

Stellungnahme des RAV

zum Gesetzentwurf der Landesregierung **Entwurf eines Gesetzes über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern und zur Änderung anderer Gesetze (Drucksache 7/3694)**

anlässlich der Anhörung im Innen- und Europaausschuss am 22. August 2019

Verfasserin: Dr. Anna Luczak, Rechtsanwältin

Technische Vorbemerkung

Angesichts der Vielzahl der geplanten Änderungen beschränkt sich die Stellungnahme darauf, zu den vorgeschlagenen Änderungen bezüglich Video-Überwachung im Polizeigewahrsam, Meldeauflagen, Besonderen Mittel der Datenerhebung, Quellen-TKÜ und Online-Durchsuchung, Gezielter Kontrolle und Rasterfahndung ausführliche Beurteilungen abzugeben (A). Es schließen sich kurze Bemerkungen zu weiteren Normen an (B).

Inhaltliche Vorbemerkung

Der Gesetzentwurf beinhaltet eine Vielzahl von Kompetenzen, die bereits sehr weit im Vorfeld von Gefahren sehr weitgehende Grundrechtseingriffe ermöglichen. Das Ansetzen bereits im Vorfeld bringt es mit sich, dass die von der Polizei zu treffende Prognose, ob tatsächlich eine Gefahr besteht, mit Unsicherheit behaftet ist.

Würde der Gesetzentwurf als Gesetz beschlossen, hätte das zur Folge, dass – im Falle polizeilicher Fehleinschätzungen, die wegen der grundsätzlichen Schwierigkeit, solche Prognosen zu treffen, unvermeidbar sind – schwerwiegende Maßnahmen gegen Personen eingesetzt werden, von denen tatsächlich keine Gefahr ausgeht.

Es könnten Telefone abgehört, Computer online durchsucht, zu diesem Zweck Drohnen heimlich auf W-LAN-Netze zugreifen und ähnliches. Diese Problematik wird noch verschärft dadurch, dass mit derartigen Methoden nicht nur auf Daten von Personen zugegriffen werden darf, bei denen die Polizei davon ausgeht, dass von ihnen eine Gefahr ausgeht, sondern auch deren engere Kontaktpersonen direkte Zielobjekte der Überwachung sein können. Hinzu kommt, dass bei Zugriffen auf Telekommunikationsinhalte immer auch völlig unbeteiligte Dritte betroffen sind, die nicht in engem, sondern nur sporadischem Kontakt mit den Personen stehen, in Bezug auf die Aufklärung betrieben werden soll.

Um die Dimensionen klar zu machen, wird beispielhaft auf zwei Erhebungen zu derartigen Maßnahmen hingewiesen: So wurden im Jahr 2014 in Berlin gegen 743 Personen strafprozessuale Telefonüberwachungsmaßnahmen angeordnet, abgehört wurden dabei insgesamt 1.504.884 Gespräche¹ – die Zahl der mitbetroffenen Gesprächspartner*innen wurde nicht erhoben, aber es ist leicht vorstellbar, dass diese Zahl fünfstellig ist. Von gefahrenabwehrenden Maßnahmen nach dem neuen BKAG von 2009, das Pate für einige der am meisten in Grundrechte eingreifende Maßnahmen des hiesigen Entwurfs stand, waren in den Jahren 2009 bis 2015 86 potentielle Gefahrverursacher*innen betroffen – »mitbetroffen« war eine Zahl von mindestens² 1.621 Personen.³ Die Streubreite ist gerade bei Maßnahmen der heimlichen Überwachung nachweislich sehr groß.

Aus Sicht der im RAV organisierten Anwältinnen und Anwälte ist die klassische Aufteilung zwischen (eher offenen und weniger eingreifenden) Maßnahmen der Abwehr von Gefahren, bei denen noch unsicher ist, ob sie sich tatsächlich verwirklichen werden, und (eher heimlichen und stärker eingreifenden) Maßnahmen der repressiven Verfolgung bereits geschehener Straftaten nicht nur verfassungsrechtlich, sondern auch politisch geboten, um zu verhindern, dass in der Bevölkerung ein Gefühl der umfassenden staatlichen Überwachung entsteht.

