



**Die Landesbeauftragte für den Datenschutz
Niedersachsen**

Die Landesbeauftragte für den Datenschutz
Prinzenstraße 5 • 30159 Hannover

Vorlage	21
zu Drs.	850

Präsidentin des
Niedersächsischen Landtages
- Landtagsverwaltung –
Ausschuss für Inneres und Sport
Postfach 4407
30044 Hannover

Vorlage	16
zu Drs.	828

Bearbeitet von: Herrn Klauke

Ihr Zeichen, Ihre Nachricht vom

Mein Zeichen (Bei Antwort angeben)
1.11-3070-12-10

Durchwahl Nr.: 05 11 120-

Hannover,
06.08.2018

**Stellungnahme zum
Entwurf eines Reformgesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze (LT-Drs. 18/850) sowie zum**

Antrag der Fraktion Bündnis 90/Die Grünen „Für ein Niedersächsisches Gefahrenabwehrgesetz ohne Symbolpolitik und Generalverdacht“ (LT-Drs. 18/828)

Anhörung im Ausschuss für Inneres und Sport am 09.08.2018

Sehr geehrte Damen und Herren,

für die Gelegenheit zur Stellungnahme zum Gesetzentwurf sowie zum Entschließungsantrag im Rahmen der Anhörung am 09.08.2018 bedanke ich mich.

Aus Sicht der Landesbeauftragten für den Datenschutz (LfD) enthält der Entwurf eine Reihe von Änderungen, die datenschutzrechtlich zu begrüßen sind. Hierzu zählen insbesondere die spezialgesetzlichen Regelungen zur Gefährderansprache (§ 12 a) sowie zur Meldeauflage (§ 16 a), die konkretere Fassung der Vorschriften zur offenen Videoüberwachung (§ 32 Abs. 3), die Schaffung einer Rechtsgrundlage für die Videoüberwachung in Gewahrsamseinrichtungen der Polizei (§ 20 Abs. 4), zur Verkehrslenkung (§ 32 Abs. 7) sowie für die sog. Abschnittsgeschwindigkeitskontrolle (§ 32 Abs. 8) und den Einsatz sog. Bodycams (§ 32 Abs. 4 und 5). Auch nähere gesetzliche Regelungen zum Einsatz einer Vertrauensperson (§ 36) sind überfällig. Erfreulich ist weiterhin, dass der Gesetzentwurf die Rechtsprechung des Bundesverfassungsgerichts zum BKA-Gesetz (NJW 2016, 1781 ff.) bereits weitgehend berücksichtigt.

Der Entwurf der Landesregierung enthält jedoch auch eine Vielzahl von Änderungen, die in die falsche Richtung weisen bzw. überarbeitungsbedürftig sind. Kritikwürdig sind insbesondere die zahlreichen neuen Befugnisnormen, die zum Teil tief in die datenschutzrechtlichen Grundrechte eingreifen und damit die Freiheit der Bürgerinnen und Bürger unangemessen beschneiden. Hierzu zählt die Einführung der Instrumente der elektronischen Aufenthaltsüberwachung (§ 17 c) und des verdeckten Eingriffs in informationstechnische Systeme (§ 33 d) sowie die Ausweitung der Datenerhebung durch



Überwachung der Telekommunikation (§ 33 a) und die sog. Wohnraumüberwachung (§ 35 a). Ferner ist zu kritisieren, dass der Gesetzentwurf an zahlreichen Stellen die Eingriffsschwelle bei zahlreichen Befugnissen in das Vorfeld einer konkreten Gefahr zieht und damit den Anwendungsbereich dieser eingriffsintensiven Überwachungsmaßnahmen erheblich ausweitet, ohne den damit verbundenen Begriff der „drohenden Gefahr“ gesetzlich näher und damit bestimmt genug zu beschreiben, vgl. z. B. §§ 16 a Abs. 2, 17 b Abs. 2, 17 c Abs. 1, 33 a Abs. 1, 33 d Abs. 1.

Dem allgemeinen Teil der Gesetzesbegründung ist zu entnehmen, dass die Umsetzung von Rechtsakten der Europäischen Union, die sich mit Erleichterungen des Datenaustausches und der Entwicklung gemeinsamer Standards für den Datenschutz im Rahmen der polizeilichen und justiziellen Zusammenarbeit der Europäischen Union in Strafsachen befassen, einem weiteren Gesetzentwurf vorbehalten bleiben soll. Dies ist aus Sicht der LfD nicht nachvollziehbar, da der Gesetzentwurf zur Änderung des Nds. SOG aus der 17. Wahlperiode (LT-Drs. 17/6232) bereits Vorschläge zur Umsetzung dieser europäischen Rechtsakte enthielt, die problemlos in den vorliegenden Gesetzentwurf hätten aufgenommen werden können.

Besonders bedauerlich ist es, dass die Datenschutzrichtlinie vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (JI-Richtlinie) mit dem vorliegenden Reformgesetz nicht aufgegriffen wird. Die JI-Richtlinie wurde mit dem Gesetz zur Neuordnung des niedersächsischen Datenschutzrechts (§§ 23 ff. NDSG) nur unzureichend im polizeilichen Gefahrenabwehrrecht umgesetzt. Insoweit verweise ich auf meine Stellungnahme gegenüber dem Landtag vom 23.04.2018. Hier besteht weiterhin dringender gesetzgeberischer Handlungsbedarf, zumal die JI-Richtlinie schon zum 06. Mai 2018 in nationales Recht hätte umgesetzt werden müssen.

Im Zuge der in der Gesetzesbegründung angekündigten nachfolgenden Novellierung zur Umsetzung von EU-Recht sollten die datenschutzrechtlichen Vorschriften im dann neuen Niedersächsischen Polizei- und Ordnungsbehördengesetz (NPOG) in Gänze neu geordnet und systematisiert werden. Für den Rechtsanwender sind die jetzigen Regelungen zum Datenschutzrecht durch die zahlreichen Novellierungen in den vergangenen Legislaturperioden nur noch schwer verständlich. Dies betrifft insbesondere die §§ 30, 31 sowie §§ 38 bis 48, soweit dort die allgemeinen Grundsätze der Datenverarbeitung für die Gefahrenabwehr geregelt werden.

I. Entwurf eines Reformgesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze (LT-Drs. 18/850)

Zum Reformgesetzentwurf nehme ich im Einzelnen wie folgt Stellung:

1. Zu Nr. 2 a), § 2 Nr. 4.

Mit dem Gesetzentwurf wird erstmals der Begriff der „dringenden Gefahr“ eingeführt und definiert. Der Gefahrbegriff der „dringenden Gefahr“ soll mit Blick auf die Rechtsprechung des Bundesverfassungsgerichts beim Ausmaß als auch bei der Wahrscheinlichkeit des Schadenseintritts strengere Anforderungen im Vergleich zur „konkreten Gefahr“ erfüllen und als Eingriffsschwelle für besonders grundrechtsintensive Maßnahmen fungieren, so z. B. für die Telekommunikations- oder Wohnraumüberwachung.

Die Legaldefinition soll für die Rechtsanwendung Rechtsklarheit schaffen. Auch wird mit dem neuen Gefahrenbegriff der „dringenden Gefahr“ versucht, eine zusätzliche erhöhte Eingriffsschwelle für besonders eingriffsintensive Instrumente der Datenerhebung zu definieren. Dieses Anliegen ist aus Sicht des Datenschutzes grundsätzlich zu begrüßen.

Jedoch darf nicht außer Acht gelassen werden, dass der Katalog der Begriffsdefinitionen zu bestimmten Gefahrenlagen im Vergleich zur bisherigen Rechtslage mit dem zusätzlichen Begriff der „dringenden Gefahr“ unübersichtlicher wird und damit für die Rechtsanwendung schwieriger zu handhaben ist. So stellt sich die Frage, ob durch eine Kombination der bereits existierenden Gefahrenbegriffe der „gegenwärtigen Gefahr“ und der „erheblichen Gefahr“ bei Eingriffsbefugnissen, die tief in die Grundrechte der Betroffenen eingreifen, nicht derselbe Regelungszweck erreichbar und damit der neue Gefahrenbegriff der „dringenden Gefahr“ entbehrlich wäre. Die „gegenwärtige Gefahr“ stellt erhöhte Anforderungen an die Eintrittswahrscheinlichkeit des schädigenden Ereignisses. Derselbe Regelungszweck findet sich als ein Teilaspekt auch im Begriff der „dringenden Gefahr“. Die Definition der „erheblichen Gefahr“ zielt darauf ab, nur Gefahrenlagen für bedeutsame Rechtsgüter als Eingriffsschwelle zu bestimmen. Dieser Regelungsinhalt findet sich auch im Begriff der „dringenden Gefahr“ wieder (eine im Hinblick auf das Ausmaß des zu erwartenden Schadens und die Wahrscheinlichkeit des Schadenseintritts erhöhte Gefahr ...).

Erschwerend für den Rechtsanwender kommt hinzu, dass der Gesetzentwurf den weiteren Begriff der „drohenden Gefahr“ zwar nicht in § 2 legal definiert, diesen aber an zahlreichen Stellen als der Gefahr vorgelagerte Eingriffsschwelle verwendet (so z. B. in § 16 a Abs. 2¹, § 17 b Abs. 1, § 17 c Abs. 1, § 33 a Abs. 1, § 33 d Abs. 1 Satz 2). Dieser Regelungsansatz, nämlich einen weiteren Gefahrenbegriff quasi durch die Hintertür ins Gesetz zu schreiben, ist nicht nachvollziehbar.

Im Ergebnis muss der Rechtsanwender daher zukünftig sechs anstelle der bisher vier Definitionen von Gefahrenlagen gegeneinander abgrenzen, um sich Klarheit darüber zu verschaffen, ob eine grundrechtsrelevante Maßnahme durchgeführt werden darf oder nicht. Die unübersichtliche und nicht vorhandene Regelungssystematik der unterschiedlichen Gefahrenbegriffe wird zukünftig dazu führen, dass nicht Rechtsklarheit sondern im Gegenteil Rechtsunsicherheit bei der Rechtsanwendung in der Praxis eintritt. Mit Blick auf den Bestimmtheitsgrundsatz bei der Normierung von Eingriffsbefugnissen zur Datenerhebung und -verarbeitung ist dieser grundlegende Mangel im Gesetzentwurf nicht hinnehmbar.

2. Zu Nr. 2 d), § 2 Nr. 14

Die Liste der Straftaten von erheblicher Bedeutung soll mit dem Gesetzentwurf um zahlreiche Delikte erweitert werden. Die Straftatenliste bildet die Eingriffsgrundlage für zahlreiche polizeiliche Standardmaßnahmen mit höchst unterschiedlicher Eingriffstiefe in die Grundrechte der Betroffenen. So ist z. B. bei einer offen durchgeführten Personenkontrolle nach § 12 Abs. 6 der Schutzbereich des Grundrechts auf informationelle Selbstbestimmung weit weniger stark tangiert als bei einer verdeckt durchgeführten Personenbeobachtung nach § 34 Abs. 1 Nr. 2. In beiden Fällen ist die Verhütung von Straftaten von erheblicher Bedeutung tatbestandliche Voraussetzung.

Es stellt sich die Frage, ob tatsächlich alle in § 2 Abs. 1 Nr. 14 aufgeführten Delikte (Straftaten von erheblicher Bedeutung) ausreichend gewichtig sind, um den damit verbundenen Eingriff in das Grundrecht auf informationelle Selbstbestimmung zu rechtfertigen, wenn es um Maßnahmen geht, die verdeckt und unter Einsatz technischer Mittel durchgeführt werden (so z. B. die verdeckt durchgeführte Personenbeobachtung). Der Straftatenkatalog umfasst auch solche Straftaten, die ein Vergehen darstellen und nicht mit einer Mindeststrafe belegt sind (z. B. §§ 130, 174 Abs. 2 StGB). Diese Straftaten kommen nicht als ausreichende Eingriffsschwelle für Datenerhebungen in Betracht, die verdeckt oder mit technischen Mitteln durchgeführt werden.

¹ Zur Definition der „drohenden Gefahr“ im Einzelnen siehe die Anmerkungen zu § 16 a.

3. Zu Nr. 2 e), § 2 Nr. 15 und 16

Mit diesen Regelungen werden die Begriffe der „terroristischen Straftat“ und die der „schweren organisierten Gewaltstraftat“ legal definiert, um damit besondere tatbestandliche Voraussetzungen für ganz bestimmte polizeiliche Maßnahmen zu schaffen. Dies ist mit Blick auf den verfassungsrechtlichen Bestimmtheitsgrundsatz grundsätzlich zu begrüßen.

Bei der „terroristischen Straftat“ orientiert sich der Straftatenkatalog ausweislich der Gesetzesbegründung an dem Katalog des § 129 a StGB. Während § 5 BKAG in Gänze auf alle in § 129 a Abs. 1 und Abs. 2 StGB genannten Straftaten verweist, führt der Straftatenkatalog die einzelnen Straftatbestände nochmals ausdrücklich auf. Diese Vorgehensweise ist nicht nachvollziehbar, zumal die Gesetzesbegründung ausdrücklich den Gleichklang mit § 5 BKAG erwähnt. Die Definition der „terroristischen Straftat“ sollte daher entsprechend § 5 BKAG erfolgen und zusätzlich um die Delikte der §§ 89 a - c sowie 129 a und b StGB ergänzt werden. Damit wird sichergestellt, dass Bundes- und Landesbehörden bei der Bekämpfung des Terrorismus von den gleichen Voraussetzungen ausgehen.

Ferner ist es aus Sicht des Datenschutzes zu begrüßen, dass es für eine polizeiliche Maßnahme zur Straftatenverhütung nicht allein ausreicht, wenn eines der genannten Delikte in Betracht kommt. Erforderlich ist zusätzlich, dass die Straftat mit einer entsprechenden terroristischen Absicht begangen werden soll. Gleiches gilt für das Vorliegen einer schweren organisierten Gewaltstraftat.

Im Zusammenspiel mit der Einführung des Gefahrenbegriffs der „dringenden Gefahr“ bedeutet dies z. B. beim Instrument der Wohnraumüberwachung, dass diese zur Straftatenverhütung im Vergleich zur bisherigen Rechtslage teilweise eingeschränkt wird. Dieser Ansatz ist aus Sicht des Datenschutzes erfreulich. Bisher war die Wohnraumüberwachung nach § 35 a zur Abwehr einer Gefahr (jetzt dringenden Gefahr) zulässig, wenn eine Person eine besonders schwerwiegende Straftat begehen wird (jetzt nur bei Vorliegen einer terroristischen Straftat mit entsprechender terroristischer Absicht).

4. Zu Nr. 3, § 12 Abs. 5, Sätze 2 und 3

Durch die Einfügung der neuen Sätze 2 bis 6 wird das Auskunftsverweigerungsrecht für Geistliche, Strafverteidiger, Rechtsanwälte und Abgeordnete gestärkt, da für diesen Personenkreis die „Güterabwägungsklausel“ zukünftig nicht gelten soll. Dies ist aus datenschutzrechtlicher Sicht zu begrüßen, obgleich das Bundesverfassungsgericht nach hiesiger Lesart ein absolutes Auskunftsverweigerungsrecht für das Recht der Gefahrenabwehr nicht ausdrücklich fordert.

Für verfassungsrechtlich nicht tragfähig wurde vom Bundesverfassungsgericht in der Entscheidung zum BKA-Gesetz nur die konkrete Ausgestaltung des Schutzes der Vertrauensverhältnisse von Rechtsanwälten zu ihren Mandanten gerügt. Eine Begrenzung des absoluten Auskunftsverweigerungsrechts nur für Strafverteidiger, wie in § 20a Abs. 1 BKAG a. F. vorgesehen, sei im Vergleich zur Tätigkeit von Rechtsanwälten in anderen Mandatsverhältnissen insofern verfassungswidrig, da hiermit für den unterschiedlichen Schutz an das Strafrecht bzw. Strafverfahrensrechts angeknüpft werde.² Mit § 12 Abs. 5 soll jedoch das Auskunftsverweigerungsrecht bei einer gefahrenabwehrrrechtlichen Maßnahme geregelt werden. In diesen Fällen schließt das Bundesverfassungsgericht eine Ausgestaltung des Schutzes von Berufsgeheimnisträgern und anderen Personengruppen nach Maßgabe einer Abwägung im Einzelfall gerade nicht aus³, im Gegenteil: Dem Gesetzgeber wird hier ein weiter Einschätzungsspielraum zugebilligt.⁴

² BVerfG NJW 2016, 1781, Rz. 257.

³ BVerfG NJW 2016, 1781, Rz. 256.

⁴ Petri, ZD 2016, 374 (375).

Im Ergebnis ist es aus Sicht des Datenschutzes daher sehr erfreulich, dass der Gesetzentwurf mit der Neufassung des § 12 Abs. 5 über die Vorgaben des Bundesverfassungsgerichts hinausgeht.

5. Zu Nr. 4, § 12a

Die erstmalige Regelung der Gefährderansprache bzw. des Gefährderanschreibens in einer eigenständigen Befugnisnorm ist ausdrücklich zu begrüßen. Mittlerweile hat sich dieses Instrument zu einer polizeilichen Standardmaßnahme entwickelt - gerade im Zusammenhang mit Sportveranstaltungen. Wegen des verfassungsrechtlichen Grundsatzes der Bestimmtheit und Normenklarheit ist es nur folgerichtig, dass der Gesetzgeber nunmehr ausdrücklich regelt, unter welchen Voraussetzungen eine solche polizeiliche Maßnahme zulässig ist.

Um der Gefahr einer Stigmatisierung entgegenzutreten, ist der gesetzlich normierte Grundsatz, Gefährderansprachen grundsätzlich an der Wohnung des Betroffenen vorzunehmen, ebenfalls zu begrüßen. Gleiches gilt für die Sonderregelung des § 12 a Abs. 2, der die Gefährderansprache bei Minderjährigen regelt und vorsieht, dass diese grundsätzlich nur im Beisein einer vertretungsberechtigten Person durchgeführt werden darf.

6. Zu Nr. 8, § 16 a

Gleiches gilt für die Normierung der Meldeauflage, die bisher ebenso wie die Gefährderansprache auf die Generalklausel des § 11 gestützt wurde. Auch hier ist es aus Gründen der Rechtsklarheit grundsätzlich zu begrüßen, dass eine eigenständige Rechtsgrundlage geschaffen wird. Die Meldeauflage gehört inzwischen ebenfalls zu den in der Praxis bewährten gefahrenabwehrrechtlichen Maßnahmen, um insbesondere im Vorfeld von Veranstaltungen Straftaten verhüten zu können.

Die vorgeschlagenen Regelungen sind jedoch in sich widersprüchlich, unsystematisch und stiften damit eher Unsicherheit als Rechtsklarheit in der praktischen Rechtsanwendung. Auch werden die tatbestandlichen Anforderungen für die Zulässigkeit einer Meldeauflage im Vergleich zum bisherigen Recht in verfassungsrechtlich bedenklicher Art und Weise erheblich abgesenkt.

Der Gesetzentwurf definiert in § 16 a Abs. 1 die Voraussetzungen, um eine Meldeauflage zur vorbeugenden Verhütung von Straftaten aussprechen zu können, wenn keine terroristische Straftat im Sinne des § 2 Nr. 15 vorliegt. Die Maßnahme soll bereits im Vorfeld einer konkreten Gefahr zulässig sein nämlich dann, „wenn bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat begehen wird“. Absatz 2 Nr. 1 wiederholt exakt diese tatbestandlichen Voraussetzungen, beschränkt diese aber auf das Vorliegen einer terroristischen Straftat. Geht es um die Verhütung einer terroristischen Straftat, so soll nach Absatz 2 Nr. 2 eine Meldeauflage auch dann in Betracht kommen, „wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird“. Diese Tatbestandsalternative fehlt hingegen bei der Anordnung einer Meldeauflage nach Absatz 1.

Regelungszweck der Meldeauflage ist es laut der Gesetzesbegründung zu § 16 a, diese als gefahrenabwehrende Maßnahme zur Straftatenverhütung insbesondere im Vorfeld von politischen oder sportlichen Veranstaltungen aussprechen zu können. Dann aber kommt eine solche Maßnahme insbesondere dann in Betracht, wenn sich aus dem individuellen Verhalten einer Person ergibt, dass sie demnächst eine Straftat begehen wird (z. B. durch Ankündigung einer Straftat zu einer bestimmten Zeit an einem bestimmten Ort durch einen Fußballhooligan). Warum die Polizei und Verwaltungsbehörden bei dieser Fallkonstellation keine Meldeauflage nach Absatz 1 verfügen dürfen, bleibt für den Rechtsanwender unklar. Auch die Gesetzesbegründung gibt hierzu keine nachvollziehbare Auskunft.

Viel schwerer wiegt jedoch die Tatsache, dass die Meldeauflage in beiden Fallvarianten zukünftig im Vorfeld einer Gefahr - hier im vorgelagerten Stadium der Straftatenverhütung, so die Gesetzesbegründung - ausgesprochen werden kann. Damit werden die Anforderungen für die Meldeauflage im Vergleich zur aktuellen Rechtslage erheblich abgesenkt, indem der Begriff der „drohenden Gefahr“ - ohne diesen näher zu definieren - durch die Hintertür ins Gesetz eingefügt wird.

Bisher war nach der Generalklausel des § 11 eine Meldeauflage nur zulässig, um eine Gefahr für die öffentliche Sicherheit und Ordnung – also eine konkrete Gefahrenlage im Sinne der Definition des § 2 Nr. 1 a – abwehren zu können.

Die Gesetzesbegründung beruft sich dabei auf die Rechtsprechung des Bundesverfassungsgerichts zum BKA-Gesetz.⁵ In der Tat hat das Bundesverfassungsgericht beiläufig Ausführungen allgemeiner Art gemacht, unter welchen Voraussetzungen der Gesetzgeber ausnahmsweise die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs weiter reduzieren kann, wenn es um den Schutz überragend wichtiger Rechtsgüter geht. Dies ist jedenfalls offensichtlich nicht der Fall, wenn es um die Anordnung einer Meldeauflage nach Absatz 1 des Gesetzentwurfs geht, die nur gewöhnliche Straftaten – nicht terroristische Straftaten – verhüten soll. Schon aus diesem Grund ist die Herabsetzung der Anforderungen an die Gefahrenlage, also eine Verlagerung der Anordnungsmöglichkeit der Meldeauflage nach Absatz 1 ins Gefahrenvorfeld, verfassungswidrig.

