**Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen**

LDI NRW, Postfach 20 04 44, 40102 Düsseldorf
Der Präsident
des Landtags Nordrhein-Westfalen
Platz des Landtags 1
40221 Düsseldorf

per E-Mail an: anhoerung@landtag.nrw.de

LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE

STELLUNGNAHME
17/645

A09, A14

Aktenzeichen
bei Antwort bitte angeben
202.1.1

Telefon 0211 38424-
Fax 0211 38424-10

Gesetzesentwurf der Landesregierung zur Stärkung der Sicherheit in Nordrhein-Westfalen – Sechstes Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen (PolG NRW)

Anhörung des Innenausschusses am 7. Juni 2018

Ihr Schreiben vom 14. Mai 2018, Ihr Zeichen: I.1

Sehr geehrter Herr Präsident,

sehr geehrte Damen und Herren Abgeordnete,

für die Gelegenheit zur Stellungnahme danke ich Ihnen.

Vorab möchte ich anmerken, dass das Vorziehen der Normierung der neuen Befugnisse und Regelungen für die Polizei bedenklich ist, weil dadurch die längst überfällige Anpassung des nordrhein-westfälischen Polizeirechts an die EU-Richtlinie 680/2016[1] (JI-Richtlinie – JI-RL) – Frist 06. Mai 2018 – sowie die EU-Verordnung 2016/679[2] (Datenschutz-

Dienstgebäude und Lieferanschrift:
Kavalleriestraße 2 - 4
40213 Düsseldorf
Telefon 0211 38424-0
Telefax 0211 38424-10
poststelle@ldi.nrw.de
www.ldi.nrw.de

Öffentliche Verkehrsmittel:
Rheinbahnlinien 704, 709, 719
Haltestelle Poststraße

[1] RICHTLINIE (EU) 2016/680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES 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.
[2] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung

grundverordnung - DSGVO) – Frist 25. Mai 2018 – unnötig verzögert wird.

Gleichzeitig wird der Zeitdruck, unter dem dieses Gesetzgebungsverfahren betrieben wird, der Relevanz der Thematik nicht gerecht. Im Hinblick auf den Umfang und die Intensität der vorgesehenen Eingriffe insbesondere auch in das Recht auf informationelle Selbstbestimmung der Betroffenen wäre eine wesentlich intensivere Befassung mit dem Gesetzentwurf notwendig. Bedauerlicherweise bin ich auch im Vorfeld erst spät beteiligt worden, so dass eine inhaltliche Auseinandersetzung mit meinen datenschutzrechtlichen Hinweisen vor der Einbringung in den Landtag NRW kaum möglich war.

A. Vorbemerkungen zum Gesetzentwurf

Mit dem vorliegenden Gesetzentwurf sollen tiefgreifende Eingriffsbefugnisse im nordrhein-westfälischen Polizeirecht geschaffen und zusätzliche Gefahrbegriffe eingeführt werden, die ein polizeiliches Handeln zeitlich weit im Vorfeld des tradierten Gefahrbegriffes ermöglichen würden. Einige der neuen Befugnisse würden eine Vielzahl in aller Regel völlig unbeteiligter Personen betreffen, also solche, die weder Störer i. S. d. §§ 4 f. PolG NRW noch Gefährder sind; andere Befugnisse erlauben heimliche Eingriffe. Viele der neuen Regelungen entsprechen nicht dem in der Begründung postulierten Anspruch, dass der bestmögliche Schutz vereint mit starken Bürgerrechten gewährleistet werden soll. Es handelt sich nämlich um Befugnisse, die in besonderer Weise in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen eingreifen.

Der Tätigkeitsbereich der Polizei soll in weiten Teilen auf das Gefahrenvorfeld ausgedehnt werden. Dabei fällt auf, dass das Polizeirecht mehr und mehr dem Recht der Nachrichtendienste angeglichen werden soll. Dies gilt sowohl für die Art der Befugnisse als auch für die Anpassung des Gefahrbegriffs auf einen Zeitraum deutlich vor dem etablierten Begriff der konkreten Gefahr.

Zudem überzeugen die in der Gesetzesbegründung für die erhebliche Ausweitung der Befugnisse genannten Gründe nicht. Der Entwurf (im Folgenden d. E.) bleibt hier vage und führt sehr allgemein aus, dass die

---

personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

Bundesrepublik *„derzeit Aktionsraum für terroristische Anschläge insbesondere durch islamistische Täter“* sei und sich *„u.a. „auch in Nordrhein-Westfalen* […] *die bestehende hohe abstrakte Gefährdung bereits durch die Vorbereitung oder Durchführung eines Anschlags konkretisiert“* habe (S. 27 d. E.). Derart allgemeine Erwägungen sind jedoch nicht als Grundlage für eine Abwägung der mit den Änderungen verfolgten Zwecken und den damit einhergehenden intensiven Grundrechtseingriffen geeignet.

