Prof. Dr. Matthias Bäcker, LL.M.
Universität Mannheim
Abteilung Rechtswissenschaft
Schloss
68131 Mannheim

Mannheim, den 8. März 2013

Stellungnahme

zu dem Entwurf eines Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft

(BT-Drs. 17/12034)

Gliederung

Ergebnisse

Im Folgenden fasse ich die wesentlichen Ergebnisse der Stellungnahme vorab thesenartig zusammen:

1. Für den Transfer gespeicherter Telekommunikationsdaten von einem Telekommunikationsdiensteanbieter zu einer Behörde bedarf es einer Übermittlungsermächtigung für den Diensteanbieter und einer Abfrageermächtigung für die Empfangsbehörde. Für die Regelung der Übermittlungsermächtigung ist der Bund zuständig. Die Gesetzgebungskompetenz für die Abfrageermächtigungen der verschiedenen Sicherheitsbehörden richtet sich nach der Kompetenz für das jeweilige behördliche Fachrecht und ist damit zwischen Bund und Ländern aufgeteilt. Der Bund als Gesetzgeber der Übermittlungsermächtigung muss vollständig und abschließend bestimmen, zu welchen Anlässen und Zielen die Daten übermittelt werden dürfen. Die Kompetenz, eine Verpflichtung (nicht nur Berechtigung) der privaten Diensteanbieter zur Datenübermittlung zu regeln, steht dem Gesetzgeber der Abfrageermächtigung zu.

2. Nach diesen Maßgaben ist die Übermittlungsermächtigung in § 113 TKG-E in zweifacher Hinsicht verfassungswidrig:

    a. Zum einen regelt die Norm lediglich, an welche Behörden Bestandsdaten übermittelt werden dürfen, nicht aber, unter welchen Voraussetzungen dies geschehen darf.

    b. Zum anderen sieht § 113 Abs. 4 Satz 1 TKG-E eine teilweise kompetenzwidrige Übermittlungspflicht der Diensteanbieter vor.

3. Die vorgesehenen Abfrageermächtigungen (Art. 2 ff. des Gesetzentwurfs) ermöglichen teilweise Bestandsdatenabrufe deutlich im Vorfeld einer konkreten Gefahr oder eines strafprozessualen Anfangsverdachts. Die in der Entwurfsbegründung und in der Gegenäußerung der Bundesregierung vorgetragene Behauptung, der Entwurf erweitere den Anwendungsbereich der Bestandsdatenabfrage gegenüber der bisherigen Rechtslage nicht, trifft daher nicht zu. Verfassungsrechtlich sind die vorgesehenen Vorfeldbefugnisse zumindest sehr heikel. Teilweise weisen diese Normen zudem erhebliche gesetzgebungstechnische Mängel auf.

4. Rechtspolitisch erscheint es mir angezeigt, im Zusammenhang mit den geplanten Abfrageermächtigungen vorzusehen, dass nach der Zuordnung einer IP-Adresse zu einem Anschlussinhaber der Betroffene benachrichtigt werden muss. Dies gilt nicht, wenn eine Benachrichtigungspflicht bereits im Zusammenhang mit den Regelungen besteht, auf deren Grundlage die zugeordneten Kommunikationsdaten gewonnen wurden.

5. Für die Erhebung von Zugangsdaten ist es verfassungsrechtlich geboten, in den Abfrageermächtigungen sowohl einen Richtervorbehalt als auch eine Benachrichtigungspflicht vorzusehen. Dies gilt nicht, soweit solche Sicherungen bereits im Zusammenhang mit den Regelungen vorgesehen sind, auf deren Grundlage die zugangsgesicherten Daten erhoben wurden bzw. erhoben werden sollen.

Die in dem Gesetzentwurf vorgesehenen Regelungen zur Bestandsdatenabfrage weisen in materiell-rechtlicher Hinsicht einige Defizite auf, die dazu führen, dass die verfassungsrechtlichen Anforderungen an solche Regelungen teilweise verfehlt werden. Dies führe ich in meiner Stellungnahme zunächst aus (unten I). Anschließend gehe ich auf die verfahrensrechtlichen Sicherungen ein, die laut der Einladung zu der Anhörung als besonders klärungsbedürftig angesehen werden (unten II).

I. Materiell-rechtliche Defizite der vorgesehenen Regelungen

Der Gesetzentwurf weist erhebliche regelungstechnische und zum Teil (auch aus den handwerklichen Problemen folgende) verfassungsrechtliche Defizite auf. Zum einen liegt dem Entwurf ein unzutreffendes Verständnis von der Gesetzgebungskompetenz und der grundrechtlichen Regelungsverantwortung des Bundes zugrunde, soweit Bestandsdatenabfragen durch Behörden ermöglicht werden sollen, für deren Fachrecht die Länder zuständig sind (unten 1). Dies führt dazu, dass § 113 TKG-E teils die Kompetenzordnung verletzt, teils regelungsbedürftige Fragen nicht regelt und so gegen Grundrechte verstößt (unten 2). Zudem sind einige der vorgesehenen Ermächtigungen zur Abfrage von Bestandsdaten im behördlichen Fachrecht misslungen (unten 3).

1. Gesetzgebungskompetenz und grundrechtliche Regelungsverantwortung des Bundes

Die Defizite des Gesetzesentwurfs beruhen zum Teil darauf, dass dem Entwurf offenkundig eine unzutreffende Vorstellung darüber zugrunde liegt, welche Fragen im Zusammenhang mit Bestandsdatenauskünften der Bund regeln darf und muss.