Der Gesetzentwurf übernimmt darüber hinaus ohne weitere Erläuterungen die allgemein formulierten Hinweise des Bundesverfassungsgerichts in den Gesetzestext. Konkretisierende gesetzliche Definitionen der eingeführten unbestimmten Rechtsbegriffe fehlen. Was ist unter den Formulierungen „innerhalb eines absehbaren Zeitraums“ oder „auf eine zumindest ihrer Art nach konkretisierte Weise“ zu verstehen? Mit Blick auf den verfassungsrechtlichen Bestimmtheitsgrundsatz geht die ständige Rechtsprechung des Bundesverfassungsgerichts davon aus, dass der Gesetzgeber die Anforderungen an eine Prognoseentscheidung hinreichend konkret und für den Rechtsanwender verständlich zu formulieren hat. Dieser Verantwortung kann sich der Gesetzgeber nicht dadurch entziehen, indem er lediglich allgemein formulierte Vorgaben des Bundesverfassungsgerichts ohne jede weitere inhaltliche Konkretisierung in den Gesetzestext einfügt. Das neue bayerische Polizeiaufgabengesetz schreibt nicht nur die Formulierungen der Urteilsbegründung des Bundesverfassungsgerichts ab, sondern versucht diese dem Bestimmtheitsgebot entsprechend konkreter zu fassen.⁶

Die Anforderungen an den Gesetzgeber, so konkret wie möglich die tatbestandlichen Voraussetzungen der „drohenden Gefahr“ zu definieren, sind auch deshalb besonders hoch, weil der Gesetzentwurf die Gefahrenschwelle für zahlreiche eingriffsintensive und zum Teil verdeckt durchgeführte Maßnahmen in das Vorfeld einer konkreten Gefahr verlagert, so bei der Anordnung einer elektronischen Aufenthaltsüberwachung, Telekommunikationsüberwachung und Online-Durchsuchung.

Ferner ist es fraglich, ob überhaupt ein tatsächlicher Bedarf für die Herabsetzung der Eingriffsschwelle bei bestimmten Maßnahmen besteht. Hierzu enthält die Gesetzesbegründung keine detaillierten Ausführungen, sondern beruft sich in allgemeiner Form auf die hohe abstrakte Gefährdungslage durch den islamistischen Terrorismus. Das Bundesverfassungsgericht führt in seiner Entscheidung zum BKA-Gesetz jedoch auch aus, dass die Anforderungen an die Gesetzgebung dann besonderes hoch sind, wenn es um heimliche polizeirechtliche Überwachungsmaßnahmen geht, die tief in die Grundrechte der Betroffenen eingreifen.⁷ Diese Anforderungen umfassen naturgemäß auch eine ordentliche und nachvollziehbare Begründung dafür, warum die bisher der Polizei zur Verfügung stehenden Überwachungsinstrumente zur Straftatenverhütung zukünftig nicht mehr ausreichend sein sollen.

⁵ BVerfG NJW 2016, 1781, Rn. 112.

⁶ Vgl. Art. 11 Abs. 3 PAG BY.

⁷ BVerfG NJW 2016, 1781, Rn. 113.

Durch die Vorverlagerung der Eingriffsschwelle bei bestimmten Maßnahmen entsteht zudem zusätzlich das Problem der Abgrenzung zwischen polizeilichen und nachrichtendienstlichen Befugnissen. Mit Blick auf das Trennungsgebot trifft daher den Gesetzgeber eine besondere Begründungspflicht, warum die bisher geltende Trennlinie der konkreten Gefahr für das polizeiliche Einschreiten nicht mehr ausreichen soll und im Ergebnis die Zuständigkeiten der Polizei mit dem Begriff der „drohenden Gefahr“ in die Nähe der nachrichtendienstlichen Aufgaben gerückt werden sollen. Die Erkenntnislage über die Begehung terroristischer Straftaten in den letzten Jahren (Anschläge des NSU sowie der islamistischen Szene) lässt nicht darauf schließen, dass die Polizeibehörden über unzureichende Ermittlungsbefugnisse zur Gefahrenabwehr oder Strafverfolgung verfügen. Vielmehr haben die bisherigen Untersuchungen ergeben, dass gravierende Mängel in der Zusammenarbeit der Sicherheitsbehörden die Hauptursache für die Nichtverhinderung der Anschläge gewesen sind. Die Ausweitung polizeilicher Befugnisse in den Grenzbereich der Zuständigkeiten des Nachrichtendienstes wird jedenfalls nicht dazu beitragen, die notwendige Zusammenarbeit zwischen den Sicherheitsbehörden bei der Terrorismusbekämpfung zu fördern.

In § 16 a Absatz 3 werden verfahrenssichernde Regelungen über die Anordnung der Meldeauflage getroffen. Danach ist die Erstanordnung der Meldeauflage durch die Polizei oder Verwaltungsbehörde bis zu einer Dauer von sechs Monaten mit mehrfacher Verlängerungsmöglichkeit zulässig. Hierbei ist zu berücksichtigen, dass die mit einer Meldeauflage verbundenen Grundrechtseingriffe für die Betroffenen mitunter erheblich sein können. Die Bewegungsfreiheit wird weitgehend eingeschränkt, wenn sich der Adressat der Meldeauflage auf einer bestimmten Polizeidienststelle zu bestimmten Zeiten (täglich) zu melden hat. Auch die stigmatisierende Wirkung einer derartigen Maßnahme ist nicht zu unterschätzen, denn das Lebensumfeld des Betroffenen wird regelmäßig Kenntnis von der Maßnahme erhalten. Insofern erscheint die im Gesetzentwurf in § 16 a Abs. 3 vorgesehene Höchstfrist von sechs Monaten mit der Verlängerungsmöglichkeit um weitere sechs Monate unangemessen hoch.

In Rheinland-Pfalz⁸ ist die Meldeauflage zunächst auf höchstens einen Monat befristet. Auch steht dort die Verlängerung der Anordnung unter Richtervorbehalt. Diese zusätzlichen verfahrensrechtlichen Anforderungen hinsichtlich der Dauer und der Anordnungsbefugnis bei einer Verlängerung der Meldeauflage sollten mit Blick auf den Verhältnismäßigkeitsgrundsatz auch in den hiesigen Gesetzentwurf aufgenommen werden.

7. Zu Nr. 10, § 17 a

Nach Abs. 1 Satz 6, 2. Alt. können zukünftig personenbezogene Daten an geeignete Beratungsstellen übermittelt werden, wenn die gefährdete Person zustimmt. Es handelt sich bei dieser Regelung um eine Datenübermittlungsvorschrift. Nach Datenschutzrecht ist eine nachträgliche Zustimmung (Genehmigung) nicht möglich. Vielmehr muss der Betroffene im Voraus zustimmen, also einwilligen. Es wird daher angeregt, den Begriff „Zustimmung“ durch den datenschutzrechtlich zutreffenden Begriff der „Einwilligung“ zu ersetzen.

8. Zu Nr. 10, § 17 b

Mit § 17 b soll die Polizei die neuen Befugnisse der Aufenthaltsvorgabe und des Kontaktverbots erhalten, sofern eine „drohende Gefahr“ für die Begehung einer terroristischen Straftat vorliegt. In erster Linie betroffen ist nach Art. 2 Abs. 2 Satz 2 GG das Grundrecht auf Freiheit der Person, das zunächst die körperliche Bewegungsfreiheit schützt. Das persönliche Umfeld des Betroffenen wird jedoch im Regelfall ebenfalls Kenntnis von der Maßnahme erhalten, so dass auch das Grundrecht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG tangiert ist.

⁸ § 12a POG RP.

Im Vergleich zur Meldeauflage greift insbesondere das Instrument der Aufenthaltsvorgabe tiefer in diese Grundrechte der Betroffenen ein. Ausweislich der Gesetzesbegründung soll sich die Vorgabe, einen bestimmten räumlichen Bereich nicht zu verlassen, auch auf ein Gebiet innerhalb einer Gemeinde (Ort oder Ortsteil) erstrecken können. Damit wird nicht nur die Bewegungsfreiheit der Betroffenen im Vergleich zur Meldeauflage umfangreicher eingeschränkt, sondern die Aufenthaltsvorgabe kann im Einzelfall auch eine erheblich größere stigmatisierende Wirkung entfalten.

Aus den zur Meldeauflage genannten Gründen ist die Anordnung von Maßnahmen nach § 17 b im Vorfeld einer Gefahrenlage abzulehnen. Ferner stellt sich die Frage – wie im übrigen bei der Meldeauflage auch –, ob die Maßnahmen der Aufenthaltsvorgabe und des Kontaktverbots überhaupt geeignet sind, um mögliche terroristische Gewalttaten zu verhindern. Dies wäre nur dann der Fall, wenn ein Aufenthaltsgebot auch in Form eines Hausarrestes ausgesprochen werden könnte. Das soll aber ausweislich der Gesetzesbegründung gerade nicht auf der Rechtsgrundlage des § 17 b möglich sein. Mithin kann durch Anordnungen nach § 17 b zwar die Bewegungsfreiheit möglicher terroristischer Gefährder erheblich eingeschränkt werden. Dieser ist aber nicht gehindert, sich im Aufenthaltsgebiet frei zu bewegen und dort seine Anschläge zu verwirklichen.

Bei den in § 17 b Absatz 3 geregelten verfahrenssichernden Maßnahmen wird in der Gesetzesbegründung zunächst davon ausgegangen, dass sowohl bei der Erstanordnung als auch bei der Verlängerung einer Maßnahme nach § 17 b ein Richtervorbehalt entbehrlich sei (Absatz 1). Im darauffolgenden Absatz 2 der Gesetzesbegründung wird jedoch widersprüchlich ausgeführt, dass wegen der besonderen Eingriffsintensität über die allgemein geltende Verpflichtung zur Rechtsbehelfsbelehrung nach § 37 Abs. 6 Verwaltungsverfahrensgesetz hinaus eine Verpflichtung zum Hinweis auf den Eilrechtsschutz aufzunehmen sei, wenn die sofortige Vollziehbarkeit der Maßnahme angeordnet wurde. Dieser letztgenannten Einordnung hinsichtlich der Eingriffstiefe ist zu folgen mit der Forderung, dass eine richterliche Anordnung zumindest für die Verlängerung einer Maßnahme nach § 17 b verfahrenssichernd in den Gesetzentwurf aufzunehmen ist.

Für die Überprüfung der Rechtmäßigkeit einer Maßnahme nach § 17 b sollen laut Gesetzesbegründung zu Absatz 3 die Verwaltungsgerichte zuständig sein. Bisher sind für den Rechtsschutz bei freiheitsbeschränkenden Maßnahmen der Polizei die Zivilgerichte nach § 19 zuständig. Insofern sollte die Zuweisung zu den Verwaltungsgerichten bei einer Aufenthaltsvorgabe und einem Kontaktverbot, die in erster Linie den Charakter einer freiheitsentziehenden Maßnahme haben, näher begründet werden.

9. Zu Nr. 10, § 17 c

Als neue Befugnis für die Polizei soll das Instrument der elektronischen Aufenthaltsüberwachung in das Gefahrenabwehrrecht eingefügt werden. Ziel der sog. elektronischen Fußfessel ist es, potentielle Straftäter davon abzuhalten, terroristische Straftaten im Sinne des § 2 Nr. 15 bzw. organisierte Gewaltstraftaten im Sinne des § 2 Nr. 16 zu begehen. Damit soll die Fußfessel primär der Verhütung von Straftaten dienen, so auch die Gesetzesbegründung zu § 17 Abs. 1.

Mit Hilfe der elektronischen Fußfessel können in erheblichem Umfang zahlreiche Informationen über die betroffene Person gewonnen werden (soziale Kontakte sowie persönliche Beziehungen zu bestimmten Personen, Möglichkeit der Erstellung eines detaillierten Bewegungsprofils). Die Maßnahme greift daher besonders tief in das Persönlichkeitsrecht des Betroffenen und damit in das Grundrecht auf informationelle Selbstbestimmung nach Art. 1 Abs. 1 Satz 1, Art. 2 Abs. 1 GG ein. Werden neben der elektronischen Fußfessel weitere Maßnahmen angeordnet, die ebenfalls tief in die Privatsphäre eindringen, wie z. B. eine Wohnraum- und Telekommunikationsüberwachung (§§ 35 a, 33 a) sowie eine Online-Durchsuchung (§ 33 d), so drängt sich die Frage nach einer „Gesamtrechnung aller staatlicher Maßnahmen“ auf. Diese darf nach der Rechtsprechung des Bundesverfassungsgerichts nicht dazu führen, dass „nahezu lückenlos alle Bewegungen und Lebensäußerun-

gen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können".⁹ Hierzu schweigt die Gesetzgebung, obwohl sich die Frage der „Gesamtrechnung“ an dieser Stelle geradezu aufdrängt, denn die Möglichkeiten der polizeilichen Überwachungsmaßnahmen bei Gefährdern werden mit dem Gesetzentwurf erheblich erweitert.

Speziell bei der Maßnahme nach § 17 c stellt sich die grundsätzliche Frage, ob die elektronische Fußfessel überhaupt ein wirksames und damit geeignetes Mittel sein kann, um Straftaten effektiv zu verhüten. Als Gefährder eingestufte Personen müssten sich davon abhalten lassen, terroristische Straftaten bzw. schwere organisierte Gewaltstraftaten zu begehen, wenn diese eine elektronische Fußfessel tragen. Dies darf aus folgenden Gründen bezweifelt werden.

Die elektronische Aufenthaltsüberwachung ist seit 2011 ein bereits bekanntes Mittel im Strafvollzug. Sie kann als Weisung im Rahmen einer Führungsaufsicht nach § 68 b Abs. 1 S. 1 Nr. 12 StGB angeordnet werden. Eine wissenschaftliche Studie der Universität Tübingen aus dem Jahr 2015 belegt, dass die elektronische Überwachung nicht den erhofften Erfolg gebracht hat. „Insgesamt sind sich alle Akteure einig, dass eine Aufenthaltsüberwachung die Begehung neuer Straftaten letztlich nicht verhindern kann“.¹⁰ Ebenfalls eindrucksvoller Beleg für die Nichtwirksamkeit, entschlossene Gefährder mittels einer elektronischen Fußfessel von Straftaten abzuhalten, ist der Mordanschlag auf einen Priester im Juli 2016 im französischen Ort Saint Etienne du Rouvray. Einer der Attentäter trug beim Anschlag eine elektronische Fußfessel.

Im Ergebnis lässt sich damit festhalten, dass aufgrund wissenschaftlicher Erkenntnisse und Erfahrungen mit terroristischen Anschlägen die Maßnahme der elektronischen Fußfessel ein untaugliches Instrument ist, um im Sinne der Gefahrenabwehr Straftaten wirksam verhindern zu können. Daher wird aus Sicht des Datenschutzes die ersatzlose Streichung des § 17 c im Gesetzentwurf empfohlen.

Die Tatbestandsvoraussetzungen des § 17 c Abs. 1 sind so formuliert, dass bereits bei einer „drohenden Gefahr“ die Anordnung einer elektronischen Aufenthaltsüberwachung in Betracht kommt. Die Verlagerung der Eingriffsschwelle in das Vorfeld der konkreten Gefahr ist unter den zu Ziffer 6 genannten Gründen abzulehnen.

Ferner ist der in Absatz 2 formulierte Behördenleitervorbehalt als unzureichende Verfahrensvorschrift zu hinterfragen. Die Eingriffstiefe der Maßnahme in die Grundrechte der Betroffenen macht es erforderlich, dass nur ein Gericht die Anordnung treffen kann. Für einen Richtervorbehalt spricht auch, dass die Tatsachengrundlage bei einer drohenden Gefahr noch dünner ist als bei einer konkreten Gefahr. Die polizeiliche Maßnahme sollte daher von einer unabhängigen Stelle überprüft und nur von dieser angeordnet werden können. Alle bekannten Gesetze oder Gesetzentwürfe, die das Instrument der elektronischen Aufenthaltsüberwachung regeln, enthalten Richtervorbehalte.¹¹

Unabhängig von der Frage des Richtervorbehaltes fällt an dieser Stelle besonders die Regelung zur Delegationsmöglichkeit nach § 17 c Abs. 2 Satz 2 ins Auge. Danach kann die Behördenleitung ihre Anordnungsbefugnis auf Dienststellenleiter sowie Beamte der Laufbahngruppe 2 ab dem zweiten Einstiegsamt übertragen. Vergleichbare Regelungen finden sich bei den besonders eingriffsintensiven Überwachungsmaßnahmen der Telekommunikationsüberwachung (§ 33 a Abs. 7 Satz 5) oder Online-Durchsuchung (§ 33 d Abs. 4 Satz 6), sofern Gefahr im Verzug vorliegt, aber auch bei weniger grundrechtsintensiven Maßnahmen, wie z. B. der Einrichtung einer Kontrollstelle (§ 14

⁹ BVerfG NJW 2016, 1781, Rn. 130.

¹⁰ Bräuchle/Kinzig, Die elektronische Aufenthaltsüberwachung im Rahmen der Führungsaufsicht, Kurzbericht über die wesentlichen Befunde einer bundesweiten Studie mit rechtspolitischen Schlussfolgerungen, Tübingen 2015, S. 12.

¹¹ Vgl. z. B. § 56 Abs. 5 BKAG, Art. 34 Abs. 3 PAG BY.

Abs. 2 Satz 1). Die Regelungen im Gesetzentwurf über die Anordnungsbefugnisse der Polizei lassen keine ausreichende Differenzierung erkennen, die dem Eingriffsgewicht und der Tragweite der jeweiligen Überwachungsmaßnahme gerecht wird. Es ist verfassungsrechtlich höchst bedenklich, wenn Überwachungsmaßnahmen, die tief in die Privatsphäre der Betroffenen eindringen und zudem noch heimlich durchgeführt werden, im Prinzip von jedem Polizeibeamten angeordnet werden können, sofern dieser nur dem ehemals höheren Dienst angehört (so durchgängig das Regelungskonzept des vorliegenden Gesetzentwurfs).

Speziell für den Fall der Maßnahme der elektronischen Aufenthaltsüberwachung findet sich beispielsweise in § 56 Abs. 5 BKAG die Regelung, dass diese nur von der Abteilungsleitung bzw. deren Stellvertretung bei Gericht beantragt werden kann. Bei Gefahr im Verzug kann die Anordnung nur durch die Abteilungsleitung oder deren Vertretung getroffen werden (§ 56 Abs. 5 Satz 2 BKAG). Eine Online-Durchsuchung kann nur der Präsident des BKA oder seine Stellvertretung bei Gericht beantragen. Eine Anordnung bei Gefahr im Verzug ist hier sogar ausdrücklich ausgeschlossen, nicht jedoch bei der Wohnraumüberwachung (§ 46 Abs. 3 Satz 2 BKAG: Anordnung nur durch den Präsidenten des BKA oder seiner Stellvertretung!).

In § 17 c Absatz 3 wird geregelt, zu welchem Zweck die Daten erhoben und gespeichert werden (Satz 1). Ferner bestimmt Satz 3, inwieweit die Daten zu anderen Zwecken geändert, genutzt oder übermittelt werden dürfen. Die Regelungen werfen Fragen auf und sind überarbeitungsbedürftig.

Der derzeitige Gesetzestext lässt offen, ob die erhobenen und gespeicherten Daten zu einem Bewegungsbild zusammengefügt werden dürfen. Demgegenüber geht die Gesetzesbegründung davon aus, dass es Ziel des § 17 c ist, die Person ständig zu überwachen und auf diese Weise die Begehung von Straftaten zu verhindern. Bei einer ständigen Überwachung wird es sich kaum vermeiden lassen, dass detaillierte Bewegungsbilder über den Aufenthaltsort des Betroffenen entstehen. Wegen der zusätzlichen über die gewöhnliche Datenerhebung hinausgehenden Grundrechtsbelastung bei der Erstellung eines Bewegungsbildes über einen längeren Zeitraum, sollte diese Form der Datennutzung ausdrücklich geregelt werden, so diese tatsächlich beabsichtigt ist.¹² Ein Richtervorhalt wäre zusätzlich unter dem Gesichtspunkt der Verhältnismäßigkeit als Verfahrensvoraussetzung erforderlich.¹³ Der Anwender einer Befugnisnorm, mit der in erheblichem Umfang in Grundrechte eingegriffen wird, muss klar erkennen können, in welchem Umfang er die Maßnahme anwenden darf.

Ferner sind die den Grundrechtseingriff flankierenden Verfahrensregelungen (neben dem fehlenden Richtervorbehalt), die mit Blick auf die Erheblichkeit des Eingriffs diesen erst verhältnismäßig ausgestalten, unzureichend. Es fehlt an einer bereichsspezifischen Löschungsvorschrift nach Beendigung der Maßnahme, um der Polizei von Anfang an die Möglichkeit einer Datenspeicherung auf Vorrat zu nehmen. Die bayerische Polizei sowie das BKA müssen die im Rahmen einer elektronischen Aufenthaltsüberwachung gewonnenen Daten spätestens nach zwei Monaten löschen.¹⁴

Der Gesetzesbegründung ist zu entnehmen, dass nach Satz 4 die nach Satz 1 erhobenen Daten gegen unbefugte Kenntnisnahme besonders zu sichern sind. Dies wird aus Sicht des Datenschutzes ebenfalls für erforderlich gehalten, jedoch fehlt im Gesetzestext bisher eine derartige Regelung. Der Gesetzestext sollte daher § 56 Abs. 2 Satz 4 BKAG entsprechend ergänzt werden.

¹² Vgl. z. B. Art. 34 Abs. 2 Satz 3 PAG BY.

¹³ Vgl. z. B. Art. 34 Abs. 3 Satz 3 PAG BY.

¹⁴ Art. 34 Abs. 4 Satz 1 PAG BY, § 56 Abs. 2 Satz 5 BKAG.

