Anlage

Landesbeauftragte
für Datenschutz
und Akteneinsicht

Stellungnahme der LDA Brandenburg

zur Anhörung im Ausschuss für Inneres und Kommunales des Landtages Brandenburg am 9. Januar 2019 zum Gesetzentwurf der Landesregierung (Drs. 6/9821) und dem Gesetzentwurf der CDU-Fraktion (Drs. 6/9828):

Zwölftes Gesetz zur Änderung des Brandenburgischen Polizeigesetz

---

Einleitung

Die mir vorgelegten Gesetzentwürfe zur Änderung des Brandenburgischen Polizeigesetzes, der Regierungsentwurf und der Entwurf der CDU –Fraktion, unterscheiden sich erheblich. Während der Regierungsentwurf sich ausschließlich auf polizeiliche Befugnisse konzentriert, beinhaltet der Fraktionsentwurf zugleich die Umsetzung der Richtlinie (EU) 2016/680 (JI-RL). Dadurch wurde dieser Entwurf nicht nur im Umfang erheblich erweitert. Er zeichnet sich durch eine klare Strukturierung und Neuordnung des gesamten Polizeirechts aus, die ich in weiten Teilen als gelungen ansehe und begrüße. Aus Gründen der größeren Praxistauglichkeit halte ich es jedoch für vorzugswürdig, die Vorgaben der EU-Richtlinie für ihren gesamten Anwendungsbereich (Gefahrenabwehr, Straftatenverhütung, - verfolgung, -vollstreckung, Straf- und Maßregelvollzug) einheitlich in einem gesonderten Gesetz zu regeln, wie es derzeit in einem Gesetzentwurf der Polizei, Justizvollzugs und Maßregelvollzugsdatenschutzgesetzes (BbgPJMDSG) vorbereitet wird. Dadurch können viele Regelungen übersichtlich, quasi vor die Klammer gezogen werden, anstatt sie in jedes der Fachgesetze einzufügen.

Im Vergleich zu dem im Juli 2018 veröffentlichten ersten Gesetzentwurf der Landesregierung wurde der vorliegende verschlankt. Einige weitreichende Eingriffsbefugnisse wie die Elektronische Aufenthaltsüberwachung zur Abwehr von Gefahren des Terrorismus und die sog. Online Durchsuchung wurden aus dem Regierungsentwurf entfernt. Der CDU Entwurf enthält dagegen nicht nur diese Eingriffsbefugnisse, sondern erlaubt in vielen einzelnen Regelungen Eingriffe unter geringeren Voraussetzungen, für weniger gewichtige Schutzgüter und über längere Zeiträume. Beide Entwürfe setzen überwiegend konsequent die Vorgaben des Bundesverfassungsgerichtsurteils vom 20. April 2016 um.

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht
Stahnsdorfer Damm 77 · 14532 Kleinmachnow · E-Mail: Poststelle@LDA.Brandenburg.de · www.LDA.Brandenburg.de
Fingerprint: E899 5780 7F65 F282 8CAC C504 37F3 83FE 0844 834D

Dennoch enthält auch der Regierungsentwurf eine deutliche Ausweitung polizeilicher Datenverarbeitungsbefugnisse und wirft erhebliche freiheits- und datenschutzrechtliche Bedenken auf. Um das Ausmaß anschaulich zu machen, erlaube ich mir eine kurze Aufzählung. Der Entwurf schafft zahlreiche neue Eingriffsbefugnisse für die Polizei: die Meldeauflage (§ 15a), die erkennungsdienstliche Behandlung, anlassbezogene Kennzeichenfahndung, Ausschreibung und verdeckte Registrierung zur Abwehr von Terrorgefahr (§ 28b), Aufenthaltsvorgaben und Kontaktverbote (§ 28c), Gewahrsam zur Verhinderung einer Straftat (§ 28d), die verdeckte Datenerhebung durch Eingriffe in informationstechnische Systeme durch Telekommunikationsüberwachung (§ 28e), und der Einsatz von Körperkameras im öffentlich zugänglichen Raum (§ 31a). Schwerwiegend ist der neue Abschnitt 1a, der explizit die Abwehr von Gefahren des Terrorismus als Aufgabe der Polizei festlegt (§ 28a) und damit zusammenhängend einen „nicht konkretisierten Gefahrenbegriff“ als Eingriffsschwelle für polizeiliches Handeln einführt. Darüber hinaus sollen bestehende Befugnisse verschärft werden, etwa durch die räumliche Ausweitung von Identitätsfeststellungen zur Bekämpfung der grenzüberschreitenden Kriminalität (§ 12), durch die Verlängerung von Speicherfristen bei Videoüberwachungen im öffentlichen Raum (§ 31) und Bild- und Tonaufzeichnungen zur Eigensicherung (§ 31a). Auch die maximale Dauer bei Observationen (§ 32) wird verlängert.

Eine Reihe von Befugnissen greifen massiv in Freiheitsrechte ein, wie etwa die Möglichkeit, im Vorfeld von feststellbaren konkreten Gefahren Aufenthaltsvorgaben und Kontaktverbote zu verhängen, und bei Zuwiderhandlungen eine vorsorgliche Ingewahrsamsnahme für bis zu 2 Wochen zu ermöglichen.
Auch die Ausweitung polizeilicher Waffen, die der Polizei gestattet, Sprengmitteln gegen Personen einzusetzen (§ 69) gehört dazu. Diese Regelungen stellen jedoch im Kern keine Verletzungen des informationellen Selbstbestimmungsrechts dar und sind daher meiner Beurteilung entzogen.

Mit fast jedem Änderungsgesetz wurden Datenverarbeitungsbefugnisse der brandenburgischen Polizei erweitert, niemals reduziert. Die Kumulation neuer Befugnisse und das Herabsenken der Einschreitschwellen auf einen Zeitpunkt, in dem (noch) keine konkrete Gefahr vorliegt, erhöhen die Datenmengen und haben inzwischen ein Ausmaß erreicht, das mir Sorge bereitet. Gerade letzteres wirft die Frage auf, ob Brandenburg mit dem Gesetzentwurf nicht bereits nahe an eine flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten herankommt. Einer darauf zielenden Absicht hat das Bundesverfassungsgericht bereits 2010 in der Entscheidung zur Vorratsdatenspeicherung eine Absage erteilt.

Der Gesetzgeber hat Vorsorge dafür zu tragen, dass nicht alle Aktivitäten der Bürger erfasst werden können, und muss gerade beim Einsatz moderner Technik, die dem Betroffenen verborgen bleibt, mittels besondere Verfahrensanforderungen der Gefährdung durch „additive Grundrechtseingriffe“ begegnen[1]. 2016 äußerte sich das Bundesverfassungsgericht in seinem Urteil zum BKA-Gesetz erneut deutlich: „Mit der Menschenwürde unvereinbar ist es, wenn eine Überwachung sich 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.“[2]. Ich mahne daher eine Gesamtbetrachtung aller polizeilichen - insbesondere heimlicher - Überwachungsmaßnahmen an.

Die Stellungnahme bezieht sich auf den Gesetzentwurf der Landesregierung (BbgPolG-RegE) und geht bei einzelnen Vorschriften auf Regelungen des CDU Gesetzentwurfs (BbgPolG-CDU-E) ein.

Die im Gesetzentwurf der Landesregierung vom Juli 2018 enthaltenen eingeschränkte Befugnis für **Molekulargenetische Untersuchungen zur Identitätsfeststellung (§ 12a BbgPolG-RegE alt) wurden in der vorliegenden Fassung nicht aufgenommen. Wir hatten der Analyse,** auf das DNA-Identifizierungsmuster (sog. genetischer Fingerabdruck, der nur nicht kodierter Teile der DNA umfasst) und die Feststellung des Geschlechts begrenzt war, zugestimmt, weil sie dem Untersuchungsumfang des § 81e StPO entsprach. Es ist jedoch vorzugswürdig ganz darauf zu verzichten.

Die in der ersten Entwurfsfassung der Landesregierung in § 28d BbgPolGE vorgesehene **elektronische Aufenthaltsüberwachung (EAÜ) zur Abwehr von Gefahren des Terrorismus** wurde nicht in den vorliegenden Regierungsentwurf übernommen. Wir begrüßen dies ausdrücklich, weil wir den Einsatz der EAÜ als Mittel zur Überwachung im Bereich der präventiven Gefahrenabwehr für nicht ausreichend begründet hielten.

Der Gesetzentwurf der CDU Fraktion beinhaltet diese Befugnis jedoch in § 45 in einer darüber noch hinausgehenden Variante. Die EAÜ soll danach zur allgemeinen Gefahrenabwehr oder zur Verhütung besonders schwerer Straftaten oder schwerwiegender Kriminalitätsphänomene eingesetzt werden können.

