vorgesehenen Normen §§ 29, 53, 57 SOG M-V stützen und deren Anforderungen genügen.

Hinsichtlich der Eingriffsnorm §§ 35 Abs. 1 S. 2, 67a Abs. 1 Nr. 2 SOG M-V bestehen auch hier keine verfassungsrechtlichen Bedenken. Die Durchsuchung wird offen durchgeführt und bei der betreffenden Person gezielt eingesetzt. Eine hohe Streubreite wird schon dadurch verhindert, dass nur die ausgeschriebene Person durchsucht werden darf, welche wiederum nach längerer Beobachtung und auf das individuelle Verhalten gestützt in höchstem Grade individualisiert ausgemacht wird.

Somit ist § 35 Abs. 2 S. 1, S. 2 SOG M-V verfassungswidrig, soweit die Eingriffe unter den Voraussetzungen von § 35 Abs. 1 S. 1 und § 35 Abs. 1 S. 2, § 67a Abs. 1 Nr. 1, § 67c Abs. 1 Nr. 2 SOG M-V gestattet werden.

VIII. Rasterfahndung, § 44 SOG M-V

Nach Ansicht der Beschwerdeführenden ist § 44 Abs. 1 Nr. 1 SOG M-V verfassungswidrig, weil durch den Verweis auf § 67a Abs. 1 SOG M-V auch Eingriffe im Vorfeld einer konkreten Gefahr ermöglicht werden. Die Rasterfahndung habe jedoch eine derart hohe Eingriffsintensität, dass sie erst bei Vorliegen einer konkreten Gefahr verhältnismäßig sein könne.

1. Eingriffsintensität

Bei der Rasterfahndung kann die Polizei ohne Verdacht die Herausgabe personenbezogener Daten bestimmter Personengruppen aus den Beständen anderer Behörden anfordern, um eine polizeipflichtige Person für weitere Aufklärungsmaßnahmen zu identifizieren. Somit ist eine Vielzahl nicht individualisierter Personen betroffen, deren Daten weitergegeben und verwendet werden. Der

Eingriff weist damit eine hohe Streubreite auf und trifft zwangsläufig zum größten Teil nicht-Störer, indem der Störer erst herausgefunden werden soll. Die Daten betreffen Name, Anschrift, Tag der Geburt sowie weitere, nicht festgelegt, sondern von den Ermittlungspersonen festzulegende Daten. Somit kann jede Art von personenbezogener Information abgefragt werden. Die Befugnisnorm entspricht insoweit § 31 Abs. 2 S. 1 PolG NW 1990, BVerfGE 115, 320. Dadurch können auch sensible, für die Ausübung anderer Grundrechte relevante Daten abgefragt und zur Herstellung eines Persönlichkeitsprofils genutzt werden. Jedenfalls nach Abschluss des Datenabgleichs und Beginn der Fahndung sind die einzelnen Personen in der Ergebnismasse nicht mehr anonym, ohne, dass ihre Störereigenschaft zweifelsfrei festgestellt wurde. Mit Ausnahme von Berufsgeheimnisträgern gibt es keine spezifischen Übermittlungsverbote. Dadurch ist eine Verknüpfung sämtlicher, bei irgendeiner öffentlichen Stelle gespeicherter Daten möglich, sodass im Ergebnis der gesamte Datenbestand als ein einziger Vorratsdatenspeicher genutzt werden kann. Die im Anschluss an die Datenabfrage durchgeführte Rasterfahndung wiederum erhöht das Risiko für die Betroffenen, Zielperson polizeilicher Maßnahmen zu werden. Darüber hinaus hat die öffentlich Durchgeführte Fahndung eine stigmatisierende Wirkung. Zudem ist der Eingriff bis zu seinem Abschluss heimlich. Eine Benachrichtigung soll erst im Rahmen der Vorgaben von § 46a SOG M-V erfolgen. Somit weist die Rasterfahndung eine hohe Eingriffsintensität auf.[65]

2. Verhältnismäßigkeit

Jedenfalls der Eingriff mittels der Rasterfahndung bei konkreter Gefahr für ein hinreichend gewichtiges Rechtsgut ist verhältnismäßig.[66]

§ 44 Abs. 1 SOG M-V schützt mit Leib, Leben und Freiheit der Person sowie Sicherheit und Bestand eines Landes, des Bundes oder der Menschheit an sich und den Bestand der demokratischen Ordnung vor terroristischen Anschlägen hinreichend gewichtige Rechtsgüter (siehe oben).

Darüber hinaus lässt § 44 Abs. 1 Nr. 1 SOG M-V jedoch den Eingriff im Vorfeld der konkreten Gefahr zu. Im Urteil zur Rasterfahndung[67] fordert das Gericht eine konkrete Gefahr. Insbesondere beschäftigt es sich darin auch mit der Gefahr terroristischer Anschläge und sog. Schläfern“, sodass die abgesenkte Eingriffsschwelle im Vorfeld der konkreten Gefahr bei Gefahren- oder personenbezogener Gefahrprognose (siehe oben), die daraufhin entwickelt wurde und sich explizit auf terroristische Gefahren bezieht, hier nicht zur Anwendung kommt. Zwar sinkt mit dem Gewicht des Rechtsguts und der Schwere des zu befürchtenden Schadens die Anforderung an die Wahrscheinlichkeit des Schadenseintritts. Dennoch kann auch für den Fall terroristischer Gefahren bei der Rasterfahndung keine Ausnahme gemacht werden. Dies bekräftigt sich insbesondere dadurch, dass das Gericht in seinem Urteil zum BKAG auf die Ausführungen über Rasterfahndung verweist und diese bekräftigt.