Bereits in der Grundentscheidung des Bundesverfassungsgerichts, in dem es das Grundrecht auf informationelle Selbstbestimmung erstmals definierte, ist ausgeführt⁴:

1 Abgeordnetenhaus Berlin, Drs. 17/2401 v. 20.07.2015, S. 4.

2 In einigen Fällen fehlen die Zahlen zu den Mitbetroffenen.

3 BT-Drs. 18/13031, S. 17 – Maßstab für Mitbetroffenheit war hier § 20 w BKAG a.F.

4 BVerfGE 65, 1, 42f.

»Individuelle Selbstbestimmung setzt voraus, dass dem Einzelnen Entscheidungsfreiheit gegeben ist. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.

Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten.

Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.«

Das Grundgesetz schützt insoweit auch vor (Selbst-)Einschränkungen, die sich Bürgerinnen und Bürger aus Furcht vor Überwachung auferlegen.

Im Zusammenspiel tiefgreifender und gleichzeitig heimlicher Befugnisse entsteht die Möglichkeit einer derart extensiven und intensiven Überwachung, dass umfassende Persönlichkeitsprofile von Personen erstellt werden können.

Nach der Rechtsprechung des Bundesverfassungsgerichts bedeutet es eine Verletzung der Menschenwürde, wenn sich eine Überwachung über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein

Persönlichkeitsprofil werden können (siehe auch die in der Gesetzesbegründung vielfach zitierte Entscheidung des BVerfG zum BKAG vom 20. April 2016, 1 BvR 966/09, Rn. 130 mit Verweis auf frühere Entscheidungen: BVerfGE 109, 279 <323>; 112, 304 <319>; 130, 1 <24>).

Wer sich sicher sein kann, dass im Normalfall nur der Staat nur dann seine private Kommunikation und sein privates Leben überwacht, wenn die eindeutige Notwendigkeit besteht, eine geschehene Straftat aufzuklären, kann sich einigermaßen sicher sein, nicht von Überwachung betroffen zu sein, wenn im engeren Umfeld keine Straftaten begangen werden. Wenn aber diffuse Gefahrenlagen schon Grund für die Überwachung nicht nur von für die Gefahr mutmaßlich verantwortlichen Personen, sondern auch von deren Kontaktpersonen sein können, ist kaum noch absehbar, wer in den Fokus gerät. Die Erfassung von Daten von Kontaktpersonen geht dabei nach dem Gesetzentwurf so weit, dass zum Beispiel nach § 27 Abs. 3 auch höchstpersönliche Daten von selbst nicht gefährlichen Kontaktpersonen erhoben werden dürfen, also biometrische und genetische Daten, solche zur Religion, zur sexuellen Orientierung etc. (siehe § 3 Abs. 5 Nr. 3).

Insgesamt gesehen gefährdet die Ausweitung der präventivpolizeilichen Befugnisse im vorgeschlagenen Gesetz Menschenwürde, das Grundrecht auf freie Entfaltung der Persönlichkeit und das Grundrecht auf informationelle Selbstbestimmung, wonach den einzelnen Bürger*innen ein autonomer Bereich privater Lebensgestaltung zusteht, in dem sie ihre Individualität entwickeln und wahren können.

Als Vorbemerkung sei abschließend noch gesagt, dass der Gesetzesentwurf sehr extensiv auf die Entscheidung des Bundesverfassungsgerichts zu den Änderungen des BKA-Gesetzes 2009 Bezug nimmt und so den Eindruck erweckt, das verfassungsrechtlich Gebotene zu regeln. Hierzu muss zunächst gesagt werden, dass das, was das Bundesverfassungsgericht mit Blick auf die neuen Kompetenzen des BKA entschieden hat – Kompetenzen, die das BKA anwenden darf, wenn es Hinweise von Geheimdiensten anderer Länder in Bezug auf Planungen von großen Terroranschlägen in der Bundesrepublik Deutschland bekommt – keineswegs ohne weiteres auf Landespolizeien übertragen werden kann.