Nach meinen Kenntnissen ist nicht belegt, dass die bisher nur im Rahmen der Führungsaufsicht in geringer Zahl erprobte Überwachungsmaßnahme zur Gefahrenab-

[1] BVerfG Urteil vom 12.04.2005, 2 BvR 581/01 Rn. 60
[2] vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, Rn.130

wehr überhaupt geeignet ist. Die Gesetzesbegründung stellt dazu lediglich ohne jede Erläuterung fest, dass im Zusammenwirken mit Aufenthaltsbestimmungen; Meldeauflagen und dem Erstellen von Bewegungsbildern ein erhebliches Potential zur Aufdeckung terroristischer oder sonst extremistischer Strukturen entsteht.

Angesichts der geringen Forschungserkenntnisse zur Wirksamkeit dieser Maßnahme bzw. erster ernüchternder Auswertungen der Maßnahme bei Führungsaufsicht[3] ist äußerste Zurückhaltung bei der Ausweitung des Einsatzes geboten. Es bestehen tiefgreifende Zweifel an der Verfassungsgemäßheit der Ausgestaltung der elektronischen Aufenthaltsüberwachung. Die EAÜ stellt einen ein äußerst weitreichender Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen, der sich – obwohl offen gestaltet – in seiner Wirkung auf das Persönlichkeitsrecht mit einer heimlichen durchgeführten Überwachung bzw. Observation vergleichen lässt. Die Maßnahme lässt aufgrund der rund um die Uhr übermittelten Daten Rückschlüsse auf den Aufenthaltsort und damit auch auf das Privatleben des Trägers zu. Besuche im öffentlichen Raum werden ebenso dokumentiert wie Besuche bei Freunden, Ärzten oder anderen Berufsgeheimnisträgern. Auch der Besuch von weltanschaulichen oder religiösen Veranstaltungen und Versammlungen wird aufgezeichnet. Da Aufenthaltsdaten in einem langfristigen Zeitraum von bis zu drei Monaten erhoben werden dürfen, werden nicht nur einzelne Situationen erfasst, sondern es lässt sich ein detailliertes Bild über das Privatleben der Person zusammensetzen und ein Bewegungsprofil erstellen. Diese Eingriffe in das Persönlichkeitsrecht stehen in keinem angemessenen Verhältnis zu dem belegten Nutzen dieser Maßnahme.

Zu den Befugnissen im Einzelnen:

zu Nr. 1: § 12 BbgPolG-RegE (Identitätsfeststellung)

Mit der Änderung des § 12 Abs. 1 Nr. 6 BbgPolG-RegE soll es der Polizei ermöglicht werden, unter den dort genannten Voraussetzungen nicht nur im brandenburgischen Gebiet der Bundesgrenze bis zu einer Tiefe von 30 Kilometern, sondern auch auf den

[3] Empirische Studie: Bräuchle/Kinzig, Die elektronische Aufenthaltsüberwachung im Rahmen der Führungsaufsicht, Kurzbericht über die wesentlichen Befunde einer bundesweiten Studie mit rechtspolitischen Schlussfolgerungen, S. 16; Bräuchle, in: Kinzig/Kerner, Tübinger Schriften und Materialien zur Kriminologie, Die elektronische Aufenthaltsüberwachung gefährlicher Straftäter im Rahmen der Führungsaufsicht, S. 164 f.

Durchgangsstraßen (Bundesautobahnen, Europastraßen und anderen Straßen von erheblicher Bedeutung für den grenzüberschreitendende Kriminalität) und in öffentlichen Einrichtungen des internationalen Verkehrs die Identität einer Person festzustellen, sog. Schleierfahndung. Dies wird damit begründet, dass der 30-Kilometer-Korridor allein der aktuellen Lage im Zusammenhang mit der Mobilität der Bevölkerung und potenzieller Straftäter nicht gerecht werde und dass eine effektive Gefahrenabwehr der Polizei nur sehr eingeschränkt möglich sei.

Die bereits in der ersten Entwurfsfassung (vom Juli 2018) enthaltene Ausweitung der Befugnisse zur Identitätsfeststellung habe ich in meiner Stellungnahme vom 9. August 2017 kritisiert. Eine noch größere Zahl von Personen grundsätzlich ereignis- und verdachtsunabhängig zu kontrollieren und damit in ihrem Recht auf informationelle Selbstbestimmung erheblich zu beeinträchtigen, war aus meiner Sicht nicht nachvollziehbar gerechtfertigt. Die neue Regelung wird unter anderem damit begründet, dass die grenzüberschreitende Kriminalität dort bekämpft werden soll, wo sie weitestgehend geschieht, nämlich gerade auf den genannten Straßen und in den öffentlichen Einrichtungen des internationalen Verkehrs.

Während die vorangegangene Gesetzesbegründung dies nur pauschal behauptete, findet sich in der vorliegenden Version eine längere Passage, die zu einzelnen Deliktsbereichen erläutert, weshalb die Ausweitung aus polizeilicher Sicht als geeignet und notwendig angesehen wird, um die grenzüberschreitende Kriminalität zu bekämpfen. Hier werden Ermittlungserkenntnisse und Zahlen der vergangenen Jahre in Bezug auf die grenzüberschreitende Eigentumskriminalität, speziell Diebstahl aus Wohnräumen, aber auch zu Kfz- Diebstählen, Ladungsdiebstählen auf Parkplätzen und Raststätten als auch die Rauschgiftkriminalität genannt, bei denen die Verkehrsinfrastruktur eine große Rolle spielt. Diese Ausführungen lassen es erstmals plausibel erscheinen, dass Kriminalitätsphänomene wie „reisende Täter“ und arbeitsteilig agierende Tätergruppen, die die Tatbegehung oft flexibel gestalten in einem Transitland für Im- und Export durch eine Erweiterung der Kontrollbefugnisse auf die genannten Straßen und öffentlichen Einrichtungen des internationalen Verkehrs wirksamer bekämpft werden könnten.

Hinzu kommt, dass der Gesetzentwurf den Begriff der Durchgangsstraßen wieder enger definiert, indem außer Bundesautobahnen und Europastraßen **sonstige Straßen** nur dann als kontrollfähig anzusehen sind, wenn sie von erheblicher Bedeutung für die

grenzüberschreitende **Kriminalität** sind. Es muss daher nicht nur ein Bezug zu grenzüberschreitendem Verkehr, sondern zu vorangegangenem strafbarem Verhalten bestehen, wodurch der Begriff ein eingrenzendes und nachprüfbares Merkmal erhält. Die Ausweitung auf den „öffentlichen Verkehrsraum“ insgesamt, wie es § 15 Abs. 1 Nr. 6 BbgPolG-CDU-E vorsieht, sehe ich als zu weitreichend und unbestimmt an.

Das dargelegte abstrakte Gefahrenpotential für geschützte Rechtsgüter entlang oder unter Ausnutzung bestimmter Verkehrswege und Einrichtungen ist immer gegen die Belastung des einzelnen Betroffenen durch verdachtsunabhängige Identitätskontrollen abzuwägen, die unterschiedslos jede Person, die sich dort aufhält, treffen kann. Vor dem Hintergrund der im Gesetzentwurf erläuterten sachlichen Zusammenhänge zwischen erhöhter Kontrolldichte und vorbeugender Bekämpfung der grenzüberschreitenden Kriminalität halte ich die geographische Ausweitung der Gebiete für Identitätskontrollen für vertretbar. Der Regierungsentwurf spricht in § 12 BbgPolG davon, dass für die Auswahl der Kontrollgebiete „polizeiliche Erkenntnisse“ maßgeblich sind, bei denen es sich laut Begründung um **nachweisbare** Erkenntnisse handeln muss. Ich empfehle, dies aus Klarstellungsgründen in den Normtext ergänzend aufzunehmen, um der restriktiven Auslegung der Befugnis zu mehr Geltung zu verhelfen.

zu Nr. 4: § 15a BbgPolG-RegE (Meldeauflage)

Mit der Einführung des § 15a BbgPolG-RegE wird eine eigenständige Rechtsgrundlage für Meldeauflagen geschaffen, sodass diese nicht mehr unter die Generalklausel fallen. Im Sinne der Normenklarheit für den einzelnen Bürger begrüße ich dies. Darüber hinaus wurde der Begriff der Straftat, in der jetzigen Fassung konkretisiert. Im Verhältnis zum ersten Entwurf, in dem eine Meldeauflage ergehen konnte, wenn Tatsachen die Annahme rechtfertigten, dass die Person eine Straftat begehen wird und die Meldeauflage zur vorbeugenden Bekämpfung der Straftat erforderlich ist, sind jetzt nur noch Straftaten gegen Leib oder Leben oder eine Straftat nach den §§ 125, 125a des Strafgesetzbuches oder nach den §§ 26, 27 oder 28 des Versammlungsgesetzes von der Vorschrift erfasst. Dies stellt meines Erachtens hinreichend sicher, dass nicht jede beliebige Straftat dazu führen kann, dass eine Person meldepflichtig wird, ihren Aufenthaltsort zu vorgegebenen Zeiten der Polizei mitzuteilen und somit in ihrem Recht auf informationelle Selbstbestimmung in unverhältnismäßiger Weise beeinträchtigt wird. Ich begrüße zudem, dass die Ermächtigung Meldeauflagen nicht bereits im Vor-

feld einer Gefahr zulässt, sondern die auf Tatsachen beruhende Prognose voraussetzt, dass die betroffene Person eine Straftat begehen wird.