Diesbezüglich hätte eine vorhergehende Bestandsaufnahme darüber, in welchen Bereichen welche konkreten Defizite bestehen, zur Erhellung des tatsächlichen Bedarfs neuer polizeilicher Maßnahmen beigetragen. Bei einer solchen Evaluation wären insbesondere auch die Aspekte zu betrachten gewesen, ob die ggf. ermittelten Defizite tatsächlich das Ergebnis fehlender Eingriffsbefugnisse sind, ob die bereits bestehenden Eingriffsbefugnisse vielleicht auch nur unzureichend genutzt wurden und/oder ob es sich um Mängel bei der Auswertung des vorhandenen Datenmaterials handelte. Ohne eine solche fundierte Grundlage lässt sich weder abschätzen noch überprüfen, ob und inwieweit es einer derartigen Ausweitung polizeilicher Befugnisse tatsächlich bedarf oder ob nicht vielmehr ihre vermeintliche symbolische Bedeutung im Hinblick auf eine wirksame Bekämpfung von Kriminalität in den Mittelpunkt der Betrachtung gerückt ist.

Die Berücksichtigung der verfassungsrechtlichen Rechtsprechung erfolgt in dem Entwurf weitgehend nur, wo sie zur Begründung herangezogen werden soll. Eine weitergehende Anpassung des gesamten PolG NRW – insbesondere bezüglich heimlicher Eingriffsmaßnahmen – an die verfassungsrechtlichen Vorgaben, wie sie das Bundesverfassungsgericht (BVerfG) beispielsweise in seinem Urteil vom 20. April 2016 (1 BvR 966/09 und 1 BvR 1140/06) zum Bundeskriminalamtgesetz (BKAG-Urteil) zusammengefasst hat, unterbleibt.

Insgesamt ist der Gesetzentwurf in seinen wesentlichen Regelungen aus datenschutzrechtlicher Sicht äußerst kritisch zu bewerten.

Gleichzeitig setzt der Entwurf aus Gründen des Datenschutzes wünschenswerte Neuerungen, wie sie in anderen Bundesländern teils schon viele Jahre gängige Praxis sind, nicht um. Hierzu gehören eine konkrete Rechtsgrundlage für die Durchführung von Zuverlässigkeitsprüfungen und Akkreditierungen durch die Polizei im Zusammenhang mit Großver-

anstaltungen[3] sowie konkrete Rechtsgrundlagen für die Speicherung von personengebundenen und ermittlungsbezogenen Hinweisen (sog. PHW und EHW).

B. Zu den einzelnen Vorschriften

Zu § 8 d. E.

Die neuen Begriffe der „drohenden" und der „drohenden terroristischen Gefahr" führen zu einer deutlichen Vorverlagerung polizeilicher Eingriffsbefugnisse. Die diesbezüglich strengen Vorgaben des BVerfG werden nicht eingehalten. Zudem sind die vorgesehenen Regelungen in sich und in Bezug auf ihre Rolle im Gesamtgefüge des Entwurfs nicht stimmig.

Auch wenn § 8 d. E. keine primär datenschutzrechtliche Regelung enthält, ist die Vorverlagerung des Gefahrenbegriffs mit einer massiven Ausweitung polizeilicher Befugnisse verbunden und damit letztlich gleichwohl zumindest mittelbar auch von datenschutzrechtlicher Relevanz.

Das BVerfG hat in seinem BKAG-Urteil u.a. seine bisherige Rechtsprechung zu den verfassungsrechtlichen Anforderungen an polizeiliche Gefahrenbegriffe vertieft und weiterentwickelt. Zwar lässt es danach bei Straftaten von erheblicher Bedeutung und insbesondere bei terroristischen Straftaten auch eine Gefahr ausreichen, die in Bezug auf die zeitlichen und inhaltlichen Anforderungen an die Konkretheit noch unterhalb des tradierten Gefahrenbegriffs liegt. Dabei macht das BVerfG jedoch deutlich, dass dem verfassungsmäßigen Gebot der Bestimmtheit und Klarheit der Definitionen eine besondere Bedeutung zukommt. Ich habe Bedenken, dass die neu geschaffenen Absätze 4 und 5 diesen Anforderungen gerecht werden.

[3] Vgl. Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Zuverlässigkeitsüberprüfungen bei öffentlichen und privaten Veranstaltungen nur im erforderlichen Maß und nach einem rechtsstaatlichen und transparenten Verfahren vom 26. April 2018.

So findet sich beispielsweise die in der Gesetzesbegründung mehrfach betonte und vom BVerfG benannte Voraussetzung, dass eine „Gefahr für ein überragend wichtiges Rechtsgut“ drohen müsse (vgl. S. 29 f. d. E.), weder in Absatz 4 noch in Absatz 5 wieder. Absatz 5 versucht sich zudem an einer eigenen Definition des Begriffs der „drohenden terroristischen Gefahr“, ohne dabei die im BKAG-Urteil des BVerfG enthaltene Definition des Begriffs des (internationalen) Terrorismus zu berücksichtigen. Das Gericht sieht diesen Begriff dabei durch den aus der Aufgabennorm des § 4a BKGA a. F. erfolgenden „*Verweis auf § 129a Abs. 1, 2 StGB in enger Anlehnung an den EU-Rahmenbeschluss vom 13. Juni 2002 und die internationale Begrifflichkeit* […] *definiert und – in Übereinstimmung mit den Vorstellungen des verfassungsändernden Gesetzgebers bei Schaffung des Art. 73 Abs. 1 Nr. 9a GG* […] *– auf spezifisch charakterisierte Straftaten von besonderem Gewicht begrenzt“*[4]*.* Dem entspricht Absatz 5 d. E. bisher nicht. Zum einen fehlt eine Inbezugnahme von § 129a Abs. 1 und 2 StGB. Zum anderen wird durch den Verweis auf Absatz 4 der Anwendungsbereich auf den gesamten Katalog der erheblichen Straftaten aus § 8 Abs. 3 d. E erstreckt.

