Baden-Württemberg
DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT

LfDI Baden-Württemberg · Postfach 10 29 32 · 70025 Stuttgart

Innenministerium
Baden-Württemberg

Datum 7. August 2017
Name Herr Broo
Durchwahl 0711/615541-39
Aktenzeichen H 1100/38
(Bitte bei Antwort angeben)

Gesetz zur Änderung des Polizeigesetzes und des Gesetzes über die Ladenöffnung in Baden-Württemberg
Ihr Schreiben vom 27. Juni 2017, Az.: 3-1101.2/268

Sehr geehrte Damen und Herren,

für die Übersendung des Gesetzentwurfs danken wir. Wir nehmen dazu wie folgt Stellung:

Der Entwurf der Landesregierung verfolgt ein klares Ziel: Die Sicherheitsbehörden bis an die Grenze des verfassungsrechtlich Zulässigen mit neuen Instrumentarien auszustatten. Wo diese Grenze aus Sicht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) verläuft, zeigt die nachfolgende fachliche Stellungnahme detailliert auf.

Ob dieses Ziel erreicht wird - und ob es überhaupt verfolgt werden sollte - wird Gegenstand der parlamentarischen Diskussion sein. Der LfDI wird hierzu zwei Aussagen treffen:

Wer an die Grenze des verfassungsrechtlich Zulässigen geht, provoziert zwei Konsequenzen: Er überantwortet die Letztentscheidung zu sicherheitspolitischen Fragen dem Verfassungsgericht und er läuft Gefahr, Anlass und Zweck der Sicherheitsnovelle aus den Augen zu verlieren. Ob die neu eingeführten bzw. verschärften Sicher-

heitsinstrumente überhaupt auf die bereits beobachteten oder zu erwartenden terroristischen Gefahren in unserem Land abgestimmt und damit erfolgversprechend sind, ist aus Sicht des LfDI nicht zu erkennen.

Zudem hat keines der neuen Sicherheitsinstrumentarien bislang seine Wirksamkeit unter Beweis gestellt. Dass sie zu einer Verbesserung der Sicherheitslage führen werden, ist daher lediglich eine mehr oder weniger plausible Vermutung. Umso wichtiger ist es, den praktischen Einsatz und die tatsächlichen Effekte dieser Instrumentarien zu beobachten und noch in dieser Legislaturperiode zu evaluieren. Neben die parlamentarische Evaluierung muss auch eine gerichtliche treten. Damit sind nicht nur die Verfassungsgerichte, sondern auch die Fachgerichte angesprochen. Diese können aber nur dann korrigierend eingreifen, wenn Betroffene sie auch zum Zweck der Kontrolle anrufen können. Dies setzt wiederum voraus, dass die geplanten heimlichen Sicherheitsmaßnahmen von unverzüglichen und umfassenden Benachrichtigungen aller Betroffenen begleitet werden.

Allgemein

Schon im Rahmen der Beteiligung an anderen Gesetzgebungsvorhaben hatten wir darauf hingewiesen, dass sich die Grenzen für gesetzgeberische Eingriffe in das Recht auf informationelle Selbstbestimmung unmittelbar aus der Verfassung ergeben. Die Ausgestaltung von Eingriffsbefugnissen muss dabei vor allem dem Grundsatz der Verhältnismäßigkeit genügen. Eingriffsbefugnisse sind zudem am rechtsstaatlichen Gebot der Normenbestimmtheit und -klarheit zu messen.

Der Gesetzentwurf übernimmt – neben einer originären Regelung zur „intelligenten“ Videoüberwachung – einzelne Instrumente sowohl des Bundeskriminalamtgesetzes (BKAG) vom 7. Juli 1997 als auch des ab dem 25. Mai 2018 geltenden Bundeskriminalamtgesetzes vom 1. Juni 2017. Die entsprechenden Bestimmungen des derzeit geltenden Bundeskriminalamtgesetzes waren Gegenstand einer Verfassungsklage, über die das Bundesverfassungsgericht mit Urteil vom 20. April 2016 (1 BvR 966/09, 1 BvR 1140/09 –, juris) entschieden hat (nachfolgend: BKAG-Urteil). Zwar hält das Gericht Maßnahmen, wie etwa die Telekommunikationsüberwachung einschließlich der sog. Quellen-Telekommunikationsüberwachung, nicht grundsätzlich als mit der Verfassung nicht vereinbar. Vielfach stellte es jedoch fest, dass die konkrete Ausgestaltung dieser Befugnisse verfassungswidrig, verfassungsrechtlich bedenklich oder nur bei verfassungskonformer Auslegung nicht zu beanstanden sei. Durch das Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes (BGBl. I S. 1354) hat der

Bundesgesetzgeber u.a. hierauf reagiert und den Versuch unternommen, Verfassungskonformität herzustellen.