Das Bundesverfassungsgericht hat die Gesetzgebungskompetenz und die grundrechtliche Regelungsverantwortung des Bundes in seiner jüngeren Rechtsprechung[1] geklärt. Danach ergibt sich die Gesetzgebungskompetenz des Bundes für den Datenschutz im Telekommunikationssektor aus Art. 73 Abs. 1 Nr. 7 GG. Der Bund darf dabei Telekommunikationsdiensteanbieter auch verpflichten, Telekommunikationsdaten zu sicherheitsbehördlichen Zwecken zu bevorraten, wie dies für Bestandsdaten in § 111 TKG vorgesehen ist.[2] Hinsichtlich des Transfers der bei den Diensteanbietern vorhandenen Daten zu den Sicherheitsbehörden ist kompetenzrechtlich zu differenzieren:

Der Datentransfer ist rechtlich als zweigliedriger Vorgang zu konzipieren (das Bundesverfassungsgericht verwendet das Bild einer Doppeltür). Damit der Datentransfer zulässig ist, bedarf es zum einen einer *Übermittlungsermächtigung*, die dem Diensteanbieter als dem ursprünglichen Dateninhaber erlaubt, die Daten an bestimmte Behörden zu bestimmten Zwecken zu übermitteln. Die Empfangsbehörde benötigt zudem eine *Abfrageermächtigung*, um die Daten abrufen und entgegennehmen zu dürfen.[3] Für die Übermittlung von Telekommunikations-Bestandsdaten durch Telekommunikationsdiensteanbieter verteilt sich die Regelungskompetenz dabei wie folgt: Allein der Bund ist gem. Art. 73 Abs. 1 Nr. 7 GG berufen, den Telekommunikationsunternehmen eine Übermittlungsermächtigung einzuräumen. Die Ge-

[1] Neben dem Bestandsdatenbeschluss, der den unmittelbaren Anlass zu dem vorliegenden Gesetzentwurf gab [BVerfGE 130, 151], ist insoweit auch das Vorratsdatenurteil [BVerfGE 125, 260] bedeutsam.
[2] BVerfGE 130, 151 (185 f.); für Verkehrsdaten ebenso BVerfGE 125, 260 (313 ff.).
[3] BVerfGE 130, 151 (184).

setzgebungskompetenz für die Abfrageermächtigungen der verschiedenen Sicherheitsbehörden richtet sich hingegen nach der Kompetenz für das jeweilige behördliche Fachrecht.[4]

Das Doppeltürmodell klärt für sich genommen noch nicht, welche Fragen im Zusammenhang mit einem Bestandsdatenabruf zwingend der Bund aufgrund seiner Kompetenz für die Übermittlungsermächtigung zu regeln hat und für welche Fragen sich die Gesetzgebungskompetenz nach der Zuständigkeit für die Abfrageermächtigungen richtet. Für die Beurteilung des vorliegenden Gesetzentwurfs sind dabei zwei Fragen bedeutsam:

Zum einen ist relevant, welcher Gesetzgeber die Telekommunikationsunternehmen verpflichten (und nicht lediglich berechtigen) kann, Bestandsdaten an Sicherheitsbehörden zu übermitteln. Das Bundesverfassungsgericht hat hierzu ausgeführt, die Regelungskompetenz für die Übermittlungsermächtigung ermögliche dem Bund lediglich, den Telekommunikationsunternehmen eine datenschutzrechtliche Erlaubnis einzuräumen, bestimmte Daten zu übermitteln. Eine Pflicht der Unternehmen zur Datenübermittlung sei hingegen als Teil des Abrufs kompetenziell den Gesetzgebern der Abfrageermächtigungen zugewiesen, also in weitem Umfang den Ländern.[5]

Zum anderen ist maßgeblich, ob der Bund bereits aufgrund seiner Kompetenz für die Übermittlungsermächtigung die materiellen Voraussetzungen eines Datentransfers regeln kann oder sogar muss. Der Entwurf beruht erkennbar auf der Annahme, für die Regelung dieser Voraussetzungen sei allein der Gesetzgeber der jeweiligen Abfrageermächtigung zuständig. Die Gegenäußerung der Bundesregierung zum ersten Einwand des Bundesrats zeigt dies deutlich.

Diese Annahme ist jedoch unzutreffend. Im Gegenteil muss der Bund abschließend regeln, aus welchen Anlässen und zu welchen Zielen die Daten höchstens[6] übermittelt werden dürfen. Die Gesetzgebungskompetenz des Bundes für den Datenschutz im Telekommunikationssektor, die Datenbevorratungen für sicherheitsbehördliche Zwecke umfasst, begründet mittelbar eine grundrechtliche Verantwortung des Bundes für den Umgang mit gespeicherten Telekommunikationsdaten. Diese Regelungsverantwortung ergibt sich aus dem verfassungsrechtlichen Zweckbindungsgrundsatz: Nur mit Blick auf die zulässigen Verwendungszwecke lässt sich die Verhältnismäßigkeit einer Datenerhebung sicherstellen. Der Bund genügt seiner Regelungsverantwortung im Hinblick auf landesrechtliche Abfrageermächtigungen nicht schon dadurch, dass die Übermittlungsermächtigung etwa bestimmte Behörden oder behördliche Aufgabenbereiche benennt, für welche die Daten zur Verfügung gestellt werden. Vielmehr muss die Übermittlung an tatbestandliche Voraussetzungen gebunden werden, die gewährleisten, dass der Datentransfer insgesamt den grundrechtlichen Anforderungen genügt.

Diese Anforderungen an die Übermittlungsermächtigung gehen aus der jüngeren Rechtsprechung des Bundesverfassungsgerichts klar hervor. Im Bestandsdatenbeschluss heißt es, der Bund dürfe die Telekommunikationsunternehmen ermächtigen, Telekommunikationsdaten für

---

[4] BVerfGE 130, 151 (200 ff.).
[5] BVerfGE 130, 151 (201).
[6] Es steht den Gesetzgebern der Abfrageermächtigungen frei, den Datenabruf durch die jeweils betroffenen Behörden an höhere Anforderungen zu binden, als sie in der Übermittlungsermächtigung vorgesehen sind.