Diese Aspekte sind nur als Beispiele für die geltend gemachten Bedenken zu verstehen. Eine abschließende Beurteilung des § 8 d. E. liegt außerhalb der rein datenschutzrechtlichen Einschätzungen.

Zu § 12a d. E.

Bezüglich der Einführung der „strategischen Fahndung“ bestehen erhebliche Bedenken hinsichtlich der Verhältnismäßigkeit. Die Polizei soll weitestgehend gleiche Rechte wie nach § 12 PolG NRW, allerdings unter wesentlich erleichterten Voraussetzungen und bezogen auf größere räumliche Bereiche, erhalten. Die Maßnahmen würden zudem fast ausschließlich Unbeteiligte treffen.

Gegen die mit der Vorverlagerung des Gefahrenbegriffs einhergehende Einführung der sogenannten „strategischen Fahndung“ erheben sich aus datenschutzrechtlicher Sicht erhebliche Bedenken.

[4] a.a.O, Rnr. 96.

Verdachtsunabhängige polizeiliche Maßnahmen sind stets von besonderer Eingriffsintensität für die Vielzahl unbescholtener Bürgerinnen und Bürger, die von ihnen betroffen sind. Dies gilt vor allem, da die vorgeschlagene Maßnahme geradezu darauf angelegt ist, fast ausschließlich unbeteiligte Personen zu treffen. Vorliegend soll es nicht dabei bleiben, dass die Betroffenen angesprochen werden. Vielmehr erfolgt regelmäßig auch eine Identitätsfeststellung, bei der personenbezogene Daten in nicht unerheblichem Umfang erhoben und verarbeitet werden. Die vorgesehene Neuregelung geht über die meisten bisherigen landesrechtlichen Pendants weit hinaus, indem sie eben nicht nur das Anhalten und Befragen, sondern gerade auch Identitätsfeststellungen zulässt. Schon der Umstand, dass der Entwurf einer Regelung des Hamburgischen Rechts ähnelt, die vom Hamburgischen Oberverwaltungsgericht (4 Bf 226/12, 5 K 1236/11) mangels Bestimmtheit und Verhältnismäßigkeit für verfassungswidrig erklärt und die mittlerweile durch den Hamburgischen Gesetzgeber geändert wurde, gibt Veranlassung, die Verhältnismäßigkeit der hier vorgeschlagene Regelung zu bezweifeln.

Besonders bedenklich erscheint dabei die extrem weite Ausgestaltung der Anwendungsmöglichkeiten bzw. die geradezu uferlose Weite möglicher Einsatzszenarien. In der Begründung wird hierzu ausgeführt: *„Satz 1 gestattet die vorgenannten Maßnahmen im ‚öffentlichen Verkehrsraum'. Hierunter fallen alle faktisch dem öffentlichen Verkehr zugänglichen Flächen und Verkehrswege, auch wenn sie im Privateigentum stehen und nicht öffentlich-rechtlich gewidmet sind* […]*. Der Straßenverkehrsraum ist daher lediglich ein Teil des öffentlichen Verkehrsraums. Gleichermaßen muss es sich bei den zu kontrollierenden Personen nicht auch zwangsläufig um (straßenverkehrsrechtliche) Verkehrsteilnehmer handeln. Der Begriff ist vielmehr im Sinne von ‚öffentlich zugänglichem Raum' zu verstehen und erfasst u.a. Örtlichkeiten wie Bahnhofshallen ebenso wie jedermann zugängliche Plätze* […]*. Dementsprechend sind auch Kontrollen in öffentlichen Verkehrsmitteln wie Straßenbahnen oder Bussen oder in öffentlich zugänglichen Parkhäusern möglich* […]*."* (S. 32 f. d. E.) Die besondere datenschutzrechtliche Relevanz der Maßnahme für die Betroffenen wird dabei grundsätzlich durchaus erkannt: *„§ 12a PolG erfasst* […] *einen beliebig großen Personenkreis. Jeder, der sich im öffentlichen Verkehrsraum aufhält, kann theoretisch einer Identitätskontrolle ausgesetzt sein, ohne dass das mit seinem Verhalten in Beziehung gebracht werden könnte oder durch ihn veranlasst wäre."* (S. 33 d. E.)

