Stellungnahme des Arbeitskreises Kritischer Jurist*innen Greifswald

zum Entwurf eines Gesetzes über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern und zur Änderung anderer Gesetze (LT-Drs. 7/3694)

im Rahmen der Anhörung des Innen- und Europaausschusses des Landtags Mecklenburg-Vorpommern am 22. August 2019

Verfasser*innen: Peter Madjarov, Frauke Wolschke, Lieven Ullwer, Florian Meier

Mitarbeit: Hannah Sophie Strewe, Pia Angelika Müller

Inhaltsverzeichnis

Zusammenfassung wesentlicher Ergebnisse

Zunächst sollen die wesentlichen Ergebnisse der Stellungnahme zusammengefasst werden:

I. Allgemeines

- An vielen Stellen kann die Gesetzgebungstechnik nicht überzeugen. Verschiedene Normen lassen sich nicht in eine stringente Struktur einordnen. Das betrifft Kernelemente des Polizeirechts wie den Gefahrenbegriff. Die folgenden systematischen Brüche erschweren ebenso das Verständnis wie exzessive Verweisungen und übermäßig lange Paragraphen.
- Der Bedarf zahlreicher Regelungen ist zweifelhaft. Zum einen wird Mecklenburg-Vorpommern mit den bereits bestehenden Regelungen immer sicherer. Zum anderen werden viele angeblich erforderlichen Befugnisse bereits durch Bundesgesetze (BKAG, StPO) abgedeckt.
- Der Gesetzentwurf berücksichtigt nicht genügend die negativen Folgen, insbesondere die beeinträchtigten Grundrechte, die zahlreiche Überwachungsbefugnisse mit sich bringen. Der Entwurf orientiert sich häufig an Entscheidungen des Bundesverfassungsgerichts, die allerdings nur die Grenze dessen bilden, was gerade noch zulässig ist. Dass andere Bundes- oder Landesgesetze vergleichbare Regelungen treffen, sagt noch nicht, dass sie auch für Mecklenburg-Vorpommern passend sind. Umgekehrt ist zu betonen, dass viele Länder auf die beabsichtigten Neuerungen bewusst verzichten.

II. Hauptkritikpunkte

1. Staatstrojaner (Online-Durchsuchung, Quellen-Telekommunikationsüberwachung)

- Der staatliche Einsatz von Spähsoftware (Staatstrojaner) begegnet erheblichen Bedenken. Er ist auf Sicherheitslücken angewiesen und begünstigt damit Gefahren für IT-Systeme, was mit der staatlichen Schutzpflicht unvereinbar ist. Wenn dennoch daran festgehalten wird, sollten diese Nachteile zumindest durch eine Informationspflicht gegenüber IT-Unternehmen und eine unabhängige Zertifizierung der Software abgemildert werden.
- Dass zum Aufspielen der Software heimlich Wohnungen betreten und durchsucht werden dürfen, ist zumindest durch eine externe Begleitung dieser Maßnahmen zu kompensieren.
- Die Online-Durchsuchung beeinträchtigt verschiedene Aspekte der Privatsphäre, die im Einzelnen mit Eingriffen aus Telekommunikations- und Wohnraumüberwachung bzw. -durchsuchung vergleichbar sind, in der Kombination aber eine neue Dimension der Grundrechtsbeeinträchtigung darstellen. Gerade weil der Bedarf zweifelhaft ist, sollte auf diese Maßnahme verzichtet werden. Als verfassungsrechtliches Minimum sind zusätzliche Einschränkungen für die Überwachung des Kernbereichs privater Lebensgestaltung und von Unbeteiligten erforderlich.
- Bei der Quellen-Telekommunikationsüberwachung besteht aufgrund der verwendeten Technik die Gefahr, dass sie zur "kleinen Online-Durchsuchung" wird. Auch wenn fraglich ist, ob eine Abgrenzung zwischen beiden Maßnahmen technisch überhaupt möglich ist, sind im Gesetz dazu klarstellende Vorgaben zu machen. Zudem ist eine fachkundige Kontrolle der Technik sicherzustellen.

2. Durchsuchung und Sicherstellung von Cloud-Daten

- Auf mobilen elektronischen Geräten wie Smartphones oder Laptops ist heutzutage eine große Menge an sensiblen Daten gespeichert. Ein Auslesen dieser Geräte greift stark in die Privatsphäre der Betroffenen ein. Dies ist mit Durchsuchungen von Sachen in der analogen Welt nicht vergleichbar. Der nun ermöglichte Zugriff auf externe Speichermedien (insb. Cloud-Daten) vertieft dies und ist zumindest unter den Vorbehalt einer gerichtlichen Anordnung zu stellen.

3. Videoüberwachung im öffentlichen Raum

- Die Videoüberwachung im öffentlichen Raum darf aufgrund ihrer großen Streubreite und umstrittenen Wirksamkeit zur Verhinderung von Straftaten keinesfalls bei Bagatelldelikten eingesetzt werden. Deshalb ist die Eingriffsschwelle in § 32 Abs. 1-3 auf Straftaten von erheblichem Gewicht auszurichten.
- Die Überwachungswirkung von sog. Übersichtsaufnahmen darf nicht unterschätzt werden. Sie sollte nur bei Vorliegen konkreter Gefahren zulässig sein.
- Jeder Kameraeinsatz im öffentlichen Raum sollte durch eindeutige Hinweispflichten transparent gemacht werden. Bei Body- und Dashcams ist zudem sicherzustellen, dass sie auch zugunsten der betroffenen Privatpersonen verwendet werden. Dies sollte über Einsichtsrechte und eine Datentreuhandstelle erfolgen.
- Die Kameraüberwachung aus der Luft mittels Drohnen verstärkt die Grundrechtsbeeinträchtigung. Sie sollte nur unter gesteigerten Voraussetzungen zulässig sein.

4. Ausweitung der "drohenden terroristischen Gefahr"

- Das Konzept der "drohenden Gefahr" wurde für terroristische Straftaten über § 67a i.V.m. § 67c bereits ins SOG M-V eingeführt. Es ermöglicht Eingriffe, wenn noch kein Schadensereignis absehbar ist, und damit weit im Vorfeld von konkreten Gefahren. Durch den Entwurf wird es auf zahlreiche eingriffsintensive Überwachungsmaßnahmen ausgedehnt. Das begegnet erheblichen verfassungsrechtlichen Bedenken.
- Wenn dennoch daran festgehalten wird, sollte diesen zumindest durch Einschränkungen im Normtext Rechnung getragen werden: Die Straftat, auf die sich die drohende Gefahr bezieht, muss erhebliche Schädigungen besonders gewichtiger Rechtsgüter und nicht lediglich Vorbereitungs- oder Unterstützungshandlungen erfassen. Die darauf beruhenden Maßnahmen dürfen nur dazu dienen, die Gefahr weiter aufzuklären.

5. Überwachung von Unbeteiligten

- Es ist verfassungsrechtlich hoch problematisch, Menschen mit der Zielperson von heimlichen Überwachungsmaßnahmen gleichzustellen, obwohl sie selbst nicht verdächtigt werden – sei es als sog. Kontakt- oder Begleitpersonen, Nachrichtenmittler*innen o.ä. Wenn dies dennoch erfolgt, ist die Überwachung durch verschiedene Beschränkungen auf ein Minimum zu reduzieren:
- Sie ist auf den Schutz überragend wichtiger Rechtsgüter zu begrenzen und darf nicht schon Delikte mittlerer Kriminalität erfassen. Auch drohende Gefahren reichen hierbei nicht aus. Es dürfen zudem nur Kommunikationsvorgänge erfasst werden, die einen Bezug zum Anlass

der Überwachung haben. Daten, die mit dem Anlass der Überwachung nichts zu tun haben, sind unverzüglich zu löschen.

6. Unabhängige Kontrolle der Polizei

- Eine unabhängige Kontrolle der Polizei ist nicht allein wegen jüngster Skandale, sondern grundlegend als menschenrechtlicher Standard geboten. Perspektivisch sollten auch strafrechtliche Ermittlungen durch eine unabhängige Institution durchgeführt werden. Als kurzfristige Maßnahme sollte zumindest eine niedrigschwellige Beschwerdestelle eingeführt werden.
- Diese Beschwerdestelle sollte unabhängig, weisungsfrei und mit Ermittlungsbefugnissen ausgestattet sein und allen Menschen offen stehen. Dies kann sich an dem/der Bürgerbeauftragen des Landes orientieren oder in dessen/deren Aufgabenbereich eingegliedert werden.
- Für eine europarechtskonforme Kontrolle der Datenverarbeitung sollten einzelne Protokollierungs- und Löschfristen angepasst werden. Zudem sollte der/die Landesdatenschutzbeauftragte wirksame Eingriffsbefugnisse haben, um gegen Datenschutzverstöße vorgehen zu können.

III. Weitere Kritikpunkte

- Das SOG M-V soll künftig auch in die Versammlungsfreiheit eingreifen dürfen (§ 78). Um keine zusätzlichen Beschränkungen dieses demokratischen Grundrechts zu ermöglichen, sollte zumindest vorgeschrieben werden, dass einzelne Befugnisse ausdrücklich nicht bei Versammlungen eingesetzt werden dürfen.
- Beim Schutz des Kernbereichs privater Lebensgestaltung (§ 26a) sollte es verdeckt ermittelnden Einsatzkräften ausdrücklich untersagt werden, intime Beziehungen mit Zielpersonen einzugehen. Die Sichtung, ob Daten aus dem Kernbereich erhoben wurden, ist durch eine polizeiunabhängige Stelle durchzuführen und sollte regelmäßig auch bei der Online-Durchsuchung vorgenommen werden.
- Beim Berufsgeheimnisschutz sollte kein Unterschied zwischen Geistlichen, Anwält*innen und Abgeordneten einerseits sowie Journalist*innen, Ärzt*innen und Psychotherapeut*innen andererseits gemacht werden. Wenn er für die zweite Gruppe weiterhin relativiert werden soll, sind striktere Anforderungen an die Abwägung zu stellen.
- Bei der Bestandsdatenauskunft (§ 33h) ist die Abfrage von dynamischen IP-Adressen und Passwörtern unter den Vorbehalt einer gerichtlichen Anordnung zu stellen.
- Bei Durchsuchungen im Rahmen einer gezielten Kontrolle (§ 35) ist zu ergänzen, dass im Einzelfall eine konkrete Gefahr bestehen muss.
- Die automatisierte Kfz-Kennzeichenerfassung (§ 43a) ist insoweit verfassungswidrig, als sie von der Bundesgrenze bis zur A20 eingesetzt werden darf, obwohl für viele Teile dieses Bereichs kein hinreichender Grenzbezug besteht.
- Mit der Verfassung unvereinbar ist ebenso, die Rasterfahndung (§ 44) auch bei drohenden Gefahren (§ 67a) zu ermöglichen.
- Meldeauflagen sollten nur zur Abwehr von schwerwiegenden Gefahren zulässig sein.

I. Allgemeines

1. Gesetzgebungstechnische Mängel

Gesetzgebungstechnisch kann der Entwurf des SOG M-V nicht überzeugen. Schon bei zahlreichen Änderungen in der Vergangenheit wurde oftmals nur das konkrete Sachproblem in den Blick genommen, ohne auf eine stimmige Einpassung in das gesamte Gesetz zu achten. Diese Entwicklung wird mit dem vorliegenden Entwurf vertieft.

- Fehlende Systematik: Das Gesetz folgt zwar im Ansatz dem Aufbau, Übergreifendes vorab zu regeln und Besonderheiten in den spezielleren Normen des jeweiligen Abschnitts festzuhalten. An vielen Stellen wird davon jedoch **ohne ersichtlichen Grund abgewichen**. Dies beeinträchtigt die Verständlichkeit und logische Stringenz des Gesetzes.

- So werden in § 3 zahlreiche Begriffsbestimmungen hinzugefügt, die oftmals wörtlich aus EU-Normen übernommen wurden. Viele dieser häufig ausführlich definierten Begriffe werden nur in sehr wenigen Normen in speziellen Abschnitten aufgegriffen (Bsp.: "Profiling" in § 3 Abs. 5 Nr. 6 ist nur für § 25a und § 45c relevant; auf die in § 3 Abs. 5 Nr. 14 definierten "genetischen Daten" nimmt gar keine Norm Bezug). Dagegen werden andere, praktisch relevantere Begriffe in Spezialnormen definiert (vgl. Kontakt- und Begleitpersonen in § 27 Abs. 3 Nr. 2). Wenn sich **nicht logisch erklären** lässt, **an welcher Stelle im Gesetz eine Definition gefunden werden kann**, wird die Chance vertan, die Handhabung des Gesetzes zu erleichtern.

- Unübersichtlich ist auch die Regelung zentraler Bestandteile des Polizeirechts. So ist **kein stimmiges Konzept des Gefahrenbegriffs** ersichtlich: Zwar werden in § 3 Abs. 3 zu Recht wichtige Gefahrenbegriffe vorab geregelt. Jedoch erst am Ende des Abschnittes zur Datenverarbeitung findet sich eine Definition für Straftaten von erheblicher Bedeutung, obwohl diese eine bedeutende Rolle dabei spielen, die Eingriffsschwelle – auch in anderen Abschnitten des Gesetzes – zu variieren. Noch gravierender trifft dies auf die Regelung der drohenden terroristischen Gefahr in § 67a zu. Bei der Einführung dieser neuen Eingriffsschwelle im vergangenen Jahr mochte der Standort der Regelung in einem Spezialabschnitt zur Aufenthaltsüberwachung und -anordnung noch verständlich gewesen sein, verdeutlichte sie damit den außergewöhnlichen Charakter dieser Figur für wenige Spezialbefugnisse. Durch den Entwurf soll dieser Gefahrenbegriff jedoch für zahlreiche weitere Befugnisse, insbesondere im Rahmen der Datenverarbeitung, anwendbar sein. Das Verbannen der Regelung in eine Spezialnorm an das Ende des Gesetzestextes wird dessen zentraler Funktion nicht gerecht und erweckt den Schein, als ob die Tragweite der Regelung verschleiert werden solle.

- An vielen Stellen wird ein definierter Begriff im Folgenden nicht für sich stehend verwendet, sondern an den jeweiligen Stellen auf die Definition verwiesen (vgl. Kontakt- und Begleitpersonen aus § 27 Abs. 3 Nr. 2 in §§ 33, 35). Damit bleibt ein Nutzen der Begriffsbestimmungen aus. Viel schwerwiegender ist aber die **exzessive Verwendung von Verweisungen** insgesamt. Zahlreiche Normen verweisen – teilweise mehrfach – auf anderweitige Regelungen. Wird der Norminhalt nur durch ausführliches Blättern im Gesetz erkennbar, ist dies wenig anwendungsfreundlich. Dadurch steigt in der Praxis die Fehleranfälligkeit.[1]

- Ein weiteres Problem ist die **ausufernde Länge vieler Paragraphen**. Auch dadurch geht die Übersichtlichkeit verloren. Oft bedarf es mehrmaligen Lesens, um den Inhalt der Norm voll zu erfassen. Gerade im Datenschutzabschnitt wird das deutlich, wenn die §§ 45 bis 48h auf über 30 Sei-

[1] Vgl. zur Problematik von Verweisungen *Mertens*, Gesetzgebungskunst im Zeitalter der Kodifikationen, 2004, 480ff.

ten geregelt sind. Ein besonderes Einzelbeispiel ist § 25, dessen Stoßrichtung gut gemeint sein mag, der aber ob seiner Länge, der Verweisungen und komplizierter Formulierungen selbst mit großem Aufwand kaum verständlich ist.

2. Bedarf für neue Befugnisse zweifelhaft

Zahlreiche vorgesehene Änderungen sind zwingend geboten. Damit wird das SOG M-V an Vorgaben angepasst, die insbesondere aus der Datenschutzgrundverordnung und JI-Richtlinie der EU sowie Entscheidungen des Bundesverfassungsgerichts folgen. Es ist begrüßenswert, dass dadurch der Schutz persönlicher Daten und damit das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger gestärkt wird. Solange die Anpassungen nur darin bestehen, das Gesetz in Einklang mit höherrangigem Recht zu bringen, sind sie in einem Rechtsstaat allerdings auch eine Selbstverständlichkeit.