Gerade deshalb halte ich die Fassung des § 19 Abs. 1 BbgPolG-CDU-E für zu weitgehend. Die Meldeauflage wird dort zwar auch zur Abwehr einer konkreten Gefahr, wie sie nach der erweiterten Definition in § 3 Nr. 4 BbgPolG-CDU-E verstanden wird, zugelassen, sie soll darüber hinaus aber auch zur Verhütung oder vorbeugenden Bekämpfung von Ordnungswidrigkeiten von erheblicher Bedeutung möglich sein. Dies halte ich angesichts der des erheblichen Eingriffs in die Handlungsfreiheit der Betroffenen für unverhältnismäßig.

zu Nr. 12: Abschnitt 1a, §§ 28a ff BbgPolG-RegE (Besondere Befugnisse zur Abwehr von Gefahren des Terrorismus)

Mit dem neu eingefügten Abschnitt 1a wird als besondere Aufgabe der Polizei die Abwehr von Gefahren des Terrorismus festgelegt. Welche Tathandlungen darunter zu verstehen sind, legt § 28a Abs. 1 BbgPolG-RegE fest, der bis auf den in Brandenburg nicht vorhandenen Begriff „international“ wortgleich der Definition in § 5 Abs.1 Bundeskriminalamtgesetz entspricht. Neben den in den nachfolgenden Paragrafen geregelten neuen polizeilichen Befugnissen besteht eine wesentliche Verschärfung darin, dass die polizeiliche Eingriffsschwelle bei diesen Straftatbeständen massiv herabgesetzt wird.

In den Befugnissen nach §§ 28b, c, d und e BbgPolG-RegE werden polizeiliche Eingriffe, u. a. Datenerhebungen, bereits im Vorfeld einer konkreten Rechtsgutgefährdung erlaubt, wenn

- bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Rechtsgutschädigung begehen wird oder
- ihr individuelles Verhalten die konkrete Wahrscheinlichkeit einer Rechtsgutsschädigung in übersehbarem Zeitraum begründet.

Die Formulierungen übernehmen den Wortlaut aus dem Urteil des Bundesverfassungsgerichts zum Bundeskriminalamtsgesetz vom 20. April 2016, auf dessen Umsetzung auch in der Begründung des Gesetzentwurfs Bezug genommen wird. Zwar hat

das Bundesverfassungsgericht in dem Urteil zum Zweck der Straftatenverhütung unter bestimmten Voraussetzungen reduzierte Vorhersehbarkeitsanforderungen für Kausalverläufe, die zu Gefahren führen können, für verfassungsgemäß erklärt, dabei aber auch die äußerste Grenze verfassungskonformer Grundrechtseingriffe zur Gefahrenabwehr formuliert.

Die Einführung des Abschnitts 1a mit den geplanten besonderen Befugnissen zur Abwehr von Gefahren des Terrorismus führt dazu, dass polizeiliche Eingriffe und dadurch ggf. auch Datenerhebungen bereits im Vorfeld einer konkreten Rechtsgutsgefährdung erlaubt werden. Ich habe erhebliche Zweifel, dass diese Änderung noch verfassungsmäßig ist. Es entsteht der Eindruck, dass das Polizeirecht immer weiter dem Recht des Verfassungsschutzes angeglichen werden soll. Mit der zeitlichen Vorverlagerung der Eingriffsbefugnisse erfolgt eine enorme Ausweitung des betroffenen Personenkreises. Wie in der vorangegangenen Version übernimmt der Entwurf die Begriffe weiterhin wortwörtlich, ohne konkrete Ausfüllung oder Definitionen, aus dem Urteil des Bundesverfassungsgerichts zum BKA-Gesetz.

Das Bundesverfassungsgericht hat in seinem Urteil zum BKA-Gesetz zwar dargelegt, dass der Gesetzgeber nicht von vornherein für jede Art der Aufgabenwahrnehmung auf die Schaffung von Eingriffstatbeständen beschränkt ist, die dem tradierten sicherheitsrechtlichen Modell der Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren entsprechen. Für bestimmte Bereiche, die schon die Straftatenverhütung bezwecken, können die Grenzen auch weiter gezogen werden, indem die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert werden (Rn. 112 d. Urteils). Allerdings bedarf es auch bei Maßnahmen zur Straftatenverhütung zumindest einer auf bestimmte Tatsachen und nicht allein auf allgemeine Erfahrungssätze gestützten Prognose, die auf eine konkrete Gefahr bezogen ist. Grundsätzlich gehört hierzu, dass insoweit ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist (Rn. 164 d. Urteils, vgl. auch BVerfGE 110, 33 <56 f., 61>; 113, 348 <377 f.>; 120, 274 <328 f.>; 125, 260 <330>). Bei terroristischen Straftaten kann stattdessen aber auch darauf abgestellt werden, ob das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft terroristische Straftaten begeht. Die Anforderungen hierfür sind in einem Gesetz normenklar zu regeln.

Die Regelung des Gesetzentwurfs geht über diese abgesteckten Grenzen hinaus. Die durch das Bundesverfassungsgericht entwickelten Vorgaben für eine vorverlagerte Einschreitschwelle im Vorfeld einer Gefahr stellen eine maximale Grenze dar. Sie wurden vom Gericht bei **Überwachungsmaßnahmen** zum Schutz **überragend wichtiger Rechtsgüter** als zulässig betrachtet (Rn 111 d. Urteils). Im vorliegenden Entwurf werden aber unter den Voraussetzungen des neuen Gefahrenbegriffs auch Maßnahmen wie Aufenthaltsvorgaben und Kontaktverbote, § 28 c Abs. 1 BbgPolG-ReGE, geregelt. Zum anderen ermöglicht der Verweis in § 28b Abs. 1 und § 28c Abs. 1 Nr. 2 BbgPolG-RegE auf eine Straftat nach § 28a Abs. 1 BbgPolG-RegE, dass unterhalb der Schwelle „überragend wichtiger Rechtsgüter" der Gefahrenbegriff zur Anwendung kommt. Gemäß § 28a Abs. 1 BbgPolG-RegE umfassen die Gefahren des Terrorismus auch Straftaten, die dazu bestimmt sind, die Bevölkerung auf erheblicher Weise einzuschüchtern oder eine Behörde /internationale Organisation rechtswidrig z. Bsp. durch Drohung zu nötigen. Diese Taten sind nicht gleichzusetzen, mit Gefahren für Leib, Leben oder Freiheit einer Person, oder Gütern der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Letztere sind als überragend wichtiger Rechtsgüter verfassungsgerichtlich anerkannt.

Die im Gesetzesentwurf reduzierten Anforderungen für eine Eingriffsbefugnis gehen für alle unter diesem Abschnitt geführten Maßnahmen über die vom Bundesverfassungsgericht gesetzte äußerste Grenze deutlich hinaus.

Die pauschale Behauptung, dass erst diese Änderungen, nämlich die Anknüpfung der Einschreitschwelle an das Vorfeldstadium, eine angemessene Reaktion auf Gefahren des Terrorismus ermöglichen, wird in der Gesetzesbegründung nicht belegt. An keiner Stelle wird erläutert, in welcher Weise Erfahrungen aus der Vergangenheit ergeben haben, dass in Anwendung der neuen Prinzipien ein terroristischer Anschlag hätte verhindert werden können. Abgestellt wird auf die - vermeintlich - gebotene Vereinheitlichung der Regelungen in Bund und Ländern, die eine Anlehnung an die entsprechenden Regelungen des BKA-Gesetzes und Abstimmungen innerhalb von Fachgremien nach sich ziehe. Daraus scheint geschlossen zu werden, dass es zur vorbeugenden Terrorismusbekämpfung unerlässlich sei, eine derart zeitlich vorverlagerte Eingriffsbefugnis zu besitzen.

Durch die Unbestimmtheit des neuen Gefahrenbegriffs wird der betroffene Personenkreis enorm ausgeweitet, denn die Maßnahmen können sich auch auf Menschen, die in keinerlei Verbindung zu terroristischen oder anderen Straftaten stehen und dies auch nicht planen, sowie auf unschuldige Kontakt- und Begleitpersonen erstrecken. Ich widerspreche ausdrücklich der Annahme auf Seite 2 der Gesetzesbegründung, dass sich die neu eingeführten Maßnahmen auf einen eng abgegrenzten Personenkreis beziehen würden. Durch die zeitliche Ausdehnung geraten deutlich mehr Personen in den polizeilichen Fokus, als dies bisher der Fall war.