Weder aus dem Gesetzentwurf, noch aus Zahlen der Polizeilichen Kriminalitätsstatistik für das Land Mecklenburg-Vorpommern oder den Berichten der Abteilung für Verfassungsschutz des Ministeriums für Inneres und Europa des Landes Mecklenburg-

Vorpommern ergibt sich, dass im Land Mecklenburg-Vorpommern für die Landespolizei dieselbe Notwendigkeit besteht wie für das BKA, terroristische Gefahren weit im Vorfeld konkreter Planungen aufzuklären. Erst recht gilt das vor dem Hintergrund, dass eine Vielzahl weitreichender Kompetenzen im neuen SOG nicht nur bei terroristischen Gefahren angewandt werden sollen darf, sondern auch schon bei Gefahren für »Leib, Leben oder Freiheit« einer Person, mit anderen Worten bereits bei der Gefahr einer einfachen Körperverletzung (=Gefahr für Leib).

Zu dem Bezug auf die Verfassungsgerichtsentscheidung von 2016 zum BKAG muss aber vor allem eines klar gestellt werden: Wenn das Bundesverfassungsgericht Gesetze kontrolliert, entscheidet es explizit, was verfassungsrechtlich überhaupt nicht mehr tragbar ist und daher laut Verfassung nicht gelten darf. Aus Entscheidungen des Bundesverfassungsgerichts zur Verfassungsmäßigkeit von Gesetzen lässt sich also nur ersehen, was nicht geregelt werden darf – es bleibt eine politische Entscheidung, was geregelt werden muss. Aus Sicht des RAV besteht keine Notwendigkeit, dass jede Landespolizei schon im Vorfeld konkreter Verbrechenplanungen mit einer Vielzahl sehr weitgehender, heimlicher Ausforschungsmethoden eine Vielzahl von Personen überwacht.

A. Ausführungen zu den einzelnen Änderungsvorschlägen

1. Videoüberwachung von polizeilichen Gewahrsamseinrichtungen - § 32 Abs. 9

Die dauernde Beobachtung von in Polizei-Gewahrsamszellen festgehaltenen Personen in von Seiten der Polizei zu bestimmenden Fällen stellt einen nicht zu rechtfertigenden Eingriff in das Recht auf informationelle Selbstbestimmung der Person dar.

Zwar könnte eine Überwachung von Gewahrsamszellen auch Vorteile für Gefangene bringen, die befürchten, polizeilichen Übergriffen ausgesetzt zu sein. Dies ist jedoch nicht der Fall, solange die Videoaufzeichnung durch die Beamten an- und abgeschaltet werden kann.

Den Rechtsanwältinnen und Rechtsanwälten des RAV wird leider nicht nur in seltenen Ausnahmefällen von Betroffenen berichtet, dass sich Polizeibeamte in polizeilichen Gewahrsamseinrichtungen unangemessen bis falsch oder sogar gewalttätig verhalten.⁵

⁵ Siehe u.a. Grundrechte-Report 1999, S. 138; Grundrechte-Report 2003, S. 70; Grundrechte-Report 2013, Seite 64; Grundrechte-Report 2016, S. 74 und S. 186.

Da Personen in Gewahrsamszellen üblicherweise allein sind und die ihnen gegenüber rechtswidrig handelnden Beamte nicht identifizieren können, wenn diese ihren Namen nicht nennen, ist ein Nachweis des Geschehens für die Betroffenen in vielen Fällen aussichtslos.