Angesichts dieser Beschreibung der Reichweite der Regelung, ist die folgende Feststellung in der Begründung nicht nachvollziehbar: *„Außerhalb des Grenzgebiets ist der Kontrollraum aber auf wenige räumliche Bereiche mit größerem abstrakten Gefahrenpotential beschränkt und die abstrakte Kontrollwahrscheinlichkeit im Einzelfall damit deutlich herabgesenkt."* (S. 33. d. E). Durch das Tatbestandsmerkmal *„Tatsachen die Annahme rechtfertigen, dass in diesem Gebiet Straftaten nach Abs. 1 begangen werden sollen"*, kommt nämlich grundsätzlich jeder Ort in Frage, an dem die Polizei Tatsachen zu erkennen glaubt, die eine entsprechende Annahme rechtfertigen. Da insbesondere Delikte nach § 12a Abs. 1 Nr. 3 d. E. (jeder Ort, an dem sich eine Person unerlaubt aufhält) und Nummer 1 (die Bandbreite der Delikte nach § 8 Abs. 3 PolG NRW ist sehr weit) praktisch überall vorkommen können, beschränkt sich der potentielle Kontrollraum keineswegs auf wenige räumliche Bereiche. Insofern besteht die Gefahr, dass es den Bürgerinnen und Bürgern künftig nicht mehr möglich sein wird, sich ohne unzumutbare Einschränkungen im öffentlichen Raum so zu bewegen, dass potentielle Kontrollräume weitestgehend vermieden werden.

Nicht nachvollziehbar ist auch die in der Begründung angeführte These: *„Eine Identitätskontrolle* […] *greift nur sehr geringfügig in die allgemeine Handlungsfreiheit und das Recht auf informationelle Selbstbestimmung ein. Der Eingriff erschöpft sich in einem Angehalten- und Befragtwerden sowie der Verpflichtung, ein mitgeführtes Ausweispapier zur Prüfung auszuhändigen. Soweit sich dabei weitere, über die Identitätsfeststellung hinausgehende Maßnahmen anschließen, beruhen diese nicht auf § 8 PolG. Die Datenverarbeitung richtet sich vielmehr nach den §§ 22 ff. PolG."* Ihren Ausgangspunkt finden diese ggf. weitergehenden Maßnahmen gleichwohl „in der strategischen Fahndung". Davon abgesehen kann die Identitätskontrolle als solche und die damit einhergehenden Datenerhebungen und -verarbeitungen, mit der nach der Intention des Gesetzentwurfes von jedermann an jedem Ort und zu jeder Zeit zu rechnen sein soll, aber auch im Übrigen keineswegs als unerheblich angesehen werden.

Angesichts der mit der Neuregelung zu besorgenden nahezu grenzenlosen Ausweitung von Identitätsfeststellungsszenarien erscheint die Vorschrift in dieser Fassung nicht verhältnismäßig.

Eine andere Bewertung ist auch unter Berücksichtigung der gegenüber dem zur Verbändeanhörung vorgelegten Entwurf vorgenommenen Änderungen nicht geboten. Zwar wurde die mögliche Anordnungsdauer

gegenüber dem Vorentwurf von drei Monaten mit Verlängerungsmöglichkeit auf 28 Tage mit Verlängerungsmöglichkeit reduziert. Auch ist zu begrüßen, dass § 12a d. E. nunmehr keine Voraussetzungsvariante mit Bezug auf die neuen Gefahrbegriffe aus § 8 Abs. 4 und 5 d. E. mehr enthält (die Begründung wurde jedoch nicht entsprechend angepasst). Trotz dieser Verbesserungen würde § 12a d. E. eine massive Ausweitung der Befugnisse gegenüber dem bisherigen § 12 PolG NRW bewirken. Warum es einer solchen Ausweitung bedürfen sollte, ist weiterhin weder aus dem Gesetzentwurf ersichtlich noch erscheint dies gerechtfertigt. Auch § 12 PolG NRW lässt bereits an Orten, von denen Tatsachen die Annahme rechtfertigen, dass dort Personen Straftaten von erheblicher Bedeutung verabreden, vorbereiten oder verüben, die Identitätsfeststellung und nach § 12 Abs. 2 PolG NRW auch weitere Maßnahmen zu. Hinzu kommen die Befugnisse aus den §§ 39 und 40 PolG NRW. Die zusätzliche Einfügung des § 12a d. E. birgt daher auch das Risiko der Doppelregelung gleichgelagerter Sachverhalte. Für die Betroffenen muss aber jederzeit klar erkennbar sein, auf welche Eingriffsbefugnis eine polizeiliche Maßnahme gestützt ist. Gerade die verschiedenen polizeilichen Spezialbefugnisse müssen eindeutig voneinander abgrenzbar und überprüfbar sein.

Sollte die vorgesehene Regelung trotz dieser massiven datenschutzrechtlichen Bedenken gleichwohl verabschiedet werden, ist sie in jedem Fall zeitlich zu befristen und sollte zudem unbedingt eine Evaluationspflicht enthalten.

Zu § 15a d. E.

Die geplante Erweiterung des Anwendungsbereiches der Videoüberwachung birgt das große Risiko einer nahezu uferlosen Ausweitung polizeilicher Videoüberwachung im öffentlichen Raum. Diese Maßnahme betrifft damit nachhaltig alle Menschen in Nordrhein-Westfalen. Dabei steht der Nachweis der Wirksamkeit polizeilicher Videoüberwachung zur Gefahrenabwehr nach wie vor aus.

Gegen die geplante Ausweitung der polizeilichen Videoüberwachung bestehen erhebliche datenschutzrechtliche Bedenken.

