



# **Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit**

zu den

**Verfassungsbeschwerden des  
Herrn Dr. Patrick Breyer, u.a.**

Aktenzeichen:

**1 BvR 1873/13 und 1 BvR 2618/13**



Die von den Beschwerdeführern angegriffenen Vorschriften wurden im Wesentlichen mit dem „Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft“ vom 20.06.2013 (BGBl. I 2013, S. 1602 ff.) eingeführt oder geändert. Hintergrund der Gesetzesänderung war ein Beschluss des Bundesverfassungsgerichts (BVerfG) vom 24.01.2012, mit dem das Gericht § 113 Absatz 1 Satz 2 des damals geltenden Telekommunikationsgesetzes (TKG) mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes für unvereinbar erklärt hatte.

Im Gesetzgebungsverfahren wurden erfreulicherweise bereits eine Reihe meiner damaligen Änderungsvorschläge berücksichtigt, eine meiner wesentlichen Forderungen, die Bestandsdatenauskunft als solche – zumindest hinsichtlich ihres Umfangs – zu hinterfragen, allerdings außer Acht gelassen. Ich halte diesen Schritt jedoch nach wie vor für erforderlich, auch wenn ich mir der grundsätzlichen Notwendigkeit der Bestandsdatenauskunft als Mittel einer effektiven Strafverfolgung durchaus bewusst bin. Das Verfahren ist jedoch nicht nur isoliert, sondern auch im Kontext einer stetig zunehmenden Anzahl von weiteren sicherheitsbehördlichen Überwachungsmaßnahmen zu betrachten. Diese stellen nicht nur individuell, sondern vor allem in ihrer Gesamtheit einen nicht mehr unerheblichen Eingriff in die vom Grundgesetz geschützten Rechte der Betroffenen dar.

Diese Stellungnahme geht in einem ersten Teil zunächst auf datenschutzrechtliche Erwägungen zu konkret mit der Bestandsdatenauskunft in Zusammenhang stehende Vorschriften ein. Der Fokus liegt hierbei schwerpunktmäßig stärker auf Normen im fachspezifischen Recht der Sicherheitsbehörden, die im Sinne des „Doppeltürenmodells“ die Ermächtigungsgrundlage für die Abfrage und Verarbeitung der Bestandsdaten durch die Bedarfsträger darstellen, als auf den in diesem Zusammenhang aus datenschutzrechtlicher Sicht weniger problematischen Vorschriften des Telekommunikationsgesetzes.

Diese Ausführungen werden im Anschluss in einem zweiten Teil mit datenschutzrechtlichen Anmerkungen zu verfahrenssichernden Maßnahmen ergänzt, die gleich für mehrere Vorschriften Relevanz entfalten und damit sozusagen „global“ behandelt werden können



### **1. § 113 Abs. 1 S. 3 i.V.m. Abs. 3 Nr. 1 (2. Alt.) TKG**

§ 113 Abs. 3 Nr. 1 TKG gestattet die Auskunft über die Zuordnung einer dynamischen IP-Adresse zu einem Anschlussinhaber nach § 113 Abs. 1 S. 3 TKG auch zur Verfolgung von Ordnungswidrigkeiten. Mangels entsprechender Beschränkungen im Gesetzentwurf ist über § 46 OWiG i.V.m. § 100j StPO-E die Auskunft für jede noch so „einfache“ Ordnungswidrigkeit zulässig. Dies widerspricht jedoch eindeutig den Vorgaben des Bundesverfassungsgerichts aus dem Urteil zur Speicherung von Vorratsdaten, wonach ausdrücklich eine entsprechende Auskunft ausschließlich zur Verfolgung besonders gewichtiger Ordnungswidrigkeiten zulässig ist, die vom Gesetzgeber explizit benannt werden müssen (BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08, Rn. 262).

Diese Problematik hatte ich – leider erfolglos – bereits 2013 im Rahmen des Gesetzgebungsverfahrens zur Neuregelung der Bestandsdatenauskunft thematisiert. Auch heute wirft diese zu weit gehende Abfragebefugnis nach wie vor erhebliche verfassungsrechtliche Bedenken auf. Nicht nur weil die Telekommunikationsanbieter den hinter der IP-Adresse stehenden Anschluss nur ermitteln können, wenn sie auf Verkehrsdaten zugreifen und insofern in den Schutzbereich des Art. 10 GG eingreifen (vgl. BVerfG NJW 2012, 1419), sondern auch aufgrund der weiterreichenden Erkenntnisse, die aus einer IP-Adressenauskunft gezogen werden können (vgl. meine Ausführungen unten bei 2 a) (2) (c) sowie in *Teil II* zum Richtervorbehalt), ist hier eine Beschränkung des Auskunftsrechts zwingend erforderlich.

### **2. Zentralstellenbefugnisse des BKA und des ZKA**

#### **a) zu § 7 Abs. 3 bis 7 BKAG (künftig: § 10 BKAG)**

Die angegriffenen Vorschriften zur Bestandsdatenabfrage knüpfen unmittelbar an die Generalklausel des § 7 Abs. 2 BKAG an, stehen also mit ihr in einem engen inhaltlichen Zusammenhang. Diese erlaubt es dem BKA, Daten zu erheben, ohne an ein konkretes Verfahren zur Gefahrenabwehr oder zur Strafverfolgung anzuknüpfen. Als tatbestandliche Begrenzung enthält die Vorschrift nur einen Verweis auf die Aufgabenzuweisung als Zentralstelle. Sie ermächtigt dazu, Daten zu erheben, um vorhandene Informationen anzureichern und Auswer-



tungen und Analysen vorzunehmen. Art und Umfang dieser Analysen und Auswertungen sind nicht näher eingegrenzt – s.u. (1).

Die spezifischen Befugnisse zur Bestandsdatenabfrage stellen keine über die Generalklausel hinausgehenden wesentlichen materiellen Anforderungen – s.u. (2).

Erhebliche potentielle Folgen für die betroffenen Personen, die dafür nicht notwendig einen aktuellen Anlass gegeben haben müssen, ergeben sich zudem aus dem Zusammenhang mit neuen Formen der polizeilichen Informationsverarbeitung. Der Zusammenhang zwischen Datenerhebung und Weiterverarbeitung wird hier bereits deshalb deutlich, weil bereits die Voraussetzungen der Bestandsdatenabfrage an die Weiterverarbeitung – „Ergänzung vorhandener Sachverhalte“ und „Auswertung und Analyse“ – anknüpfen – s.u. (3).