Für viele andere Regelungen ist aber nicht ersichtlich, dass für sie ein praktischer Bedarf besteht, der die teilweise gravierenden Freiheitsbeschränkungen rechtfertigt. Zum einen ist grundsätzlich hervorzuheben, dass **die Zahl der Straftaten immer weiter zurück geht**. Das betrifft nicht nur das Hellfeld der polizeilich registrierten Straftaten,[2] sondern auch das in Untersuchungen ermittelte Dunkelfeld.[3] Entgegen vielerorts verbreiteter Ansichten ist Mecklenburg-Vorpommern ein sicheres Land und die Tendenz gar positiv. Vor diesem Hintergrund können zusätzliche eingriffsintensive Befugnisse allenfalls punktuell in Betracht kommen. Sofern in der Gesetzesbegründung konkrete Deliktsfelder angesprochen werden, wird oft eine terroristische Bedrohungen angeführt. Es ist jedoch zu berücksichtigen, dass dafür gem. § 5 Abs. 1 BKAG **das BKA zuständig** ist.[4] Diesbezüglich müsste erst einmal dargelegt werden, in welchen Konstellationen neben den bundes- auch landesrechtliche Befugnisse benötigt werden.[5] Im Übrigen konnte die Polizei auch mit dem bis jetzt bestehenden Instrumentarium zahlreiche Straftaten verhindern. Für die wenigen Fälle, in denen das nicht gelang, scheinen vielmehr andere Defizite verantwortlich als angeblich fehlende Befugnisse, die nun eingeführt werden müssten.[6]

Soweit andere Regelungen auf den Bereich der Organisierten Kriminalität (OK) abzielen, so ist hervorzuheben, dass sich polizeiliche Ermittlungen meistens auf Personen beziehen dürften, die sich bereits "im strafbaren Bereich aufhalten". Sowohl bei Terrorismus als auch Organisierter Kriminalität sind vielfach schon Vorbereitungs- und Organisationstätigkeiten strafbar. Ab Vorliegen eines Anfangsverdachts ermittelt die Polizei zusammen mit der Staatsanwaltschaft aber **nach Maßgabe der StPO**. Für diese Fälle besteht dann kein *polizeirechtlicher* Bedarf nach neuen Eingriffsbefugnissen.[7]

Ein wesentlicher Grund für die Ausweitung zahlreicher Polizeibefugnisse dürfte vielfach ein "Mitschwimmen im Strom der Sicherheitsgesetzgebung" sein, der in den letzten Jahren zu vielen Verschärfungen von Polizei- und Straf(verfahrens)gesetzen geführt hat. Dies zeigen etwa die zahlreichen Verweise auf erweiterte Befugnisse in Bundes- und Landesgesetzen, die sich in der Gesetzes-

---

2 Vgl. *LKA M-V*, Polizeiliche Kriminalstatistik für das Land Mecklenburg-Vorpommern, 2018.

3 Vgl. *Balschmiter u.a.*, Befragung zur Sicherheit und Kriminalität in Mecklenburg-Vorpommern, Abschlussbericht zur zweiten Befragung 2018.

4 In der Regel dürfte schon eine originäre Zuständigkeit bestehen, die gem. Nr. 1 bei länderübergreifenden Gefahren vorliegt. Zumindest auf Ersuchen des LKA ist dies aber stets möglich.

5 Vgl. *Buermeyer*, Stellungnahme zum Brandenburgischen Polizeigesetz, Innenausschuss LT Brandenburg, S. 5.

6 Hierzu etwa: https://www.dw.com/de/medien-berliner-polizei-fahndete-viel-zu-spät-nach-dem-attentäter-anis-amri/a-40530160 (07.08.2019); https://www.spiegel.de/politik/deutschland/fall-anis-amri-sonderermittler-wirft-behoerden-versagen-vor-a-1172571.html (07.08.2019); *Jost*, Abschlussbericht des Sonderbeauftragten des Senats für die Aufklärung des Handelns der Berliner Behörden im Fall AMRI, 2017.

7 Vgl. *Buermeyer*, Stellungnahme zum Brandenburgischen Polizeigesetz, Innenausschuss LT Brandenburg, S. 5.

begründung finden. Diese Gesamtentwicklung ist geprägt von einem Sicherheitsdenken, das trotz verbesserter objektiver Sicherheit auf ein wachsendes Sicherheitsbedürfnis in der Bevölkerung reagieren möchte. Das bloße Sicherheitsgefühl ist aber kein legitimes Schutzgut von grundrechtsbeschränkenden Maßnahmen – zumal es ohnehin unerreichbar ist.[8]

Schließlich wird auch in anderen Bereichen nicht fundiert dargelegt, dass die Polizei in M-V genau diese Befugnisse braucht. Dass sie auch in manch anderen Ländern bestehen, ist noch kein Grund sie einzuführen – zumal nicht erwähnt wird, dass oftmals die Mehrheit der Länder auf entsprechende Regelungen bewusst verzichtet. Stattdessen wäre es ein Gebot rationaler Gesetzgebung, dass **die bestehenden Befugnisse zunächst evaluiert** würden. Das trifft insbesondere auf neuere Befugnisse der Datenerhebung wie Bestandsdatenauskunft oder Bodycams zu. Es ist aber immerhin begrüßenswert, dass nun in § 116 eine Evaluierungspflicht eingeführt wird – auch wenn die Frist durchaus hätte kürzer ausfallen können.[9]

3. Fehlende Abwägung der widerstreitenden Interessen

Zahlreiche Formulierungen in neuen Eingriffsbefugnissen werden wörtlich aus Passagen der Bundesverfassungsgerichtsentscheidung übernommen. Das ist schon aus Gründen der Gewalten(ver)teilung problematisch, schließlich ist es weder Anspruch noch Aufgabe des Gerichts, Formulierungsgehilfe der Parlamente zu sein. Im Gegenteil ist es die **originäre Aufgabe des gewählten Landtags, widerstreitende Interessen in Ausgleich zu bringen** und in allgemeingültige Gesetze zu schreiben. Insofern möchten wir an die Abgeordneten appellieren, diese Aufgabe wahrzunehmen.

Hierbei ist zu berücksichtigen, dass **das Bundesverfassungsgericht nur die Grenze** dessen formuliert, **was verfassungsrechtlich gerade noch zulässig** ist. Ein Mehr an Sicherheit bedeutet aber immer auch die Verkürzung von Freiheitsrechten. Es darf keinen Automatismus geben, dass die Polizei immer alles tun darf, was gerade noch erlaubt ist. Die wörtliche Übernahme von Verfassungsgerichtsentscheidungen schafft keine Balance zwischen Sicherheit und Freiheit, sondern bedient einseitig die Interessen der Sicherheitsbehörden.[10] Andere Länder beweisen jedoch, dass das Parlament einen Gestaltungsspielraum hat und diese Balance austariert werden kann..[11]

Weiterhin ist zu berücksichtigen, **in welchem Kontext die als Vorlage dienenden Entscheidungen stehen.** Die meist zitierte betrifft das BKA-Gesetz, das spezifisch auf die Terrorabwehr zugeschnitten ist. Die Aussagen des Gerichts beziehen sich daher nur auf diesen Phänomenbereich und sind nicht ohne Weiteres auf ein allgemeines Polizeigesetz wie das SOG M-V übertragbar. Gleiches gilt übrigens für die Orientierung an Regelungen des aktualisierten BKAG.[12] Auch ist zu berücksichtigen, dass die Entscheidungen nur einzelne Aspekte einer Regelung behandeln können. Wenn erklärt wird, welche Gefahrenlage mindestens bestehen muss, damit eine Maßnahme ergriffen werden kann, ist damit noch nicht ausgesagt, auf wen sie sich beziehen darf und welches Verfahren eingehalten werden muss.

---

8 Vgl. *Thiel*, Die "Entgrenzung" der Gefahrenabwehr, 2010, 188ff., *Gusy*, Vom "Neuen Sicherheitsbegriff" zur "Neuen Sicherheitsarchitektur", in: Würtenberger u.a. (Hrsg.), Innere Sicherheit im europäischen Vergleich, 2012, 71 (74f.).

9 Vgl. *Gazeas*, Stellungnahme zum Polizeigesetz NRW vom 13.11.2018, Innenausschuss LT NRW, Nr. 17/945, S. 16.

10 Vgl. *Buermeyer*, Stellungnahme zum BKA-Gesetz, 16.03.2017, Innenausschuss BT, A-Drs. 18(4)806 E, S. 3.

11 Dass in der Begründung die Frage nach "Alternativen" mit "keine" beantwortet wird (S. 8f.), ist eigentlich ein Armutszeugnis des Gesetzgebers, aber leider deutschlandweit gängige Praxis.

12 Vgl. *Buermeyer*, Stellungnahme zum BKA-Gesetz, 16.03.2017, Innenausschuss BT, A-Drs. 18(4)806 E, S. 3: "kein Muster-Polizeigesetz" für Landesgesetzgeber. Der Landesinnenminister Caffier hat aber genau dieses Gesetz zum Vorbild erklärt, vgl. Protokoll der 40. Sitzung des Landtags am 27. Juni 2018, S. 98.

II. Hauptkritikpunkte

1. Einführung von Staatstrojanern, Online-Durchsuchung und Quellen-Telekommunikationsüberwachung

a. Zum Einsatz von Staatstrojanern

Um die in §§ 33c, 33d Abs. 3 eingeführten Maßnahmen der Online-Durchsuchung und Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) durchführen zu können, ist der Einsatz von staatlicher Spionagesoftware – dem sog. Staatstrojaner – vorgesehen, die der Polizei Zugriff auf die betroffenen Systeme gewährt.[13]

- Mit dem Staatstrojaner ist ein Einsatzmittel geplant, das die Sicherheit im digitalen Raum gefährdet. Der Einsatz ist nur möglich, wenn **Sicherheitslücken** in den betroffenen IT-Systemen vorhanden sind, um durch diese Zugriff auf das Zielsystem zu erhalten.[14] Die Folge ist, dass mit der Regelung ein **Interesse dafür** geschaffen wird, **solche Lücken offen zu lassen**: das Ergebnis könnte sein, dass die Polizei den Hersteller*innen gefundene Sicherheitslücken nicht mehr meldet, um effektiv die Maßnahmen der Online-Durchsuchung und der Quellen-TKÜ durchführen zu können.[15] Diese nicht geschlossenen Lücken in IT-Systemen könnten nicht nur Behörden ausnutzen, sondern auch Dritte, die diese „Hintertüren" zu anderen Zwecken missbrauchen.[16] Gerade dieser Aspekt zeigt, wie widersprüchlich der Einsatz des Staatstrojaners ist: Statt mehr Sicherheit zu schaffen, werden **Missbrauchsmöglichkeiten begünstigt.** Fragwürdig erscheint, inwieweit die Nutzung des Staatstrojaners der staatlichen Schutzpflicht überhaupt noch Rechnung tragen kann. Dazu kommt, dass es nach dem jetzigen Stand der Technik **nicht möglich** sein wird, die **Auswirkungen** der Software in den betroffenen Systemen nachhaltig **zu beheben** und auf „null" zu setzen.[17] Durch das Aufspielen des Trojaners wird „eine sichere und vertrauenswürdige Informationsverarbeitung nicht mehr gewährleistet."[18]

- Im neuen Gesetzesentwurf ist zudem geplant, dass zur Infiltration des Staatstrojaners auf die betroffenen Systeme das Betreten und Durchsuchen von Räumlichkeiten – damit auch der Wohnraum – und das Durchsuchen von Sachen erlaubt werden sollen (vgl. § 33c Abs. 5 sowie § 33d Abs. 3 S. 3). Die Intensität der Grundrechtsbeeinträchtigung, die mit der **heimlichen Wohnungsbegehung** einerseits und der verdeckten Überwachung andererseits einhergeht, muss dazu führen, dass wenigstens die Überwachung innerhalb enger Grenzen gehalten wird.[19] Im Gegensatz zur offenen Wohnungsdurchsuchung fehlt aber ein Anwesenheitsrecht der Betroffenen. Es ist daher zweifelhaft, inwieweit sichergestellt werden kann, dass die Räumlichkeiten der Betroffenen lediglich zur Infiltration des informationstechnischen Geräts betreten und durchsucht werden. Dem Entwurf fehlt es hier bspw. an einer **umfänglichen Dokumentationspflicht**. Eine **unabhängige Kontrollstelle** bzw. ihre Mitarbeiter*innen sollten sowohl das **Durchsuchen von Sachen als auch das Betreten und Durchsuchen von Räumlichkeiten begleiten**.

[13] LT-Drs. 7/3694, S. 178ff.; vgl. auch *Derin/Golla,* Der Staat als Manipulant und Saboteur der IT-Sicherheit? Die Zulässigkeit von Begleitmaßnahmen zu „Online-Durchsuchung" und Quellen-TKÜ, NJW 2019, 1111 (1111).

[14] *Blechschmitt,* Strafverfolgung im digitalen Zeitalter. Auswirkungen des stetigen Datenaustauschs auf das strafrechtliche Ermittlungsverfahren, MMR 2018, 361 (365).

[15] *Blechschmitt*, MMR 2018, 361 (365) m.w.N.; *Buermeyer,* Stellungnahme zum BKA-Gesetz, 16.03.2017, Innenausschuss BT, A-Drs. 18(4)806 E, S. 13f.

[16] Gemeint ist der Bereich der sog. Cyber-Kriminalität, vgl. *Buermeyer,* ebd., S. 14.

[17] *Arzt,* Stellungnahme zum Brandenburgischen Polizeigesetz, 09.01.2019, Innenausschuss LT Brandenburg, S. 39 m.w.N.

[18] *Arzt*, ebd., S. 39 m.w.N.

[19] *Soiné,* Die strafprozessuale Online-Durchsuchung, NStZ 2018, 497 (501).

- Es fehlen Regelungen, die die Sicherung der Schutzlücken betreffen. Der Staatstrojaner wäre nur denkbar, wenn die Behörden ihrer staatlichen Schutzpflicht durch eine gesetzliche Verpflichtung nachkommen müssten, wie zum Beispiel einer **Informationspflicht bestehender Sicherheitslücken gegenüber den IT-Unternehmen**. Zudem müsste gewährleistet sein, dass die Software fehlerfrei funktioniert und technisch nur das kann, was rechtlich erlaubt ist. Neben der Überarbeitung der inhaltliche Vorgaben in § 33c Abs. 3 sollte eine unabhängige Stelle vorgesehen werden, die diese überwacht. Dies könnte etwa durch die **Zertifizierung der Software durch den*die Bundes- oder Landesdatenschutzbeauftragte*n** erfolgen.[20]

b. Zum Einsatz der Online-Durchsuchung, § 33c

Mit der Einführung der Online-Durchsuchung soll es den Polizeibehörden ermöglicht werden, auf Systeme (wie z.B. das Smartphone, den Computer oder andere Speichermedien) von Betroffenen verdeckt zuzugreifen, um über einen längeren Zeitraum Daten erheben und sammeln zu können.[21] Im Gegensatz zur klassischen Hausdurchsuchung, in der die Polizei Wohnungen oder andere Räumlichkeiten sichtbar betritt und mit Kenntnis der Betroffenen durchsucht, werden mit der Online-Durchsuchung verdeckt über einen längeren Zeitraum Daten gesammelt.[22] Im Gegensatz zur Wohnraumüberwachung ist sie nicht auf einen Ort und im Gegensatz zur Telekommunikationsüberwachung nicht nur auf Kommunikationsinhalte, die mit anderen Menschen geteilt werden beschränkt. Sie erfasst auch Dokumente , die niemals an Dritte gelangen sollten. Für Betroffene ist das Ausmaß dieser „Durchsuchung“ kaum bis gar nicht abschätzbar – sie ist eine **Überwachungsmaßnahme von bisher nicht gekannter Intensität**.

Verschiedene Einzelaspekte, die auch im Zusammenhang mit anderen Maßnahmen problematisch sind und in dieser Stellungnahme deshalb übergreifend behandelt werden, erlangen im Rahmen der Online-Durchsuchung eine besondere Qualität. Folgende Punkte sind in diesem Zusammenhang explizit zu berücksichtigen:

- Die Maßnahme kann neben den Vorgaben aus § 33c Abs. 1 Nr. 1, 2 **bereits beim Vorliegen einer „drohende[n] Gefahr“** nach § 67a Abs. 1 und damit trotz des tiefgreifenden Eingriffs bereits im Gefahrenvorfeld angeordnet werden (vgl. S. 19ff. der Stellungnahme).

- Durch § 33c Abs. 1 Satz 4a können Personen von der Maßnahme umfasst werden, die lediglich ungewollt ermittlungsrelevante Informationen gespeichert haben. Damit sind **Unbeteiligte betroffen** (vgl. S. 21ff. Stellungnahme). Die Bestimmung aus § 33c Abs. 1 Satz 4 dürfte nach den Maßstäben des BVerfG ohnehin **zu unbestimmt** sein: Nach Auffassung des Gerichts ist die Anwendung der Online-Durchsuchung auf andere Personen nur anwendbar, „wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Zielperson dort ermittlungsrelevante Informationen speichert ***und*** *ein auf ihre eigenen informationstechnischen Systeme beschränkter Zugriff zur Erreichung des Ermittlungsziels nicht ausreicht.*“[23] Der zweiten Voraussetzung fehlt es im vorliegenden Gesetzesentwurf vollkommen.

- In Bezug auf die Regelung des Schutzes des Kernbereichs privater Lebensgestaltung (§ 26a, siehe dazu S. 29f. der Stellungnahme) heißt es im § 33c Abs. 2, dass, **soweit möglich**, kernbereichsrelevante Daten nicht erhoben werden dürfen. **Der Kernbereichsschutz könnte leer laufen.** Gerade

[20] Vgl. *Gazeas*, Stellungnahme zum Polizeigesetz NRW, Juni 2018, S. 19f.

[21] *Singelnstein/Derin*, Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, NJW 2017, 2646 (2646f.).

[22] *Petri*, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, G Rn. 617.

[23] BVerfGE 141, 220 (273f. = Rn. 115).

die Qualität der Online-Durchsuchung allein macht einen wirksamen Schutz schon nahezu unmöglich. Fast alle Daten auf den betroffenen Geräten – Smartphone, Computer usw. – werden sensibelste Informationen von und über Betroffenen offenlegen, sodass die **Erstellung von Persönlichkeitsprofilen** ohne Probleme möglich sein wird.[24] Es fehlt an Regelungsmechanismen, die die Auswertung der erhobenen Daten betreffen.

