Dr. Anna Luczak
Rechtsanwältin

Kottbusser Damm 94
10967 Berlin
Telefon: 030 5471 6772
Fax: 030 5471 6770

An das
Bundesverfassungsgericht
Schlossbezirk
76131 Karlsruhe

3. Juni 2021

Verfassungsbeschwerde

1. der Frau Katrin Hildebrandt, …,

2. des Herrn …,

3. der Frau Salome Krug, …,

4. des Herrn …,

5. des Herrn …,

gegen

§ 26a Abs. 3 S. 1 Halbsatz 2, Abs. 4 und 5,

§ 33 Abs. 2,

§ 33b Abs. 1 Satz 2,

§ 33c Abs. 1 Satz 2 und 4 sowie Abs. 5,

§ 33d Abs. 1 Satz 1 Nr. 2 - 4 sowie Abs. 3,

§ 34 S. 1,

§ 35 Abs. 1, Abs. 2 S. 2,

§ 44 Abs. 1 Nr. 1,

§ 46a Abs. 2,

§ 48b Abs. 1 und 2

des Gesetzes über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern (Sicherheits- und Ordnungsgesetz - SOG M-V) in der Fassung des Gesetzes über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern und zur Änderung anderer Gesetze vom 27. April 2020 (GVOBl. M-V S. 334).

Namens und in Vollmacht der Beschwerdeführerinnen und Beschwerdeführer wird Verfassungsbeschwerde erhoben mit der Rüge der Verletzung des Grundrechts auf informationelle Selbstbestimmung und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) sowie des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG) und des Rechts auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG).

Gliederung des Schriftsatzes

A. Vorbemerkung

Die Beschwerdeführerinnen und Beschwerdeführer wenden sich gegen verschiedene Bestimmungen des neuen Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern. Sie wenden sich insbesondere gegen die Ausweitung polizeilicher Überwachungsbefugnisse und gegen das Fehlen von Mechanismen und Vorkehrungen zum Schutz ihrer Grundrechte.

Die Verfassungsbeschwerde bietet die Gelegenheit, die vom Bundesverfassungsgericht im Urteil zum BKA-Gesetz aufgestellten Anforderungen an polizeiliche Befugnisse fortzuentwickeln und zu präzisieren. Der mecklenburg-vorpommerische Gesetzgeber nimmt zwar für sich in Anspruch, die Vorgaben aus dem Urteil zum BKA-Gesetz umzusetzen, dies ist ihm jedoch nur teilweise gelungen. Namentlich bei den folgenden Aspekten weist das Gesetz verfassungsrechtliche Mängel auf:

- Das SOG M-V ermöglicht intensive Grundrechtseingriffe im Vorfeld einer konkreten Gefahr, ohne die Anforderungen an eine solche Vorverlagerung der Eingriffsbefugnisse hinreichend auszugestalten. Insbesondere wird an Straftatbestände angeknüpft, die ihrerseits bereits im Vorfeld einer Rechtsgutsverletzung ansetzen. Zudem sieht das SOG M-V auch bei der Rasterfahndung und bei Eingriffen in das Wohnungsgrundrecht eine Absenkung der Eingriffsschwelle vor, obwohl für die Maßnahmen von Verfassungs wegen eine konkrete Gefahr oder sogar eine dringende Gefahr vorliegen muss.
- Der Schutz des Kernbereichs privater Lebensgestaltung beim Einsatz besonderer Mittel der Datenerhebung ist unzureichend ausgestaltet. Insbesondere verfehlt das Gesetz die Vorgaben zum Abbruch der Maßnahme bei einem unbeabsichtigten Eindringen in den Kernbereich und zur Sichtung der erhobenen Daten durch eine unabhängige Stelle.

- Indem das Gesetz weitgehende Ausnahmen von der Benachrichtigungspflicht statuiert, verletzt es das Recht auf effektiven Rechtsschutz.
- Auch die Aufsicht durch den Datenschutzbeauftragten oder die Datenschutzbeauftragte genügt nicht den verfassungsrechtlichen Anforderungen, da es an einer ausreichenden Anordnungsbefugnis fehlt.

Daneben wirft die Verfassungsbeschwerde verschiedene Rechtsfragen auf, die in der bisherigen Rechtsprechung des Bundesverfassungsgerichts noch gar nicht oder nur ansatzweise geklärt sind. Dies betrifft insbesondere folgende Aspekte:

- Das Gesetz erlaubt den Einsatz von Staatstrojanern für die Online-Durchsuchung und die Quellen-Telekommunikationsüberwachung, ohne hinreichende Schutzvorkehrungen dagegen zu treffen, dass Sicherheitslücken durch die Polizei zurückgehalten werden. Das verletzt das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in seiner objektiv-rechtlichen Dimension.
- Daneben ermöglicht das SOG M-V aber auch das heimliche Betreten und Durchsuchen von Wohnraum, um einen Staatstrojaner auf Endgeräten zu installieren. Die Befugnis verletzt das Grundrecht auf Unverletzlichkeit der Wohnung, da die Maßnahme nicht den Schrankenregelungen des Art. 13 GG genügt.
- Der Einsatz unbemannter Flugkörper (Drohnen) genügt nicht den verfassungsrechtlichen Anforderungen, weil die Offenheit der Maßnahme nicht hinreichend sichergestellt ist.

B. Sachverhalt

I. Die angegriffenen Regelungen

Gegenstand der Verfassungsbeschwerde ist die neue Fassung des SOG M-V, die am 5. Juni 2020 in Kraft getreten ist und sowohl gesetzliche Erweiterungen als auch neue Eingriffsermächtigungen enthält. Im Einzelnen werden nachfolgend überblicksartig dargestellte Regelungen angegriffen:

1. Besondere Mittel der Datenerhebung (§ 33 SOG M-V)

§ 33 SOG ermächtigt zum Einsatz besonderer Mittel der Datenerhebung, namentlich zur längerfristigen Observation, zum verdeckten Einsatz technischer Mittel, zum Einsatz von Vertrauenspersonen und zum Einsatz verdeckter Ermittler.

Nach dem bisherigen § 33 Abs. 2 Satz 1 SOG M-V konnten besondere Mittel der Datenerhebung angewendet werden, wenn „Tatsachen die Annahme der Begehung von Straftaten von erheblicher Bedeutung (§ 49) rechtfertigen und die Aufklärung des Sachverhalts zum Zwecke der Verhütung solcher Straftaten oder ihrer möglichen Verfolgung auf andere Weise nicht möglich ist“. Diese Eingriffsbefugnis wurde in zweierlei Hinsicht ausgeweitet. Erstens wurden die von § 49 SOG-MV in Bezug genommenen Delikte um verschiedene Vergehen erweitert. Zweitens ist der Einsatz der besonderen Mittel der Datenerhebung nicht mehr nur dann erlaubt, wenn die Aufklärung des Sachverhalts ansonsten unmöglich wäre, sondern auch wenn sie ansonsten wesentlich erschwert wäre.

Zusätzlich wurde in § 33 Abs. 2 Satz 3 SOG M-V eine weitere Eingriffsschwelle speziell zur Verhütung terroristischer Straftaten geschaffen. Die Norm verweist auf die Voraussetzungen des ebenfalls neu eingeführten § 67a Abs. 1 SOG M-V, der in zwei an die Rechtsprechung des Bundesver-

fassungsgerichts angelehnten Alternativen im Vorfeld einer konkreten Gefahr ansetzt und zur Definition der in Betracht kommenden terroristischen Straftaten auf den Katalog des § 67c SOG M-V verweist.

Der Schutz des Kernbereichs privater Lebensgestaltung soll bei Maßnahmen nach § 33 SOG M-V durch den neu eingeführte § 26a SOG M-V gewährleistet werden. § 26a Abs. 3 Satz 1 SOG M-V schreibt grundsätzlich den Abbruch der Maßnahme vor, wenn während der Erhebung Tatsachen die Annahme rechtfertigen, dass Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erfasst werden. Allerdings sieht § 26a Abs. 3 Satz 1 Halbsatz 2 SOG M-V von diesem Erfordernis zwei Ausnahmen in Form des Gefährdungs- und des Verwendungsvorbehaltes vor: Von einem Abbruch der laufenden Maßnahme kann dann abgesehen werden, wenn dieser entweder einerseits mit der Gefährdung der eingesetzten Polizeibeamtinnen und Polizeibeamten oder Vertrauenspersonen verbunden wäre oder andererseits deren weitere Verwendung gefährden würde. Nach § 26a Abs. 4 SOG M-V 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 sonstigen Daten genügt nach § 26a Abs. 5 SOG M-V im Fall der Unterbrechung die Sichtung durch die behördliche Datenschutzbeauftragte bzw. den behördlichen Datenschutzbeauftragten.

§ 46a Abs. 1 Satz 1 Nr. 2 SOG M-V regelt die Benachrichtigung der betroffenen Personen von dem Einsatz besonderer Mittel der Datenverarbeitung. Nach § 46a Abs. 2 Satz 1 SOG M-V erfolgt die Benachrichtigung, „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“. Im Fall der Benachrichtigung über besondere Mittel der Datenverarbeitung ist nach § 46a Abs. 2 Satz 2 SOG M-V auch eine Gefährdung der weiteren Verwendung von Vertrauenspersonen und verdeckt Ermittelnden „als bedeutender Belang zu berücksichtigen“.

2. Wohnraumüberwachung (§ 33b SOG M-V)

Die zuvor in § 34b SOG M-V a.F. enthaltene Befugnis zum Einsatz technischer Mittel zur Wohnraumüberwachung wurde insofern ausgeweitet, als sie gemäß § 33b Abs. 1 Satz 2 ebenfalls im Vorfeld einer konkreten Gefahr unter den Voraussetzungen des § 67a Abs. 1 SOG zulässig ist.

3. Online-Durchsuchung (§ 33c SOG M-V)

Mit § 33c SOG-MV wurde eine Befugnis zum Einsatz technischer Mittel zum Eingriff in informationstechnische Systeme (sogenannte Online-Durchsuchung) geschaffen. Zur Bestimmung der Eingriffsschwelle wird in § 33c Abs. 1 Satz 2 SOG M-V ebenfalls auf die Voraussetzungen des § 67a Abs. 1 SOG M-V verwiesen. Nach § 33c Abs. 1 Satz 4 darf auch in informationstechnische Systeme von Nicht-Verantwortlichen eingegriffen werden, wenn Tatsachen die Annahme rechtfertigen, dass eine verantwortliche Person dort ermittlungsrelevante Informationen speichert. § 33c Abs. 5 SOG M-V ermächtigt u.a. zum Betreten und Durchsuchen von Räumlichkeiten der betroffenen Personen, soweit dies zur Durchführung der Maßnahme erforderlich ist. Dies soll den physischen Zugriff auf das Gerät ermöglichen, um eine Späh-Software (sogenannter Staatstrojaner) zu installieren.

4. TKÜ und Quellen-TKÜ (§ 33d SOG M-V)

Die zuvor in § 34a SOG M-V a.F. geregelte Befugnis zur Telekommunikationsüberwachung wurde insofern ausgeweitet, als in § 33d Abs. 1 Satz 1 Nr. 2 bis 4 SOG M-V ebenfalls auf die Voraussetzungen des § 67a Abs. 1 SOG M-V Bezug genommen wird. Eingeführt wurde zudem die Befugnis zu Eingriffen in informationstechnische Systeme zur Durchführung der Telekommunikationsüberwachung (sogenannte Quellen-TKÜ, § 33d Abs. 3 Satz 1 SOG M-V). Darüber hinaus dürfen nach § 33d Abs. 3 Satz 2 auch die auf dem informationstechnischen System gespeicherten Inhalte und Umstände der Kommunikation überwacht und aufgezeichnet werden, wenn

sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können (sogenannte „kleine Online-Durchsuchung“). Nach § 33d Abs. 3 Satz 3 SOG M-V ist die in § 33c Abs. 5 SOG M-V geregelte Befugnis zum Betreten und Durchsuchen von Räumlichkeiten entsprechend anzuwenden.

5. Einsatz unbemannter Luftfahrtsysteme (§ 34 SOG M-V)

Die Neuregelung des § 34 SOG zum Einsatz von unbemannten Luftfahrtsysteme ergänzt zum einen die Ermächtigungen zum Einsatz der besonderen Mittel der Datenerhebung nach den §§ 33 ff SOG M-V (§ 34 S. 1 Nr. 2-5 SOG M-V) und stellt außerdem eine Ermächtigung für die Erhebung von Bild- und Tonaufnahmen von öffentlichen Veranstaltungen und Ansammlungen oder an öffentlich zugänglichen oder gefährdeten Orten gemäß § 32 Abs. 1, 3 oder 4 SOG M-V durch das Mittel des Drohnen-Einsatzes dar (§ 34 S. 1 Nr. 1 SOG M-V).

6. Ausschreibung zur polizeilichen Beobachtung und gezielten Kontrolle (§ 35 SOG M-V)

Der Anwendungsbereich der bereits in § 35 Abs. 1 SOG M-V a.F. enthaltenen Befugnis zur sog. Ausschreibung zur polizeilichen Beobachtung wurde durch die Neufassung erheblich erweitert. Die bisher abschließende Aufzählung der erhebbaren Daten (Personalien sowie bestimmte Angaben zu Fahrzeugen) ist in S. 1 der Neufassung nur noch exemplarisch. Gegenstand der Ausschreibung kann seitdem jede Art personenbezogener Daten sein. Der in Bezug genommene Straftatenkatalog des § 49 SOG M-V wurde ausgeweitet und die Ausschreibung ist nunmehr auch zur Verhütung und vorbeugenden Bekämpfung terroristischer Straftaten (§ 67c SOG M-V) zulässig. Die Gefahrenschwelle wurde hier zudem durch einen Verweis auf § 67a Abs. 1 SOG M-V abgesenkt.

In § 35 Abs. 2 SOG M-V wurde die Befugnis der Ausschreibung zur gezielten Kontrolle neu geschaffen. Sie ermöglicht in S. 2 die Identitätsfeststellung von Personen sowie die Durchsuchung von Sachen, die sich in den ausgeschriebenen Fahrzeugen befinden. Darüber hinaus dürfen die ausgeschriebenen Personen durchsucht werden. Die nach Abs. 1 und Abs. 2 gewonnenen Daten werden an die ausschreibende Behörde übermittelt.

7. Rasterfahndung (§ 44 SOG M-V)

Die Eingriffsschwelle der Rasterfahndung wurde ebenfalls durch einen neuen Verweis in § 44 Abs. 1 Nr. 1 SOG M-V auf § 67a Abs. 1 SOG M-V abgesenkt.

8. Fehlende Anordnungsbefugnis der oder des Landesbeauftragten für den Datenschutz (§ 48b SOG M-V)

Im Zusammenhang mit allen angegriffenen Überwachungs- und Weiterverarbeitungsermächtigungen wenden sich die Beschwerdeführerinnen und Beschwerdeführer gegen die in § 48b Abs. 1, Abs. 2 SOG M-V geregelte Einschränkung der Anordnungsbefugnis durch den Landesbeauftragten oder die Landesbeauftragte für Datenschutz.

II. Die Beschwerdeführerinnen und Beschwerdeführer

1. Beschwerdeführerin zu 1

Die Beschwerdeführerin zu 1 ist Rechtsanwältin in Rostock mit den Tätigkeitsschwerpunkten Strafrecht und Asyl- und Aufenthaltsrecht. Sie vertritt u.a. Personen, die als terroristisch oder extremistisch bezeichnet wurden, und Personen, die als Unterstützerinnen oder Unterstützer solcher Organisationen angesehen wurden, weil sie sich in ihrem Umfeld aufhielten oder Kontakt zu anderen als Unterstützerinnen oder Unterstützer eingestuften Personen hatten. Unter anderen bearbeitet sie mehrere Ermittlungsverfahren wegen des Verdachts der Vorbereitung einer schweren

staatsgefährdenden Gewalttat nach § 89a StGB, sowie auf dem Gebiet des Ausländer- und Asylrechts Verfahren gegen Personen, die als islamistische und/oder terroristische Gefährder eingeschätzt und abgeschoben wurden.

Die Beschwerdeführerin erledigt ihre Geschäfte als Anwältin unter anderen via Telefon und Computer, zudem nutzt sie diverse Chatdienste. Hierbei nutzt sie auch Dienste mit Ende-zu-Ende-Verschlüsselung. Informationen über ihre Mandanten und Mandantinnen speichert die Beschwerdeführerin zu 1 in den Geräten der IT-Infrastruktur ihrer Kanzlei. Dabei handelt es sich auch um Informationen über die politischen Aktivitäten ihrer Mandantinnen und Mandanten, an denen unter anderem ausländische Geheimdienste ein starkes Interesse haben könnten.

2. Beschwerdeführer zu 2

Der Beschwerdeführer zu 2 ist Journalist und wohnhaft in Hamburg, vormals in Rostock. Der Beschwerdeführer recherchiert und schreibt als freier Journalist für verschiedene, vorrangig überregionale Medien wie die dpa oder die Tageszeitung taz. Einer seiner Themenschwerpunkte ist der politische Extremismus, er befasst sich daneben seit einigen Jahren auch mit Migration/Asyl und der Situation von Flüchtlingen. Zudem recherchiert und berichtet er aktuell vermehrt über Wirtschafts- und Organisierte Kriminalität sowie über verwandte Deliktfelder wie Steuerhinterziehung und Geldwäsche. In den genannten, naturgemäß sehr verschlossenen Themengebieten ist er als Journalist in besonderem Maße auf die Zusammenarbeit mit Informantinnen und Informanten angewiesen.

Der Beschwerdeführer zu 2 unterhält enge Kontakte zu Personen aus den genannten Bereichen, die sich im Raum Rostock, seinem früheren Wohnort im von Sicherheitsbehörden als extremistisch eingestuften Milieu bewegen. Dabei ist es zumindest möglich, dass diese ihm Informationen übermittelnden Personen unter polizeilicher Beobachtung stehen oder dass sogar Strafermittlungsverfahren wegen schwerwiegender Straftaten, unter

Umständen sogar wegen terroristischer Straftaten, gegen sie geführt werden. Der Beschwerdeführer zu 2 kommuniziert mit solchen Personen unter anderem per E-Mail und über Chats, jeweils mit Ende-zu-Ende-Verschlüsselung.

3. Beschwerdeführerin zu 3

Die Beschwerdeführerin zu 3 ist politische Aktivistin im Bereich der Klima-, Umwelt- und Verkehrspolitik. In diesem politischen Betätigungsfeld ist sie seit Jahren regional im Umfeld ihres Wohnorts Greifswald und überregional an Aktionen beteiligt und hat unter anderem auch Versammlungen selbst angemeldet. Konkret war sie aktiv in Zusammenhang mit den Protesten gegen die Ostseepipeline, Braunkohletagebau-Anlagen und gegen die Rodung des Hambacher Forstes und Dannenröder Wald.