Zur Bedeutung von hoheitlichen Videoüberwachungsmaßnahmen in öffentlich zugänglichen Bereichen ist zunächst noch einmal Folgendes festzustellen:

Das Grundrecht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung verbürgt nach der Rechtsprechung des BVerfG das Recht des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, und daher grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen. Es gewährleistet dabei nicht allein den Schutz der Privat- und Intimsphäre, sondern trägt auch den informationellen Schutzinteressen des Einzelnen, der sich in die Öffentlichkeit begibt, Rechnung. Insoweit umfasst das Recht auf informationelle Selbstbestimmung auch das Recht des Einzelnen, sich insbesondere in der Öffentlichkeit frei und ungezwungen bewegen zu können, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung gemacht zu werden.

Personenbezogene Videoüberwachungsmaßnahmen in öffentlich zugänglichen Bereichen greifen in dieses Grundrecht ein. Zu den öffentlich zugänglichen Bereichen zählen beispielsweise Straßen, Wege, Fußgängerzonen, Plätze, Parks und Grünanlagen. Eine Videoüberwachung dieser Orte betrifft mithin einen erheblichen Teil des gesellschaftlichen Lebens. Solche Maßnahmen müssen daher stets in einem angemessenen Verhältnis zu den zu schützenden Belangen der betroffenen Bürgerinnen und Bürger stehen. Hierbei sind insbesondere folgende Gesichtspunkte von Bedeutung: Zum einen greifen Videoüberwachungsmaßnahmen in diesen Bereichen besonders intensiv in das Recht auf informationelle Selbstbestimmung ein, da sich Bürgerinnen und Bürger dort typischerweise länger aufhalten und diese Bereiche u.a. auch der Entfaltung sozialer Kommunikation dienen. Zudem ist zu berücksichtigen, dass verdachtslose Eingriffe mit großer Streubreite, bei denen zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem etwaigen Fehlverhalten Einzelner stehen, mit einer großen Eingriffsintensität verbunden sind. Daher würde eine großflächige Videoüberwachung öffentlich zugänglicher Bereiche unverhältnismäßig in das Recht auf informationelle Selbstbestimmung der davon betroffenen Bürgerinnen und Bürger eingreifen. Vielmehr ist eine hinreichend klare und begrenzte räumliche Beschränkung derartiger Maßnahmen gesetzlich zu regeln. Eine Beschränkung auf Kriminalitätsschwerpunkte – wie bisher – ist ein geeignetes Kriteri-

um, das einen angemessenen Ausgleich zwischen den Sicherheitsinteressen und dem Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger schafft.

Der Gesetzentwurf sieht dagegen in § 15a Abs. 1 Nr. 2 d. E. die Befugnis zu einer großflächigen, nahezu uferlosen Videoüberwachung vor; für eine polizeiliche Videoüberwachung öffentlich zugänglicher Bereiche zur Verhütung von Straftaten soll es nunmehr ausreichen, dass „tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dort Straftaten von erheblicher Bedeutung verabredet, vorbereitet oder begangen werden“. Es handelt sich also um eine Ausweitung in mehrfacher Hinsicht: Kombiniert mit dem Wegfall des Erfordernisses der konkret nachweisbaren Wiederholungsgefahr und der Darlegungspflicht, dass der Ort auch von seiner Beschaffenheit geeignet sein muss, Kriminalität zu begünstigen, wird der Anwendungsbereich neben der Begehung auch auf die Verabredung und Vorbereitung von Straftaten ausgeweitet. Damit gäbe es praktisch keinerlei sachliche und örtliche Beschränkung für den polizeilichen Einsatz von Videokameras mehr. Letztlich dürfte es keine öffentlich zugänglichen Bereiche geben, an denen die Begehung oder Verabredung von – ggf. auch erheblichen – Straftaten auszuschließen wäre. Dieser Effekt wird noch dadurch verstärkt, dass mit der Forderung nach lediglich tatsächlichen Anhaltspunkten, die eine entsprechende Annahme rechtfertigen müssen, die Anforderungen an die Erkenntnislage in der neuen Nummer 2 gegenüber der bisherigen Variante aus Nummer 1 viel geringer sind (zum Vergleich: Nummer 1 verlangt Tatsachen, die die Annahme rechtfertigen). Vergleichbar geringe Anforderungen an die Erkenntnislage gibt es hinsichtlich Eingriffsbefugnissen der Polizei an anderer Stelle im PolG NRW bisher nicht. Allein im Zusammenhang mit dem Kernbereichsschutz werden gleich geringe Voraussetzungen gestellt. Die Regelungen zum Kernbereichsschutz dienen, im Gegensatz zu den Eingriffsbefugnissen, jedoch gerade dazu, Eingriffe in die Grundrechte der betroffenen Person abzumildern. Solche Regelungen sollten daher nicht als Muster für die Ausgestaltung polizeilicher Eingriffsbefugnisse herangezogen werden.