- Im Entwurf heißt es weiterhin, dass für „eine effektive Gefahrenabwehr, insbesondere im Bereich des Terrorismus […] die hierfür erforderlichen Instrumente an die Hand gegeben werden [müssen]. Dazu gehört auch die Maßnahme des verdeckten Eingriffs in informationstechnische Systeme."[25] Dem ist entgegen zu halten, dass die Befugnis der **Online-Durchsuchung bereits auf Bundesebene** für das BKA vorgesehen ist (vgl. dazu oben S. 9). Auch ist das BKA die zuständige Behörde, die sich umfassend mit dem Bereich des Terrorismus auseinanderzusetzen hat. Es würden zahlreiche **Doppelzuständigkeiten** entstehen, wenn die geplanten Befugnisse wie die Online-Durchsuchung auf Landesebene eingeführt würden. Damit ist nicht ersichtlich, dass ein Bedarf zur Einführung dieser Maßnahme auf Landesebene besteht. Zudem haben auch andere Bundesländer (z.B. Brandenburg[26], Sachsen[27], NRW[28] oder Baden-Württemberg[29]) trotz der Novellierung der dortigen Polizeigesetze bewusst auf die Einführung der Online-Durchsuchung verzichtet. In Rheinland-Pfalz ist die Befugnis bereits seit 2011 eingeführt, wurde aber noch kein einziges Mal angewandt.[30] Vor diesem Hintergrund ist äußerst zweifelhaft, ob die Einführung der Online-Durchsuchung für das Land Mecklenburg-Vorpommern wirklich notwendig ist. Nach hier vertretener Auffassung bedarf es dieser grundrechtsintensiven Maßnahme nicht.

c. Zum Einsatz der Quellen-TKÜ, § 33d

Auch die Einführung der Quellen-TKÜ ist vorgesehen (vgl. § 33d). Bei dieser Befugnis liegt der Schwerpunkt auf der laufenden Telekommunikation von Personen.[31] Wie bei der Online-Durchsuchung ist es zur Durchführung der Quellen-TKÜ notwendig, dass auf die betroffenen Geräte der Staatstrojaner gespielt wird, um die gewollten Daten vor ihrer Verschlüsselung sammeln zu können.[32] Auch diese geplante Maßnahme löst **weitreichende Bedenken** aus. Mit der Einführung der Befugnis besteht die **Gefahr**, dass sie sich zu **einer „kleinen Online-Durchsuchung"**[33] entwickelt. Beide unterscheiden sich lediglich im Hinblick auf die erhobenen Daten: bei der Quellen-TKÜ dürfen nur solche Daten erfasst werden, die die Telekommunikation betreffen, bei der Online-Durchsuchung alle außerhalb der Kommunikation.[34] Es muss sichergestellt werden, dass mit der Anordnung der Quellen-TKÜ auch allein Kommunikationsdaten erfasst werden. Inwieweit eine Trennung zwischen beiden Bereichen stattfinden soll, ist unklar, da eine derart **technische Trennung nach heuti-**

---

24 Vgl. *Singelnstein/Derin*, NJW 2017, 2646 (2647), *Soiné,* NStZ 2018, 497 (497). Dies ist als Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu werten, vgl. BVerfGE 120, 274 (302ff.); 141, 220 (303 = Rn. 209).

25 LT-Drucksache 7/3694, S. 179.

26 LTO v. 13.03.2019, abrufbar unter: https://www.lto.de/recht/nachrichten/n/brandenburg-landtag-beschliesst-polizeigesetz-buerger-freiheit-terrorismus/ (07.08.2019).

27 *Debski,* LVZ v. 22.01.2019, abrufbar unter: https://www.lvz.de/Region/Mitteldeutschland/CDU-und-SPD-einigen-sich-in-Sachsen-auf-neues-Polizeigesetz (07.08.2019).

28 https://fdp.fraktion.nrw/content/rasche-und-lurbke-polizei-und-burgerrechte-starken (07.08.2019).

29 https://www.gruene-landtag-bw.de/index.php?id=14427 (07.08.2019).

30 https://www.landtag.rlp.de/landtag/drucksachen/2752-17.pdf, S. 20 (07.08.2019).

31 *Singelnstein/Derin*, NJW 2017, 2646 (2647).

32 *Kingreen/Poscher*, Polizei- und Ordnungsrecht mit Versammlungsrecht, 10. Aufl., München 2018, § 13 Rn. 139.

33 BT-Drs. 18/12785, 50; *Kruse/Grzesiek*, KritV 100 (2017), 331 (335ff.).

34 BVerfGE 120, 274 (308f.); *Singelnstein/Derin*, NJW 2017, 2646 (2647).

gem Stand der Technik nicht möglich ist.[35]

Einen weiteren Punkt betrifft die Durchsuchung der gespeicherten Kommunikation – z.B. Chatverläufe –, die im § 33d Abs. 3 S. 2 vorgesehen ist. Es sollen auch Inhalte und Umstände der Kommunikation überwacht werden dürfen, die bereits vor der Anordnung auf dem betreffenden Gerät produziert/gespeichert wurden. Im Gegensatz zu § 100a Abs. 5 StPO fehlt es im vorliegenden Gesetzesentwurf an einer Beschränkung. In § 100a Abs. 5 StPO wird vermerkt, dass der Telekommunikationsvorgang **erst *ab Anordnung*** *der Überwachung* aufgezeichnet werden darf. Mit einer solchen Beschränkung könnte sichergestellt werden, dass die Quellen-TKÜ auch nur die Telekommunikation umfasst und **nicht etwa als „kleine Online-Durchsuchung“** stattfindet. Hier ist zwar einzuwenden, dass auch mit einer derartigen Regelung die Prüfung der vorangegangenen Kommunikation unvermeidbar wäre. Erst wenn dieses Dilemma aufgelöst werden kann, kann die Quellen-TKÜ als polizeiliche Antwort darauf angesehen werden, dass sich das Kommunikationsverhalten vom klassischen Telefon auf verschlüsselte Wege verlagert.[36]

- Zudem stellt sich die Frage, wie die **richterliche Kontrolle** solche Feinheiten überblicken kann. Um die Quellen-TKÜ (gleiches gilt für die Online-Durchsuchung) durchführen zu können, werden Polizeibehörden auch verschiedene Software von privaten Anbieter*innen nutzen, um die Zielsysteme infiltrieren zu können.[37] Es wird für den*die Richter*in **nicht erkennbar** sein, **wie umfassend die Funktionen der Schadsoftware sind** und welche Auswirkungen diese im Einzelnen mit sich bringen.[38] Dieser mögliche Verlust richterlicher Kontrolle dürfte derart ins Gewicht fallen, dass die Einführung dieser Maßnahme gänzlich zu überdenken ist – gerade vor dem Hintergrund ihrer Grundrechtsintensität. Wie bei der Online-Durchsuchung ergibt sich auch für die Befugnis der Quellen-TKÜ **kein Bedarf**. Zu groß ist die Gefahr, dass sie sich zu einer „kleinen Online-Durchsuchung“ entwickelt und für Informationen genutzt wird, die über die laufende Telekommunikation hinausgehen. So haben bspw. die Bundesländer Brandenburg[39] und Sachsen[40] bewusst auf die Einführung der Quellen-TKÜ verzichtet.

2. Durchsuchungen und Sicherstellungen von Cloud-Daten (§ 57 Abs. 2, § 61 Abs. 1 S. 2-6)

a. Zur Persönlichkeitsrelevanz von Daten auf mobilen elektronischen Geräten

Bei Durchsuchungen von Sachen i.S.d. § 57 Abs. 1 entspricht es der wohl herrschenden Meinung, dass in diesem Zusammenhang auch das Auslesen von elektronischen Geräten wie Handys umfasst ist, obwohl Daten keine körperlichen Gegenstände i.S.d. § 90 BGB sind.[41] Angesichts der technischen Entwicklung wird diese Gleichsetzung den damit verbundenen Grundrechtsbeeinträchtigungen nicht gerecht, da Daten auf Smartphones heutzutage eine besondere Persönlichkeitsrelevanz haben. Zwar betont das Bundesverfassungsgericht immer wieder das Recht auf informationelle Selbstbestimmung, doch hat dies in den Durchsuchungs- und Sicherstellungsbefugnissen (§§ 57f., 61f.) noch keinen Niederschlag gefunden. Dabei wäre auch in Deutschland eine Anpassung an den tech-

35 Siehe dazu auch *Roggan,* Stellungnahme zum Brandenburgischen Polizeigesetz, 03.01.2019, Innenausschuss LT Brandenburg, S. 38f.

36 Dies führt das Innenministerium als Begründung an, vgl. LT-Drs. 7/3694, S. 185 sowie Pressemitteilung Nr. 27 vom 29.01.2019.

37 *Gazeas,* Stellungnahme zum Polizeigesetz NRW, Juni 2018, S. 19 m.w.N.

38 *Gazeas*, Stellungnahme zum Polizeigesetz NRW, Juni 2018, S. 19.

39 LTO v. 13.03.2019, abrufbar unter: https://www.lto.de/recht/nachrichten/n/brandenburg-landtag-beschliesst-polizeigesetz-buerger-freiheit-terrorismus/ (07.08.2019).

40 *Debski,* LVZ v. 22.01.2019, abrufbar unter: https://www.lvz.de/Region/Mitteldeutschland/CDU-und-SPD-einigen-sich-in-Sachsen-auf-neues-Polizeigesetz (07.08.2019).

41 Vgl. *Kingreen/Poscher*, Polizei- und Ordnungsrecht, 10. Aufl. 2018, § 17 Rn. 12.

nischen Fortschritt geboten. Denn während bei der Durchsuchung von Sachen der Standardfall die Durchsuchung von Handtaschen oder Kfz ist, bei denen im analogen Zeitalter typischerweise allenfalls persönliche Daten im Umfang eines Adressbuchs erfasst werden, sind auf elektronischen Geräten **regelmäßig umfangreiche Daten mit erheblichem Persönlichkeitsbezug** vorhanden, weshalb deren **Durchsuchung in der Intensität eher mit der einer Wohnung als einer Handtasche vergleichbar** ist. In den USA hat die Rechtsprechung reagiert und betont, dass die Durchsuchung eines Smartphones nicht mit der einer Brieftasche oder eines Adressbuches vergleichbar ist, sondern die unverbrüchliche Privatsphäre berührt.[42]

b. Zur Erweiterung der Durchsuchung und Sicherstellung auf getrennte Speichermedien

Nun soll im Rahmen der Durchsuchung aber nicht mehr nur auf die Daten des gesuchten Geräts zugegriffen werden, sondern gem. Abs. 2 auch die Daten ausgelesen werden, die sich auf räumlich getrennten Speichermedien (i.d.R. sogenannte Cloud-Daten) befinden. Diese Daten haben aber **mit der Durchsuchung einer Sache praktisch nichts mehr zu tun** – es handelt sich bei Abs. 2 der Sache nach um **eine eigenständige Datenerhebungsbefugnis**. In § 61 Abs. 2 werden nunmehr die Voraussetzungen geregelt, unter denen diese Daten "sichergestellt", d.h. durch die Behörden gespeichert werden dürfen. Diese beiden Neuerungen stellen massive Eingriffe in verschiedene Grundrechte dar, gegen die erhebliche Bedenken bestehen.

- Der Gesetzentwurf scheint die Intensität der Grundrechtsbeeinträchtigung, die eine Durchsuchung von Speichermedien mit sich bringt, nicht vollständig zu erfassen. Er verweist darauf, dass das Bundesverfassungsgericht die Durchsuchung von Cloud-Daten im Rahmen der Online-Durchsuchung grundsätzlich gebilligt hat,[43] verschweigt aber, dass für diese Maßnahme im BKA-Gesetz besonders hohe materielle Voraussetzungen bestehen müssen. Eine Durchsuchung von Sachen ist hingegen schon verdachtsunabhängig an sogenannten gefährlichen Orten zulässig. Mit keinem Wort werden die dadurch hervorgerufenen Grundrechtseingriffe erwähnt. Dabei handelt es sich um einen **Eingriff in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme bzw. das Telekommunikationsgeheimnis gem. Art. 10 GG**.[44] Zu berücksichtigen ist auch, dass externe Speichermedien regelmäßig nicht nur von einer Person genutzt werden. Angebote wie iCloud, GoogleDrive oder Dropbox werden regelmäßig sowohl im geschäftlichen als auch im privaten Bereich zum Teilen von vertraulichen Daten genutzt. Diese Betroffenheit Dritter steigert die Eingriffsintensität erheblich. Zur Wahrung der Verhältnismäßigkeit ist ein Eingriff über die Voraussetzungen des Abs. 1 hinaus zumindest **auf erhebliche Gefahren zu begrenzen**.[45]

- Der Gesetzentwurf gibt vor, sich bei der Erweiterung der Durchsuchungsbefugnisse an § 110 Abs. 3 StPO zu orientieren.[46] Dabei wird zunächst unterschlagen, dass diese strafprozessuale Durchsuchung nur auf Anordnung der Staatsanwaltschaft erfolgen darf. Dies entspräche im Polizeigesetz in

---

42 Vgl. Supreme Court of the United States, RILEY v. CALIFORNIA, No. 13–132. Argued April 29, 2014 — Decided June 25, 2014 =573 U.S. 373; dazu *Kreissl*, Einige soziologische Befunde zu Überwachungstechnologien im Ermittlungsverfahren, in: Barton/Kölbel/Lindemann (Hrsg.), Wider die wildwüchsige Entwicklung des Ermittlungsverfahrens, 2015, 355 (361f.)

43 LT-Drs. 7/3694, S. 258.

44 Vgl. *Hermann/Soiné*, NJW 2011, 2922 (2923), *Singelnstein*, NStZ 2012, 593 (594), *Graulich*, in: Arndt/Fetzer/Scherer/Graulich, TKG, 2. Aufl. 2015, § 88 Rn. 6. Der Schutz des IT-Grundrechts besteht unabhängig davon, wie leicht darauf zugegriffen werden kann, vgl. BVerfGE 120, 274 (315). Es ist also für die Schwere des Eingriffs unerheblich, wenn der Zugang auf die Cloud-Daten nur deshalb leicht ist, weil die betroffene Person das Passwort im Handy gespeichert hat und dieses wiederum über keinen wirksamen Passwortschutz verfügt.

45 Vgl. *Bayer. Datenschutzbeauftragter*, Stellungnahme zu BayPAG, 21.12. 2017, S. 10.

46 LT-Drs. 7/3694, S. 258; der Sache nach dürfte das Vorbild aber eher Art. 22 BayPAG sein, das bisher als einziges Landespolizeigesetz eine entsprechende Befugnis zur Cloud-Durchsuchung enthält.

etwa, wenn sie von der Behördenleitung angeordnet werden müsste. Viel gewichtiger ist aber, dass die StPO-Regelung für Sichtungen von Daten eingeführt wurde, die im Rahmen einer Wohnraumdurchsuchung erhoben werden. Für die Gesamtmaßnahme müssen also schon erhebliche materielle Voraussetzungen erfüllt sein und zudem regelmäßig eine gerichtliche Anordnung vorliegen.[47] Die Durchsuchung der Cloud im Rahmen des § 57 ist dagegen nicht nur "Beifang" einer Wohnungsdurchsuchung, sondern stellt einen eigenen Grundrechtseingriff dar. Dementsprechend ist schon **für diesen Zugriff auf die Daten eine gerichtliche Anordnung erforderlich**.[48]

- In § 61 Abs. 1 S. 4 ist für die "Sicherstellung" der Cloud-Daten eine gerichtliche Entscheidung unverzüglich nachzuholen. Dies orientiert sich zwar an den genannten strafprozessualen Regelungen, verkennt aber die gewichtigen Unterschiede. Auch hier ist eine *vorherige* gerichtliche Entscheidung zu fordern.

- Schließlich ist auch der **Kernbereichs- und Berufsgeheimnisschutz unzureichend**. Dieser wird lediglich im Rahmen der Sicherstellung in § 61 Abs. 1 S. 5 erwähnt, jedoch betrifft er nur die Verarbeitung bereits erhobener Daten. Es wird überhaupt nicht beachtet, dass er schon bei der Durchsuchung gem. § 57 Abs. 2 zu berücksichtigen ist, gerade weil die Betroffenen durch eine Änderung des § 58 Abs. 1 kein Anwesenheitsrecht mehr haben. Auch hier zeigt sich, dass es sich bei der Cloud-Durchsuchung der Sache nach um eine Datenerhebungsbefugnis handelt, bei der der Kernbereichs- und Berufsgeheimnisschutz vollumfänglich anzuwenden ist.