Von zentraler Bedeutung für die Frage der Verfassungsmäßigkeit heimlicher Überwachungsmaßnahmen der Polizei ist die Beschränkung dieser Maßnahmen auf die Abwehr von Gefahren des internationalen Terrorismus. Denn nur Schutzgüter von hohem verfassungsrechtlichem Gewicht können solche tief in die Privatsphäre eingreifenden Ermittlungs- und Überwachungsbefugnisse überhaupt rechtfertigen. Der Begriff des internationalen Terrorismus „ist dabei durch die Aufgabenbeschreibung des § 4a Abs. 1 BKAG **und dessen Verweis auf § 129a Abs. 1, 2 StGB** *[Hervorhebung durch Uz.]* in enger Anlehnung an den EU-Rahmenbeschluss vom 13. Juni 2002 und die internationale Begrifflichkeit … definiert“.[1] § 5 Absatz 1 Satz 2 des neuen Bundeskriminalamtgesetzes enthält nunmehr eine entsprechende ausdrückliche Definition dieses Begriffs. Sämtlichen heimlichen Ermittlungs- und Überwachungsbefugnisse des Bundeskriminalamtgesetzes, die das Bundesverfassungsgericht in seinem BKAG-Urteil als dem Grunde nach noch verfassungsgemäß akzeptiert hat, liegt die **gesetzliche** Beschränkung auf die Terrorismusabwehr zugrunde: „Die Eingriffsbefugnisse sind dabei gemäß § 20g Abs. 1 Nr. 1 BKAG darüber hinaus weiter dadurch eingeschränkt, dass Maßnahmen zum Schutz der genannten Rechtsgüter [Anm.: Leib, Leben oder Freiheit einer Person] nur erlaubt sind, wenn diese durch eine der in § 4a Abs. 1 Satz 2 BKAG genannten Straftaten bedroht sind. Dies ergibt sich schon aus der Aufgabennorm des § 4a BKAG selbst, in die die Befugnisse der §§ 20a ff. BKAG eingebunden sind. **Die Eingriffsbefugnisse werden so auf die Abwehr von Gefahren des internationalen Terrorismus begrenzt.** *[Hervorhebung durch Uz.]* … Ungeachtet der Frage, wo diesbezüglich die verfassungsrechtlichen Grenzen für solche Maßnahmen im Allgemeinen - etwa auch für entsprechende Befugnisse nach den Landespolizeigesetzen - liegen, **wird damit jedenfalls vorliegend den Verhältnismäßigkeitsanforderungen genügt**.“[2] *[Hervorhebung durch Uz.]*

Zwar ist ausdrückliche Zielsetzung auch des vorliegenden Gesetzentwurfs die Abwehr von Straftaten mit terroristischem Hintergrund. Eine diesbezügliche gesetzliche Beschränkung entsprechend § 4a BKAG (bzw. § 5 Absatz 1 Satz 2 BKAG neu) erfolgt jedoch weder bei § 23b noch bei § 27c des Entwurfs – im Gegensatz zu § 27b. Näheres hierzu nachfolgend.

[1] BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09, 1 BvR 1140/09 –, juris, Rn 96
[2] Fn 1, Rn 156

Auch der **Bestimmtheitsgrundsatz** stellt an Befugnisse zur heimlichen Datenerhebung und -verarbeitung, die tief in die Privatsphäre hineinwirken können, besonders strenge Anforderungen. Dabei gilt es, vor allem zwei Aspekt zu berücksichtigen: Zum einen muss die von heimlichen Überwachungsmaßnahmen betroffene Person erkennen können, bei welchen Anlässen und unter welchen Voraussetzungen ein Verhalten mit dem Risiko der Überwachung verbunden ist. Zum anderen muss das Gesetz der gesetzesausführenden Verwaltung für ihr Verhalten hinreichend klare steuernde und begrenzende Handlungsmaßstäbe vorgeben, indem sich die tatbestandlichen Voraussetzungen der geregelten Maßnahmen dem Gesetz hinreichend deutlich entnehmen lassen: „Die Entscheidung über die Grenzen der Freiheit des Bürgers darf nicht einseitig in das Ermessen der Verwaltung gestellt sein (…). Dem Gesetz kommt im Hinblick auf den Handlungsspielraum der Exekutive eine begrenzende Funktion zu, die rechtmäßiges Handeln des Staates sichern und dadurch auch die Freiheit der Bürger vor staatlichem Missbrauch schützen soll.“[3] Zwar ist es dem Gesetzgeber „nicht grundsätzlich verwehrt, zur Umschreibung des Anlasses und der weiteren Voraussetzungen der Straftatenverhütung unbestimmte Rechtsbegriffe zu benutzen. Die Auslegungsbedürftigkeit als solche steht dem Bestimmtheitserfordernis nicht entgegen, solange die Auslegung unter Nutzung der juristischen Methodik zu bewältigen ist (…) und die im konkreten Anwendungsfall verbleibenden Ungewissheiten nicht so weit gehen, dass Vorhersehbarkeit und Justitiabilität des Verwaltungshandelns gefährdet sind“.[4] Hinter diesen Anforderungen bleibt der Entwurf vielfach zurück. Im Einzelnen hierzu nachfolgend.