Ich habe erhebliche Zweifel, dass der Gefahrenbegriff, wie er im brandenburgischen Gesetzentwurf Abschnitt 1a verwendet wird, in seiner Unbestimmtheit noch mit dem Rechtsstaats- und Ordnungsprinzip im Einklang steht. Das Rechtsstaatsprinzip, verankert in Art. 6 Europäische Menschenrechtskonvention, Art. 20 Abs. 3, 103 Abs. 2 GG, bestätigt durch die ständige Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte verlangt, dass polizeiliche Befugnisse so klar formuliert sein müssen, dass die Normadressaten ihr Verhalten darauf anpassen können. Die allgemeinen Feststellungen des Bundesverfassungsgerichts in dem Urteil sind deshalb aus meiner Sicht ausfüllungsbedürftig, damit sie dem Gebot der Normenklarheit genügen. Zwar ist es prinzipiell mit dem Bestimmtheitsgebot vereinbar, wenn eine Norm ausgelegt werden muss. Dies muss mit den juristischen Auslegungsmethoden möglich sein. Der Betroffene muss ab- bzw. vorhersehen können, wann der Anwendungsbereich der Norm eröffnet ist. Im Gesetzentwurf des Brandenburgischen Polizeigesetzes werden die Voraussetzungen aus dem Urteil lediglich wortwörtlich übernommen, sodass dem Einzelnen eine Beurteilung, wann die Schwelle des polizeilichen Einschreitens zulässigerweise erreicht ist, nicht möglich ist. Historisch betrachtet bricht der verwendete „Gefahrenbegriff“ mit dem im Sicherheits- und Verfassungsrecht verwurzelten Ordnungsprinzip, wonach ein Tatverdacht oder eine konkrete Gefahr für ein polizeiliches Handeln vorliegen muss.[4] Vor diesem Hintergrund trägt die vorgenommene Definitionserweiterung des durch bisherige Rechtsprechung ausgefüllten konkreten Gefahrenbegriffs in § 3 Nr. 4 b. BbgPolG-CDU-E auf die vorverlagerte Eingriffsbefugnis nicht zur Klarheit bei.

Die Gesetzesbegründung führt auf Seite 16 aus, dass, da die Formulierungen den Anforderungen des Bundesverfassungsgerichts für hinreichend bestimmte Kriterien ge-

[4] s. Ausarbeitung der Wissenschaftlichen Dienste des Bundestages, v. 27.7.2018, WD 3 - 3000 – 226/18

nügten, eine weitere Konkretisierung nicht erforderlich sei, sodass durch die Regelung eine notwendige flexible polizeiliche Reaktion auf entsprechende Anhaltspunkte ermöglicht werde.

Diese Auffassung teile ich nicht. Sie steht im Widerspruch zum Urteil des Bundesverfassungsgerichts, wonach die Anforderungen an ein Abweichen von den tradierten sicherheitsrechtlichen Gefahrenabwehrkategorien normenklar zu regeln sind. Es ist nicht erkennbar, wie viele Tage oder Wochen ein übersehbarer Zeitraum maximal beinhalten darf. Im Extremfall könnte dieser Zeitraum unerträglich weit ausgedehnt werden, so dass ggf. unbeteiligte Personen wochenlang einer polizeilichen, eventuell sogar verdeckten Maßnahme ausgesetzt sind. Dies stellt einen massiven Eingriff in das Grundrecht auf informationelle Selbstbestimmung aus Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG dar. In der Gesetzesbegründung findet sich zu der Frage eines übersehbaren Zeitraumes die Aussage, dass dessen Umfang lageabhängig sei und in der Regel „nicht mehr als Tage bis maximal Wochen“ umfasse. Das ist keine ausreichende Konkretisierung.

Die unklaren und ausfüllungsbedürftigen gesetzlichen Begriffe sind meines Erachtens auch in der praktischen Anwendung sowohl durch die Polizei als auch durch die zuständige Datenschutzaufsicht problematisch. Denn mangels einer Definition, wann beispielsweise individuelles Verhalten einer Person in einem „übersehbarer Zeitraum“, die „konkrete Wahrscheinlichkeit“ für eine Straftatbegehung begründet, kann dies nicht mithilfe bestehender juristischer Auslegungsmethoden bestimmt werden. Auf nicht absehbare Zeit wird die Deutungshoheit bei der praktischen Anwendung allein bei der Polizei und den vor Ort eingesetzten Polizeibeamten liegt. Da es einige Zeit dauern wird, bis sich eine Rechtsprechungspraxis hierzu ausbildet, ist die Ausfüllung des neuen Gefahrenbegriffs bis auf weiteres von der subjektiven Einschätzung der ausführenden Beamten abhängig. Eine derart weite Bewertungs- und Entscheidungskompetenz steht den Polizei- und Ordnungsbehörden nicht zu.

Eine zusätzliche Unsicherheit in der Normanwendung ergibt sich aufgrund des situationsabhängigen Merkmals in § 28a Abs. 1 Nr. 1 BbgPolG. Danach enthält die Definition des Terrorismusbegriffs das unbestimmte Merkmal „einschüchtern“. Es handelt sich um eine Gefahr des Terrorismus, wenn die Straftat in § 129a StGB bezeichnet und dazu bestimmt ist, die Bevölkerung auf erhebliche Weise einzuschüchtern. „Einschüchtern“ ist davon abhängig, welche Reaktion die Tat in der Bevölkerung auslöst.

Das Merkmal ist damit situationsabhängig und allein von der persönlichen Einschätzung abhängig.

zu § 28 b Abs. 2 BbgPolG-RegE (Identitätsfeststellung)

In Anlehnung an meine Anmerkung zu § 12 empfehle ich, den Wortlaut zu präzisieren und vor die Worte polizeiliche Erkenntnisse noch „nachweisbare“ einzufügen.

zu § 28 c BbgPolG-RegE (Aufenthaltsvorgabe und Kontaktverbot)

Die Schaffung einer Regelung, die für eine Person das Verlassen ihres Wohn- oder Aufenthaltsorts erlaubsnispflichtig macht bzw. eine Aufenthaltsvorgabe von bis zu sechs Monaten und ein Kontaktverbot zu bestimmten Personen erlaubt, stellt einen massiven Eingriff in das Freiheitsrecht eines Betroffenen dar. Ich halte diese Maßnahme für ungeeignet und unverhältnismäßig, sehe jedoch das informationelle Selbstbestimmungsrecht nicht primär betroffen.

zu § 28 e BbgPolG-RegE (Datenerhebung durch Eingriffe in informationstechnische Systeme)

Die neu in das Polizeigesetz eingefügte Regelung erlaubt die Überwachung und Aufzeichnung des Telekommunikationsverkehrs (TKÜ) durch den verdeckten Einsatz „technischer Mittel“ in informationstechnischen Systemen (z. Bsp. Computer oder Smartphones). Damit wird die Ermittlungsmethode der sog. "Quellen-TKÜ" eingeführt, die dazu dient, Kommunikationsinhalte trotz zunehmender Nutzung internetbasierter Telekommunikation und verbreiteter Nutzung kryptographischer Verfahren zu erheben und auszuleiten. Dazu ist es erforderlich, die Daten auf dem Telekommunikationsgerät des Nutzers, also an der „Quelle“ abzugreifen.

Von der in der vorherigen Fassung des Gesetzentwurfs (vom Juli 2018) enthaltenen zusätzlichen Befugnis, sonstige, nicht zur laufenden Telekommunikation bestimmte, personenbezogener Daten aus einem informationstechnischen System zu suchen und zu erheben (sog. „Online Durchsuchung“) hat der Regierungsentwurf Abstand genommen. Dies begrüße ich ausdrücklich.

Die Quellen-TKÜ ist – sofern sie sich **ausschließlich** auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt - ein Grundrechtseingriff von erheblichem Gewicht in die Vertraulichkeit individueller Kommunikation, Art. 10 GG. Das Grund-

recht auf Gewährleistung der Vertraulichkeit und Integrität eines informationstechnischen Systems (Art. 2 Abs.1 i.v.m. Art. 1 Abs.1 GG) ist hingegen in diesen Fällen nicht tangiert.[5] Es besteht trotzdem ein erhebliches Gefährdungspotential, wenn ein komplexes informationstechnisches System zum Zweck der Telekommunikationsüberwachung infiltriert wird, da mit der Infiltration die entscheidende Hürde genommen ist, um das System insgesamt auszuspähen. Es ist fraglich, ob mittels der bestehenden EDV-Maßnahmen überhaupt gesichert werden kann, dass ein zu diesem Zweck eingesetzter Staatstrojaner nicht doch auf die im System gespeicherten Daten zugreift und damit einen stärkeren Eingriff verkörpert, als eigentlich zulässig ist. Ich habe erhebliche Zweifel, ob die Verfahren, die für diese Maßnahme entwickelt wurden, die vom Bundesverfassungsgericht gesetzte Bedingung umsetzen können. Bisher hatten wir keine Gelegenheit, einen entsprechenden Vorgang zu prüfen.