3. Videoüberwachung im öffentlichen Raum

Das SOG M-V enthält bereits verschiedene Befugnisse zur offenen Videoüberwachung (genauer: Bild- und Tonaufnahmen sowie -aufzeichnungen), die mit dem neuen Entwurf punktuell erweitert werden. Neben grundsätzlicher Kritik sehen wir verschiedene Einzelaspekte besonders kritisch:

a. Grundsätzliche Kritik an Videoüberwachung im öffentlichen Raum

Grundsätzlich kann festgestellt werden, dass Videos des Tatgeschehens die Aufklärung durch die Strafverfolgungsbehörden vereinfachen und effizienter machen. Dieser Faktor ist allerdings auf der repressiven Seite der polizeilichen Maßnahmen verortet. Studien zur präventiven Wirkung von Videoüberwachung zeigen dagegen ambivalente Ergebnisse. Bei Deliktstypen (etwa Eigentums- und Drogendelikte) führt die Videoüberwachung wohl eher zur Verlagerung der Taten, während etwa Affekttaten (insbesondere Gewaltdelikte) durch Kameras nicht verhindert werden.[49] Bei der Betrachtung der präventiven Aspekte ist vor allem der „Chilling-Effekt“ hervorzuheben. Dieser beschreibt den Prozess, bei dem ein*e Bürger*in allein durch die Möglichkeit der Sanktionierung seines*ihres Verhaltens eine Selbsteinschränkung vornimmt. Dieser Abschreckungseffekt kann dazu führen, dass von Grundrechten nicht Gebrauch gemacht wird, weil die Angst vor negativen Konsequenzen, nicht ausschließlich staatlichen Ursprungs, zu groß ist.[50] Das stellt besondere Anforderungen an die Verhältnismäßigkeit dieses vorgelagerten Grundrechtseingriffs.

---

47 Vgl. BGHSt 44, 265 (273), *Hermann/Soiné*, NJW 2011, 2922 (2923), vgl. für Emails BVerfGE 124, 43 (67)

48 Vgl. *Graulich*, Stellungnahme zu BayPAG, 14.03.2018, S. 15, Bayer. Datenschutzbeauftragter, Stellungnahme zu BayPAG, 21.12. 2017, S. 11; ebenso in den USA Supreme Court of the United States, RILEY v. CALIFORNIA, No. 13–132. Argued April 29, 2014 — Decided June 25, 2014 = 573 U.S. 373.

49 Vgl. *Petri*, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, G Rn. 773.

50 Vgl. *Petri*, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, G Rn. 763; BVerfGE 65, 1 (42f.).

b. Überwachung von öffentlichen Veranstaltungen oder Ansammlungen sowie im übrigen öffentlichen Raum

- Die Neustrukturierung der Normen zur Videoüberwachung in Abs. 1-3 geben Anlass, sie einer kritischen Prüfung zu unterziehen. § 32 Absatz 1 Nr. 1 soll es den Ordnungsbehörden ermöglichen, Aufzeichnungen von Verhaltens- und Zustandsstörern in Bild und Ton anzufertigen, wenn Tatsachen die Annahme rechtfertigen, dass dabei Straftaten begangen werden. Problematisch erscheint hieran die niedrige Schwelle der nicht weiter konkretisierten Straftat, sowie das Ausreichen der tatsachenbasierten Annahme. Für ortsgebundene Kameras im öffentlichen Raum gem. Abs. 2 reicht sogar die Erwartung irgendeines schädigenden Ereignisses aus, das damit sogar unterhalb der Schwelle von Ordnungswidrigkeiten liegen kann. So bleibt jedenfalls unklar, ob auch für **Bagatelldelikte** ein Kameraeinsatz in Frage käme, wobei an der **Verhältnismäßigkeit dieser Maßnahme** gezweifelt wird. Denn die verdachtsunabhängige Videoüberwachung im öffentlichen Raum stellt für die Betroffenen nicht nur einen erheblichen Grundrechtseingriff dar, sondern bringt auch weitere soziale Folgen mit sich (Chilling-Effekt). Das Bundesverfassungsgericht verlangt für derartige Informationserhebungen, die eine unbestimmte Vielzahl an Leuten erfassen, die dazu keinerlei Anlass gegeben haben, dass sie dem Schutz eines Rechtsguts von erheblichem Gewicht dienen muss.[51] Die nicht nur punktuelle Videoüberwachung ist daher in Abs. 1-3 **auf Straftaten erheblichen Gewichts zu begrenzen**.[52]

- In Abs. 1 Nr. 2 sollen Bildaufnahmen zwecks **Übersichtsaufnahmen zur Lenkung und Leitung der Einsätze** neu eingeführt werden. Dabei ist schon unklar, was unter der Voraussetzung „erforderlich zur Lenkung und Leitung des Einsatzes“ bedeuten soll. Es ist **nicht ersichtlich**, dass diese Formulierung die Einsatzmöglichkeiten **in irgendeiner Weise beschränkt**.[53] Besonders problematisch scheint dabei auch die Tatsache, dass die Bilder so hochauflösend angefertigt werden, dass Einzelpersonen unproblematisch identifiziert werden können. So macht es aus datenschutzrechtlicher Sicht keinen Unterschied, ob es sich lediglich um eine Übersichtsaufnahme oder um eine gezielte Gruppenaufnahme handelt. Schon die Möglichkeit der Identifizierung – deren (Nicht-)Vornahme für Betroffene nicht ersichtlich ist –, stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar.[54] Stattdessen sollte auch für Übersichtsaufnahmen an der **Voraussetzung einer konkreten Gefahr festgehalten werden**. Da lediglich punktuelle und nicht auf Einzelpersonen zielende Aufnahmen eine eher geringe Eingriffsintensität haben, gelten aufgrund der polizeirechtlichen Je-desto-Formel auch nur moderate Anforderungen.[55]

- Insbesondere für die ortsgebundene Videoüberwachung gem. Abs. 2 und 3 sollten Vorschriften hinzugefügt werden, die **sichtbare Hinweise** auf den Kameraeinsatz (vgl. § 8 Abs. 2 S. 3 PolDVG HH) sowie **Prüffristen** für das Vorliegen der Voraussetzungen festschreiben.

c. Bodycams (§ 32a) und Dashcams (§ 32 Abs. 8)

Die Nutzung von Bodycams ist dem SOG nicht im eigentlichen Sinne mit der geplanten Neuregelung hinzugefügt worden. Bis Mitte Februar 2019 wurden schon testweise verschiedene Kameratypen in der Praxis genutzt. Die Ergebnisse dieser Testphase wurden jedoch nicht öffentlich darge-

51 BVerfG, Beschluss vom 18. Dezember 2018 – 1 BvR 142/15 –, Rn. 98f.
52 Vgl. § 21 Abs. 3 PolG BW, dazu VGH Mannheim, NVwZ 2004, 498.
53 So für das BayVersammlG ausdrücklich BVerfGE 122, 342 (368 = Rn. 129).
54 Vgl. *Schenke*, Polizei- und Ordnungsrecht, 10. Aufl. 2018, Rn. 186, BVerfGE 122, 342 (368ff. = Rn. 130, 132)
55 Vgl. *Schenke*, Polizei- und Ordnungsrecht, 10. Aufl. 2018, Rn. 77; wenn die Übersichtsaufnahmen ausdrücklich im Normtext erhalten bleiben sollen, muss als verfassungsrechtliches Minimum normiert werden, in welchen Situationen sie *im Einzelfall* zulässig sind, vgl. VerfGH Berlin, NVwZ-RR 2015, 577 (580).

stellt und es soll nun mit der Neuregelung die Grundlage geschaffen werden, die Cams auch ohne Auswertung der Testphase nutzen zu können. So erscheint es fragwürdig, an Bodycams in dieser Form festzuhalten. Die Einwände sind grundsätzlich auf die geplante Einführung von Kameras an Fahrzeugen gem. § 32 Abs. 8 (sog. Dashcams) übertragbar. Für diese sollte ebenfalls eine Pre-Recording-Funktion[56] vorgesehen werden.

- Es ist zwar zu begrüßen, dass das Gesetz mit der im Einzelfall bevorstehenden Gefahr für Leib und Leben relativ hohe Voraussetzungen verlangt und vorschreibt, dass die Daten verschlüsselt zu speichern sind. Sowohl durch **Pre-Recording** (§32a Abs. 1) als auch durch die Speicherung wird allerdings massiv in das allgemeine Persönlichkeitsrecht der Betroffenen eingegriffen, gerade weil **auch unbeteiligte Dritte** von Aufnahmemaßnahmen betroffen sein werden. Hinzu kommt, dass insbesondere die präventive Wirkung von Videoüberwachung nicht eindeutig belegt ist, bezüglich gewaltbereiter Personen unter Drogen- und insbesondere Alkoholeinfluss wird – wenn überhaupt – eine provozierende Wirkung angenommen.[57] Insofern sollten die Regelungen in besonderem Maße auf ihre **Verhältnismäßigkeit** hin betrachtet werden und auch an weniger intensiven Alternativregelungen (z.B. aus anderen Bundesländern) gemessen werden.

- Bedenken ergeben sich aus der nicht konkretisierten Anforderung, dass die **Aufzeichnungen offen anzufertigen** sind. Es wäre wünschenswert diesbezüglich einige Klarstellungen in den Entwurf aufzunehmen, wie Außenstehenden die Aufzeichnungssituation erkenntlich gemacht wird. Es ist dringend zu empfehlen, wie auch im privaten Bereich, eine **Mitteilungspflicht** in den Gesetzestext aufzunehmen, wie es § 15c S. 2 PolG NRW vorsieht. Dieser könnte in der Praxis durch Verteilen von Kontaktkarten an die gefilmten Personen oder durch eine leicht erkennbare „Warnweste“ mit einer geeigneten Aufschrift nachgekommen werden. Diese Überlegungen zur Mitteilungspflicht sollten auch in Mecklenburg-Vorpommern Gehör finden, um den unklaren Begriff der „offenen Aufzeichnung“ zu konkretisieren.

- Bezüglich der Speicherung ist auf die in § 46h Abs. 1 SOG MV festgehaltenen Grundsätze hinzuweisen, die u.a. verlangen, die Aufzeichnungen von Unbeteiligten zu **anonymisieren**. Die erforderliche Verpixelung kann nach derzeitigem Stand der Technik nicht durch eine Software, sondern nur manuell durchgeführt werden. Dies stellt jedoch nicht nur fachliche Anforderungen an die durchführende Person, sondern führt ebenso dazu, dass sie die unverpixelten Aufnahmen zumindest wahrnimmt. Um einen möglichst hohen Grad der Anonymisierung und an fachlicher Expertise zu erreichen, sollte die Verarbeitung der Aufnahmen einzig eine **Datentreuhandstelle** übernehmen.[58] So kann auch gewährleistet werden, dass die Daten neben dem Schutz der Einsatzkräfte auch dem Schutz der Betroffenen dienen.

- Das Speichern wird bei der Pre-Recording-Funktion erst auf Knopfdruck der Einsatzkraft aktiviert. Um sicherzustellen, dass dies nicht nur von deren Wohlwollen abhängt, sollte das Recht der Gefilmten festgeschrieben werden, die Speicherung der Aufnahmen zu verlangen, vgl. § 27a IV 2 Nr. 3 BPolG. Dies sollte durch das Recht ergänzt werden, diese bei der Überprüfung der Rechtmä-

---

[56] Im Pre-Recording-Modus zeichnet die Kamera durchgängig Bild und Ton auf und lädt die Daten in den Zwischenspeicher. Diese Daten werden fortlaufend mit neuen überschrieben, sofern nicht die endgültige Speicherung durch die tragende Person veranlasst wird.

[57] Vgl. *Roggan*, Stellungnahme zum Brandenburgischen Polizeigesetz vom 03.01.2019, S.22; *Seckelmann*, Body-Cams als „New Tools of Governance“, in: von Lucke/Lenk (Hrsg,), Festschrift für Heinrich Reinermann, 2017, 291 (299), *Scharlau*, Stellungnahme zur Einführung einer Bodycam im SächsDVG vom 11.03.2019, S. 4f.

[58] Vgl. *Seckelmann*, Body-Cams als „New Tools of Governance“, in: von Lucke/Lenk (Hrsg,), Festschrift für Heinrich Reinermann, 2017, 291 (300).

ßigkeit der Maßnahme auch einzusehen.[59] Zudem sollte eine Aufzeichnungs- und Auswertungspflicht bei Anwendung unmittelbaren Zwangs in Betracht gezogen werden.[60]

d. Drohneneinsatz (§ 34)

In § 34 wird für verschiedenen Formen der Datenerhebung geregelt, dass diese auch mittels sog. Drohnen erfolgen dürfen. Laut Gesetzesbegründung soll keine Ausweitung der bestehenden Befugnisse erfolgen.[61] Allerdings kann sich aus dem **Drohneneinsatz eine neue Qualität der Maßnahme** ergeben. Denn Drohnen können aufgrund der Flughöhe deutlich mehr Unbeteiligte erfassen und zudem Beobachtungen an Orten ermöglichen, an denen nicht damit zu rechnen ist. Durch die **erhöhte Streubreite** und den **Überraschungseffekt** der Maßnahme sind **gesteigerte Anforderungen** an den Drohneneinsatz in Betracht zu ziehen. Gerade aufgrund der mitunter geringen Größe der eingesetzten Geräte können Betroffene den Einsatz oder zumindest seine*n Urheber*in nicht wahrnehmen. Damit wird bei Maßnahmen gem. § 32 die erforderliche Offenheit der Datenerhebung unterlaufen. Entsprechend der soweit ersichtlich einzigen polizeigesetzlichen Regelung zum Drohneneinsatz in Art. 47 BayPAG ist festzuschreiben, dass durch begleitende Maßnahmen wie Hinweise **die Offenheit der Maßnahme gewahrt** sein muss.

4. Zum Konzept der „drohenden Gefahr“

a. Grundprobleme der Vorverlagerung

Bereits 2018 wurde ein erweiterter Gefahrenbegriff mit der sog. Elektronischen Fußfessel in M-V eingeführt. Gem. § 67a Abs. 1 kann sie die Polizei bereits anordnen, wenn noch kein annähernd konkretes Geschehen absehbar ist, es aber in groben Zügen in einem überschaubaren Zeitraum erwartet wird oder das individuelle Verhalten von Personen eine solche Wahrscheinlichkeit begründen soll. Es handelt sich nahezu im Wortlaut um die Definition, die das Bundesverfassungsgericht für die „drohende Gefahr“ verwendet.[62] Neu ist, dass im Gesetzesentwurf nun zahlreiche schwerwiegende Eingriffsmaßnahmen mit § 67a Abs. 1 verbunden werden sollen (vgl. §§ 33-33d, 35, 44, 52b i.V.m. § 67a I). Im Vordergrund steht der Bereich der Vorfeldgefahren: Es geht speziell um Situationen, in denen sich das wahrscheinliche Schadensereignis noch nicht konkret bestimmen lässt.[63] Im Unterschied zu den bisherigen Gefahrenbegriffen liegt der **Fokus nicht mehr** überwiegend **auf dem** möglicherweise eintretenden **Schaden**.[64] An einigen Stellen wird auch von einer ***„personifizierten Gefahr“***[65] oder ***"Gefahr einer Gefahr"***[66] gesprochen. Grundrechtsintensive Befugnisse wie die Online-Durchsuchung (§ 33c) oder die Quellen-TKÜ (§ 33d Abs. 2) sollen bereits anwendbar sein, wenn allein das Verhalten von Personen als allgemein gefährlich eingestuft wird. Auch das Betreten und Durchsuchen von Räumlichkeiten – wie der Wohnung – sowie das Durchsuchen von Sachen werden zur Durchführung beider Maßnahmen möglich sein. Wie sich aber ein gefährliches Verhalten bestimmen lässt oder welche Parameter für ein solches Verhalten sprechen, wird aus dem

59 Vgl. *Scharlau*, Stellungnahme zur Einführung einer Bodycam im SächsDVG vom 11.03.2019, S. 10.
60 Vgl. *Scharlau*, Stellungnahme zur Einführung einer Bodycam im SächsDVG vom 11.03.2019, S. 8.
61 LT-Drs. 7/3694, S. 190f.
62 Vgl. BVerfGE 141, 220 (272f. = Rn. 112). Da sich diese Eingriffsschwelle gem. § 67a Abs. 1 nur auf terroristische Straftaten i.S.d. § 67a bezieht, kann auch von einer "drohenden terroristischen Gefahr" gesprochen werden.
63 Vgl. dazu BVerfGE 141, 220 (272f. = Rn. 112).
64 *Austermann/Schlichte,* Gefährliche Begriffe?! Über „Gefährder“ und drohende Gefahren, KJ 2018, 479 (481f.); *Leisner-Egensberger,* Polizeirecht im Umbruch: Die drohende Gefahr, DÖV 2018, 677 (680).
65 Vgl. dazu *Austermann/Schlichte,* KJ 2018, 479 (481f., 487ff.); *Kuch,* Gefährder in Haft? Kritische Anmerkungen zu einem bayerischen Experiment, DVBl. 2018, 343 (347).
66 *Deutscher Anwaltsverein*, Stellungnahme Nr. 54/2018 zum Brandenburgischen Polizeigesetz, November 2018, S. 8f.

Gesetzesentwurf nicht ersichtlich.