Sie steht bei ihrer politischen Betätigung in engem Kontakt mit zahlreichen anderen Personen, die in diesem Feld engagiert sind. Die Beschwerdeführerin zu 3 ist im Mecklenburg-Vorpommern-weiten Bündnis gegen die Verschärfung des SOG M-V engagiert und hat in diesem Zusammenhang in mehreren Städten Versammlungen angemeldet. Als Anmelderin wurde sie dabei im Vorfeld von Polizeibehörden des Landes Mecklenburg-Vorpommern kontaktiert und ihr der Einsatz von bestimmten Personen als Ordnerinnen oder Ordner untersagt, weil diese polizeibekannt seien.

Im Zusammenhang mit Protestaktionen suchten der Beamte des Staatsschutzes (Polizeieinheit Mobile Aufklärung Extremismus/MAEX) ihren Wohnsitz auf und befragten ihre Mitbewohner und Mitbewohnerinnen zu ihrer Person.

Gegen die Beschwerdeführerin zu 3 selbst wurden bereits Ermittlungsverfahren wegen Vorwürfen des Verstoßes gegen das Versammlungsgesetz, Nötigung oder gefährlichen Eingriffs gegen den Straßenverkehr geführt. Gegen andere Personen aus demselben Bereich des politischen Aktivismus wurden auch noch schwerer wiegende Vorwürfe erhoben.

Die Beschwerdeführerin zu 3 kommuniziert unter anderem per E-Mail und über Chats, jeweils mit Ende-zu-Ende-Verschlüsselung.

4. Beschwerdeführer zu 4

Der Beschwerdeführer zu 4 ist Jurist und in Rostock als Sozialarbeiter in einer Gemeinschaftsunterkunft für Asylsuchende tätig. Er besucht seit 2003 regelmäßig die Heim- und Auswärtsspiele des F.C. Hansa Rostock. Er hat am 05.06.2016 eine Demonstration im Zusammenhang mit einem Spiel des F.C. Hansa Rostock in Magdeburg angemeldet. Der Beschwerdeführer genießt in der Fan-Szene Vertrauen und ist bekannt. Sein Rat in Bezug auf den Umgang mit polizeilichen Maßnahmen oder Ermittlungsverfahren wird häufig gesucht. Der Beschwerdeführer zu 4 beobachtet regelmäßig im In- und Ausland Strafverfahren gegen organisierte Fußballfans. Dafür war er zum Beispiel im Jahr 2014 in Istanbul, um mit Football Supporter Europe (FSE) Strafprozesse gegen organisierte türkische Fans zu beobachteten, die an Demonstration auf dem Taksim-Platz teilgenommen haben sollen. Der Beschwerdeführer zu 4 geht davon aus, dass dieser Besuch und seine Kontakte zu den dortigen Angeklagten auch für türkische Sicherheitsbehörden von Interesse sind. Für seine Kommunikation mit anderen organisierten Fußballfans nutzt der Beschwerdeführer zu 4 auch Kommunikationswege, die Ende-zu-Ende verschlüsselt sind.

Seit 2018 engagiert sich der Beschwerdeführer zu 4 für Asylsuchende und hat auch in diesem Bereich viele Kontakte. Der Beschwerdeführer zu 4 wirkte ferner an der Gründung eines Mecklenburg-Vorpommern-weiten Bündnis gegen die Verschärfung des SOG M-V mit.

5. Beschwerdeführer zu 5

Der Beschwerdeführer zu 5 ist seit 2008 Mitglied beim F.C. Hansa Rostock e.V. und Dauerkarteninhaber auf der Südtribüne des Ostseestadions – dem Bereich der aktiven Fan-Szene. Er ist sehr gut vernetzt in der Fan-Szene

des F.C. Hansa Rostock und unterstützt auch Beschuldigte von Strafverfahren in diesem Zusammenhang mit Hinweisen auf Anwältinnen und Anwälte oder ähnliches. Er setzte sich mit anderen Fans u.a. öffentlich für die Einführung einer unabhängigen Beschwerdestelle für durch Polizeibeamte begangene Straftaten oder eben gegen die Novellierung des SOG M-V wie verabschiedet, ein. Der Beschwerdeführer zu 5 nahm im Juli 2015 auf Einladung der Football Supporters Europe an einer Veranstaltung zum Thema Fanrechte in Irland teil.

C. Zulässigkeit

Die Verfassungsbeschwerde ist zulässig.

I. Frist

Die Jahresfrist des § 93 Abs. 3 BVerfGG ist gewahrt. Die Verfassungsbeschwerde richtet sich gegen Regelungen, die mit Artikel 1 des Gesetzes über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern und zur Änderung anderer Gesetze vom 27. April 2020 (GVOBl. M-V S. 334) eingeführt wurden und am 5. Juni 2020 in Kraft getreten sind.

II. Beschwerdebefugnis

Die Beschwerdeführerinnen und Beschwerdeführer zu 1 bis 5 sind im Sinne von § 90 Abs. 1 BVerfGG beschwerdebefugt. Es ist zumindest möglich, dass die Grundrechte der Beschwerdeführerinnen und Beschwerdeführer durch die angegriffenen Regelungen verletzt werden, und die Regelungen betreffen die Beschwerdeführerinnen und Beschwerdeführer selbst, gegenwärtig und unmittelbar.

1. Grundrechtsrügen

Die Beschwerdeführerinnen und Beschwerdeführer rügen hinsichtlich der Eingriffsermächtigungen aus §§ 33 i.V.m. 26a und 46a, 33c, 33d, 34, 35, 44 SOG M-V, die Verletzung ihrer Grundrechte auf informationelle Selbstbestimmung und auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), wobei hinsichtlich §§ 33, 33b, 33c, 33d, 35 und 44 SOG M-V die Grundrechte insbesondere betroffen sind, indem die Eingriffsschwelle für diese Maßnahmen auf das Vorfeld konkreter Gefahren abgesenkt wird und in § 48b SOG M-V keine ausreichenden Kontrollmechanismen durch den Landesdatenschutzbeauftragten vorgesehen sind.

Hinsichtlich §§ 33c und 33d SOG M-V rügen sie außerdem die Verletzung des Fernmeldegeheimnisses (Art. 10 GG), hinsichtlich §§ 33b, 33c Abs. 5 und 33d Abs. 3 Satz 3 SOG M-V auch eine Verletzung von Art. 13 GG.

2. Eigene und gegenwärtige Beschwer

Die Beschwerdeführerinnen und Beschwerdeführer werden mit einiger Wahrscheinlichkeit zukünftig von Maßnahmen auf der Grundlage der angegriffenen Ermächtigungen betroffen sein.

a) Wahrscheinlichkeit der Betroffenheit von heimlichen Maßnahmen nach §§ 33, 33b, 33c, 33d, 35 SOG M-V

Eine gegenwärtige Betroffenheit der Beschwerdeführerinnen und Beschwerdeführer ergibt sich schon aus der Streubreite der angegriffenen Befugnisse (vgl. zu diesem Maßstab BVerfGE 150, 309, 325f), insbesondere soweit sie im Vorfeld einer konkreten Gefahr unter Bezugnahme auf die §§ 49 und 67a i.V.m. 67c SOG M-V ansetzen und hierbei auch Dritte miterfassen.

Hinzu kommt, dass die Beschwerdeführerinnen und Beschwerdeführer aufgrund ihrer beruflichen oder persönlichen Aktivitäten noch sehr viel wahrscheinlicher als der Bevölkerungsdurchschnitt von Maßnahmen erfasst werden, die auf die angegriffenen Ermächtigungsnormen zu individualbezogenen verdeckten Überwachungsmaßnahmen gestützt werden. Insgesamt gilt für die angegriffenen Maßnahmen der §§ 33, 33b, 33c, 33d, 35 SOG M-V, dass darin die Eingriffsschwelle in den Bereich der diffusen Sachlagen vorverlagert ist, in denen personenbezogene Gefährderprognosen nicht anders als anhand von Einschätzungen der ideologischen Neigung und dem sozialen Umfeld der betroffenen Person getroffen werden können. Die Beschwerdeführerinnen und Beschwerdeführer sind einem größeren Risiko als der durchschnittliche Bürger oder die durchschnittliche Bürgerin ausgesetzt, Zielobjekt solcher Maßnahmen zu werden, weil sie

mehr Kontakte in die verschiedensten Lebenswelten haben und gleichzeitig exponiert agieren.

Bei allen fünf Beschwerdeführerinnen und Beschwerdeführern ist ferner nicht auszuschließen, dass sie als direkte Zielpersonen von Maßnahmen nach §§ 33, 35 in Betracht gezogen werden, weil sie als „Kontaktpersonen“ im Sinne des § 27 Abs. 3 Nr. 2 SOG M-V angesehen werden.

Im Einzelnen ist dazu in Bezug auf die Beschwerdeführerinnen und Beschwerdeführer Folgendes zu ergänzen: Die Beschwerdeführerin zu 1 und der Beschwerdeführer zu 2 stehen aufgrund ihrer beruflichen Betätigung als Journalist und als Strafverteidigerin bzw. Anwältin für Asyl- und Aufenthaltsrecht mit einer Vielzahl von Personen in Kontakt, die von der Polizei dem Bereich des Extremismus zugeordnet werden und daher entweder als direkte Zielpersonen mit den genannten heimlichen Methoden polizeilich überwacht werden oder als Kontaktpersonen zu solchen Personen (§ 27 Abs. 3 Nr. 2 SOG M-V). Beide nutzen bei der Kommunikation mit solchen Personen technische Hilfsmittel wie Messenger-Dienste über ihre Smartphones oder so genannte Chat-Rooms über Computer oder treffen sich mit solchen Personen im öffentlichen Straßenraum. Für beide besteht daher das Risiko, dass sie als Dritte durch Überwachungsmaßnahmen miterfasst werden, sei es in Form des Mitverfolgens ihrer Kommunikation mit Ziel- oder Kontaktpersonen bei der Quellen-TKÜ oder des direkten Zugriffs auf ihre IT-Systeme, weil die Polizei annimmt, dass dort ermittlungsrelevante Informationen einer des Terrorismus verdächtigen Person gespeichert sind, in Form des Mithörens eines Treffens durch eine V-Person oder in Form von Abhörmaßnahmen in- oder außerhalb von Wohnungen oder durch die Kontrolle eines nach § 35 SOG M-V ausgeschriebenen Fahrzeugs, in dem sie auf dem Weg zu einem Gespräch mit einem Informanten oder zu einem Gerichtstermin mitfahren.

Der Umstand, dass die Beschwerdeführerin zu 1 sowie der Beschwerdeführer zu 2 als Berufsgeheimnisträger und Berufsgeheimnisträgerin durch

§ 26b SOG M-V besonders geschützt sind, steht ihrer Beschwer nicht entgegen, da dieser Schutz aufgrund der in § 26b SOG M-V vorgesehenen Ausnahmeregelungen nicht vollständig ist.

Für die Beschwerdeführerin zu 3 und die Beschwerdeführer zu 4 und 5 gilt, dass sie aufgrund ihrer Betätigung im Bereich des politischen Aktivismus oder in der Fußballszene des F.C. Hansa Rostock sowohl aufgrund ihrer Kontakte zu Dritten, die Zielpersonen polizeilicher Überwachung sein können, von Maßnahmen mitbetroffen sein können als auch selbst Gegenstand von Überwachungen als Ziel- oder als Kontaktperson zu Zielpersonen. Sowohl der Bereich des politischen Aktivismus als auch die Fußball-Szene steht im Fokus der polizeilichen Aufmerksamkeit, da in diesem Zusammenhang auch regelmäßig Ermittlungsverfahren wegen schwererer Straftaten geführt werden. In Zusammenhang mit Großveranstaltungen wie Großdemonstrationen oder so genannten Risikospielen sind polizeiliche Aufklärungsmaßnahmen im Vorfeld üblich. In Mecklenburg-Vorpommern sind Fälle von Einsätzen ausländischer Verdeckter Ermittler oder Durchsuchungen auf präventivpolizeilicher Grundlage zur Vorfeldaufklärung von politischen Protesten bekannt geworden, es ist wahrscheinlich, dass weiterhin entsprechende verdeckte Maßnahmen in diesen Bereichen eingesetzt werden.

Die Beschwerdeführerin zu 3 und die Beschwerdeführer zu 4 und 5 sind dabei in ihren jeweiligen Szenen exponiert, treten öffentlich auf und stehen in Verbindung zu einem Netzwerk von anderen aktiven Personen. Daher sind sie jedenfalls – wie die Beschwerdeführerin zu 1 und der Beschwerdeführer zu 2 – stärker als der Durchschnitt der Bevölkerung der Gefahr ausgesetzt, dass sie von Überwachungsmaßnahmen mitbetroffen sind, indem sie zum Beispiel in einem Auto mitfahren, das nach § 35 SOG M-V zur Beobachtung ausgeschrieben ist, oder indem sie mit einer Person online kommunizieren, die wiederum als Ziel- oder Kontaktperson von Überwachungsmaßnahmen betroffen ist.

b) Wahrscheinlichkeit der Betroffenheit von Maßnahmen gemäß § 34 SOG M-V

Hinsichtlich der Betroffenheit durch den Einsatz unbemannter Luftfahrsysteme nach § 34 S. 1 Nr. 2-5 SOG M-V gilt das unter a) zur Betroffenheit von Maßnahmen nach den §§ 33 ff SOG M-V ausgeführte. Hinsichtlich der Betroffenheit durch den Einsatz unbemannter Luftfahrsysteme nach § 34 S. 1 Nr. 1 SOG M-V gilt, dass die Beschwerdeführerinnen und Beschwerdeführer aufgrund der Überwachung des öffentlichen Raums, die über den Einsatz von Drohnen für Überblicksaufnahmen sehr breit gestreut sein kann, selbst und gegenwärtig betroffen sind, indem sie Menschenansammlungen wie zum Beispiel bei öffentlichen Kultur- oder Wahlkampfveranstaltungen besuchen oder - im Fall des Beschwerdeführers zu 2 - beobachten, oder indem die Beschwerdeführer zu 4 und 5 sich zu Fußballspielen bewegen oder indem die Beschwerdeführerin zu 3 an öffentlichen politischen Aktionen teilnimmt, die nicht unter das Versammlungsgesetz fallen.

c) Wahrscheinlichkeit der Betroffenheit von Rasterfahndung nach § 44 SOG M-V

Vom erweiterten Anwendungsbereich der Maßnahme der Rasterfahndung können nach der Gestalt der Regelung die Beschwerdeführerinnen und Beschwerdeführer wie die Bevölkerung insgesamt ohne weiteres betroffen sein. Die Rasterfahndung kann naturgemäß alle betreffen, deren Daten in Datei-Systemen von Behörden, anderen öffentlichen Stellen und von Stellen außerhalb der öffentlichen Verwaltung gespeichert sind.

d) Besonderes Schutzbedürfnis hinsichtlich IT-Sicherheit

Die Beschwerdeführerinnen und Beschwerdeführer zu 1 bis 5 sind darauf angewiesen, dass – infolge der Fehlbarkeit menschlichen Handelns als solche unvermeidbare – Sicherheitslücken ihrer IT-Systeme schnellstmöglich geschlossen werden. Denn je länger eine Sicherheitslücke besteht, desto höher die Wahrscheinlichkeit, dass sie durch interessierte Kreise gefunden

und für Angriffe auf die IT-Systeme der Beschwerdeführerinnen und Beschwerdeführer missbraucht wird.

Die Beschwerdeführer zu 1 und 2 bedürfen eines besonderen Schutzniveaus von IT-Systemen und IT-gestützter Kommunikation, um als Rechtsanwältin bzw. Journalist bei der Kommunikation mit einem bestimmten Kreis von Mandantinnen und Mandanten bzw. Informantinnen und Informanten die Vertraulichkeit sicherstellen zu können.

Die Beschwerdeführer zu 4 und 5 müssen aufgrund ihrer auch internationalen Aktivitäten im Bereich der Fußball-Szene unter anderem befürchten, dass zum Beispiel ausländische Geheimdienste – wie im Fall des Beschwerdeführers zu 4 der türkische – sich darum bemühen könnten, Zugriff auf ihre IT-Systeme zu erhalten. Dasselbe gilt für die Beschwerdeführerin zu 3 insoweit Klima- und Umwelt-Aktivistinnen und -Aktivisten nicht nur in Zusammenhang mit Themen von internationaler Bedeutung wie der Ostsee-Pipline oder bei Protesten anlässlich von Regierungs-Gipfeln international kooperieren.

Jedenfalls haben alle Beschwerdeführerinnen und Beschwerdeführer ein legitimes privates Interesse daran, dass ihre IT-Systeme nicht von ausländischen Diensten oder kriminellen Organisationen infiltriert und überwacht werden.

3. Unmittelbare Beschwer

Die Beschwerdeführerinnen und Beschwerdeführer sind durch die angegriffenen Regelungen auch unmittelbar beschwert. Denn sie können als potenziell Betroffene nicht ohne weiteres gegen konkrete Umsetzungsakte gerichtlich vorgehen, weil sie während der Umsetzung der angegriffenen Maßnahme keine Kenntnis von deren Umsetzung erlangen und auch in Fällen, in denen eine nachträgliche Bekanntgabe vorgesehen ist, davon aufgrund weitreichender Ausnahmetatbestände langfristig abgesehen wer-

den kann (siehe zu diesem Maßstab nur BVerfGE 141, 220, 261). Hinsichtlich der verdeckt einzusetzenden Maßnahmen der §§ 33 ff SOG M-V erschließt sich dies unmittelbar. Hinsichtlich der angegriffenen vermeintlichen offenen Maßnahmen des Drohneneinsatzes bei Großveranstaltungen nach § 34 S. 1 Nr. 1 SOG M-V und der Identitätsfeststellung und Durchsuchung gemäß § 35 Abs. 2 SOG M-V anlässlich von Ausschreibungen nach § 35 Abs. 1 SOG M-V ist folgendes auszuführen:

Der Einsatz von – aufgrund des technischen Fortschritts immer kleineren und unauffälligeren – unbemannten Fluggeräten ist in der realen Umsetzung nicht tatsächlich offen. Den Betroffenen, von denen im Anwendungsbereich des § 34 S. 1 Nr. 1 SOG M-V durch solche Drohnen Bilder gemacht werden, wird oftmals nicht bewusst sein, dass sie gefilmt werden. Selbst wenn sie wahrnehmen, dass ein unbemanntes Fluggerät über ihnen fliegt, können sie nicht erkennen, ob dieses filmt und wer dieses einsetzt. Aufgrund der Ausgestaltung der Regelung wird die Anfertigung von Bildmaterial durch die Polizei auch nicht in jedem Einzelfall in anderer Form publik gemacht. Die Betroffenen müssen daher beim Aufenthalt in größeren Menschenansammlungen davon ausgehen, dass die gesetzliche Option des Drohnen-Einsatzes unter solchen Umständen dazu führt, dass sie und ihre Handlungen in der Öffentlichkeit gefilmt werden.