Für das Erfordernis einer konkreten Gefahr spricht zudem, dass die Maßnahme die hohe Gefahr des Missbrauchs sensibler Daten und eine extrem weite Streubreite kombiniert. Gerade bei der Kombination mehrerer Faktoren, die eine Maßnahme intensivieren, ist von einem umso schwereren Grundrechtseingriff auszugehen. Zudem müssen bei der Gefahrprognose im Vorfeld einer konkreten Gefahr die betroffenen Personen gerade so individualisierbar sein, dass die Maßnahme gezielt eingesetzt werden kann. Die Datenabfrage und der Datenabgleich für die Rasterfahndung sind gerade keine Maßnahmen, die Einzelpersonen treffen, sondern ganze Personengruppen. Die Gefahrkategorien im Vorfeld sind somit nicht nur von der Eingriffsschwelle her nicht angemessen, sie passen auch nicht

[65] Zum Ganzen ausführlich BVerfGE 115, 320 (347ff).
[66] vgl. BVerfGE 141, 220 (303).
[67] BVerfGE 115, 320.

zur Art der Maßnahme und sind daher schon faktisch nicht erfolgversprechend anwendbar. Eine Übertragung der Rechtsprechung zum Gefahrenvorfeld ist daher ebenfalls nicht denkbar.

Somit ist der Eingriff im Vorfeld der Gefahr unverhältnismäßig.

3. Ergebnis

§ 44 Abs. 1 Nr. 1 SOG M-V ist verfassungswidrig.

IX. Unzureichende Befugnisse des Landesdatenschutzbeauftragten, § 48b SOG M-V

Abschließend bringen die Beschwerdeführenden vor, dass § 48b SOG M-V keine ausreichend wirksame Kontrolle der heimlichen Überwachungsmaßnahmen gewährleistet. Um den rechtmäßigen Gebrauch von heimlichen Eingriffsbefugnissen sicher zu stellen, ist eine wirksame und effektive Aufsicht notwendig, die eine wirksame Umsetzung der gesetzlichen Anforderungen an die Maßnahme gewährleistet.[68]

§ 48b SOG M-V verweist hauptsächlich auf die Anordnungsbefugnisse aus Art. 56 Abs. 1 lit. a-i, t und Art. 58 Abs. 1, Abs. 2 lit. a, b, Abs. 3 lit. a, b der DSGVO. Art. 57 der VO 2016/679 (DSGVO) regelt die Aufgaben, Art. 58 DSGVO die Befugnisse der Aufsichtsbehörde. Gem. § 48b Abs. 1 SOG M-V ist die zum Datenschutz beauftragte Person somit befugt, Sachverhalte zu untersuchen, Warnungen auszusprechen, zu beraten und Stellungnahmen abzugeben. Subsidiär dazu gewährt § 48b Abs. 2 SOG M-V eine Anordnungsbefugnis im Rahmen der RL 2016/680 (JI-RL), die jedoch nur zum Tragen kommt, wenn eine Anordnung wegen Verletzung wesentlicher datenschutzrechtlicher Vorschriften erforderlich ist und dadurch die Arbeit der Sicherheitsbehörden nicht wesentlich beeinträchtigt wird. Die Löschung personenbezogener Daten darf grundsätzlich nicht angeordnet werden. Darüber hinaus können Verstöße gegen die JI-RL beanstandet und durch die zuständige Rechts- oder Fachaufsicht Maßnahmen ergriffen werden.

Eine effektive Durchsetzung von Regeln kann zwar nur gewährleistet werden, wenn zur Durchsetzung auch Anordnungsbefugnisse existieren. Diese hat jeweils nur die Aufsichtsbehörde in uneingeschränktem Umfang. Zwar hat somit die zum Datenschutz beauftragte Person nur untergeordnete und beschnittene Anordnungsbefugnisse. Allerdings können die Aufsichtsbehörden im Zweifel womöglich sogar bessere, passgenauere Anordnungen erlassen und durchgeführte Maßnahmen fachgerechter beanstanden. Entscheidend ist, dass überhaupt eine wirksame Kontrolle gewährleistet ist. Dabei ist es nicht unschädlich, dass sich diese auf verschiedene Behörden verlagert. Nach § 48b SOG M-V ist die für den Datenschutz zuständige Person damit betraut, die Vorgänge zu überblicken und rechtswidrige Eingriffe an die jeweils zuständigen Aufsichtsbehörden zu kommunizieren. Diese sind wiederum dafür zuständig, Maßnahmen zu ergreifen und die rechtmäßige Anwendung der Eingriffsbefugnisse durchzusetzen. Durch die Arbeitsteilung wird die Überwachung der Sicherheitsbehörden jedoch nicht weniger wirksam.

Insoweit ist eine Verfassungswidrigkeit nach Auffassung der BRAK nicht festzustellen, da sich dies in der Einschätzungsprärogative des politisch legitimierten Gesetzgebers über spezifische Fragen der Zweckmäßigkeit bewegen dürfte.

- - -

[68] BVerfGE 141, 220 (284).