Dies lässt Zweifel an der hinreichenden Normenbestimmtheit und Verhältnismäßigkeit zu; mindestens aber sind die angegriffenen Vorschriften eng auszulegen. Es ist allerdings fraglich, ob eine enge Auslegung nach der Neufassung mit dem Gesetz zur Neustrukturierung des Bundeskriminalamts<sup>1</sup> möglich ist (§§ 9, 10 BKAG n.F.). Denn die kaum eingegrenzten Möglichkeiten, Daten im Vorfeld von Gefahren allein zur strategischen und operativen Analyse zu erheben, werden durch die neue Verweisung auf § 2 Abs. 6 BKAG nochmals deutlicher herausgestellt – s.u. (4).

#### (1) Reichweite des § 7 Abs. 2 bis 7 BKAG, Datenerhebung als Zentralstelle

Anders als die Generalklauseln in den Landespolizeigesetzen oder in § 29 Abs. 1 S. 1 BPolG knüpft § 7 Abs. 2 BKAG nicht an eine konkrete Aufgabe zur Gefahrenabwehr an, sondern vielmehr nur an die Aufgabe der Zentralstelle. Innerhalb dieser Aufgabe verlangt die Vorschrift keinen konkreten Anlass für Datenerhebungen. Gemäß § 7 Abs. 2 S. 1 BKAG müssen die Daten lediglich der „Ergänzung vorhandener Sachverhalte“ oder „sonst zu Zwecken der Auswertung“ (nach §§ 9, 10 i.V.m. § 2 Abs. 6 BKAG n.F. darüber hinaus Analysen u.a.) dienlich sein.

---

<sup>1</sup> BGBl. I 2017, 1354; §§ nach dem Gesetz zur Neustrukturierung des Bundeskriminalamts werden folgend zitiert als „BKAG n.F.“



### *(a) Zentralstellenaufgabe*

Die Zentralstellenaufgabe ist abstrakter als die sonst von Polizeibehörden wahrgenommenen Aufgaben. Sie umfasst auch allgemeine Tätigkeiten der Gefahrenvorsorge und der vorbeugenden Straftatenbekämpfung. Sie beschränkt sich also nicht darauf, konkrete Gefahren abzuwehren oder aktuelle Strafverfahren durchzuführen (Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, Mannheim 2009, S. 22).

Der Begriff und Umfang der Zentralstellenaufgabe ist nur sehr vage definiert. § 7 Abs. 2 S. 1 verweist auf § 2 Abs. 2 Nr. 1 BKAG, der seinerseits auf § 2 Abs. 1 BKAG Bezug nimmt.

Gemäß § 2 Abs. 2 Nr. 1 BKAG hat das Bundeskriminalamt „alle Informationen zu sammeln und auszuwerten“, die erforderlich sind, um die Polizeibehörden des Bundes und der Länder gemäß § 2 Abs. 1 BKAG bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung zu „unterstützen“.

Gesetzlich normiert sind als Unterstützungsbefugnisse die zentrale Datenhaltung (§§ 7 bis 13 BKAG), die internationale Zusammenarbeit (§§ 14 bis 15a BKAG) sowie Unterstützung und Koordination bei der Strafverfolgung (§§ 16 bis 20 BKAG). Zentrale Datenhaltung und internationale Zusammenarbeit sind mit umfassenden Möglichkeiten zum Datenaustausch verbunden.

Zusätzlich ist die zugrunde liegende Gesetzgebungsbefugnis in den Blick zu nehmen. Diese ergibt sich aus Art. 73 Abs. 1 Nr. 10 i.V.m. Art. 87 Abs. 1 S. 2 GG. Wenn und soweit Straftaten länderübergreifende, internationale oder sonstige erhebliche Bedeutung i.S.d. § 2 Abs. 1 BKAG haben, ist die Arbeit der damit befassten Polizeidienststellen zwangsläufig zu koordinieren. Dem dient das Bundeskriminalamt als beim Bund auf Grundlage des Art. 87 Abs. 1 S. 2 GG eingerichtete „Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen“. Nach zutreffender Ansicht beschränkt sich die Zentralstellenaufgabe deshalb auf die koordinierende Tätigkeit (vgl. zum Ganzen ausführlich Ibler in: Maunz/Dürig, Grundgesetz-Kommentar, 79. EL Dezember 2016, Art. 87 Rn. 121 und 131). Das schließt nach dieser in der Literatur vertretenen Auffassung nicht aus, der Zentralstelle Exekutivbefugnisse einzuräumen, auf deren Grundlage sie personenbezogene Daten erheben, speichern und nutzen darf. Diese Exekutivbefugnisse darf der Gesetzgeber ihr auf Grundlage des Art. 87 Abs. 1 S. 2 aber nur einräumen, wenn und soweit diese erforderlich sind, um die Koordinierungsaufgabe zu erfüllen.



Entsprechend dieser Koordinierungsaufgabe waren die Datenerhebungsbefugnisse in § 7 BKAG ursprünglich darauf beschränkt, Daten bei öffentlichen Stellen, insbesondere Polizeidienststellen zu sammeln, um diese – ggf. in Zentralstellendateien – zusammenfassen und im polizeilichen Verbund an die zuständigen Behörden steuern zu können. Die Befugnis, Daten bei privaten Dritten erheben zu können, wurde erst später mit den Terrorismusbekämpfungsgesetzen hinzugefügt (zur Entwicklung siehe Graulich in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 1. Auflage 2014, § 7 BKAG Rn. 1). Mit der Änderung durch das Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes kommt es zu einer weiteren Ausdehnung (dazu unten b).

Welche Daten für die Koordinierung erforderlich sind, bestimmt das Gesetz nicht näher. Durch den Verweis auf § 2 BKAG lässt § 7 Abs. 2 BKAG es allgemein ausreichen, die Polizeibehörden der Länder zu „unterstützen“. Die tatbestandliche Formulierung des § 2 Abs. 2 Nr. 1 BKAG, nach der das Bundeskriminalamt „alle hierfür erforderlichen Informationen zu sammeln und auszuwerten“ hat, ist insofern ähnlich weit gefasst, wie die Formulierung in § 3 Abs. 1 BVerfSchG, die ebenfalls allgemein von „Sammlung und Auswertung“ von Informationen spricht, dort bezogen auf verfassungsfeindliche Bestrebungen.