Dasselbe gilt für die Weitergabe von im Rahmen einer Kontrolle aufgrund einer Ausschreibung nach § 35 SOG M-V gewonnenen Daten. Wenn die Beschwerdeführerinnen und Beschwerdeführer aufgrund einer Ausschreibung nach § 35 Abs. 1 SOG M-V als ausgeschriebene oder miterfasste Personen nach § 35 Abs. 2 SOG M-V kontrolliert werden, wird ihnen nicht von Gesetzes wegen der Anlass der Kontrolle bekannt und daher auch nicht die Möglichkeit, dass ihre Daten nach § 35 Abs. 2 S. 2 SOG M-V an die ausschreibende Behörde weitergegeben werden.

Insofern haben beide gesetzlichen Ermächtigung als solche bereits unmittelbare Wirkung für die Beschwerdeführerinnen und Beschwerdeführer, die aufgrund ihrer Lebenspraxis wahrscheinlich von diesen Maßnahmen

betroffen sind. Sie müssen damit rechnen, ohne ihr Wissen gefilmt zu werden und dass bei Kontrollen erhobene Daten an andere Polizeibehörden weitergegeben werden.

III. Subsidiarität

Der Subsidiaritätsgrundsatz steht der Verfassungsbeschwerde nicht entgegen. Die neuen Regelungen des SOG M-V werfen spezifisch verfassungsrechtliche Fragen auf, hinsichtlich derer eine Einzelfallentscheidung eines Instanzengerichts keine verbesserte Entscheidungsgrundlage bieten kann. Außerdem ist den Beschwerdeführerinnen und Beschwerdeführern auch nicht zumutbar, zunächst den Instanzenweg zu beschreiten, da entweder in Bezug auf die Maßnahmen, die auf die angegriffenen Regelungen gestützt werden könnten, faktisch nur nachträglich um Rechtsschutz bei den Verwaltungsgerichten nachgesucht werden kann, oder den Beschwerdeführerinnen und Beschwerdeführern erst gar nicht zur Kenntnis gelangt, dass sie von heimlichen Maßnahmen betroffen waren, weil sie darüber erst nach Ablauf längerer Zeit oder im Einzelfall auch gar nicht unterrichtet werden (§ 46a Abs. 4 S. 4 SOG M-V). Vorbeugender Rechtsschutz ist in Bezug auf die angegriffenen Regelungen durch die Beschwerdeführerinnen und Beschwerdeführer nicht zu erhalten, da sie naturgemäß im Vorfeld von heimlichen Maßnahmen nicht wissen können, dass solche Maßnahmen gegen sie eingesetzt werden.

Ein vorbeugender Rechtsschutz in Gestalt einer vorbeugenden Unterlassungs- oder Feststellungsklage ist den Beschwerdeführerinnen und Beschwerdeführern zumindest sehr weitgehend nicht eröffnet. Denn solche Klagen setzen nach gefestigter Rechtsprechung voraus, dass sich ein drohendes Verwaltungshandeln bzw. ein zukünftiges Rechtsverhältnis bereits hinreichend konkret abzeichnet und die für eine Rechtmäßigkeitsprüfung erforderliche Bestimmtheit aufweist (vgl. zur vorbeugenden Unterlassungsklage nur BVerwGE 45, 99, 105; sowie zur Feststellungsklage BVerwGE 59, 310, 318).

Eine nähere Bestimmung drohender Überwachungsmaßnahmen und anschließender Datenweiterarbeitungen ist den Beschwerdeführerinnen und Beschwerdeführern jedoch nicht möglich. Hierzu müssten sie nämlich ein konkretes behördliches Verfahren bezeichnen können, in dessen Rahmen ihnen eine Überwachung – sei es als Zielpersonen oder als Drittbetroffenen – droht. Aus ihrer Betroffenenperspektive lassen sich solche Verfahren im Voraus aber nicht absehen.

Hinsichtlich des nach dem Wortlaut des Gesetzes „offenen", tatsächlich aber nur schwerlich wahrnehmbaren Drohneneinsatzes nach § 34 S. 1 Nr. 1 SOG M-V ist festzuhalten: Gerade bei Großveranstaltungen wie Fußballspielen oder Wahlkampfveranstaltungen ist nahe liegend, dass unbemannte Luftfahrsysteme in einer Form eingesetzt werden, die für die gefilmten Personen nicht wahrnehmbar ist und über die sie nach dem Gesetz als Betroffene auch nicht in jedem Fall informiert werden müssen. Wenn Betroffenen aber gar nicht wissen, dass sie mittels Einsatz einer Drohne gefilmt wurden, können sie auch keine rechtliche Überprüfung der einzelnen Maßnahme anstrengen.

Hinsichtlich offener Annexmaßnahmen des § 35 Abs. 2 SOG M-V (Identitätsfeststellung und Durchsuchung bei Ausschreibungen zur gezielten Kontrolle nach § 35 Abs. 1 SOG M-V) sieht S. 2 vor, dass die aus solchen Maßnahmen gewonnenen Erkenntnisse an die ausschreibende Polizeibehörde übermittelt werden. Eine Mitteilung an die Betroffenen, dass die aufgrund der offenen Maßnahmen zu ihnen gewonnenen Daten in Zusammenhang mit einer Ausschreibung nach § 35 Abs. 1 SOG M-V übermittelt werden, ist jedoch nicht vorgesehen. Gegen diese verdeckte Datenweitergabe ist daher mangels Kenntnis für die Betroffenen der ordentliche Rechtsweg nicht effektiv nutzbar.

D. Begründetheit

Die Verfassungsbeschwerde ist begründet.

I. Besondere Mittel der Datenerhebung (§ 33 SOG M-V)

Die in § 33 SOG M-V enthaltene Ermächtigung zu Datenerhebungen durch längerfristige Observationen, Bild- und Tonaufnahmen bzw. -aufzeichnungen außerhalb von Wohnungen und den Einsatz von Vertrauenspersonen und verdeckt Ermittelnden verletzt das Recht auf informationelle Selbstbestimmung. Dies ergibt sich zunächst daraus, dass sowohl § 33 Abs. 2 Satz 1 SOG M-V also auch § 33 Abs. 2 Satz 3 i.V.m. § 67a Abs. 1 SOG M-V solche Datenerhebungen auch im Vorfeld konkreter Gefahren zulassen (dazu unter 1.). Zudem sind die Regelungen zum Kernbereichsschutz (dazu unter 2.) und zu den Benachrichtigungspflichten (dazu unter 3.) unzureichend.

1. Unzureichende Eingriffsschwelle

Der mecklenburg-vorpommersche Gesetzgeber nimmt für sich in Anspruch, die vom Bundesverfassungsgericht im Urteil zum BKA-Gesetz aufgestellten Vorgaben für eine Vorverlagerung polizeilicher Eingriffsbefugnisse umzusetzen (siehe u.a. Gesetzbegründung LT-Drs. 7/3694). Dies ist ihm jedoch nicht gelungen.

Der Gesetzgeber hat es versäumt, die in § 33 Abs. 2 Satz 1 SOG M-V enthaltene Gefahrenschwelle, die weitgehend dem vom Bundesverfassungsgericht für verfassungswidrig erklärten § 20g Abs. 1 Satz 1 Nr. 2 BKAG a.F. entspricht, anzupassen. Er hat, im Gegenteil, die von § 49 SOG M-V in Bezug genommenen Delikte um verschiedene Vergehen erweitert und die Befugnis dahingehend ausgeweitet, dass die Maßnahme auch dann zulässig ist, wenn die Aufklärung des Sachverhalts ansonsten wesentlich erschwert

wäre. Zusätzlich wurde in § 33 Abs. 2 Satz 3 SOG M-V eine weitere Eingriffsschwelle speziell zur Verhütung terroristischer Straftaten geschaffen, die ebenfalls nicht den verfassungsrechtlichen Vorgaben entspricht.

Im Folgenden werden zunächst die verfassungsrechtlichen Anforderungen an die Gefahrenschwelle dargestellt (dazu unter a). Sodann wird dargelegt, dass sowohl die in § 33 Abs. 2 Satz 1 SOG M-V enthaltene Gefahrenschwelle (dazu unter b) als auch diejenige aus § 33 Abs. 2 Satz 3 SOG M-V (dazu unter c) nicht diesen Anforderungen genügen.

a) Maßstab

Der Einsatz der in § 33 Abs. 1 SOG M-V genannten Datenerhebungsmittel kann je nach Einsatzmodalität eine hohe Eingriffsintensität aufweisen (BVerfGE 141, 220, 286f). Eine gesetzliche Eingriffsermächtigung, die eingriffsintensive Einsatzformen erlaubt, muss daher an eine hinreichend konturierte tatsächliche Eingriffsschwelle und an den Schutz besonders wichtiger Rechtsgüter gebunden werden (BVerfGE 141, 200, 269ff).

Von Verfassungs wegen ist der Gesetzgeber allerdings nicht darauf angewiesen, solche Datenerhebungen in tatsächlicher Hinsicht von der hergebrachten polizeilichen Eingriffsschwelle einer konkreten Gefahr abhängig zu machen. Er darf der Polizei auch Datenerhebungen im Vorfeld einer konkreten Gefahr erlauben, wenn er den Eingriffsanlass gleichwohl hinreichend konturiert beschreibt. Das Bundesverfassungsgericht hat in dem Urteil zum BKAG zwei Typen von Schadensprognosen genannt, die auch eingriffsintensive verdeckte Überwachungsmaßnahmen legitimieren können.

Zum einen dürfen solche Maßnahmen an eine ereignisbezogene Prognose in einer Situation gebunden werden, in der noch Informationslücken bestehen (BVerfGE 141, 220, 272):

Allgemeine Erfahrungssätze reichen […] allein nicht aus, um den Zugriff zu rechtfertigen. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die im

Einzelfall die Prognose eines Geschehens, das zu einer zurechenbaren Verletzung der hier relevanten Schutzgüter führt, tragen […]. Eine hinreichend konkretisierte Gefahr in diesem Sinne kann danach schon bestehen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen dafür zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann.

Werden diese Ausführungen in polizeirechtliche Terminologie „übersetzt", so entspricht dieser Prognosetyp zumindest weitgehend dem polizeilichen Gefahrenverdacht. Die Prognose bleibt auf ein konkretes, ansatzweise konturiertes Schadensereignis bezogen. Allerdings werden noch weitere Informationen benötigt, um eine tragfähige Gefahrprognose zu erstellen.

Zum anderen hält das Bundesverfassungsgericht das Zugrundelegen eines anderen Prognosetyps für zulässig, der deutlich stärker vom hergebrachten Regelungsmodell der konkreten Gefahr abweicht. Die Formulierung aus dem Urteil zum BKAG lautet wie folgt (BVerfGE 141, 220, 272f; für eine Erstreckung auch über den Sonderfall der Terrorismusbekämpfung hinaus nunmehr BVerfG, Beschl. v. 27.05.2020, 1 BvR 1873/13, 1 BvR 2618/13, Rn. 149):

In Bezug auf terroristische Straftaten, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, können Überwachungsmaßnahmen auch dann erlaubt werden, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird."

Das polizeiliche Wahrscheinlichkeitsurteil, das die Grundlage einer Überwachungsmaßnahme bildet, bezieht sich in dieser Fallkonstellation nicht auf ein zumindest ansatzweise konturiertes zukünftiges Ereignis, sondern auf eine Person. Die hergebrachte Gefahrprognose wird mithin durch eine „Gefährderprognose“ ergänzt (vgl. zu unterschiedlichen Deutungen der zitierten Ausführungen des Bundesverfassungsgerichts in der juristischen Literatur beispielhaft Darnstädt, DVBl 2017, S. 88ff; Kulick, AöR 143 (2018), S. 175ff; Enders, DÖV 2019, S. 205ff; Ogorek, JZ 2019, S. 63ff; Bäcker, in: Kulick/Goldhammer, Der Terrorist als Feind?, 2020, S. 147, 155ff; Kießling, ebd., S. 261, 264ff).

b) § 33 Abs. 2 Satz 1 SOG M-V

§ 33 Abs. 2 Satz 1 SOG M-V entspricht weitgehend der vom Bundesverfassungsgericht für verfassungswidrig erklärten Vorschrift des § 20g Abs. 1 Satz 1 Nr. 2 BKAG a.F. Sie knüpft nicht an die herkömmliche polizeirechtliche Terminologie der konkreten Gefahr für ein Rechtsgut an (vgl. etwa § 45 Abs. 1 Satz 1 Nr. 1 BKAG n.F.), sondern lässt es genügen, dass „Tatsachen die Annahme der Begehung von Straftaten von erheblicher Bedeutung (§ 49) rechtfertigen“.

Die Vorschrift schließt damit nicht aus, dass sich die Prognose allein auf allgemeine Erfahrungssätze stützt. Sie enthält weder die Anforderung, dass ein wenigstens seiner Art nach konkretisiertes und absehbares Geschehen erkennbar sein muss, noch die alternative Anforderung, dass das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründen muss, dass sie in überschaubarer Zukunft terroristische Straftaten begeht. Damit gibt sie den Behörden und Gerichten keine hinreichend bestimmten Kriterien an die Hand und eröffnet Maßnahmen, die unverhältnismäßig weit sein können (vgl. BVerfGE 140, 220, 29).

Darüber hinaus schützen die in § 49 SOG M-V genannten Straftatbestände jedenfalls zu einem großen Teil nicht Rechtsgüter, die als besonders gewichtig anzusehen sind. Das gilt insbesondere hinsichtlich der neu in den § 49 SOG M-V aufgenommenen Straftaten der Computersabotage in einem besonders schweren Fall (§ 303b Abs. 4 StGB), der Geldwäsche (§ 261 StGB) und des Einschleusens von Ausländern (§ 96 Abs. 2 AufenthG).

Auch die Eingriffsschwellen zur Verhinderung terroristischer Straftaten genügen nicht den verfassungsrechtlichen Anforderungen.

c) § 33 Abs. 2 Satz 3 SOG-MV i.V.m. § 67a Abs. 1 SOG M-V

Die in § 33 Abs. 1, 2 Satz 3 i.V.m. § 67a Abs. 1 SOG M-V enthaltenen Eingriffstatbestände lehnen sich eng an die Formulierungen des Bundesverfassungsgerichts an. Dies ist für sich genommen verfassungsrechtlich nicht zu beanstanden, wenngleich der Gesetzgeber sich damit seiner Gestaltungsaufgabe weitgehend entzogen hat, die verfassungsrechtlichen Anforderungen in eine in sich kohärente fachrechtliche Terminologie zu überführen. Verfassungswidrig sind diese Vorschriften jedoch insoweit, als sie die Gegenstände der angeordneten polizeilichen Wahrscheinlichkeitsurteile abweichend von dem Bundesverfassungsgericht beschreiben. Die angegriffenen Normen verlangen nämlich nicht die Prognose von Schäden für bestimmte Rechtsgüter, sondern von bestimmten Straftaten bzw. einer Affinität bestimmter Personen zu bestimmten Straftaten. Dieser abweichende Regelungsansatz wäre nur dann unschädlich, wenn die in Bezug genommenen Straftaten jeweils unmittelbar hinreichend gewichtige Rechtsgüter schädigen würden. Dies ist jedoch nicht der Fall.

§ 33 Abs. 1, 2 Satz 3 i.V.m. § 67a Abs. 1 Nr. 1 SOG M-V greift den ersten Prognosetyp im Gefahrenvorfeld aus dem Urteil zum BKAG auf, der dem polizeilichen Gefahrenverdacht entspricht oder zumindest nahekommt. Das zu prognostizierende Schadensereignis muss nach § 67a Abs. 1 Nr. 1 SOG M-V in einer terroristischen Straftat bestehen. Dieser Begriff wird in

§ 67c SOG M-V definiert. Terroristische Straftaten sind danach verschiedene Normen des StGB sowie des Gesetzes über die Kontrolle von Kriegswaffen, des Waffengesetzes und des Völkerstrafgesetzbuches, die im In- oder Ausland begangen werden. Darüber hinaus müssen die Taten dazu bestimmt sein, die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates, eines Landes oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen und gleichzeitig durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat, ein Land oder eine internationale Organisation erheblich schädigen können.

§ 67c SOG M-V nimmt damit zwar Straftatbestände in Bezug, die sich auf den Schutz besonders wichtiger Rechtsgüter zurückführen lassen. Allerdings wird durch einige der Tatbestände im Rahmen der präventiv ausgerichteten Eingriffsermächtigung die tatsächliche Eingriffsschwelle entgrenzt. Grund hierfür ist, dass die Tatbestände Handlungen verbieten und unter Strafe stellen, die teils weit im Vorfeld von Rechtsgutsverletzungen angesiedelt sind.

Diese mittelbare Entgrenzung des tatsächlichen Eingriffsanlasses lässt sich anhand von § 89a StGB illustrieren, auf den § 67c Nr. 1 SOG M-V ausdrücklich verweist. Diese Norm stellt die Vorbereitung eines terroristischen Anschlags durch einen potentiellen Einzeltäter bereits in einem sehr frühen Stadium unter Strafe, wenn noch kaum absehbar ist, ob der Täter sein Vorhaben letztlich in die Tat umsetzen können wird. Die Rechtsprechung begrenzt die sehr weit gefasste Norm vor allem, indem sie hohe Anforderungen an den subjektiven Tatbestand stellt (vgl. BGH, Urt. v. 8.05.2014, 3 StR 243/13, Rn. 45; BGH, Urt. v. 27.10.2015, 3 StR 218/15 Rn. 10).

Diese Begrenzung wirkt sich jedoch im präventivpolizeilichen Handlungsfeld allenfalls schwach aus. Denn im Vorfeld lassen sich die genauen Ab-

sichten und die Motivation des Betroffenen kaum erschließen. Als strafrechtlicher Vorfeldtatbestand bietet § 89a StGB daher kaum Anknüpfungspunkte für eine präventivpolizeiliche Schadensprognose. Diese Prognose kann vielmehr in weitem Umfang nur an hoch ambivalente und vage Ereignisse anknüpfen. Dieser Effekt verstärkt sich noch, wenn eine polizeiliche Ermächtigung wie § 33 Abs.1, 2 Satz 3 i.V.m. § 67a Abs. 1 SOG M-V den Eingriffsanlass ins Vorfeld der hergebrachten Eingriffsschwelle der konkreten Gefahr verschiebt.