Positiv ist zu bewerten, dass dieser Eingriff in dem vorliegenden Regierungsentwurf nicht unter den Voraussetzungen des bestehenden § 33a Abs. 1 BbgPolG, sondern ausschließlich zur Abwehr von Gefahren des Terrorismus erlaubt werden soll. Diese Beschränkung wird jedoch dadurch relativiert, dass mit Absatz 1 Satz 4 die Möglichkeit besteht, den Eingriff weit im Vorfeld einer konkreten Gefahr vorzunehmen. Meine grundsätzliche Kritik dazu habe ich oben zu Nr. 12 geäußert.

Zweifel hinsichtlich der Umsetzbarkeit der strikten Anforderungen an Eingriffe in informationstechnische Systeme lassen sich auch aus Absatz 3 der Regelung ableiten. Die Vorgabe, dass durch die Infiltration vorgenommene Veränderungen wieder rückgängig gemacht werden müssen und die ausgeleitete Kommunikation oder kopierte Daten vor Veränderungen, unbefugter Löschung oder Kenntnisnahme zu schützen sind, werden unter den Vorbehalt gestellt, dass dies nach dem Stand der Technik möglich ist. Dabei handelt es sich jedoch nicht um verhandelbare Maßgaben. Wenn nicht sichergestellt ist, dass die Anforderungen an Maßnahmen gemäß Absatz 1 und 2 zu erfüllen sind, ist ein Eingriff aus meiner Sicht unverhältnismäßig und damit verfassungswidrig.

[5] s. Urteil BVerfG vom 27.02.2008, 1 BvR 370/07, 1 BvR 595/07, Rnr. 189, 190

Kernbereich, Verwendung und Löschung von Daten

Absatz 4 Satz 3 des Entwurfs regelt eine Unterbrechung der Datenerhebung fest, wenn erkennbar wird, dass in den Kernbereich privater Lebensgestaltung oder in ein geschütztes Vertrauensverhältnis eingegriffen wird. Absatz 9 regelt das weitere Verfahren, insbesondere die Verwendung der Daten. Das Bundesverfassungsgericht hat in seinem Urteil zum Bundeskriminalamtgesetz erneut bestätigt, dass die Durchführung besonders eingriffsintensiver Überwachungsmaßnahmen besondere Anforderungen an den Schutz des Kernbereichs privater Lebensgestaltung stellt. Der Schutz dieses Kernbereichs dürfe auch nicht durch Abwägungen mit den Sicherheitsinteressen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes relativiert werden. Vorkehrungen sind nicht nur gegen das Miterfassen von Kernbereichsinformationen auf der Ebene der Datenerhebung zu treffen, sondern auch auf der Ebene der Auswertung und Verwertung, für den Fall, dass eine Erhebung kernbereichsrelevanter Informationen nicht vermieden werden konnte. (vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, Rn.124 -129). Die Sichtung der erfassten höchstpersönlichen Daten muss nicht durch eine unabhängige Stelle erfolgen, aber, vor einer Auswertung muss unverzüglich geprüft werden, ob es sich um Daten handelt, die gelöscht werden müssen.

Die in § 28 e Absatz 9 BbgPolG-RegE enthaltene Verweisung auf § 33b Abs. 8-11 BbgPolG, steht mit den gerichtlichen Vorgaben zur Verwendung nicht in Einklang. Bei der Verweisung handelt es sich um spezielle Vorschriften zur netzbasierten Telekommunikationsüberwachung. Absatz 9 dieser Norm erlaubt die weitere Verwendung der Daten zur Abwehr einer gegenwärtigen Gefahr für bedeutende Rechtsgüter, vorausgesetzt es wird eine richterliche Entscheidung beim Amtsgericht darüber eingeholt (Abs. 10). Dies widerspricht zum einen der Regel, **jegliche** Verwendung auszuschließen, zum anderen wird nicht unmittelbar deutlich, ob die Entscheidung auch bei Gefahr im Verzuge ausschließlich durch das Gericht getroffen wird. Aufgrund der Eingriffstiefe der Befugnis empfehle ich dringend, die wesentliche Frage des weiteren Verwendung erhobener Daten normenklar in § 33d selbst zu regeln.

Benachrichtigungen

Absatz 9 der Vorschrift verweist hinsichtlich der Unterrichtung der betroffenen Person auf die grundlegende Verpflichtung, bei verdeckten Maßnahmen den Betroffenen nachträglich über die Datenerhebung zu benachrichtigen. Diese bei eingriffsintensiven

Maßnahmen wesentliche Schutzvorkehrung, ist für den Anwender gesetzestechnisch unübersichtlich geregelt. Die Entwurfsfassung des § 28 e verweist in Absatz 9 auf die entsprechende Regelung des § 33b Abs. 8 -11 BbgPolG, der wiederum auf § 29 Abs. 7 und 8 sowie § 33a Abs. 6 BbgPolG verweist. Aus Gründen der Übersichtlichkeit und Verständlichkeit empfehle ich, von Kettenverweisungen Abstand zu nehmen. Sofern die Benachrichtigungspflicht nicht einzeln in jeder Norm gefasst werden soll, könnte eine Zusammenfassung aller Benachrichtigungspflichten nach dem Muster des § 74 BKAG erfolgen.

Die **Quellen-TKÜ** (und auch die Online-Durchsuchung, s. CDU-E § 49) ist angesichts des hohen Grundrechtseingriffs auch aus technischer und organisatorischer Sicht insbesondere aus folgenden Gründen als kritisch anzusehen:

- Die Software muss auf dem IT-System der betroffenen Person aufgebracht werden. Das heimliche Aufspielen von Software auf ein IT-System erfordert eine Software-Schwachstelle des betroffenen IT-Systems. Zur Infektion werden mindestens mittlere, im Regelfall sogar schwere bis kritische Schwachstellen benötigt. Der externe Zugang zur Überwachungssoftware erfordert die Öffnung der Firewall und mindestens eines Netzwerk-Ports. Diese Öffnung der Netzwerkschnittstelle könnte auch von Kriminellen missbräuchlich verwendet werden. Bekannt gewordene Schwachstellen sollten schnellstmöglich an die jeweiligen Hersteller übermittelt werden, damit diese entsprechende Maßnahmen ergreifen können. Ein Sammeln und Ausnutzen von Schwachstellen durch öffentliche Stellen ist unter allen Umständen zu vermeiden.

- Es ist nicht auszuschließen, dass aufgrund der Komplexität der eingesetzten Software diese auch Fehler enthalten kann. Dadurch wäre die Integrität des infiltrierten IT-Systems gefährdet. Eine Offenlegung des Quellcodes und eine Prüfung und Zertifizierung der Überwachungssoftware durch eine unabhängige Institution sind unabdingbar.

- Die auf dem IT-System erfassten bzw. erhobenen Daten könnten auch durch auf dem IT-System bereits installierte Schadsoftware weiterverarbeitet bzw. versendet werden. Durch den Einsatz von kryptographischen Verfahren ist eine missbräuchliche Nutzung der erhobenen Daten zu verhindern. Die Verschlüsselungsverfahren und die entsprechenden Schlüssellängen müssen sich nach dem jeweiligen Stand der Technik richten.

- Es ist unklar, wie sich die manipulativen Eingriffe in informationstechnische Systeme auf die Gerichtsfestigkeit der Beweise auswirken. Ein wesentlicher Grundsatz der Forensik ist, Manipulationen an informationstechnischen Geräten zu verhindern. Vor jedweder Analyse ist ein Image der Datenträger zu erstellen, damit die originalen Datenträger für Beweiszwecke erhalten bleiben.

Das für Inneres zuständige Mitglied der Landesregierung sollte ermächtigt werden, durch Rechtsverordnung über die grundlegenden technischen und organisatorischen Anforderungen für Maßnahmen nach Absatz 1 zu regeln. Die technischen Einzelheiten sollten in einer technischen Richtlinie detailliert beschrieben werden.

zu Nr. 13: § 29 BbgPolG-RegE (Grundsätze der Datenerhebung)

Mit der Neufassung des § 29 Abs. 6 BbgPolG-RegE wird der Kernbereich privater Lebensgestaltung in ausreichender Weise geschützt. Es werden somit datenschutzrechtliche Belange des Betroffenen gewahrt.