Aus dem Begriff der „Verhütung“ in § 2 Abs. 1 BKAG ergibt sich, dass unter anderem die Informationssammlung im Vorfeld von Gefahren bzw. Straftaten umfasst ist. Ebenso ist aus dem Umkehrschluss aus § 7 Abs. 2 S. 3 BKAG herzuweisen, dass die Datenerhebung durch das BKA nicht auf bereits laufende Strafverfahren begrenzt ist. Vielmehr kann das BKA demnach bereits vor Einleitung eines Strafverfahrens – und bevor ein entsprechender Anfangsverdacht vorliegt – personenbezogene Daten erheben. Damit kann dieses unabhängig von den Voraussetzungen der §§ 161, 163 StPO Ermittlungen durchführen, auch zu Personen, gegen die aktuell kein Strafverfahren geführt wird. Zusätzlich ergibt sich dies aus dem Regelungszusammenhang mit § 8 BKAG, der die Informationssammlung zu Zwecken der Vorsorge ermöglicht. Untermauert wird dies durch die Formulierung, nach der das Ziel der Datenerhebung unter anderem sein darf, bereits vorhandene Sachverhalte zu ergänzen. Dies betrifft auch bereits abgeschlossene Verfahren, die aus Gründen der Gefahren- bzw. Strafverfolgungsvorsorge gespeichert sind, insbesondere gemäß § 8 BKAG. Bei diesen kann es sich um Personen handeln, bei denen die gegen sie laufenden Strafverfahren endgültig eingestellt oder die aus Mangel an Beweisen freigesprochen wurden (vgl. § 8 Abs. 3 BKAG, dazu ausführlicher unten 3.).

Mein Eindruck aus der Praxis anlässlich einer kürzlich durchgeführten datenschutzrechtlichen Kontrolle bestätigt insoweit, dass die Erhebungsschwelle



niedrig ist. Ein Prüfbericht hierzu liegt derzeit noch nicht vor. Allerdings erhebt das BKA Daten nicht völlig anlasslos, da in der Regel Anfragen oder Hinweise anderer Stellen vorliegen.

#### *(b) Auswertung und Analyse, Anreicherung von Daten*

Ziel der Datenerhebung ist es, vorhandene Sachverhalte zu ergänzen oder sonst Daten „zu Zwecken der Auswertung“ zu erheben.

Vorhandene Sachverhalte sind sämtliche beim Bundeskriminalamt gespeicherten personenbezogenen Daten. Diese können bislang in Amts-, Zentralstellen- und Verbunddateien gespeichert sein.

Damit kann das BKA praktisch ohne tatbestandliche Begrenzungen beliebig Daten zu Personen „anreichern“, die nur aus Vorsorgegründen bereits gespeichert sind. Dies umfasst im Zusammenwirken mit den übrigen Vorschriften auch Personen, bei denen die gegen sie geführten Strafverfahren eingestellt oder die freigesprochen worden sind.

Ebenfalls weit zu lesen ist das Tatbestandsmerkmal „oder sonst zu Zwecken der Auswertung“. Nach der Literatur erlaubt dies dem BKA nicht, völlig neue Erkenntnisse zu erheben, sondern es muss auch insoweit an den vorhandenen Informationsstand anknüpfen (Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, Mannheim 2009, S. 23 m.w.N.; Kugelmann, BKA-Gesetz, 1. Auflage 2014, § 7 Rn. 10). Nach dem Sinn und Zweck der bisher bestehenden Vorschriften ist dieser Ansicht zuzustimmen.

Dem entspricht nach meinem Eindruck die bisherige Praxis. Insoweit ist zu konstatieren, dass Daten bislang nicht erhoben werden, um diese in großem Umfang in Analysedateien zu stellen. Das ändert allerdings nichts an dem wenig eingegrenzten Wortlaut, der eine Änderung dieser Praxis in der Zukunft jedenfalls möglich erscheinen lässt.

Das Gesetz zur Neustrukturierung des Bundeskriminalamts stellt die weitreichenden Möglichkeiten zur Datenerhebung nochmals deutlicher heraus. Die neuen §§ 9 Abs. 1, 10 Abs. 1 BKAG n.F. nennen jetzt nicht nur ausdrücklich den Zweck der „Analyse“ neben der „Auswertung“, sondern enthalten zusätzlich jeweils eine neue Verweisung auf § 2 Abs. 6 BKAG. Danach darf das BKA eigene Daten zu folgenden Zwecken erheben:



- „1. strategische und operative kriminalpolizeiliche Analysen, Statistiken, einschließlich der Kriminalstatistik, und Lageberichte zu erstellen und hierfür die Entwicklung der Kriminalität zu beobachten und auszuwerten,*  
*2. die erforderlichen Einrichtungen für alle Bereiche kriminaltechnischer Untersuchungen und für kriminaltechnische Forschung zu unterhalten und die Zusammenarbeit der Polizei auf diesen Gebieten zu koordinieren,*  
*3. polizeiliche Methoden und Arbeitsweisen der Kriminalitätsbekämpfung zu erforschen und zu entwickeln sowie*  
*4. angemessene organisatorische und technische Vorkehrungen sowie Verfahren zur Umsetzung von Datenschutzgrundsätzen, insbesondere der Grundsätze der Datenvermeidung und Datensparsamkeit, einschließlich der Pseudonymisierung, zu entwickeln.“*

Weder Anlass noch Umfang der hierfür erforderlichen Daten sind näher eingegrenzt. Ebenso fehlen Angaben zum betroffenen Personenkreis. Damit darf das Bundeskriminalamt nach dem Wortlaut der Vorschrift alle personenbezogenen Daten bei öffentlichen oder privaten Stellen erheben, die es benötigt, um strategische oder operative Analysen, Lageberichte oder Statistiken zu erstellen.

Beispielsweise schließt es der Wortlaut nicht aus, zu diesem Zweck Daten darüber zu erheben, welche Personen die Polizeibehörden im Umfeld bestimmter Kriminalitätsbereiche vermuten, und zu diesen Personen weitere Daten zu erheben und in Prüfdateien hinzuzuspeichern (vgl. §§ 18 Abs. 3, 19 Abs. 3 BKAG n.F.). Einzelne Personen könnte das BKA in Lageberichte aufnehmen, die bundesweit an alle Polizeibehörden verteilt werden. Die Neufassung könnte so ausgelegt werden, hier sehr weit in das Vorfeld reichende Möglichkeiten zu eröffnen, auch wenn dafür nach meinem Eindruck seitens des BKA kein praktischer Bedarf besteht.