Die zusätzlichen Anforderungen, die § 67c SOG M-V an eine terroristische Straftat stellt, sind teilweise weiter als die des § 89a StGB selbst und sind daher nicht geeignet, der Entgrenzung der Eingriffsbefugnis entgegenzuwirken. Somit verstärken die materiell-strafrechtliche und die prozedural-polizeirechtliche Vorverlagerung einander, so dass sich der Eingriffstatbestand nahezu auflöst und Überwachungsmaßnahmen beinahe nach Belieben ermöglicht werden.

Beispielsweise macht sich nach § 89a Abs. 1, Abs. 2 Nr. 2 StGB unter anderem strafbar, wer sich vielfältig nutzbare Gegenstände beschafft, um damit einen terroristischen Anschlag zu begehen. Den Straftatbestand erfüllt etwa der Kauf von Unkrautvernichtungsmitteln in der Absicht, daraus Sprengstoff herzustellen.

Grundlage für die Anwendung der polizeilichen Kompetenzen aus § 33 Abs. 1, 2 Satz 3 i.V.m. § 67a Abs. 1 Nr. 1 SOG M-V wären in diesem Fall erste Anhaltspunkte dafür, dass jemand in absehbarer Zeit Unkrautvernichtungsmittel kaufen könnte – wenn gleichzeitig anzunehmen wäre, dass er das Unkrautvernichtungsmittel bei einem terroristischen Anschlag einsetzen will. Die zweitere Annahme kann dabei aber nur auf Faktoren wie den persönlichen Überzeugungen und den sozialen Beziehungen des Betroffenen gestützt werden, die einen so schwerwiegenden Grundrechtseingriff für sich genommen nicht ansatzweise rechtfertigen können.

Gleichfalls durch eine inadäquate Bezugnahme auf strafrechtliche Vorfeldtatbestände zu weit gefasst ist § 33 Abs. 1, 2 Satz 3 i.V.m. § 67a Abs. 1 Nr. 2 SOG M-V, der die „Gefährderprognose“ des Bundesverfassungsgerichts aufgreift. Diese Regelung erfordert ein personenbezogenes Wahrscheinlichkeitsurteil darüber, dass die Zielperson der Überwachungsmaßnahme zukünftig eine terroristische Straftat begehen wird, ohne dass sich diese Straftat bereits näher konturiert abzeichnen müsste. Die Legaldefinition der terroristischen Straftat in § 67c SOG M-V ist verfassungsrechtlich als Element einer präventiv ausgerichteten Eingriffsermächtigung insoweit unbedenklich, als sie sich auf schwere Gewalttaten bezieht, die mit einer spezifisch terroristischen Zielsetzung begangen werden und eine herausgehobene Schadenseignung aufweisen.

Jedoch verweist § 67c SOG M-V auch auf strafrechtliche Vorfeldtatbestände, die im Kontext einer präventiv ausgerichteten personenbezogenen Prognose wiederum die tatsächliche Eingriffsschwelle entgrenzen lassen können. Insbesondere gilt dies für die in § 67c Nr. 1 SOG M-V in Bezug genommenen Vereinigungstatbestände der § 129a und § 129b StGB. Diese Normen stellen Gründungs-, Beteiligungs- und Unterstützungshandlungen im Zusammenhang mit terroristischen Vereinigungen unter Strafe. Im Zusammenwirken mit diesen Tatbeständen erlaubt § 33 Abs. 1, 2 Satz 3 i.V.m. § 67a Abs. 1 Nr. 2 SOG M-V eingriffsintensive Überwachungsmaßnahmen bereits dann, wenn von der Zielperson der Maßnahme eine vereinigungsbezogene Handlung erwartet wird, ohne dass sich diese konkret abzeichnen müsste. Denkbar wäre sogar, eine „Gefährderprognose“ abzugeben, ohne dass sich die betreffende Vereinigung bereits benennen ließe oder überhaupt existieren müsste, zumal § 129a StGB gerade auch die Gründung einer terroristischen Vereinigung untersagt. Erst recht setzt § 33 Abs. 1, 2 Satz 3 i.V.m. § 67a Abs. 1 Nr. 2 SOG M-V, soweit er auf § 129a und § 129b StGB bezogen wird, keine auch nur vagen Anhaltspunkte dafür voraus, dass sich die betroffene Person selbst einmal an Gewalttaten einer terroristischen Vereinigung beteiligen oder sonst zu ihnen beitragen wird. Insgesamt ermöglichen die Normen Überwachungsmaßnahmen in diffusen

Sachlagen, in denen die personenbezogene „Gefährderprognose“ zwangsläufig primär auf der ideologischen Neigung und dem sozialen Umfeld der betroffenen Person und damit auf hochgradig ambivalenten und wenig aussagekräftigen Umständen beruht. Die verfassungsrechtlichen Anforderungen an personenbezogene Wahrscheinlichkeitsurteile als Grundlage eingriffsintensiver Maßnahmen werden damit weit verfehlt.

Darüber hinaus verstoßen die angegriffenen Normen auch gegen das aus dem Rechtsstaatsprinzip erwachsende Gebot der Normklarheit. Die Normenklarheit setzt der Verwendung gesetzlicher Verweisungsketten Grenzen. An einer normenklaren Rechtsgrundlage fehlt es zwar nicht schon deshalb, weil in einer Norm auf eine andere Norm verwiesen wird. Doch müssen Verweisungen begrenzt bleiben, dürfen nicht durch die Inbezugnahme von Normen, die andersartige Spannungslagen bewältigen, ihre Klarheit verlieren und in der Praxis nicht zu übermäßigen Schwierigkeiten bei der Anwendung führen. Unübersichtliche Verweisungskaskaden sind mit den grundrechtlichen Anforderungen daher nicht vereinbar (BVerfGE 154, 152, Rn. 215).

Dem werden die angegriffenen Regelungen nicht gerecht. Zahlreiche Verweisungen zwischen verschiedenen Eingriffsbefugnissen, Legaldefinitionen und Strafgesetzen schaffen ein unübersichtliches Regelungsgeflecht, in dem nur schwer erkennbar ist, welche Befugnisse unter welchen Voraussetzungen einsetzbar sind. Für die Befugnisse nach § 33 Abs. 1 SOG M-V erweitert beispielsweise § 33 Abs. 2 Satz 3 durch einen Verweis auf die Voraussetzungen des § 67a Abs. 1 SOG M-V. Dieser verweist wiederum in Nr. 1 und 2 auf die Legaldefinition der terroristischen Straftat in § 67c SOG M-V, der seinerseits einen Katalog von Straftaten im StGB und anderen Gesetzen enthält, welche teilweise selbst Verweise auf andere Normen enthalten (z.B. § 129a Abs. 2 Nr. 2 StGB, der auf § 303b StGB verweist, der auf § 303a StGB verweist).

2. Unzureichender Kernbereichsschutz in § 26a SOG M-V

Die Regelung des § 26a SOG M-V gewährleistet nur unzureichenden Schutz des Kernbereichs privater Lebensgestaltung. Als vor die Klammer gezogene Regelung gilt § 26a SOG M-V für alle, insbesondere die verdeckten Maßnahmen des SOG M-V. Die folgenden Erläuterungen gelten daher für sämtliche, zur Datenerhebung ermächtigende Normen des SOG M-V, die keine Spezialregelung für den Kernbereichsschutz enthalten, erfolgen aber hier im Hinblick auf die Ermächtigung zum Einsatz besonderer Mittel der Datenerhebung nach § 33 Abs. 1 SOG M-V.

Die Regelung des § 26a SOG M-V versteht sich als Umsetzung der bundesverfassungsgerichtlichen Vorgaben an den Schutz des Kernbereiches privater Lebensgestaltung (vgl. LT-Drs. 7/3694 S. 156) kann diese jedoch nur teilweise erfüllen. So sieht § 26a Abs. 3 Satz 1 SOG M-V grundsätzlich ein Abbrucherfordernis für Maßnahmen vor, wenn während der Erhebung Tatsachen die Annahme rechtfertigen, dass Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erfasst werden. Allerdings sieht § 26a Abs. 3 Satz 1 Halbsatz 2 SOG M-V von diesem Erfordernis zwei Ausnahmen in Form des Gefährdungs- und des Verwendungsvorbehaltes vor: Von einem Abbruch der laufenden Maßnahme kann dann abgesehen werden, wenn dieser entweder einerseits mit der Gefährdung der eingesetzten Polizeibeamtinnen und Polizeibeamten oder Vertrauenspersonen verbunden wäre oder andererseits deren weitere Verwendung gefährden würde. Diese Vorbehalte genügen den vom Bundesverfassungsgericht aufgestellten Grundsätzen zum Schutz des Kernbereichs privater Lebensgestaltung nicht.

In seinem Urteil zum „großen Lauschangriff“ hat das Bundesverfassungsgericht die Grundsätze zum Schutz des Kernbereichs privater Lebensgestaltung aufgeführt und dabei klargestellt, dass der Grundsatz der Normklarheit verlangt, dass Befugnisnormen deutliche Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung enthalten müssen (BVerfGE 109, 279, 318ff).

Dies weiter konkretisierend ist in der Entscheidung zum BKAG ausgeführt (BVerfGE 141, 220, 277):

Der Kernbereich privater Lebensgestaltung beansprucht gegenüber allen Überwachungsmaßnahmen Beachtung. Können sie typischerweise zur Erhebung kernbereichsrelevanter Daten führen, muss der Gesetzgeber Regelungen schaffen, die einen wirksamen Schutz normenklar gewährleisten.

Aufgrund des in § 26a Abs. 3 Satz 2 Halbsatz 2 SOG M-V enthaltenen Gefährdungs- und Verwendungsvorbehalts fällt die Regelung hinter den Anforderungen des Bundesverfassungsgerichts zurück. Ausgangspunkt der Bewertung ist hierbei die herausragende Bedeutung des Kernbereichs privater Lebensgestaltung als Ausprägung von Art. 1 GG. Als solche ist der Schutz des Kernbereichs absolut und damit keiner Abwägung – auch nicht mit den höchsten Sicherheitsinteressen – zugänglich. Ein Eingriff in den Kernbereich privater Lebensgestaltung führt somit stets zur Verfassungswidrigkeit der Maßnahme (vgl. BVerfGE 141, 220, 278; *Hong*, Der Menschenwürdegehalt der Grundrechte, 2019, S. 441ff).

Gleichzeitig stellt nicht jede tatsächliche Erfassung höchstpersönlicher Informationen stets einen Verstoß gegen die Verfassung oder eine Verletzung der Menschenwürde dar. Aufgrund der bestehenden Prognose- und Handlungsunsicherheiten, mit denen Sicherheitsbehörden bei der Wahrnehmung ihrer Aufgaben konfrontiert sind, kann das Eindringen in den Kernbereich nicht in jedem Fall von vornherein ausgeschlossen werden (BVerfGE 141, 220, 278). In Ansehung dieser Erwägungen hat das Bundesverfassungsgericht daher ein zweistufiges Schutzkonzept entwickelt, wobei erst bei einem Verstoß gegen dieses auch von einem Verfassungsverstoß ausgegangen werden kann. Demnach sind bei der Datenerhebung – auf der ersten Stufe – Vorkehrungen zu treffen, die eine unbeabsichtigte Miterfassung von Informationen aus dem Kernbereich nach Möglichkeit ausschließen. Bei der Aus- und Verwertung von Daten – auf der zweiten Ebene – müssen die Folgen eines dennoch nicht vermiedenen Eindringens

in den Kernbereich privater Lebensgestaltung strikt minimiert werden (BVerfGE 141, 220, 278 ff).

Schon der in § 26a Abs. 3 Satz 2 Alternative 1 SOG M-V verankerte Gefährdungsvorbehalt, der eine Ausnahme vom Abbrucherfordernis bei der Gefährdung der eingesetzten Polizeibeamten oder Vertrauenspersonen vorsieht, genügt diesen Anforderungen nicht.

Der absolute Schutz des Kernbereichs privater Lebensgestaltung gilt unbedingt und vorbehaltslos. Zwar verlangt das Bundesverfassungsgericht im Vorfeld der Datenerhebung, dass hinsichtlich verletzungsgeneigter Maßnahmen lediglich „*durch vorgelagerte Prüfung sicherzustellen ist, dass die Erfassung von kernbereichsrelevanten Situationen oder Gesprächen jedenfalls insoweit ausgeschlossen ist, als sich diese mit praktisch zu bewältigendem Aufwand im Vorfeld vermeiden lässt*“ (BVerfGE 141, 220, 279).

Einerseits beziehen sich die Ausführungen und das zweistufige Modell des Bundesverfassungsgerichts jedoch ausschließlich auf unbeabsichtigte Eingriffe (BVerfGE 141, 200, 278).

Diese Konstellation unbeabsichtigter Eingriffe hat § 26a Abs. 1 Satz 1 Alternative 1 SOG M-V gerade nicht im Auge: Die Regelung sieht nämlich eine Ausnahme vom Abbrucherfordernis in Situationen vor, in denen eingesetzte Beamte sowie Vertrauenspersonen wider besseres Wissen und zum Schutz ihrer Individualrechtsgüter in den Kernbereich privater Lebensgestaltung eindringen. Mithin sieht § 26a Abs. 1 Satz 1 Alternative 1 SOG M-V explizit die Möglichkeit eines wissentlichen und damit beabsichtigten Eindringens in den Kernbereich vor.

Dass dies verfassungswidrig ist, ergibt sich aus der expliziten Feststellung des Bundesverfassungsgerichts in seinem Urteil zum BKAG, dass Maßnahmen, in deren Lauf sich abzeichnet, dass der Kernbereich betroffen werden könnte, „*in jedem Fall*“ abzubrechen sind (BVerfGE 141, 220, 279).

Somit ist der Gefährdungsvorbehalt in § 26a Abs. 3 Satz 1 Alternative 1 SOG M-V als solcher insgesamt Ausdruck einer unzulässigen Güterabwägung zwischen dem Schutz des Kernbereichs privater Lebensgestaltung und den Individualrechtsgütern der eingesetzten Personen. Wenn die Forderungen des Bundesverfassungsgerichts, im Sinne des Optimierungsgebots Ermittlungstechniken einzusetzen, die die Beeinträchtigung des Kernbereichs soweit möglich ausschließen, erfüllt werden sollen, kann ein Gefährdungsvorbehalt nicht zulässig sein. Jedenfalls bei tatsächlich festgestellten Beeinträchtigungen des Kernbereichs ist der Abbruch des Eingriffs zwingend geboten und hat – soweit nicht faktisch unmöglich – ausnahmslos zu erfolgen. Eine Rücksichtnahme auf andere Rechtsgüter ist aufgrund der keiner Abwägung zugänglichen Menschenwürdegarantie ausgeschlossen (*Sachs*, Schriftliche Stellungnahme zum Gesetzentwurf der Landesregierung 14/10089, S. 8f, LT NRW 19 A 0303/14/195, S. 191, in Bezug auf eine vergleichbare in § 16 Abs. 2 Satz 1 PolG NRW aufgenommene Regelung).

Der absolute Schutz des Kernbereichs führt dazu, dass in Fällen, in denen verdeckt ermittelnde Polizeibeamte oder Vertrauenspersonen gefährdet sein könnten, wenn sie nicht Erkenntnisse aus dem Kernbereich erheben, von Verfassungs wegen entweder diese Personen gar nicht eingesetzt werden dürften oder Vorkehrungen getroffen werden müssten, die eine Gefährdung verhindern.

Diese Ausführungen gelten erst recht für den in § 26a Abs. 3 Satz 1 Alternative 2 SOG M-V verankerten Verwendungsvorbehalt, der ebenfalls nicht mit dem absoluten Schutz, der dem Kernbereich privater Lebensführung als Ausprägung der Menschenwürdegarantie zukommt, vereinbar ist. Dieser Vorbehalt gestattet eine Ausnahme des Abbruchserfordernisses bei in den Kernbereich eindringenden Maßnahmen der Datenerhebung, wenn durch den Abbruch die weitere Verwendung der eingesetzten Personen für Ermittlungszwecke gefährdet werden würde.

Zwar bezweckt die Vorschrift die Erreichung eines legitimen Zwecks, nämlich die Aufgabenerfüllung der Sicherheitsbehörden durch verdeckte, gesetzlich zugelassene Datenerhebung. Allerdings gestattet die Vorschrift explizit das bewusste Eindringen in die höchstpersönliche Intimsphäre zur Sicherung der Aufgabenwahrung und kollidiert dahingehend mit dem menschenwürdebegründeten Schutz des Kernbereichs. Dies stellt eine verfassungsrechtlich unzulässige Abwägung den Kernbereichs mit öffentlichen Sicherheitsinteressen dar (vgl. so insgesamt *Roggan*, Gutachten zum Entwurf eines neuen SOG M-V (Drs. 7/3694), S. 7).

Unzureichend ist ferner die verfahrensrechtliche Ausgestaltung des Kernbereichsschutzes auf der zweiten Ebene, soweit sie die nach § 33 SOG M-V erhobenen Daten betrifft. Erforderlich wäre eine Sichtung der erhobenen Daten durch eine unabhängige Stelle, die von § 26a Abs. 5 SOG M-V nicht gewährleistet wird.

Nach der Rechtsprechung des Bundesverfassungsgerichts ist bei der Wohnraumüberwachung und bei der Online-Durchsuchung eine Sichtung durch eine unabhängige Stelle erforderlich (BVerfGE 109, 279, 333 f; 141, 220, 307). Bei der Telekommunikationsüberwachung ist nach der Rechtsprechung eine Sichtung durch eine innerbehördliche Stelle zulässig, da die Telekommunikationsüberwachung „*ihrem Gesamtcharakter nach nicht in gleicher Weise durch ein Eindringen in die Privatsphäre geprägt wie die Wohnraumüberwachung oder auch die Online-Durchsuchung*“ (BVerfGE 141, 220, 312).

Die Gesetzesbegründung des SOG M-V bezieht sich auf diese Entscheidung und überträgt sie auf die von § 26a Abs. 5 erfassten Befugnisse. Auch wenn es noch keine verfassungsgerichtliche Entscheidung zum Kernbereichsschutz bei Video-und Tonaufzeichnungen außerhalb der Wohnung oder beim Einsatz verdeckter Ermittler gibt, ist der Entscheidung zum BKA-Gesetz (BVerfGE 141, 220, 295) jedoch zu entnehmen, dass es annimmt, dass der Kernbereich auch außerhalb von Wohnungen betroffen sein kann „*- sei es im Auto, sei es abseits in einem Restaurant, sei es zurückgezogen bei einem*

Spaziergang - mit einiger Wahrscheinlichkeit höchstvertrauliche Situationen erfasst werden können, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind".