Das Bundesverfassungsgericht hat in seinem Urteil zum BKA-Gesetz (Rn. 123 d. Urteils) klargestellt, dass der Kernbereich privater Lebensgestaltung gegenüber allen Überwachungsmaßnahmen Beachtung beansprucht. Wenn die Überwachungsmaßnahmen typischerweise zu einer Erhebung kernbereichsrelevanter Daten führen können, muss der Gesetzgeber Regelungen schaffen, die einen wirksamen Schutz normenklar gewährleisten (vgl. BVerfGE 109, 279 <318 f.>; 113, 348 <390 f.>; 120, 274 <335 ff.>). Dies ist mit der Regelung des § 29 Abs. 6 PolGBbg-E in Ausführung des oben genannten Urteils geschehen. Nach dem Bundesverfassungsgericht ist der Schutz des Kernbereichs privater Lebensgestaltung strikt und darf nicht durch Abwägung mit Sicherheitsinteressen nach Maßgabe des Verhältnismäßigkeitsprinzips relativiert werden (Rn. 124 d. Urteils, vgl. BVerfGE 109, 279 <314>; 120, 273 <339>; stRspr). Bei der Durchführung von Überwachungsmaßnahmen muss dem Kernbereichsschutz sowohl auf der Ebene der Datenerhebung als auch auf der Ebene der anschließenden Auswertung und Verwertung Rechnung getragen werden (Rn. 126 d. Urteils, vgl. BVerfGE 120, 274 <337 ff.>; 129, 208 <245 f.>). Wenn erkennbar wird, dass eine Überwachung in den Kernbereich privater Lebensgestaltung eindringt, muss die Überwachungsmaßnahme abgebrochen werden (Rn. 128 d. Urteils, vgl. BVerfGE

109, 279 <318, 324, 331>; 113, 348 <392>; 120, 274 <338>). Wenn die Erhebung kernbereichsrelevanter Daten nicht vermieden werden konnte, sind die Daten von einer unabhängigen Stelle zu sichten und die kernbereichsrelevanten Daten herauszufiltern, bevor die Daten von der Sicherheitsbehörde verwendet werden (Rn. 129 d. Urteils, vgl. BVerfGE 109, 279 <331 f., 333 f.>; 120, 274 <338 f.>).

§ 29 Abs. 6 S. 2 PolGBbg-E bestimmt, dass die Datenerhebung zu unterbrechen ist, wenn erkennbar wird, dass durch die Erhebung in den Kernbereich privater Lebensgestaltung eingedrungen wird. Damit wird der Vorgabe, dass der Kernbereichsschutz schon bei der Erhebung der Daten zu beachten ist, Rechnung getragen. Die Überprüfung der Daten durch das Amtsgericht als unabhängiger Stelle, bevor die Daten weiter verarbeitet werden dürfen, wird von § 29 Abs. 6 S. 3 BbgPolG-RegE umgesetzt.

Das Bundesverfassungsgericht stellt zudem klar, dass der Gesetzgeber die sofortige Löschung von gegebenenfalls erfassten höchstpersönlichen Daten vorsehen und jegliche Verwendung ausschließen muss. Die Löschung muss so protokolliert werden, dass eine spätere Kontrolle ermöglicht wird (Rn. 129 d. Urteils, vgl. BVerfGE 109, 279 <318 f., 332 f.>; 113, 348 <392>; 120, 274 <337, 339>). Dies wird durch § 29 Abs. 6 S. 5 und 6 PolGBbg-E erreicht. Satz 7 stellt darüber hinaus klar, dass die Protokolldaten später nur dazu verwendet werden dürfen, zu überprüfen, ob die Maßnahme rechtmäßig durchgeführt worden ist.

zu Nr. 14: § 31 BbgPolG-RegE (Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie auf öffentlich zugänglichen Straßen und Plätzen)

§ 31 Absatz 2 S. 3 der Regelung erweitert die Speicherfrist von Bildaufnahmen, die die Polizei an öffentlich zugänglichen Straßen und Plätzen anfertigen darf, von bisher 48 Stunden auf zwei Wochen. Dies ist eine um das Siebenfache erhöhte Speicherfrist zum momentan geltendenRecht. Die Ausführungen für die Erforderlichkeit einer zweiwöchigen Speicherdauer überzeugen unter Verhältnismäßigkeitsgesichtspunkten nicht. Bei der Norm handelt es sich um eine Befugnis der Polizei zur Gefahrenabwehr, also um präventives Tätigwerden in einem konkret benannten Bereich, um dort Straftaten zu verhüten. Kommt es zu einer Straftat oder Ordnungswidrigkeit, können die Bildaufnahmen zur repressiven Verfolgung von Straftaten oder Ordnungswidrigkeiten

ohnehin solange gespeichert werden, wie sie für diese Zwecke benötigt werden, § 31 Abs. 2 S. 4 BbgPolG.

Die Gesetzesbegründung stellt allerdings darauf ab, dass durch eine generelle Verlängerung der Speicherdauer sowohl im Nachgang als auch im Vorfeld einer Straftat wichtige Erkenntnisse zum Täter erlangt werden könnten. Falls sich der Täter im Nachgang einer Straftat an einen (anderen) videoüberwachten Ort begebe, könnten dadurch beispielsweise das Fluchtverhalten und die Fluchtwege eines Attentäters/einer Attentäterin, das Aussehen oder mögliche Mittäter oder Kontaktpersonen noch nach Tagen bzw. Wochen aufgeklärt und durch die dabei erlangten Erkenntnisse weitere Folgetaten verhindern werden. Außerdem sei auch an erst nach und nach eingehende Hinweise zu denken, die den zwischenzeitlichen Aufenthalt des Täters an einem videoüberwachten Ort begründeten. Solche Aufnahmen sollten daher nicht vorschnell gelöscht werden, damit die Erkenntnisse nicht verloren gingen.

Zwar ist die Sorge nachvollziehbar, dass bei einer zeitnahen Löschung von Videoaufnahmen die Möglichkeit besteht, dass der Täter sich vor oder nach der Tat an einem videoüberwachten Ort aufgehalten hat und dort ggf. Mittäter getroffen hat. Diese Erkenntnisse könnten möglicherweise weitere Straftaten verhindern. Dennoch sollte die vorliegende Befugnis der Polizei, bestimmte Orte videoüberwachen zu dürfen, nicht dazu dienen, auf Vorrat Filmaufnahmen über einen längeren Zeitraum zu speichern, nur für die ungewisse Annahme, dass eine Person sich nach einer bereits begangenen Straftat an einen anderen videoüberwachten Ort begibt und damit dann ein Abgleich mit bereits bestehenden Aufnahmen möglich wäre. Dies gilt ebenso für den Fall, dass eine Person sich vor der Begehung einer Straftat an einem anderen videoüberwachten Ort aufgehalten hat und nach der Tat ein Abgleich ermöglicht werden soll. Die zweiwöchige Speicherfrist würde eine Vielzahl unbeteiligter Personen über einen langen Zeitraum betreffen, die sich lediglich an einem der benannten Orte aufhalten, ohne dass sie selbst im Zusammenhang mit der Straftat stehen oder selbst eine begangen hätten. Daher ist die pauschale Erweiterung der Speicherfrist unter datenschutzrechtlichen Aspekten unverhältnismäßig und unzulässig.

Als weniger einschneidende Maßnahme wäre es denkbar, nach der Begehung einer Straftat nach § 129a StGB an allen Orten, an denen die Polizei Videoüberwachungen nach § 31 BbgPolG-RegE durchführt, die Speicherfrist manuell von 48 Stunden auf

zwei Wochen hochzusetzen, da in diesem Fall ein begründeter Anlass hierfür bestünde.

zu Nr. 15: § 31a BbgPolG-RegE (Datenerhebung zur Eigensicherung)

Die Regelung entspricht der im Juli 2018 vorgelegten Entwurfsfassung des Brandenburgischen Polizeigesetzes. Die Änderung im Absatz 1 betrifft Bildaufnahmen sowie Bild- und Tonaufzeichnungen in Fahrzeugen der Polizei, die bereits bisher im Polizeigesetz als Befugnis normiert waren. Die Löschfrist wird jedoch von bisher einem Tag nach der Aufnahme auf zwei Wochen verlängert. Diese erhebliche Ausweitung ist nur im Zusammenhang mit der in Absatz 2 gefassten Neuregelung, die ebenfalls eine Zweiwochenfrist vorsieht, vertretbar.