Im Ergebnis begrenzt § 7 Abs. 2 BKAG deshalb nur wenig, welche Daten das Bundeskriminalamt erheben darf. Dies wirft aus meiner Sicht erhebliche verfassungsrechtliche Fragen auf (kritisch etwa Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, Mannheim 2009, S. 23). Zu Recht wird deshalb betont, die Generalklausel zur Datenerhebung für Zwecke der Zentralstelle sei zu weit und zu pauschal, um schwerer wiegende Grundrechtseingriffe zu rechtfertigen (Bäcker a.a.O.). In der Praxis berücksichtigt das BKA dies bislang nach meinem Eindruck.





*(c) Beispiele für Zentralstellentätigkeit*

Ein Beispiel aus der Praxis für die Zentralstellentätigkeit ist die verfahrensübergreifende Auswertung von Funkzellenabfragen aus verschiedenen Strafverfahren. Geprüft habe ich eine von mehreren Dateien, in der solche Daten zusammengeführt und abgeglichen werden (vgl. meinen 26. TB, Nr. 10.2.9.3). Die Generalklausel des § 7 Abs. 2 BKAG dient in solchen Zusammenhängen dazu, die Daten der Polizeibehörden zu erfassen und in einer auf § 7 Abs. 1 BKAG gestützten Datei zentral zu speichern und auszuwerten. Ergeben sich Kreuztreffer, hat das BKA – ggf. parallel zu den jeweiligen Ermittlungsbehörden – die gesetzliche Befugnis, Bestandsdaten zu den festgestellten Anschlüssen abzufragen. Die Datei habe ich gemäß § 25 BDSG beanstandet. Denn die Generalklausel in § 7 Abs. 1 BKAG rechtfertigt nach meiner Auffassung wegen ihrer allgemeinen Formulierung keine intensiven Grundrechtseingriffe, wie hier die Speicherung von Daten aus einer Vielzahl von Funkzellenabfragen. Die Eingriffsintensität entspricht nach meiner Ansicht der einer Rasterfahndung, wobei hier gleichzeitig Art. 10 GG betroffen ist. Meine datenschutzrechtlichen Bedenken hatte ich bereits vor Einrichtung der Datei schriftlich mitgeteilt, als mich das Bundesministerium des Innern zur Errichtungsanordnung angehört hatte. Dieses hat die Errichtungsanordnung aber gleichwohl erlassen. In diesem Beispiel hat das Bundeskriminalamt aber nicht selbst Bestandsdaten zu den festgestellten Rufnummern erhoben, sondern die Datenabgleichsergebnisse den Ländern zurückgemeldet, die dann die entsprechenden Möglichkeiten hatten.

Weitere Beispiele aus meiner datenschutzrechtlichen Kontrollpraxis sind Anfragen ausländischer Polizeidienststellen, ob beispielsweise bestimmte Personen oder Zusammenhänge in der Bundesrepublik Deutschland polizeilich bekannt sind. Die ausländischen Behörden erbitten diese Informationen, um dort strafrechtliche Ermittlungen zu führen. Das BKA fragt dann bei den Behörden der betroffenen Bundesländer an und steuert die Ergebnisse unter den Voraussetzungen des § 14 BKAG an die anfragende ausländische Stelle. Diese kann auf der Grundlage der Informationen dann auch ohne formelles Rechtshilfeersuchen weiter ermitteln. Dieses Beispiel zeigt, dass innerhalb der Koordinierungsaufgabe polizeiliche Datenübermittlungen gegebenenfalls parallel zu den strafrechtlichen Ermittlungsverfahren stattfinden. Gegenstand einer solchen Tätigkeit sind auch Bestandsdatenabfragen.

Nicht auszuschließen ist insoweit, dass Strafermittlungen durch nachrichtendienstliche strategische Überwachungen ausgelöst werden, bei denen zum Bei-



spiel eine IP-Adresse oder eine Rufnummer auffällt. Dies könnte zwar schwere Straftaten betreffen, ist darauf aber keineswegs begrenzt.

## (2) spezifische Befugnisse zur Bestandsdatenabfrage

### (a) § 7 Abs. 3 S. 1 BKAG (§ 10 Abs. 1 S. 1 BKAG n.F.)

Die Bestandsdatenabfrage gemäß § 7 Abs. 3 S. 1 BKAG umfasst die gemäß §§ 95 und 111 TKG erhobenen Daten. Durch die tatbestandliche Anknüpfung an § 7 Abs. 2 BKAG dient sie den oben beschriebenen Zwecken, ist also tatbestandlich nur wenig eingegrenzt und auch ohne eine Gefahrenlage oder den Verdacht einer Straftat oder Ordnungswidrigkeit zulässig (siehe oben).

Damit ist die Bestandsdatenabfrage in unterschiedlich eingriffsintensiven Zusammenhängen denkbar. Sie kann beispielsweise auf der einen Seite lediglich dazu dienen, bereits vorhandene Daten aktuell zu halten (z.B. mit der Frage, ob eine bestimmte Rufnummer noch immer einer bestimmten Person zugewiesen ist). Auf der anderen Seite ist denkbar, dass die Daten mit anderen Daten umfangreich verknüpft und ausgewertet werden. Dies kann etwa bei „relevanten“ Personen festgestellte ausgehende oder eingehende Anrufe betreffen oder etwa bei einem sichergestellten oder überwachten Webserver festgestellte Aufrufe bestimmter Internetseiten. Der Wortlaut der gesetzlichen Vorschriften würde es prinzipiell erlauben, die Bestandsdaten zu diesen Kontakten abzufragen. Zu Zwecken der Ergänzung vorhandener Sachverhalte und der Auswertung und Analyse wäre dann denkbar, die Daten als „Prüffall“ zu speichern, zumindest nach der gesetzlichen Neuregelung der §§ 18 Abs. 3 und 19 Abs. 3 BKAG n.F. (siehe oben) oder sogar als Daten zu Kontakt- und Begleitpersonen.