Eine Videoüberwachung in polizeilichen Gewahrsamseinrichtungen **könnte** insoweit Abhilfe schaffen – allerdings nur, wenn das Gesetz eine lückenlose und flächendeckende Dokumentation vorschreiben würde. Denn nur, wenn durchgehend gefilmt wird, kann die Tatsache, dass das Geschehen in einer bestimmten Zelle oder zu einer bestimmten Zeit nicht aufgezeichnet wurde, in einem nachfolgenden Verfahren als Indiz dafür gewertet werden, dass etwas verborgen werden soll.

Weil die im Gesetzentwurf vorgeschlagene Maßnahme eben keine umfassende Aufzeichnung vorsieht, bietet sie keinen Schutz vor unangemessenem bis gewalttätigem Verhalten in Gewahrsamseinrichtungen. Sie entspricht entgegen der Gesetzesbegründung eben deshalb auch keineswegs der Empfehlung von Amnesty International im Bericht zu rechtswidriger Polizeigewalt in Deutschland von 2010.

Da die Ermessensnorm – so wie sie im Gesetzentwurf formuliert ist – keinen Schutz gegen rechtswidriges Polizeihandeln bietet, ist der in der Videoüberwachung liegende Eingriff nicht zu rechtfertigen, dem die Betroffenen unausweichlich ausgesetzt sind, während sie im Gewahrsam festgehalten werden. Es stellt eine deutlich über die Freiheitsentziehung als solche hinausgehende Beeinträchtigung dar, wenn eine in Unfreiheit befindliche Person einer Dauer-Beobachtung ausgesetzt ist. Dass das gesamte Verhalten der Gefangenen in der Zelle nach dem Gesetzentwurf nicht nur beobachtet, sondern sogar aufgezeichnet werden darf, verschärft die Problematik noch.

Abschließend sei bemerkt: Soll – wie in der Gesetzesbegründung ausgeführt – Suizid oder gesundheitlichen Notfällen vorgebeugt werden, liegt es auch näher, die betroffenen Personen in anderen Einrichtungen, wie zum Beispiel Krankenhäusern, unterzubringen.

2. Meldeauflagen - § 52 b

Grundsätzlich ist es aus Sicht der Anwältinnen und Anwälte des RAV zu begrüßen, dass mit § 52 b nun eine gesetzliche Grundlage für ein in der Praxis bereits vielfach angewandtes Handeln geschaffen wird. Leider geht jedoch die Regelung über das hinaus, was die bisherige Praxis war. Dafür besteht aus anwaltlicher Sicht zum einen

kein Bedarf, zum anderen birgt die weitreichende Formulierung des Gesetzesentwurfs die Gefahr, dass es zu unverhältnismäßigen Anordnungen kommt.

Hier ist vor allem die Regelung des § 52 b Abs. 5 gemeint, wonach eine Meldeauflage für die Dauer von bis zu drei Monaten erteilt werden kann. Es ist durchaus fragwürdig, ob es überhaupt möglich ist, eine sichere Prognose dazu zu stellen, dass über einen derart langen Zeitraum für jeden einzelnen Tag die Gefahr einer Straftatbegehung droht. Der Gesetzesentwurf selbst gibt in der Begründung auch gar kein Beispiel dafür, dass über 90 Tage hinweg eine Meldeauflage die Begehung einer Straftat verhindern soll – das im Gesetzesentwurf benannte Beispiel lautet, dass sich aus dem Spielplan für Fußballveranstaltungen ergibt, dass betroffene Personen »bei einer Reihe von Risiko-Spielen« Straftaten begehen könnten (S. 253 des Entwurfs). Hier wäre aber gerade keine Meldeauflage für die Dauer von drei Monaten verhältnismäßig, sondern mehrere Meldeauflagen für jeden einzelnen Spieltag.