10. Zu Nr. 12 a), § 20 Abs. 4 Satz 4

Mit dem neuen Satz 4 in § 20 Abs. 4 soll erstmals eine ausdrückliche Rechtsgrundlage für die Videoüberwachung in Gewahrsamseinrichtungen der Polizei geschaffen werden. Dieses Anliegen ist aus Sicht der LfD grundsätzlich zu begrüßen, denn die bisher in Einzelfällen durchgeführte Videoüberwachung von in Gewahrsam genommenen Personen durch die Polizei ist wegen einer fehlenden gesetzlichen Rechtsgrundlage rechtswidrig. Die Thematik der fehlenden Rechtsgrundlage für eine Datenverarbeitung wurde mit dem Ministerium für Inneres und Sport (MI) im Jahr 2017 ausführlich erörtert.

Nach Kenntnis der LfD¹⁵ findet derzeit in den Gewahrsamszellen der Polizeidirektion Göttingen und der Polizeidirektion Osnabrück eine anlassbezogene Videoüberwachung statt. Ferner kündigte das MI im April 2017 an, zukünftig in allen polizeilichen Gewahrsamseinrichtungen Videoüberwachungsanlagen vorhalten zu wollen. Hintergrund dieser Ankündigung war der Selbstmord des terrorverdächtigen Häftlings Al-Bakr in einer sächsischen Justizvollzugsanstalt im Oktober 2016, der auch Gegenstand umfangreicher Presseberichterstattung war. Seinerzeit vertrat das MI die Rechtsauffassung, dass § 20 Abs. 4 Satz 3 Nds. SOG eine ausreichende Rechtsgrundlage für die Videoüberwachung von Gewahrsamseinrichtungen sei.

Die LfD ist der Ansicht, dass § 20 Abs. 4 Satz 3 keine ausreichende Rechtsgrundlage für eine Videoüberwachung von Gewahrsamszellen sein kann. Datenerhebungen mittels einer Videoüberwachung sind nach der neueren höchstrichterlichen Rechtsprechung in einer bereichsspezifischen Rechtsgrundlage zu normieren, die den verfassungsrechtlichen Grundsätzen der Bestimmtheit und Normenklarheit genügt. Ein Rückgriff auf Generalklauseln oder Normen, die gerade nicht einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung ausdrücklich regeln, ist unzulässig.¹⁶ Zahlreiche Länder verfügen daher bereits über entsprechende Befugnisnormen in ihren Polizeigesetzen.¹⁷

Nach § 20 Abs. 4 Satz 3 dürfen der festgehaltenen Person Beschränkungen auferlegt werden, die der Zweck der Freiheitsentziehung oder die Ordnung im Gewahrsam erfordern. Unter Beschränkungen sind in erster Linie Maßnahmen zu verstehen, die die Bewegungsfreiheit der Person (z. B. Fesselung) oder die allgemeine Handlungsfreiheit einschränken (z. B. Wegnahme von Gegenständen). Der Begriff der „Beschränkung“ ist als Generalklausel zu verstehen und damit nicht bestimmt genug, um Eingriffe in das Grundrecht auf informationelle Selbstbestimmung zu rechtfertigen.

In der Gesetzesbegründung wird nunmehr ausgeführt, dass angesichts der Schwere des Eingriffs durch eine offene Beobachtung der betroffenen Person eine spezifische gesetzliche Regelung zur Videoüberwachung für erforderlich gehalten wird. Damit schließt sich im Ergebnis das MI der Rechtsauffassung der LfD an.

Bei einer Videoüberwachung von in Gewahrsam genommenen Personen, die dieser Maßnahme schutzlos ausgeliefert sind, spielt der Grundsatz der Verhältnismäßigkeit eine überaus wichtige Rolle. Davon geht auch die Gesetzesbegründung aus. Denkbar sind je nach Gefahrenlage eine Dauerüberwachung oder eine nur zeitweise stattfindende Beobachtung. Geht es allein um den Schutz von Bediensteten oder Dritten, so kommt eine Videoüberwachung nur in Betracht, wenn diese Personen Kontakt mit dem Häftling haben. Um den Verhältnismäßigkeitsgrundsatz auch im Tatbestand eindeutig zu verankern, sollte daher die Formulierung „wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen“ ersetzt werden durch die Formulierung „wenn und soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen“.

¹⁵ Schreiben des Niedersächsischen Ministeriums für Inneres und Sport (MI) vom 04.04.2017.

¹⁶ BVerfG, NVwZ 2007, 688; BVerwGE 139, 323-336, Rz. 28.

¹⁷ Z. B. § 21 Abs. 4 PolG BW; § 8 Abs. 4 PolEDVG HH; § 34 Abs. 3 S. 3 HSOG; § 39 Abs. 4 SOG LSA; § 204 Abs. 4 S. 2 LVwG SH.

Aus Sicht des Datenschutzes ist es erfreulich, dass nur eine offene Beobachtung mittels Bildübertragung zulässig sein soll. Bildaufzeichnungen sind daher ausdrücklich ausgeschlossen. Auch beschränkt § 20 Abs. 3 Satz 4 die Videoüberwachung auf den Schutz der betroffenen Personen gegen Gefahren für Leib oder Leben. Zur Straftatenverhütung, so wie in anderen Ländern vorgesehen¹⁸, darf die Videoüberwachung damit zukünftig nicht eingesetzt werden.

Zwingend erforderlich bei einer Videoüberwachung von Inhaftierten sind auch Regelungen, die den Kernbereich der privaten Lebensgestaltung schützen. Der Gefangene ist einer Beobachtung in einer kleinen Gewahrsamszelle ansonsten völlig schutzlos ausgeliefert. Dies ist mit dem Grundrecht der Menschenwürde nicht vereinbar.¹⁹

11. Zu Nr. 18 a) bb), § 30 Abs. 4 Satz 2

Mit dem neuen Satz 2 in Abs. 4 Satz 1 soll die Unterrichtungspflicht bei Datenerhebungen mit besonderen Mitteln oder Methoden ausgeweitet werden. Damit wird auf die Rechtsprechung des Bundesverfassungsgerichts zum BKA-Gesetz reagiert. Danach entsprechen verdeckt durchgeführte Maßnahmen nur dann dem Grundsatz der Verhältnismäßigkeit, wenn diese gleichzeitig den Anforderungen an Transparenz, individuellem Rechtsschutz und aufsichtlicher Kontrolle genügen. Hierzu gehört auch, dass bei heimlich durchgeführten Maßnahmen zur Gewährung individuellen Rechtsschutzes die Betroffenen nachträglich zu benachrichtigen sind. Insofern ist es folgerichtig, dass bei Datenerhebungen nach § 45 a (Rasterfahndung) zukünftig die betroffenen Personen unterrichtet werden sollen, wenn sich nach Auswertung der Daten weitere Maßnahmen anschließen.

Neben der Rasterfahndung ist zukünftig eine Unterrichtungspflicht auch für eine Videoüberwachung nach § 32 Abs. 2 vorzusehen,²⁰ die in § 30 Abs. 2 Nr. 1 ebenso wie die Rasterfahndung (§ 30 Abs. 2 Nr. 3) als verdeckte Datenerhebung anzusehen ist und die ebenso darauf abzielt, konkrete Verdachtsmomente gegenüber bestimmten Personen zu gewinnen. Insofern wird das Urteil des Bundesverfassungsgerichts an dieser Stelle nur unzureichend umgesetzt. Die Landesregierung sieht bislang keinen Grund, auch im Falle einer verdeckten Videoüberwachung nachträglich die Betroffenen zu benachrichtigen.²¹ Die Rasterfahndung ist jedoch mit der Maßnahme einer verdeckt durchgeführten Videoüberwachung öffentlich zugänglicher Räume durchaus vergleichbar.

Bei der sog. positiven Rasterfahndung werden zum Zweck der Gefahrenabwehr in einem ersten Schritt Massendatensätze von zunächst unverdächtigen Personen maschinell gegeneinander abgeglichen. Davon erfahren die Betroffenen nichts. Verläuft die Rasterung erfolgreich, stehen von nun an bestimmte Personen im Fokus der polizeilichen Ermittlungen. Es können sich in einem zweiten Schritt weitere offen oder verdeckt durchgeführte Maßnahmen anschließen, die jedoch ihrerseits eine eigenständige Rechtsgrundlage erfordern (z. B. Identitätsfeststellung nach § 13 oder Observation nach § 34). Spätestens zu diesem Zeitpunkt besteht eine Unterrichtungspflicht. Die Polizei hat grundsätzlich offenzulegen, dass die Tatsachen, die zur Begründung der Anschlussmaßnahme herangezogen werden, mit Hilfe einer Rasterfahndung gewonnen wurden. Nur so kann diese Gegenstand einer nachträglichen richterlichen Überprüfung werden.

Im Bereich der Gefahrenabwehr fällt besonders ins Gewicht, dass Ermittlungsmaßnahmen nicht zwangsläufig wie im Strafverfahren gegen bestimmte Personen geführt werden. Dort kann eine etwaige Datenerhebung im Vorfeld zum Gegenstand des Strafprozesses gemacht werden. Diese ist dann für den Betroffenen nachvollziehbar und wird Gegenstand einer nachträglichen gerichtlichen Überprüfung.²² Dass die Anordnung der Rasterfahndung unter Richtervorbehalt steht, mache eine

¹⁸ Z. B. § 21 Abs. 4 PolG BW.

¹⁹ Vgl. hierzu die Regelungen in den Justizvollzugsgesetzen der Länder, z. B. § 144 Abs. 4 JVollzGB LSA.

²⁰ Sofern nicht dem Vorschlag gefolgt wird, die Befugnisnorm des § 32 Abs. 2 ersatzlos zu streichen!

²¹ LT-Drs. 17/6232, S. 43.

²² So das BVerfG, NJW 2016, 1781, Rn. 267.

nachträgliche gerichtliche Überprüfung nicht überflüssig, denn nur in dieser könne die Rechtmäßigkeit der Durchführung der Maßnahme - u. a. ob und in welchem Umfang von dieser Gebrauch gemacht wurde - überprüft werden.

Deckungsgleich ist die Sachlage beim Instrument der verdeckten Videoüberwachung nach § 32 Abs. 2. Auch hier werden in einem ersten Schritt die Daten einer Vielzahl unverdächtigter Personen erhoben. Durch gezielte Bildauswertung können dann bestimmte Personen in Verdacht geraten, gegen die in einem zweiten Schritt Anschlussmaßnahmen ergriffen werden.

Kommt es dann nur zu gefahrenabwehrrechtlichen Maßnahmen, die im Sande verlaufen, schließt sich demnach kein Strafverfahren an, wird der davon Betroffene nichts von der verdeckt durchgeführten Maßnahme der Videoüberwachung erfahren. Diese wäre demnach einer richterlichen Kontrolle vollständig entzogen. Ferner ist zu berücksichtigen, dass im Gegensatz zur Rasterfahndung die verdeckte Videoüberwachung anordnungslos durchgeführt werden kann (weder Richter- noch Behördenleitervorbehalt). Umso wichtiger ist es, dass über den Weg der Benachrichtigung eine nachträgliche gerichtliche Kontrollmöglichkeit eröffnet wird.

Die gleichen Überlegungen gelten auch bei einer Maßnahme nach § 32 Abs. 5 (§ 32 Abs. 6 neu), sofern das sog. Kennzeichenlesegerät als verdeckt durchgeführte Datenerhebung eingesetzt wird und ein sog. „Trefferfall“ vorliegt. Auch hier ist eine Unterrichtung der betroffenen Personen nach hiesiger Lesart des Urteils des Bundesverfassungsgerichts zum BKA-Gesetz gesetzlich vorzusehen.

12. Zu Nr. 18 b) aa) - cc), § 30 Abs. 5 Satz 1

Mit der Neufassung des Satzes 1 in § 30 Abs. 5 werden die Gründe zusammengefasst, aus denen eine Zurückstellung der Benachrichtigung der Betroffenen möglich ist. Das damit verbundene Systematisierungsanliegen, diese Gründe in einer abschließenden Aufzählung zusammenzufassen, ist mit Blick auf die erleichterte Rechtsanwendung zu begrüßen. Verfassungsrechtlich problematisch ist jedoch der Zurückstellungsgrund des § 30 Abs. 5 Satz 1 Nr. 2. Danach kann von einer Benachrichtigung zunächst abgesehen werden, solange Zwecke der Verfolgung einer Straftat entgegenstehen.

Zu den Anforderungen an eine dem Verhältnismäßigkeitsgrundsatz genügende Ausgestaltung von heimlich durchgeführten Maßnahmen gehört die gesetzliche Anordnung von Benachrichtigungspflichten. Ausnahmen von dem Grundsatz der nachträglichen Benachrichtigung sind nur in Abwägung mit verfassungsrechtlich geschützten Rechtsgütern Dritter möglich. Diese Ausnahmen sind auf das unbedingt erforderliche Maß zu beschränken.²³

Vor dem Hintergrund dieser gefestigten Rechtsprechung ist die Vorschrift des § 30 Abs. 5 Satz 1 Nr. 2 zu weit gefasst. Danach wird die Benachrichtigung zurückgestellt, solange der Zweck der Verfolgung einer Straftat entgegensteht. Eine Einschränkung auf erhebliche oder besonders schwerwiegende Straftaten sieht der derzeitige Gesetzeswortlaut nicht vor. Demnach kann die Unterrichtung derzeit auch zurückgestellt werden, wenn es um die Strafverfolgung von Bagatelldelikten wie z. B. einer Beleidigung geht. Das Recht auf Unterrichtung wird für die Betroffenen daher nach der vorliegenden Fassung des Ausnahmegrundes über das verfassungsrechtlich zulässige Maß eingeschränkt.

²³ BVerfG NJW 2016, 1781, Rn. 136.

13. Zu Nr. 18 b) dd), § 30 Abs. 5 Satz 2

Mit der beabsichtigten Änderung wird die Frist zur Überprüfung einer weiteren Zurückstellung der Benachrichtigung durch das Gericht von sechs Monaten auf ein Jahr verlängert. Dies stellt eine Verschlechterung der Rechte der Betroffenen dar. Aus Sicht des Datenschutzes ist die Verlängerung der Frist um sechs Monate daher abzulehnen.

Zu Nr. 18 c), § 30 Abs. 7 neu

Mit der Neuformulierung des Abs. 7 soll eine Vorschrift geschaffen werden, die es unter den dort genannten Voraussetzungen ermöglicht, endgültig von einer Benachrichtigung der Betroffenen bei verdeckten Datenerhebungen abzusehen.

Die vorgeschlagene Regelung orientiert sich an den Vorgaben des Bundesverfassungsgerichts, das vergleichbare Vorschriften (§ 20 w Abs. 3 Satz 5 BKAG a. F. bzw. § 74 Abs. 3 Satz 4 BKAG n. F. sowie § 101 Abs. 6 Satz 3 StPO) verfassungsrechtlich nicht beanstandet hat. Danach kann nach Ablauf von fünf Jahren endgültig von einer Benachrichtigung abgesehen werden, wenn die Voraussetzungen für eine Unterrichtung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden. Ferner muss hinzukommen, dass die weitere Verwendung der Daten gegen den Betroffenen ausgeschlossen ist und die Daten gelöscht werden.²⁴

Der vorgeschlagene Gesetzestext setzt diese Vorgaben im Wesentlichen um. Zur Klarstellung, dass eine weitere Verwendung der Daten tatsächlich ausgeschlossen ist, sollte der Gesetzgeber jedoch nicht nur fordern, dass die „Voraussetzungen für eine Löschung der Daten vorliegen“. Vielmehr sollte der Wortlaut im Sinne des § 74 Abs. 3 Satz 5 BKAG konkretisiert werden. Danach kann von einer Benachrichtigung nur dann endgültig abgesehen werden, wenn „die Daten gelöscht wurden“. Es ist allerdings dann sicherzustellen, dass die fraglichen Daten für die durchzuführende gerichtliche Überprüfung noch zur Verfügung stehen.

10. Zu Nr. 19, § 31 a

Die Einführung eines über die Vorgaben des Bundesverfassungsgerichts hinausgehenden absoluten Datenerhebungsverbots bei bestimmten Berufsheimnisträgern (Geistliche, Strafverteidiger, Rechtsanwälte und Abgeordnete) wird aus datenschutzrechtlicher Sicht ausdrücklich begrüßt.²⁵

Allerdings wird das Datenerhebungsverbot nur auf Datenerhebungen begrenzt, die mit besonderen Mitteln und Methoden erfolgen. Dies ist nicht nachvollziehbar, wenn in der Begründung Bezug auf vergleichbare Regelungen im BKAG und in der StPO genommen wird. Der Schutz zeugnisverweigerungsberechtigter Berufsheimnisträger nach § 160 a Abs. 1 StPO, an den sich § 31 a neu vom Wortlaut her anlehnt und der demnach dieselben Berufsgruppen umfasst, bezieht sich sowohl auf verdeckt als auch auf offen durchgeführte Ermittlungsmaßnahmen.²⁶ Sämtliche Ermittlungsmaßnahmen, die auf die Erforschung des Sachverhaltes ausgerichtet sind, werden von § 160 a Abs. 1 StPO erfasst, also auch offen durchgeführte Datenerhebungsmaßnahmen wie z. B. §§ 99, 110, 161 StPO.²⁷ Um das nach der Gesetzesbegründung zu § 31 a Abs. 1 angestrebte absolute Datenerhebungsverbot bei Geistlichen, Strafverteidigern, Rechtsanwälten und Abgeordneten zu erreichen, müsste die Vorschrift daher sämtliche Formen der Datenerhebung - verdeckt wie auch offen durchgeführte Maßnahmen - umfassen.

²⁴ BVerfG, NJW 2016, 1781, Rn. 262 m. w. N.

²⁵ Siehe dazu auch die Ausführungen unter Zif. 4

²⁶ BeckOK StPO/Sackreuther, § 160a, Rn. 3.

²⁷ KK-StPO/Griesbaum, § 160a, Rn. 4.

11. Zu Nr. 19, § 31 b

Die bisher an verschiedenen Stellen des Gesetzes normierten Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung sollen nach dem Gesetzentwurf zukünftig in der Norm des § 31 b zusammengeführt werden. Ferner werden die Schutzvorschriften im Lichte der Rechtsprechung des Bundesverfassungsgerichts erweitert und so der Kernbereichsschutz verbessert. Dieses Vorgehen ist mit Blick auf eine Vereinfachung der Rechtsanwendung zwar verständlich, sollte aber aus den nachfolgenden Gründen kritisch hinterfragt werden. Das Bundesverfassungsgericht hat im Einzelnen unterschiedliche Vorgaben für die Phase der Datenerhebung und die sich anschließende Phase der Auswertung und Verwertung gemacht, die je nach Maßnahme durchaus unterschiedlich zu betrachten sind.

Nach Absatz 1 darf eine Datenerhebung mit besonderen Mitteln oder Methoden nicht angeordnet werden, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dadurch nicht nur zufällig Daten erhoben werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Diese Vorgabe mag für die bisher vorhandenen Maßnahmen der Wohnraum- oder Telekommunikationsüberwachung umsetzbar sein, nicht aber für die neue Maßnahme der sog. Online-Durchsuchung nach § 33 d.

Der verdeckte Eingriff z. B. in den Privatcomputer oder das Smartphone einer Zielperson führt zwangsläufig dazu, dass auch Daten erhoben werden, die dem Kernbereichsschutz unterfallen. Die Maßnahme der Online-Durchsuchung erfasst naturgemäß zunächst sämtliche Daten des informationstechnischen Systems und damit auch höchstpersönliche Daten des Betroffenen. Es wird heutzutage keinen PC oder kein Smartphone geben, auf dem sich nicht Daten befinden, die dem Kernbereich privater Lebensgestaltung zuzuordnen sind. Insofern könnte eine Maßnahme nach § 33 d bei wörtlicher Anwendung des § 31 b Abs. 1 Satz 1 in keinem Fall angeordnet werden. Konsequenterweise geht z. B. § 49 Abs. 7 Satz 1 BKAG davon aus, dass eine Online-Durchsuchung nur dann unzulässig ist, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden. Im Ergebnis muss es daher eine spezielle Regelung zum Kernbereichsschutz bei einer Maßnahme nach § 33 d geben, die die Besonderheiten der Maßnahme bei der Durchführung in den Blick nimmt.

Gegen das Regelungskonzept zum Schutz des Kernbereichs privater Lebensgestaltung in einer einzigen Norm, die für alle Datenerhebungen mit besonderen Mitteln oder Methoden einheitlich Anwendung finden soll, spricht auch die Tatsache, dass in den Sätzen 2 und 3 des Absatzes 1 Regelungen enthalten sind, die sich nur auf die Wohnraumüberwachung beziehen.

Nach Absatz 5 kann bei Gefahr im Verzug die Dienststellenleitung bei Aufzeichnungen entscheiden, ob Daten erhoben wurden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Eine derartige Regelung, die es der Polizei ermöglichen soll, in Ausnahmefällen bei Gefahr im Verzug auch kurzfristig Aufzeichnungen vorzunehmen und damit handlungsfähig zu sein, ist nach der Rechtsprechung des Bundesverfassungsgerichts grundsätzlich möglich.²⁸ Jedoch sollen hierbei nicht zur Zweifelsfälle herausgefiltert werden, sondern weiterer Zweck dieser Sichtung der Aufzeichnungen ist auch eine Rechtmäßigkeitskontrolle der Maßnahme durch eine unabhängige Stelle insgesamt.²⁹ Daher ist es nicht ausreichend, wenn die Sichtung allein von der Dienststellenleitung vorgenommen wird, die bei Gefahr im Verzug die Maßnahme selbst angeordnet hat. Es wird daher zur verfassungsmäßigen Absicherung vorgeschlagen, die Regelung des Absatzes 5 dahingehend zu erweitern, dass eine weitere unabhängige Stelle mit über die Auswertung entscheidet.³⁰

²⁸ BVerfG NJW 2016, 1781, Rn. 204.

²⁹ BVerfG NJW 2016, 1781, Rn. 200 und 204.

³⁰ So z. B. nach § 49 Abs. 8 Satz 1 BKAG der Datenschutzbeauftragte des BKA.

12. Zu Nr. 20 a), § 32 Abs. 1 Satz 1

Die gesetzliche Klarstellung der Differenzierung zwischen Bildübertragungen und Bildaufzeichnungen wird begrüßt. Der mit einer Videoüberwachung verbundene Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen verlangt nach einer bereichsspezifischen und präzise formulierten Rechtsgrundlage, so dass für die Polizei deutlich wird, in welcher Form und zu welchem Zweck personenbezogene Daten erhoben werden dürfen.