„bestimmte, von ihm im Einzelnen zu regelnde Zwecke“[7] zu übermitteln. Es folgt ein Verweis auf das Vorratsdatenurteil, in dem das Bundesverfassungsgericht ausgeführt hat, mit der dort gegenständlichen Speicherungsverpflichtung sei im Sinne einer „datenschutzrechtlichen Verklammerung von Eingriff und Rechtfertigung“[8] eine „den Verhältnismäßigkeitsanforderungen genügende normenklare Begrenzung der Datenverwendung“ untrennbar verbunden.[9] Zu den vom Bund zu schaffenden Regelungen gehöre daher „die Festlegung der qualifizierten Voraussetzungen für eine Verwendung der Daten zum Zwecke der Strafverfolgung, der Gefahrenabwehr oder der Gefahrenprävention durch die Nachrichtendienste“.[10] Im Übrigen zeigt sich die Regelungsverantwortung des Bundes auch darin, dass das Bundesverfassungsgericht im Bestandsdatenbeschluss § 113 Abs. 1 Satz 2 TKG für verfassungswidrig erklärt hat, da diese Norm zu niedrige Anforderungen an die Abfrage von Zugangsdaten stellt.[11] Wäre es allein Sache der Gesetzgeber der Abfrageermächtigungen, diese Anforderungen zu regeln, so hätte § 113 Abs. 1 Satz 2 TKG mit dieser Begründung nicht beanstandet werden können.

2. Defizite von § 113 TKG-E

Auf dieser Grundlage lassen sich die Defizite von § 113 TKG-E benennen. Die Vorschrift verletzt teilweise die Kompetenzordnung und verstößt teilweise gegen Grundrechte, indem sie die Regelungsverantwortung des Bundes verfehlt.

§ 113 Abs. 4 Satz 1 TKG-E ist teilweise kompetenzwidrig, da diese Vorschrift eine Übermittlungspflicht der Telekommunikationsunternehmen auch insoweit vorsieht, als für die zugehörigen Abfrageermächtigungen eine Gesetzgebungskompetenz der Länder besteht. Denn die Regelungsbefugnis für eine solche Übermittlungspflicht folgt der Regelungsbefugnis für die Abfrageermächtigung. Hinsichtlich der bundesrechtlichen Abfrageermächtigungen, die der Gesetzentwurf enthält, ist § 113 Abs. 4 Satz 1 TKG-E hingegen zwar kompetenzgemäß, aber redundant, da diese Normen – systematisch korrekt – durchweg ausdrücklich eine Übermittlungspflicht begründen. § 113 Abs. 4 Satz 1 TKG-E sollte daher ersatzlos gestrichen werden.

Hingegen fehlen in § 113 TKG-E Übermittlungstatbestände, welche die geregelten Datenübermittlungen legitimieren könnten. § 113 Abs. 3 TKG-E regelt lediglich, an welche Behörden die Daten übermittelt werden dürfen, nicht aber, unter welchen Voraussetzungen dies zulässig ist. Entgegen der Auffassung der Bundesregierung ist der Bund aber nicht nur befugt, sondern grundrechtlich verpflichtet, solche Voraussetzungen zu normieren. Da § 113 TKG-E nach der Entwurfsbegründung den Anwendungsbereich der Bestandsdatenabfrage gegenüber dem bisherigen Zustand nicht erweitern soll,[12] bietet es sich an, § 113 Abs. 3 TKG-E nach dem Vorbild des derzeit geltenden § 113 Abs. 1 Satz 1 TKG umzugestalten.[13] Zusätzlich

[7] BVerfGE 130, 151 (201).
[8] BVerfGE 125, 260 (346).
[9] BVerfGE 125, 260 (344).
[10] BVerfGE 125, 260 (346).
[11] BVerfGE 130, 151 (207 ff.).
[12] So S. 15 des Entwurfs und die Gegenäußerung der Bundesregierung auf S. 38; tendenziell anders hingegen S. 21 des Entwurfs, wo es heißt, § 113 Abs. 3 TKG-E solle lediglich „vorbehaltlich der Regelungen in den Fachgesetzen den Kreis der berechtigten Behörden gegenüber der bislang geltenden Rechtslage beibehalten“.
[13] In der Folge müssten allerdings auch zahlreiche der vorgesehenen bundesrechtlichen Abfrageermächtigungen geändert werden, siehe dazu eingehend unten bei I. 3.

muss die Übermittlung von Zugangsdaten (§ 113 Abs. 1 Satz 2 TKG-E) daran gebunden werden, dass die Voraussetzungen vorliegen, unter denen diese Daten genutzt werden dürfen.[14]

3. Defizite der geplanten bundesrechtlichen Abfrageermächtigungen

Die in dem Gesetzentwurf vorgesehenen Abfrageermächtigungen weisen weitere Defizite auf. Teils sind sie normsystematisch misslungen, teils bestehen gegen sie auch verfassungsrechtliche Bedenken.

a) § 7 BKAG-E

Fragen wirft zunächst die in § 7 Abs. 3 BKAG-E enthaltene Abfrageermächtigung für das Bundeskriminalamt in seiner Funktion als Zentralstelle auf. Sie vermittelt eine weitreichende Befugnis zu Bestandsdatenabrufen im Vorfeld konkreter Gefahren oder strafprozessualer Verdachtslagen, die sich verfassungsrechtlich nicht halten lässt.