Eng verbunden mit dem Erfordernis der hinreichenden Bestimmtheit von Eingriffsregelungen und damit der Vorhersehbarkeit und Justitiabilität der Eingriffe ist die Frage der Wehrfähigkeit von Grundrechtseingriffen. Gerade bei heimlichen Eingriffen fehlt es an einer hinreichenden Möglichkeit des Betroffenen, das grundrechtsverkürzende Verwaltungshandeln zu rügen, einer Selbstkontrolle der Verwaltung und ggf. der Fremdkontrolle durch die Gerichte zuzuführen. Dies wiegt umso schwerer, als das Verwaltungshandeln mangels hinreichend bestimmter gesetzlicher Direktiven bereits in besonderer Weise der externen Kontrolle bedarf. Leider geht der Gesetzentwurf hier über das verfassungsrechtlich gebotene absolute Minimum nicht hinaus. So wäre es insbesondere angezeigt, die Benachrichtigungspflichten zugunsten der Betroffenen effektiver auszugestalten und dafür Sorge zu tragen, dass die in der Praxis zu beobachtende Verkehrung von regelmäßig nachträglicher Information des Betroffenen und nur ausnahmsweise unterbleibender Benachrichtigung wieder näher an

[3] BVerfG, Beschluss vom 3. März 2004 – 1 BvF 3/92 –, juris, Rn 104, 105
[4] Fn 3, Rn 111

das verfassungsrechtlich Gebotene heranrückt. Dies lässt sich nur durch eine schärfere Eingrenzung der Ausnahmetatbestände und eine strenge Evaluation der Benachrichtigungspraxis auf Basis gesetzlich vorgegebener Dokumentationspflichten erreichen. Dies versäumt der Gesetzentwurf in einer mit dem Rechtsstaatsprinzip nicht mehr zu vereinbarenden Weise.

Zu den einzelnen Änderungen

Zu Artikel 1 Nummer 6 (§ 21 PolG)

Zutreffend weist die Begründung darauf hin, dass die automatische Auswertung einen zusätzlichen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen darstellt. Widersprüchlich ist es jedoch, wenn im Weiteren einerseits eine höhere Eingriffsintensität verneint, andererseits aber eine Eingriffserhöhung aufgrund der quantitativen Steigerung der Datenverarbeitungsmöglichkeiten „nicht verkannt“ wird. Auch ist die Aussage, die automatisierte Auswertung von Verhaltensmustern, wie etwa Bewegungsabläufen oder Gruppenbildung, erfolge nicht anhand personenbezogener Merkmale, schlichtweg nicht nachvollziehbar. Zu den „persönlichen und sachlichen Verhältnissen“ einer Person (§ 3 Absatz 1 des Landesdatenschutzgesetzes - LDSG) gehören auch Verhaltensweisen der Person.[5] Gerade das Erkennen solcher („auffälligen“) Verhaltensmuster ist das Ziel der „intelligenten“ Videoüberwachung.

Nach unserer Auffassung wirkt die Software gestützte Auswertung der Videoaufnahmen anhand zuvor festgelegter Algorithmen tatsächlich eingriffsintensivierend. In seiner Entscheidung zur polizeilichen Rasterfahndung stellt das Bundesverfassungsgericht fest: „Als Fahndungsmethode weist die Rasterfahndung die Vorteile auf, die automatisierte, rechnergestützte Operationen generell mit sich bringen, ermöglicht also die Verarbeitung nahezu beliebig großer und komplexer Informationsbestände in großer Schnelligkeit. Ein herkömmliches Verfahren, die nach dem Modell abgestufter Erkenntnisverdichtung erfolgende Ermittlungstätigkeit, wird hierdurch mit einer bislang unbekannten Durchschlagskraft versehen …. In grundrechtlicher Hinsicht führt die neue Qualität der polizeilichen Ermittlungsmaßnahme zu einer erhöhten Eingriffsintensität.“[6] Inhaltlich lässt sich dies zwanglos auf die „intelligente“ im Unterschied zur „einfachen“ Videoüberwachung übertragen. Von einer erhöhten Grundrechtsrelevanz ist daher auszugehen.