Eine Beobachtung mittels Bildübertragung in Form des sog. Monitoring-Verfahrens ist eindeutig dem Zweck der Gefahrenabwehr zuzuordnen, denn die Erhebung der Bilddaten in Echtzeit dient dem Erkennen von Gefahrensituationen, auf die unmittelbar reagiert werden kann, um einen Schadenseintritt zu vermeiden. Bildaufzeichnungen dienen nicht nur der Abwehr einer Gefahr oder Verhütung einer Straftat. Mit ihnen kann strafbares Verhalten dokumentiert werden, um Täter zu identifizieren und Strafverfolgungsmaßnahmen einzuleiten. Die aufgezeichneten Bilder können in einem späteren Strafverfahren als Beweismittel verwendet werden. Daher leistet die Datenerhebung mittels einer Bildaufzeichnung einen Beitrag zur Strafverfolgung. Die Neuformulierung des § 32 Abs. 1 berücksichtigt diese unterschiedlichen Zwecke bei der Datenerhebung nunmehr ausdrücklich. Dies schafft Rechtsklarheit bei der Frage, zu welchem Zweck die Daten verarbeitet werden.

13. Zu Nr. 20 b), § 32 Abs. 2

Mit der vorgeschlagenen Änderung soll eine verdeckte Anfertigung von Aufzeichnungen nur noch zulässig sein, wenn es um die Verhütung von Straftaten geht. Das Instrument der verdeckten Videoüberwachung bleibt damit erhalten und wird nicht in Frage gestellt. Dies ist aus folgenden Gründen nicht akzeptabel.

Eine verdeckte Videoüberwachung greift in besonders starkem Maße in das Grundrecht auf informationelle Selbstbestimmung ein. Es ist daher besonders sorgfältig zu prüfen, inwieweit eine derartige Maßnahme zum Zweck der Gefahrenabwehr erforderlich ist. Werden lediglich Bildaufzeichnungen vorgenommen - also gerade keine Bildübertragungen - so ist nicht erkennbar, wie akute Gefahrenlagen mit Hilfe der Videoüberwachung beseitigt werden können. Auch fehlt der Videoüberwachung nach dieser Vorschrift der einer offenen Maßnahme innewohnende Abschreckungseffekt, mit dem sich allenfalls eine Präventivmaßnahme begründen ließe. Vielmehr dient § 32 Abs. 2 ausschließlich dem Zweck, durch nachträgliche Auswertung des Bildmaterials Strafverfahren einleiten zu können. Dies aber ist verfassungswidrig, denn für eine Regelung zu Bildaufzeichnungen, die in keinem denkbaren Fall auch zum Zweck der Gefahrenabwehr genutzt werden können, fehlt dem Landesgesetzgeber die Gesetzgebungskompetenz.³¹ Die Vorschrift des § 32 Abs. 2 ist daher ersatzlos zu streichen, zumal nach Kenntnis der LfD die verdeckte Videoüberwachung in der Polizeipraxis auch keine Rolle spielt. Die Regelung läuft daher ins Leere. Nur in Rheinland-Pfalz existiert derzeit noch eine vergleichbare Regelung,³² in Berlin hat der Gesetzgeber eine verdeckt durchgeführte Videoüberwachung ausdrücklich untersagt.³³

Die betroffenen Personen einer verdeckt durchgeführten Videoüberwachung mittels Anfertigung von Aufzeichnungen werden in der Regel nichts von dieser Maßnahme erfahren. Damit sind die Rechtsschutzmöglichkeiten gegen eine Datenerhebung nach § 32 Abs. 2 verkürzt. Insofern ist die Eingriffsmaßnahme vergleichbar mit den in § 37 a aufgeführten Maßnahmen, die einer besonderen parlamentarischen Rechtmäßigkeitskontrolle unterliegen. Auch fehlt eine Regelung zur Anordnungsbefugnis (kein Behördenleiter- bzw. Richtervorbehalt). Die bisherige Regelung des § 32 Abs. 2 ist daher auch aus diesen Gründen verfassungswidrig.

³¹ Vgl. Roggan NVwZ 2001, 134 (139).

³² § 27 Abs. 2 POG RP.

³³ § 24 Abs. 1 S. 3 ASOG BE.

Daher müssen zumindest weitere, die Maßnahme flankierende Regelungen getroffen werden, die erst zur Verhältnismäßigkeit einer verdeckten Videoüberwachung führen. So ist die parlamentarische Kontrolle durch den sog. § 37 a - Ausschuss notwendig. Aufzunehmen sind alle verdeckt durchgeführten Eingriffsmaßnahmen, um mangelnde Rechtsschutzmöglichkeiten der betroffenen Personen durch eine parlamentarische Kontrolle zu kompensieren. Dies betrifft neben der Rasterfahndung nach § 45a³⁴ auch die verdeckte Anfertigung von Aufzeichnungen nach § 32 Abs. 2, die in § 30 Abs. 2 Satz 1 Nr. 1 ausdrücklich als „verdeckte Datenerhebung“ genannt wird.

Aus Sicht des Datenschutzes wäre es jedoch vorzugswürdiger, § 32 Abs. 2 ersatzlos zu streichen.

14. Zu Nr. 20 c), § 32 Abs. 3

Die Neuregelung der offenen Videoüberwachung zur Gefahrenabwehr ist mit Blick auf die verfassungsrechtlichen Anforderungen an die Bestimmtheit und Normenklarheit einer in Grundrechte eingreifenden Rechtsnorm überfällig. Die derzeit geltende Rechtslage ist verfassungsrechtlich bedenklich. § 32 Abs. 3 Satz 1 ist zu weitgehend und zu unbestimmt formuliert,³⁵ weil eine Videoüberwachung nach derzeitigem Recht durchgeführt werden kann, wenn diese zur Erfüllung von Aufgaben nach § 1 Abs. 1 erforderlich ist. Insofern ist der Regelungsansatz zu begrüßen, dass die Eingriffsvoraussetzungen im Gesetzentwurf nunmehr klarer und damit einschränkender definiert werden.

Alle Formen der Videoüberwachung durch Bildübertragung oder Bildaufzeichnung, greifen erheblich in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen ein. Es ist daher nicht nachvollziehbar, warum diese Maßnahme auch in Fällen von Ordnungswidrigkeiten Anwendung finden soll (§ 32 Abs. 3 Satz 1 Nr. 1 und Nr. 2). Vielmehr sollte die Videoüberwachung als Mittel der Gefahrenabwehr aus Gründen der Verhältnismäßigkeit nur zur Verhütung von Straftaten zulässig sein.³⁶

Nach Absatz 3 Nr. 3 soll zukünftig eine offene Videoüberwachung öffentlich zugänglicher Räume in Form der Bildübertragung an besonders gefährdeten Objekten zulässig sein, wenn dies zur Erfüllung von Aufgaben nach § 1 Abs. 1 erforderlich ist. Es ist fraglich, ob die Verweisung auf § 1 Abs. 1 verfassungsrechtlichen Anforderungen genügt, um den Umfang und den Zweck der Videoüberwachung bestimmt genug zu regeln. Ausweislich der Gesetzesbegründung besteht der Zweck der Videoüberwachung in den Fällen des Absatzes 3 Nr. 3 darin, Versorgungseinrichtungen, ausländische Vertretungen, Amtsgebäude und ähnliche Objekte vor Anschlägen zu schützen. Es geht also auch hier um die Verhütung von Straftaten. Somit sollte dieser Zweck auch gesetzlich ausdrücklich normiert werden.

Die Regelung zur Kenntlichmachung in Absatz 3 Satz 2 entspricht den allgemeinen datenschutzrechtlichen Grundanforderungen für eine offen durchgeführte Videoüberwachung. Eine Vorschrift über die Kennzeichnung der offenen Videoüberwachung findet sich mittlerweile in allen Landesgesetzen. Daher ist die vorgeschlagene Gesetzesänderung überfällig. In einigen Ländern muss auch auf die verantwortliche Stelle hingewiesen werden.³⁷ Dies ist bürgerfreundlich und sinnvoll, da die Betroffenen sogleich wissen, wer für die Videoüberwachung verantwortlich ist und an wen sie sich bei Fragen wenden können (z. B. die Kommune oder die Polizei in den Fällen des Abs. 3).

³⁴ Zukünftig soll die Rasterfahndung Gegenstand des § 37a-Berichts sein, vgl. hierzu Nr. 30 a) (§37a) des Gesetzentwurfs.

³⁵ VG Hannover NVwZ-RR 2011, 943 (945).

³⁶ Vgl. z. B. § 21 Abs. 2 u. Abs. 3 PolG BW; § 15 a Abs. 1 PolG NW; § 24 Abs. 1 ASOG BE.

³⁷ Z. B. § 14 Abs. 3 S. 2 Hess.SOG.

Mit der Kennzeichnung wird nicht nur die Offenheit der Videoüberwachung sichergestellt. Gleichzeitig kommt die verantwortliche Stelle damit auch ihren Informationspflichten gegenüber den Betroffenen zum Zeitpunkt der Datenerhebung nach. Diese wurden durch das neue europäische Datenschutzrecht erheblich erweitert - auch bei Datenerhebungen im Anwendungsbereich der sog. JI-Richtlinie. Hier sind zukünftig die Regelungen des § 50 NDSG zu beachten, der als Verweisnorm zur Klarstellung mit in den Gesetzestext aufgenommen werden sollte.

Mit der Änderung im neuen § 32 Abs. 3 Satz 3 Nr. 1 (Streichung der Worte „von erheblicher Bedeutung oder Straftaten nach § 224 StGB“) werden die Möglichkeiten, Bildaufzeichnung zum Zweck der Verhütung von Straftaten anzufertigen, erheblich ausgeweitet. Zukünftig können sowohl Bildübertragungen zum Zweck der Straftatenverhütung vorgenommen und daneben gleichzeitig (oder stattdessen?) auch Bildaufzeichnungen (auch) zur Strafverfolgung angefertigt werden. Die Gesetzesbegründung führt dazu aus, dass zukünftig auch einfache Straftaten, wie etwa Beleidigungen auf sexueller Grundlage oder aber Diebstahlshandlungen in Form des sog. „Antanzens“ mit Hilfe des aufgezeichneten Bildmaterials verfolgt werden sollen. Im Ergebnis werden damit beide Formen der Videoüberwachung als gleichrangige Maßnahmen für zulässig erklärt. Dies ist mit Blick auf die Gesetzgebungskompetenz des Landesgesetzgebers, der nur Maßnahmen regeln kann, die dem Gefahrenabwehrrecht zuzurechnen sind, als zu weitgehend abzulehnen. Vielmehr ist am Vorrang der Videoüberwachung in Form der Bildübertragung festzuhalten und zwar aus folgenden Gründen:

Im Gefahrenabwehrrecht dient die Videoüberwachung primär dem Zweck, Gefahrensituationen zu bereinigen bzw. Straftaten zu verhüten. Dies setzt voraus, dass die Behörden im Vorfeld der Realisierung der Gefahr bzw. der Begehung der Straftat die Möglichkeit haben einzugreifen. Nur im Fall einer Bildübertragung ist diese Möglichkeit gegeben, denn nur dann kann der Beamte, der die Situation in Echtzeit beobachtet, Hilfe anfordern und somit originär gefahrenabwehrrechtlich tätig werden.

Anders sieht es bei der Videoüberwachung in Form der Bildaufzeichnung aus. Eine offen durchgeführte Bildaufzeichnung hat zwar nach überwiegender Lesart auch einen präventiven und damit gefahrenabwehrrechtlichen Effekt. Würde man dies verneinen, so stünde dem Landesgesetzgeber gar keine Regelungskompetenz zu. Bei der Bildaufzeichnung liegt der Schwerpunkt des Zwecks der Datenverarbeitung jedoch bei der Aufklärung von Vorgängen im Nachgang des Geschehens. Das Bildmaterial soll dazu dienen, die begangenen Straftaten aufzuklären und die Strafverfolgung sicherzustellen. Die Strafverfolgung ist aber der Gefahrenabwehr bzw. Verhütung von Straftaten im Anwendungsbereich des Gefahrenabwehrrechts nachgelagert und damit nachrangig zu regeln. Dies sollte der Gesetzgeber berücksichtigen und den Tatbestand für die Anfertigung von Bildaufzeichnungen daher wesentlich enger formulieren als bei Bildübertragungen.

Mit der Ausweitung der Möglichkeiten zur Anfertigung von Bildaufzeichnungen verschärft sich das bereits vorhandene Problem einer fehlenden bereichsspezifischen Regelung zur Höchstspeicherdauer von Bildmaterial. So erledigt sich bei videoüberwachten Veranstaltungen der zum Zeitpunkt der Datenerhebung ursprünglich verfolgte Zweck, z. B. die Verhinderung von Taschendiebstählen, spätestens mit dem Ende der Veranstaltung. Bildaufzeichnungen müssen unverzüglich nach dem Ende der Veranstaltung ausgewertet und gelöscht werden, wenn keine strafbaren Handlungen auf der Veranstaltung begangen wurden bzw. auf dem Bildmaterial erkennbar sind. Gleiches gilt für Bildaufzeichnungen, die an kriminalitätsbelasteten öffentlich zugänglichen Räumen angefertigt wurden. Auch diese sind ohne Zeitverzug in regelmäßigen Abständen auszuwerten und zu löschen, wenn sich keine Straftaten feststellen lassen.

Für eine zeitlich unbegrenzte Speicherung der Daten besteht keine Erforderlichkeit. Ohne gesetzliche Löschfristen, die eine unverzügliche Auswertung sicherstellen, bestünde die Gefahr einer Vorratsdatenspeicherung von Videomaterial bei der Polizei bzw. den Gefahrenabwehrbehörden. Daher

gibt es in nahezu allen Ländern Regelungen über Höchstspeicherfristen.³⁸ Nach Ablauf dieser Fristen dürfen die Bildaufzeichnungen nur noch zu bestimmten Zwecken verwendet werden (u. a. Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung oder zur Geltendmachung öffentlich-rechtlicher Ansprüche).

Ich rege daher an, in § 32 Abs. 3 bereichsspezifische Löschrufen aufzunehmen, die vorsehen, dass Bildaufzeichnungen regelmäßig zeitnah nach der Datenerhebung zu löschen bzw. zu vernichten sind. Klare gesetzliche Löschrufen tragen auch dazu bei, dass die Behörden Aufzeichnungen landesweit nach einheitlichen Maßstäben speichern und löschen. Der Rückgriff auf die allgemeine Löschrufvorschrift des § 39 a hilft hier nicht weiter, weil dort keine Fristen genannt sind.

Mit Urteil vom 09.06.2016 stellte das Verwaltungsgericht Hannover fest, dass die Polizeidirektion Hannover von insgesamt 78 betriebenen Kameras 56 abzuschalten hat.³⁹ Von diesen 56 Kameras wurden 11 auf der Rechtsgrundlage des § 32 Abs. 3 Satz 2 Nds. SOG betrieben. Die Polizeidirektion konnte hier nicht den Nachweis führen, dass die Kameras an Orten aufgestellt sind, an denen künftig Straftaten begangen werden. Es lagen keine oder nur unzureichende Statistiken über begangene Straftaten vor. Auch war im Einzelnen aus den Akten nicht mehr nachvollziehbar, aus welchen Gründen eine Kamera installiert wurde.

Für die Frage der Rechtmäßigkeit einer Videoüberwachung an sog. Kriminalitätsschwerpunkten (§ 32 Abs. 3 Satz 1 Nr. 1) ist jedoch eine entsprechende Faktenlage zwingend notwendig - sowohl zum Zeitpunkt der Installation der Kamera als auch fortlaufend während der Durchführung der Maßnahme. Zum einen ist nach dem Wortlaut des Gesetzentwurfs der Nachweis zu führen, dass es sich bei dem beobachteten Ort um einen solchen handelt, an dem wiederholt Straftaten oder nicht geringfügige Ordnungswidrigkeiten begangen wurden. Nur dann kommt eine Videoüberwachung überhaupt in Betracht. Zum anderen ist zusätzlich eine Prognoseentscheidung nötig, dass an diesem Ort auch künftig Straftaten oder nicht geringfügige Ordnungswidrigkeiten begangen werden. Diese Prognoseentscheidung ist fortlaufend zu überprüfen und zu hinterfragen. Geht das Straftatenaufkommen signifikant zurück, wäre eine Videoüberwachung nicht mehr erforderlich und damit rechtswidrig.

Aus den im verwaltungsgerichtlichen Verfahren gewonnenen Erkenntnissen wird daher angeregt, dass der Gesetzgeber in § 32 für die Fälle der Videoüberwachung von Orten mit hoher Kriminalitätsbelastung eine Regelung aufnimmt, die der anordnenden Behörde die Dokumentation der Maßnahme vorschreibt.⁴⁰ Auch eine zeitliche Befristung der Videoüberwachung⁴¹ ist in diesen Fällen sinnvoll. Rechtzeitig vor Ablauf der Maßnahme hätte dann die anordnende Behörde zu prüfen und gerichts fest nachzuweisen, dass die Voraussetzungen nach § 32 Abs. 3 Satz 1 Nr. 1 immer noch vorliegen.

Die Gesetzesänderungen in § 32 Absatz 3 werden dazu führen, dass die Videoüberwachung öffentlicher Räume vor dem Hintergrund der angespannten Sicherheitslage erheblich ausgeweitet wird. Dabei ist zu berücksichtigen, dass die Maßnahme einer Videoüberwachung tief in das Grundrecht auf informationelle Selbstbestimmung der betroffenen Bürgerinnen und Bürger eingreift. Betroffen ist eine Vielzahl von Personen, die sich rechtstreu verhalten, in deren Grundrechte der Staat aber dennoch eingreift. Die Streubreite einer Datenerhebung mittels Bildübertragung oder Bildaufzeichnung ist damit erheblich. Umso dringender stellt sich die Frage der Rechtfertigung des Grundrechtseingriffs. Objektiver Maßstab kann hier die Anzahl der an dem Ort begangenen Straftaten sowie deren Qualität sein. Auch das subjektive Sicherheitsempfinden der Bevölkerung wird immer

³⁸ Vgl. z. B. PAG BY, Art. 31 Abs. 4 (drei Wochen) ; § 31 Abs. 5 PolG BW (vier Wochen) ; § 24 Abs. Abs. 2 ASOG BE ; § 31 Abs. 1 BbgPolG; § 29 Abs. 4 BremPolG; § 14 Abs. 2 S. 2 Hess.SOG (unverzüglich); § 15a Abs 2 PolG NW (14 Tage).

³⁹ Pressemitteilung des VG Hannover vom 09.06.2016; VG Hannover ZD 2016, 502.

⁴⁰ vgl. z. B. § 15a Abs. 4 S. 1 PolG NW.

⁴¹ § 15a Abs. 4 S. 2-4 PolG NW.

wieder als Argument angeführt. Wissenschaftliche Untersuchungen zur Effektivität der Videoüberwachung sind zum Teil widersprüchlich. Die Ergebnisse sind offenbar abhängig vom jeweiligen Vorverständnis des Auftraggebers.⁴² Eine kürzlich veröffentlichte Evaluationsstudie zur polizeilichen Videoüberwachung in Nordrhein-Westfalen kommt ebenfalls zu keinem eindeutigen Ergebnis, ob und in welchem Umfang eine Videoüberwachung einen wirksamen Beitrag zur öffentlichen Sicherheit leistet.⁴³

Der Gesetzgeber hat diese diffuse Erkenntnislage bei der Gesetzgebung zu berücksichtigen. Da es um den Schutz von Grundrechten geht, muss er sich Klarheit darüber verschaffen, ob der mit der Videoüberwachung angestrebte Zweck auch tatsächlich erreicht wird. Es wird daher angeregt, eine Evaluierungsklausel für § 32 Abs. 3 vorzusehen⁴⁴ und damit Art. 5 des Gesetzentwurfs entsprechend zu erweitern.

15. Zu Nr. 20 d), § 32 Abs. 4 Satz 2

Mit § 32 Abs. 4 Satz 2 soll eine neue Regelung zur Anfertigung von Bild- und Tonaufzeichnungen durch die Polizei geschaffen werden. Die Kameras (sog. „Bodycams“) befinden sich hierbei am Körper des Polizeibeamten. Der Einsatz von Bodycams greift in erheblichem Umfang in das Grundrecht auf informationelle Selbstbestimmung ein.

Betroffen sind nicht nur Personen, die in unmittelbarem Kontakt mit dem kameraführenden Polizeibeamten stehen, sondern auch Dritte, die sich zufällig im Aufnahmebereich der Kamera befinden. Bei den mobil geführten Körperkameras kommt im Vergleich zu fest installierten Videoanlagen hinzu, dass der Aufnahmebereich der Kamera deutlich flexibler und eher zufällig ist. Für die Betroffenen ist nicht erkennbar, welchen Raum die Kamera tatsächlich erfasst. Daher ist es aus Sicht des Datenschutzes grundsätzlich zu begrüßen, dass mit § 32 Abs. 4 Satz 2 eine spezialgesetzliche Rechtsgrundlage für den Einsatz dieser neuen Technologie geschaffen wird.

Körperkameras dürfen von der Polizei nach dem vorgeschlagenen Wortlaut bei der Durchführung von Maßnahmen der Gefahrenabwehr in öffentlich zugänglichen Räumen eingesetzt werden. Erfasst werden daher ausnahmslos alle polizeilichen Maßnahmen, die nach dem Gefahrenabwehrrecht auf der Grundlage des zukünftigen NPOG bzw. anderer Rechtsvorschriften zulässig sind. So sind z. B. auch Bild- und Tonaufzeichnungen im Rahmen einer Befragung nach § 12 grundsätzlich möglich. Schutzziel der Norm ist es jedoch, gewalttätige Übergriffe insbesondere auf Polizeibeamte zu verhindern. Dann sollte aber auch der Tatbestand einengender gefasst und ausschließlich auf Maßnahmen bezogen werden, die typischerweise zu Konfliktsituationen führen können.⁴⁵

Eine Datenerhebung mittels Körperkamera darf nach dem Wortlaut der Norm nur stattfinden, wenn dies nach den Umständen zum Schutz von Polizeibeamten oder Polizeibeamtinnen oder Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist. Nach der Legaldefinition des § 2 Nr. 1 ist eine Gefahr eine konkrete Gefahr, das heißt eine Sachlage, bei der im einzelnen Fall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für die öffentliche Sicherheit oder Ordnung eintreten wird. Damit ist die Eingriffsschwelle gesetzlich klar definiert, es muss eine konkrete Gefahrensituation vorliegen. Die Ausführungen zur Vorverlagerung des Einschaltzeitpunkts in der Gesetzesbegründung, wonach eine Situation ausreichend sein soll, „die aufgrund von polizeilichem Erfahrungswissen die Gefahr einer gewalttätigen Eskalation in sich birgt“, finden keinen Anknüpfungspunkt im Gesetzeswortlaut.