- Diese Punkte **begünstigen** eine **fehlerhafte Praxis**. Je weiter eine Maßnahme im Vorfeld von Gefahren angesiedelt ist, desto wahrscheinlicher werden gegen Betroffene Maßnahmen angeordnet, die auf einer Fehleinschätzung beruhen, schwer in ihre Intimsphäre eingreifen und deren Folgen in den meisten Fällen nicht mehr rückgängig zu machen sind. Dazu kommt, dass auch die Formulierung „*innerhalb eines überschaubaren Zeitraums*“ **zu unbestimmt** sein dürfte und einen weiteren Faktor für eine fehleranfällige Praxis darstellt. Was damit gemeint ist – wie viele Tage, Wochen, Monate usw. –, wird nicht ersichtlich.[67] Dies dürfte auch hinter den Anforderungen von Art. 6 lit. a JI-Richtlinie liegen, der zumindest eine Straftat in "naher Zukunft“ fordert.[68] Umso mehr Bedenken bestehen, wenn Maßnahmen wie die Online-Durchsuchung an dieses Konzept geknüpft werden. Bereits die jetzigen Gefahrenbegriffe im Polizeirecht sind von Unsicherheiten gekennzeichnet, da auch sie an eine Gefahrenprognose geknüpft sind.[69] Die „drohende Gefahr“ begibt sich aber in einen noch unsichereren Bereich. Fragwürdig ist, wie grundrechtlicher Schutz nachhaltig gewährleistet werden soll, wenn bestimmte Maßnahmen aufgrund von Risikohypothesen angeordnet werden können, die in einer späteren gerichtlichen Auseinandersetzung für die Richter*innen kaum bis gar nicht nachvollziehbar sein können.

- Zugleich kann die Verbindung schwerwiegender Maßnahmen mit der „drohenden Gefahr“ **mittelbar negative gesellschaftliche Folgen** nach sich ziehen. Die Abkehr von den bisherigen Gefahrenbegriffen schafft falsche Anreize: Bürger*innen könnten versuchen, sich konform zu verhalten, um keine „allgemeine Gefährlichkeit“ aufzuweisen.[70] Für sie wird nicht nachvollziehbar sein, wann ihr Verhalten „gefährlich“ sein soll.[71]

b. Geschützte Rechtsgüter und Zielrichtung der Befugnisse

Zu weitgehend und damit verfassungswidrig ist die Konzeption der drohenden terroristischen Gefahr hinsichtlich des Katalogs der terroristischen Straftaten in § 67c, auf die sie sich beziehen kann. Denn dieser umfasst zahlreiche Tatbestände der **Vorfeldkriminalität**. So zählt bspw. bereits die Finanzierung terroristischer Aktivitäten (§ 89c StGB) oder die Unterstützung einer terroristischen Vereinigung (§ 129a Abs. 5 StGB) als terroristische Straftat. Das Bundesverfassungsgericht lässt die drohende Gefahr ausreichen, wenn der Eintritt eines bestimmten Schadens ungewiss ist. Doch bei den genannten Straftatbestände muss überhaupt kein Schaden vorliegen, es reicht ebenso die abstrakte Gefährlichkeit. Die Kombination von § 67a mit § 67c hat dadurch zur Folge, dass eine Person heimlich überwacht werden darf, wenn die grob umrissene Möglichkeit besteht, sie könnte eine Terrororganisation unterstützen. Der **Bezug zum abzuwehrenden Schaden ist in noch weitere Ferne gerückt**.[72] Zugespitzt reichte dann die "Gefahr einer Gefahr einer Gefahr". Wegen erheblicher verfassungsrechtlicher Bedenken gegen solch eine noch weitere Vorverlagerung der Eingriffsbefugnisse wurden in Nordrhein-Westfalen und Niedersachsen entsprechende Straftaten aus dem Katalog gestrichen.[73] In Mecklenburg-Vorpommern sollte das Gleiche geschehen.

---

67 Vgl. *Gazeas*, Stellungnahme zur Änderung des Polizeigesetzes NRW, Juni 2018, S. 11f.

68 Vgl. *Petri*, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, G Rn. 627.

69 *Hanschmann,* „Gefährder“ – eine neue alte Figur im Öffentlichen Recht, KJ 2017, 434 (439).

70 Die sogenannten „Chilling Effects“, vgl. dazu *Digitalcourage*, Stellungnahme zur Änderung des Polizeigesetzes NRW, 9.11.2018, S. 8f.

71 Vgl. *Scharlau*, Stellungnahme von Amnesty International zur Änderung des Polizeigesetzes NRW, 31.05.2018, S. 23f.

72 Vgl. *Gazeas*, Stellungnahme zur Änderung des Polizeigesetzes NRW, 08.11.2018, S. 6f.

73 Vgl. die Synopse zu NPOG, https://wiki.freiheitsfoo.de/uploads/Main/20190802-Synopse-NdsSOG-NPOG-4spaltig.pdf, S. 5 (13.08.2019).

- Schließlich ist zu kritisieren, dass die Eingriffsschwelle der drohenden terroristischen Gefahr sich nicht auf aufklärende Maßnahmen beschränkt. Im Polizeirecht dienen Befugnisse im Gefahrenvorfeld dazu, **lediglich weitere Informationen zu beschaffen**, durch die eine verlässliche Gefahrenprognose ermöglicht wird. Ist die Polizei unsicher, ob eine konkrete Gefahr vorliegt, darf sie etwa durch offene Befragungen oder bei erheblichen Gefahren etwa auch durch verdeckte Observationen ermitteln, ob eine Gefahr vorliegt. Auch das Bundesverfassungsgericht bezieht sich in seinen Ausführungen zur drohenden Gefahr nur auf Überwachungsmaßnahmen.[74] Nicht zulässig sind dagegen Maßnahmen, die auf eine Abwehr der Gefahr abzielen, ohne dass Klarheit herrscht, ob sie überhaupt vorliegt.[75] Eine solche **Maßnahme mit sanktionierendem Charakter** ist etwa die Meldeauflage in § 52b. Hier sollte der Verweis auf § 67a Abs. 2 gestrichen werden.

5. Überwachung von Unbeteiligten

a. Grundprobleme der Umfeldüberwachung

Nach allgemeinen Prinzipien des Polizeirechts dürfen sich Maßnahmen grundsätzlich nur gegen diejenigen richten, die für eine Gefahr verantwortlich sind, gegen Dritte dagegen nur unter den strengen Voraussetzungen des sog. polizeilichen Notstands, was den Regelungen der §§ 68ff entspricht. Diese werden im vorliegenden Entwurf jedoch an zahlreichen Stellen aufgeweicht und **Unbeteiligte** damit **häufiger zum Ziel** gerade auch **verdeckter Überwachungsmaßnahmen**. Eine solche Entwicklung ist **insgesamt kritisch zu betrachten und besonders restriktiv einzugrenzen**, da diese Maßnahmen eine enorme Streuwirkung besitzen und somit einen besonders schweren Grundrechtseingriff darstellen.

Schon beim Abhören einer Zielperson wird nicht nur registriert, was diese ihrem*ihrer Partner*in berichtet, sondern auch umgekehrt. Wird aber neben der eigentlichen Zielperson auch die Schwester, der Arbeitskollege oder eine andere Kontaktperson abgehört, findet gleichzeitig auch eine **Erfassung deren privaten Umfeldes** statt. Dadurch entsteht ein **Schneeballeffekt**. Zwar sind Maßnahmen gegen das Umfeld von Verdächtigen schon bisher gängige Praxis. Die entsprechenden Normen wurden jedoch vom Bundesverfassungsgericht als zu weitgehend eingestuft[76], weshalb auch im SOG M-V Anpassungen vorgenommen werden müssen. Wenn sich nun um eine bestimmtere Regelung der Umfeldüberwachung bemüht wird, ist das zwar grundsätzlich zu begrüßen. In verschiedenen Punkten sind die Regelungen aber immer noch zu weitgehend und damit unverhältnismäßig. Im Übrigen ist darauf hinzuweisen, dass es auch hier nicht darum gehen sollte, verfassungsrechtliche Minimalstandards einzuhalten. Vielmehr sollten die negativen Folgen der Überwachung von Unbeteiligten verstärkt in den Blick genommen und die Befugnisse deshalb noch weiter begrenzt werden.

b. Begrenzung auf den Anlass der Überwachung

Datenerhebungen im Umfeld von Verdächtigen dienen oftmals dem **Ziel, ein bestimmtes Milieu auszuforschen**, wenn gegen die Zielperson nicht genügend Handfestes vorliegt, aber die Vermutung besteht, dass sich in deren Umfeld "schon irgendetwas finden lässt". Wenn einmal eine entsprechende Hypothese im Raum steht, kann sich dieses Vorgehen verselbstständigen. Dies haben etwa die Ermittlungen in Folge der Morde des Nationalsozialistischen Untergrunds (NSU) gezeigt, die bis zur Selbstenttarnung des NSU vornehmlich gegen die Angehörigen und das Umfeld der Op-

---

74 Vgl. BVerfGE 141, 220 (272f. = Rn. 112).

75 Vgl. *Löffelmann*, Stellungnahme zum Gesetz zur effektiveren Überwachung gefährlicher Personen vom 17.05.2017, S. 6f.

76 Vgl. BVerfGE 113, 348 (380f. = Rn. 130ff.)

fer gerichtet waren und sich auf das Konzept der Kontakt- und Begleitpersonen stützten. Allenfalls bei niedrigschwelligen Maßnahmen ist es der Polizei gestattet, erst durch Ermittlungen gegen Unbeteiligte neue Ermittlungsansätze zu gewinnen. Bei intensiven, insbesondere heimlichen Maßnahmen ist die **Überwachung strikt auf den auslösenden Anlass** zu begrenzen. Das gilt bei präventiven Ermittlungen zur Verhinderung von Straftaten noch stärker als bei der Aufklärung bereits begangener Taten.[77] Vor diesem Hintergrund begegnen insbesondere die Generalermächtigung zur Überwachung von Kontakt- und Begleitpersonen gem. § 27 Abs. 3 Nr. 2, aber auch einzelne Aspekte der §§ 33ff. erheblichen Bedenken.

- Die Datenerhebungen bei Unbeteiligten[78] sind auf diejenigen Kommunikationsvorgänge zu begrenzen, die sich **allein auf die Gefahr beziehen, die Anlass für die Überwachung war** und einen Bezug zur Zielperson hat. **Daten, die keinen Bezug zum Anlass der Maßnahme haben, sind unverzüglich zu löschen.**

Bsp.: Die verdächtige Zielperson benutzt regelmäßig den Telefonanschluss ihrer Nachbarin. Diese berichtet ihrer Freundin von ihrem letzten Familienurlaub. Dieses aufgezeichnete Gespräch ist unverzüglich zu löschen.

Dies ist nicht nur rechtspolitisch geboten, um Anreize für eine unzulässige Milieuerforschung zu vermeiden. Auch verfassungsrechtlich ist dies zwingend. Denn im Gefahrenvorfeld ist die Umfeldüberwachung eine zu rechtfertigende Ausnahme, die daher schon im Tatbestand auf das unbedingt Nötige zu begrenzen ist.[79] Die allgemeinen Prüf- und Löschvorgaben gem. §§ 45, 45a reichen hierzu nicht aus, da sie u.U. erst Jahre später zur Löschung von Daten führen, die mit einer prognostizierten Tat und der verdächtigen Person nichts zu tun haben. Nur so wird die eingangs erwähnte Streuwirkung, die schon durch die bloße erstmalige Erfassung entsteht, einigermaßen begrenzt werden. Ein Bedürfnis für die Speicherung von Daten, die nichts mit einer Gefahr zu tun haben, ist nicht ersichtlich. Schließlich greifen die geforderten Einschränkungen schon nicht, wenn sich bei der Überwachung von Unbeteiligten ein Bezug zum Anlass der Maßnahme ergibt. Im Übrigen dürfte die Speicherung dieser Daten auch nicht durch Informations-, Dokumentations- und Protokollierungspflichten geboten sein. Denn diese beziehen sich regelmäßig nur auf äußere Umstände der Überwachung, nicht auf ihren Inhalt.[80]

Vorschlag: Die beiden eingangs dieses Absatzes formulierten Sätze werden in § 27 Abs. 3 sowie §§ 33b-d im Bezug auf Daten der jeweils betroffenen Unbeteiligten eingefügt.[81] *Es bietet sich auch eine Orientierung an § 26a Abs. 2 an.*

- Einen Ansatz dieser Einschränkung gibt es bereits in § 33a Abs. 4. Doch es ist nicht ersichtlich, weshalb **Daten, die ausschließlich einen Bezug zu Unbeteiligten** gem. § 33 Abs. 4 oder **Berufsgeheimnisträger*innen** gem. § 26b haben, nicht **unverzüglich zu löschen** sind. Die in der Begrün-

---

77 Vgl. eingehend *Bäcker*, Kriminalpräventionsrecht, 2015, 95f., 102., 145, in diese Richtung auch BVerfGE 141, 220 (273ff. = Rn. 115f.).

78 Seien es Kontakt- und Begleitpersonen i.S.d § 27 Abs. 3 Nr. 2, Inhaber*innen von Wohnungen, in denen sich die Zielperson aufhalten könnte, bzw. von Geräten, die für die Kommunikation der Zielperson genutzt werden, gem. §§ 33b Abs. 2, 33c Abs. 1 S. 4, 33d Abs. 1 S. 1 Nr. 3 und 4.

79 Vgl. *Bäcker*, Kriminalpräventionsrecht, 2015, 145f.

80 Selbst § 46f Abs. 1 Nr. 3, der die Protokollierung von Daten vorschreibt, die zur Feststellung der erhobenen Daten erforderlich ist, bezieht sich nicht auf deren Inhalt, sondern ausweislich der Gesetzesbegründung auf Metadaten, vgl. LT-Drs. 7/3694, S. 285.

81 Zur Klarstellung, dass dies keine datenschutzrechtlichen Belange unterlaufen darf, kann der Halbsatz "soweit nicht Informations-, Dokumentations- und Protokollierungspflichten gem. §§ 46-46f. entgegenstehen" hinzugefügt werden.

dung genannten Normen lassen keinen Anwendungsbereich erkennen.[82] Ein solcher ist allenfalls für die äußeren Umstände, nicht jedoch für den Inhalt der Datenerhebung ersichtlich. Das im vorigen Absatz Gesagte ist hierauf übertragbar.

c. Anforderungen an die Eingriffsschwelle

- Die **Eingriffsschwelle** für die Umfeldüberwachung gem. § 27 Abs. 3 Nr. 2 ist **zu niedrig angesetzt**. Diese bezieht sich auf Straftaten von erheblicher Bedeutung (§ 49) und terroristische Straftaten (§ 67c). Das Bundesverfassungsgericht sieht die Rechtfertigung der Inanspruchnahme von Kontakt- und Begleitpersonen darin, dass sie für "überragend wichtige Gemeinwohlinteressen" erfolgt.[83] Der Straftatenkatalog des § 49 umfasst aber auch Taten wie einfachen Raub gem. § 249 StGB, der in M-V mehr als 500 Mal jährlich registriert wird, Meineid gem. § 154 StGB, Propagandadelikte gem. § 86a StGB und sog. **Vorfeldtatbestände**, die Vorbereitungshandlungen weit im Vorfeld konkreter Gefahren unter Strafe stellen. Eine solch weite Fassung, die sich **hinsichtlich Schwere und zeitlicher Nähe von besonders schweren Straftaten entfernt**, ist als **unverhältnismäßig** und daher verfassungswidrig einzustufen.

- Gleiches gilt auch für die **Verknüpfung** des § 27 Abs. 3 Nr. 2 **mit drohenden terroristischen Gefahren** i.S.d. § 67a, bei den besonderen Mitteln der Datenerhebung in § 33 Abs. 2 S. 3 sowie bei gezielter Kontrolle und polizeilicher Beobachtung in § 35 Abs. 1 S. 1 und 2. Wenn beim sog. Gefährder keine hinreichenden Anhaltspunkte vorliegen, die eine konkrete Gefahr begründen, mag das für das Bundesverfassungsgericht ausreichen, um etwa V-Personen oder Peilsender auf ihn anzusetzen, nicht aber auf Personen aus seinem Umfeld. Im Übrigen fällt es schon **logisch schwer, sich Fälle vorzustellen**, in denen noch keine konkretisierte Straftat absehbar ist, die Polizei aber davon ausgeht, dass Kontaktpersonen Kenntnis von dieser (welcher?) Straftat haben, sie daraus Vorteile ziehen oder unwissentlich dafür eingesetzt werden – genau das sind aber die Voraussetzungen des § 27 Abs. 3 Nr. 2a-c.

6. Unabhängige Kontrolle der Polizei

Der Zuwachs an Ermittlungs- und Eingriffsbefugnissen der Polizei erfordert es, gleichzeitig für wirksame Mechanismen zu sorgen, die die Einhaltung dieser Kompetenzen kontrollieren und Fehlverhalten aufklären und abstellen. Dem rechtsstaatlichen Grundsatz der Gewaltenteilung folgend, ist dies klassischerweise Aufgabe der Gerichte. Doch nachträglicher gerichtlicher Rechtsschutz dauert oftmals mehrere Jahre und bindet große finanzielle und personelle Ressourcen. Dass intensive Überwachungsmaßnahmen oftmals unter dem Vorbehalt gerichtlicher Anordnung stehen, ist zwar ein wichtiges Mittel, um rechtswidrige Polizeimaßnahmen zu verhindern, stößt in der Praxis aber an verschiedenen Stellen an Grenzen.[84] Das Gewaltenteilungsprinzip kennt aber auch weitere Einrichtungen der *checks & balances*. In diesem Zusammenhang soll zunächst ein Überblick über Bedarf und Formen von unabhängigen Kontrollinstanzen für die Polizeibehörden gegeben werden (a.). Danach soll als wichtige und einfach umzusetzende Lösung eine unabhängige Beschwerdestelle genauer beschrieben werden (b.), ehe auf spezielle Kontrollmechanismen im Bereich des Datenschutzes eingegangen wird, die bereits im SOG angelegt sind (c.).