§ 31a Absatz 2 führt zum Zweck der Eigensicherung die Erlaubnis für die Polizei ein, in öffentlich zugänglichen Räumen Bildaufnahmen sowie Bild- und Tonaufzeichnungen durch körpernah getragene technische Mittel durchzuführen (sog. Body-Cams). Damit wird die bestehende Eigensicherungsmaßnahme auf sämtliche Personen- und Fahrzeugkontrollen der Polizei ausgeweitet, wenn der Einsatz einer Körperkamera nach den Umständen zum Schutz gegen eine Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist. Die neue Befugnis greift schon aufgrund ihrer Streubreite erheblich in das Recht auf informationelle Selbstbestimmung ein. Die Anzahl Betroffener ist bei Aufnahmen und Aufzeichnungen größer, da Einsätze räumlich nicht mehr auf das Polizeifahrzeug beschränkt sind. Betroffene sind zudem nicht nur die Zielpersonen des Einsatzes, sondern auch Dritte, die sich zufällig im öffentlichen Raum im Aufnahmebereich der Kamera befinden und erfasst werden.

Grundsätzlich ist zu begrüßen, dass für die Datenerhebung mittels körpernah getragener Kameras eine ausdrückliche Rechtsgrundlage geschaffen werden soll. Im Hinblick auf den Verhältnismäßigkeitsgrundsatz bestehen jedoch Zweifel an der Geeignetheit und Erforderlichkeit der Eingriffsbefugnis. Ob eine Kamera tatsächlich die erhofften Auswirkungen, vor allem Abschreckungseffekte hat, sollte mittels einer objektivierten Evaluierung eines Pilotprojekts ausgewertet werden. Die Begründung verweist darauf, dass der Einsatz von Körperkameras bei Pilotprojekten (z. Bsp. in Frankfurt am Main) zu einer erhöhten Kooperationsbereitschaft bei Betroffenen in Konfliktsituationen geführt, Solidarisierungseffekte von Unbeteiligten reduziert und damit insgesamt die

Zahl der Übergriffe auf Einsatzkräfte verringert habe. Diese Bewertung beruht zwar auf polizeilichen Erfahrungen, entspricht aber nicht einer nach wissenschaftlichen Maßstäben ausgerichteten Wirkungsanalyse. Ob die festgestellten positiven Effekte tatsächlich auf die Wirkung der Kameras oder möglicherweise auf andere Faktoren zurückgehen, sollte untersucht werden. Ein Rückgang von Angriffen könnte mit statistischen Schwankungen oder damit zusammenhängen, dass an den ausgewählten Brennpunkten im Test ein höherer Personaleinsatz vorgehalten wurde. Zudem wurden in den Pilotprojekten auch Beamte, die erkennbar eine Body-Cam trugen, Ziel von Angriffen und Widerstandshandlungen[6]. Erstaunlicherweise enthält die Gesetzesbegründung auch keine Hinweise auf Erfahrungen, die mit der in Brandenburg bereits existierenden Regelung zur Bild- und Tondatenerhebung in Polizeifahrzeugen § 31a BbgPolG gemacht wurden.

Ich empfehle, die Eingriffsbefugnis zu befristen und die Maßnahme nach Zeitablauf von max. zwei Jahren zu evaluieren. In dieser Zeit könnte ein brandenburgisches Pilotprojekt durchgeführt werden. Erst danach ist eine verantwortliche Abwägungsentscheidung zwischen den Einschränkungen des Rechts auf informationelle Selbstbestimmung und präventiven Effekten möglich.

Positiv zu bewerten ist, dass im Regierungsentwurf von einem Einsatz der Körperkameras in Wohnungen abgesehen wurde und Bereiche, in denen Berufsgeheimnisträger ihrer Tätigkeit nachgehen, ausgeschlossen wurden. Die Befugnis Körperkameras auch in Wohnungen einzusetzen, wie es in § 44 Abs. 4 Satz 3 BbgPolG-CDU-E vorgesehen ist, sehe ich als unverhältnismäßig an. Es handelt sich dabei um einen Eingriff in die durch Artikel 13 Grundgesetz (GG) geschützte Unverletzlichkeit der Wohnung. Zur Abwehr dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, dürfen gemäß Absatz 4 des Artikels technische Mittel zur Überwachung von Wohnungen zwar eingesetzt werden, dies jedoch nur auf Grund einer richterlicher Anordnung. Ein Richtervorbehalt ist im CDU-Gesetzentwurf jedoch weder vorgesehen noch wird er laut Gesetzesbegründung für erforderlich gehalten. Der Gesetzentwurf geht davon aus, dass es sich bei den Körperkameras nicht um technische Überwachungsmittel im Sinne des Absatz 4 handelt, da die Aufnahmen nicht verdeckt erfolgen. Maßgeblich seien daher nur die Schranken

[6] vgl. Abschlussbericht des Polizeipräsidiums Frankfurt am Main über die Erfahrungen des Einsatzes der mobilen Videoüberwachung gem. § 14 Abs. 6 HSOG im Rahmen der Maßnahmen „Alt-Sachsenhausen“ sowie im Bereich des 1. Polizeireviers des Polizeipräsidiums Frankfurt am Main vom 1.10. 2014, Zf. 2.1.1

des Absatzes 7. Dem ist entgegenzuhalten, dass es keine Anhaltspunkte im Text des Artikels 13 dafür gibt, dass die Überwachung begriffsnotwendig heimlich erfolgen muss. Zudem kommt der in § 44 Abs. 4 Satz 3 eingefügte Vorbehalt, die Maßnahme sei erlaubt, „sofern damit nicht die Überwachung der Wohnung verbunden ist“ einer Neudefinition von Wohnraumüberwachung gleich. Der Gesetzgeber würde definieren, dass der Einsatz der Körperkameras in Wohnraum nicht unter den verfassungsrechtlichen Begriff der technischen Wohnraumüberwachung zu fassen ist. Dies ist angesichts der objektiven Überwachungseigenschaft von Körperkameras nicht nachvollziehbar.

Die Nutzung der Körperkameras schließt die Möglichkeit von Vorabaufnahmen (sog. „Pre-recording“) in Absatz 2 Satz 3-5 der Vorschrift ein. Dies bedeutet, dass die von dem Beamten aktivierte Kamera permanent, auch dann, wenn keine gewalttätige Eskalation bei der Kontrolle eintritt, die Bild- und Tondaten erfasst, diese erhobenen Daten für einen vorkonfigurierten Zeitraum (hier 60 Sekunden) in einem Kurzzeitspeicher ablegt und danach überschreibt. Erst durch eine zweite Aktivierung des Beamten wird die permanente Aufzeichnung ausgelöst, die dann jedoch die vorangegangenen 60 Sekunden mitumfasst.

Der Einsatz von „Pre-recording“ stellt einen Grundrechtseingriff dar. Dadurch wird völlig anlasslos das gesamte Geschehen einer Kontrolle „auf Vorrat“ aufgezeichnet, was ich verfassungsrechtlich für äußerst problematisch halte.

Unklar ist zudem die Frage wie die Transparenz für Betroffene praktisch hergestellt werden soll. Das Pre-recording muss aus Transparenzgründen für den Betroffenen und ggf. Dritte deutlich erkennbar sein, damit diese ggf. gegen die Kameraüberwachung effektiv vorgehen können. Um die Body-Cam rechtmäßig nutzen zu können, müsste daher in der Praxis darüber aufgeklärt werden, dass die Kamera eingeschaltet ist, aber ein Überschreiben der Daten stattfindet, solange die Speicherungsvoraussetzungen nicht eintreten. Ob die Nutzung in diesem Fall noch eine Abschreckungswirkung entfaltet, ist fraglich. Der kameraführende Beamte dürfte jedenfalls nicht den Eindruck erwecken oder gezielt falsch informieren, dass bereits eine dauerhafte Aufnahme stattfindet, obwohl dies tatsächlich nicht der Fall ist.

Dass die Funktion der Vorabaufzeichnung aus technischer Sicht erforderlich sei, wie die Begründung vorgibt, damit die Entstehung einer Gefahrenlage ohne Verzögerung

dokumentiert werden könne, reicht aus meiner Sicht nicht. Die Beweisführung im Falle eines Übergriffs ist nicht nur mithilfe der aufgezeichneten Bildaufnahmen möglich, sondern wie bisher auch mithilfe der Aussagen der beteiligten Beamten. Andere Länder, die die Befugnis zur Datenerhebung mittels Körperkamera bereits eingeführt haben (vgl. Nordrhein-Westfalen: § 15c PolGNRW) verzichten auf das Pre-recording.

Ich empfehle daher dringend, diese Funktion zu streichen, bzw. eine Evaluation der Maßnahme abzuwarten (s. o.). Jedenfalls sollten nur Kameras zum Einsatz kommen, bei denen technisch eine Abschaltung der Pre-recording-Funktion vorgenommen werden kann.