Der Anwendungsbereich von § 7 Abs. 3 BKAG-E geht über die in der Entwurfsbegründung beispielhaft angeführten akuten Krisenlagen (Suizidankündigung, Androhung eines Amoklaufs) weit hinaus. Die Datenerhebungsermächtigung in § 7 Abs. 2 BKAG, an die § 7 Abs. 3 BKAG-E anknüpft, ermächtigt das Bundeskriminalamt vielmehr zu Datenerhebungen weit im Vorfeld solcher Krisenlagen, um dem heutigen (Selbst-)Verständnis des Amts als „Intelligence-Behörde“[15] Rechnung zu tragen. Die vorgesehene Regelung eröffnet dem Bundeskriminalamt danach die Befugnis, Bestandsdatenabfragen zur Unterstützung von kriminalstrategischen Analysen zu nutzen, die es unabhängig von konkreten Verdachtsmomenten durchführt.[16] Entgegen der Entwurfsbegründung und der Gegenäußerung der Bundesregierung kann daher im Hinblick auf § 7 BKAG-E keine Rede davon sein, dass der Entwurf den bisherigen Anwendungsbereich der Bestandsdatenabfrage beibehielte.

Eine so weit gefasste Abfrageermächtigung ist mit den Grundrechten der Betroffenen nicht vereinbar. Das ergibt sich bereits aus dem Bestandsdatenbeschluss des Bundesverfassungsgerichts. Dort hat das Gericht die in § 113 Abs. 1 Satz 1 TKG enthaltenen Übermittlungsvoraussetzungen einer konkreten Gefahr und eines strafprozessualen Anfangsverdachts als „verfassungsrechtlich noch hinnehmbar“ bezeichnet. Daraus ist zu schließen, dass eine im Vorfeld von Gefahr und Verdacht angesiedelte Abfrageermächtigung zumindest deutliche tatbestandliche Qualifikationen etwa im Hinblick auf das Gewicht drohender Schäden enthalten müsste, um den grundrechtlichen Anforderungen zu genügen. Solche qualifizierenden Tatbestandsmerkmale lassen sich § 7 Abs. 3 BKAG-E auch dann nicht entnehmen, wenn diese Norm im Zusammenhang mit der Aufgabenzuweisung in § 2 Abs. 1, Abs. 2 Nr. 1 BKAG gelesen wird, da der dort verwandte Begriff der „Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung“ wenig restriktiv gefasst ist.[17] Der Anwendungsbereich der Norm wird auch nicht dadurch hinreichend begrenzt, dass wegen des Verweises auf § 7 Abs. 2 BKAG die Daten nur zur Ergänzung oder Anreicherung bereits vorhandener Datenbestände erhoben

[14] Vgl. BVerfGE 130, 151 (208 f.).
[15] *Abbühl,* Der Aufgabenwandel des Bundeskriminalamtes, 2010, S. 353 ff.; aus der Eigenperspektive des Bundeskriminalamts zu dessen „Intelligence-Arbeit“ etwa *Ahlf/Daub/Lierscher/Störzer,* BKAG, § 2 Rn. 11 und 34.
[16] Ähnlich zu § 7 Abs. 2 BKAG etwa *Papsthart,* in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 7 BKAG Rn. 3: die Datenerhebungsbefugnis beziehe sich „auf Straftaten, aber auch auf kriminelle Strukturen“.
[17] Näher *Ahlf/Daub/Lierscher/Störzer,* BKAG, § 2 Rn. 28 ff.;

werden dürfen,[18] da diese Beschränkung nichts am Vorfeldcharakter der Auswertungstätigkeit ändert.

Regelungstechnisch könnte § 7 Abs. 3 BKAG-E verfassungskonform gefasst werden, indem die Abfragebefugnis an das Erfordernis einer konkreten Gefahr gebunden wird. Der Sinn der Ermächtigung läge dann vor allem darin, Krisensituationen aufzulösen, auf die das Bundeskriminalamt im Rahmen seiner Auswertungstätigkeit stößt. Die in der Entwurfsbegründung angeführten Beispielsfälle ließen sich auf diesem Weg durchaus bewältigen. Eine Nutzung der Bestandsdatenabfrage für kriminalstrategische Analysen im Vorfeld konkreter präventivpolizeilicher oder strafprozessualer Verfahren – und damit im Rahmen der „Intelligence-Arbeit" des Bundeskriminalamts – schiede hingegen aus.

Sollen dem Bundeskriminalamt hingegen Bestandsdatenabfragen gerade für kriminalstrategische Auswertungszwecke ermöglicht werden, müsste eine Vorfeldermächtigung geschaffen werden, deren Anwendungsbereich durch geeignete tatbestandliche Qualifikationen zu begrenzen wäre. Zudem müsste auch § 113 Abs. 3 TKG-E so angepasst werden, dass Datenübermittlungen im Gefahrvorfeld ermöglicht werden.[19] Eine solche Vorfeldermächtigung bliebe allerdings angesichts der Ausführungen im Bestandsdatenbeschluss verfassungsrechtlich riskant.

b) § 7 ZFdG-E

Die Erwägungen zu § 7 BKAG-E lassen sich weitgehend auf § 7 Abs. 5 ZFdG-E übertragen, der dem Zollkriminalamt Bestandsdatenabfragen in seiner Funktion als Zentralstelle ermöglichen soll. Auch hier müsste die geregelte Datenabfrage entweder an das Erfordernis einer konkreten Gefahr für die Schutzgüter des ZFdG oder zumindest an einen materiell deutlich qualifizierten Vorfeldtatbestand gebunden werden.