[5] Dammann, in: Simitis (Hrsg.), BDSG, 8. Auflage 2014, § 3 Rn 10
[6] Beschluss vom 4. April 2006 – 1 BvR 518/02 –, juris, Rn 122

Gegen die Angemessenheit der Regelung haben wir unter dem Vorbehalt, dass der Einsatz solcher Systeme auf die räumlichen und inhaltlichen Voraussetzungen, wie sie im Gesetzentwurf angelegt sind, beschränkt bleibt, letztlich keine durchgreifenden Bedenken. Insofern ist die Verwendung des Wortes „zunächst“ im ersten Absatz dritter Satz der Begründung irritierend und sollte gestrichen werden. Jedenfalls würde sich die Frage der Verhältnismäßigkeit im engeren Sinne erneut und verschärft stellen, wenn die Maßnahmen auf weitere Bereiche ausgedehnt werden sollten.

Allerdings bedarf es aus unserer Sicht eines Ausgleichs, um die mit der Maßnahme verbundenen erhöhten Risiken auszugleichen. Soll künftig die Videoüberwachung in der „intelligenten“ Form erfolgen, bedarf es der herkömmlichen „Vollüberwachung“ der betreffenden Örtlichkeiten nicht mehr. Ausdrücklicher polizeilicher Mehrwert der automatisierten Auswertung ist es ja gerade, Polizeivollzugsbeamte von der Pflicht zur kontinuierlichen Überwachung der Monitore zu entbinden. Nur noch dann, wenn das System einen „Alarmfall“ herausgefiltert hat, soll geprüft werden, ob tatsächlich Straftaten drohen und weitere präventive Maßnahmen nötig werden, etwa indem Einsatzbeamte vor Ort geschickt werden. Damit entfallen aber auch die Notwendigkeit einer Dauerübertragung der Videoaufnahmen sowie deren vollständige Speicherung. Es reicht aus, nur die Geschehensabläufe zu übertragen und aufzuzeichnen, die von dem System als polizeilich relevant erkannt werden. Ein solcher grundrechtsschonender Einsatz von Videotechnik verringert - in der Terminologie des Bundesverfassungsgerichts - „Verdachtslosigkeit“, „Massenhaftigkeit“ und „Streubreite“ der Maßnahme und so deren Eingriffsintensität. In Betracht käme im Übrigen neben der örtlichen auch eine zeitliche Eingrenzung der Videoüberwachung gemäß polizeilicher Prognose. Gegen einen in der Erprobungs- und Übergangsphase parallelen Betrieb der herkömmlichen und der intelligenten Videoüberwachung hätten wir allerdings keine durchgreifenden Bedenken, wohl aber gegen einen dauerhaften Parallelbetrieb.

Bezüglich des Wortlauts von § 21 Absatz 4 Satz 2 haben wir Bedenken, ob dem Bestimmtheitsgrundsatz ausreichend Rechnung getragen ist. Wenn als Eingriffsvoraussetzung auf „Verhaltensmuster“ (die Begründung spricht von „typischen“ oder „auffälligen“ Verhaltensmustern) abgestellt wird, „die auf die Begehung von Straftaten hindeuten“, fehlen unseres Erachtens die von der Rechtsprechung geforderten begrenzenden Elemente (siehe oben). Insbesondere der von der Videoüberwachung betroffene Bürger kann sich nicht sicher sein, welche seiner Verhaltensweisen vom Algorithmus möglicherweise als polizeilich relevantes Verhalten (fehl)gedeutet wird.

Schnelles Laufen, etwa an einer Haltestelle, freundschaftliches Schulterklopfen, das Unterhaken des Ehepartners oder harmlose Raufereien Jugendlicher können schnell dazu führen, dass Betroffene sich polizeilichen Maßnahmen ausgesetzt sehen. „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. … Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“[7] Diese Aussagen im Volkszählungsurteil gelten hier in besonderem Maße. Wir regen deshalb an, § 21 Absatz 4 Satz 2 konkreter zu fassen, etwa folgendermaßen: „Die automatische Auswertung darf nur auf das Erkennen solcher Verhaltensmuster ausgerichtet sein, welche die konkrete Wahrscheinlichkeit begründen, dass es in absehbarer Zeit zu einer Straftat kommt.“

Darüber hinaus sollte je nach Entwicklungsstand der eingesetzten Algorithmen für jedermann erkennbar publik gemacht werden, welche Verhaltensweisen es sind, die als relevant eingestuft werden. Dies kann durch entsprechende Hinweise und Piktogramme am Einsatzort, aber auch durch transparente Erklärungen etwa auf Webseiten der Polizei geschehen.

Da mit dem Einsatz intelligenter Videoüberwachungssysteme (datenschutz-)rechtlich und technisch Neuland betreten wird, begrüßen wir es, wenn wir in die fachliche Entwicklung einbezogen werden. Für unabdingbar halten wir es, den Prozess wissenschaftlich zu begleiten. Eine entsprechende Evaluierungsklausel sollte deshalb in den Gesetzentwurf aufgenommen werden.