Diese hohe Kernbereichsrelevanz lässt eine Sichtung durch eine unabhängige Stelle bei Maßnahmen nach § 33 SOG M-V notwendig erscheinen.

3. Unzureichende Benachrichtigungspflicht

Die Regelung in § 46a SOG M-V über die Benachrichtigung der Personen, die von verdeckten Überwachungsmaßnahmen betroffen sind, steht nicht in jeder Hinsicht mit der Verfassung in Einklang.

Im Anschluss an eingriffsintensive verdeckte Überwachungsmaßnahmen ist eine Benachrichtigung der betroffenen Personen grundrechtlich geboten. Dies folgt zum einen aus dem Grundrecht, in das die jeweilige Überwachungsmaßnahme eingreift, zum anderen aus der Rechtsweggarantie des Art. 19 Abs. 4 GG. Denn die Benachrichtigung ermöglicht zum einen den betroffenen Personen eine Orientierung über ihre Stellung zu der Überwachungsbehörde. Zum anderen ist sie faktische Voraussetzung dafür, dass die betroffenen Personen wirksam gerichtlich gegen die Überwachung vorgehen können. Dementsprechend muss der Gesetzgeber eine grundsätzliche Benachrichtigungspflicht schaffen, von der nur in besonderen Ausnahmefällen abgewichen werden darf (vgl. BVerfGE 141, 220, 282; BVerfG, Beschl. v. 27.05.2020, 1 BvR 1873/13, 1 BvR 2618/13, Rn. 245f).

§ 46a Abs. 1 Nr. 2 SOG M-V sieht zwar die Benachrichtigung über den Einsatz besonderer Mittel der Datenerhebung nach § 33 Abs. 1 SOG M-V vor. Diese Benachrichtigungspflicht wird jedoch durch § 46a Abs. 2 Satz 2 SOG M-V relativiert.

Die Bestimmung verstößt bereits gegen das Gebot der Normenklarheit, da sich ihr kein eindeutiger Regelungsgehalt entnehmen lässt. Während § 46a Abs. 2 Satz 1 SOG M-V unter bestimmten Voraussetzungen einen Aufschub der Benachrichtigung erlaubt, ist nach § 46a Abs. 2 Satz 2 SOG M-V „auch

eine Gefährdung der weiteren Verwendung von Vertrauenspersonen und verdeckt Ermittelnden als bedeutender Belang zu berücksichtigen“. Es bleibt unklar, in welchem Rahmen diese „Berücksichtigung“ zu erfolgen hat. Der Zusammenhang zu Satz 1 legt nahe, dass auch unter den Voraussetzungen des Satzes 2 ein Aufschub zulässig sein soll. Aus Gründen der Normenklarheit hätte eine solche Rechtsfolge jedoch explizit in das Gesetz aufgenommen werden müssen.

Darüber hinaus ist der Zurückstellungsgrund verfassungsrechtlich nur tragfähig, soweit er sich auf die Benachrichtigung gerade über den personenbezogenen Einsatz des verdeckt Ermittelnden oder der Vertrauensperson bezieht. Soweit die Norm jedoch weitergehend auch die Benachrichtigung über andere Überwachungsmaßnahmen potentiell für einen langen Zeitraum (vgl. § 46a Abs. 4 Nr. 1 (für § 33b Abs. 9) und Nr. 2 SOG-MV) ausschließt, fehlt es an einer hinreichenden Verbindung zwischen der Maßnahme und dem Benachrichtigungsausschluss (diese wird aber in der verfassungsgerichtlichen Rechtsprechung verlangt: BVerfGE 109, 279, 366f; 141, 220, 320).

Sollte einem verdeckt Ermittelnden oder einer V-Person aufgrund der Benachrichtigung eine Enttarnung und deshalb die Gefahr für hochrangige Individualrechtsgüter drohen, wäre ohnehin schon der Zurückstellungstatbestand des § 46a Abs. 2 Satz 1 Alt. 2 SOG M-V erfüllt.

II. Wohnraumüberwachung (§ 33b SOG M-V)

Die Befugnis zur Wohnraumüberwachung im Vorfeld konkreter Gefahren aus § 33b Abs. 1 Satz 2 i.V.m. § 67a Abs. 1 SOG M-V verletzt das Grundrecht auf Unverletzlichkeit der Wohnung.

Für die besonders tief in die Privatsphäre eindringenden Eingriffe der Wohnraumüberwachung verlangt Art. 13 Abs. 4 GG eine dringende Gefahr. Der Begriff der dringenden Gefahr nimmt dabei nicht nur im Sinne des qualifizierten Rechtsgüterschutzes auf das Ausmaß, sondern auch auf die

Wahrscheinlichkeit eines Schadens Bezug (vgl. BVerfGE 141, 220, 271). Die Anforderungen an das Vorliegen einer dringenden Gefahr sind streng und gehen über diejenigen einer konkreten Gefahr hinaus (BVerfGE 141, 220, 296).

§ 33b Abs. 1 Satz 2 i.V.m. § 67a Abs. 1 SOG M-V gestattet hingegen die Wohnraumüberwachung im Vorfeld einer konkreten Gefahr. Anders als § 20g Abs. 1 Satz 1 Nr. 2 BKAG a.F., der vom Bundesverfassungsgericht nicht beanstandet wurde (vgl. BVerfGE 141, 220, 298), knüpft § 33b Abs. 1 Satz 2 SOG M-V nicht an eine dringende Gefahr an. Zwar sieht § 33b Abs. 1 Satz 1 SOG M-V als Eingriffsschwelle eine gegenwärtige Gefahr vor, die in § 3 Abs. 3 Nr. 2 SOG M-V definiert wird. § 33b Abs. 1 Satz 2 SOG M-V steht jedoch selbstständig daneben und verweist lediglich auf die Voraussetzungen des § 67a Absatz 1 SOG M-V (siehe zur Kritik des § 67a die Ausführungen unter D.I.1).

III. Online-Durchsuchung (§ 33c SOG M-V)

§ 33c SOG M-V führt eine Ermächtigung zur Online-Durchsuchung ein. Die Durchführung der Maßnahme wird einerseits gemäß § 33c Abs. 1 Satz 1 SOG M-V unter den wörtlich übernommenen, vom Bundesverfassungsgericht in diesem Zusammenhang aufgestellten Voraussetzungen gestattet (vgl. BVerfGE 141, 220, 270f).

Darüber hinaus gestattet § 33c Abs. 1 Satz 1, 2 SOG M-V aber die Online-Durchsuchung unter Verweis auf die vorgelagerte Gefahrenschwelle des § 67a Abs. 1 SOG M-V (siehe zur Kritik des § 67a die Ausführungen unter D.I.1). § 33c Abs. 3-5 SOG M-V ermächtigen zudem zu Vorbereitungsmaßnahmen für die Online-Durchsuchung, darunter zum Betreten und Durchsuchen von Wohnungen zu diesem Zweck.

Diese beiden eng miteinander zusammenhängenden Normen werfen im Hinblick auf mehrere Aspekte verfassungsrechtliche Bedenken auf. Im Folgenden wird zunächst dargelegt, dass die Eingriffsschwelle des § 33c

Abs. 1 Satz 2 SOG M-V (dazu unter 1.) und der Einsatz gegen Nicht-Verantwortliche (dazu unter 2.) nicht mit dem IT-Grundrecht in Einklang stehen. Dann wird herausgearbeitet, wie die Eingriffsschwelle für das Betreten von Wohnraum zur Vorbereitung einer Online-Durchsuchung hinter den verfassungsrechtlichen Anforderungen an die Voraussetzungen für einen Eingriff in die Unverletzlichkeit der Wohnung zurückfällt (dazu unter 3). Schließlich wird dargestellt, wie die Ermächtigungen zum Einsatz von Staatstrojanern auch staatliche Schutzpflichten aus dem IT-Grundrecht verletzen (dazu unter 4).

1. Unzureichende Eingriffsschwelle

§ 33c Abs. 1 SOG M-V gestattet den Zugriff auf informationstechnische Systeme, einschließlich der so genannten Online-Durchsuchung. Die Online-Durchsuchung unterscheidet sich qualitativ von anderen, ähnlich gelagerten Maßnahmen: Im Gegensatz zu der offen durchgeführten Hausdurchsuchung findet die Online-Durchsuchung verdeckt statt und erstreckt sich über einen längeren Zeitraum; im Unterscheid zur Wohnungsüberwachung ist sie nicht auf einen bestimmten Ort und im Gegensatz zur Telekommunikationsüberwachung nicht auf mit Dritten geteilte Kommunikationsinhalte beschränkt.

Nach der Rechtsprechung des Bundesverfassungsgerichts dringt der Zugriff auf informationstechnische Systeme „besonders tief“ in die Privatsphäre ein (vgl. BVerfGE 141, 220, 269). „*Wegen der oft höchstpersönlichen Natur*“ der von einem Eingriff in dieses Grundrecht betroffenen Daten, „*die sich insbesondere auch aus deren Verknüpfung ergibt, ist ein Eingriff in dieses Grundrecht von besonderer Intensität*“ und „*seinem Gewicht nach mit dem Eingriff in die Unverletzlichkeit der Wohnung vergleichbar*“ (BVerfGE 141, 220, 304).

Gerade um der besonderen Intensität dieses Eingriffs Rechnung zu tragen, hat das Bundesverfassungsgericht das Grundrecht auf Gewährleistung der

Vertraulichkeit und Integrität informationstechnischer Systeme als eine eigenständige Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abgeleitet (vgl. BVerfGE 120, 274, 303ff).

Der Zugriff auf IT-Systeme kann unter heutigen Bedingungen sogar einen noch deutlich tiefergehenden Eingriff in die Privatheit bedeuten als die Wohnraumüberwachung. Der Eingriff in dieses Grundrecht durch den verdeckten Zugriff auf informationstechnische Systeme unterliegt deshalb den beschriebenen Erfordernissen der Eingriffsschwelle einer konkretisierten Gefahr, die sich aus dem Gebot der Verhältnismäßigkeit im engeren Sinne ergibt (vgl. BVerfGE 141, 220, 305).

Für die Durchführung der Online-Durchsuchung fordert der mecklenburg-vorpommerische Gesetzgeber in § 33c Abs. 1 Satz 1 SOG M-V tatsächliche Anhaltspunkte für eine konkrete Gefahr für ein überragend wichtiges Rechtsgut, darunter Leib, Leben und Freiheit der Person sowie solche Güter der Allgemeinheit, deren Bedrohung die Grundlage oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt und übernimmt damit wörtlich die Vorgaben des Bundesverfassungsgerichts (vgl. BVerfGE 120, 274, 326ff).

Verfassungswidrig ist die Vorschrift jedoch insoweit, wie sie in § 33c Abs. 1 Satz 2 SOG M-V durch den Verweis auf § 67a Abs. 1 SOG M-V den Zugriff auf informationstechnische Systeme auch im Vorfeld einer konkreten Gefahr zulässt. Die Vorverlagerung der Gefahrenschwelle bleibt hinter den Anforderungen des Bundesverfassungsgerichts zurück. Dieses führt aus (BVerfGE 120, 274, 329):

Ein Zugriff auf das informationstechnische System kann schon gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein

werden, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann.

Dem genügt § 33c Absatz 1 Satz 2 i.V.m. § 67 Abs. 1 SOG M-V nicht, da der Strafkatalog des § 67a Abs. 1 SOG M-V diverse Vorfeldtatbestände wie etwa § 129a StGB erfasst, die bereits weit im Vorfeld der Rechtsgutsverletzung angesiedelte Vorbereitungshandlungen unter Strafe stellen (siehe dazu die Ausführungen unter D.I.1).

2. Unverhältnismäßiger Einsatz gegenüber Nicht-Verantwortlichen

Darüber hinaus ermächtigt § 33c Abs. 1 Satz 4 SOG M-V zum Zugriff auf die informationstechnischen Systeme anderer Personen, die weder Verhaltens- noch Zustandsstörer sind, sofern Tatsachen für die Annahme bestehen, dass ein Störer dort ermittlungsrelevante Informationen speichert.

Das Bundesverfassungsgericht fordert für die Erstreckung der Online-Durchsuchung auf die informationstechnischen Systeme Dritter, dass einerseits tatsächliche Anhaltspunkte dafür bestehen, dass die Zielperson dort ermittlungsrelevante Informationen speichert und andererseits, dass ein auf die eigenen informationstechnischen Systeme der betroffenen Person beschränkter Zugriff zur Erreichung des Ermittlungsziels nicht ausreicht (BVerfGE 141, 220, 274).

Anders als in § 33b Abs 2 Nr. 2 SOG M-V hinsichtlich der Wohnraumüberwachung fehlt es an dieser zweiten Voraussetzung der Erforderlichkeit in § 33c Abs. 1 Satz 4 SOG M-V (so auch AKJ Greifswald, Stellungnahme zum Entwurf eines Gesetzes über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern und zur Änderung anderer Gesetze, LT-Drs. 7/3694, S. 11).

3. Verletzung von Art. 13 GG durch Wohnungsbetretungsbefugnis

§ 33c Abs. 5 ermächtigt zum verdeckten Durchsuchen von Sachen und zum verdeckten Betreten und Durchsuchen von Räumlichkeiten der betroffenen Person, soweit dies zur Durchführung der Online-Durchsuchung bzw. der Quellen-TKÜ erforderlich ist. Damit erlaubt es das Betreten von Wohnungen, um Staatstrojaner auf informationstechnischen Systemen zu installieren. Die Erforderlichkeit in diesem Sinne soll laut Gesetzesbegründung dann gegeben sein, wenn der Zugriff über die Kommunikationsverbindungen des Systems unmöglich ist (LT-Drs. 7/3694, S. 182).

Im Gegensatz zum Betreten von Wohnungen zur Installation von Anlagen zur akustischen Wohnraumüberwachung nach § 100c StPO (vgl. dazu Hegmann, in: BeckOK StPO, 39. Ed. 1.1.2021, § 100c Rn. 3) ist die Befugnis zum heimlichen Betreten der Wohnung zum Zwecke der Online-Durchsuchung keine Annexkompetenz. Denn das Betreten der Wohnung ist für die Durchführung dieser Maßnahme gerade nicht typisch. Stattdessen sind zahlreiche andere Arten vorstellbar, wie das Zielsystem infiziert werden kann. Dies wird auch an der Gesetzesbegründung deutlich, die die Infizierung des Systems über dessen Kommunikationsverbindungen als den Regelfall ansieht (vgl. LT-Drs. 7/3694, S. 182).

Darüber hinaus folgt schon aus dem verfassungsrechtlichen Schutz des Wohnraums, dass das Betreten oder Durchsuchen zur Vorbereitung einer Online-Durchsuchung eine Maßnahme von erheblichem eigenem Gewicht darstellt. Insofern kann diese Vorbereitungshandlung weder auf die Grundnorm selbst noch auf die polizeiliche Generalklausel gestützt werden, sondern bedarf einer eigenen Ermächtigungsgrundlage (vgl. Derin/Golla, NJW 2019, 1111, 1112f, Soiné, NVwZ 2012, 1585, 1589).

Die Regelungen der § 33c Abs. 5 und § 33d Abs. 3 Satz 3 SOG M-V zeugen davon, dass auch der mecklenburg-vorpommerische Gesetzgeber davon ausgeht, dass es einer Ermächtigungsnorm zu Betreten von Wohnungen

bedarf. Allerdings genügen die Regelungen dem Schutzgehalt von Art. 13 GG und dessen Schranken-Konzeption nicht.

Die Rechtfertigungsschwellen für Beeinträchtigungen der Unverletzlichkeit der Wohnung unterscheiden sich danach, um welche Art von Eingriffen es sich handelt: Die Schranke des Art. 13 Abs. 2 GG, die sich auf Durchsuchungen bezieht, ist auf das Betreten und Durchsuchen von Wohnraum als Vorbereitungsmaßnahme für die Online-Durchsuchungen und Quellen-TKÜ schon nicht anwendbar. Eine Durchsuchung im Sinne des Art. 13 Abs. 2 GG 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 offenlegen oder herausgeben will*“ (BVerfGE 76, 83, 89).

Kennzeichnend ist die Offenheit der Maßnahme (vgl. Roggan, Gutachten zum Entwurf eines neuen SOG M-V, Drs. 7/3694, S. 26 m.w.N.).

Das Betreten und Durchsuchen von Wohnraum zur Infiltration informationstechnischer Systeme findet im Gegensatz dazu planmäßig heimlich statt. Insofern können Befugnisse, wie sie in § 33c Abs. 5 SOG M-V vorgesehen sind, nicht auf die Schrankenregelung des Art. 13 Abs. 2 GG gestützt werden (vgl. Roggan, Gutachten zum Entwurf eines neuen SOG M-V (Drs. 7/3694), S. 26, so im Hinblick auf das BayPAG auch Löffelmann, Stellungnahme zum Gesetzesentwurf der Staatsregierung für ein Gesetz zur Neuordnung des bayrischen Polizeirechts, LT-Drs. 17/20425, S. 50).

Die Ermächtigung kann ebenso wenig auf die Schranken des Art. 13 Abs. 3, 4 oder 5 GG gestützt werden. Diese beziehen sich allein auf den Einsatz technischer Mittel zur Überwachung der Wohnung und damit auf eine andere Rechtsfolge. Insbesondere ist das Betreten und Durchsuchen von Wohnraum zur Vorbereitung der Online-Durchsuchung nicht als weniger eingriffsintensive Maßnahme gegenüber der Wohnraumüberwachung von der Schranke des Art. 13 Abs. 4 GG erfasst. Dies ist einerseits mit der ausdifferenzierten Schrankensystematik des Art. 13 GG und dem „Auffang-Vorbehalt“ in Art. 13 Abs. 7 GG nicht vereinbar. Darüber bezieht sich Art. 13

Abs. 4 GG auf die akustische und optische Wohnraumüberwachung zu präventiven Zwecken. Demgegenüber stellt das Betreten von Wohnraum zur Vorbereitung einer Online-Durchsuchung eine wesensmäßig andere Grundrechtsbeeinträchtigung dar. Selbst wenn eine Anwendung des Art. 13 Abs. 4 GG in Betracht käme, würde § 33c Abs. 5 SOG M-V aber den Anforderungen des Art. 13 Abs. 4 GG nicht entsprechen, wonach eine dringende Gefahr vorliegen muss, die ihrem Inhalt nach noch über die konkrete Gefahr hinaus geht. § 33c Abs. 5 i.V.m. § 33c Abs. 1 Satz 2 i.V.m § 67a Abs. 1 SOG M-V gestattet aber das Betreten und Durchsuchen von Wohnraum für die Vorbereitung der Online-Durchsuchung bereits im Vorfeld konkreter Gefahren (siehe zur Kritik des § 67a die Ausführungen unter D.I.1).