---

82 LT-Drs. 7/3694, S. 176.

83 BVerfGE 141, 220 (293 = Rn. 169).

84 Vgl. *Gusy*, Zukunft der Richtervorbehalte, in: Barton/Kölbel, Lindemann, Wider die wildwüchsige Entwicklung des Ermittlungsverfahrens, 2015, 195 (197ff.).

a. Unabhängige Kontrollinstanzen für die Polizeibehörden in Mecklenburg-Vorpommern

aa. Notwendigkeit einer unabhängigen Beschwerdestelle

Schon seit vielen Jahren empfehlen internationale Menschenrechtsorganisationen der Bundesrepublik Deutschland, Beschwerdestellen einzurichten, die mutmaßliche Menschenrechtsverletzungen durch die Polizei zum Gegenstand ihrer Arbeit machen.[85] Auch der Europäische Gerichtshof für Menschenrechte (EGMR) hat in diversen Urteilen in den letzten Jahrzehnten eine klare Linie entwickelt, welche Bedingungen bei Beschwerden bzw. Ermittlungsverfahren gegen Polizeibeamt*innen erfüllt sein müssen, damit die Aufklärung als unabhängig und rechtsstaatlich ordnungsgemäß durchgeführt gelten kann. Diese Grundsätze basieren auf Artikel 2 (Recht auf Leben) sowie Artikel 3 (Verbot der Folter) der Europäischen Menschenrechtskonvention (EMRK) und sind speziell für Fälle von schweren Verletzungen oder Tod in Obhut der Polizei entwickelt worden. Sie sind aber auch bei niedrigschwelligerem strafbarem oder nicht-strafbarem Fehlverhalten von Polizeibeamt*innen als Aufklärungsempfehlung wichtig und nützlich. Die Grundsätze lauten: Unabhängigkeit, Angemessenheit, Unverzüglichkeit, öffentliche Überprüfung sowie die Einbeziehung der Opfer bzw. Beschwerdeführenden.[86]

bb. Lösungsvorschlag: Polizeibeauftragte*r und Stelle für strafrechtliche Ermittlungen

Für die lange überfällige Umsetzung dieser Grundsätze bietet sich speziell in Mecklenburg-Vorpommern eine zweistufige Lösung an: Erstens sollte eine **unabhängige Beschwerdestelle** für Fehlverhalten von Polizeibeamt*innen eingerichtet werden. In einem zweiten Schritt sollte eine **unabhängige Ermittlungsbehörde** eingerichtet werden, die jedes strafrechtliche Ermittlungsverfahren gegen Polizeibeamt*innen durchführt. Denn strafrechtliche Ermittlungen gegen Polizeibeamt*innen gestalten sich insofern problematisch, als dass Ermittler*innen hier im eigenen kollegialen Umfeld tätig werden müssen, wodurch insbesondere der Grundsatz der Unabhängigkeit verletzt wird. Die jüngsten Meldungen zu mutmaßlichen Strafvereitelungen gegen hochrangige Polizeibedienstete[87] zeigen zudem, wie schwierig Ermittlungen in den aktuellen Strukturen sind. Die geplante Reform des SOG M-V sollte deshalb dazu genutzt werden, dieses Problem zu lösen. Nicht ausreichend ist die Einrichtung eines eigenen Dezernats für interne Ermittlungen oder die Abgabe eines Ermittlungsverfahrens an eine andere Polizeidienststelle. Und auch die Stelle des*der Polizeibeauftragte*n kann dies nicht leisten. Bei dem Verdacht einer Straftat gibt sie das Verfahren an die Staatsanwaltschaft ab. Dieser obliegt sodann gemäß § 160 StPO die Pflicht zur Sachverhaltsaufklärung, die wiederum auf die Ressourcen einer Ermittlungsbehörde angewiesen ist. Für den notwendigen Aufbau dieser Institution können andere europäische Staaten als Vorbild dienen.[88]

b. Beschwerdestelle für polizeiliches Fehlverhalten

Die Möglichkeit der Beschwerde über polizeiliches Fehlverhalten muss ausgebaut und institutionalisiert werden. Dies reicht von nicht-strafbarem Verhalten wie diskriminierenden Äußerungen gegenüber Bürger*innen im Rahmen von Polizeieinsätzen über Verstöße gegen datenschutzrechtliche Bestimmungen bis hin zu schweren Missständen in der Polizei. In der jüngeren Vergangenheit zeig-

85 *Töpfer/Peter,* Unabhängige Polizeibeschwerdestellen. Was kann Deutschland von anderen europäischen Staaten lernen?, 2017, 8.

86 Vgl. *Menschrechtskommissar des Europarats*, Opinion of the Commissioner for Human Rights Concerning Independent and Effective Determination of Complaints against the Police, 2009, S. 3.

87 https://www.nordkurier.de/mecklenburg-vorpommern/neue-ermittlungen-gegen-ranghohe-polizeibeamte-aus-mv-1336411908.html (13.08.2019).

88 *Töpfer/Peter,* Unabhängige Polizeibeschwerdestellen. Was kann Deutschland von anderen europäischen Staaten lernen?, 2017, 13ff.

te sich auch in Mecklenburg-Vorpommern **in diversen Fällen der Bedarf nach einer unabhängigen Kontrollinstanz**. Skandale um einen Polizeibediensteten, der ausgerechnet im Zuge eines Strafverfahrens wegen eines Sexualdeliktes gegenüber einer minderjährigen Zeugin sexuelle Avancen machte, zeigen, genauso wie Verstrickungen von Einsatzkräften in rechtsextreme Zusammenhänge, dass die bisherigen Instanzen nicht ausreichen, um Fehlverhalten jenseits von datenschutz- und strafrechtlichen Fragen entgegenzuwirken. Auch der Bund Deutscher Kriminalbeamter von Mecklenburg-Vorpommern (BDK M-V) fordert inzwischen eine unabhängige Beschwerdestelle.[89]

aa. Unabhängige Beschwerdestellen in anderen Bundesländern

Mittlerweile existieren in einigen Bundesländern (u.a. Baden-Württemberg, Rheinland-Pfalz, Schleswig-Holstein, Nordrhein-Westfalen und Sachsen) sogenannte Landespolizeibeauftragte bzw. zentrale Beschwerdestellen für die Polizei. Allen gemeinsam ist, dass sie für strafrechtliche Ermittlungen gegen Polizeibeamt*innen nicht zuständig sind. (siehe Punkt 6.a.bb.). Sie unterscheiden sich jedoch in ihrer gesetzlichen Verankerung, ihrer strukturellen Einbindung in den Behördenapparat und ihrem konkreten Aufgabenbereich deutlich, weshalb wir im Folgenden die wichtigsten Kernelemente hervorheben möchten.

Dass es für eine solche Beschwerdestelle **Bedarf** gibt, zeigen die **Erfahrungen aus anderen Ländern**, in denen diese für Beschwerden sowohl von Bürger*innen als auch von Polizeibediensteten zuständig sind. Bei der zentralen Beschwerdestelle der sächsischen Polizei gingen seit ihrer Einführung im Jahr 2016 **konstant** gut 200 Beschwerden pro Jahr ein, davon eine einstellige Anzahl von Polizeibediensteten.[90] Bei der Landespolizeibeauftragten in Rheinland-Pfalz zeigt sich ein relativer und absoluter **Zuwachs** von Bürger_innenbeschwerden vom Berichtszeitraum 2015-2016 zu 2017-2018,[91] was wohl auf den ansteigenden **Bekanntheitsgrad** der Institution zurückzuführen ist.

bb. Ausgestaltung, Aufgabenbereich und Kompetenzen

Eine unabhängige Beschwerdestelle sollte auf drei Säulen stehen: **Unabhängigkeit, Weisungsfreiheit** von übergeordneten Behörden (z.B. Innen- oder Justizministerium) sowie **eigene Ermittlungsbefugnisse** zur Erfassung eines Sachverhalts. Als Beispiel für solche eigenen Ermittlungsbefugnisse seien z.B. ein eigenes Akteneinsichtsrecht[92], Zutrittsrechte zu den Dienststellen sowie die Rechte, Zeug*innen verbindlich zu laden oder Einsätze zu begleiten, genannt.

Die konkreten Aufgaben einer solchen Beschwerdestelle wären zum Beispiel: Stärkung des Vertrauens der Bürger*innen in die Arbeit der Polizei, erhöhte Bürger*innennähe in der polizeilichen Arbeit, erhöhte Transparenz der polizeilichen Aufgabenerfüllung und Erkennen von kritikwürdigem oder fehlerhaftem Verhalten oder Handeln der Polizei. Auch in der Ausbildung von Anwärter*innen auf den Polizeidienst sollten exemplarisch Fälle besprochen werden, um eine nachhaltige Veränderung von Missständen zu gewährleisten.

cc. Organisatorisch-struktureller Aufbau

Organisatorisch-strukturell sollte die Beschwerdestelle nicht weisungsgebunden an eine übergeordnete Behörde sein. Ein Abhängigkeitsverhältnis gegenüber einem Ministerium sollte unbedingt vermieden werden. Für die neu zu schaffende Institution könnte sich insofern eine **strukturelle Anbin-**

89 https://www.bdk.de/der-bdk/aktuelles/eine-deutlich-erkennbare-linie-gegen-rechtsextremismus-und-seine-netzwerke-durch-deutschland-ziehen-2013-der-bdk-bundesvorstand-muss-handeln (07.08.2019).
90 Zentralen Beschwerdestelle der sächsichen Polizei, Jahresberichte: 2016, S. 4, 2017 S. 5, 2018 S. 5.
91 Der Beauftragte für die Landespolizei Rheinland-Pfalz, Tätigkeitsberichte: 2015/2016 S. 34, 2017/2018, S. 8;
92 Vgl. § 16 Abs. 4 i.V.m. § 4 Abs. 1 Bürger- und Polizeibeauftragtengesetz Schleswig-Holstein.

dung an den*die Bürgerbeauftrage*n des Landes[93] anbieten, der*die seine*ihre Aufgabe aus Art. 36 der Landesverfassung Mecklenburg-Vorpommerns ableitet und dessen*deren konkrete Ausgestaltung im Petitions- und Bürgerbeauftragtengesetz (PetBüG M-V) geregelt ist. Der*die Bürgerbeauftragte wird vom Landtag gewählt und ist diesem rechenschaftspflichtig. Aus einer solchen Anbindung könnten sich **Synergien** ergeben und der Aufwand der Etablierung einer solchen Stelle würde deutlich reduziert. Dies betrifft einerseits den erforderlichen hohen Bekanntheitsgrad, andererseits Aufgaben wie die Informationspflicht für Betroffene oder Tätigkeitsberichte an den Landtag. Darüber hinaus ist eine **wissenschaftliche Begleitung** der Einführung einer unabhängigen Beschwerdestelle empfehlenswert, um eine fruchtbare Evaluation und Umsetzung der Ziele zu gewährleisten.

dd. Beschwerderecht von Betroffenen

Grundsätzlich muss für Betroffene von polizeilichem Fehlverhalten ein niedrigschwelliger Zugang zu der Beschwerdestelle gewährleistet werden. Hier könnte ebenfalls die Institution des*der Bürgerbeauftragten als Vorbild dienen, der*die gem. § 1 Abs. 1 PetBüG M-V für jede Person **unabhängig von Geschäftsunfähigkeit, Wohnsitz oder Staatsangehörigkeit** zuständig ist. Gerade bei Personen ohne festen Wohnsitz oder nichtdeutschen Staatsangehörigen besteht aus Angst vor Diskriminierungen oder anderweitigen negativen Konsequenzen eine Hemmschwelle, eine Polizeidienststelle aufzusuchen, um eine Beschwerde vorzutragen bzw. Anzeige zu erstatten. Auch Opfern von **Polizeigewalt** kann eine solche Stelle Abhilfe schaffen. Diese berichten vielfach, dass der Gang zur Polizeidienststelle zur Anzeigenerstattung eine außerordentlich hohe Belastung sei. Aber **auch und gerade für Polizeikräfte** kann eine unabhängige Beschwerdestelle hilfreich sein, da das Beschreiten des Dienstwegs oft als unangebracht bzw. unkollegial empfunden wird und sich für die Aufklärung struktureller Missstände nicht eignet.

c. Verbesserungen beim Datenschutz notwendig

Die Polizei hat Zugriff auf eine Vielzahl mitunter sensibler Daten von Bürger*innen. Verschiedene Skandale haben in den letzten Monaten gezeigt, dass damit erhebliche Grundrechtsgefährdungen einhergehen können. Die Datenverarbeitung durch die Polizei ist durch die Betroffenen regelmäßig nicht überprüfbar und Rechtsschutzmöglichkeiten dadurch eingeschränkt. Im Bereich des Datenschutzes ist deshalb eine effektive externe Kontrolle notwendig, um polizeiliches Fehlverhalten zu verhindern und aufzuklären. In Umsetzung der JI-Richtlinie sieht der Gesetzentwurf in dieser Hinsicht viele signifikante Verbesserungen vor, die zu begrüßen sind. Dennoch greifen einige Vorkehrungen für einen wirksamen Datenschutz zu kurz.

- Durch Art. 25 JI-Richtlinie ist zwingend vorgeschrieben, dass verschiedene Vorgänge der Datenverarbeitung protokolliert werden müssen. Dies wird in § 46e umgesetzt. Gerade der Nordkreuz-Skandal verdeutlicht die Notwendigkeit der Protokollierung: Vor Kurzem wurde bekannt, dass vermutlich durch einen Polizisten Adressen und Geburtsdaten von vermeintlichen politischen Gegner*innen, die er aus Behördenbeständen abfragte, an die rechtsextreme Gruppierung gelangten.[94] In Abs. 2 sollte jedoch hinzugefügt werden, dass **alle Modalitäten der Datenverarbeitung** gem. Abs. 1 (also auch Erhebung, Veränderung und Löschung) **möglichst präzise zugeordnet** werden können. Denn auch dahingehend sind Datenmissbrauch und Manipulationen nicht auszuschließen. Weiterhin sollte in § 46e Abs. 4 S. 1 Nr. 5 klargestellt werden, dass Protokollierungen nur für

93 Vorbilder können Rheinland-Pfalz und Schleswig-Holstein sein.
94 https://taz.de/Rechter-Terror-in-Deutschland/!5608261/ (13.08.2019).

die Strafverfolgung, die sich auf den Missbrauch der protokollierten Daten durch Dritte beziehen, verwendet werden dürfen. Denn die Protokollierungen dienen **ausschließlich dem Schutz der Betroffenen**.[95] Schließlich muss die Löschfrist in Abs. 4 S. 2 verlängert werden, da die Protokollierungen weiterhin eine **externe Kontrolle ermöglichen** sollen. Wenn Protokollierungen am Ende des Folgejahres zu löschen sind, kann es sein, dass sie nicht von der turnusmäßig zweijährigen Kontrolle der*des Landesdatenschutzbeauftragten abgedeckt werden. Wenn diese Kontrolle etwa im September erfolgt, sind alle Abfragen von Oktober bis Dezember desselben Jahres nicht mehr kontrollierbar. Dies ist **verfassungs- und europarechtswidrig**.[96] Insbesondere wenn die Protokollierungen keine Daten enthalten, die die Betroffenen belasten, ist nicht einzusehen, warum die Protokollierungen vor den eigentlichen Daten zu löschen sind.[97]

- Auch die Kontrollbefugnisse, die dem*der Landesdatenschutzbeauftragten in § 48b eingeräumt werden, greifen zu kurz. Diese bestehen gem. Abs. 3 im Wesentlichen aus Beanstandungs- und Informationsrechten. Anordnungsbefugnisse sind nur in begrenztem Umfang und unter äußerst strengen Voraussetzungen in Abs. 2 vorgesehen. Dabei verlangt Art. 47 Abs. 2 der JI-Richtlinie *wirksame Abhilfe*befugnisse, die sich von der in § 48b Abs. 1 vorgesehenen "Untersuchung" und der früher geforderten "Einwirkung" unterscheiden. Um bei Datenschutzverstößen effektiv abhelfen zu könne, muss der*die Landesdatenschutzbeauftragte konkrete Schritte anordnen können, wenn er*sie diese nicht selbst vornehmen kann. Ohne wirksame Anordungsbefugnisse ist die Vorschrift daher europarechtswidrig.[98] Die Gesetzesbegründung ist offenkundig von einem Verständnis geprägt, das Eingriffe des*der Landesdatenschutzbeauftragten als Ermittlungshindernisse für die Polizeiarbeit begreift.[99] Eine rechtmäßige Verarbeitung von Daten muss aber **auch im Interesse der Polizei** liegen, da eine fehlerhafte Datenverarbeitung auch die Gefahr fehlerhafter Ermittlungsergebnisse mit sich bringt. Es gibt dagegen keinen Grund anzunehmen, dass der*die Landesdatenschutzbeauftragte bei rechtmäßig erhobenen Daten von den Anordnungsbefugnissen Gebrauch macht.[100] Unabhängig davon liegt der Sinn wirksamer Datenschutzvorschriften im Schutz der Bürger*innen. Er ist essentiell, um das Recht auf informationelle Selbstbestimmung zu gewährleisten.