Warum dies einen Unterschied macht, kann wiederum ein Beispiel zeigen: Im Laufe von drei Monaten finden vier solche Spiele statt, wobei aber zwischen dem zweiten und dritten der Spiele ein Zeitraum von vier Wochen liegt, in dem kein solches Spiel angesetzt ist. Bei einer Meldeauflage über die Dauer von drei Monaten müsste sich die Person aber auch in diesen Wochen melden und könnte zum Beispiel keine auswärtige Geschäftsreise unternehmen.

Problematisch ist in Zusammenhang mit der Anordnung längerfristiger Meldeauflagen, dass Widersprüche nach § 56 b Abs. 2 S. 3 keine aufschiebende Wirkung haben sollen, so dass Personen, die sich dagegen wenden, verwaltungsgerichtliche Eilverfahren durchführen müssten, um eine Aufhebung der Meldeauflage für bestimmte Zeiträume zu erreichen.

Die Höchstgrenze für Meldeauflagen muss vor diesem Hintergrund deutlich verkürzt werden. Alternativ müsste mindestens klarstellend ein Passus eingefügt werden, dass eine Meldeauflage, die einen längeren Zeitraum als 48 Stunden betrifft, nur dann verhängt werden darf, wenn die Prognose gestellt werden kann, dass für jeden einzelnen der Tage in dem gesamten Zeitraum die Gefahr besteht, dass Straftaten begangen werden.

Zu weitgehend ist in diesem Zusammenhang auch die geplante neue Regelung des § 55 Abs. 1 Nr. 5, wonach zur Durchsetzung von Meldeauflagen Gewahrsam angeordnet

werden kann. Gilt eine Meldeauflage über einen langen Zeitraum hinweg, ist die Wahrscheinlichkeit, dass ein einzelner Meldetermin verpasst wird, größer als bei einer kurzfristigen Maßnahme. Dass in so einem Fall gleich Gewahrsam droht, bedeutet eine übermäßige Freiheitseinschränkung.

3. Besondere Mittel der Datenerhebung § 33 Abs. 1 i.V.m. Abs. 2 S. 2 Nr. 2

In Bezug auf die Regelung zu besonderen Mitteln der Datenerhebung nach § 33 Abs. 1 ist zunächst ausdrücklich zu begrüßen, dass mit § 33 a ein Richtervorbehalt eingeführt worden ist.

Kritikwürdig ist jedoch die sehr weitgehende Einbeziehung von Kontaktpersonen und der nicht ausreichende Schutz Dritter.

Nach § 33 Abs. 2 S. 2 Nr. 2 darf jede einzelne der Maßnahmen (sei es eine längerfristige Observation oder der Einsatz von verdeckt ermittelnden Polizeibeamten) auch gegen Kontaktpersonen nach § 27 Abs. 3 Nr. 2 eingesetzt werden, also gegen Personen, von denen selbst keine Gefahr ausgeht, von denen die Polizei nur annimmt, dass sie zum Beispiel Kenntnis von Planungen anderer haben. Wie bereits in den einleitenden Bemerkungen ausgeführt, verschiebt eine solche Erweiterung des Kreises von Personen, die tief greifenden und heimlichen Überwachungsmaßnahmen ausgesetzt sein dürfen, über den Kreis der tatsächlich gefährlichen Personen hinaus das Grundgefüge der Gesellschaftsordnung. Wenn es solche Kompetenzen gibt, wonach zum Beispiel ein verdeckter Ermittler auf die Freundin oder die Familie einer gefährlichen Person angesetzt werden dürfte, kann in der Bevölkerung ein allgemeines Gefühl der möglichen Überwachung entstehen. Dies ist mit Blick auf eine freiheitliche Gesellschaft unbedingt zu vermeiden.

Erst recht gilt dies für mitbetroffene Dritte. Nach § 33 Abs. 4 dürfen solche Maßnahmen auch eingesetzt werden, wenn Dritte unvermeidbar mitbetroffen sind – was im Übrigen in der Praxis auch regelmäßig der Fall ist, da solche längerfristigen heimlichen Maßnahmen das gesamte Leben der Zielperson begleiten, in dem immer auch Dritte eine Rolle spielen, seien es Kinder und andere Verwandte, Nachbar*innen, Geschäftspartner*innen, Freund*innen, Mitbewohner*innen, Lehrer*innen, Verkäufer*innen etc.