Die Ermächtigung des § 33c Abs. 5 SOG M-V kann auch nicht auf Art. 13 Abs. 7 GG gestützt werden. Unter Eingriffen und Beschränkungen im Sinne des Art. 13 Abs. 7 GG sind Beeinträchtigungen des Schutzbereiches, die weder eine Durchsuchung im Sine des Art. 13 Abs. 2 GG noch den Einsatz technischer Mittel im Sinne der Absätze 3, 4 oder 5 darstellen, zu verstehen (vgl. Papier, in: Maunz/Dürig, Grundgesetz, 92. EL August 2020, Art. 13 Rn. 117; Roggan, Gutachten zum Entwurf eines neuen SOG M-V, LT-Drs. 7/3694, S. 27).

Darüber hinaus erfüllt § 33c Abs. 5 SOG M-V jedenfalls auch nicht die verfassungsrechtlichen Voraussetzungen an eine Rechtfertigung nach Art. 13 Abs. 7 GG. Dieser verlangt ebenfalls das Vorliegen einer dringenden Gefahr, über die § 33c Abs. 5 SOG M-V durch den Verweis auf Voraussetzungen des § 67a Abs. 1 SOG M-V hinausgeht.

Eine Rechtfertigung für Eingriffe nach § 33c Abs. 5 SOG M-V findet sich auch nicht in ungeschriebenen, verfassungsimmanenten Schranken des Art. 13 GG. Dagegen spricht schon der Wortlaut von Art. 13 Abs. 7 GG. Dieser lässt sonstige, in den Art. 2 bis 6 nicht genannte Beeinträchtigungen nur unter bestimmten Voraussetzungen zu und stellt somit eine abschließende Schrankenregelung dar (Mittag, NVwZ 2005, 649, 651f).

Insofern findet die Beeinträchtigung des Schutzgehaltes von Art. 13 GG durch die Ermächtigungen in § 33c Abs. 5 und § 33d Abs. 3 Satz 3 SOG M-V keine verfassungsrechtliche Rechtfertigung.

4. Verletzung staatlicher Schutzpflichten für die IT-Sicherheit

Die Befugnis zur Onlinedurchsuchung verletzt darüber hinaus die aus dem IT-Grundrecht folgende staatliche Schutzpflicht. Das IT-Grundrecht hat eine objektiv-rechtliche Dimension, die den Staat zu Schutzmaßnahmen für die IT-Sicherheit verpflichtet (dazu unter a). Das Ausnutzen von Sicherheitslücken bzw. Schwachstellen in IT-Systemen kann gravierende Folgen haben (dazu unter b). Aus der staatlichen Pflicht zum Schutz der Integrität und Vertraulichkeit informationstechnischer Systeme folgt, dass das Land Mecklenburg-Vorpommern die genannten Befugnisse mit einem effektiven Schwachstellen-Management hätte verbinden müssen, welches insbesondere die Verwendung von Sicherheitslücken verhindert, die dem Hersteller des betreffenden Systems noch nicht bekannt sind, sog. Zero-Days (dazu unter c) Dem genügt das Land Mecklenburg-Vorpommern jedoch nicht (dazu unter d).

Die derzeitige Ausgestaltung von § 33c verletzt daher die Beschwerdeführerinnen und Beschwerdeführer in ihren Grundrechten auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bzw. Art. 2 Abs. 1 GG.

a) Staatliche Schutzpflicht

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 1 Abs. 1 i.V.m. Art. 1 GG bzw. Art. 2 Abs. 1 GG ist nicht nur ein subjektives Abwehrrecht gegen staatliche Eingriffe. Es begründet – wie schon der Begriff „Gewährleistung“ zeigt – auch eine staatliche Pflicht, dazu beizutragen, dass die Sicherheit der informationstechnischen Infrastruktur der Bundesrepublik ein hohes Niveau er-

reicht. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme trägt so einerseits der hohen Bedeutung der Informationstechnik für die Funktionsfähigkeit von Staat und Gesellschaft, andererseits der erheblichen Verwundbarkeit dieser Technologie Rechnung (vgl. etwa Sachs/Krings, JuS 2008, 481, 486; Kutscha, NJW 2008, 1042, 1044; Roßnagel/Schnabel, NJW 2008, 3534, 3535; Heckmann, in FS Käfer, 2009, S. 129, 133 ff; Hoffmann-Riem, JZ 2009, 165 ff.; ders., AöR 134 (2009), 513 ff.; ders. JZ 2014, 53 ff.; Becker, NVwZ 2015, 1335, 1339 f).

Die objektiv-rechtliche Dimension des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist praktisch hoch bedeutsam. Einerseits ist die Relevanz informationstechnischer Systeme, die das Bundesverfassungsgericht im Jahr 2008 zur Anerkennung einer neuen Ausprägung des Allgemeinen Persönlichkeitsrechts in Form des IT-Grundrechts bewegte, in den vergangenen Jahren noch gewachsen – insbesondere durch die nahezu lückenlose Verwendung sog. Smartphones, aber auch durch den noch einmal gestiegenen Verbreitungs- und Vernetzungsgrad der bereits 2008 existierenden IT-Systeme. Informationstechnische Systeme sind dadurch auch zentral geworden für die Wahrnehmung und Ausübung anderer Grundrechte wie der Wissenschafts-, Meinungs-, Presse-, Versammlungs-, Vereinigungs- und Berufsfreiheit (vgl. Heckmann, in: FS Käfer, 2009, S. 129, 135), der deshalb von der Sicherheit von IT-Systemen als einer „Querschnittsbedingung für die Grundrechtsausübung“ spricht).

Andererseits ist die objektiv-rechtliche Dimension des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme bedeutsam, da solche Systeme strukturell bedingt stets eine Vielzahl von Sicherheitslücken aufweisen, die eigenständig zu Fehlfunktionen führen oder durch Dritte missbräuchlich ausgenutzt werden können. Die Sicherheit informationstechnischer Systeme ist daher als dauerhafte öffentliche Aufgabe anzusehen. Diese Aufgabe kann der Staat allerdings weitgehend nicht eigenhändig erfüllen, da es ihm hierfür sowohl an Ressourcen

als auch an Expertise fehlt. In erster Linie obliegt es vielmehr den Herstellern von informationstechnischen Systemen und der darauf laufenden Software, vermeidbare Sicherheitslücken nicht entstehen zu lassen und später erkannte Sicherheitslücken zeitnah zu schließen. Die staatliche Gewalt kann hierbei lediglich eine unterstützende Rolle einnehmen. Welche Beiträge sie dazu übernimmt, hängt von Gestaltungsentscheidungen ab, für die das Grundgesetz beträchtliche Spielräume lässt. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist in seiner objektiv-rechtlichen Dimension erst verletzt, wenn die staatlichen Anstrengungen offenkundig unzureichend sind (vgl. zu den aus unterschiedlichen Grundrechten hergeleiteten staatlichen Schutzpflichten etwa BVerfGE 49, 89, 142; 77, 17, 214f; 88, 203, 251ff; 92, 26, 46; 106, 28, 37; 125, 39, 78f; 143, 313, 337f).

Der grundrechtliche Mindeststandard wird allerdings zumindest dann unterschritten, wenn eine staatliche Stelle ohne zureichenden Grund eine Gefährdungslage für die Vertraulichkeit und Integrität der informationstechnischen Infrastruktur in der Bundesrepublik bewusst aufrechterhält oder sogar selbst schafft. Eine solche Situation kann im Zusammenhang mit Online-Durchsuchungen oder Quellen-TKÜ abhängig von den genutzten Infiltrationsweg auftreten. Insbesondere ist dies der Fall, wenn für die Infiltration des Zielsystems eine noch unbekannte Sicherheitslücke von Hardware oder Software ausgenutzt wird (sogenannter Zero-Day). Da ein Zero-Day dem Hersteller und den Nutzern des betroffenen informationstechnischen Systems noch unbekannt ist, gibt es gegen ihn aus Sicht dieser Personen keine wirksamen Gegenmaßnahmen. Soweit die Sicherheitslücke sich prinzipiell durch eine Anpassung des Systems (etwa ein Software-Update) schließen ließe, steht der dafür erforderliche technische Baustein noch nicht zur Verfügung. Für die ansonsten notfalls mögliche und gebotene vollständige oder partielle Außerbetriebnahme des Systems besteht aus Sicht der betroffenen Personen kein Anlass, solange die Sicherheitslücke nicht bekannt ist.

Sicherheitsbehörden können Zero-Days ausnutzen, um informationstechnische Systeme zu infiltrieren und so eine Online-Durchsuchung oder eine Quellen-TKÜ zu ermöglichen. Dieser Infiltrationsweg erzeugt jedoch einen Zielkonflikt zwischen den Sicherheitsbelangen, denen die Maßnahme dient, und dem durch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität gewährleisteten Anliegen, dass der Staat zur Sicherheit der informationstechnischen Infrastruktur in der Bundesrepublik beiträgt. Im Sinne der Effektivität der Überwachungsmaßnahme muss die Sicherheitslücke möglichst lange geheim gehalten werden. Wird die Sicherheitslücke bekannt, besteht die Gefahr, dass sie geschlossen wird und darum die Infiltration von Vornherein misslingt oder die Maßnahme vorzeitig abgebrochen werden muss. Selbst nach Beendigung der einzelnen Überwachungsmaßnahme besteht ein Interesse daran, den Zero-Day weiterhin geheim zu halten, um ihn für weitere Online-Durchsuchungen oder Quellen-TKÜ nutzen zu können.

b) Auswirkungen von Sicherheitslücken/Schwachstellen in IT-Systemen

Die Ausnutzung von Zero-Days durch staatliche Stellen kann zugleich in mehrfacher Hinsicht die Bedrohungslage für die informationstechnische Infrastruktur in der Bundesrepublik aufrechterhalten oder sogar noch verschärfen. Wird eine Sicherheitslücke aus den eben genannten Gründen geheim gehalten, so trägt die handelnde Behörde durch ihr Unterlassen dazu bei, dass diese Sicherheitslücke nicht geschlossen wird. Da sich aus technischer Sicht die Infiltration informationstechnischer Systeme durch staatliche Stellen und durch Kriminelle nicht unterscheiden, perpetuiert dieses Unterlassen das Risiko krimineller Übergriffe auf die informationstechnische Infrastruktur. Einen darüberhinausgehenden Beitrag zur Schwächung der Informationssicherheit in der Bundesrepublik leistet der Staat dann, wenn eine Behörde Informationen über eine Sicherheitslücke nicht selbst generiert, sondern von Dritten bezieht. Werden Zero-Days auf dem Markt eingekauft, so stützt die beschaffende staatliche Stelle diesen Markt

aktiv. Schon wegen der strengen strafrechtlichen Regulierung des Umgangs mit Informationen und Software, die zum Ausspähen oder Abfangen von Daten bestimmt sind (vgl. § 202c StGB), ist anzunehmen, dass die Akteure auf diesem Markt regelmäßig zumindest in einem rechtlichen Graubereich agieren. Die staatliche Unterstützung dieses Marktes birgt darum das erhebliche Risiko, mittelbar Straftaten zu begünstigen. Sie kann zudem zur Stabilisierung des Marktes und zur Vermehrung der angebotenen Sicherheitslücken beitragen, die dann auch von Dritten aufgekauft und ausgenutzt werden können. Im besten Fall konkurrieren die Behörden unmittelbar mit Unternehmen und Sicherheitsdienstleistern um den Ankauf der entsprechenden Informationen, treiben den Preis in die Höhe und schwächen Programme, die mittels monetärer Anreize zur Aufdeckung von Schwachstellen animieren (sog. Bug Bounty).

Geraten Zero-Days in die falschen Hände, kann das gravierende Folgen haben. Die Entwicklung von Schadsoftware dauert im Median 22 Tage (vgl. RAND Corporation, Zero Days, Thousands of Nights, online abrufbar unter https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf - zuletzt abgerufen am 25.05.2021, S. 57).

Werden die IT-Systeme von Infrastruktureinrichtungen oder Krankenhäusern geschädigt, sind auch Todesfälle nicht ausgeschlossen. Das ist kein weitgehend hypothetisches Szenario, das als Restrisiko der sicherheitsbehördlichen Aufklärung außer Acht gelassen werden könnte.

Eine staatliche Stelle, die über einen geheim gehaltenen Bestand von Informationen über Zero-Days verfügt, ist schließlich selbst ein lohnendes Angriffsziel für Kriminelle, die sich diese Informationen beschaffen und für eigene Zwecke nutzen können. Hierbei handelt es sich nicht um ein hypothetisches Szenario, das als Restrisiko der staatlichen Aufklärung außer Acht bleiben könnte. Solche Angriffe liegen vielmehr ausgesprochen nahe und sind schon vorgekommen. So hat im Mai 2017 das Schadprogramm „WannaCry“ weltweit erhebliche Schäden verursacht. Dabei wurden IT-

Systeme von Behörden und Unternehmen, insbesondere auch von britischen Krankenhäusern lahmgelegt und nur gegen Lösegeldzahlung wieder freigegeben. Das Schadprogramm nutzte eine Sicherheitslücke in Windows-Betriebssystemen aus, welche die kriminellen Angreifer nach verbreiteter Einschätzung mitsamt der zugehörigen Angriffswerkzeuge bei der US-amerikanischen National Security Agency (NSA) ausgespäht hatten, die ihrerseits diese Sicherheitslücke für eigene Zwecke eingesetzt und geheim gehalten hatte (vgl. etwa http://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung - zuletzt abgerufen am 25.05.2021).

Es liegt fern, dass deutsche Sicherheitsbehörden die bei ihnen vorhandenen Informationen über Sicherheitslücken bedeutend besser schützen können als die NSA. Vielmehr ist anzunehmen, dass ein Verlust sich nie ausschließen lässt. Mit vergleichbaren Vorfällen infolge einer Sammlung von Sicherheitslücken bei deutschen Behörden wäre daher zu rechnen.

c) Staatliche Schutzpflicht aus dem IT-Grundrecht in Bezug auf Sicherheitslücken

Werden die Risiken und die möglichen Erträge der staatlichen Infiltration informationstechnischer Systeme mithilfe von Zero-Days einander gegenübergestellt, so ergibt sich, dass dieser Infiltrationsweg ausgeschlossen werden muss. Die durch die Nutzung und Geheimhaltung von Zero-Days eröffneten oder zumindest erhöhten Risiken wiegen äußerst schwer.

Zum einen kann der kriminelle Missbrauch der geheim gehaltenen Sicherheitslücken hochrangige Rechtsgüter empfindlich bedrohen. Nahezu alle lebenswichtigen Leistungen werden heute mit informationstechnischer Unterstützung erbracht. Ebenso verfügen so gut wie sämtliche staatlichen und gesellschaftlichen Einrichtungen, deren Ausfall oder Funktionsstörung schwere Schäden verursachen kann, über informationstechnische Komponenten. Werden solche informationstechnischen Komponenten gestört, so kann dies zu Leistungsausfällen oder Schadensereignissen führen,

die schlimmstenfalls den Verlust von Menschenleben zur Folge haben können. Beispielsweise hat das oben erwähnte Schadprogramm „WannaCry“ informationstechnische Systeme in britischen Krankenhäusern infiltriert. In der Folge mussten unter anderem geplante Operationen verschoben werden. Auch rund 450 Rechner der Deutschen Bahn wurden infiziert, was unter anderem zum Ausfall einer regionalen Leitstelle führte. Ein weiterer Angriff, der auf von der NSA erbeuteter Technologie basierte, führte dazu, dass bei dem Arzneimittelunternehmen Merck ein kritischer Minderbestand eines Impfstoffs eintrat. Zum anderen erstreckt sich die Bedrohung durch den Missbrauch von Zero-Days auf praktisch die gesamte Bevölkerung, also ganz überwiegend auf Menschen, die für sicherheitsbehördliche Überwachungsmaßnahmen keinen Anlass geben. Es fehlt mithin vollständig an einer Zurechnungsbeziehung zwischen diesen Menschen und den Belangen, die der Geheimhaltung von Sicherheitslücken zugrunde liegen. Angesichts dessen und wegen der drohenden schweren Schäden ist die Grenze der Aufopferungspflicht des Einzelnen für das Gemeinwohl deutlich überschritten.

Hingegen wiegt der Effektivitätsverlust, der durch ein Verbot der Ausnutzung von Zero-Days für die Aufgabenerfüllung der Sicherheitsbehörden droht, weniger schwer. Zwar haben die Belange, denen Online-Durchsuchungen und Quellen-Telekommunikationsüberwachungen des BKA dienen, schon wegen der grundrechtlich gebotenen restriktiven Fassung des Eingriffstatbestands durchweg hohes Gewicht. Jedoch können diese Belange zumeist auch auf weniger riskanten Wegen erreicht werden. So ist es aus objektiv-rechtlicher Sicht beispielsweise unbedenklich, wenn zur Infiltration des Zielsystems einer Online-Durchsuchung bzw. einer Quellen-Telekommunikationsüberwachung eine physische Zugriffsmöglichkeit (etwa im Rahmen einer Durchsuchung) oder eine bereits bekannte, auf diesem System jedoch noch nicht geschlossene Sicherheitslücke ausgenutzt werden. Soweit im Einzelfall eine Infiltration auf solchen Wegen nicht mög-

lich sein sollte, ist der damit verbundene Ausfall dieser Überwachungsmaßnahmen hinzunehmen und auf andere, gegebenenfalls teurere Maßnahmen auszuweichen.

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verpflichtet die staatliche Gewalt mithin dazu, auf die Nutzung und Geheimhaltung von Zero-Days zum Zweck der Infiltration informationstechnischer Systeme zu verzichten. Es ist Sache des Gesetzgebers, diese Pflicht durch ein ausdrückliches gesetzliches Verbot umzusetzen. Nur durch ein ausdrückliches Verbot erhalten die Sicherheitsbehörden eine eindeutige Vorgabe, die das objektiv-grundrechtlich nicht hinzunehmende Risiko für die Sicherheit der informationstechnischen Infrastruktur der Bundesrepublik sicher ausschließt.