c) § 22 BKAG-E, § 15 ZFdG-E

§ 22 Abs. 2 Satz 1 BKAG-E und § 15 Abs. 2 Satz 1 ZFdG-E verfehlen die grundrechtlichen Anforderungen an Ermächtigungen zur Bestandsdatenabfrage. Beide Regelungen erlauben eine solche Abfrage bereits dann, wenn sie zur Erfüllung der jeweils in Bezug genommenen behördlichen Aufgabe erforderlich ist. Ob damit überhaupt ein äußerer Eingriffsanlass beschrieben wird, mag dahinstehen. Jedenfalls bewegen sich die geregelten Eingriffsschwellen deutlich unterhalb des Erfordernisses einer konkreten Gefahr,[20] ohne dass diese Vorverlagerung durch geeignete tatbestandliche Qualifikationen ausgeglichen würde.

d) 20b BKAG-E, § 22a BPolG

§ 20b Abs. 3 Satz 1 BKAG-E und § 22a Abs. 1 Satz 1 BPolG-E befremden aus polizeirechtssystematischer Sicht. Diese Vorschriften binden präventivpolizeiliche Bestandsdatenabfragen daran, dass die Abfragen „für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes einer Person" erforderlich sind. Diese Formulierung, die sich in vielen strafpro-

[18] Vgl. *Bäcker,* Terrorismusabwehr durch das Bundeskriminalamt, 2009, S. 23.
[19] Vgl. zum Anpassungsbedarf bei § 113 Abs. 3 TKG-E oben bei I. 2.
[20] Vgl. beispielhaft zu dem gleichartig konstruierten Art. 31 Abs. 1 Nr. 1 bayPAG *Berner/Köhler/Käß,* PAG, 20. Aufl., Art. 31 Rn. 6: Deutung als abstrakte Gefahr; generelle verfassungsrechtliche Bedenken etwa bei *Petri,* in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl., Rn. G 170.

zessualen Eingriffsermächtigungen findet,[21] ist im Polizeirecht höchst unüblich.[22] Sie dürfte darum in diesen Regelungen Verwirrung stiften und ohne Not erhebliche Interpretationsprobleme aufwerfen. Diese absehbaren Probleme begründen die – dem Gesetzgeber zuzurechnende – Gefahr, dass die Eingriffstatbestände letztlich keine eingriffsbegrenzende Wirkung entfalten. Daraus ergeben sich erhebliche Zweifel an ihrer Verfassungsmäßigkeit.

Auch die in beiden Regelungen jeweils enthaltenen Verweise auf andere Befugnisregelungen[23] sind in diesem Zusammenhang wenig hilfreich. Insbesondere wird nicht deutlich, ob diese Verweise generell den Tatbestand der Abfrageermächtigung ausfüllen sollen oder ob sie sich nur auf die Personen beziehen, deren Aufenthaltsort erforscht werden soll. Handelt es sich um tatbestandliche Verweisungen, so ist unklar, welchen Sinn daneben die dem Strafprozessrecht entlehnte Formulierung „für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes einer Person“ haben soll.

Ich empfehle dringend, diese Vorschriften so umzuformulieren, dass der Eingriffstatbestand klar wird. Dieser Tatbestand sollte zudem anhand von Regelungsbausteinen gestaltet werden, die im Polizeirecht geläufig sind. Hierfür bietet sich in erster Linie das hergebrachte Erfordernis einer konkreten Gefahr für die jeweiligen gesetzlichen Schutzgüter an. Falls – über die bisherige Rechtslage hinausgehend – präventivpolizeiliche Bestandsdatenabfragen des Bundeskriminalamts bzw. der Bundespolizei auch im Gefahrvorfeld ermöglicht werden sollen, sollte zumindest an geläufigere Regelungsmuster angeknüpft werden. Verfassungsrechtlich wäre eine Vorfeldbefugnis nach meiner Einschätzung am ehesten in § 20b Abs. 3 BKAG-E zulässig, da die präventivpolizeiliche Aufgabe des Bundeskriminalamts nach § 4a BKAG und die zugehörigen Befugnisregelungen in §§ 20a ff. BKAG auf die Verhütung schwerer Straftaten mit hohem Schadenspotenzial abzielen.

II. Das Erfordernis ergänzender verfahrensrechtlicher Sicherungen im behördlichen Fachrecht

Ergänzend zu den materiell-rechtlichen Übermittlungs- und Abfragetatbeständen ist zu erwägen, ob der Bestandsdatenabruf an zusätzliche verfahrensrechtliche Schutzvorkehrungen gebunden werden sollte. Zu denken ist zunächst an einen Richter- oder einen sonstigen Kontrollvorbehalt, um den Grundrechten des Betroffenen bereits bei der Entscheidung über einen Bestandsdatenabruf Rechnung zu tragen.[24] Daneben stellt sich die Frage, ob der Betroffene zumindest im Anschluss an einen heimlich durchgeführten Bestandsdatenabruf von dem Abruf zu benachrichtigen ist, damit er seine informationelle Stellung gegenüber der handelnden Behörde einschätzen und gegebenenfalls Rechtsbehelfe einlegen kann.[25]

Allerdings müssen von Verfassungs wegen nicht alle heimlichen oder überraschenden Grundrechtseingriffe unter Richtervorbehalt gestellt werden. Auch eine aktive Benachrichtigung des

---

[21] Vgl. beispielhaft § 98a Abs. 1, § 100a Abs. 1 Nr. 3, § 100f Abs. 1, § 100h Abs. 1 Satz 1 StPO.
[22] Im BPolG findet sich diese Formulierung bislang überhaupt nicht, im BKAG nur in § 20g Abs. 2 Nr. 3.
[23] Von § 20b Abs. 3 Satz 1 BKAG-E auf § 20b Abs. 1 und 2 BKAG; von § 22a Abs. 1 Satz 1 BPolG-E auf § 21 Abs. 1 und 2 BPolG.
[24] Allgemein zur grundrechtssichernden Bedeutung von Richtervorbehalten BVerfGE 120, 274 (331 ff.); 125, 260 (337 ff.).
[25] Zu den Funktionen von transparenzsichernden Regelungen BVerfGE 120, 351 (360 f.); 125, 260 (335).