4. Verschiedene Formen der Telekommunikationsüberwachung (insb. Onlinedurchsuchung und Quellen-TKÜ §§ 33 c, 33 d)

Aus der Erfahrung der im RAV organisierten Rechtsanwältinnen und Rechtsanwälte besteht in Bezug auf die Überwachung der Telekommunikation neben den strafprozessualen Befugnissen schon kein weiterer Bedarf an entsprechenden Eingriffsgrundlagen. Bei konkreten Planungen schwerwiegender Taten ist schon jetzt die strafprozessuale Überwachung nach den §§ 100 a StPO ff. möglich (vgl. § 89a StGB). Ein darüber hinaus bestehender Bedarf für eine Landespolizei ist – wie bereits in den einleitenden Bemerkungen ausgeführt – äußerst fraglich.

Zur präventivpolizeilichen Online-Durchsuchung durch das BKA hat ein Gutachten des Max-Planck-Instituts für Ausländisches und Internationales Strafrecht⁶ ergeben, dass in fünf Jahren überhaupt nur in **zwei** Fällen insgesamt fünf derartige Anordnungen nach § 20k BKAG a.F. ergingen. Aufgrund von technischen Problemen führte nur eine dieser fünf Anordnungen letztlich auch dazu, dass Daten von insgesamt zwei Zielsystemen ausgeleitet wurden, wobei insgesamt ca. 70.000 Inhalte erhoben wurden – allerdings keine verfahrensrelevanten Daten.⁷ Explizit festgestellt wurde in dem Gutachten auch, dass es sich um eine zeitaufwändige und vorbereitungsintensive Maßnahme handelt. Dasselbe gilt für die Quellen-TKÜ, bei der die Entwicklung der Überwachungsmittel regelmäßig so arbeits- und zeitintensiv ist, dass sie bei Fertigstellung bereits veraltet sind.⁸

Das spricht nicht nur dagegen, dass für die Einführung einer präventivpolizeilichen Kompetenz zur Online-Durchsuchung überhaupt ein Bedarf bei der Landespolizei Mecklenburg-Vorpommern besteht. Es erscheint auch fraglich, dass – würde sie eingeführt – überhaupt die Mittel dafür vorhanden wären, die Kompetenz auch einzusetzen.

Es spricht auch dagegen, dass Eilkompetenzen – wie in § 33 c Abs. 10 und 33 d Abs. 4 vorgesehen – überhaupt notwendig sind. Es ist schon kaum ein Fall vorstellbar, in dem eilig gehandelt werden muss, aber noch die Erstellung einer Überwachungs-Software abgewartet werden kann. Denn weder Online-Durchsuchung noch Quellen-TKÜ können innerhalb kurzer Zeit umgesetzt werden. Während der Erarbeitung der technischen Tools kann aber ohne weiteres auch ein Antrag an das Gericht formuliert werden. Das sieht im Übrigen auch das BKA so.⁹

6 BT-Drs. 18/13031, S. 23.

7 BT-Drs. 18/13031, S. 38.

8 BT-Drs. 18/13031, S. 40.

9 Laut Gutachten des MPI, BT-Drs. 18/13031, S. 42.

Zu den technischen Problemen, bei der Quellen-TKÜ das verfassungsrechtliche Gebot zu erfüllen, dass ausschließlich die laufende Kommunikation überwacht wird,¹⁰ werden hier keine weiteren Ausführungen gemacht – gleichwohl sei angemerkt, dass dies auch in den Augen der Anwältinnen und Anwälte des RAV eines der Hauptprobleme dieser Ermittlungsmethode darstellt.