### (b) § 7 Abs. 3 S. 2 BKAG (§ 10 Abs. 1 BKAG n.F.), Zugangssicherungs-codes

Ein praktischer Bedarf für diese Vorschrift besteht nicht und die Reichweite der Vorschrift ist unklar. Auf der einen Seite stellt auch sie auf die Zentralstellenfunktion des Bundeskriminalamts ab. Auf der anderen Seite verlangt sie zusätzlich, dass „die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen“. Welche Nutzungen dies sein sollen, nennt die Vorschrift hingegen nicht. Insofern umschreibt sie nur sehr ungenau, zu welchen Zwecken das BKA Zugangscodes in seiner Funktion als Zentralstelle erheben darf.



Vor allem nennt sie keine zulässige Nutzung, die mit der Zentralstellenaufgabe des Bundeskriminalamts in Zusammenhang steht:

Passwörter, PIN und PUK können nötig sein, um auf Endgeräte oder Speicher zugreifen zu können (z.B. auf Cloud-Dienste). Insofern ist mit der „Nutzung“ der Daten offenbar gemeint, diese Daten als Zugangsschlüssel bei einer weitergehenden Maßnahme zu erlauben. Eine Vorschrift zur Erhebung der Zugangsschlüssel ist daher nur dann in sich logisch, wenn das betreffende Gesetz auch weitere Maßnahmen vorsieht, die eine „Nutzung“ der entsprechenden Bestandsdaten – hier in Form von Zugangscodes – sachlogisch voraussetzen. Im polizeilichen Kontext sind jedoch insoweit nur Maßnahmen zur Abwehr einer konkreten Gefahr und Maßnahmen innerhalb eines strafprozessualen Ermittlungsverfahrens denkbar. Eine Datenerhebung zu Zwecken der Zentralstellenaufgaben, die einen – ggf. heimlichen – Zugriff auf Telekommunikationsendgeräte (entweder als Telekommunikationsüberwachung oder als Beschlagnahme) oder auf in der Cloud gespeicherte Daten umfasst, ist aber im Bundeskriminalamtgesetz nicht vorgesehen. Eine Ausnahme dazu bilden lediglich die Vorschriften zur Bekämpfung des internationalen Terrorismus (insb. § 20k BKAG). Dort sieht aber § 20b Abs. 3 BKAG eine eigenständige Befugnis zur Bestandsdatenabfrage vor. Für strafprozessuale Maßnahmen enthält die Strafprozessordnung mit § 100j ebenfalls eine eigene Vorschrift. § 7 Abs. 2 BKAG ist als Grundlage für intensive Grundrechtseingriffe – wie oben dargelegt – nicht geeignet. Daher kann das BKA auf Grundlage dieser Vorschrift keine Beschlagnahmen vornehmen oder gar auf Telekommunikationsinhaltsdaten zugreifen.

Eine extensivere Auslegung der Vorschrift, nach der die Daten nur deshalb erhoben werden sollten, um diese für eine bloß potentiell denkbare Nutzung in Dateien zu speichern, wäre unverhältnismäßig. Im Ergebnis ergibt § 7 Abs. 3 S. 2 BKAG schon aus sachlogischen Gründen keinen Sinn, weil es keine durch die Vorschrift vorausgesetzten – konkreten – Nutzungsmöglichkeiten gibt.

Dementsprechend besteht nach meiner Einschätzung beim BKA keinerlei praktischer Bedarf für diese Vorschrift.

*(c) § 7 Abs. 4 BKAG (§ 10 Abs. 2 BKAG n.F.), dynamische IP-Adressen*

Die Abfrage dynamischer IP-Adressen ist ein erheblicher Grundrechtseingriff. Zum einen können die Telekommunikationsanbieter den hinter der IP-Adresse stehenden Anschluss nur ermitteln, wenn sie auf Verkehrsdaten zugreifen und



insofern in den Schutzbereich des Art. 10 GG eingreifen (BVerfG NJW 2012, 1419). Zum anderen können die IP-Adressen mit weiteren Informationen verknüpft sein, auf die die Behörden Zugriff haben, sei es durch der Bestandsdatenabfrage vorausgegangene oder nachfolgende Maßnahmen oder durch den Datenaustausch zwischen Sicherheitsbehörden.

Menschen hinterlassen im Internet mehr Spuren denn je. War es vor einem Jahrzehnt noch die mehr oder weniger gelegentliche Sitzung am heimischen Computer, so trägt doch die große Mehrheit der Menschen inzwischen einen leistungsfähigen Rechner permanent in der Tasche. Dieser ist ständig über Mobilfunk mit dem Internet verbundenen. Die dabei entstehenden Daten werden in dem kaum überschaubaren Netzwerk durch eine Vielzahl von Servern aufgezeichnet und erlauben umfangreiche Persönlichkeitsprofile. Diese können Aufschluss über aufgerufene Internetangebote, mithin die Interessen der betroffenen Person geben. Sie können ebenso die von ihr genutzten Dienste zur Kommunikation mit anderen Menschen oder in sozialen Netzwerken betreffen. Dies kann ihre persönlichen, aber auch ihre gesellschaftlichen oder politischen Aktivitäten offenlegen. Je größer die Zugriffsmöglichkeiten auf diese Daten sind, desto eher sind tiefergehende Analysen zu der Person oder gar Profilbildungen möglich.

Bei einer engen Auslegung könnte eine vereinzelte Abfrage durch das BKA in seiner Zentralstellenfunktion noch als verhältnismäßig anzusehen sein. So wäre etwa der Fall denkbar, in dem das BKA auf einer „Internetstreife“ Erkenntnisse über den Anfangsverdacht einer Straftat oder einer Gefahrenlage erhält (z.B. Bombendrohung, Verkauf von gestohlenen Kreditkartendaten etc.). Dann wäre die Abfrage der IP-Adresse ggf. ein erster Anknüpfungspunkt, um den Sachverhalt an eine zuständige Strafverfolgungs- oder Polizeibehörde weiterzuleiten. Auf eine derart enge Auslegung beschränkt sich der Wortlaut allerdings nicht.