Selbst wenn entgegen der oben begründeten Auffassung eine staatliche Infiltration informationstechnischer Systeme mithilfe von noch unbekannten Sicherheitslücken verfassungsrechtlich überhaupt rechtfertigungsfähig wären, müsste die gesetzliche Grundlage der Infiltration zumindest Vorgaben für ein behördliches Schwachstellen-Management enthalten. Nur aufgrund von prozeduralen Sicherungen und materiellen Kriterien für ein solches Schwachstellen-Management kann das enorme Risiko für die informationstechnische Infrastruktur der Bundesrepublik hinnehmbar sein. In diesem Rahmen wäre ein Bündel von maßstabsbildenden Faktoren zu beachten, etwa

- die Verbreitung einer Sicherheitslücke
    - in quantitativer Hinsicht: Zahl der betroffenen Nutzerinnen und Nutzer,
    - in qualitativer Hinsicht: Art der betroffenen Nutzerinnen und Nutzer,
- das Gewicht der Sicherheitslücke
    - zur Ausnutzung erforderlicher Aufwand,

    - aus der Ausnutzung resultierender Schaden,

- die Wahrscheinlichkeit, dass Betroffene die Ausnutzung der Lücke bemerken und im Einzelfall Gegenmaßahmen einleiten,
- die Wahrscheinlichkeit einer technischen Lösung für die Lücke,
- die Wahrscheinlichkeit einer Verbreitung der technischen Lösung,
- Möglichkeiten zur Linderung der Folgen einer (zeitweisen) Geheimhaltung der Lücke,
- die Wahrscheinlichkeit, dass Dritte die Lücke finden,

(vgl. Herpig, Schwachstellen-Management für mehr Sicherheit, 2018, abrufbar unter https://www.stiftung-nv.de/sites/default/files/vorschlag.schwachstellenmanagement.pdf - zuletzt abgerufen am 25.05.2021).

d) Bisherige Gesetze des Landes Mecklenburg-Vorpommern

Zum Umgang des Landes Mecklenburg-Vorpommern mit Zero-Days sind keine Äußerungen bekannt, auch die Gesetzesbegründung zum SOG schweigt zu dieser Frage.

Bisher gibt es keinen Prozess zur Bewertung von Schwachstellen, die Behörden des Landes Mecklenburg-Vorpommern zur Quellen-TKÜ und Online-Durchsuchungen nutzen wollen, sowie keine Verfahren und Kriterien, nach denen über eine Meldung der Schwachstelle an die Hersteller entschieden werden kann. Auch auf Bundesebene sind hinsichtlich der auch Bundesbehörden betreffenden Befugnisse für die Online-Durchsuchung und Quellen-TKÜ keine derartigen Prozesse bekannt.

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

Die Befugnis zur Telekommunikationsüberwachung und zur Quellen-Telekommunikationsüberwachung verstoßen gegen das Fernmeldegeheimnis, soweit sie im Vorfeld einer konkreten Gefahr erlaubt sind (dazu unter 1).

Die Befugnis nach § 33d Abs. 3 Satz 2 SOG M-V verstößt zudem gegen das IT-Grundrecht, weil es sich in der Sache um eine Online-Durchsuchung handelt (dazu unter 2). Zu beanstanden sind ferner die Wohnungsbetretungsbefugnis nach § 33d Abs. 3 Satz 3 i.V.m. § 33c Abs. 5 SOG M-V sowie das Fehlen von Vorschriften zum Schutz vor Sicherheitslücken (dazu unter 3).

1. Unzureichende Eingriffsschwelle

§ 33d SOG M-V ermächtigt zum Telekommunikationsüberwachung, die in Art. 10 Abs. 1 GG eingreift. Das Bundesverfassungsgericht hat ferner entschieden, dass auch die Quellen-TKÜ einen Eingriff in Art. 10 Abs. 1 GG darstellt, sofern durch technische Maßnahmen – wie von § 33d Abs. 3 Satz 1 Nr. 1 SOG M-V verlangt – sichergestellt wird, dass ausschließlich laufende Telekommunikation erfasst wird (vgl. BVerfGE 141, 220, 309f).

Die in § 33d SOG M-V geregelten Maßnahmen können eine hohe Eingriffsintensität aufweisen und sind daher von Verfassungs wegen an eine hinreichend restriktive und in tatsächlicher Hinsicht konturierte Eingriffsschwelle zu binden. Das Bundesverfassungsgericht im Urteil zum BKAG eine Regelung dann als verfassungsgemäß erachtet, wenn sie für solche Maßnahmen die Eingriffsschwelle einer dringenden Gefahr vorsah, nämlich „*die auf den Schutz qualifizierter Rechtsgüter gerichtete und allein auf die Abwehr dringender Gefahren beschränkte Befugnis zur Überwachung gegenüber den polizeirechtlich Verantwortlichen*“ des § 20l Abs. 1 Satz 1 Nr. 1 BKAG a.F. (vgl. BVerfGE 141, 220, 310), während es die Erstreckung der Telekommunikationsüberwachung nach § 20l Abs. 1 Satz 1 Nr. 2 BKAG a.F. „*auf Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie terroristische Straftaten vorbereiten*“ wegen Verstoßes gegen den Bestimmtheitsgrundsatz und das Verhältnismäßigkeitsprinzip als verfassungswidrig eingestuft hat (vgl. BVerfGE 141, 220, 310).

Diese Anforderungen werden nicht eingehalten, soweit in § 33d Abs. 1 Satz 1 Nr. 2 bis 4 SOG M-V auf die Voraussetzungen des § 67a Abs. 1 SOG M-V verwiesen wird (vgl. hierzu bereits oben unter D.I.1).

2. „Kleine Online-Durchsuchung“ (§ 33d Abs. 3 Satz 2 SOG M-V)

Es ist Voraussetzung einer nur an Art. 10 Abs. 1 GG zu messenden Quellen-TKÜ, dass ausschließlich „laufende Kommunikation“ erhoben wird (BVerfGE 120, 274, 309; vgl. zu Begriff und Inhalt eingehend Buermeyer, StV 2013, 470).

Der Grundrechtsschutz „lediglich“ nach Art. 10 Abs. 1 GG erstreckt sich nicht auf die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Telekommunikation („kondensierte“ Kommunikation). Gilt ein heimlicher staatlicher Zugriff der Ausforschung dieser Inhalte, so misst sich dessen Zulässigkeit vielmehr an den weitaus strengeren Anforderungen des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (BVerfGE 120, 274, 308).

§ 33d Abs. 3 Satz 2 SOG M-V soll jedoch über die laufende Kommunikation hinaus auch die Erhebung „gespeicherter Inhalte und Umstände der Kommunikation“ – also das Auslesen quasi „kondensierter“ Kommunikation – unter den erleichterten Voraussetzungen der Quellen-TKÜ gestatten.

Der Gesetzgeber begründet das damit, dass der Eingriff eine erheblich geringere Intensität und Reichweite aufweise als die Online-Durchsuchung. Er erfasse keine nur der betroffenen Person (und nicht auch Kommunikationspartnern) bekannten Inhalte und gehe nicht über das hinaus, was die Strafverfolgungsbehörden mit einer herkömmlichen Telekommunikationsüberwachung ermittelt haben würden, wenn die betroffene Person diesen Kommunikationsweg gewählt hätte. Insofern würden sich die Voraussetzungen aus Art. 10 Abs. 1 GG als hinreichend erweisen (LT-Drs. 7/3694, S. 185).

Indes ist bereits die Figur der Quellen-TKÜ für laufende Kommunikation eine Ausnahme von der Regel, dass Trojaner-Einsätze einen Eingriff in das IT-Grundrecht darstellen; hinzu kommt, dass diese Ausnahme aus technischer Sicht ihrerseits eine fragwürdige, da kontrafaktische ist. Und Ausnahmen können gerade nicht analog angewendet werden, sondern sind restriktiv auszulegen.

Nach dem Gesetzentwurf soll nicht sämtliche gespeicherte Kommunikation als Quellen-TKÜ auslesbar sein, sondern nur solche Kommunikationsinhalte, die nach der richterlichen Anordnung gespeichert wurden (LT-Drs. 7/3694, S. 186).

Anders als in § 100a Abs. 5 Satz 1 Nr. 1 lit. b StPO hat diese zeitliche Einschränkung aber keinen Niederschlag im Gesetzeswortlaut gefunden. Hinzu kommt, dass der Trojaner zunächst alle gespeicherten Kommunikations-Inhalte auslesen und auswerten, um entscheiden zu können, welche davon nach dem Anordnung der Maßnahme gespeichert wurden, so dass sie als Quellen-TKÜ erhoben werden können. In dieser vollumfänglichen, zeitlich naturgemäß nicht begrenzten Auswertung der gespeicherten Kommunikationsinhalte liegt jedoch bereits eine dem Staat zuzurechnende Kenntnisnahme und damit eine Online-Durchsuchung, auch wenn die Daten nicht ausgeleitet, sondern noch „vor Ort“ auf dem infizierten System der Zielperson analysiert werden. Das Gesetz erlaubt somit eine stillschweigende Online-Durchsuchung, um festzustellen, welche ehemaligen Kommunikationsinhalte der Staatstrojaner unter den leichteren Voraussetzungen einer Quellen-TKÜ ausleiten darf.

Schließlich ist zu berücksichtigen, dass eine solche Ausweitung der Quellen-TKÜ auf frühere Kommunikation auch im Tatsächlichen auf allzu schwankendem Grund steht. Denn schon ein aus welchen Gründen auch immer falscher Zeitstempel einer gespeicherten Nachricht würde dazu führen, dass Inhalte ausgelesen würden, die vor Beginn einer Maßnahme gespeichert wurden. Dies jedoch würde bewirken, dass statt der angeordneten Quellen-TKÜ eine „irrtümliche“ Online-Durchsuchung durchgeführt

würde. Der Irrtum ändert jedoch nichts an der damit verbundenen Eingriffstiefe und die anzusetzenden verfassungsrechtlichen Anforderungen an eine Rechtfertigung dieses Eingriffs.

3. Wohnungsbetretungsbefugnis und Verletzung der Schutzpflicht

Die in § 33d Abs. 3 Satz 3 i.V.m. § 33c Abs. 5 SOG M-V enthaltene Befugnis zum Betreten und Durchsuchen von Wohnungen verstößt gegen Art. 13 GG (vgl. dazu bereits oben unter D.III.3).

§ 33d Abs. 3 SOG M-V verstößt schließlich auch gegen das IT-Grundrecht in seiner objekt-rechtlichen Dimension, da es an einem effektiven Schwachstellenmanagement fehlt (vgl. dazu bereits oben unter D.III.4).

V. Einsatz unbemannter Luftfahrsysteme (§ 34 SOG M-V)

Die Neuregelung des § 34 SOG M-V zum Einsatz von Drohnen, im Gesetz bezeichnet als unbemannte Luftfahrtsysteme, ist zum einen verfassungswidrig, soweit durch den Einsatz von Drohnen die angegriffenen Ermächtigungen zum Einsatz der besonderen Mittel der Datenerhebung, der Überwachung und Aufzeichnung der Telekommunikation und des verdeckten Zugriffs auf informationstechnische Systeme erst ermöglicht oder erweitert werden und soweit diese Ermächtigungen verfassungswidrig sind. Zum anderen ist die Neuregelung auch insoweit verfassungswidrig als damit Erhebung von Bild- und Tonaufnahmen von öffentlichen Veranstaltungen und Ansammlungen oder an öffentlich zugänglichen oder gefährdeten Orten gemäß § 32 Abs. 1, 3 oder 4 SOG M-V durch das Mittel des Drohnen-Einsatzes geregelt ist.

Hinsichtlich des Drohnen-Einsatzes als Mittel der Datenerhebung nach § 34 Nr. 2-5 SOG M-V in Verbindung mit den Ermächtigungsnormen der §§ 33 SOG M-V ergibt sich die Verfassungswidrigkeit aus den in Bezug auf die Ermächtigungsnormen §§ 33-33d dargelegten Gründen (siehe D.I.-IV).

Hinsichtlich der Variante § 34 Nr. 1 SOG M-V, wonach in Verbindung mit § 32 Abs. 1, 3, 4 und 10 SOG M-V nach dem Wortlaut des Gesetzes Drohnen zur „offenen“ Aufzeichnung oder Aufnahme von Menschenansammlungen eingesetzt werden können, beruht die Verfassungswidrigkeit darauf, dass im Gesetz keine ausreichende Schutzvorkehrung dafür vorgesehen ist, dass die jeweilige Maßnahme tatsächlich „offen“ umgesetzt wird. Denn Drohnen können in eine solchen Flughöhe eingesetzt werden oder so klein sein, dass ihr Einsatz mit den menschlichen Sinnesorganen nicht wahrnehmbar ist. Die Betroffenen eines solchen „offenen“ Einsatzes sollen zwar nach dem Wortlaut des Gesetzes auf die Datenverarbeitung „in geeigneter Weise“ hingewiesen werden, aber nach § 32 Abs. 6 SOG M-V soll dieser Hinweis wegen Gefahr im Verzug auch unterbleiben können.

Die Vorgabe des § 32 Abs. 6 S. 3 SOG M-V, dass eine wegen Gefahr im Verzug unterbliebene Mitteilung unverzüglich nachzuholen ist, muss dabei ins Leere gehen, weil klar ist, dass eine Drohne, die entweder öffentlichen Veranstaltungen und Ansammlungen oder öffentlich zugängliche oder gefährdete Orte filmt, dabei eine Vielzahl von Personen aufnimmt, die nur zeitweise vor Ort sind und sich danach wieder zerstreuen. Eine „Nachholung“ der Mitteilung, nachdem sich die Personen vom Ort weg bewegt haben, kann daher gar nicht alle Betroffenen der Maßnahme erreichen.

§ 34 Nr. 1 SOG M-V ist daher aufgrund der möglichen Anwendbarkeit des § 32 Abs. 6 S. 2 SOG M-V auf entsprechende Einsätze verfassungswidrig.

Hinzu kommt, dass die Streubreite des Eingriffs bei gleichzeitig nur theoretischer „Offenheit“ seine Verhältnismäßigkeit an sich in Frage stellt. Die Aufzeichnung einer öffentlichen Ansammlung zum Beispiel von Fußball-Anhängerinnen und Anhängern vor und bei einem Fußballspiel ermöglicht es der Polizei, die soziale Interaktion zwischen einer Vielzahl von Personen nachzuvollziehen. Wie in der Entscheidung zum bayerischen Versammlungsgesetz festgehalten (BVerfGE 122, 342, 370) stellen derartige Aufzeichnungen faktisch Datenvorratsspeicher dar. Im Geltungsbereich des Grundrechts auf informationelle Selbstbestimmung ist darauf zu achten,

dass nicht durch umfassende Registrierung die Erstellung von Persönlichkeitsprofilen ermöglicht wird (dazu allgemein BVerfGE 65, 1, 43ff). Auch der Einsatz einer polizeilichen Drohne, der zum Beispiel über den Stadionsprecher vor einem Fußballspiel kund getan wird, bedeutet insoweit eine Einschränkung des Vertrauens der Betroffenen, dass sie nicht Gegenstand umfassender staatlicher Überwachungsmaßnahmen sind.

VI. Ausschreibung zur polizeiliche Beobachtung und gezielte Kontrolle (§ 35 SOG M-V)

Die Ermächtigung zu personenbezogenen Ausschreibungen in § 35 SOG M-V verletzt das Recht auf informationelle Selbstbestimmung. Schon bei der Ausschreibung werden personenbezogene Daten verarbeitet und damit in dieses Grundrecht eingegriffen. Dies gilt ebenso für die Übermittlung der im Rahmen einer Polizeimaßnahme gewonnenen Erkenntnisse an die ausschreibende Behörde. Ein Grundrechtseingriff liegt erst recht vor, soweit die angegriffene Vorschrift zu zusätzlichen Datenerhebungen ermächtigt.

Die Ermächtigungsnormen aus § 35 SOG M-V sind verfassungswidrig, weil sie zu tiefgreifenden Grundrechtseingriffen ermächtigen, ohne dass die in der Norm genannten Voraussetzungen für die jeweilige Ausschreibung gewährleisten, dass sich die Maßnahme stets auf den Schutz hinreichend gewichtiger Rechtsgüter richtet (1). Soweit die Ausschreibung zur gezielten Kontrolle zusätzliche Datenerhebungen ermöglicht, fehlen jegliche tatbestandliche Voraussetzungen. Auch dies verfehlt die verfassungsrechtlichen Anforderungen (2). Soweit die Norm sich auf die vorbeugende Bekämpfung von Straftaten im Sinne der Strafverfolgungsvorsorge bezieht, besteht zudem keine Gesetzgebungskompetenz des Landes Mecklenburg-Vorpommern (3).

1. Zu niedrige materielle Eingriffsschwelle für die Ausschreibung

Die gesetzlichen Voraussetzungen, unter denen § 35 Abs. 1 (ggf. i.V.m. Abs. 2 S. 1) SOG M-V eine Ausschreibung ermöglicht, werden den verfassungsrechtlichen Anforderungen nicht gerecht, die an solch einen Grundrechtseingriff zu stellen sind.

Bei der Ausschreibung zur polizeilichen Beobachtung handelt es sich um einen schwerwiegenden Grundrechtseingriff. Bei zufälligen Kontrollen wird die ausgeschriebene Person als besonders gefährlich stigmatisiert. Dieser Effekt tritt nicht nur gegenüber den kontrollierenden Polizeikräften ein, sondern wirkt auch auf die betroffene Person und etwaige Mitreisende, indem diese wahrnehmen, dass sich die Kontrolle durch den Datenabgleich verzögert. Unabhängig von der zusätzlichen Befugnis des § 35 Abs. 2 SOG M-V kann die Ausschreibung auch weitere Maßnahmen zur Folge haben. Der Einschüchterungseffekt erfolgt gerade bei allgemeinen Kontrollen wie sie teilweise an Grenzen oder bei Großveranstaltungen durchgeführt werden dadurch, dass die Betroffenen nicht erfahren, dass und warum eine Ausschreibung vorliegt. Für sie wird jedoch ersichtlich, dass sie stärker kontrolliert werden als andere.

Die besondere Schwere des Grundrechtseingriffs resultiert auch daraus, dass die Ausschreibung ermöglicht und bezweckt, Bewegungsprofile zu erstellen (vgl. BT-Drs. 12/989, S. 43) und die ausschreibende Behörde so ein umfassendes Bild der privaten Lebensgestaltung der ausgeschriebenen Person erhält (vgl. BVerfGE 120, 378, 401; 141, 220, 287; Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, G Rn. 1104).