Zu Artikel 1 Nummer 7 (§ 23b PolG)

Der Wortlaut des § 23b Absatz 1 Satz 1 Nummer 1 beschränkt die Telekommunikationsüberwachung nicht auf die Abwehr der Gefahren des internationalen Terrorismus. Dazu fehlen, im Unterschied zu § 27b Absatz 1 Satz 1, die hierfür erforderlichen begrenzenden Elemente (Verweis auf die in § 129a StGB konkret definierten, schwerwiegenden Straftaten[8]). Ohne diese wäre nach dem Gesetzeswortlaut eine Telekommunikationsüberwachung auch in Fällen der Allgemeinkriminalität, beispielsweise einer Körperverletzung, zulässig. Dies entspricht zum einen nicht der Zielsetzung

[7] BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83 - u.a.; juris, Rn 148
[8] BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07 –, juris, Rn 106

des Gesetzes und verstößt nach unserer Auffassung insoweit gegen klar den Verhältnismäßigkeitsgrundsatz.

Dieser Mangel setzt sich in verstärktem Maß in den weiteren in § 23b Absatz 1 Satz 1 geregelten Fällen fort. § 23b Absatz 1 Satz 1 Nummer 2 und 3 weicht von dem „tradierten sicherheitsrechtlichen Modell der Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren“ ab.[9] Die Einschreitschwellen werden deutlich ins Vorfeld konkreter Gefahrenlagen verschoben. Das Bundesverfassungsgericht hat eine solche Erweiterung ausdrücklich nur in Bezug auf terroristische Straftaten akzeptiert.[10] Zwar werden in § 23b Absatz 1 Satz 1 Nummer 2 und 3 Buchstaben a bis c die Eingriffsvoraussetzungen jeweils enger gefasst als in § 23b Absatz 1 Satz 1 Nummer 1. Jedoch werden dabei nur Teilaspekte dessen, was für Terrorismusstraftaten kennzeichnend ist, übernommen. Es fehlt an einer weiteren wesentlichen Begrenzung. Denn der Terrorismusbegriff setzt (kumulativ) voraus, dass es um Straftaten geht, welche die in § 129a Absatz 1 und 2 des Strafgesetzbuches genannten Straftatbestände erfüllen (siehe oben) Die jeweilige Bezugnahme auf § 23b Absatz 1 Satz 1 Nummer 1 ist von daher zu weitgehend. Auch unter diesem (weiteren) Gesichtspunkt erscheinen die Regelungen verfassungsrechtlich nicht haltbar.

Bei der Bestimmung der Einschreitschwellen übernimmt der Gesetzentwurf in § 23b Absatz 1 Satz 1 Nummer 2 und 3 größtenteils wörtlich die für eine hinreichende Bestimmtheit erforderlichen „Anforderungen“ des Bundesverfassungsgerichts.[11] Zweifel bestehen, ob damit dem Bestimmtheitsgrundsatz tatsächlich Rechnung getragen wird. Wonach bestimmt sich ein „übersehbarer Zeitraum“? Wann ist die Begehungsweise einer künftigen Straftat „ihrer Art nach konkretisiert“? Welches „individuelle Verhalten“ begründet die konkrete Wahrscheinlichkeit künftiger terroristischer Straftaten? Ob eine Auslegung dieser unbestimmten Begriffe „unter Nutzung der juristischen Methodik“ noch zu bewältigen ist und einerseits der Polizei damit ein unter rechtsstaatlichen Gesichtspunkten hinreichend erkennbarer Handlungsrahmen vorgegeben wird, andererseits für den Bürger Klarheit besteht, wann sein Verhalten das Risiko einer heimlichen Überwachung begründet, ist mehr als fraglich.[12] Diese Bedenken gelten auch hinsichtlich aller weiteren Vorschriften des Gesetzentwurfs, die den Kreis der Betroffenen gleichlautend bestimmen.

---

[9] FN 1, Rn 112
[10] Fn 1, Rn 164 a.E. „in Bezug auf terroristische Straftaten kann der Gesetzgeber stattdessen aber auch“
[11] Fn 1, Rn 165
[12] insoweit auch: Stellungnahme Nr. 33/2017 vom 12.04.2017 des DAV zum Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes

Die Bedenken hinsichtlich der „regulären“ Telekommunikationsüberwachung gelten erst recht für die Quellen-Telekommunikationsüberwachung gemäß § 23b Absatz 2 des Entwurfs.

In § 23b Absatz 9 Satz 6 sollte das Wort „verwendet“ durch die Wörter „zur Kenntnis genommen, genutzt oder übermittelt“ ersetzt werden.

Nach § 23 Absatz 10 Satz 3 ist die Zurückstellung der Benachrichtigung zu dokumentieren. Klarstellend sollten hier die Wörter „mit Gründen“ eingefügt werden („Die Zurückstellung ist **mit Gründen** zu dokumentieren.“; vgl. insoweit auch § 101 Absatz 5 Satz 2 StPO).