Auch die Datenerhebung nach § 7 Abs. 4 BKAG knüpft nicht an ein konkretes Ermittlungsverfahren oder eine Gefahrenlage an. Der Wortlaut lässt es ausdrücklich zu, den hinter der dynamischen IP-Adresse stehenden Anschluss zu erheben, um „vorhandene Sachverhalte zu ergänzen“ oder sonst zu „Zwecken der Auswertung“. Die Auswertung kann sich etwa darauf beziehen, die Kontakte und das Umfeld bestimmter „polizeibekannter“ Personen auszuleuchten, auch ohne an ein konkretes Strafverfahren anzuknüpfen (Ergänzung vorhandener Sachverhalte zu Zwecken der Auswertung). Soweit eine IP-Adresse einer natürlichen Person zugewiesen ist, ist die Eingriffsintensität insofern allerdings weniger danach zu differenzieren, ob es sich um eine dynamische oder eine statische IP-Adresse handelt. Faktisch dürften allerdings dynamische IP-



Adressen häufiger natürliche Personen bzw. deren privates Surfverhalten betreffen.

Wie bereits oben dargelegt, kann das BKA Nutzern zugewiesene IP-Adressen in Dateien der Gefahrenvorsorge gemäß § 8 BKAG speichern (oben b). § 2 Abs. 1 Nr. 3 BKADV erlaubt ausdrücklich, auch dynamische IP-Adressen zu speichern.

### (3) Potentielle Folgen für die Betroffenen im künftigen Recht

Wie dargelegt, lassen es die angegriffenen Vorschriften genügen, wenn das Ziel der Datenerhebung gemäß § 10 BKAG n.F. lediglich darin besteht, „vorhandene Sachverhalte“ zu ergänzen bzw. sonst zu Zwecken der „Auswertung und Analyse“ Daten zu erheben. Insofern sind die Erhebungsbefugnisse des § 7 Abs. 2 bis 7 BKAG bzw. §§ 9, 10 BKAG n.F. nicht isoliert zu betrachten, sondern stets im Zusammenhang mit den Möglichkeiten der weiteren Verwendung der erhobenen Daten.

#### (a) *Umfassendere Informationsbestände*

Intensive Grundrechtseingriffe können sich nicht nur aus dem jeweiligen Ermittlungseingriff selbst, sondern auch aus der weiteren Verwendung der erhobenen Daten ergeben. Eine eigenständige Eingriffswirkung entfaltet auch ihre Speicherung in elektronischen Dateien. Dies betrifft die spezifisch breitenwirksamen Grundrechtsgefährdungspotenziale, insbesondere solche der elektronischen Datenverarbeitung. Das Bundesverfassungsgericht hat hierzu in zahlreichen Entscheidungen Stellung genommen, auf die es in der Grundsatzentscheidung zum BKAG vom 20.04.2016 verweist (BVerfG NJW 2016, 1781, Abs. Nr. 103; vgl. BVerfGE 100, 313, 358 ff.; 115, 320, 341 ff.; 125, 260, 316 ff.; 133, 277, 335 ff.). Es verweist auf seine ständige Rechtsprechung zur Zweckbindung und Zweckänderung (Abs. Nr. 276, beginnend mit einem Verweis auf BVerfGE 65, 1 – Volkszählung). Der Gesetzgeber nimmt offenbar an, das Bundesverfassungsgericht wolle mit der Grundsatzentscheidung zum BKAG wesentliche für die elektronischen Datenbanksysteme der Polizeien entwickelten Grundsätze zurücknehmen, weil es das bisherige „vertikale“ Datenschutzkonzept durch ein „horizontal“ wirkendes ersetzt habe (vgl. BT-Drs. 18/11163, S. 73). Dafür spricht jedoch nach hiesiger Auffassung nichts. Im Gegenteil. Das Gericht weist zutreffend auf Folgendes hin:



*„Dabei hat der Gesetzgeber in seine Abwägung auch die Entwicklung der Informationstechnik einzustellen, die die Reichweite von Überwachungsmaßnahmen zunehmend ausdehnt, ihre Durchführbarkeit erleichtert und Verknüpfungen erlaubt, die bis hin zur Erstellung von Persönlichkeitsprofilen reichen.“ (BVerfG NJW 2016, 1781, Abs. Nr. 99).*

Daher lassen sich auch scheinbar harmlose Datenerhebungen nicht unabhängig von der Frage des Verwendungszusammenhangs beurteilen. Dies gilt gerade dann, wenn der Gesetzgeber bereits die Erhebung nicht von einem konkreten Anlass abhängig macht, sondern ihre Voraussetzungen an das Ziel der Weiterverarbeitung anknüpft (Ergänzung vorhandener Sachverhalte, Auswertung und Analyse).

§§ 13 ff. BKAG n.F. sehen ein neues Informationssystem beim BKA vor, welches die bisherigen Amts- und Zentralstellendateien ablöst. Gleichzeitig sehen §§ 29 ff. BKAG n.F. einen neuen bundesweiten Informationsverbund vor. Der künftige Informationsverbund und das Informationssystem werden nicht mehr in logische Dateien gegliedert sein. Dies war in den bisherigen Verbundsystemen INPOL und PIAV ebenso vorgesehen, wie bei bisherigen Zentralstellendateien beim BKA. Alle Daten kommen stattdessen ohne nähere Zweckbestimmung in einen „großen Topf“ und können miteinander abgeglichen werden. Die Methoden des Datenabgleichs sind nicht eingegrenzt. Alle Daten und Datenfelder sind personenübergreifend beliebig miteinander verknüpfbar. Jeder Abgleich kann zu weiteren Datenverknüpfungen führen und damit wiederum die Speicherdauer perpetuieren.

Gemäß § 13 Abs. 2 BKAG kann das BKA die Daten ausdrücklich zur „polizeilichen Informationsverdichtung“ durch Abklärung von Hinweisen und Spurenansätzen, zur Durchführung von Abgleichen von personenbezogenen Daten und zur Unterstützung bei der Erstellung von strategischen Analysen und Statistiken verwenden. Daraus ergibt sich, dass das Bundeskriminalamt alle Daten im Informationssystem und im Informationsverbund umfassend verknüpfen, abgleichen und mit technischen Verfahren auswerten und analysieren darf.

Dies ermöglicht Systeme, die nicht mehr personenorientierte Datensätze speichern, sondern unabhängig von Dateigrenzen ereignisorientiert arbeiten: Die Daten zu einer Person werden mit einem Ereignis verknüpft, das seinerseits mit weiteren Personen, Ereignissen, Institutionen oder Sachen verknüpft wird. Die Zahl der Verknüpfungsebenen ist nicht begrenzt. Damit könnten die zu einer Person gespeicherten Daten zunehmend diffundieren.