⁴² Petri, Liskens/Denninger, G Rn. 202.

⁴³ Forschungsbericht Nr. 143 des KFN, Ergebnisse der Evaluation der polizeilichen Videobeobachtung in Nordrhein-Westfalen gemäß § 15 a PolG NRW.

⁴⁴ Vgl. § 15a Abs. 5 PolG NW; § 70 ASOG BE.

⁴⁵ So z. B. § 29 Abs. 5 PolG HB bezogen auf Anhalte- und Kontrollmaßnahmen im öffentlichen Verkehrsraum.

Neben Bild- sollen auch Tonaufzeichnungen nach § 32 Abs. 4 Satz 2 angefertigt werden dürfen, wenn dies nach Umständen zum Schutz von Polizeibeamtinnen oder Polizeibeamten oder von Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist. Wie bei der Videoüberwachung wird auch bei Körperkameras angenommen, dass der Einsatz dieser Technik die Betroffenen davon abhält, Straftaten zu begehen (präventive Wirkung). Tonaufnahmen stellen einen zusätzlichen Grundrechtseingriff in das Recht am gesprochenen Wort dar. Ob neben der Bild- auch die Möglichkeit der Tonaufzeichnung einen abschreckenden Effekt gegenüber dem potentiellen Angreifer hat, ist mehr als fraglich.⁴⁶ Lediglich bei Beleidigungsdelikten könnte das Mittel der Tonaufzeichnung präventiv wirken. Diese sind jedoch gerade nicht vom Schutzzweck der Norm umfasst, denn Anlasstaten sind ausschließlich Körperverletzungs- oder Tötungsdelikte. Ton- neben Bildaufzeichnungen sind damit nicht geeignet und erforderlich, um den mit der Norm verfolgten Zweck zu erreichen. Auch für den weiteren Zweck der Strafverfolgung sind Bildaufnahmen als Beweismittel ausreichend, um die von der Norm erfassten Delikte zu sanktionieren.

Ferner soll der Polizeibeamte die Aufzeichnung bereits dann vornehmen dürfen, wenn eine Situation vorliegt, die nach polizeilicher Erfahrung die Gefahr einer gewalttätigen Eskalation in sich birgt, so jedenfalls die Ausführungen zum Einsatzzeitpunkt in der Gesetzesbegründung. Damit wird dem Polizeibeamten ein großer Handlungsspielraum für den Einsatz der Körperkameras eröffnet, der weit in das Vorfeld einer konkreten Gefahrenlage für Leib oder Leben hinreicht. Stellt sich dann im weiteren Verlauf heraus, dass „nur“ der Vorwurf einer Beleidigung im Raum steht, es aber nicht zu einer Gewalteskalation gekommen ist, wäre bei einer reinen Bildaufzeichnung eine Strafverfolgung nicht möglich, bei einer zusätzlichen Tonaufzeichnung schon.

Die Möglichkeit der Tonaufzeichnung beeinflusst daher bewusst oder unbewusst die Entscheidung des Beamten dahingehend, die Technik auch in Fällen zum Einsatz zu bringen, bei denen es gar nicht um Gewaltsituationen geht. Es besteht die Gefahr, dass vorsorglich zu Beweis Zwecken die Kamera und damit auch der Ton eingeschaltet werden, um auf jeden Fall die Beleidigung strafrechtlich ahnden zu können. Mit dem Schutzzweck der Norm, die Polizeibeamtinnen oder Polizeibeamten vor Gefahren für Leib oder Leben zu schützen, ist dies jedoch nicht zu vereinbaren. Auch aus diesem Gesichtspunkt sollte daher von Tonaufzeichnungen abgesehen werden.

Nach § 32 Abs. 4 Satz 3 ist die Verwendung von Bodycams kenntlich zu machen. Damit soll es sich beim Einsatz von Körperkameras um eine offen durchgeführte Maßnahme handeln, die präventiv wirkt und das Polizeivollzugspersonal so vor körperlichen Angriffen schützt. Daher ist es unverzichtbar, dass die Maßnahme bzw. die Aufzeichnung - wie es der Gesetzentwurf vorsieht - offen durchgeführt wird. Um den präventiven Effekt einer Körperkamera am wirkungsvollsten erzielen zu können, reicht jedoch eine bloße Erkennbarkeit der Maßnahme für den Betroffenen nicht aus (z. B. durch Anlegen einer Warnweste „Videodokumentation“). Es sollte vielmehr die Pflicht der Polizeibeamtin oder des Polizeibeamten normiert werden, vor dem Einschalten der Kamera die direkt betroffene Person über die Art und den Umfang des Einsatzes der Kamera mündlich zu informieren.⁴⁷ Dies trägt insgesamt zur Transparenz der Maßnahme bei. Auch ist zu beachten, dass zum Zeitpunkt der Datenerhebung der Polizeivollzugsbeamte die Pflicht hat, die betroffene Person nach § 50 NDSG über ihre Rechte zu informieren. Neben der Pflicht zur Kenntlichmachung sollte daher in Satz 3 auch auf § 50 NDSG verwiesen werden.

Die Aufzeichnungen mittels Bodycams sind doppelunktionaler Natur. Einerseits dienen diese präventiven Zwecken durch Abschreckung, andererseits werden mit den Aufzeichnungen auch Beweismittel für spätere Strafverfahren erhoben (repressiver Zweck). Bei streitigen Konfliktsituationen können die Aufzeichnungen beispielsweise auch entlastendes Beweismaterial für denjenigen enthalten, der sich dem Vorwurf einer Straftat zum Nachteil eines Polizeibeamten ausgesetzt sieht. Oder aber es tritt der Fall ein, dass sich die Polizeibeamten ihrer Meinung nach korrekt verhalten haben, gleichwohl werden von der betroffenen Person strafrechtliche Vorwürfe erhoben. Daher

⁴⁶ Kipker/Gärtner NJW 2015, 296 (297).

⁴⁷ Kipker/Gärtner NJW 2015, 296 (299).

muss eine Norm, die den Einsatz von Körperkameras zulässt, auch Regelungen enthalten, wie im Weiteren mit den Aufnahmen umzugehen ist.⁴⁸ Es darf nicht allein den handelnden Polizeibeamten überlassen bleiben, was mit den Aufzeichnungen geschieht und wann diese gelöscht werden.

Ferner sollte eine spezielle Aufbewahrungs- bzw. Löschungsregelung für das aufgezeichnete Datenmaterial im Gesetz verankert werden, die diese Aspekte mit in den Blick nimmt. Ein Rückgriff auf die allgemeine Regelung des § 39 a ist nicht ausreichend, da diese Vorschrift keine Fristen festlegt. Auch führt die Anwendung dieser allgemeinen Löschungsregelung dazu, dass es letztlich die Polizei selbst - im Regelfall sogar der aufzeichnende Beamte - in der Hand hat, wann das Datenmaterial gelöscht wird. Zu denken ist an eine Regelung, die eine Sichtung und Auswertung des Datenmaterials durch Personen vorsieht, die in keiner Weise mit dem aufgezeichneten Geschehen zu tun haben (neutrale Stelle⁴⁹). Ausdrückliche Regelungen zur Löschung der Aufzeichnungen finden sich in den Gesetzen von Hessen⁵⁰ und Hamburg.⁵¹ In Bremen⁵² gibt es darüber hinaus eine gesetzlich geregelte Aufbewahrungsfrist von zwei Monaten.

Belastbare wissenschaftliche Untersuchungen zum Einsatz von Körperkameras und zur Frage, ob diese tatsächlich eine präventive Wirkung entfalten und damit das Polizeivollzugspersonal wirksam vor körperlichen Übergriffen schützen können, liegen derzeit nicht vor. Die Ergebnisse des Pilotversuchs in Hessen deuten allenfalls auf einen deeskalierenden Trend hin.⁵³ Ferner bestehen erhebliche Zweifel an der wissenschaftlichen Methodik und Objektivität des hessischen Pilotversuchs.⁵⁴ Auch besteht durchaus die Möglichkeit, dass der Einsatz von Körperkameras gerade nicht deeskalierend wirkt, sondern die Konfliktsituation hierdurch noch angeheizt wird, weil sich der betroffene Bürger aus seiner Sicht permanent dem unbegründeten Vorwurf von Gewaltbereitschaft und Kriminalität ausgesetzt sieht.⁵⁵

Fundierte Erkenntnisse zur Wirksamkeit der Maßnahme sind in jedem Fall unerlässlich, denn nur dann lässt sich der mit dem Einsatz von Körperkameras verbundene Eingriff in das Grundrecht auf informationelle Selbstbestimmung rechtfertigen. Daher wird angeregt, die Norm des § 32 Abs. 4 Satz 2 zeitlich zu befristen und die Maßnahme mit in die Evaluierungsklausel nach Artikel 5 des Gesetzentwurfs aufzunehmen.

16. Zu Nr. 20 e), § 32 Abs. 5

Mit der neuen Regelung des § 32 Abs. 5 soll eine Rechtsgrundlage für die sog. Pre-Recording-Funktion beim Einsatz von Bodycams geschaffen werden. Schaltet der Polizeibeamte die Kamera an, so wird nicht erst ab diesem Zeitpunkt das Bildmaterial gespeichert, sondern die Bildspeicherung umfasst einen weiteren Zeitraum von 30 Sekunden, der unmittelbar vor dem Einschaltzeitpunkt liegt.

Problematisch ist hierbei, dass die Betroffenen nach § 32 Abs. 4 Satz 3 über diese Maßnahme erst in Kenntnis gesetzt werden, wenn die Kamera eingeschaltet ist. Die diesem Zeitpunkt vorgelagerte Datenerhebung und -speicherung auf der Grundlage des § 32 Abs. 5 erfolgt ohne Kenntnis der betroffenen Person und somit verdeckt. Ferner werden durch die Pre-Recording-Funktion fortlaufend Daten von Personen erhoben und gespeichert, die polizeilich überhaupt nicht in Erscheinung treten.

⁴⁸ BeckOK PolR NRW, Worms/Gusy, § 8 Rn. 66.

⁴⁹ Kipker/Gärtner NJW 2015, 296 (299); BeckOK PolR NRW, Worms/Gusy, § 8 Rn. 66.

⁵⁰ § 14 Abs. 6 S. 3 Hess. SOG.

⁵¹ § 8 Abs. 5 S. 3 PolEDVG HH.

⁵² § 29 Abs. 5 S. 4 BremPolG.

⁵³ Stoklas, ZD-Aktuell 2014, 04388.

⁵⁴ Zander, Body-Cams im Polizeieinsatz, S. 52 f.

⁵⁵ Kipker/Gärtner NJW 2015, 296 (297).

Werden Daten bei der betroffenen Person ohne deren Kenntnis erhoben, treffen den Gesetzgeber im Vergleich zu offen durchgeführten Maßnahmen größere Anforderungen hinsichtlich der Formulierung der Bestimmtheit der Eingriffsnorm. Es bleibt aber nach dem Gesetzeswortlaut völlig offen, wann und unter welchen Voraussetzungen die Polizei von der Pre-Recording-Funktion Gebrauch machen darf.

Die Tatsache, dass die Aufnahmezeit nur 30 Sekunden beträgt und die Bildsequenzen fortlaufend überschrieben und damit gelöscht werden, lässt die Qualität der Maßnahme nach § 32 Abs. 5 als Grundrechtseingriff nicht entfallen. Davon geht zutreffend auch die Gesetzesbegründung aus. Nicht geteilt wird allerdings die Einschätzung, dass es sich nur um „flüchtige“ und „oberflächige“ Grundrechtseingriffe handelt. Die 30-Sekunden-Sequenzen können Daten von zahlreichen Personen erfassen, die keine Veranlassung für eine polizeiliche Maßnahme gegeben haben. Die Streubreite der Eingriffsnorm des § 32 Abs. 5 ist daher vergleichsweise groß. Hinzu kommt, dass die Datenerhebung und –speicherung für die betroffenen Personen nicht erkennbar ist im Gegensatz zu einem offenen Einsatz der Bodycam nach § 32 Abs. 4 Satz 2.

Im Ergebnis ist daher die Regelung des § 32 Abs. 5 wegen Verstoßes gegen den Bestimmtheitsgrundsatz verfassungswidrig.

17. Zu Nr. 20 g), § 32 Abs. 7

Mit § 32 Abs. 7 soll eine Vorschrift für die Bildübertragung zum Zweck der Lenkung und Leitung des Straßenverkehrs ins Gesetz aufgenommen werden. Damit wird eine Forderung der LfD aufgegriffen, denn die Videoüberwachung des Straßenverkehrs zum Zweck der Gefahrenabwehr bedarf einer bereichsspezifischen Rechtsgrundlage. Auch wenn nur Übersichtsaufnahmen angefertigt werden, können nach dem Stand der heutigen Technik durch nachträgliche Auswertung personenbezogene Daten generiert werden (Fahrzeugkennzeichen oder einzelne Personen), so zutreffend die Gesetzesbegründung unter Berufung auf die Rechtsprechung des Bundesverfassungsgerichts.

Die Regelung des § 32 Abs. 7 lässt nur die Videoüberwachung des Straßenverkehrs in Form der Bildübertragung vor. Bildaufzeichnungen sind damit ausgeschlossen. Diese Einschränkung wird aus Sicht des Datenschutzes ausdrücklich begrüßt. Gleichwohl wird die Erhebung personenbezogener Daten nur ausnahmsweise zur Zweckerreichung erforderlich sein. Übersichtsaufnahmen dürften in der Regel ausreichen, um den Verkehrsfluss zu steuern. Dieser Vorrang der Übersichtsaufnahme sollte im Gesetzestext verankert werden. Die Verarbeitung personenbezogener Daten sollte nur zulässig sein, um aufgetretene Gefahrenlagen beseitigen zu können, z. B. um bei einem Auffahrunfall erkennen zu können, ob Personen verletzt sind und durch den Rettungsdienst versorgt werden müssen. Nur in diesen Fällen ist es erforderlich, von der Übersichtsaufnahme in die Zoomfunktion zu wechseln.

18. Zu Nr. 20 g), § 32 Abs. 8

Die Neuregelung setzt die Forderung der LfD um, für die sog. Abschnittskontrolle zur Überwachung der Geschwindigkeiten von Kraftfahrzeugen eine ausdrückliche Rechtsgrundlage zu schaffen. Eine eigenständige Befugnisnorm ist jedenfalls für den Fall der Geschwindigkeitsübertretung zwingend erforderlich. Nur für den Fall, dass die Fahrzeugdaten unmittelbar nach der Erfassung (Einfahrt in den Streckenabschnitt, 1. Kamera) technisch spurlos, anonym und ohne einen Personenbezug herzustellen wieder gelöscht werden (Ausfahrt aus dem Streckenabschnitt, 2. Kamera), hat das Bundesverfassungsgericht in seiner Entscheidung zum Kennzeichenlesegerät ausnahmsweise keinen Eingriff in das Grundrecht auf informationelle Selbstbestimmung angenommen (sog. Nichttref-ferfall).⁵⁶ Für den Fall der Geschwindigkeitsübertretung bilden die bei der Ein- und Ausfahrt erhobenen Fahrzeugdaten jedoch die Grundlage für die sich anschließende Maßnahme zur Feststellung

⁵⁶ BVerfG NJW 2008, 1505 (1507).

des Fahrers. Hierzu wird mittels einer dritten Kamera ein Frontbild des Fahrzeugs gefertigt, auf dem auch der Fahrer zu erkennen ist. Rechtsgrundlage hierfür ist § 100h Abs. 1 Satz 1 Nr. 1 StPO i. V. m. § 46 OWiG. Für derartige Fallkonstellationen liegt zweifellos schon bei der Datenerhebung mittels der 1. Kamera ein Grundrechtseingriff vor. Die Erhebung und Verwendung der Daten bedarf dann einer gesetzlichen Regelung, die jedenfalls den allgemeinen Anforderungen an die Bestimmtheit und Verhältnismäßigkeit von Befugnisnormen entsprechen muss (sog. Trefferfall).⁵⁷

§ 32 Abs. 8 setzt diese Vorgaben des Bundesverfassungsgerichts um. Es wird eine Regelung für die Speicherung, Veränderung und Nutzung der erhobenen Fahrzeugdaten zum Zwecke der Feststellung der Durchschnittsgeschwindigkeit geschaffen. Damit wird auch der „Nichttrefferfall“ im Gesetz ausdrücklich datenschutzrechtlich geregelt. Dies ist auch erforderlich, denn anders als beim Kennzeichenlesegerät werden die Daten bei der Abschnittsgeschwindigkeitskontrolle doch für einen gewissen Zeitraum - nämlich für die Zeit der Durchfahrt durch die Überwachungsanlage - gespeichert.

19. Zu Nr. 21, § 32 a

Nach § 32 a sind nicht öffentliche Stellen zukünftig verpflichtet, der Polizei auf Anforderung Einsichtnahme in Bild- oder Tonaufzeichnungen über öffentlich zugängliche Räume zu gewähren bzw. entsprechende Aufzeichnungen auszuhändigen.

Die Regelung ist dazu bestimmt, Gefahren für die Sicherheit oder den Bestand des Bundes oder eines Landes sowie für Leib, Leben oder Freiheit einer Person abwehren zu können.

Die Notwendigkeit für eine derartige Regelung, die den Polizeibehörden zum Zweck der Gefahrenabwehr praktisch den Zugriff auf alle Bild- und Tonaufzeichnungen ermöglicht, die von nicht-öffentlichen Stellen angefertigt wurden (Anwendungsbereich des Art. 6 Abs. 1 f) DS-GVO bzw. § 4 Abs. 1 Nr. 2 und 3 BDSG), ist nicht erkennbar. Die Ausführungen in der Gesetzgebungsbegründung geben keinen Aufschluss über die Gesetzgebungsmotive.

Die Eingriffsintensität dieser Maßnahme ist erheblich. Durch die Aushändigung der Aufzeichnungen und die sich anschließende Auswertung verarbeitet die Polizei massenweise Daten von Personen, die keinen Anlass für eine polizeiliche Maßnahme gegeben haben. Nach § 32 Abs. 2 kann auch eine Anordnung zur Durchsetzung der Aushändigung der Aufzeichnungen getroffen werden. Die Polizei soll die Maßnahme daher im Ergebnis auch mit Verwaltungszwang durchsetzen können. Die mit der Bild- oder Tonaufzeichnung verbundenen Eingriffe in die Grundrechte der Betroffenen werden damit durch eine Maßnahme nach § 32 a weiter vertieft, indem nicht nur die ursprünglich verantwortliche Stelle sondern auch die Polizei - also staatliche Organe - Zugriff auf die Daten erhalten. Vom Regelungsgehalt und der Zielsetzung ist § 32 a vergleichbar mit einer Beschlagnahme im Rahmen eines Strafverfahrens. Diese steht jedoch grundsätzlich unter dem Vorbehalt der Anordnung durch das Gericht, § 98 Abs. 1 Satz 1 StPO. Es sprechen also gewichtige Gründe dafür, eine Anordnung nach § 32 a Abs. 2 nicht nur unter den Vorbehalt der Behördenleitung zu stellen, sondern unter einen Richtervorbehalt.

20. Zu Nr. 23 a), § 33 a Abs. 1

Durch die Neufassung des § 33 a Abs. 1 werden die Voraussetzungen für eine Telekommunikationsüberwachung im Vergleich zur bisherigen Rechtslage wesentlich erweitert. Zum einen wird die Maßnahme auch zum Zweck der Strafverhütung zugelassen. Bisher ist eine Überwachung der Telekommunikation nur zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person zulässig. Zum anderen wird in Fällen der Verhütung terroristischer Straftaten die Gefahrenschwelle in das Vorfeld einer konkreten Gefahr verlagert und damit erheblich abgesenkt (drohende

⁵⁷ BVerfG NJW 2008, 1505 (1507).

Gefahr in den Fällen des Absatzes 1 Satz 1 Nr. 2 und 3). Darüber hinaus kann sich die Maßnahme nun auch gegen sogenannten Nichtstörer – Nachrichtenmittler – richten (Satz 1 Nr. 4 und 5).

Die Neuregelung orientiere sich weitgehend an der entsprechenden Vorschrift des § 20 I Abs. 1 BKAG a. F., so die Gesetzesbegründung. Diese habe das Bundesverfassungsgericht für verfassungskonform erklärt. Hierbei wird jedoch außer Acht gelassen, dass die alte Regelung des § 20 I Abs. 1 mitnichten eine so weitreichende Telekommunikationsüberwachung zuließ wie die vorliegende Regelung des § 33 a Abs. 1, der sich am neuen § 51 Abs. 1 BKAG orientiert. Der Bundesgesetzgeber hat nach der Entscheidung des Bundesverfassungsgerichts im Vergleich zur streitbefangenen Norm des § 20 I BKAG a. F. „draufgesattelt“, die Eingriffsschwelle der drohenden Gefahr eingeführt und damit den Anwendungsbereich der Telekommunikationsüberwachung wesentlich erweitert. Diese Erweiterung war gerade nicht Gegenstand der Entscheidung des Bundesverfassungsgerichts.

Aus den unter Ziffer 6 genannten Gründen ist die Ausweitung der Telekommunikationsüberwachung nach § 33 a Abs. 1 durch die Einführung der drohenden Gefahr aus Sicht des Datenschutzes wegen Verstoßes gegen den Bestimmtheitsgrundsatz und den Grundsatz der Verhältnismäßigkeit abzulehnen. Festzuhalten bleibt auch, dass die Gesetzesbegründung mit keinem Wort darauf eingeht, warum die Möglichkeiten der Telekommunikationsüberwachung zur Gefahrenabwehr und Straftatenverhütung aus Sicht der Praxis zwingend erweitert werden müssen.