Weitgehendere Anordnungsbefugnisse des*der Datenschutzbeauftragten sind etwa in Sachsen in § 40 Abs. 2 S. 5 SächsDSUG vorgesehen. Nach diesem Vorbild sollte der*die Datenschutzbeauftragte auch in M-V über Anordnungsbefugnisse verfügen.[101]

---

95 Vgl. *Burghardt/Reinbacher*, BeckOK Datenschutzrecht, § 76 BDSG Rn. 18; *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, Rn. 323; *Piltz*, NVwZ 2018, 696 (700f.).

96 Vgl. BVerfGE 141, 220 (302f., 323 = Rn. 205, 272), *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, § 1 Rn. 324.

97 Vgl. BVerfGE 141, 220 (302f. = Rn. 205), *Burghardt/Reinbacher*, BeckOK Datenschutzrecht, § 76 BDSG Rn. 19.

98 So für § 16 BDSG auch *Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, G Rn. 1167, *Thiel*, in: Gola/Heckmann, Bundesdatenschutzgesetz, 13. Auflage 2019, § 16 Rn. 8; *Körffer*, in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, § 16 BDSG Rn. 3; *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, Rn. 116f.; ausführlich *Schulze Lohoff/Bange*, Die (fehlenden) Abhilfebefugnisse des BfDI nach § 16 Abs. 2 BDSG, ZD 2019, 199.

99 1. Vgl. LT-Drs. 7/3694, S. 236f. Dies kommt etwa auch im Verweis auf Erwägungsgrund 82 der JI-Richtlinie zum Ausdruck, welcher vorschreibt, dass die Befugnisse der/des Datenschutzbeauftragten die Vorschriften des Strafverfahrens nicht berühren sollen. Damit ist jedoch nicht gemeint, dass keine Änderung bzgl. der Datenverarbeitung angeordnet werden darf, weil zur präventiven Gefahrenabwehr erhobene Daten sich potentiell auf ein Strafverfahren auswirken können. Vielmehr soll dies hervorheben, dass die Kontrolle der/des Datenschutzbeauftragten ein von der Staatsanwaltschaft geleitetes, auf eine gerichtliche Kontrolle zielendes Strafverfahren nicht zu ersetzen vermag, wie der anschließende Verweis auf die Unabhängigkeit der Gerichte zeigt.

100 Vgl. *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, Rn. 116f.

101 Selbst gem. § 69 Abs. 2 BKAG umfassen die Befugnisse bei erheblichen Datenschutzverstößen auch Löschungen und stehen nicht unter dem Vorbehalt, dass die Aufgabenwahrnehmung der Polizei nicht wesentlich beeinträchtigt werden darf. Es ist nicht einzusehen, weshalb es ein überwiegendes Interesse an der Verarbeitung von Daten gibt,

III. Weitere Kritikpunkte

1. Einschränkung der Versammlungsfreiheit (§ 78)

Das SOG M-V soll künftig auch die Versammlungsfreiheit einschränken. Deshalb wurde in § 78 bei den eingeschränkten Grundrechten Art. 8 GG aufgenommen, um dem verfassungsrechtlichen Zitiergebot Rechnung zu tragen. Das Zitiergebot soll dafür sorgen, dass sich das Parlament der freiheitsverkürzenden Wirkung bewusst wird, die ein neues oder geändertes Gesetz mit sich bringt.[102] Dies wird jedoch mit der geplanten Änderung des § 78, die übrigens im Rahmen der Verbandsanhörung noch keine Rolle spielte, nicht erreicht. Vielmehr schafft es Unklarheiten zum Verhältnis von Versammlungs- und allgemeinem Polizeigesetz und bringt die Gefahr einer Versammlungsrechtsbeschränkung "durch die Hintertür" mit sich.

- Anlass ist die Entscheidung des Bundesverfassungsgerichts zur Kennzeichenerfassung in Hessen, nach der Kontrollstellen zur Verhinderung von versammlungsrechtlichen Straftaten einen Eingriff in Art. 8 GG darstellen und nur dann in Polizeigesetzen zulässig sind, wenn das Zitiergebot eingehalten wird.[103] Da das SOG M-V in § 29 Abs. 1 S.2 Nr. 4e eine entsprechende Regelung enthält, soll die Änderung des § 78 dazu dienen, diesen formellen Fehler zu heilen.[104] Eine freiheitsfreundliche Gesetzgebung hätte stattdessen **auf die versammlungsbeschränkende Regelung verzichtet, schließlich kommen auch andere Länder** (Baden-Württemberg, Berlin und das Saarland) **schon immer ohne entsprechende Kontrollstellen aus**.

- Mit der Änderung des § 78 gehen aber auch schwierige Rechtsfragen zum Verhältnis von Versammlungs- und Polizeigesetz einher. Über lange Zeit galt durch den Grundsatz der Spezialität des Versammlungsrechts ("Polizeifestigkeit"), dass versammlungsbeschränkende Maßnahmen nur auf Grundlage des Versammlungsgesetzes möglich waren, das Polizeigesetz insoweit nicht zur Anwendung kam. Im Zuge der Föderalismusreform erließen einzelne Länder teilweise eigene Versammlungsgesetze und/oder erklärten das jeweilige Polizeigesetz für anwendbar. Aufgrund des hohen Rangs der Versammlungsfreiheit ist es aber weiterhin so, dass das Polizeigesetz nicht ohne Weiteres auf Versammlungen anwendbar ist; vielmehr ist genau zu prüfen, ob die jeweiligen Befugnisse auf die Anforderungen des Grundrechts zugeschnitten sind.[105] Deshalb sind etwa Meldeauflagen nicht anwendbar, solange das Zitiergebot nicht eingehalten wird.[106] Die Folgewirkungen der Änderung des § 78 wurden im Entwurf – soweit ersichtlich – nicht beachtet.

- Neben den Kontrollstellen des § 29 können zahlreiche weitere Befugnisse in die Versammlungsfreiheit eingreifen. Hier soll sich auf den Einsatz von Kameras (§§ 32, 32a) und Meldeauflagen (§ 52b) beschränkt werden, wobei die Folgewirkungen auch für andere Maßnahmen (etwa Platzverweise, § 52) zu prüfen wären.

- Als unproblematisch ist jedenfalls die Regelung zur offenen Videoüberwachung gem. § 32 Abs. 1 zu nennen, die Versammlungen ausdrücklich aus dem Anwendungsbereich ausklammert. Für die

die unter erheblichen Rechtsverstößen erlangt wurden. Das SOG M-V sollte zumindest nicht hinter den Vorgaben des BKAG zurückbleiben.

102 Vgl. *Enders*, in: BeckOK GG, Art. 19 Rn. 15.

103 BVerfG, Beschl. v. 18.12.2018 - 1 BvR 2795/09 -, Rn. 61f.

104 So die Begründung in LT-Drs. 7/3694, S. 213, 267f.

105 Vgl. *Hong*, in: Peters/Janz, Handbuch Versammlungsrecht, 2015, B Rn. 88.

106 Vgl. einerseits *Trurnit*, in: BeckOK PolR BW, § 3 Rn. 31 für Baden-Württemberg, andererseits *Ullrich*, in: BeckOK PolR Nds § 10 Rn. 7 für Niedersachsen. Mit der eingangs genannten Entscheidung des Bundesverfassungsgerichts dürfte die anders lautende Entscheidung BVerwGE 129, 142 (147) überholt sein, vgl. auch die Kritik bei *Trurnit*, NVwZ 2012, 1079 (1081f.); *Groscurth*, in: Peters/Janz, Handbuch Versammlungsrecht, 2015, G Rn. 18, *Kniesel/Poscher*, in: Lisken/Denninger, Handbuch Polizeirecht, 6. Aufl. 2018, K Rn. 154).

Verwendung von **Dashcams gem. § 32 Abs. 8 fehlt dagegen eine entsprechende Einschränkung**.

Vorschlag: Statt der Einschränkung in Abs. 1 einen neuen Abs. 11 anfügen: "Für den Einsatz technischer Mittel zur offenen Bild- und Tonaufnahme sowie zur Bild- und Tonaufzeichnung bei Versammlungen ist nur das Versammlungsgesetz anwendbar." oder *"Diese Vorschrift findet bei Versammlungen im Sinne des Versammlungsgesetzes keine Anwendung".*

- Im Zusammengang mit Bodycams und Meldeauflagen ist dagegen geregelt, dass die Vorschriften des Versammlungsrechts unberührt bleiben (§§ 32a Abs. 6 S. 2, 52b Abs. 4 S. 2). Es ist allerdings **unklar, was mit dieser Norm gemeint ist**, schließlich kann es einerseits bedeuten, dass die Befugnisse des Versammlungsgesetzes vorgehen, andererseits dass diese zusätzlich zum Polizeigesetz anwendbar sind. Bei der Einführung der Bodycams ging die Landesregierung davon aus, dass die Verwendung von Bodycams im Anwendungsbereich des Versammlungsgesetzes ausgeschlossen sei, weil dessen Geltung in § 32 Abs. 9 a.F. als unberührt bleibend bezeichnet wurden.[107] In einer entsprechenden Norm zur Aufenthaltsanordnung gem. § 67b Abs. 5 sollte dagegen gemeint sein, dass die in Bezug genommene Regelung weiterhin anwendbar bleibt.[108] Auch im aktuellen Gesetzentwurf wird dieses Verständnis für die Formulierung "bleiben unberührt" zugrunde gelegt.[109] Und für Meldeauflagen werden Versammlungen ausdrücklich als Anwendungsbereich genannt.[110] Damit wird deutlich, dass die Änderung des § 78 entgegen der Begründung **auch in anderen Befugnissen Einschränkungen in die Versammlungsfreiheit ermöglichen wird**. Dem sollte jedoch nicht gefolgt werden. Wenn die Kontrollstellen beibehalten werden, sollte in den anderen Normen klargestellt werden, dass die Spezialität des Versammlungsgesetzes nicht weiter aufgeweicht wird.

Vorschlag: In §§ 32a Abs. 6 S. 2, 52b Abs. 4 S. 2 "Diese Vorschrift findet bei Versammlungen im Sinne des Versammlungsgesetzes keine Anwendung".

2. Schutz des Kernbereichs privater Lebensgestaltung (§ 26a)

Die Regelung zum Schutz des Kernbereichs privater Lebensgestaltung gem. § 26a ist grundsätzlich zu begrüßen. Dieser darf nicht unter staatlicher Beobachtung stehen, sondern muss frei von staatlichen Eingriffen bleiben.[111] Gerade verdeckte Maßnahmen wie die Online-Durchsuchung können regelmäßig dazu führen, dass Informationen erhoben werden, die dem Kernbereich privater Lebensgestaltung zuzuordnen sind.[112] Das wurde im Gesetzentwurf auch berücksichtigt, allerdings sollte die enthaltene Regelung zum **Kernbereichsschutz ergänzt** werden.

- Im Entwurf zielt die Vorschrift vorrangig auf Maßnahmen, die die Überwachung von Personen mit technischen Mitteln betreffen.[113] Eine besondere Gefährdung ergibt sich aber für Einsatzbereiche

---

[107] LT-Drs. 7/1320, S. 26. Für Bodycams in Form von Helmkamera wurde dies von Beweissicherungs- und Festnahmeeinheiten bei Demonstrationen aber regelmäßig ignoriert, vgl. aktuell zum Versammlungsgeschehen am 08.05.2019 in Demmin den Bericht der Demobeobachtungsgruppe: https://recht-kritisch.de/demobeobachtung-demmin-2019 (13.08.2019).

[108] LT-Drs. 7/1320, S. 35.

[109] Vgl. zum Verhältnis von Meldeauflagen gem. § 52 b neben Platzverweisen gem. § 52 sowie von Online-Durchsuchung gem. § 33c neben Cloud-Durchsuchung gem. § 57 Abs. 2 LT-Drs. 7/3694, S. 252, 259. Gleiches gilt auch in anderen Normen des SOG M-V (vgl. §§ 70, 74) und in anderen Polizeigesetzen (vgl. § 60 SOG LSA, Art. 77 BayPAG).

[110] LT-Drs. 7/3694, S. 252.

[111] BVerfGE 6, 32 (41); BVerfGE 109, 279 (313).

[112] *Schenke*, Polizei- und Ordnungsrecht, 10. Aufl., 2018, Rn. 190b.

[113] Im Entwurf wird vor allem auf allgemeine Passagen zum Kernbereichsschutz aus dem Urteil des BVerfG zum BKAG (BVerfGE 141, 220) sowie auf Entscheidungen zur technischen Mitteln wie Onlinedurchsuchung sowie Wohnraum- und Telekommunikationsüberwachung Bezug genommen (BVerfGE 120, 274; 129, 208). Nur diese behandelt auch der als Vorbild genannte § 100d StPO. Siehe dazu LT-Durcksache 7/3694 S. 156ff..

von **verdeckten Ermittler*innen (VE)** und **V-Leuten**. Bei diesen Tätigkeiten wird eine Vielzahl an Informationen der betroffenen Personen in Erfahrung gebracht. Gerade durch die **aktive Kommunikation** zeigt sich die Intensität solcher Maßnahmen: Anders als bei verdeckten Dateneingriffen wie der Online-Durchsuchung interagieren die Betroffenen und die VE oder V-Leute über eine längere Zeit miteinander.[114] Informationen werden nicht aufgezeichnet, aber können durch Gespräche in Erfahrung gebracht werden. Wie groß das Ausmaß eines solchen Einsatzes sein kann, zeigt bspw. der Fall aus Hamburg um die VE „Maria B.“. Während ihres verdeckten Einsatzes in der linksalternativen Szene soll sie eine intime Beziehung mit einer Person aus der Szene eingegangen sein.[115] Bei solch einem Kontakt ist es möglich, dass gerade durch diesen kernbereichsrelevante Informationen zur Sprache kommen und gesammelt werden könnten.[116] Das kann **folgenreich für die Betroffenen** sein. Schließlich glauben sie vermeintlich an das Bestehen einer realen Beziehung mit einer Person, die nicht im Einsatz für die Polizei ist. Laut Bundesverfassungsgericht gehört der Ausdruck von höchstpersönlichen Empfindungen und der vertrauliche Kontakt im engsten privaten Umfeld zum Kernbereich.[117] § 26a Abs. 1 bietet keinen hinreichenden Schutz, weil beim VE-Einsatz der Kernbereich regelmäßig nicht das *alleinige* Ziel der Maßnahme ist. Dieser sollte durch einen zweiten Satz ergänzt werden, der diese besondere Form der kernbereichsrelevanten Datenerhebung von vornherein ausschließt: Empfohlen wird ein **Verbot** für VE und V-Leute, dass das **Eingehen von intimen Kontakten bzw. Beziehungen** zum Inhalt hat.

- Da § 26a Abs. 1 keinen umfassenden Schutz des Kernbereichs auf der Ebene der Datenerhebung bietet, bedarf es einer unabhängigen Kontrolle auf der **Ebene der Datenverarbeitung**.[118] Da auch bei der **Online-Durchsuchung regelmäßig Kernbereichsaspekte betroffen** sind, ist in Abs. 4 zu ergänzen, dass die Verwendung der erlangten Daten ebenso gerichtlich zu bestätigen wie bei Daten, die aus Wohn- und Geschäftsräumen erhoben wurden. In Abs. 5 ist die verfassungsrechtlich geforderte Kontrolle nicht ausreichend, weil der*die behördliche Datenschutzbeauftragte keine **hinreichend unabhängige Instanz** ist. Der Absatz sollte dahingehend geändert werden, dass die Prüfung von Daten, deren Erhebung wegen Kernbereichsbezug gem. Abs. 3 unterbrochen wurde, von der*dem Landesdatenschutzbeauftragten oder einer anderen institutionell unabhängigen Stelle durchzuführen ist.

---

114 *Hohnerlein,* Verdeckte Ermittler – verdeckter Rechtsstaat?, NVwZ 2016, 511 (513).

115 *Hahn,* SZ v. 28.08.2015, abrufbar unter: https://www.sueddeutsche.de/politik/linksautonome-in-hamburg-enttarnung-einer-ermittlerin-1.2623704 (06.08.2019).

116 *Hohnerlein,* NVwZ 2016, 511 (514).

117 BVerfGE 141, 220 (276ff. = Rn. 119ff.) Das OVG Hamburg, NVwZ-RR 2018, 886 äußerte sich (nur) deshalb nicht zu dieser Frage, weil die Polizei die Maßnahme schon umfassend als rechtswidrig anerkannt hatte.