§ 23b Absatz 12 Satz 3 sieht eine aufschiebend bedingte Weiterverarbeitungs- und Übermittlungssperre vor. Damit wird Bezug genommen auf die Fallgestaltungen des § 85. Angeregt wird folgende Fassung: „Personenbezogene Daten, die nicht entsprechend den Anforderungen des Satzes 1 gekennzeichnet sind, dürfen solange nicht gemäß § 85 weiter verarbeitet werden, bis eine Kennzeichnung entsprechend den Anforderungen des Satzes 1 erfolgt ist.“ Auf die Ausführungen zu § 85 wird verwiesen.

Um die Tatsachengrundlage für die Feststellung zu verbessern, ob und gegebenenfalls inwieweit die mit den intensiven Eingriffen jeweils verfolgten Ziele erreicht wurden, halten wir eine zeitnahe Ergebnisdokumentation für geboten. Gesetzestechnisch kann dem etwa dadurch Rechnung getragen werden, dass in Absatz 14 nach dem Wort „Landtag“ die Wörter „auf der Grundlage jeweils zeitnah dokumentierter Ergebnisberichte der verantwortlichen Polizeidienststelle“ eingefügt werden.

Zu Artikel 1 Nummer 8 (§§ 27b und 27c)

Zu § 27c

Im Unterschied zu § 23b umschreibt § 27b Absatz 1 bis zu dem Wort „wenn“ zutreffend den Begriff der Gefahren des internationalen Terrorismus. Die Beschränkung auf diesen Schutzzweck kann eine solche Maßnahme grundsätzlich rechtfertigen. Soweit § 27c in seinen Eingriffsvoraussetzungen auf § 27b Absatz 1 verweist, bestehen die zu § 23b geltend gemachten Bedenken insoweit hier nicht. Bedenken bestehen jedoch auch hinsichtlich der Bestimmtheit der Regelung, soweit es um den be-

troffenen Personenkreis bzw. der Einschreitschwelle geht; auf die entsprechenden Ausführungen zu § 23b wird verwiesen.

Nach Absatz 2 Satz 2 ist folgender Satz einzufügen: „Ist es der betroffenen Person untersagt, sich ohne Erlaubnis der zuständigen Polizeidienststelle von ihrem Wohn- oder Aufenthaltsort oder aus einem bestimmten Bereich zu entfernen (§ 27b Absatz 1), gilt Satz 2 für den Bereich, in dem sie sich befugt aufhalten darf, entsprechend.“ In Satz 10 sind nach dem Wort „Person“ die Wörter „oder innerhalb Bereichs, in dem sie sich nach § 27b Absatz 1 befugt aufhalten darf“ einzufügen. Aus Gründen der Verhältnismäßigkeit bedarf es für die genannten Bereiche derselben Beschränkungen der Überwachung wie für die Wohnung. Auch die erste Variante der nach § 27b Absatz 1 zulässigen Aufenthaltsvorgaben bezweckt, den Aufenthalt an Orten zu verhindern, an denen sich das Risiko der Verwirklichung der zu verhütenden Straftaten erhöht. Mit der Untersagung, sich aus einem definierten Bereich zu entfernen, wird zum Ausdruck gebracht, dass das Risiko, dass es innerhalb dieses Bereichs zu der befürchteten Straftat kommt, gering ist. Dies rechtfertigt es allenfalls, mittels einer elektronischen Fußfessel zu kontrollieren, ob sich die betroffene Person in diesem Bereich aufhält oder ihn verlässt. Für die Erhebung darüber hinausgehende Aufenthaltsdaten gibt es keine Notwendigkeit. Hier überwiegen die schutzwürdigen Interessen der betroffenen Person.

Absatz 2 Satz 3 regelt die Zwecke, für welche die aus der Aufenthaltsüberwachung erhobenen Daten genutzt werden dürfen. Die einzelnen Alternativen betreffen teils die Nutzung im Rahmen des ursprünglichen präventiven Erhebungszwecks, teils aber auch Zweckänderungen.

Die Zweckbestimmung der Datenerhebung ist klar präventiv formuliert: Nach Absatz 1 letzter Halbsatz sollen Überwachung und Datenverwendung dazu dienen, von der Begehung terroristischer Straftaten abzuhalten. Wenn **Absatz 2 Satz 3 Nummer 1 2. Alternative sowie Nummer 3** zu einer Datennutzung „zur Strafverfolgung“ berechtigt, stellt dies zum einen ein völlig anderen Zweck dar als derjenige, welcher der Datenerhebung zugrunde liegt. Zum anderen bestehen Bedenken, ob eine Datenverwendungsregelung zu rein repressiven Zwecken der Strafverfolgung noch von der Gesetzgebungskompetenz des Landes gedeckt ist. **Absatz 2 Satz 3 Nummer 4** stellt dagegen eine Zweckänderungsvorschrift dar, die jedenfalls in die Gesetzgebungszuständigkeit des Landes fällt. Auch wenn die Datenerhebung im Rahmen der „elektronischen Fußfessel“ nicht den heimlichen Überwachungsmaßnahmen zuzurechnen sein dürfte, die Gegenstand des BKAG-Urteils waren, so ist die Eingriffstiefe der