Anlässlich der Anhörung zum Gesetzentwurf der Landesregierung aus der letzten Legislaturperiode (LT-Drs. 17/6232) haben die Vertreter der Polizeigewerkschaften keine Regelungslücke gesehen und damit keinen Erweiterungsbedarf bei den polizeilichen Überwachungsmaßnahmen angemahnt - im Gegenteil: Die Gewerkschaftsvertreter haben die seinerzeit vorgeschlagenen Einschränkungen bei polizeilichen Datenerhebungsmaßnahmen (z. B. bei der Wohnraumüberwachung, Abschaffung des Kennzeichenlesegeräts) als für die Praxis der Polizeiarbeit irrelevant bewertet. Die Vertreter der Polizei haben weder die Ausweitung bestehender Befugnisse noch die Einführung völlig neuer Überwachungsmaßnahmen für erforderlich gehalten.

21. Zu Nr. 23 b, § 33 a Abs. 2 und 3

Durch die neuen Absätze 2 und 3 soll in Niedersachsen zukünftig die Telekommunikationsüberwachung auch in der Form der sog. Quellen-TKÜ zulässig sein. Diese Maßnahme wird für erforderlich gehalten, um auch verschlüsselt stattfindende Kommunikation abhören zu können. Dafür müssen die Polizeibehörden auf das Endgerät der Zielperson eine Software aufspielen, die die Kommunikation vor der Verschlüsselung mitschneidet und an die Polizei ausleitet. Es ist unstrittig, dass diese Form der Telekommunikationsüberwachung einen schwerwiegenden Eingriff in die Grundrechte der Betroffenen darstellt (Art. 10 Abs. 1 GG) und damit die verfassungsrechtlichen Grundsätze der Bestimmtheit und Verhältnismäßigkeit besonders sorgfältig bei der gesetzgeberischen Ausgestaltung zu beachten sind.

Vorweg ist festzustellen, dass schon die Durchführung der laufenden Telekommunikationsüberwachung in Niedersachsen aus Sicht des Datenschutzes rechtswidrig ist. Die datenschutzrechtlichen Mängel der durch das LKA Niedersachsen betriebenen Überwachungsanlage sind bis zum heutigen Tag nicht behoben. Zur Problematik wird auf die Antworten der Landesregierung auf mündliche Anfragen der Fraktion der FDP aus dem Jahr 2015 und 2016 verwiesen.⁵⁸ Der dort geschilderte Sachstand entspricht unverändert der aktuellen Situation. Die Technik des LKA ist demnach veraltet und entspricht nicht den Anforderungen des Datenschutzes und der Datensicherheit.

⁵⁸ LT-Drs. 17/4865, Nr. 56; 17/5030, Nr. 30 und 31; 17/5210, Nr. 54 und 55.

Es stellt sich daher die Frage, wie die neuen Überwachungsinstrumente der Quellen-TKÜ nach § 33 a Abs. 2 - aber auch der Online-Durchsuchung nach § 33 d - praxistauglich und den gesetzlichen Anforderungen entsprechend in Niedersachsen in absehbarer Zeit umgesetzt werden können. Es ist zu erwarten, dass zwar für beide Maßnahmen im Polizei- und Ordnungsbehördengesetz eine Rechtsgrundlage geschaffen wird, die neuen Überwachungstechniken in der Praxis jedoch nicht eingesetzt werden können. Im Ergebnis schafft der Gesetzgeber mit den Eingriffsbefugnissen gemäß § 33 a Abs. 2 und § 33 d leerlaufende Platzhalter, und das vor dem Hintergrund der Gesetzesbegründung, die an zahlreichen Stellen die Ausweitung polizeilicher Befugnisse angesichts der aktuellen Bedrohungslage durch den internationalen Terrorismus als unumgänglich beschreibt.

§ 33 a Abs. 2 Nr. 1 bestimmt, dass die Maßnahme der Quellen-TKÜ nur zulässig sein soll, wenn durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Kommunikation überwacht und aufgezeichnet wird. Dies entspricht auf den ersten Blick den Anforderungen, die das Bundesverfassungsgericht an eine TKÜ-Maßnahme in Abgrenzung zur Online-Durchsuchung stellt. Danach dürfen Maßnahmen der TKÜ allein die Inhalte und die Umstände der laufenden Kommunikation erfassen. Sie sind damit ausschließlich an Art. 10 Abs. 1 GG zu messen.⁵⁹ Die Online-Durchsuchung greift hingegen in das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ein und ist daher im Vergleich zur TKÜ als die grundrechtintensivere Maßnahme einzustufen. In beiden Fällen ist es jedoch erforderlich, das Zielsystem mit einem Staatstrojaner zu infiltrieren. Dies bedeutet, dass zunächst immer in die Integrität und Vertraulichkeit des Zielgerätes eingegriffen werden muss. Bei der TKÜ-Maßnahme muss dieser Eingriff jedoch durch rechtliche und technische Vorgaben so eingeschränkt werden, dass nur Daten über die laufende Kommunikation erfasst und ausgeleitet werden. Daraus folgt jedoch, dass jede TKÜ-Maßnahme in Form der Quellen-TKÜ immer auch die Funktion besitzt, eine Online-Durchsuchung durchzuführen.

Ist unter diesen Voraussetzungen eine trennscharfe Abgrenzung bei der praktischen Anwendung zwischen Quellen-TKÜ und Online-Durchsuchung überhaupt möglich? Dies wird von Fachleuten grundsätzlich bezweifelt. Eine Quellen-TKÜ greife immer auch in das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ein, denn die technischen Anforderungen zur Beschränkung der Maßnahme auf Vorgänge der laufenden Kommunikation seien praktisch nicht zu erfüllen.⁶⁰

Hinzu kommt das Problem der Überprüfbarkeit der Software bei Anordnung der Maßnahme durch das Gericht. Der Richter müsste schlüssig nachvollziehen können, ob die für eine Quellen-TKÜ eingesetzte Software tatsächlich in ihrer Funktion technisch so reduziert ist, dass nur die laufende Kommunikation erfasst und ausgeleitet wird. Selbst bei technischen Fachkenntnissen wird die Prüfung dem Richter kaum möglich sein, da die Sicherheitsbehörden in der Regel Software von Privat Anbietern einsetzen und diese keine Auskunft über die genaue Funktionsweise der Technik erteilen. Es ist daher vom Gesetzgeber zu fordern, dass bei einer Maßnahme nach § 33 a Abs. 2 eine unabhängige, sachverständige Stelle die eingesetzte Software zertifiziert und freigibt, so dass der Richter auf einer gesicherten Tatsachengrundlage eine Anordnung treffen kann.

22. Zu Nr. 23 d), § 33 a Abs. 5

Die Ergänzung des Absatzes 5 um Nutzungsdaten ist gerade mit Blick auf Suizidfälle oder Amokläufe, die in Internetforen oder sozialen Netzwerken angekündigt werden und daher unter das Telemediengesetz (TMG) fallen, nachvollziehbar, um eine Gesetzeslücke zu schließen.

⁵⁹ BVerfGE 120, Rn. 184.

⁶⁰ Kruse/Grzesiek, KritV 2017, 331 (335); Blechschmidt, StraFo 2017, 361 ff.

23. Zu Nr. 23 f), § 33 a Abs. 6 und 7

Mit § 33 a Abs. 6 werden sämtlichen Maßnahmen des § 33 a unter Richtervorbehalt gestellt. Dies ist bei der Telekommunikationsüberwachung nachvollziehbar, denn hierdurch erfolgt ein tiefer Eingriff in die Grundrechte der betroffenen Person. Dieser Eingriff ist jedoch nicht annähernd vergleichbar mit einem Auskunftsverlangen der Polizei über Nutzungsdaten. Kommunikationsinhalte werden bei dieser Maßnahme nicht erfasst. Es sollte daher kritisch hinterfragt werden, ob der Richtervorbehalt im Fall des § 33 a Abs. 5 tatsächlich erforderlich ist.

Die in Absatz 7 Satz 6 formulierte Delegationsmöglichkeit bei der Anordnung einer TKÜ-Maßnahme bei Gefahr im Verzug auf Dienststellenleiter sowie Beamte der Laufbahngruppe 2 ab dem zweiten Einstiegsamt wird aus den unter Ziffer 9 genannten Gründen als zu weitgehend abgelehnt.

24. Zu Nr. 25, § 33 c

Die Erweiterung des Auskunftsverlangens um die Bestandsdaten nach § 14 TMG mit der Ergänzung des § 33 c Abs. 1 ist mit Blick auf eine wirksame Gefahrenabwehr bei Suizid- oder Amokfällen datenschutzrechtlich nicht zu beanstanden. Mit der Änderung des Satzes 3 wird das Recht des Betroffenen auf Unterrichtung zwar erweitert. Der völlige Ausschluss der Unterrichtung bei Bestandsdatenabfragen ist jedoch aus Sicht des Datenschutzes nicht nachvollziehbar. Es werden von der Polizei Daten ohne Kenntnis des Betroffenen erhoben, so dass grundsätzlich eine Information erforderlich ist.

25. Zu Nr. 26, § 33 d

Mit der Einfügung des § 33 c soll eine Befugnisnorm für die sogenannte Online-Durchsuchung als polizeiliche Standardmaßnahme geschaffen werden. Mit diesem Instrument ist die Polizei in der Lage, die gesamte Kommunikation der Zielperson zu erfassen und darüber hinaus auch sämtliche auf dem infiltrierten Endgerät gespeicherte Daten. Ferner kann eine Online-Durchsuchung dazu genutzt werden, um einen großen Lauschangriff durchzuführen, indem die Umgebung heimlich mit den Funktionen des Endgeräts (Kamera-/Mikrofonfunktion des PC oder Smartphones) überwacht wird.

Eine Maßnahme nach § 33 c ist damit wesentlich breiter angelegt als eine Wohnraum- oder Telekommunikationsüberwachung. Sie dringt tief und umfassend in die Privatsphäre der betroffenen Person ein und ist damit – zumal heimlich durchgeführt – ein schwerwiegender Grundrechtseingriff, an den besonders hohe verfassungsrechtliche Anforderungen zu stellen sind.

Nach Absatz 1 Satz 2 Nr. 1 und Nr. 2 ist eine Online-Durchsuchung auch zulässig zur Straftatenverhütung im Vorfeld einer konkreten Gefahrenlage. Bezug genommen wird nicht auf einen definierten Straftatenkatalog wie bei vergleichbar eingriffsintensiven Maßnahmen (Wohnraum- und Telekommunikationsüberwachung), sondern es ist ausreichend, dass eine Schädigung der in Absatz 1 Satz 1 genannten Rechtsgüter eintritt. Welche Straftatbestände darunter zu verstehen sind, lässt sich bei Absatz 1 Satz 1 Nr. 1 noch erschließen, denn hier sind die Schutzgüter Leib, Leben oder Freiheit einer Person aufgeführt. Anders verhält es sich jedoch bei der Bezugnahme auf Absatz 1 Satz 1 Nr. 2. Hier ist für den Rechtsanwender nicht ohne weiteres erkennbar, welche Straftatbestände betroffen sind, wenn es um „Güter der Allgemeinheit, deren Bedrohung, die Grundlage oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt“, geht. Es bestehen daher verfassungsrechtliche Bedenken, da § 33 Abs. 1 Satz 2 zu unbestimmt formuliert ist.

Ferner gestattet § 33 c Abs. 1 Satz 2 die Online-Durchsuchung zur Straftatenverhütung im Vorfeld einer konkreten Gefahrenlage (drohende Gefahr). Dies ist aus den unter Ziffer 6 genannten Gründen verfassungsrechtlich nicht hinnehmbar.

§ 33 d Abs. 1 Satz 4 verweist auf § 33 a Abs. 6 (wohl richtigerweise § 33 a Abs. 4), der die technischen Schutzmaßnahmen der Quellen-TKÜ für entsprechend anwendbar erklärt. Hier gilt das unter Ziffer 21 Gesagte. Es ist fraglich, ob das LKA technisch überhaupt in der Lage ist, eine Online-Durchsuchung in der Praxis ohne neuen Dienstleister durchzuführen. Die Vorschrift des § 33 d ist daher aus Sicht der LfD eine leere Hülle ohne praktischen Nutzen. Zudem stellt sich ebenfalls das Problem der Nichtüberprüfbarkeit der zum Einsatz kommenden Infiltrationssoftware durch den anordnenden Richter, insbesondere wenn Trojaner zum Einsatz kommen, die von Privatunternehmen zur Verfügung gestellt werden (s. auch Ziffer 21).

Ferner ist auf einen staatlichen Zielkonflikt hinzuweisen, den der Einsatz von Staatstrojanern mit sich bringt. Einerseits erlässt der Staat umfangreiche Vorschriften, die dem Schutz der IT-Systeme vor Cyberangriffen dienen. Andererseits benötigen die Polizeibehörden jedoch Sicherheitslücken, um gezielt und vom Nutzer unerkannt Spähsoftware einsetzen zu können. Welche Ausmaße Cyberangriffe über Sicherheitslücken erreichen können, hat im Mai 2017 der Ausbruch des Schadprogramms WannaCry für Windows Betriebssysteme verdeutlicht. Auf einen Schlag wurden über 230.000 Rechner in 150 Staaten infiziert und Lösegeldzahlungen erpresst. Der Auslandsgeheimdienst der USA nutzte zuvor diese Sicherheitslücke über fünf Jahre für staatliche Spähmaßnahmen, ohne Microsoft zu informieren. Eine Befugnisnorm wie § 33 d, die auf das Vorhandensein von Sicherheitslücken in Betriebssystemen angewiesen ist, schafft daher Fehlanreize, die die Sicherheit des Internets in höchstem Maße gefährden. Dritte können diese technischen Schutzlücken für kriminelle Zwecke ausnutzen. Schließlich wird das vom Bundesverfassungsgericht entwickelte Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme praktisch ad absurdum geführt, wenn der Staat bewusst Sicherheitslücken offenhält und damit diese Grundrechte aushöhlt, um eine Online-Durchsuchung durchführen zu können.

Aus Sicht des Datenschutzes und der Datensicherheit wird daher dringend davon abgeraten, die Vorschrift des § 33 d in das neue NPOG einzufügen.

Ergänzend ist anzumerken, dass die Regelung in Absatz 4 Satz 6 zu weitgehend ist (Delegationsmöglichkeit der Behördenleitung bei der Anordnung bei Gefahr im Verzug). Ferner ist es fraglich, ob eine Anordnungsbefugnis der Polizeibehörden bei Gefahr im Verzug bei einer Online-Durchsuchung in Betracht kommt. Sind überhaupt zeitkritische Fälle denkbar? Jedenfalls fehlt in § 49 BKAG, auf dessen Regelungen die Gesetzesbegründung Bezug nimmt, diese Möglichkeit der Anordnung.

Die Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung nach § 31 b sind für die Maßnahme der Online-Durchsuchung untauglich (vgl. die Anmerkungen unter Ziffer 11). Es wäre auf jeden Fall eine spezielle Regelung zum Kernbereichsschutz in § 33 d aufzunehmen, die anhand der Vorgaben des Bundesverfassungsgerichts⁶¹ das tatsächliche Vorgehen auf der Erhebungs- und Verwertungsebene abbildet.

26. Zu Nr. 27, § 34 Abs. 1 bis 3

Mit der teilweisen Neufassung des Absatzes 1 sollen die tatbestandlichen Anforderungen für eine verdeckt durchgeführte Personenbeobachtung konkreter gefasst werden, um den Vorgaben des Bundesverfassungsgerichts zum Bestimmtheitsgrundsatz bei heimlich durchgeführten Überwachungsmaßnahmen zu genügen. Grundsätzlich ist an diesem Regelungsziel nichts auszusetzen. Es wird jedoch mit den vorliegenden Vorschlägen verfehlt.

Indem in § 34 Abs. 1 Nr. 2 die tatbestandlichen Voraussetzungen für eine verdeckte Personenbeobachtung zur Straftatenverhütung wortgleich wie z. B. in § 16 a (Meldeaufgabe) formuliert sind

⁶¹ BVerfG NJW 2016, 1781, Rn. 219 f.

(„drohende Gefahr“), werden die auf Tatsachen beruhenden Anforderungen an die Prognoseentscheidung nicht erhöht, sondern im Gegenteil abgesenkt. Dies entspricht nicht den in der Gesetzgebung zitierten Ausführungen des Bundesverfassungsgerichts zu den Bestimmtheitsanforderungen an den Tatbestand einer Eingriffsnorm. Danach müssen die Anforderungen an eine Prognoseentscheidung hinreichend gehaltvoll ausgestaltet sein, um Behörden und Gerichten ausreichend bestimmte Kriterien an die Hand zu geben.⁶² An dieser Stelle zeigt sich deutlich, dass das Bundesverfassungsgericht dem Gesetzgeber nur Hinweise jedoch keine konkreten Formulierungsvorschläge an die Hand gibt.

Ferner wird im Vergleich zur bisherigen Rechtslage der Anwendungsbereich der verdeckten Observation erweitert, indem nicht mehr eine gegenwärtige Gefahr für die aufgeführten Rechtsgüter verlangt wird, sondern das Vorliegen einer konkreten Gefahr ausreichen soll. Eine Begründung für die Absenkung der Eingriffsschwelle wird jedoch nicht geliefert.

Nicht nachvollziehbar ist die Erweiterung um terroristische Straftaten in Absatz 1 Nr. 2 zur Straftatenverhütung neben den bisher genannten erheblichen Straftaten. Der Straftatenkatalog zur Definition der erheblichen Straftaten (§ 2 Nr. 14) umfasst nach hiesigem Verständnis auch den Katalog der terroristischen Straftaten nach § 2 Nr. 15.

Nicht zu beanstanden, weil die Anordnungsvorsetzungen erhöhend, ist die Regelung in Absatz 2, wonach Maßnahmen nach Absatz 1 nur noch vom Amtsgericht angeordnet werden können. Bisher konnte eine längerfristige Observation von der Behördenleitung angeordnet werden. Auf Grund des Richtervorbehalts ist es auch nachvollziehbar, dass die Dauer der Erstanordnung von einem Monat auf drei Monate erhöht wird.

Die Delegationsregelung nach Absatz 3 Satz 5 bei einer Anordnung durch die Behördenleitung bei Gefahr im Verzug ist zu weitreichend. Hier sind die Verfahrensregelung z. B. nach § 45 Abs. 3 Satz 2 BKAG restriktiver und damit vorzugswürdig.

§ 34 Abs. 1 gibt nur die Befugnis, Personenbeobachtungen über einen längeren Zeitraum verdeckt durchzuführen. Nicht spezialgesetzlich geregelt sind bisher Datenerhebungen durch längerfristige Observation, die offen - also mit Kenntnis der Zielperson - vorgenommen werden.

Mit Blick auf die zunehmend angespannte terroristische Gefahrenlage dürfte das Mittel der Datenerhebung durch eine längerfristige Observation von Gefährdern für die Polizei immer wichtiger werden. Ferner wurden nach hiesiger Kenntnis Sexualstraftäter, die ihre Strafe abgesessen haben und bei denen die Voraussetzungen für eine Sicherungsverwahrung nicht vorliegen, in der Vergangenheit von der Polizei über einen längerfristigen Zeitraum offen beobachtet.

Bisher konnten offen durchgeführte Observationen nur auf die Datenerhebungsgeneralklausel des § 31 Abs. 1 Satz 1 Nds. SOG gestützt werden. Dies gilt jedenfalls für eine kurzfristig durchgeführte Datenerhebung wie die spontane Beobachtung aber auch für die nur wenige Stunden oder Tage dauernde Observation von Gefährdern. Eine längerfristige und damit auch geplante offene durchgeführte Observation kann jedoch schwerlich auf eine Generalbefugnisnorm gestützt werden. Eine derartige Observation greift in erheblichem Umfang in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen ein. Sie ist auch für das persönliche Umfeld der Zielperson jederzeit erkennbar und entfaltet daher im Vergleich zur verdeckten Observation eine erhebliche stigmatisierende Wirkung.

Es wird daher aus Sicht des Datenschutzes empfohlen, die Änderungen in § 34 auch zu nutzen, um eine typischerweise in der Polizeipraxis zur Anwendung kommende Maßnahme der offenen Observation normenklar zu regeln. Ein Rückgriff auf die Generalklausel, der um der effizienten Gefahrenabwehr willen in atypischen Situationen auch intensive Grundrechtseingriffe rechtfertigen

⁶² BVerfG NJW 2016, 1781, Rn. 165.

kann, wird unzulässig, wenn die Situation von einer atypischen zu einer typischen geworden ist und sich für die Maßnahme Standards entwickelt haben.⁶³ Dies ist laut Gesetzesbegründung auch der Grund für die Regelung der Gefährderansprache und der Meldeauflage. Gleiches muss auch für das Mittel der offen durchgeführten Observation gelten, die mittlerweile in nahezu allen Polizeigesetzen spezialgesetzlich geregelt ist.

27. Zu Nr. 28, § 35

Zur verfassungsrechtlichen Absicherung soll bei Maßnahmen nach § 35 Abs. 1 (Datenerhebung durch den verdeckten Einsatz technischer Mittel außerhalb von Wohnungen) grundsätzlich ein Richtervorbehalt eingeführt werden. Dies stärkt die Rechte der Betroffenen und ist daher aus Sicht des Datenschutzes zu begrüßen.

28. Zu Nr. 29, § 35 a

Nach der Gesetzesbegründung sollen die Regelungen zur Wohnraumüberwachung unter Berücksichtigung der Entscheidung des Bundesverfassungsgerichts zum BKA-Gesetz grundlegend überarbeitet werden. Dabei wird jedoch der Anwendungsbereich im Vergleich zur bisherigen Rechtslage ohne nachvollziehbare Begründung teilweise erweitert. So ist die Wohnraumüberwachung bisher nur zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person zulässig, künftig ist „nur“ noch das Vorliegen einer dringenden Gefahr vonnöten. Nach der Definition des § 2 Nr. 4 umfasst die dringende Gefahr weitere Schutzgüter, nämlich neben Leib, Leben und Freiheit auch z. B. Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt. Auch sind die Wahrscheinlichkeitsanforderungen für einen Schadenseintritt beim Begriff der gegenwärtigen Gefahr höher als bei der dringenden Gefahr.

Ferner lässt § 35 a Abs. 1 Nr. 1 b die akustische Wohnraumüberwachung zur Verhütung terroristischer Straftaten zu. Bisher musste eine besonders schwerwiegende Straftat nach § 2 Nr. 10 Nds. SOG vorliegen. Der Katalog gemäß § 2 Nr. 15 zur Definition terroristischer Straftaten ist jedoch weiter gefasst als in § 2 Nr. 10 Nds. SOG. Auch dies bedeutet im Ergebnis eine Ausweitung der Maßnahme der Wohnraumüberwachung.