Neben der Bildaufzeichnung erlaubt die Vorschrift auch Tonaufzeichnungen, was nach der Gesetzesbegründung die präventive Wirkung erhöhen soll. Geht man davon aus, dass es vor tätlichen Auseinandersetzungen verbale beleidigende und aggressive Äußerungen gibt, könnte es sein, dass die Aufzeichnung der Kommunikation – vorausgesetzt der Betroffene wird darauf hingewiesen – deeskalierend wirkt. Hier könnten Erfahrungen aus der Anwendung der bereits bestehenden Befugnis (§ 31a Absatz 1), Tonaufnahmen in Fahrzeugen der Polizei aufzuzeichnen, hilfreich sein. Leider enthält die Begründung diesbezüglich keine Hinweise. Kommt es zu einem Übergriff, der mit Bild und Ton gespeichert wird, muss dieses Material sowohl der Polizei als auch der betroffenen Person zur Auswertung zur Verfügung stehen. Im Rahmen eines Pilotprojektes stimme ich daher einer Tonaufzeichnung zu. Nach einer gründlichen Auswertung der Erfahrungen sollte geprüft werden, ob der Zweck, Eskalationsverläufe zu unterbrechen und z. Bsp. Solidarisierungen Dritter gegen die Polizei zu verhindern, tatsächlich durch Tonaufnahmen messbar besser erfüllt wird als durch reine Bildaufzeichnungen. Wird erkennbar, dass Tonaufzeichnungen vorrangig Verwendung finden, um nach erfolgten Übergriffen mündlich erteilte polizeiliche Weisungen oder Beleidigungen der eingesetzten Beamten zu dokumentieren, haben sie sich als ungeeignet für den Zweck erwiesen, eine Gefahr für Leib, Leben oder Freiheit abzuwehren. Für Beweiszwecke eines Bagatelldelikts wie Beleidigung ist eine Tonaufzeichnung des gesprochenen Wortes nicht als verhältnismäßig anzusehen.

In der bisherigen, räumlich auf den Einsatz in Fahrzeugen der Polizei beschränkten Regelung mussten die Bild- und Tonaufzeichnungen am Tage nach dem Anfertigen gelöscht oder vernichtet werden. Durch den Verweis auf die in Absatz 1 Satz 4 eingefügte Änderung, wird die Löschfrist auf zwei Wochen erweitert. Wie in der Begrün-

dung erwähnt, sollen die zu Zwecken der Eigensicherung gefertigten Aufzeichnungen als Nebeneffekt auch dann zur Verfügung stehen, wenn polizeiliches Handeln im Falle eines Vorwurfs pflichtwidrigen oder strafbaren Verhaltens durch Auswertung der Daten überprüft werden soll. Zur Wahrung effektiver Betroffenenrechte (Auskunft und Einsichtnahme in die Bild- und Tonaufzeichnung) ist eine längere Mindestspeicherdauer erforderlich. Diese Verlängerung auf bis zu zwei Wochen halte ich im Hinblick auf diesen Zweck für vertretbar. Sie stellt potenziell eine Verbesserung der Betroffenenrechte dar. Es ist jedoch durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass das Datenmaterial vor unbefugten, auch manipulativen Zugriffen geschützt ist.

Der Gesetzestext enthält darüber hinaus keine Regelung dazu, wie der Auswertungsvorgang durch die Polizei erfolgen soll. Aus Transparenzgründen sollte festgelegt werden, wer die Aufzeichnungen auswertet. Zugleich ist ein Auskunftsrecht für Betroffene vorzusehen.

zu Nr. 16: § 32 BbgPolG-RegE (Datenerhebung durch Observation)

Die Änderung des § 32 BbgPolG-RegE beabsichtigt ausweislich der Gesetzesbegründung eine angemessene Erweiterung der Dauer der kurzfristigen Observation. Bisher kann eine anordnungsfreie und damit kurzfristige Observation durchgeführt werden, wenn sie durchgehend nicht länger als 24 Stunden dauert oder sie nur an bis zu zwei Tagen erfolgt. Dabei bedingen sich die Alternativen gegenseitig, das heißt, es ist nicht möglich, an zwei Tagen durchgehend zu observieren; dies muss unterbrochen erfolgen. Das zulässige Höchstmaß einer kurzfristigen Observation beträgt somit bisher jeweils 23 Stunden und 59 Minuten an insgesamt zwei Tagen oder einmalig durchgehend 24 Stunden.

Durch die Gesetzesänderung soll die durchgehende, kurzfristige Observation auf 48 Stunden erhöht und die Anzahl der Tage auf drei erhöht werden. Obwohl der Regierungsentwurf gegenüber dem Entwurf vom Juli 2018 die Anzahl der zulässigen Observationsstunden und Tage reduziert hat, habe ich Bedenken. Die Verlängerung der Observierungszeiten führt dazu, dass anhaltend in die datenschutzrechtlichen Belange der betroffenen Personen und ihrer Kontakt- oder Begleitpersonen eingegriffen wird. Leider wird auch hier in der Gesetzesbegründung nicht in ausreichendem Umfang dar-

gelegt, warum die Erhöhung der Observierungszeiten erforderlich ist. Es gibt keinerlei Ausführungen dazu, dass die bisher bestehenden Zeiten sich als zu kurz erwiesen hätten, um eine vorbeugende Bekämpfung von Straftaten gewährleisten zu können. Vielmehr wurde lediglich erläutert, dass Observationen ein probates Mittel seien, um im Rahmen der vorbeugenden Bekämpfung von Straftaten mögliche Tatvorbereitungshandlungen erkennen und entstehende Gefahren verhindern bzw. abwehren zu können. Durch die Erweiterung könnten Überwachungsmaßnahmen auch über das Wochenende und an Feiertagen eigenständig durchgeführt werden. Dies genügt den Anforderungen an eine Erforderlichkeit nicht. Ich empfehle, die bisherigen Observationszeiten beizubehalten.

Im Vergleich mit anderen Bundesländern würde Brandenburg mit der vorgesehenen Neuregelung auch einen vergleichsweise langen Observierungszeitraum erlauben. Sachsen, Nordrhein-Westfalen und Bayern erlauben weiterhin nur die bisherigen durchgehenden 24 Stunden bzw. zwei Tage. Auch angesichts der Regelungen dieser Vergleichsländer erschließt sich die deutlich darüber hinausgehende brandenburgische Regelung nicht.

Positiv zu bewerten ist allerdings, dass die längerfristige Observation zukünftig unter einem Richtervorbehalt steht bzw. bei Gefahr im Verzug durch die Behördenleitung angeordnet werden soll. Durch die Einbindung des Gerichts als unabhängiger Stelle wird eine Überprüfung der Notwendigkeit eines Eingriffs in das informationelle Selbstbestimmungsrecht der betroffenen Personen erreicht.

zu Nr. 17: § 33 BbgPolG-RegE (Datenerhebung durch den verdeckten Einsatz technischer Mittel zum Abhören und Aufzeichnen des gesprochenen Wortes und zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen)

Durch die Änderung des § 33 BbgPolG-RegE soll der verdeckte Einsatz technischer Mittel, soweit er länger als durchgehend 48 Stunden oder an mehr als drei Tagen erfolgen soll, durch ein Gericht, bei Gefahr im Verzug durch die Behördenleitung angeordnet werden können. Der kurzfristige Einsatz, der die obigen Zeiten nicht überschreitet, soll (weiterhin) von der Behördenleitung angeordnet werden. Ausweislich der Gesetzesbegründung soll durch die zeitliche Beschränkung des Richtervorbehalts ein Gleichklang mit § 32 Abs. 1 BbgPolG-RegE hergestellt werden, damit die kurzfris-

tigen (anordnungsfreien) Observationen vom Einsatz technischer Mittel begleitet werden können. Hier empfehle ich, um einen Gleichklang mit § 32 BbgPolG-RegE zu erzielen, den Richtervorbehalt bei einer Maßnahme ab durchgehend **24 Stunden** bzw. mehr als **zwei** Tagen festzuschreiben.

Dass der Einsatz technischer Mittel zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes grundsätzlich unabhängig von der Dauer vom Gericht angeordnet werden muss, begrüße ich ausdrücklich. Bisher war es der Behördenleitung möglich, solange die Maßnahme einen Monat nicht überschritt, die Einsatzzeit technischer Mittel (unter Verhältnismäßigkeitsaspekten) selbst zu bestimmen. Durch die Einbindung des Gerichts als unabhängiger Stelle wird eine unabhängige Überprüfung der Notwendigkeit eines Eingriffs in das informationelle Selbstbestimmungsrecht der betroffenen Personen erreicht.

Allgemein empfehle ich, für die Verarbeitung personenbezogener Daten, die durch einen besonders schwerwiegenden Eingriff in Persönlichkeitsrechte Betroffener gewonnen werden, auf die Möglichkeit der Ad-hoc-Freigabe (Nr. 5 Dateienrichtlinie-Polizei, § 48 Abs. 5 BbgPolG) zu verzichten.

Kleinmachnow, den 7. Januar 2019

Dagmar Hartge
LDA Brandenburg