Betroffenen nach einem solchen Eingriff ist nicht durchweg verfassungsrechtlich geboten. Maßgeblich kommt es hierfür vielmehr vor allem auf die Intensität des jeweils geregelten Grundrechtseingriffs an;[26] hinsichtlich einer Benachrichtigungspflicht ist zudem bedeutsam, ob für den Betroffenen auch ohne aktive Benachrichtigung eine hinreichende und zumutbare Möglichkeit besteht, von dem Eingriff zu erfahren.[27] Ein kumulativer Verzicht sowohl auf eine unabhängige Vorabkontrolle als auch auf eine nachträgliche Benachrichtigung des Betroffenen erscheint mir allerdings bei heimlichen Eingriffen nur dann zulässig, wenn diese – trotz der Heimlichkeit – lediglich geringes Gewicht aufweisen. Denn wenn beide Sicherungen fehlen, wird die Exekutive faktisch sehr weitgehend von einer Grundrechtskontrolle durch eine unabhängige Stelle freigestellt.

Soweit heimliche Grundrechtseingriffe allerdings tatsächlich nur ein niedriges Gewicht aufweisen, halte ich derartige Verfahrensregelungen auch rechtspolitisch zumindest nicht für zwingend geboten. Von Kontrollvorbehalten für solche Eingriffe würde ich sogar abraten. Insbesondere flächendeckende Richtervorbehalte auch für eher bagatellarische Eingriffsmaßnahmen dürften dem Ziel, die Grundrechte gegenüber heimlichen oder überraschenden Eingriffen präventiv zu schützen, letztlich insgesamt zuwiderlaufen, da in der Praxis eine (weitere) Reduktion der vorbehaltsrichterlichen Prüfungsdichte zu erwarten stünde.

In der Folge stellt sich die Frage nach verfahrensrechtlichen Sicherungen meiner Ansicht nach primär für zwei Sonderfälle der Bestandsdatenabfrage, die zumindest potenziell eine erhöhte Eingriffsintensität aufweisen,[28] nämlich die Zuordnung von IP-Adressen[29] und die Erhebung von Zugangsdaten, mit denen der Zugriff auf Endgeräte sowie auf lokale oder netzbasierte Speichereinrichtungen geschützt wird.[30]

1. Reichweite der Gesetzgebungskompetenz des Bundes

Zu beachten ist dabei, dass die Gesetzgebungskompetenz für die angesprochenen verfahrensrechtlichen Sicherungen sich nach der Kompetenz für die Abfrageermächtigung richtet.[31] Der Bund kann darum Richtervorbehalte und Benachrichtigungspflichten nicht in § 113 TKG-E verbindlich für alle Bestandsdatenabfragen vorgeben. Derartige Regelungen wären vielmehr in die fachrechtlichen Abfrageermächtigungen aufzunehmen, die Art. 2 ff. des Gesetzentwurfs vorsehen. Hinsichtlich landesrechtlicher Abfrageermächtigungen ist es – selbstverständlich im Rahmen der grundrechtlichen Vorgaben – Ländersache, ob und welche verfahrensrechtlichen Schutzregelungen geschaffen werden sollen.

Da demnach verfahrensrechtliche Sicherungen sinnvoll nur bereichsspezifisch zu den einzelnen Abfrageermächtigungen eingerichtet werden können, sollte bei der Ausgestaltung solcher Sicherungen auch der jeweils bereichsspezifische normative Kontext einbezogen werden: So unterscheiden sich die Eingriffsintensität von Bestandsdatenabfragen und der Schutzbedarf

---

[26] Zu Richtervorbehalten BVerfGE 118, 168 (202); 120, 274 (331); 125, 260 (337); zu Benachrichtigungspflichten BVerfGE 118, 168 (209 f.); 130, 151 (210).
[27] In diese Richtung BVerfGE 118, 168 (200, 208 ff.).
[28] Zur prinzipiell begrenzten Eingriffsintensität von Bestandsdatenabfragen BVerfGE 130, 151 (189 ff., 197, 205).
[29] § 113 Abs. 1 Satz 3 TKG-E für dynamisch vergebene IP-Adressen, § 112 Abs. 2 i.V.m. § 111 Abs. 1 Satz 1 Nr. 1 TKG für statisch vergebene IP-Adressen.
[30] § 113 Abs. 1 Satz 2 TKG-E.
[31] BVerfGE 125, 260 (346 f.); 130, 151 (210).

der Betroffenen ebenso wie das Gewicht gegenläufiger Interessen, die gegen einen Kontrollvorbehalt oder eine Benachrichtigungspflicht sprechen, je nach handelnder Behörde und maßgeblichem Rechtsregime.

Eine detaillierte und differenzierte Erörterung aller Abfrageermächtigungen, die der Gesetzentwurf vorsieht, würde allerdings den Rahmen dieser Stellungnahme sprengen. Die folgenden Ausführungen beschränken sich darum auf das Strafverfahrensrecht als das praktisch bedeutsamste und typischerweise schärfste Eingriffsregime. Sie lassen sich auf die anderen Regime nicht unbesehen und in allen Einzelheiten übertragen, die Grundüberlegungen dürften jedoch verallgemeinerbar sein.