Maßnahme jedenfalls im Wesentlichen gleich zu bewerten. Dies hat zur Folge, dass für auch für Zweckänderungen in diesem Bereich das Kriterium der hypothetischen Datenneuerhebung gelten muss. Voraussetzung für eine Zweckänderung wäre danach, dass die neue Nutzung der Daten dem Schutz von Rechtsgütern eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Vor diesem Hintergrund erscheint Nummer 4 zu weit gefasst.

Absatz 2 Satz 3 Nummer 2 1. Alternative und Nummer 5 dürften als weitere Nutzung im Rahmen des ursprünglichen Zwecks zulässig sein. Bei Absatz 2 Satz 3 Nummer 2 2. Alternative bestehen indes Zweifel an der Geeignetheit. Inwieweit eine elektronische Überwachung ermöglichen soll festzustellen, ob die betroffene Person mit einer anderen Person in einen verbotenen Kontakt tritt, ist nicht nachvollziehbar. Denkbar wäre dies allenfalls dann, wenn die andere Person ebenfalls elektronisch überwacht wird. In allen anderen Fällen lassen sich allein aus einer rein ortsbezogene Überwachung keinerlei Erkenntnisse darüber gewinnen, mit wem sich die betroffene Person trifft oder mit wem sie sonst Kontakt aufnimmt, etwa fernmündlich oder über soziale Netzwerke.

Bei Absatz 3 Satz 1 ist zweifelhaft, ob der Landesgesetzgeber die Polizeien des Bundes und der anderen Bundesländer zur Datenübermittlung verpflichten oder diesen jedenfalls eine Übermittlungsbefugnis einräumen kann.

Auch die in Absatz 4 geregelten Datenübermittlungsbefugnisse müssen den Anforderungen in Bezug auf das Kriterium der hypothetischen Datenneuerhebung genügen.[13] Auf die Ausführungen zu Absatz 2 Satz 3 wird insoweit verwiesen. Auch im Übrigen gelten die hinsichtlich Absatz 3 im Einzelnen vorgebrachten Bedenken für die Übermittlungsbefugnisse entsprechend.

Zu Artikel 1 Nummer 12 (§§ 84 b und 85 PolG neu)

Zu § 85

Wenn in Absatz 1 das Wort „Verarbeitung“ verwendet wird, werden nach der Terminologie des Landesdatenschutzgesetzes (LDSG) sämtliche Verarbeitungsschritte gemäß § 3 Absatz 2 LDSG umfasst. An dieser Stelle ist dies zwar vertretbar, da die

[13] Fn 1, Rn 307

Absätze 2 bis 5, auf die verwiesen wird, jeweils unterschiedliche Verarbeitungsschritte betreffen. In den nachfolgenden Absätzen sollten diese Verarbeitungsschritte allerdings eindeutiger gefasst werden. So betreffen – in Anlehnung an das BKAG-Urteil - Absatz 2 die Fälle, in denen es um die weitere Nutzung im Rahmen der **ursprünglichen** Zwecke[14], und Absatz 3 die Fälle, in denen es um weitere Nutzung für **andere** als die ursprünglichen Zwecke (Zweckänderung)[15] geht. In Absatz 2 Satz 1 und in Absatz 3 Satz 1 sollte deshalb das Wort „weiterverarbeiten“ jeweils durch die Wörter „weiter nutzen“ ersetzt werden. Damit wäre auch klargestellt, dass die vom Verarbeitungsbegriff mit umfasste Datenübermittlung, die in Absatz 4 geregelt wird, an dieser Stelle nicht gemeint ist.

An dieser Stelle wird nochmals darauf hingewiesen, dass dem § 23b die „gesetzlich näher bestimmte Dimension“ fehlt.[16] Dieser Mangel, der die Verhältnismäßigkeit der nach Maßgabe dieser Vorschriften erfolgenden Datenerhebung grundsätzlich in Frage stellt, strahlt auch auf die Regelung über die weitere Verarbeitung dieser Daten aus. Nur unter diesem Vorbehalt sind die nachfolgenden Ausführungen zu verstehen.