Auch die Begründung untermauert die Besorgnis, dass die neue Befugnis hinsichtlich der in Frage kommenden Orte uferlos sein würde. Die dort genannten Beispiele belegen, dass es künftig möglich sein soll, auf dieser Grundlage komplette Innenstädte permanent per Videokameras zu überwachen. Die Vorbereitung der Delikte an den bekannten Örtlich-

keiten der Nummer 1 kann nämlich praktisch überall erfolgen und durch die jederzeitige Austauschbarkeit dieser Orte auch ständig wechseln. Um alle diese Orte jederzeit im Blick haben und im richtigen Moment die erhofften Erkenntnisse erzielen zu können, müsste die Polizei somit alle potentiellen Orte ständig überwachen. Danach verbliebe jedoch im Innenstadtbereich praktisch kein Raum mehr, in dem sich unbeteiligte Bürger und Bürgerinnen noch unbeobachtet aufhalten könnten.

Eine solch ausufernde und grenzenlose Videoüberwachung verkennt die eingangs dargelegten verfassungsmäßigen Anforderungen an einen zulässigen polizeilichen Einsatz von Videokameras.

Die weiterhin geltenden Mechanismen der Ausschilderung (Absatz 1 Satz 2), Befristung auf ein Jahr (Absatz 4) und Begrenzung der Speicherdauer auf grundsätzlich 14 Tage (Absatz 2) können die Zweifel an der Verhältnismäßigkeit der neuen Regelungen nicht ausräumen. Die Ausweitung der Videoüberwachung würde somit das Grundrecht auf informationelle Selbstbestimmung in unzulässiger Weise beschneiden.

Ergänzend sei angemerkt, dass die Frage, ob die Videobeobachtung ein geeignetes Mittel zur Wahrung oder Schaffung der Inneren Sicherheit ist, nach wie vor nicht abschließend beantwortet ist. Es ist offen, ob polizeiliche Videoüberwachung öffentlich zugänglicher Bereiche prinzipiell dazu geeignet ist, Straftaten zu vermeiden; dies bedürfte eingehender empirischer Untersuchungen. Belastbare Erkenntnisse, in welchem Umfang Videoüberwachung tatsächlich zur Gefahrenabwehr beiträgt, gibt es nach meinen Kenntnissen weiterhin nicht. In vielen Situationen werden sich potentielle Täter möglicherweise auch nicht durch eine Videoüberwachung von der Begehung von Straftaten abhalten lassen, beispielsweise aufgrund von Alkohol- oder Drogenkonsum sowie bei der Beschaffungskriminalität, oder sie versuchen, durch „Vermummung“ die Feststellung ihrer Identität zu verhindern. Oftmals dürfte der Einsatz von Videoüberwachungsmaßnahmen im Übrigen nur zu einer räumlichen Verlagerung der Kriminalität führen.

Aus diesem Grund ist es – gerade auch aus datenschutzrechtlicher Sicht – abzulehnen, dass die bisherige Befristung und Evaluierung durch die Aufhebung des Absatz 5 ersatzlos entfallen ist.

Die bisherige Regelung des § 15a PolG NRW stellt auch vor diesem Hintergrund insgesamt einen angemessenen Ausgleich zwischen den Sicherheitsinteressen und dem Recht auf informationelle Selbstbestimmung der Betroffenen dar. Die gegenwärtige Rechtslage bietet der Poli-

zei in datenschutzgerechter Weise einen ausreichenden Handlungsspielraum, Orte mit einem hohen Gefährdungspotenzial mittels Videokameras zu überwachen. Eine gesetzliche Regelung zur Ausweitung dieses Handlungsspielraums erscheint nicht erforderlich. Es sollte vielmehr die Effektivität der auf der Basis der bestehenden Befugnisnorm durchgeführten Maßnahmen untersucht werden.

Selbst wenn jedoch eine Ausweitung von Videoüberwachung nachweisbar erforderlich wäre, müsste diese auf jeden Fall maßvoll und verhältnismäßig erfolgen und insbesondere dem Grundrecht der Betroffenen auf informationelle Selbstbestimmung hinreichend Rechnung tragen. Das ist hier jedoch aus den oben dargelegten Gründen nicht der Fall. Eine polizeiliche Videoüberwachung ist vielmehr auch weiterhin auf enge, gesetzlich klar geregelte und abgrenzbare Einzelfälle zu beschränken.

Von der vorgesehenen Neuregelung ist deshalb unbedingt abzusehen.

Eine Befristung der Videoüberwachungsregelung ist auf jeden Fall weiterhin erforderlich. Sie gewährleistet, dass Wirksamkeit und Notwendigkeit der Befugnisnorm regelmäßig überprüft werden. Die Befassung des Landtags mit diesen Fragen stellt sicher, dass weiterhin eine kritische Auseinandersetzung unter Beteiligung der Öffentlichkeit sowie Sachverständiger aus Wissenschaft und Praxis erfolgt.

Zu § 20c d. E.

Die mit § 20c d. E. geregelte Möglichkeit der Telekommunikationsüberwachung (TKÜ) inklusive Quellen-TKÜ ist an den strengen Vorgaben des BVerfG bezüglich heimlicher Überwachungsmaßnahmen zu messen. Es bestehen Bedenken, ob diese hinreichend beachtet wurden. Außerdem birgt sie Risiken im Hinblick auf die IT-Sicherheit.