2. Zuordnung von IP-Adressen

Die Eingriffsintensität der Zuordnung einer IP-Adresse zu einem Anschlussinhaber lässt sich kaum allgemeingültig bestimmen. Für sich genommen hat die Aussage, dass eine bestimmte IP-Adresse (bei dynamischer Adressierung: zu einem bestimmten Zeitpunkt) dem Anschluss einer bestimmten Person zugewiesen war, nur einen sehr geringen Informationswert. Maßgeblich ist vielmehr, wie umfangreich und aussagekräftig die Kommunikationsdaten sind, die aufgrund der Zuordnung auf einen bestimmten Betroffenen bezogen werden können. Beispielsweise macht es einen erheblichen Unterschied, ob der Absender einer einzelnen E-Mail identifiziert oder ob ein großer Datenbestand zugeordnet werden soll, der etwa von dem Betreiber eines Webanalysetools[32] oder dem Betreiber eines Dienstes des *social web*[33] erlangt wurde.

Die Zuordnung einer IP-Adresse zu einem Anschlussinhaber muss darum hinsichtlich ihrer Eingriffsintensität und damit auch hinsichtlich der gebotenen materiell-rechtlichen wie verfahrensrechtlichen Anforderungen zusammen mit den vorgelagerten Fragen betrachtet werden, wer welche Kommunikationsdaten in Verbindung mit einer IP-Adresse speichern darf und unter welchen Voraussetzungen solche Daten an staatliche Stellen übergeben werden dürfen. Die Anforderungen an die Zuordnung einer IP-Adresse müssen dementsprechend als Baustein eines komplexen Schutzkonzepts begriffen werden, das insgesamt die Grundrechte des Betroffenen sowohl gegenüber der staatlichen Gewalt als auch gegenüber privaten Dritten gewährleistet. Weitere Bausteine dieses Schutzkonzepts sind:

- rechtliche Anforderungen an die Zuweisung von IP-Adressen durch die Betreiber von Internetzugangsdiensten – bisher erhalten natürliche Personen in der Regel dynamische IP-Adressen zugewiesen, auch wenn einige Zugangsanbieter IP-Adressen bereits heute quasi-statisch vergeben; nach einer flächendeckenden Einführung von IPv6 wird es jedoch technisch und wirtschaftlich möglich sein, auch natürlichen Personen durchweg statische IP-Adressen zuzuweisen;

[32] Soweit dieser die IP-Adressen der Nutzer von Angeboten erhebt und speichert, welche das Tool eingebunden haben. Beispielsweise ermöglicht Google Analytics den Anbietern eine Anonymisierung durch einen Steuerbefehl, aufgrund dessen die letzten 8 Bit der übermittelten IP-Adressen vor der Speicherung gelöscht werden; vgl. zu den Anforderungen an einen datenschutzkonformen Einsatz von Google Analytics etwa http://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_fuer_Webseitenbetreiber_in_Hamburg_01.pdf.

[33] Etwa bei einem Bloghoster oder einem sozialen Netzwerk, soweit der Betreiber die Klarnamen der Nutzer nicht erhebt oder zumindest nicht verifiziert.

- soweit IP-Adressen dynamisch zugewiesen werden: rechtliche Anforderungen an die Speicherung der Verkehrsdaten, mit deren Hilfe der Zugangsanbieter solche IP-Adressen bestimmten Anschlussinhabern zuordnen kann;
- rechtliche Anforderungen an die Speicherung von Kommunikationsdaten und zugehörigen IP-Adressen durch Kommunikationspartner des Adressinhabers, wobei der Begriff des Kommunikationspartners weit zu verstehen ist und jeden umfasst, der im Rahmen eines netzbasierten Kommunikationsvorgangs die IP-Adresse eines Kommunikationsbeteiligten übermittelt erhält (also beispielsweise auch die Betreiber von eingebundenen Diensten wie *social plugins* oder Webanalysetools);
- rechtliche Anforderungen an die Übermittlung von Kommunikationsdaten und zugehörigen IP-Adressen durch einen Kommunikationspartner des Adressinhabers an staatliche Stellen auf eigene Initiative dieses Kommunikationspartners;
- rechtliche Anforderungen an die hoheitliche Erhebung von Kommunikationsdaten und zugehörigen IP-Adressen bei einem Kommunikationspartner des Adressinhabers durch staatliche Stellen.

Diese Bausteine sind überwiegend dem allgemeinen oder bereichsspezifischen Datenschutzrecht zuzuordnen. Sie können insoweit hier nicht vertieft werden.[34] Besonderes Augenmerk sollte allerdings gerade mit Blick auf das Strafverfahren dem letzten Punkt gelten. Der gegenwärtige Rechtszustand ist insoweit höchst unbefriedigend. Dies gilt insbesondere für die Fallkonstellation, dass ein Unternehmen, welches über komplexe Datenbestände verfügt, seine Bestände aufgrund eines bestimmten behördlichen Erkenntnisinteresses auswerten und die Ergebnisse übermitteln soll. In der Praxis der Strafverfolgung finden solche Auswertungen – gerade auch mit Blick auf Datenbestände, welche netzbasierte Kommunikation zum Gegenstand haben – durchaus häufig statt; es fehlt jedoch hierfür an einer spezifischen Rechtsgrundlage, die der besonderen Eingriffsintensität derartiger Analysen hinreichend Rechnung trägt.[35]

Werden an die Datenauswertung und die folgende Datenübermittlung an die Strafverfolgungsbehörden hingegen keine hinreichenden Anforderungen erhoben, lässt sich das dadurch begründete rechtsstaatliche Defizit auf der nachgelagerten Ebene der Zuordnung der übermittelten Daten zu einem bestimmten Anschlussinhaber nicht mehr überzeugend einfangen. Insbesondere würde es mir nicht einleuchten, an die Zuordnung von IP-Adressen schon deswegen pauschal hohe materiell-rechtliche und verfahrensrechtliche Anforderungen zu errichten, weil in bestimmten Fallkonstellationen auf diese Weise sehr umfangreiche und aussagekräftige Kommunikationsdatenbestände zugeordnet werden können. Vielmehr muss berücksichtigt werden, dass die Zuordnung je nach Fallgestaltung auch dazu dienen kann, deutlich weniger sensible Informationen zu gewinnen.[36]

---

[34] Vgl. beispielhaft für datenschutzrechtliche Fragen in diesem Zusammenhang, die in jüngerer Zeit diskutiert wurden: zu Implikationen der Umstellung auf IPv6 aus rechtsdogmatischer und rechtspolitischer Sicht *Freund/Schnabel,* MMR 2011, S. 495; *Nietsch,* CR 2011, S. 763; zur Speicherung von Verkehrsdaten durch Internetzugangsprovider BGH, Urteil vom 13. Januar 2011 - III ZR 146/10 -, NJW 2011, S. 1509; zur datenschutzrechtlichen Bewertung des von Facebook bereitgestellten „Gefällt mir"-Buttons *Piltz,* CR 2011, S. 657.