Absatz 3 regelt die neue Nutzung von Daten, die im Rahmen eines konkreten Ermittlungsverfahrens durch eine konkrete Polizeidienststelle erhoben wurden, zu einem anderen als dem Zweck, zu dem sie ursprünglich erhoben wurden (Zweckänderung). Eine solche Zweckänderung kann sich immer nur auf die Daten beziehen, welche die Polizeidienststelle selbst erhoben hat. Die weitere Nutzung als konkreter Ermittlungsansatz durch eine andere Polizeidienststelle würde eine vorherige Übermittlung dieser Daten an die andere Dienststelle voraussetzen. Durch das Wort „Polizeivollzugsdienst“, der sämtliche in § 70 Absatz 1 PolG genannten Dienststellen einschließt, kommt diese Beschränkung nicht hinreichend zum Ausdruck. Es sollte deshalb die in Absatz 2 gewählte Formulierung übernommen werden: „Die **Dienststellen des Polizeivollzugsdienstes** können zur Erfüllung ihrer Aufgaben die … **selbst** erhobenen Daten … worden sind, **weiter nutzen**, wenn …“. Fraglich ist des Weiteren, ob Absatz 3 Nummer 1 neben Nummer 3 eine eigenständige Bedeutung zukommt.[17]

In Absatz 4 Satz 1 sollten die Wörter „entsprechender Beachtung“ durch die Wörter „den Voraussetzungen“ ersetzt werden. Die derzeitige Textfassung begegnet unter Bestimmtheitsgesichtspunkten erheblichen Bedenken. Bedenken hinsichtlich der

[14] Fn 1, Rn 278
[15] Fn 1, Rn 284
[16] Fn 1, Rn 300
[17] Fn 1, Rn 290 als Zusammenfassung der Rn 288 und 289

Normenbestimmtheit und Normenklarheit bestehen insbesondere auch im Hinblick auf die gewählte Regelungstechnik: „Erreicht der Gesetzgeber die Festlegung des Normeninhalts aber - wie hier - nur mit Hilfe zum Teil langer, über mehrere Ebenen gestaffelter, unterschiedlich variabler Verweisungsketten, die bei gleichzeitiger Verzweigung in die Breite den Charakter von Kaskaden annehmen, leidet die praktische Erkennbarkeit der maßgebenden Rechtsgrundlage. Der Prüfvorgang wird dadurch fehleranfällig.“[18] Dies ist wenig anwenderfreundlich und sollte durch leichter verständliche Regelungen vereinfacht werden

Verfassungsrechtlich äußerst bedenklich erscheint die Regelung zur Datenübermittlung ins Nicht-EU-Ausland (Absatz 4 Satz 1 und 2 in Verbindung mit § 43 PolG). Die Ausführungen im BKAG-Urteil zu dieser Thematik[19] werfen hier eine Reihe von Fragen auf, insbesondere ob die Abhandlung der komplexen Materie mit einem Satz abgetan werden kann. So fordert das Bundesverfassungsgericht u.a. etwa, dass gewährleistet sein muss, dass die übermittelten Daten im Empfängerstaat weder zu politischer Verfolgung noch unmenschlicher oder erniedrigender Bestrafung oder Behandlung verwendet werden („Der Gesetzgeber hat insgesamt Sorge zu tragen, dass der Schutz der Europäischen Menschenrechtskonvention und der anderen internationalen Menschenrechtsverträge (vgl. Art. 1 Abs. 2 GG) durch eine Übermittlung der von deutschen Behörden erhobenen Daten ins Ausland und an internationale Organisationen nicht ausgehöhlt wird“)[20] sowie dass sich die übermittelnde Polizeidienststelle über das geforderte Schutzniveau vergewissern und die Gründe hierzu nachvollziehbar dokumentieren muss („Die Entscheidung muss durch die Datenschutzbeauftragten überprüfbar sein und einer gerichtlichen Kontrolle zugeführt werden können“).[21] Diese Maßgaben müssen „in einer den Grundsätzen der Bestimmtheit und Normenklarheit entsprechenden Weise gesetzlich ausgeformt sein.“ Wir verweisen insoweit auf die Regelung des § 27 Absatz 1 BKAG-neu in Verbindung mit §§ 78 bis 80 BDSG-neu und empfehlen dringend, sich an dem dortigen Wortlaut zu orientieren. Demgegenüber sichern die äußerst knappen Übermittlungsregelungen des Absatzes 4 diese Vorgaben in keiner Weise, sie bedürfen einer grundlegenden Überarbeitung.

Fazit

[18] Fn 2, Rn 132
[19] Fn 1, Rn 323 ff.
[20] Fn 1, Rn 336
[21] Fn 1, Rn 339

Ob das Sicherheitspaket einer Überprüfung auf Kosten und Nutzen standhält, wird das Parlament entscheiden. Aus Sicht des LfDI ist sein Nutzen offen - sicher sind bereits jetzt seine Kosten: Wir alle bezahlen die Hoffnung auf mehr Sicherheit mit der realen Einbuße an Freiheit.

Mit freundlichen Grüßen
In Vertretung
gez. Volker Broo