TKÜ und insbesondere die Quellen-TKÜ nach Absatz 2 sind schwere Eingriffe in Art. 10 Abs. 1 Grundgesetz (GG). Für solche Befugnisse zur heimlichen Datenerhebung, die tief in die Privatsphäre hineinwirken können, stellt der Grundsatz der Normenklarheit und Bestimmtheit be-

sonders strenge Anforderungen auf und ist insoweit mit den jeweiligen materiellen Anforderungen der Verhältnismäßigkeit eng verbunden.[5]

Dabei lässt Absatz 1 Nummer 1 d. E. TKÜ und Quellen-TKÜ auch zur Abwehr von Gefahren für Leib und Leben ohne jeglichen Terrorismus-Bezug zu. Das BVerfG hat jedoch im BKAG-Urteil selbst weniger schwerwiegende heimliche Eingriffsbefugnisse (Rn. 156) und die Quellen-TKÜ (Rn. 229) nur deshalb als verhältnismäßig und damit mit der Verfassung vereinbar angesehen, weil diese explizit zur Abwehr terroristischer Straftaten geschaffen wurden. Auch wenn das BVerfG offen gelassen hat, *„wo diesbezüglich die verfassungsrechtlichen Grenzen für solche Maßnahmen im Allgemeinen – etwa auch für entsprechende Befugnisse nach den Landespolizeigesetzen – liegen“*, stellt es doch heraus, dass Quellen-TKÜ nur zum *„Schutz von besonders gewichtigen Rechtsgütern vor besonders bedrohlichen Angriffen zulässig“* ist.[6] Vor diesem Hintergrund bestehen erhebliche Bedenken, ob der Einsatz von Quellen-TKÜ zur Abwehr von Gefahren für Leib und Leben ohne terroristischen Bezug diesen Verhältnismäßigkeitsanforderungen standhält.

Bezüglich Absatz 1 Nummer 2 verwundert, dass § 8 Abs. 5 d. E. zunächst teilweise wiederholt und dann doch auf dessen Nummern 1 – 3 verwiesen wird. Dabei bleibt unklar, welche Funktion § 8 Absatz 5 d. E. im Gefüge des neuen PolG NRW eigentlich einnehmen soll. Insoweit dürfte es an der verfassungsmäßig gebotenen Normenklarheit fehlen.

Zwar fordert Absatz 2 zu Recht, dass die Quellen-TKÜ sich ausschließlich auf Kommunikationsvorgänge beschränken muss, da es sich sonst um eine eingriffsintensivere Online-Durchsuchung handeln würde, die an noch engeren Verhältnismäßigkeitskriterien zu messen wäre. Jedoch halten Experten eine solche Beschränkung für technisch kaum möglich. Um die Rechtmäßigkeit des Einsatzes und die Verfassungskonformität des Programms zur Durchführung der Quellen-TKÜ überprüfen zu können, bedarf es u. a. der vollständigen Offenlegung des Quellcodes. Es sollten entsprechende Regelungen getroffen werden.

Des Weiteren sollte aufgenommen werden, dass die Ausleitung und Datenerhebung von visualisierten Darstellungen der Telekommunikation wie „application-shots“ unzulässig ist.

[5] Vgl. BVerfG, BKAG-Urteil, Rn. 94.
[6] a.a.O. Rn. 156.

In Absatz 3 sollte die Pflicht zum Schutz der kopierten Daten um die Anforderung *„nach dem Stand der Technik“* ergänzt werden.

Darüber hinaus ist zu besorgen, dass mit der Quellen-TKÜ das Interesse der Sicherheitsbehörden einhergehen könnte, Sicherheitslücken offen zu halten, um Systeme von Zielpersonen infiltrieren zu können. Dabei wäre es im Sinne der Cybersicherheit und des Schutzes aller Bürgerinnen und Bürger, diese Sicherheitslücken zeitnah an die zuständigen Behörden, die Betroffenen und Unternehmen zu melden, damit die Lücken baldmöglich geschlossen werden können. Durch die Schaffung neuer Rechtsgrundlagen für Quellen-TKÜ zur Strafverfolgung in der StPO, in den Verfassungsschutzgesetzen sowie in immer mehr Polizeigesetzen zur Gefahrenabwehr verschärft sich diese Problematik zusehends und potenzieren sich die Risiken sowohl für die Rechte der Bürgerinnen und Bürger als auch für die IT-Sicherheit.

Falls Absatz 7 – die Begründung führt hierzu nichts aus – sogar auch die Pflicht für Diensteanbieter enthalten soll, den Polizeibehörden bestehende Sicherheitslücken auch proaktiv mitzuteilen und diese nicht zu schließen oder Sicherheitslücken gar erst zu schaffen, stellt dies eine besondere Qualität der Gefährdung der IT-Sicherheit dar, deren Verhältnismäßigkeit im Hinblick auf die damit einhergehende massenhafte Gefährdung informationstechnischer Systeme unbeteiligter Personen durch Schaffung oder Offenhaltung von Sicherheitslücken höchst bedenklich erscheint.

Zu § 34c d. E.

Die elektronische Aufenthaltsüberwachung (EAÜ) stellt einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung dar. Sie sollte daher keinesfalls Anwendung im Zusammenhang mit den problematischen neuen Gefahrenbegriffen des § 8 Abs. 4 und 5 d. E. (s. hierzu o.) finden. Die geplanten Möglichkeiten der zweckändernden Verarbeitung von durch EAÜ erhobenen Daten entsprechen teilweise nicht den vom BVerfG aufgestellten Grundsätzen für Zweckänderungen.