Zusätzlich erlaubt § 16 Abs. 4 BKAG dem BKA, die Daten aus dem Informationssystem mit anderen Daten abzugleichen, auf die es zur Erfüllung seiner Aufgaben „zugreifen“ darf. Dies setzt lediglich einen Grund zu der Annahme voraus, dies sei zur Erfüllung einer Aufgabe erforderlich.

Damit ist nicht nur der interne Abgleich innerhalb der polizeilichen Systeme zulässig. Vielmehr können auch externe Systeme einbezogen werden, auf die das BKA Zugriff hat (z.B. Europol, SIS, VIS, ggf. künftige Systeme, die auf europäischer Ebene diskutiert oder geschaffen werden, wie etwa PNR zu Flugpassagieren, Entry-Exit-System, ETIAS).

Nach bisherigem Recht sind gemäß § 34 BKAG für jede Datei in einer Errichtungsanordnung Rechtsgrundlage und Zweck der Datei festzulegen. Vor allem hieraus ergibt sich die – zumindest logische – Trennung der Datenbestände in verschiedene Dateien, die jeweils spezifischen Zwecken dienen. Jeweils auf den Dateizweck bezogen sind insbesondere der weitere Inhalt der Datei, die Möglichkeiten, die Daten zu erschließen und Prüffristen und Speicherdauer festzulegen. Die Pflicht, dies in Errichtungsanordnungen festzulegen, ist im künftigen Recht ersatzlos gestrichen. Damit fällt zudem eine wesentliche Grundlage für datenschutzrechtliche Kontrollen durch die Landebeauftragten für den Datenschutz und durch mich weg. Die Errichtungsanordnungen dienten bei Kontrollen als wesentlicher Maßstab für die datenschutzrechtliche Bewertung und waren ein effektives Hilfsmittel, Datenbestände und die jeweiligen polizeilichen Ziele der Datenverarbeitung im Überblick zu behalten.

Vielmehr sollen nur noch Kategorien der Datenverarbeitung „beschrieben“ werden (nicht: „festgelegt“, § 80 Abs. 1 BKAG n.F.). Die Polizeibehörden sind damit nicht mehr verpflichtet, konkret festzulegen, welchem Zweck solche „Kategorien von innerhalb seines Informationssystems durchgeführten Tätigkeiten der Datenverarbeitungen“ dienen soll. Deshalb sind die tatsächlichen Folgen derzeit kaum abschätzbar, zumal mir noch keine konkreten Pläne für ein neues Informationssystem vorliegen.

#### *(b) „Prüffälle“*

Künftig darf das BKA Personen darüber hinaus für bis zu zwei Jahre als „Prüffälle“ speichern, um zu klären, ob diese als Beschuldigte, Verdächtige oder andere Personen – also z.B. als Kontakt- und Begleitpersonen oder als Hinweisgeber – in Betracht kommen (§§ 18 Abs. 3, 19 Abs. 3 BKAG n.F.). Ob derartige



Personen auf Grundlage des bisherigen § 7 Abs. 1 BKAG gespeichert werden dürfen, war bislang streitig. Das BKA und das Bundesministerium des Innern teilten bisher meine Auffassung nicht, dass es nach der bisherigen Rechtslage unzulässig ist, Prüffälle mit dem Ziel der „Anreicherung“ von Daten zu speichern, ohne dass gleichzeitig die Voraussetzungen des § 8 Abs. 2 bzw. Abs. 5 BKAG vorliegen (siehe dazu meinen 26. Tätigkeitsbericht Nr. 10.2.9.3, S. 111). Dies ist mit der neuen Rechtslage insoweit klargestellt. Die Datenerhebungen nach §§ 9, 10 BKAG n.F. dienen auch bei „Prüffällen“ dazu, vorhandene Sachverhalte zu ergänzen (also „anzureichern“) bzw. Daten auszuwerten und zu analysieren. Dies kann auch Kontakt- und Begleitpersonen und die weiteren in § 19 BKAG n.F. genannten Personengruppen betreffen.

Die Anreicherung von Informationen und die darauf basierende Analyse ist nur dann als verhältnismäßig anzusehen, wenn die Betroffenen dafür einen hinreichenden Anlass gegeben haben, der Zweck der Datensammlung auf diesen Anlass Bezug nimmt und der Speicherzeitraum eng begrenzt ist. Dies kann im Strafverfahren – je nach Gewicht des Vorwurfs und Umfang der Datenverarbeitung – ein strafrechtlicher Anfangsverdacht sein. Ebenso kann dies bei Gefahren zulässig sein. Dabei sind dann die Eintrittswahrscheinlichkeit und das Gewicht der betroffenen Rechtsgüter ins Verhältnis zum Umfang der Speicherung und des Analyseumfangs zu setzen. Hierzu enthalten die angegriffenen Vorschriften im Zusammenwirken mit den Vorschriften zur Datenverarbeitung jedoch nach hier vertretener Auffassung nur ungenaue Vorgaben. Dies gilt umso mehr, als die bislang als wesentliche Verfahrenssicherung vorgesehenen Errichtungsanordnungen künftig wegfallen.

#### (4) Zweifel an Normenklarheit und Verhältnismäßigkeit

Die Zusammenhänge zwischen der Erhebung und der weiteren Verwendung personenbezogener Daten hat das Bundesverfassungsgericht in ständiger Rechtsprechung hervorgehoben. Sie waren gerade auch der Anlass, hinsichtlich der Regelungen zur Bestandsdatenabfrage entsprechend zu differenzieren (BVerfG NJW 2012, 1419, 1422, Abs. Nr. 123 m.w.N.).

Zutreffend weist die Entscheidung des Bundesverfassungsgerichts auf die für sich genommen beschränkte Aussagekraft von Bestandsdaten hin, insbesondere, weil diese für sich genommen keine Profilbildung ermöglichen (BVerfG NJW 2012, 1419, S. 1424, Abs. Nr. 139 und S. 1426 f., Abs. Nr. 159). Folgerichtig war insofern § 113 TKG trotz der weit umschriebenen Verwendungsmöglichkeiten zumindest in seiner Grundstruktur nicht zu beanstanden (BVerfG NJW





2012, 1419, 1427, Abs. Nr. 164), da er insoweit nur als Öffnungsklausel verstanden wird und die näheren Voraussetzungen des Zugriffs im jeweiligen Fachrecht zu regeln ist (BVerfG NJW 2012, 1419, 1428, Abs. Nr. 170). Ebenso folgt daraus aber, dass die daran anknüpfenden Vorschriften zur Erhebung und weiteren Verwendung der Daten im jeweiligen Zusammenhang darauf zu überprüfen sind, welche potentiellen Folgen sich für die Betroffenen ergeben.