Ein anderes Problem stellt sich bei den Kompetenzen für Online-Durchsuchung und Quellen-TKÜ nach dem Gesetzentwurf gleichermaßen: Der Schutz des Kernbereichs privater Lebensgestaltung ist für beide Kompetenzen in § 26 a nicht hinreichend gewährt. Dies gilt insbesondere in der Auswertungsphase, in der die aus den heimlichen Maßnahmen gewonnenen Daten analysiert werden. Hier ist vom Bundesverfassungsgericht in Bezug auf die Online-Durchsuchung nach dem BKAG entschieden worden, dass die Regelung des § 20 Abs. 7 Satz 3 und Satz 4 BKAG a.F. verfassungswidrig war, wonach die Daten durch den Datenschutzbeauftragten und weitere Bedienstete des BKA auf ihren Kernbereichsgehalt gesichtet werden sollten.¹¹ Hierzu hat das Bundesverfassungsgericht festgehalten, dass die verfassungsrechtlich gebotene Sichtung durch eine unabhängige Stelle maßgeblich dem Ziel dient, kernbereichsrelevante Daten so frühzeitig herauszufiltern, dass sie den Sicherheitsbehörden nach Möglichkeit nicht offenbar werden und dass das wiederum voraussetzt, dass die Kontrolle im Wesentlichen von externen, nicht mit Sicherheitsaufgaben betrauten Personen wahrgenommen wird, weshalb also eine Kontrolle durch behördeninterne Datenschutzbeauftragte nicht ausreichend ist.¹² Auch die »Sachleitung« eines Gerichts genügt (diesen Anforderungen) nicht.

Sollte also – entgegen allem oben Gesagten – daran festgehalten werden, dass in einer Änderung des SOG auch Kompetenzen zur Online-Durchsuchung und zur Quellen-TKÜ eingeführt werden, muss eine Regelung eingeführt werden, wonach ein Gericht mit diesen Methoden erhobene Daten vor der Auswertung durch die Polizei auf etwaige kernbereichsrelevante Inhalte hin überprüft und die Löschung dieser kernbereichsrelevanten Inhalte vornimmt.¹³

5. Gezielte Kontrolle - § 35 Abs. 2

10 BVerfG, Urteil 27.02.2008, 1 BvR 370/07, 1 BvR 595/07.

11 BVerfG, Urteil 20.04.2019, 1 BvR 966/09, Rn. 223.

12 BVerfG, Urteil 20.04.2019, 1 BvR 966/09, Rn. 224f.

13 Hierbei ist auf die Einhaltung ausreichender Aufbewahrungsfristen für die Lösungsprotokolle zu achten: BVerfG, Urteil 20.04.2019, 1 BvR 966/09, Rn. 226.

Die Einführung einer Kompetenz zur gezielten Kontrolle von Personen, die zur polizeilichen Beobachtung ausgeschrieben sind, ist nicht verfassungsgemäß. Mit dieser Kompetenz wird die Möglichkeit zur Identitätsfeststellung und Durchsuchung von den dafür vorgesehenen gesetzlichen Voraussetzungen (siehe §§ 29, 53 und 57 SOG MV) abgekoppelt und weit ins Vorfeld tatsächlich bestehender Gefahren verlagert und auf Personen ausgeweitet, von denen keine Gefahr ausgeht. Es darf dann zum Beispiel die Identität jeder Person überprüft werden, die sich in einem Fahrzeug befindet, von dem angenommen wird, dass dieses Fahrzeug auch eine Person nutzt, von der angenommen wird, dass sie erhebliche Straftaten begehen wird.

Um eine überschießende Überwachung mit den in der einführenden inhaltlichen Anmerkung dargelegten Folgen für die Gesellschaft zu vermeiden, ist auf die Einführung dieser Regelung zu verzichten. So ist zum Beispiel in Sachsen-Anhalt die Ausschreibung zur polizeilichen Beobachtung geregelt (§ 19 Abs. 1 und 2 SOG LSA), dann aber explizit verfügt (19 Abs. 3 SOG LSA):

Gegen eine Person, die unter polizeilicher Kontrolle steht oder ein nach Absatz 1 ausgeschriebenes Kraftfahrzeug führt, sind beim Antreffen andere Maßnahmen nur zulässig, wenn jeweils die besonderen rechtlichen Voraussetzungen für diese Maßnahmen erfüllt sind.