Die EAÜ ist am Grundrecht auf informationelle Selbstbestimmung zu messen, da die elektronische Überwachung des Aufenthaltsorts Rück-

schlüsse auf die persönliche Lebensgestaltung zulässt. Daten, die über den Standort einer Person Auskunft geben, sind personenbezogene Informationen. Auch wenn die Datenerhebung im Rahmen der EAÜ nicht den heimlichen Überwachungsmaßnahmen zuzurechnen sein dürfte, ist die Eingriffstiefe der Maßnahme jedenfalls im Wesentlichen doch gleich zu bewerten. Dabei ist auch zu berücksichtigen, dass die Maßnahme eine lückenlose Nachverfolgung des jeweiligen Standorts der betroffenen Person, also die Erstellung eines vollständigen Bewegungsprofils, ermöglicht und erlaubt. Damit handelt es sich generell um eine besonders eingriffsintensive Maßnahme. Insbesondere vor dem Hintergrund, dass die Maßnahme wohl auch für Fälle der „drohenden“ oder jedenfalls der „drohenden terroristischen Gefahr“ zugelassen werden soll, mithin für Fälle, in denen der Maßnahmenzeitpunkt deutlich vor dem traditionellen Gefahrbegriff liegt, bestehen durchgreifende datenschutzrechtliche Bedenken hinsichtlich der Verfassungsmäßigkeit der geplanten Maßnahme. Auch für den Einsatz zu präventiv-polizeilichen Zwecken gilt, dass mit Blick auf die teils erheblichen Belastungen durch die EAÜ und den derzeitigen Forschungsstand zu ihrer Wirksamkeit die elektronische Aufenthaltsüberwachung weiterhin als Ultima Ratio verstanden werden sollte. Diese Aspekte finden sich im vorgelegten Gesetzentwurf nicht wieder.

Bezüglich des Verweises aus Absatz 1 auf § 8 Abs. 5 Nr. 1 bis 3 d. E. gelten die Ausführungen zu § 20c d. E. und § 8 Abs. 5 d. E. und die damit zum Ausdruck gebrachten Bedenken hinsichtlich der ausreichenden Normenklarheit entsprechend.

Absatz 3 Satz 9 regelt die Zwecke, für welche die aus der Aufenthaltsüberwachung erhobenen Daten genutzt werden dürfen. Die einzelnen Alternativen betreffen teils auch die Nutzung im Rahmen des ursprünglichen präventiven Erhebungszwecks. Soweit die Alternativen jedoch Zweckänderungen darstellen, richtet sich deren Zulässigkeit nach dem Kriterium der hypothetischen Datenneuerhebung. Voraussetzung für eine Zweckänderung ist danach, dass die neue Nutzung der Daten dem Schutz von Rechtsgütern eines solchen Gewichts dient, die verfassungsrechtlich die Neuerhebung dieser Daten mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnte. Wie oben bereits festgestellt ist die Eingriffstiefe der EAÜ mit der einer heimlichen Überwachung durchaus vergleichbar. Dies gilt vor allem vor dem Hintergrund, dass die Maßnahme jedenfalls auch für Fälle der *„drohenden terroristischen Gefahr“* zugelassen werden soll, mithin für Fälle, in denen der Maßnah-

menzeitpunkt deutlich vor dem traditionellen Gefahrbegriff liegt. Gleichzeitig ist zu berücksichtigen, dass das BVerfG die Straftaten nach ihrer Erheblichkeit einteilt in *„erhebliche Straftaten“*, *„schwere Straftaten“* und *„besonders schwere Straftaten“*.[7] Vor diesem Hintergrund erscheint zumindest die Möglichkeit der Nummer 1, wonach die nach § 34c d. E. erhobenen Daten ohne weitere Abwägung bereits zur Verfolgung von Straftaten von lediglich erheblicher Bedeutung verwendet werden können, als mit den Maßgaben der Zweckänderung nicht vereinbar. An dieser Einschätzung vermag auch die in der Begründung zu § 34c d. E. (vgl. S. 42 d. E.) getroffene pauschale Feststellung, alle in Absatz 2 Satz 9 genannten Zwecke dienten *„überragenden Gemeinwohlinteressen“*, nichts zu ändern.

Bei Absatz 3 Satz 9 Nummer 2 Alternative 2 bestehen bereits Zweifel an der Geeignetheit der zweckändernden Verwendung zur Erreichung des genannten Ziels. Inwieweit eine elektronische Überwachung ermöglichen soll festzustellen, ob die betroffene Person mit einer anderen Person in einen verbotenen Kontakt tritt, ist nicht nachvollziehbar. Regelmäßig dürften sich aus einer rein ortsbezogenen Überwachung keinerlei Erkenntnisse darüber gewinnen lassen, mit wem sich die überwachte Person trifft oder sonst Kontakt aufnimmt, sei es fernmündlich oder auf elektronischem Wege.

In Absatz 3 sollte im letzten Satz die Pflicht zum Schutz der Daten um die Anforderung *„nach dem Stand der Technik“* ergänzt werden.

Mit freundlichen Grüßen

Helga Block

Helga Block

[7] Zuletzt BKAG-Urteil, Rn. 107.