Eine besondere Eingriffsqualität besteht darüber hinaus für sog. Kontakt- und Begleitpersonen nach § 27 Abs. 3 Nr. 2 SOG M-V, deren Antreffen mit der ausgeschriebenen Person ebenfalls übermittelt und gespeichert wird. Da die Polizeikräfte regelmäßig keine Erkenntnisse darüber haben können, in welcher Beziehung zu der ausgeschriebenen Person diejenigen stehen,

die im gleichen Fahrzeug angetroffen werden, werden regelmäßig eher zufällige Begleitpersonen von der Maßnahme betroffen (Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, G Rn. 1106). Doch auch wenn die Vorgaben des § 27 Abs. 3 Nr. 2 SOG M-V eingehalten werden, handelt es sich immer noch um einen sehr großen Personenkreis. Er erfasst zum einen Personen, die nichts von der Gefahr einer Straftat wissen, die Anlass für die Überwachung ist. Zum anderen reichen für einen „nicht nur flüchtigen Kontakt" Personen aus dem gesamten – sowohl beruflichen als auch privaten – Lebensumfeld (BVerfGE 133, 277, 349).

Für die gezielte Kontrolle gemäß § 35 Abs. 2 SOG M-V kommt hinzu, dass zu dieser zusätzlich gemäß § 43 Abs. 1 Nr. 4 SOG M-V die automatisierte Kfz-Kennzeichenerfassung eingesetzt werden kann, was die Grundrechtsrelevanz weiter steigert (vgl. BVerfGE 120, 378, 406f).

Aufgrund der dargelegten Schwere des Grundrechtseingriffs bedarf die Ausschreibung einer hinreichend konturierten tatsächlichen Eingriffsschwelle und ist auf den Schutz gewichtiger Rechtsgüter zu beschränken (vgl. zur Übertragung der im BKAG-Urteil entwickelten Maßstäbe auf Überwachungsmaßnahmen minderer Eingriffsintensität BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, Rn. 146ff). § 35 Abs. 1 SOG M-V beinhaltet aber keine der Schwere des Eingriffs entsprechend hohen Voraussetzungen.

Zum einen ist die in S. 1 enthaltene Eingriffsbefugnis zu weit. Sie enthält weder die Anforderung, dass ein wenigstens seiner Art nach konkretisiertes und absehbares Geschehen erkennbar sein muss, noch die alternative Anforderung, dass das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründen muss, dass sie in überschaubarer Zukunft terroristische Straftaten begeht. Zum anderen sind die Straftatkataloge der § 49 SOG M-V zu weitreichend (siehe D.I.1.b).

Zum anderen ist nach S. 2 eine Ausschreibung auch bei Vorliegen einer drohenden terroristischen Gefahr i.S.d. § 67a SOG M-V möglich. Dies ist wegen

der Weite des Tatbestands des § 67a SOG M-V verfassungswidrig (siehe D.I.1.c).

2. Fehlen zusätzlicher Anforderungen für die Durchsuchung

Die Ermächtigung zur gezielten Kontrolle ist auch insoweit verfassungswidrig, als sie in § 35 Abs. 2 S. 2 SOG M-V weitergehende Erhebung von Daten und deren anschließende Übermittlung erlaubt, ohne dass dazu ein gesonderter Anlass besteht. Soweit gem. S. 3 die für die Identitätsfeststellung und Durchsuchung geltenden Vorschriften „im Übrigen“ anzuwenden sind, ergibt sich aus Systematik und Zweck der Regelung sowie den Gesetzesmaterialien (LT-Drs. 7/3694, S. 193), dass mit der Anwendung lediglich die diesbezüglichen Verfahrensvorschriften gemeint sind.

Das erhebliche Gewicht des Grundrechtseingriffs wird dadurch weiter verschärft. Denn diese Maßnahmen erfolgen zwar offen. Die besondere Eingriffstiefe gerade der Durchsuchung ergibt sich jedoch zum einen daraus, dass keine Anhaltspunkte dafür bestehen müssen, dass die Maßnahmen relevante Erkenntnisse zutage fördern. Ein Zweck soll bereits sein „den Druck zu erhöhen, potentielle Gefährder zu verunsichern und hierdurch gegebenenfalls von ihrem beabsichtigten Tun abzubringen“ (LT-Drs. 7/3694, S. 193). Gerade die Durchsuchung der Person ist ein besonders tiefer Eingriff in die Privatsphäre. Diese bewusst einschüchternde Maßnahme ist weiterhin nicht nur auf die Zielperson gerichtet, sondern erfasst bei einer Fahrzeugkontrolle auch die weiteren Insassen, deren Sachen ebenfalls durchsucht werden dürfen. Dies betrifft auch Personen, die die ausgeschriebene Person rein zufällig begleiten.

Die Weitergabe an und Verarbeitung durch die ausschreibende Behörde erfolgt dann zum anderen verdeckt. Diese kann in der Folge eine große Anzahl verschiedener Informationen zusammenfügen. Das daraus erstellte Persönlichkeitsprofil der ausgeschriebenen Person wird noch detaillierter und ist für diese damit ein besonders schwerwiegender Eingriff (vgl. BVerfGE 120, 378, 406f). Weiterhin wird der Kreis der Betroffenen noch größer.

Daher handelt es sich bei der gezielten Kontrolle sowohl in der Tiefe als auch in der Breite um eine besonders einschneidende Maßnahme.

Selbst bei schwerwiegenden Gefahren darf jedoch nicht darauf verzichtet werden, dass die Maßnahme im konkreten Fall erforderlich ist (vgl. BVerfGE 120, 378, 428f). Das hat zur Folge, dass die Umstände, die eine Ausschreibung zur polizeilichen Beobachtung und damit das Erstellen von Bewegungsprofilen rechtfertigen, nicht automatisch ausreichen, um auch eine Identitätsfeststellung weiterer Personen oder zusätzliche Durchsuchungen zu rechtfertigen. Gerade weil daraus ein Persönlichkeitsprofil erstellt werden kann, dürfen in dieses nur Informationen einfließen, für deren Erhebung auch ein konkreter Anlass bestand. Es ist daher verfassungsrechtlich geboten, dass die in § 35 Abs. 2 S. 2 SOG M-V genannten Befugnisse nur unter den Voraussetzungen ausgeübt werden, die §§ 29, 53, 57 SOG M-V an die jeweilige Maßnahme stellen (soweit andere Polizeigesetzen eine gezielte Kontrolle vorsehen, wird dies explizit genannt, vgl. § 17 Abs. 3 HSOG, § 40 Abs. 2 BayPAG, § 56 Abs. 1 S. 2 Nr. 2 PolG B-W).

3. Keine Gesetzgebungskompetenz zur vorbeugenden Bekämpfung von Straftaten

Abschließend ist darauf hinzuweisen, dass es insoweit an einer Gesetzgebungskompetenz des Landes Mecklenburg-Vorpommern fehlt, als der Grundrechtseingriff gem. § 35 Abs. 1 SOG M-V „zur vorbeugenden Bekämpfung“ von Straftaten erfolgen soll. Denn nach der Regelungskonzeption des SOG M-V ist davon eine Materie erfasst, die in die konkurrierende Gesetzgebungskompetenz des Bundes fällt. Eine landesrechtlichen Regelung ist durch den insoweit abschließenden § 163e StPO gesperrt.

Nach der Legaldefinition des § 7 Abs. 1 Nr. 4 SOG M-V soll die „vorbeugende Bekämpfung von Straftaten“ sowohl die Verhütung von Straftaten (Verhinderungsvorsorge) als auch die Vorsorge für die Verfolgung künftiger Straftaten (Strafverfolgungsvorsorge) umfassen (vgl. zur Abgrenzung VGH

Mannheim, Urt. v. 15.5.2014 – 1 S 815/13, juris Rn. 38ff). Nach der ursprünglichen Ansicht des Gesetzgebers waren beide Bereiche dem gemäß Art. 70 GG in die Zuständigkeit der Länder fallenden Gefahrenabwehrrecht zuzuordnen (so auch LVerfG M-V, LKV 2000, 149, 151 sowie LKV 2000, 345, 347). Dies ist jedoch hinsichtlich der Strafverfolgungsvorsorge überholt. Denn auch wenn für diesen Bereich noch keine Straftat begangen worden sein muss, dienen die zu diesem Zwecke erhobenen Daten dazu, in einem künftigen Ermittlungs- und Hauptverfahren verwendet zu werden. Die Strafverfolgungsvorsorge geschieht mithin in zeitlicher Hinsicht präventiv, betrifft aber gegenständlich das repressiv ausgerichtete Strafverfahren. Maßnahmen zu diesem Zweck fallen als Teil des Strafverfahrens gemäß Art. 74 Abs. 1 Nr. 1 GG unter die konkurrierende Gesetzgebungskompetenz des Bundes (BVerfGE 113, 348, 369ff; 150, 244, 273f).

Zwar liegen die Verhütung künftiger Straftaten und die Vorsorge für deren Verfolgung oft eng beieinander. Der Landesgesetzgeber darf daher auch gefahrenabwehrrechtliche Regelungen erlassen, die zugleich präventiv und repressiv wirken. Dann ist regelmäßig im Einzelfall zu prüfen, welchem Zweck eine Maßnahme schwerpunktmäßig dient. Bei der Ausgestaltung der Regelung muss sich der Landesgesetzgeber aber auf die Zweckrichtung beschränken, die in seiner Kompetenz liegt. Für die Beurteilung, ob eine Norm eine verfassungsrechtliche Kompetenzgrundlage hat, kommt es auf eine genaue Bestimmung der ihr bei objektivierter Sicht unterliegenden Zweckrichtung an. Die Schaffung oder selbständige Erweiterung von Eingriffsbefugnissen zur Verfolgung von Zwecken, die durch die jeweilige Kompetenz nicht gedeckt sind, kann durch die inhaltliche Nähe der Regelungsbereiche nicht gerechtfertigt werden (BVerfGE 150, 244, 275f).

Die Eingriffsbefugnis „zur vorbeugenden Bekämpfung solcher Straftaten“ in § 35 Abs. 1 SOG M-V hat nach objektiv Auslegung eine repressive Zweckrichtung. Denn sie ergänzt den bereits zuvor explizit genannten präventiven Zweck der Verhütung künftiger Straftaten. Nach § 7 Abs. 1 Nr. 4

SOG M-V fallen sowohl die Verhinderungs- als auch die Strafverfolgungsvorsorge unter diesen Begriff der vorbeugenden Bekämpfung von Straftaten. Die Nennung neben der Verhütung von Straftaten in § 35 Abs. 1 SOG M-V kann daher logisch nur bedeuten, dass die Eingriffsbefugnis um den Zweck der Strafverfolgungsvorsorge erweitert wird.

Der Bund hat für die polizeiliche Beobachtung und gezielte Kontrolle bereits eine Regelung in § 163e StPO getroffen, die eine weitergehende Gesetzgebung des Landes sperrt.

Gemäß § 163e Abs. 1 S. 1 StPO ist die Ausschreibung zur polizeilichen Beobachtung nur bei bereits begangenen Straftaten zulässig. In Abs. 1 S. 2, Abs. 2 werden differenzierte Anforderungen festgelegt, welche Personen und Sachen ausgeschrieben werden dürfen. Die Gesetzesmaterialien enthalten keine explizite Aussage darüber, ob diese Regelung als abschließend angesehen wurde (BT-Drs. 12/989, S. 43f). Aus dem Gesamtkontext ergibt sich jedoch, dass eine weitergehende landesrechtliche Regelung ausgeschlossen sein soll. Aufgrund des schweren Grundrechtseingriffs ist für die Ausschreibung gem. § 163e Abs. 4 StPO eine gerichtliche Anordnung vorgesehen. Es wäre widersprüchlich, wenn der Gesetzgeber eine solche verfahrensrechtliche Absicherung bei bereits begangenen Straftaten vorsehen wollte, wenn zugleich landesrechtlich Daten für ein Strafverfahren ohne eine solche erhoben werden dürften. In § 35 Abs. 5 SOG M-V bedarf dagegen erst die Verlängerung der Ausschreibung einer gerichtlichen Anordnung. Darüber hinaus wurde in § 163e StPO weder die Befugnis zur gezielten Kontrolle aufgenommen, noch wurde vorgesehen, dass die Ausschreibung zur polizeilichen Beobachtung im Vorfeld einer konkretisierten Gefahr erfolgen darf (so in §§ 35 Abs. 1 S. 2 i.V.m. 67a Abs. 1 SOG M-V). Dass in § 35 Abs. 1 und 2 SOG M-V nunmehr eine Ausweitung dieser Befugnisse im Bereich der Strafverfolgungsvorsorge eingeführt wird, widerspricht dem Gesamtkonzept des § 163e StPO, womit die Landesregelung unzulässig ist.

VII. Rasterfahndung (§ 44 SOG M-V)

Der in § 44 Abs. 1 Nr. 1 SOG M-V eingefügte Verweis auf die Voraussetzungen des § 67a Abs. 1 SOG M-V genügt nicht den verfassungsrechtlichen Anforderungen, die an die Eingriffsschwelle der Rasterfahndung zu stellen sind.

Aufgrund der hohen Eingriffsintensität der Maßnahme gebietet es das Verhältnismäßigkeitsprinzip, dass die Eingriffsschwelle einer konkreten Gefahr nicht unterschritten werden darf. Die Rasterfahndung hat eine hohe Eingriffsintensität, weil durch sie eine große Menge und Vielfalt personenbezogener Daten erhoben und abgeglichen werden kann und sie sich zudem gegen eine sehr große Zahl von Personen richtet, die hierzu keinen Anlass gegeben haben. Ob die Betroffenen Tatverdächtige oder Störer sind oder nicht, soll gerade erst herausgefunden werden, sei es bereits durch die Rasterung anhand weiterer Kriterien, sei es erst durch die sich anschließenden konventionellen personenbezogenen Ermittlungsmaßnahmen (BVerfGE 115, 320, 347ff, insb. 355).

Damit eine Rasterfahndung verhältnismäßig ist, muss daher eine Sachlage vorliegen, bei der im konkreten Fall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für diese Rechtsgüter eintreten wird. Auch bei einer Dauergefahr gelten diese Anforderungen an die hinreichende Wahrscheinlichkeit des Schadenseintritts sowie an die konkrete Tatsachenbasis der Wahrscheinlichkeitsprognose (BVerfGE 115, 320, 363ff).

Das BVerfG hat in seiner Entscheidung zum BKAG die dortige Regelung zur Rasterfahndung (damals § 20j, jetzt § 48 Abs. 1 BKAG) gebilligt und explizit betont, dass die Norm deshalb als verhältnismäßig ausgestaltet angesehen werden kann, weil über allgemeine Befugnis-Norm des damaligen § 20a Abs. 2 BKAG eine konkrete Gefahr vorausgesetzt ist (BVerfGE 141, 220, 303; vgl. auch Ruthig, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2018, § 48 BKAG Rn. 13).

Die Regelung des §§ 44 Abs. 1 Nr. 1 i.V.m. 67a Abs. 1 SOG M-V genügt dem Verhältnismäßigkeitsgrundsatz nicht, weil hier gerade keine konkrete Gefahr Voraussetzung für die Maßnahme ist (so auch Roggan, NJ 2020, 290, 297). In der Gesetzesbegründung des SOG M-V ist die Rechtsprechung des BVerfG zum BKAG zitiert (LT-Drs. 7/3694, S. 213), allerdings falsch verortet. Denn die zitierten Formulierungen des BVerfG zur Erweiterung des „tradierten sicherheitsrechtlichen Modells der Abwehr konkreter (...) Gefahren" beziehen sich nicht auf die Rasterfahndung, bei der das BVerfG das Vorliegen einer konkreten Gefahr verlangt. Denn die Erweiterung bezieht Sachverhalte mit ein, bei denen „sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt" (BVerfGE 141, 220, 272f), also keine konkrete Gefahr vorliegt.

Eine Vorverlagerung im Sinne des Tatbestandes des § 67a Abs. 1 SOG M-V ist in Bezug auf die Rasterfahndung verfassungswidrig, weil in § 67a Abs. 1 SOG M-V nur ein Teil der Mindestanforderungen erfüllt ist, die nach der Entscheidung zum BKAG aber bei einer Vorverlagerung eines Eingriffs vorliegen muss. Nach der verfassungsgerichtlichen Rechtsprechung darf eine Rasterfahndung nicht schon im Vorfeld einer konkreten Gefahr ermöglicht werden, denn sie würde zu vollständig verdachtslos und mit hoher Streubreite erfolgenden Grundrechtseingriffen führen, die Informationen mit intensivem Persönlichkeitsbezug erfassen können (BVerfGE 115, 320, 362f).

Insoweit § 44 SOG M-V auf § 67a Abs. 1 Nr. 2 SOG M-V verweist, ist die Norm auch in sich widersprüchlich. Denn nach § 67a Abs. 1 Nr. 2 SOG M-V muss aus dem individuellen Verhalten einer Person die Wahrscheinlichkeit eines Schadenseintritts abgeleitet werden können – die Rasterfahndung nach § 44 SOG M-V soll aber eine solche Person erst individualisieren.

VIII. Eingeschränkte Befugnisse der oder des Landesbeauftragten für den Datenschutz (§ 48b SOG M-V)

Da für die Verarbeitung von durch heimliche Maßnahmen gewonnenen Daten mangels regelmäßiger Offenlegung individueller Rechtsschutz nur sehr eingeschränkt sichergestellt werden kann, kommt der Gewährleistung einer effektiven Kontrolle durch eine unabhängige Stelle umso größere Bedeutung zu. Diese Kontrolle muss rechtlich und faktisch wirksam ausgestaltet werden und die Kontrollstelle mit effektiven Befugnissen ausgestattet sein (BVerfGE 133, 277, 369; 141, 220, 284).

Insgesamt widerspricht es schon dem Regelungsgefüge von Datenschutzgrundverordnung und JI-Richtlinie, dass im SOG auf Art. 58 der DSGVO und nicht auf Art. 47 Abs. 2 der JI-Ri Bezug genommen wird.

Die weitere Einschränkung des § 48b Abs. 1 SOG M-V, der nur die Befugnisse aus Art. 58 Abs. 2 a) und b) bezüglich Warnung und Verwarnung der DSGVO enthält, nicht aber die aus Art. 58 Abs. 2 c) bis j) DSGVO bezüglich Anweisungen und Anordnungen gegenüber dem Verantwortlichen, sowie des § 48b Abs. 2 SOG M-V, dass weitergehende Maßnahmen durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz nur angeordnet werden dürfen, 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, widerspricht einer Effektivität der Anordnungsbefugnis. Sie widerspricht im Übrigen auch den Vorgaben aus Art. 47 Abs. 2 lit. b und c der JI-Ri.

Dr. Anna Luczak
Rechtsanwältin