Die Erweiterungen hinsichtlich der Anwendungsmöglichkeit des § 35 a sind in Gänze abzulehnen. Im Gesetzentwurf der Vorgängerregierung (LT-Drs. 17/6232) wurde noch vorgeschlagen, die Wohnraumüberwachung zum Zweck der Straftatenverhütung ersatzlos zu streichen. Ausweislich der damaligen Gesetzesbegründung besteht kein praktisches Bedürfnis, derartig grundrechtsintensive Eingriffe in die Privatsphäre zum Zweck der Verhütung schwerwiegender Straftaten vorzunehmen. Die Vertreter der Polizeigewerkschaften haben diesem Streichungsvorschlag im Rahmen der Anhörung in Kenntnis der aktuellen Bedrohung durch den islamistischen Terrorismus nicht widersprochen. Daraus lässt sich nur schließen, dass der vorliegende Änderungswunsch weit über das Ziel hinausschießt.

Die in Absatz 4 Satz 5 geregelte Delegationsmöglichkeit bei der Anordnungsbefugnis von der Behördenleitung auf Dienststellenleiter oder Beamte der Laufbahngruppe 2 ab dem zweiten Einstiegsamt ist zu weitgehend. Wohnraumüberwachungen sollten wegen der besonderen Grundrechtsrelevanz bei Gefahr im Verzug nur von der Behördenleitung oder der Stellvertretung angeordnet werden dürfen.

⁶³ Pieroth/Schlink/Kniesel, Polizei- und Ordnungsrecht, 9. Aufl., § 7, Rn. 20.

29. Zu Nr. 30, § 36

Mit den vorgeschlagenen Änderungen sollen die Anforderungen für die Anordnung einer Datenerhebung durch Vertrauenspersonen erhöht und damit die Vorgaben des Bundesverfassungsgerichts umgesetzt werden (Absätze 2 bis 4). Ferner wird in Absatz 5 erstmals gesetzlich bestimmt, wann eine Person nicht als Vertrauensperson verwendet werden darf.

Durch die Neufassung der Absätze 2 und 3 ist vorgesehen, dass die Erstanordnung des Einsatzes von Vertrauenspersonen - sofern dieser sich gegen eine bestimmte Person richtet - zukünftig unter Richtervorbehalt steht. Nur bei Gefahr im Verzug kann die Polizei derartige Einsätze anordnen. Eine richterliche Bestätigung ist dann unverzüglich zu beantragen. In den übrigen Fällen des § 36 Abs. 1, wenn sich der Einsatz der Vertrauensperson also nicht gegen eine bestimmte Person richtet, verbleibt es bei der Möglichkeit der Anordnung durch die Polizei, Regelung des Absatzes 4. Bisher genügte für den Einsatz von Vertrauenspersonen generell eine Anordnung der Behördenleitung.

Nach der Gesetzesbegründung sollen diese Regelungen der Rechtsprechung des Bundesverfassungsgerichts zum BKA-Gesetz entsprechen. Das Gericht habe einen Richtervorbehalt nur gefordert, wenn die Datenerhebung durch die Vertrauensperson gezielt bestimmte Personen betrifft. Bewege sich die Vertrauensperson bei ihrem Einsatz zunächst allein im Milieu, um Vertrauen aufzubauen und finde demzufolge keine auf eine bestimmte Person bezogene Datenerhebung statt, dann könne auch die Anordnung wie bisher die Polizei treffen.

Dieser Lesart der Urteilsbegründung des Bundesverfassungsgerichts kann nicht gefolgt werden. Zunächst ist festzustellen, dass eine Überwachungsmaßnahme durch eine Vertrauensperson immer mit schweren Eingriffen in das Grundrecht auf informationelle Selbstbestimmung der betroffenen Personen verbunden ist. Auch in der Phase der Vertrauensbildung wird die Vertrauensperson erfahrungsgemäß personenbezogene Daten erheben und verarbeiten, um diese anschließend gegebenenfalls als Erkenntnisse über die Zielperson verwenden zu können. Eine Verarbeitung personenbezogener Daten wird daher in allen Einsatzszenarien einer Vertrauensperson stattfinden. Alles andere anzunehmen, wäre blauäugig und praxisfern.

Schließlich hat sich das Bundesverfassungsgericht anhand des § 20 g Abs. 3 BKAG a. F. eingehend mit der Frage auseinandergesetzt, wann ein Richtervorbehalt bei den Maßnahmen des § 20 g Abs. 2 a. F. wegen des großen Eingriffsgewichts in Betracht kommt. Es hat nur die Anfertigung von Bildaufnahmen im dort genannten Umfang sowie kurzfristige Observationen - auch mittels Bildaufzeichnungen oder technischer Mittel - vom Richtervorbehalt ausgenommen. In den übrigen Fällen des § 20 g Abs. 2 a. F. - also gerade auch für den Einsatz von Vertrauenspersonen (§ 20 g Abs. 2 Nr. 4 BKAG a. F.) - hat das Gericht hingegen die Anordnung durch ein Gericht unmissverständlich und ohne jede Ausnahme gefordert: „Demgegenüber ist eine unabhängige Kontrolle verfassungsrechtlich unverzichtbar, wenn Observationen im Sinne des § 20 g Abs. 2 Nr. 1 BKAG längerfristig - ... - durchgeführt werden, wenn nicht öffentliche Gespräche erfasst oder Vertrauenspersonen eingesetzt werden.“⁶⁴ Folglich ist die Regelung des § 36 Abs. 4 ersatzlos zu streichen. Die Erstanordnung des Einsatzes von Vertrauenspersonen ist in allen Fällen von einem Gericht zu treffen.

Die Regelung zur Maximaldauer des Einsatzes einer Vertrauensperson (ein Jahr) in Absatz 2 Satz 2 ist kritikwürdig. Die Höchstfrist für die Erstanordnung ist zu lang und sollte deutlich reduziert werden, so wie in anderen Polizeigesetzen üblich.⁶⁵

⁶⁴ BVerfG NJW 2016, 1781, Rn. 174.

⁶⁵ Vgl. z. B. § 45 Abs. 5 Satz 3 BKAG: drei Monate; ebenso Art. 37 Abs. 3 Satz 2 i. V. m. Art. 36 Abs. 3 Satz 3 PAG BY: sechs Monate.

Grundlegende Wertentscheidungen - erst recht über den Umfang von Eingriffsbefugnissen des Staates in Grundrechte der Bürger - sollten allein dem förmlichen Gesetzgebungsverfahren vorbehalten bleiben. Die Datenerhebung bzw. Informationsbeschaffung durch Vertrauenspersonen greift besonders tief in die Grundrechte der Betroffenen ein, zumal die Maßnahme verdeckt durchgeführt wird. Auch ist zu berücksichtigen, dass die Daten von einer Privatperson im Auftrag der Polizei erhoben werden. Daher wird der Ansatz in Absatz 5 begrüßt, gesetzliche Regelungen zu schaffen, wann eine Person nicht als Vertrauensperson eingesetzt werden darf.

Die grundlegenden Wertentscheidungen bei einer Datenerhebung mittels Vertrauenspersonen betreffen jedoch auch andere Fragen, die nicht mit Hilfe von Verwaltungsvorschriften der Polizei beantwortet werden können. So muss es gesetzliche Regelungen zur Zuverlässigkeit der eingesetzten Personen sowie zur Überprüfung des Wahrheitsgehaltes der erhobenen Daten geben. Letzteres folgt auch zwingend aus europäischem Recht, Art. 4 Abs. 1 Buchst. d) bzw. Art. 7 JI-Richtlinie. Andere Länder, wie z. B. Bayern, verfügen bereits über derartige gesetzliche Vorgaben, die auch in den hiesigen Gesetzentwurf zu übernehmen sind.⁶⁶

30. Zu Nr. 31, § 36a

Neu aufgenommen werden soll in Absatz 4 eine Anordnungsregelung bei Gefahr im Verzug. Hiernach kann der Einsatz eines verdeckten Ermittlers zukünftig auch durch die Polizei angeordnet werden. Die Gesetzesbegründung schildert detailliert in Betracht kommende Fälle aus der Praxis, die eine Ergänzung im vorgeschlagenen Sinne erforderlich erscheinen lassen. Andere Gefahrenabwehrgesetze, die bereits das Urteil des Bundesverfassungsgerichts zum BKA-Gesetz umgesetzt haben, verfügen ebenfalls über Anordnungsregelungen bei Gefahr im Verzug.⁶⁷

Schon bisher darf eine Maßnahme nach § 36 a nur vom Amtsgericht Hannover angeordnet werden und zwar unabhängig davon, ob sich der Einsatz des verdeckten Ermittlers gegen eine bestimmte Person richtet oder nicht. Vor dem Hintergrund der zu § 36 beabsichtigten Differenzierung bei der Anordnungsbefugnis zwischen Gericht und Polizei und der Bundesverfassungsgerichtsentscheidung zur Verfassungsmäßigkeit des § 20g Abs. 3 Satz 1 BKAG a. F. ist es erstaunlich, dass bei § 36 a in der Frage der Anordnungsbefugnis keine Änderung und damit Differenzierung vorgeschlagen wird.

31. Zu Nr. 32, § 37

Die Präzisierungen in der Datenübermittlungsvorschrift in Absatz 2, welche Daten zukünftig in der Kontrollmeldung aufgenommen werden dürfen, sind mit Blick auf den Bestimmtheitsgrundsatz nicht zu beanstanden.

Ferner bestimmt Absatz 3 Satz 8, dass eine Verlängerung der Ausschreibung über ein Jahr hinaus zukünftig vom Amtsgericht angeordnet werden muss. Dies stärkt die Rechte der Betroffenen und ist daher aus Sicht des Datenschutzes zu begrüßen.

31. Zu Nr. 33 a), § 37 a Abs. 1

Die Aufnahme der Rasterfahndung sowie der Datenerhebung durch Vertrauenspersonen in den Katalog der Maßnahmen nach Abs. 1, die einer parlamentarischen Kontrolle unterliegen, ist mit Blick auf die Entscheidung des Bundesverfassungsgerichts zum BKAG - so die Gesetzesbegründung - folgerichtig. Bei der Rasterfahndung nach § 45a handelt es sich um eine verdeckt durchgeführte Maßnahme. Gleiches gilt für die Maßnahme nach § 36.

⁶⁶ Vgl. z. B. Art. 38 Abs. 6 PAG BY.

⁶⁷ Vgl. z. B. Art. 37 Abs. 2 Satz 2 i. V. m. Art. 36 Abs. 4 Satz 2 bis 4 PAG BY; § 45 Abs. 3 Satz 2 BKAG.

Der Katalog ist jedoch um weitere Überwachungsmaßnahmen zu ergänzen, die der Polizei ebenfalls eine verdeckte Datenerhebung ermöglichen. Dies gilt im Fall der verdeckten Videoüberwachung nach § 32 Abs. 2 sowie bei einer verdeckten Datenerhebung durch Kernzeichenlesegeräte nach § 32 Abs. 6 Satz 6.⁶⁸ Dementsprechend ist die Aufzählung der Maßnahmen in Absatz 1 entsprechend zu erweitern, sofern die genannten Regelungen wegen fehlender Anwendung in der polizeilichen Praxis nicht ersatzlos gestrichen werden.

32. Zu Nr. 33 b), § 37 a Abs. 2

Das Bundesverfassungsgericht hat zu verdeckt durchgeführten Maßnahmen zum Zwecke der Gefahrenabwehr (Regelungen im BKAG) im Einzelnen ausgeführt:⁶⁹

„Da sich die Durchführung von heimlichen Überwachungsmaßnahmen der Wahrnehmung der Betroffenen und der Öffentlichkeit entzieht und dem auch Benachrichtigungspflichten oder Auskunftsrechte mit der Möglichkeit anschließenden subjektiven Rechtsschutzes nur begrenzt entgegenwirken können, sind hinsichtlich der Wahrnehmung dieser Befugnisse regelmäßige Berichte des Bundeskriminalamtes gegenüber Parlament und Öffentlichkeit gesetzlich sicherzustellen. Sie sind erforderlich und müssen hinreichend gehaltvoll sein, um eine öffentliche Diskussion über Art und Ausmaß der auf diese Befugnisse gestützten Datenerhebung, einschließlich der Handhabung der Benachrichtigungspflichten und Löschungspflichten, zu ermöglichen und diese einer demokratischen Kontrolle und Überprüfung zu unterwerfen.“

Diese Vorgaben des Bundesverfassungsgerichts zum Inhalt der Berichte sollen nunmehr in Abs. 2 Satz 2 umgesetzt werden. Es fehlen jedoch Angaben zur Handhabung der Löschungspflichten. Hier ist eine Ergänzung erforderlich.

Ferner ist nach den Vorgaben des Bundesverfassungsgerichts sicherzustellen, dass neben dem Parlament auch die Öffentlichkeit unterrichtet wird. Dies ist durch die Vorschrift des § 37 a Abs. 3 ausgeschlossen, wonach die Verhandlungen des Ausschusses vertraulich sind. Auch an dieser Stelle ist daher nachzubessern.⁷⁰

33. Zu Nr. 34 a), § 38 Abs. 2

Bisher enthielt § 38 Abs. 1 keine Regelung welche polizeilichen Datenverarbeitungsvorgänge im Einzelnen von einer Verarbeitung im Rahmen der Aufgabenerfüllung erfasst werden. Dies soll vor dem Hintergrund der in der Gesetzesbegründung zitierten Entscheidung des OLG Lüneburg mit dem neuen Absatz 2 näher ausgeführt werden. Danach wird für den Rechtsanwender klargestellt, dass auch eine Verarbeitung zum Zweck der Dokumentation, Vorgangsverwaltung, Datenschutzkontrolle, Datensicherung oder zum ordnungsgemäßen Betrieb einer Datenverarbeitungsanlage zulässig ist. Hiergegen bestehen keine datenschutzrechtlichen Bedenken.

Jedoch bestimmt Satz 2 in Absatz 2, dass die Regelungen des Abs. 1 Satz 3 für die zuvor genannten Fälle der Datenverarbeitung nicht anzuwenden sind mit der Folge, dass es bei der Speicherung dieser Daten zu keiner Festlegung des Zwecks kommt. Dies ist abzulehnen. Art. 4 Abs. 1 Buchst. b) und c) JI-Richtlinie verlangen, dass bei einer Verarbeitung von Daten immer der genaue Zweck zu bestimmen und festzulegen ist. Dementsprechend ist § 25 NDSG formuliert, mit dem unter anderem Art. 4 JI-Richtlinie in nationales Recht umgesetzt wird und der auch für die polizeiliche Datenverarbeitung im Sinne des § 38 anwendbar ist.

⁶⁸ Vgl. dazu die Ausführungen zu Zif. 9.

⁶⁹ BVerfG NJW 2016, Rn. 143.

⁷⁰ Vgl. Art. 52 Abs. 2 PAG BY.

Die genaue Festlegung des Zwecks bei allen Formen der Datenverarbeitung spielt eine zentrale Rolle im Datenschutzrecht. Nur so ist es überhaupt möglich zu entscheiden, in welchen Fällen eine Zweckänderung vorliegt, die grundsätzlich einer Legitimation durch eine gesetzliche Vorschrift bedarf. Die Nichtanwendung des Absatzes 1 Satz 3 hätte zur Folge, dass der Rechtsanwender von einem Verarbeitungszweck in allen Fällen des Absatzes 2 ausgehen darf. Dies ist aber gerade nicht der Fall, denn es kommt sehr wohl darauf an, ob Daten beispielsweise zur Datenschutzkontrolle oder zur Vorgangsverwaltung gespeichert worden sind. Das zeigt sich auch in der Aufzählung in § 39 Abs. 2 Satz 1, der zwischen Daten zum Zweck der Datenschutzkontrolle und Vorgangsverwaltung unterscheidet. Ferner gibt es Regelungen im Gesetz, die nur für Daten, die zum Zweck der Datenschutzkontrolle gespeichert sind, bestimmten Anforderungen formulieren.

34. Zu Nr. 34 c), § 38 Abs. 3

Mit der Neufassung des Absatzes 3 soll die Kennzeichnungspflicht für personenbezogene Daten eingeführt werden, die im Rahmen einer Rasterfahndung erhoben werden. Dies entspricht den Vorgaben des Bundesverfassungsgerichts aus dem BKA-Gesetz-Urteil. Bei der Rasterfahndung handelt es sich wie bei den Datenerhebungen mit besonderen Mitteln und Methoden ebenfalls um eine verdeckte Maßnahme, so dass bei Zweckänderungen bestimmte gesetzliche Vorgaben zu beachten sind, deren Einhaltung durch die Kennzeichnung der Daten sichergestellt wird.

Konsequenterweise sind auch Daten, die aus einer verdeckten Videoüberwachung nach § 32 Abs. 2 oder einer Maßnahme nach § 32 Abs. 6 Satz 6 gewonnen wurden, zu kennzeichnen. Abs. 3 ist daher entsprechend zu ergänzen.

35. Zu Nr. 35 a), § 39 Abs. 1

Die Änderungen sind ausweislich der Gesetzesbegründung den Vorgaben geschuldet, die das Bundesverfassungsgericht für eine zweckändernde Verwendung von personenbezogenen Daten aufgestellt hat. Der Gesetzgeber kann eine weitere Nutzung der Daten auch zu einem anderen Zweck als dem der ursprünglichen Datenerhebung erlauben. Jedoch muss er dabei berücksichtigen, dass dem Eingriffsgewicht bei der Datenerhebung auch bei der weiteren Nutzung Rechnung getragen wird.

Hierbei gilt es, den Grundsatz der hypothetischen Datenneuerhebung zu beachten. Eine Zweckänderung setzt danach voraus, dass die neue Nutzung der personenbezogenen Daten einem Rechtsgüterschutz oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnte.⁷¹ Kongruenz hinsichtlich des Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts ist nur bei den besonders eingriffsintensiven Maßnahmen der Wohnraumüberwachung und der sog. Online-Durchsuchung erforderlich.⁷²

Vor diesem Hintergrund wird die Einbeziehung der Rasterfahndung in die neue Zweckänderungsvorschrift des § 39 Abs. 1 Nr. 2 begrüßt. Bei der Rasterfahndung handelt es sich um eine heimlich durchgeführte Maßnahme mit erheblichem Eingriffsgewicht in das Grundrecht auf informationelle Selbstbestimmung. Dies ist auch bei einer zweckändernden Datennutzung zu berücksichtigen.

Darüber ist nach der zitierten Rechtsprechung des Bundesverfassungsgerichts für Daten, die im Rahmen einer Wohnraumüberwachung nach § 35a oder einer Online-Durchsuchung nach § 33 d erhoben wurden, eine gesetzliche Regelung erforderlich, die sicherstellt, dass eine zweckändernde Nutzung nur bei Vorliegen einer dringenden oder hinreichend konkretisierten Gefahrenlage möglich

⁷¹ BVerfG NJW 2016, 1781, Rn. 287, 288.

⁷² BVerfG NJW 2016, 1781, Rn. 291.

ist. Dies ergibt sich für den Rechtsanwender nicht ohne weiteres aus der derzeitigen Formulierung des § 39 Abs. 1 Nr. 1.⁷³

36. Zu Nr. 35 b), § 39 Abs. 2

Mit den Änderungen in Absatz 2 Satz 1 sollen die Zweckänderungsregelungen für die aufgeführten einer strengen Zweckbindung unterliegenden Datenkategorien klarer und bestimmter als bisher formuliert werden. Eine Zweckdurchbrechung bei Daten, die z. B. ausschließlich zur Vorgangsverarbeitung oder Datenschutzkontrolle gespeichert sind, ist zukünftig - wie bisher - zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person oder zur Aufklärung einer Straftat von erheblicher Bedeutung möglich (§ 39 Abs. 2 Nr. 1). Zusätzlich wird einschränkend bestimmt, dass die Daten „zu diesem Zweck auch nach Maßgabe der Vorschriften der Strafprozessordnung hätten erhoben werden dürfen“. Die Gesetzesbegründung enthält keine erläuternden Ausführungen über die Gründe für diese Einschränkung. Es kann nur vermutet werden, dass damit die Vorgaben des Bundesverfassungsgerichts zur zweckändernden Verwendung von Daten nach dem Kriterium der „hypothetischen Datenneuerhebung“ umgesetzt werden sollen.

An dieser Stelle wird mehr als deutlich, dass die für den Rechtsanwender ohne schon schwer verständlichen Vorschriften der §§ 38, 39 zu Fragen der Speicherung, Veränderung, Nutzung und Zweckänderung von Daten weiter verkompliziert werden und dringend einer grundlegenden Überarbeitung bedürfen. Die vom Bundesverfassungsgericht aufgestellten Kriterien zur hypothetischen Datenneuerhebung, die bei Zweckänderungen zu beachten sind, werden an dieser Stelle und in den folgenden Änderungsvorschlägen nur unzureichend umgesetzt. So ist es zweifelhaft, ob die genannten Datenkategorien unabhängig von der Frage, im Rahmen welcher Befugnisnorm diese erhoben wurden (offen, verdeckt, mit welchem Eingriffsgewicht?), zum Zweck der Aufklärung von Straftaten von erheblicher Bedeutung genutzt werden dürfen. Straftaten von erheblicher Bedeutung umfassen nach dem Katalog des § 2 Nr. 14 auch Straftatbestände, die dem Bereich der mittleren Kriminalität zuzurechnen sind. Stammen Daten beispielsweise aus einer Wohnraumüberwachung (optisch/akustisch?) zur Gefahrenabwehr und werden diese Daten nachfolgend ausschließlich noch zum Zweck der Vorgangsverwaltung gespeichert, dann dürfen diese Daten nach den Vorgaben des Bundesverfassungsgerichts zweckändernd gerade nicht für die Verfolgung von „nur“ erheblichen Straftaten verwendet werden. Dies aber bringen die vorgeschlagenen Änderungen ebenso wenig klar zum Ausdruck wie die Vorgabe, dass die Verwendung von Daten, die aus einer optischen Wohnraumüberwachung stammen, für Strafverfolgungszwecke generell unzulässig ist.⁷⁴

Die neu eingefügte Zweckänderungsvorschrift des Absatzes 2 Satz 1 Nr. 2 ist verfassungswidrig und damit ersatzlos zu streichen. Zwar wird hier die Zweckänderung nur zugelassen, wenn dies zur Verhütung terroristischer Straftaten erforderlich ist. Es geht also um schwerwiegendere Straftaten als in der Nr. 1. Jedoch werden die Anforderungen an die Prognoseentscheidung, ob überhaupt eine Straftat begangen werden soll, in das Vorfeld einer konkreten Gefahr vorverlagert.