[35] Allgemein zu den mit solchen Auswertungen verbundenen strafprozessualen Fragen *Brodowski,* ZIS 2012, S. 474.

[36] Vgl. zu den materiell-rechtlichen Anforderungen an die Abfrage von Zugangsdaten BVerfGE 130, 151 (209).

Angesichts dessen hielte ich es insbesondere für überzogen, die Zuordnung einer IP-Adresse an einen Richtervorbehalt zu binden. Eine solche Regelung würde vielmehr einer Banalisierung des Richtervorbehalts als Schutzinstrument Vorschub leisten und könnte schlimmstenfalls das Gegenteil des intendierten prozeduralen Grundrechtsschutzes bewirken.

Sinnvoll, wenn auch nicht in jedem denkbaren Fall verfassungsrechtlich geboten erscheint es mir hingegen vorzusehen, dass der Betroffene nach der Zuordnung der IP-Adresse zu benachrichtigen ist. Denn immerhin hat die Zuordnung zur Folge, dass der Betroffene gegenüber den Strafverfolgungsbehörden individualisiert wird und so unmittelbar in ihr Blickfeld gerät. Ab diesem Zeitpunkt ist eine Benachrichtigung zudem in jedem Fall faktisch möglich.

Ich schlage darum vor, die Benachrichtigungsregelung in § 101 Abs. 1 und 4 StPO auf die Fälle des § 100j Abs. 2 StPO-E zu erstrecken. Allerdings ist eine gesonderte Benachrichtigung über die Zuordnung der IP-Adresse entbehrlich, wenn der Betroffene bereits über die Maßnahme zu benachrichtigen ist, mit der die zugeordneten Kommunikationsdaten erlangt wurden. Darum sollte in die Benachrichtigungsregelung eine entsprechende Subsidiaritätsklausel aufgenommen werden.

3. Erhebung von Zugangsdaten

Eine Zugangsdatenabfrage nach § 100j Abs. 1 Satz 2 StPO sollte meiner Ansicht nach sowohl unter Richtervorbehalt gestellt als auch durch eine nachträgliche Benachrichtigungspflicht ergänzt werden. Dies halte ich auch für verfassungsrechtlich geboten.

Maßgeblich hierfür ist die besondere Eingriffsintensität der Zugangsdatenabfrage. Zwar dient diese Datenerhebung letztlich dazu, weitere Daten zu erlangen oder zu entschlüsseln. Diese weiteren Daten können wiederum mit unterschiedlichen Maßnahmen gewonnen werden, die unterschiedlich intensiv in Grundrechte eingreifen. Die Eingriffsintensität einer Zugangsdatenabfrage kann in der Folge – insoweit ähnlich wie bei der Zuordnung einer IP-Adresse – nicht pauschal bestimmt werden.[37] Die Zugangsdatenabfrage zeitigt aber in jedem Fall eine zusätzliche eigenständige und erhebliche Eingriffswirkung dadurch, dass sie den informationellen Selbstschutz des Betroffenen vereitelt und so sein Vertrauen in die Privatheit seiner Kommunikationsbeziehungen frustriert.[38]

Angesichts dessen muss zum einen das Geheimhaltungsinteresse des Betroffenen, das sich in der Zugangssicherung manifestiert, vor der Entscheidung über den Bruch dieser Sicherung von einer unabhängigen Stelle mit den gegenläufigen hoheitlichen Erkenntnisinteressen abgewogen werden. Für das Strafverfahrensrecht ergibt sich daraus das Erfordernis eines Richtervorbehalts. Zum anderen muss der Betroffene über die Vereitelung seines informationellen Selbstschutzes informiert werden, um einschätzen zu können, welche Kenntnisse die Strafverfolgungsbehörden über ihn erlangen konnten.

Ein Richtervorbehalt und eine Benachrichtigungspflicht sind allerdings dann entbehrlich, wenn solche Sicherungen bereits für die Maßnahme bestehen, mit welcher die Strafverfol-

---

[37] Vgl. BVerfGE 130, 151 (208 f.).

[38] Allgemein zur grundrechtlichen Bedeutung informationellen Selbstschutzes BVerfGE 115, 166 (184 ff.); 120, 274 (306); BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 23. Oktober 2006 - 1 BvR 2027/02 -, juris, Tz. 29; *Hohmann-Dennhardt,* RDV 2008, S. 1.

gungsbehörde die zugangsgesicherten Daten erhebt. Es bietet sich darum an, in die verfahrensrechtlichen Schutznormen entsprechende Subsidiaritätsklauseln aufzunehmen.

Eine Benachrichtigungspflicht kann weiter dann entfallen, wenn die Zugangsdaten sich auf Gegenstände oder Datenbestände beziehen, welche die Strafverfolgungsbehörde gegenüber dem Betroffenen offen erlangt. In einem solchen Fall muss der Betroffene damit rechnen, dass die Behörde sich auch die erforderlichen Zugangsdaten beschafft hat oder beschaffen wird.