So sollte nach Ansicht des Republikanischen Anwältinnen- und Anwaltsvereins auch die Regelung in Mecklenburg-Vorpommern gestaltet werden.

6. Rasterfahndung - § 44

Aus dem bereits in Bezug auf Online-Durchsuchung und Quellen-TKÜ zitierten Gutachten des Max-Planck-Instituts für Ausländisches und Internationales Strafrecht ergibt sich auch, dass eine Kompetenz für die Durchführung von präventivpolizeilichen Rasterfahndungen in der Praxis nicht benötigt wird. Die Rasterfahndung nach § 20j BKAG a.F. wurde in den fünf Jahren nach ihrer Einführung im Jahr 2009 vom BKA genau einmal eingesetzt.¹⁴

Außerdem gilt wiederum das in Bezug auf Online-Durchsuchung und Quellen-TKÜ ebenso Gültige: Eine Eilkompetenz ist nicht erforderlich, weil eine Rasterfahndung lange und aufwändige Vorbereitung erfordert.¹⁵

14 BT-Drs. 18/13031, S. 21.

15 BT-Drs. 18/13031, S. 42.

B. Ergänzende kurze Anmerkungen und redaktionelle Hinweise

zu § 25 b: Soweit im Gesetz vorgesehen ist, dass gerichtliche Entscheidungen auch ohne Anhörung und Bekanntgabe wirksam werden können, ist übersehen worden, eine flankierende Regelung zur nachträglichen Unterrichtung einzufügen, sobald eine Information über die Maßnahme die Erreichung ihres Ziels nicht mehr gefährdet.

zu § 26 b Abs. 2: Es gilt das bereits mehrfach Gesagte: Nicht jede Regelung des BKAG ist für jedes Land erforderlich. Aus Sicht des RAV ist es nicht nachvollziehbar, welchen Grund es dafür geben sollte, den Schutz von vertraulichen Gesprächen mit nicht-anwaltlichen Berufsgeheimnis-Träger*innen wie Ärzt*innen, Seelsorger*innen etc. so weit erodieren zu lassen, wie es § 26 b Abs. 2 vorsieht. Die Regelung ist zu streichen.

zu § 45 a: Es ist zu begrüßen, dass mit § 45 a nunmehr eine gesetzliche Regelung für Aussonderungsprüffristen gespeicherter personenbezogener Daten vorgesehen wird. Es wird angeregt, neben den genannten Fristen explizit eine Frist zur Aussonderungsprüffrist in Bagatellfällen von drei Jahren einzuführen.

zu 48 Abs. 5: Offenbar ist übersehen worden, dass bei Auskunftsverweigerung neben der Kontrolle durch die oder den Datenschutzauftragte/n auch eine Kontrolle im verwaltungsgerichtlichen Verfahren in Betracht kommt. Es ist zu ergänzen, dass die dokumentierten Gründe auch dahin zu übermitteln sind bzw. eine Sperrerklärung abzugeben ist.

zu § 57 Abs. 2: Während bei der Regelung zur Sicherstellung (§ 61) im Entwurf ein Richtervorbehalt vorgesehen ist, fehlt er bei der Regelung der Durchsuchung von elektronischen Speichermedien nach § 57 Abs. 2. Ein Richtervorbehalt ist aber aufgrund der Grundrechtseingriffstiefe einer Durchsuchung von elektronischen Speichermedien, bei denen eine Kernbereichsrelevanz regelmäßig auf der Hand liegt, nicht verzichtbar.

Berlin, den 09. August 2019