Auch die beabsichtigten Änderungen in Satz 2, die ausweislich der Gesetzesbegründung die Vorgaben des Bundesverfassungsgerichts zur zweckändernden Verwendung von Daten umsetzen sollen, sind unzureichend und nicht geeignet, die Kriterien der hypothetischen Datenneuerhebung für den Rechtsanwender verständlich und handhabbar umzusetzen.

Dass an dieser Stelle des Gesetzentwurfs dringender Nachbesserungsbedarf besteht, zeigen die Gesetze derjenigen Länder, die ihre datenschutzrechtlichen Vorschriften an die Vorgaben des Bundesverfassungsgerichts bereits angepasst haben.

⁷³ Vgl. hierzu § 12 Abs. 3 BKAG; Art. 48 Abs. 4 PAG BY.

⁷⁴ BVerfG NJW 2016, 1781, Rn. 317.

37. Zu Nr. 35 f), § 39 Abs. 6

Die Ergänzung des Abs. 6 in Satz 1 um den Zweck der Strafvollstreckung begegnet keinen datenschutzrechtlichen Bedenken. Die Gesetzesbegründung ist insoweit nachvollziehbar, um die Erforderlichkeit zur zweckändernden Datennutzung zu begründen.

Bei den weiteren Änderungen in Satz 1 und im neuen Satz 2 soll die Verwendung von Daten, die zum Zweck der Gefahrenabwehr erhoben wurden, für Zwecke der Strafverfolgung erheblich eingeschränkt werden. Bisher konnten die Behörden sämtliche Daten aus der Gefahrenabwehrtätigkeit ohne Begrenzung auch für strafprozessuale Zwecke nutzen. Diese uferlose Zweckänderungsregelung ist seit der Rechtsprechung des Bundesverfassungsgerichts zum BKA-Gesetz verfassungswidrig. Insofern wird das Regelungsziel aus Sicht des Datenschutzes ausdrücklich begrüßt.

Die Änderungen sind jedoch auch an dieser Stelle für den Rechtsanwender wenig verständlich und setzen die Vorgaben des Bundesverfassungsgerichts nur unzureichend um. Es fehlt eine ausdrückliche Regelungen über Daten, die aus einer Wohnraumüberwachung stammen und zum Zweck der Strafverfolgung weiterverarbeitet werden sollen. Hier schließt Art. 13 Abs. 3 GG die Weiterverarbeitung von Daten, die aus einer optischen Wohnraumüberwachung stammen, zur Straftatenverfolgung aus.⁷⁵ Andere Polizeigesetze sehen daher eine ausdrückliche Regelung für derartige Fälle vor.⁷⁶ Auch sind spezielle die Zweckänderung einschränkende Regelungen für Daten verfassungsrechtlich geboten, die aus einer Online-Durchsuchung stammen.⁷⁷

38. Zu Nr. 35 g), § 39 Abs. 7

Eine Datennutzung nicht nur zu Ausbildungs-, sondern zukünftig auch zu Fortbildungszwecken zuzulassen, begegnet keinen datenschutzrechtlichen Bedenken. Die Erforderlichkeit der zweckändernden Datenverwendung wird in beiden Fällen gesehen. Die Zielrichtung der Änderung des Abs. 7, den Grundsatz der Anonymisierung der Daten stärker als bisher zu betonen, wird begrüßt.

39. Zu Nr. 36, § 39 a Abs. 2

Die beabsichtigte Einführung einer Dokumentationspflicht für die Löschung personenbezogener Daten, die mit besonderen Mitteln oder Methoden oder mittels einer Rasterfahndung erhoben wurden, sollen die besonderen Vorgaben des Bundesverfassungsgerichts für Daten umsetzen, die aus verdeckt durchgeführten Überwachungsmaßnahmen stammen. Es fehlen die Maßnahmen der verdeckten Videoüberwachung (§ 32 Abs. 2) sowie des verdeckt durchgeführten Einsatzes des Kennzeichenlesegeräts (§ 32 Abs. 6 Satz 6).

Die Ausführungen des Bundesverfassungsgerichts zur Protokollierungspflicht⁷⁸ beziehen sich nicht nur auf den Vorgang der Datenlöschung. Vielmehr fordert das Gericht eine umfassende Protokollierungspflicht für sämtliche Verfahrensschritte, die im Zusammenhang mit einer verdeckt durchgeführten Überwachungsmaßnahme zur Gefahrenabwehr stehen. Nur dann sei sichergestellt, dass die Maßnahme nachträglich umfassend von der Datenschutzbehörde kontrolliert werden könne. Ferner komme hinzu, dass sich die Aufklärung und Abwehr von Gefahren nicht wie im Strafprozess im Wege eines Ermittlungsverfahrens, das sich immer gegen eine bestimmte Person richte, vollziehe. Somit sei die Nachvollziehbarkeit der Datenerhebung für die Betroffenen bei Gefahrenabwehrmaßnahmen nicht in jedem Fall gewährleistet. Auch bei einer richterlichen Anordnung ändere sich hieran nichts, denn der Richter prüfe nur das Vorliegen der Voraussetzungen durch Durchführung der verdeckten Überwachungsmaßnahme nicht aber, ob und in welcher Art und Weise die Maßnahme durchgeführt werde.

⁷⁵ Vgl. dazu BVerfG NJW 2016, Rn. 317.

⁷⁶ Vgl. Art. 48 Abs. 4 Satz 2 Nr. 2 PAG BY; § 23 Abs. 7 PolG BW.

⁷⁷ Vgl. § 12 Abs. 3 BKAG.

⁷⁸ BVerfG NJW 2016, 1781, Rn. 267.

Folglich wird angeregt, im Gesetz umfassende Protokollierungs- und Dokumentationspflichten bei verdeckt durchgeführten Überwachungsmaßnahmen zu verankern, die auch die Durchführung bzw. Ausführung der Maßnahme betreffen (Zeit, Ort, Umfang/Dauer der Maßnahme, betroffene Personen etc.). Nur dann ist sichergestellt, dass die jeweilige Überwachungsmaßnahme umfassend datenschutzrechtlich im Nachgang überprüft werden kann.⁷⁹

Schriftform- und Begründungserfordernis bei der Beantragung der Maßnahme, wie sie im Gesetz an verschiedenen Stellen vorgesehen sind, reichen nicht aus, um die Vorgaben des Bundesverfassungsgerichts umzusetzen. Diese dokumentieren nur die Tatsachen, die den Tatbestand der jeweiligen Befugnisnorm zum Zeitpunkt der Anordnung ausfüllen. Zur datenschutzrechtlichen Kontrolle der Ausführung der Maßnahme können diese Verfahrensvorschriften der Datenschutzbehörde keine Erkenntnisse liefern.

Dass die in Satz 1 genannten Daten ausschließlich nur zum Zweck der Datenschutzkontrolle verwendet werden dürfen (Satz 2), wird aus Sicht des Datenschutzes begrüßt. Hier wird allerdings ein möglicher Widerspruch zu § 39 Abs. 2 gesehen. Dort dürfen Daten, die der Dokumentation oder Vorgangsverwaltung dienen (Satz 1 Nr. 1) oder zum Zweck der Datenschutzkontrolle gespeichert werden, unter bestimmten Voraussetzungen zu anderen Zwecken verwendet werden. Die in § 39 Abs. 2 aufgeführten Protokollierungsdaten über die Löschung fallen ebenfalls unter die in § 39 Abs. 2 genannten Datenkategorien. Insofern herrscht für den Rechtsanwender Unklarheit, wie mit Protokollierungsdaten über den Löschungsvorgang umzugehen ist.

40. Zu Nr. 37, § 40 Abs. 1

Die vorgeschlagenen Änderungen sind dem Grunde nach nicht zu beanstanden. Sie setzen die Vorgaben des Bundesverfassungsgerichts bei Datenübermittlungen um. Es soll sichergestellt werden, dass der Datenübermittlungsvorgang bei Daten, die aus verdeckt durchgeführten Überwachungsmaßnahmen stammen, ausreichend dokumentiert wird und der dokumentierte Vorgang mindestens zwei Jahre aufzubewahren ist. Somit ist gewährleistet, dass die vom Bundesverfassungsgericht geforderte regelmäßige Kontrolle von Datenübermittlungen durch die Datenschutzbehörden stattfinden kann.

41. Zu Nr. 39 b), § 44 Abs. 2 Satz 2

Mit der Gesetzesänderung ist beabsichtigt, Daten oder Abbildungen einer Person zum Zweck der Ermittlung der Identität oder des Aufenthaltsortes oder zur Warnung auch über das Internet öffentlich bekannt zu geben. Damit soll offenbar die sog. Öffentlichkeitsfahndung in sozialen Netzwerken auf eine gesetzliche Grundlage gestellt werden. Eine Datenübermittlung auf im Ausland liegende Server soll allerdings nur zulässig sein, wenn ein angemessenes Datenschutzniveau im Sinne des § 4 b Abs. 3 BDSG⁸⁰ gewährleistet ist.

Die Vorschrift des § 44 Abs. 2 wurde 1997 in das Nds. SOG eingefügt. Zu dieser Zeit befand sich das Internet als Kommunikationsmedium in den Kinderschuhen. Soziale Netzwerke, die dem Internetzeitalter 2.0 zugeschrieben werden, waren noch völlig unbekannt. Folglich hatte der Gesetzgeber seinerzeit in erster Linie die öffentliche Bekanntgabe von personenbezogenen Daten in Zeitungen, Fernsehen, Rundfunk und durch Aushänge oder Lautsprecherdurchsagen im Blick.

Im Vergleich zum Internet zeichnen sich diese Formen der öffentlichen Bekanntgabe dadurch aus, dass die Vorgänge nach einiger Zeit in Vergessenheit geraten und auch nicht mehr ohne weiteres recherchierbar sind. Anders sieht es mit Veröffentlichungen im Internet aus und dies unbeschadet

⁷⁹ Vgl. hierzu die detaillierten Regelungen im BKAG.

⁸⁰ Jetzt wohl §§ 78 ff. BDSG.

des Speicherortes (im In- oder Ausland). Für einen gewissen Zeitraum steht die Information, z. B. dass nach einer bestimmten Person wegen der Gefahr der Begehung einer Straftat gefahndet wird (§ 44 Abs. 2 Nr. 2), einer unbestimmten Anzahl von Internetnutzern jederzeit abrufbar zur Verfügung. Diese Personen können ungehindert auf den Fahndungsauftrag zugreifen, die entsprechende Internetseite kopieren und weiterverbreiten, so dass diese auch noch nach Löschung der entsprechenden Behördenseite im Internet zur Verfügung steht.

Der Eingriff in den Schutzbereich des Grundrechts auf informationelle Selbstbestimmung mittels Öffentlichkeitsfahndung im Internet zum Zweck der Gefahrenabwehr ist damit umfassender und tiefergehend, als bei den bisher in Absatz 2 geregelten Fällen. Dies berücksichtigt die vorgesehene Regelung nicht in ausreichendem Maße. Vielmehr soll in allen Fällen - und damit auch für die Internetfahndung - eine Straftat von erheblicher Bedeutung als Eingriffsvoraussetzung genügen. Der Straftatenkatalog des § 2 Nr. 14 umfasst jedoch auch Straftaten, die dem Bereich der mittleren Kriminalität zuzuordnen sind. Die Internetfahndung sollte - wenn überhaupt - nur für Fälle schwerster Kriminalität zulässig sein.

Ferner stellt sich die Frage der praktischen Umsetzung der Vorgaben des Satzes 2 durch die Behörden. Zunächst müssten diese die genauen Standorte der Server ermitteln, um anhand des dort geltenden Datenschutzrechts überprüfen zu können, ob ein angemessenes Datenschutzniveau für die übermittelten Daten besteht. Dies dürfte im Regelfall auf erhebliche Schwierigkeiten stoßen. Ferner kommt erschwerend hinzu, dass der EuGH in seiner Entscheidung zur Frage der datenschutzrechtlichen Verantwortlichkeit bei der Nutzung von Facebook darauf hingewiesen hat, dass auch der Betreiber einer Facebook-Seite neben dem Unternehmen Facebook für die Verarbeitung der Daten der Besucher seiner Seite verantwortlich ist.⁶¹ Diese datenschutzrechtliche Verantwortlichkeit betrifft sämtliche Pflichten, die bei einer Datenverarbeitung zu erfüllen sind, so auch die Pflicht der Datenlöschung z. B. in Fällen, in denen sich herausstellt, dass die Person, nach der im Internet gefahndet wird, die falsche ist. Ob die Behörden die Löschung als verantwortliche Stelle unverzüglich und für die Betroffenen nachvollziehbar durchführen können, wenn die personenbezogenen Daten auf Servern im Ausland liegen, ist mehr als fraglich.

Aus den genannten Gründen ist Öffentlichkeitsfahndung im Internet durch Datenübermittlungen ins Ausland aus Sicht des Datenschutzes abzulehnen. Die Nutzung von sozialen Netzwerken durch Behörden zur Öffentlichkeitsfahndung wird nach wie vor kritisch gesehen. Die vorgeschlagene Regelung verstärkt die vorhandenen Bedenken. Zur Gesamthematik wird auf den 22. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz Niedersachsen und dort auf die Ausführungen auf den Seiten 130 ff. verwiesen.

42. Zu Nr. 41, b) § 45 a Abs. 2

Die Anordnung einer Rasterfahndung soll zukünftig unter Richtervorbehalt (Amtsgericht) gestellt werden. Dies wird mit Blick auf die Eingriffstiefe in das Grundrecht auf informationelle Selbstbestimmung und die Streubreite dieser Maßnahme ausdrücklich begrüßt. Der damit verbundene Wegfall der Unterrichtung der LfD ist konsequent und entspricht der bisherigen Gesetzessystematik. Auch in den übrigen gesetzlich geregelten Fällen einer richterlichen Anordnung einer Maßnahme ist keine Beteiligung der LfD vorgesehen. Im Übrigen ist die LfD zukünftig verpflichtet (§ 48), in regelmäßigen Abständen heimlich durchgeführte Überwachungsmaßnahmen datenschutzrechtlich zu überprüfen. Hierzu gehört auch die Rasterfahndung.

Im Vergleich zu anderen Ländern enthält die Vorschrift zur Rasterfahndung in Niedersachsen bisher keine besonderen die Maßnahme flankierenden Verfahrensvorschriften. Diese sind aber mit Blick auf die Eingriffstiefe und Streubreite des Instruments der Rasterfahndung zwingend erforder-

⁶¹ EuGH, Urteil vom 05.06.2018, C-210/16, Rn. 39.

lich, um dem Grundsatz der Verhältnismäßigkeit zu genügen. Hierzu gehören insbesondere Regelungen zu Löschungspflichten. Diese sollen sicherstellen, dass eine Verwendung personenbezogener Daten auf die die Datenverarbeitung rechtfertigenden Zwecke begrenzt bleibt und nach deren Erledigung nicht mehr möglich ist.⁸² So enthalten die Polizei- und Gefahrenabwehrgesetze in anderen Ländern spezielle Regelungen zur Löschung von Daten, die im Rahmen einer Rasterfahndung erhoben wurden.⁸³ Es wird demnach angeregt, § 45a um eine spezielle Regelung zur Datenlöschung zu ergänzen.

43. Zu Nr. 43, § 48

Mit Absatz 1 im neuen § 48 sollen Protokollierungspflichten über die Datenerhebung für bestimmte eingriffsintensive Maßnahmen, vor allem für verdeckt durchgeführte, festgeschrieben werden. Dies ist eine Folge aus dem Urteil des Bundesverfassungsgerichts zum BKA-Gesetz und soll dort genannte Vorgaben umsetzen.

Hinzuweisen ist darauf, dass die Vorschrift nicht alle im Polizeigesetz enthaltenen Datenüberwachungsmaßnahmen enthält, die heimlich und mit großer Streubreite und somit mit einer schwerwiegenden Eingriffstiefe in die Grundrechte durchgeführt werden. Es fehlen die Maßnahmen nach § 32 Abs. 2 und § 32 Abs. 6 Satz 6.

Das Bundesverfassungsgericht hat entschieden, dass nicht nur die Datenerhebungen zu protokollieren sind, sondern auch die Verarbeitungsvorgänge der Übermittlung und Löschung.⁸⁴ Dies ist durch § 39 a Abs. 2 (Löschung) bzw. § 40 Abs. 1 (Übermittlung) sichergestellt, so die Gesetzesbegründung. Ferner enthält das neue Polizei- und Ordnungsbehördengesetz an weiteren Stellen spezielle Vorschriften über die Protokollierung bestimmter Datenverarbeitungsvorgänge, so z. B. die Dokumentationspflichten bei der Anordnung von Maßnahmen oder für den Kernbereichsschutz. Mithin könnte für den Rechtsanwender der Eindruck entstehen, dass für die übrigen Fälle, bei denen das Gesetz keine ausdrückliche Dokumentation verlangt, eine solche entfällt.

Da jeder Datenverarbeitungsvorgang nach der Rechtsprechung des Bundesverfassungsgerichts mit einem Grundrechtseingriff für die Betroffenen verbunden ist, muss jegliche Datenverarbeitung transparent, nachvollziehbar und einer Rechtmäßigkeitskontrolle zugänglich sein. Dies setzt voraus, dass die Behörde die generelle Pflicht hat, die gesamte Datenverarbeitung in einer nachprüfbar- und dokumentierbaren Art und Weise zu dokumentieren. Eine solche gesetzliche Regelung, die dies für die Polizeibehörden im Anwendungsbereich der JI-Richtlinie in Niedersachsen im Einzelnen sicherstellt, ist § 35 Abs. 2 NDSG. Diese Norm sollte in § 48 Abs. 1 als Verweisnorm aufgenommen werden.⁸⁵

Gegen die Regelung des § 48 Absatz 2, der eine regelmäßige Kontrolle der Verarbeitung der aufgeführten Daten vorschreibt und ebenfalls der Rechtsprechung des Bundesverfassungsgerichts geschuldet ist, bestehen keine Bedenken. In diesem Zusammenhang hat das Bundesverfassungsgericht darauf hingewiesen, dass der Gesetzgeber den durch die regelmäßigen Prüfungen entstehenden zusätzlichen Aufwand auch bei der Personalausstattung der Datenschutzbehörden angemessen zu berücksichtigen hat.⁸⁶

⁸² BVerfG NJW 2016, Rn. 144.

⁸³ Vgl. z. B. § 46 Abs. 4 PAG BY; § 47 Abs. 3 ASOG BE; § 46 Abs. 3 Bbg.PolG; § 26 Abs. 3 Hess.SOG; § 31 Abs. 3 PolG NW.

⁸⁴ BVerfG NJW 2016, 1781, Rn. 129, 144, 322.

⁸⁵ So z. B. im BKAG, § 81 BKAG.

⁸⁶ BVerfG NJW 2016, 1781, Rn. 141.

44. Zu Artikel 5 des Gesetzentwurfs, Evaluierung

Mit Artikel 5 soll eine Evaluierungspflicht für bestimmte neue Überwachungsmaßnahmen in das Gesetz aufgenommen werden.

Diese betrifft die Meldeauflage nach § 16 a Abs. 2, die Aufenthaltsvorgabe und das Kontaktverbot nach § 17 b, die elektronische Aufenthaltsüberwachung nach § 17 c, die Quellentelekommunikationsüberwachung nach § 33 a Abs. 2 sowie den verdeckten Eingriff in informationstechnische Systeme nach § 33 d. Diese Maßnahmen sollen bis Ende 2023 auf ihre Geeignetheit und Wirksamkeit hin überprüft werden.

Die Überlegung, neue eingriffsintensive Maßnahmen auf ihre Praxistauglichkeit zu untersuchen, wird aus Sicht des Datenschutzes grundsätzlich unterstützt. Jedoch sollten weitere Überwachungsinstrumente in die Evaluierungspflicht aufgenommen werden, wie z. B. die neuen Maßnahmen des § 32 Abs. 4 Sätze 2 und 3 sowie Abs. 5 (Bodycams) und § 32 Abs. 8 (Section Control). Auch die mit dem Gesetzentwurf beabsichtigte Ausweitung der Videoüberwachung mittels Bildaufzeichnung sowie die Vorschrift des § 32 a sollten kritisch auf ihre Tauglichkeit zur Gefahrenabwehr hinterfragt und damit in Art. 5 aufgenommen werden.

II. Zum Entschließungsantrag der Fraktion Bündnis 90/Die Grünen (LT-Drs. 18/828). Für ein Niedersächsisches Gefahrenabwehrgesetz ohne Symbolpolitik und Generalverdacht:

Zu den im Entschließungsantrag angesprochenen datenschutzrechtlichen Vorschlägen nehme ich wie folgt Stellung:

Zahlreiche angesprochene Themen finden sich auch im vorliegenden Gesetzentwurf wieder, so z. B. die Forderungen, eine Legaldefinition für „terroristische Straftaten“ einzuführen oder die Gefährderansprache gesetzlich zu normieren (Ziffern 6 und 9). Insofern kann ich im Einzelnen auf die dazu gemachten Ausführungen im Rahmen meiner Stellungnahme - insbesondere zu den besonders grundrechtsrelevanten Überwachungsmaßnahmen der §§ 17 c, 32 a Abs. 2, 33 d (Ziffern 12 bis 13) und zur Videoüberwachung (Ziffern 14 bis 16) - verweisen.

Ferner sind verschiedene Punkte schon im Gesetzentwurf der Landesregierung vom 03.08.2016, LT-Drs. 17/6232, enthalten, so u. a. die Ziffern 8 bis 11, 15 und teilweise 16. Auch hierzu hat meine Behörde sowohl schriftlich als auch mündlich im Rahmen der Anhörung im Innenausschuss umfassend Stellung genommen. Um Wiederholungen zu vermeiden, verweise ich daher auf die dort gemachten Ausführungen.

Mit freundlichem Gruß

Barbara Thiel