118 Vgl. BVerfGE 141, 220 (278ff., 314 = Rn. 126ff., 241).

3. Schutz von zeugnisverweigerungsberechtigten Personen (§ 26b)

Mit der Neuregelung des § 26b sollen zwingende Vorgaben des Bundesverfassungsgerichts eingehalten werden.[119] Gem. Abs. 2 werden allerdings nur Geistliche, Anwält*innen und Abgeordnete umfassend geschützt. Der Schutz insb. von Ärzt*innen, Psychotherapeut*innen und Journalist*innen soll dagegen nicht gelten, wenn die Datenerhebung zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit erforderlich ist. Für eine hinreichende Absicherung dieser besonders schutzwürdigen Personen ist aber als Mindeststandard eine **umfassende Verhältnismäßigkeitsprüfung** geboten.[120] Zumindest dies sollte in S. 1 klargestellt werden, indem diese Belange positiv als Teil der Abwägung erwähnt werden. Dabei sollte festgehalten werden, dass die Abwägung nur bei Straftaten von erheblicher Bedeutung zulasten des Berufsgeheimnisses ausfällt (vgl. § 160a StPO).[121]

Eine Differenzierung zwischen den verschiedenen Berufsgruppen, die zur Zeugnisverweigerung berechtigt sind, ist zwar verfassungsrechtlich grundsätzlich zulässig.[122] Das SOG orientiert sich hier an § 160a StPO. Zumindest bei Psychotherapeut*innen, die im Rahmen ihrer Tätigkeit regelmäßig Gespräche über besonders sensible Themen führen, spricht aber viel dafür, ihnen den absoluten Vertraulichkeitsschutz zu gewähren.[123] Im Übrigen **zeigen aber andere Länder, dass ein umfassender Schutz aller zeugnisverweigerungsberechtigten Personen in Polizeigesetzen möglich, sinnvoll und praktikabel ist** (vgl. Art. 49 BayPAG, § 16 Abs. 5 PolG NRW).

4. Festhalterecht bei Identitätsfeststellungen für Ordnungsbehörden (§ 29 Abs. 2)

Erst nach der Verbandsanhörung wurde das Recht von Beschäftigten der Ordnungsbehörden eingefügt, Personen festzuhalten, um Identitätsfeststellungen zu ermöglichen. Es stimmt zwar, dass einzelne Länder diese Befugnis ebenfalls vorsehen. Trotzdem gilt zu bedenken, dass die Anwendung physischen Zwangs bisher aus guten Gründen der Polizei vorbehalten war. Denn Polizeikräfte sind für solche Situationen, die immer auch ein **nicht zu unterschätzendes Eskalationspotential beinhalten, besonders ausgebildet**. Bei sonstigen Verwaltungsbeschäftigten ist das im Allgemeinen nicht zu erwarten. Die Gesetzesbegründung macht auch keinerlei Angaben dazu, wie eine entsprechende Ausbildung sichergestellt werden kann. Mit der Verleihung von Zwangsmitteln an andere Personen als Polizeikräfte sehen wir zudem die Gefahr, dass dies ein erster Schritt zur Schaffung einer "Polizei zweiter Klasse" ist, wie sie teilweise in anderen Ländern eingeführt wurde.[124] Dem stehen dort zu Recht erhebliche Bedenken entgegen.

5. Bestandsdatenauskunft (§ 33h)

Der Anwendungsbereich der Bestandsdatenauskunft wird dahingehend ausgeweitet, dass neben Telekommunikations- auch Telemedienbestandsdaten erhoben werden. Dabei war schon die bisherige Regelung hoch umstritten. Gegen diese ist eine **Verfassungsbeschwerde beim Landesverfassungsgericht anhängig**, daneben eine gegen etwas engere Bundesregelungen **ebenfalls beim Bundesverfassungsgericht**.[125] In diesem Zusammenhang wurde vielfältige bemerkenswerte Kritik geäußert, die eine umfassende Prüfung der bisherigen Befugnisse nahelegt. An dieser Stelle soll

[119] BVerfGE 141, 220 (281f., 318ff. = Rn. 131ff., 255ff.)
[120] Vgl. *Puschke/Singelnstein*, NJW 2008, 113 (117).
[121] Vgl. *Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, G Rn. 165.
[122] Vgl. BVerfGE 129, 208 (262ff. = Rn. 255ff).
[123] Vgl. *Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, G Rn. 164.
[124] Strikt gegen die Ausstattung des Kommunalen Ordnungsdienstes mit Zwangsmitteln auch die GDP in Schleswig-Holstein: https://www.shz.de/regionales/kiel/es-darf-keine-billig-polizei-geben-id19404651.html.
[125] Vgl. http://bestandsdatenauskunft.de/ (07.08.2019) und https://bdamv.wordpress.com/ (07.08.2019).

aber lediglich auf Aspekte eingegangen werden, die in den letzten zwei Jahren einen dringenden Änderungsbedarf der aktuellen Befugnisse zur Bestandsdatenauskunft anzeigen.

- § 33h sieht keinerlei eigene Verfahrensschritte vor, die die Rechte der Betroffenen wahren. Dabei betrifft zumindest die Abfrage von Passwörtern gem. Abs. 1 S. 2 und von dynamischen IP-Adressen gem. Abs. 2 besonders sensible Daten.[126] Da die Betroffenen davon oftmals nichts erfahren,[127] ist eine **besondere Sicherung im Verfahren** vorzusehen. Dazu reicht es nicht, dass bei der Passwortabfrage auch die Voraussetzungen für die spätere Nutzung erfüllt sein müssen; es bedeutet *stets* einen besonders schweren Eingriff, wenn der Schlüssel zu besonders gesicherten Daten heimlich erlangt wird, egal welche Qualität diese Daten haben. Nicht ohne Grund wird in zahlreichen Bundes- und Landesgesetzen die **Passwortabfrage unter Richtervorbehalt** gestellt.[128] Gleiches gilt für die **Abfrage dynamischer IP-Adressen.** Der EGMR hat kürzlich festgestellt, dass Art. 8 EMRK eine gerichtliche Entscheidung gebietet, weshalb die aktuelle Regelung auch **europarechtswidrig** ist.[129]
- Im Rahmen der anhängigen Verfassungsbeschwerde beim Bundesverfassungsgericht musste die Bundesregierung dem Bundesverfassungsgericht mitteilen, dass die Zahl der **Bestandsdatenabfragen u.a. durch das BKA in den letzten Jahren massiv angestiegen** ist. Darauf reagierte die Bundesdatenschutzbeauftragte mit einer kritischen Stellungnahme, in der sie darlegte, dass die Datenabfragen zunehmend die Erstellung von Persönlichkeitsprofilen ermöglichten. Dabei werde durch die geringen materiellen Voraussetzungen und die behördeninterne Organisation ermöglicht, dass **sensible Daten schon beim Verdacht geringfügiger Rechtsverstöße einer Vielzahl an Angestellten zugänglich** sei.[130] Gerade angesichts der jüngsten Skandale in M-V, durch die bekannt wurde, dass Behördendaten an rechtsextreme Kreise gelangten, sollte zunächst dringend überprüft werden, wie viele und welche Bestandsdaten abgefragt werden und welchen Stellen sie zugänglich sind.

6. Polizeiliche Beobachtung und gezielte Kontrolle (§ 35)

Die auf EU-rechtlichen Grundlagen[131] beruhende Norm wird im Entwurf erheblich erweitert. Durch die Ergänzung der "drohenden terroristischen Gefahr" über § 67a betrifft dies auch die polizeiliche Beobachtung. Gegen Teile der Norm bestehen Bedenken bzgl. ihrer Bestimmtheit und Fragen der Gesetzgebungskompetenz, die hier lediglich kurz erwähnt werden sollen. Gewichtiger sind aber Einwände gegen die in Abs. 2 neu geschaffene Befugnis zur gezielten Kontrolle. Die Formulierung, dass Identitätsfeststellungen sowie Durchsuchungen von Personen und Sachen "unbeschadet anderer Vorschriften" möglich sein sollen, hat zur Folge, dass eine Person, ihr Fahrzeug und ihre sonstigen Sachen **allein aufgrund der Tatsache, dass sie ausgeschrieben ist, jederzeit durchsucht** werden kann. Es braucht **keinen Anhaltspunkt, dass sie irgendetwas mit sich führt, was für die Gefahrenabwehr relevant** ist. Die Möglichkeit, diese Maßnahmen ohne einen konkreten Anlass durchzuführen, wird zwar in Art. 36 Ratsbeschluss 2007/533/JI optional

---

126 Diese sind über das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme bzw. das Telekommunikationsgeheimnis gem. Art. 10 GG besonders geschützt, vgl. BVerfGE 120, 274 (324 = Rn. 234ff), 130, 151 (181 = Rn. 116)

127 Es besteht zwar eine Benachrichtigungspflicht gem. § 46 Abs. 1 S. 1 Nr. 4, die aber gem. Abs. 2 stark verzögert oder unterbleiben kann.

128 Vgl. § 10 Abs. 3, 40 Abs. 3 BKAG, § 22a Abs. 2 BPolG, § 33 Abs. 3 POG RP, § 33c Abs. 4 NPOG.

129 EGMR, Bendik v. Slowenien, 24.4.2018, No. 62357/14 Rn. 122ff.

130 Vgl. https://www.spiegel.de/netzwelt/web/bestandsdatenauskunft-datenschuetzerin-bemaengelt-bundesdatengesetz-a-1237640.html, http://bestandsdatenauskunft.de/wp-content/uploads/2019/04/bda-bund_breg_2019-12-19_anon.pdf, http://bestandsdatenauskunft.de/wp-content/uploads/2019/01/BfDI-StN_anon.pdf.

131 Art. 99 SDÜ, Art. 36 Ratsbeschluss 2007/533/JI.

vorgesehen, **allerdings schon in der EU-Norm unter den Vorbehalt gestellt, dass dies mit den nationalen Verfassungen vereinbar** ist. Da bei einer Ausschreibung zur gezielten Kontrolle nicht absehbar ist, mit wem diese Person künftig in eine Polizeikontrolle geraten wird und welche Gegenstände diese dabei mitführen werden, wären tief in das Persönlichkeitsrecht eingreifende Maßnahmen wie pauschale Durchsuchungen unverhältnismäßig. Daher sind diese **ohne konkrete Gefahr verfassungswidrig**.[132] Andere Länder stellen daher klar, dass Identitätsfeststellungen und Durchsuchungen nur nach Maßgabe der jeweiligen Vorschriften zulässig sind.[133] Die Landesregierung verweist zwar durchaus auf andere Länder, begründet die gezielte Kontrolle aber ausdrücklich damit, dass *durch sie* Anschlussbefugnisse ermöglicht und zusätzliche Erkenntnisse erlangt werden sollen. Nicht die Voraussetzungen der Anschlussbefugnisse, sondern nur deren Verfahrensvorschriften sollen gem. § 35 Abs. 2 S. 3 anzuwenden sein. Wenn diese Kontrollen dem Ziel dienen sollen, "der offenen Ermittlungsphase den Druck zu erhöhen" und "potentielle Gefährder zu verunsichern", dann hat das nichts mehr mit der Abwehr konkreter Gefahren zu tun.[134] Diese Methoden passen nicht in einen freiheitlichen Rechtsstaat und sind klar als verfassungswidrig einzustufen. Im Übrigen sei darauf hingewiesen, dass einige Länder auf die gezielte Kontrolle verzichten.[135] Die polizeiliche Beobachtung wird zudem oftmals unter Richtervorbehalt gestellt,[136] während Abs. 5 dies nur für die Verlängerung der Ausschreibung vorsieht.

Vorschlag: Abs. 2 sollte komplett gestrichen werden. Abs. 3-5 sollten dahingehend angepasst werden, dass eine gerichtliche Anordnung von Beginn an erforderlich ist.

7. Automatisierte KfZ-Kennzeichenerfassung (§ 43a)

Die Vorschrift lässt sich aufgrund vielerlei Gründe rechtspolitisch hinterfragen. Da sie aber im Wesentlichen unverändert bleiben soll, wird hier lediglich auf den verfassungsrechtlich zwingenden Änderungsbedarf eingegangen, der sich entgegen der Auffassung der Landesregierung in Folge der jüngsten Entscheidungen des Bundesverfassungsgerichts ergibt. Denn als Mittel der Schleierfahndung zur Bekämpfung der grenzüberschreitenden Kriminalität **muss die Kennzeichenerfassung einen klaren örtlichen und sachlichen Grenzbezug haben**.[137] Nach Nr. 6 sollen die Kontrollen aber von der Bundesgrenze bis zur A20 möglich sein. Dies ist schon deshalb **völlig unverhältnismäßig, weil damit fünf der siebengrößten Städte des Landes und ein Großteil der Bevölkerung von der Maßnahme betroffen sein können**. Nicht nachvollziehbar ist auch, offenkundig die gesamte Küstengrenze als Grenzgebiet anzusehen, obwohl grenzüberschreitender KfZ-Verkehr in nennenswertem Maße allenfalls in den Fährhäfen Rostock und Sassnitz stattfindet. Fällt es schon schwer, für Greifswald bei einer Distanz von ca. 80 km zur polnischen Grenze einen Grenzbezug zu erkennen, erscheint eine Kfz-Kennzeichenerfassung zur Bekämpfung der grenzüberschreitenden Kriminalität in Wismar als völlig unverständlich, ist doch der nächste Bezugspunkt ein ca. 70 km entfernter Fährhafen.[138] Wenn die Landesregierung stattdessen einen Einsatz lediglich von der polnischen Landesgrenze bis einschließlich dem östlichen Teil der A 20 ermöglichen wollte,[139] müsste eine hinreichend bestimmte Regelung vorgelegt werden, deren Verhältnismäßigkeit dann gesondert

132 Vgl. *von der Grün*, BeckOK PolG BW, § 25 Rn. 4.
133 Vgl. Art. 40 BayPAG, § 25 PolG BW, § 17 HSOG, § 37 ThPAG.
134 Vgl. LT-Drs. 7/3694, S. 191f. Dass es § 35 Abs. 2 eine eigenständige Durchsuchungsbefugnis begründen soll, zeigt auch deren Erwähnung in § 57.
135 Vgl. § 27 ASOG BE, § 32 POG RP, § 40 PolG SN.
136 Vgl. § 163e StPO, § 187 LVwG SH.
137 BVerfG, Beschl. v. 18.12.2018 - 1 BvR 142/15 -, Rn. 147ff.
138 Über die B105 ist Wismar auch von der polnischen Grenze gut erreichen, ohne die A20 zu überqueren.
139 Sowohl LT-Drs. 5/3735, S. 32.

geprüft werden müsste. In der jetzigen Form ist § 43a Abs. 1 Nr. 6 jedenfalls verfassungswidrig.

8. Rasterfahndung (§ 44)

Die Rasterfahndung soll künftig auch bei drohenden terroristischen Gefahren (§67a) zulässig sein. Das **Bundesverfassungsgericht, die rechtswissenschaftliche Literatur, der Bundes- und sogar der bayrische Landesgesetzgeber sind sich jedoch einig, dass die Rasterfahndung nur bei konkreten Gefahren eingesetzt werden** darf.[140] Auch wenn die Landesregierung darauf verweist, dass die abgesenkte Gefahrenschwelle der drohenden Gefahr vom Bundesverfassungsgericht akzeptiert wird,[141] übersieht sie, dass sich Maßnahmen zur Überwachung von identifizierten Gefährder*innen fundamental von einem Verfahren unterscheiden, das gefährliche Personen überhaupt erst identifizieren soll. § 44 Abs. 1 Nr. 1 ist daher verfassungswidrig.

9. Meldeauflagen (§ 52b)

Es ist aus rechtsstaatlichen Gründen sehr zu begrüßen, dass die bisher auf die Generalklausel der §§ 13, 16 gestützten Meldeauflagen nunmehr eine ausdrückliche Regelung in § 52b erfahren.

- Dem Zugewinn an Bestimmtheit läuft jedoch der **weite Anwendungsbereich** der Maßnahme zuwider, die künftig zur Verhinderung jedweder Art von Straftat eingesetzt werden dürfen soll. Die Vorgabe, an bestimmten Tagen an einen festgelegten Ort gebunden zu sein, **beeinträchtigt die betroffene Person erheblich in ihren Entfaltungsmöglichkeiten**. Dabei kann nicht nur die Allgemeine Handlungsfreiheit gem. Art. 2 Abs. 1, sondern auch die Freizügigkeit gem. Art. 11 GG betroffen sein. Ein solch tiefgreifender Eingriff erscheint **allenfalls gerechtfertigt, wenn er schwerwiegende Gefahren abwehren soll**.[142] Diese Begrenzung sollte bereits in den Tatbestand der Norm aufgenommen werden.[143]

- Daneben halten wir für nicht hinreichend belegt, dass diese Maßnahme (im Gegensatz zu anderen Ländern) nur von der Polizei und nicht von den Ordnungsbehörden erlassen werden soll. Dies liefe dem in § 7 Abs. 1 Nr. 3 zum Ausdruck kommenden Grundsatz zuwider, wonach die **Zuständigkeit der Ordnungsbehörden außer bei unaufschiebbaren Maßnahmen dem polizeilichen Eingreifen vorgeht**.[144]

---

[140] BVerfGE 115, 320 (360 = Rn. 133), *Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, G Rn. 1070; § 48 BKAG, Art. 46 BayPAG mit LT-Drs. 17/20425, 68.

[141] LT-Drs. 7/3694, S. 191f.

[142] Vgl. § 15a PolG Bbg; *Ipsen*, Stellungnahme zur Reform des Niedersächsischen Polizeigesetzes vom 04.07.2018, S. 5.

[143] Allgemein dazu BVerfGE 120, 274 (315ff. = Rn. 207ff.).

[144] Vgl. dazu auch *Denninger*, in: Handbuch des Polizeirechts, 6. Aufl. 2018, D Rn. 241ff.