Wie oben ausführlich dargelegt, sind die Erhebungsbefugnisse gemäß § 7 Abs. 2 bis 7 BKAG bzw. §§ 9, 10 BKAG n.F. in Verbindung mit den Vorschriften zur weiteren Speicherung und Nutzung der Daten sehr weit gefasst. Sie setzen weder einen Anfangsverdacht einer Straftat oder Ordnungswidrigkeit voraus noch den Verdacht einer konkreten Gefahr. Vielmehr vermischen sie tatbestandlich Voraussetzungen und weitere Folgen, indem sie lediglich voraussetzen, dass die Daten zur „Ergänzung vorhandener Sachverhalte“ bzw. zur „Auswertung und Analyse“ durch die Zentralstelle erforderlich sind. Dies schließt gerade nicht aus, dass die Daten als Baustein in Profilbildungen zu einzelnen Personen einfließen. Dies erhöht die Eingriffsintensität erheblich.

*„Bezogen auf die Gefahrenabwehr, in die der Gesetzgeber die Gefahrenvorsorge gerade nicht einbezogen hat, ergibt sich bei verständiger Auslegung das Erfordernis einer „konkreten Gefahr“ im Sinne der polizeilichen Generalklauseln als Voraussetzung für solche Auskünfte. Diese Schwelle ist freilich niedrig und umfasst auch den Gefahrenverdacht. Ebenso beschränkt sie Auskünfte nicht von vornherein auf Polizeipflichtige im Sinne des allgemeinen Polizei- und Ordnungsrechts. Sie ist damit jedoch nicht so entgrenzt, dass sie angesichts des gemäßigten Eingriffsgewichts unverhältnismäßig wäre.“ (BVerfG NJW 2012, 1419, 1429, Abs. Nr. 177).*

Da es insoweit aber an tatbestandlichen Begrenzungen fehlt, die den Anlass der Datenerhebung normenklar und verhältnismäßig regeln, bestehen erhebliche Zweifel an der Verfassungsmäßigkeit des § 7 Abs. 2 – 7 BKAG bzw. der §§ 9, 10 BKAG n.F. Besonders gilt dies im Hinblick auf die nicht konkret eingegrenzten Abfragen von Zugangscodes nach § 7 Abs. 3 S. 3 BKAG bzw. § 10 Abs. 1 S. 2 BKAG n.F. (vgl. dazu BVerfG NJW 2012, 1419, 1430, Abs. Nr. 185).



## b) § 7 ZFdG

Zu § 7 ZFdG gilt weitgehend das oben zu § 7 BKAG Gesagte. Allerdings ist der Wortlaut des § 7 ZFdG noch allgemeiner formuliert.

Er nennt nicht den Zweck, vorhandene Sachverhalte zu ergänzen oder sonstige Zwecke der Auswertung. Er knüpft an die „Aufgabe als Zentralstelle nach § 3“ an (§ 7 Abs. 5 S. 1 ZFdG) und ist nicht auf bestimmte Teilbereiche beschränkt. Die Aufgaben der Zentralstelle sind in elf Absätzen in § 3 ZFdG beschrieben. Dies sind unter anderem:

- Entdeckung unerkannter Steuerfälle,
- Verhütung und Verfolgung von Straftaten und Ordnungswidrigkeiten (Abs. 1),
- einzelfallunabhängige Marktbeobachtung (Beobachtung des innerstaatlichen, innergemeinschaftlichen, grenzüberschreitenden und internationalen Waren-, Kapital- und Dienstleistungsverkehrs, Abs. 2),
- Informationsverarbeitung der Zollfahndung (Abs. 3),
- Koordinierung und Lenkung von Ermittlungen der Zollfahndungsämter (Abs. 5),
- die internationale Zusammenarbeit (Abs. 6)
- zollfahndungsspezifische Analysen, Statistiken und Lagebildern (Abs. 8 Nr. 4).

Zur Zentralstellenaufgabe gehört gemäß § 3 Abs. 9 ZFdG ausdrücklich, alle dafür notwendigen Informationen zu sammeln und auszuwerten. Über diese Vorschrift werden die Zentralstellenaufgaben gleichzeitig mit den Aufgaben des Zollkriminalamts nach §§ 4 und 5 ZFdG verknüpft (eigene Strafverfolgungsaufgaben, Sicherungs- und Schutzmaßnahmen). Unklar ist, wie sich die Zentralstellenaufgabe nach § 3 Abs. 2 i.V.m. Abs. 9 ZFdG zur Datensammlung nach § 9 ZFdG verhält, der insoweit eine eigenständige Rechtsgrundlage für die Datenerhebung vorsieht, allerdings nicht die Bestandsdatenabfrage. Diese kann dann über § 7 Abs. 5 bis 9 ZFdG durchgeführt werden. Dies umfasst vom Wortlaut der Vorschrift die Beobachtung quasi des gesamten innerstaatlichen, innergemeinschaftlichen, grenzüberschreitenden und internationalen Waren-, Kapital- und Dienstleistungsverkehrs. Nur in der Überschrift des § 9 ZFdG ist dies auf „bestimmte“ Verkehre beschränkt, im Tatbestand jedoch nicht.



### 3. Polizeiliche Befugnisse zur Gefahrenabwehr und zur Strafverfolgung

#### a) § 22a BPolG

§ 22a BPolG ist ebenfalls weit gefasst. Die Bestandsdatenabfrage ist nach dieser Vorschrift nicht durchgehend daran geknüpft, ob eine konkrete Gefahr vorliegt, wie dies verfassungsrechtlich gefordert ist. § 22a Abs. 1 BPolG stellt die Voraussetzungen der Bestandsdatenabfrage mit denen der Erhebungsgeneral Klausel in § 21 Abs. 1 und 2 BPolG gleich. Maßgebliches Kriterium ist danach lediglich die Erforderlichkeit für die Aufgabenerfüllung bzw. ein weiter Tatbestand zur Straftatenbekämpfung im Vorfeld.

§ 22a Abs. 1 i.V.m. § 21 Abs. 1 BPolG lässt es damit ausreichen, dass die Bestandsdatenabfrage erforderlich ist, um eine – irgendeine – Aufgabe der Bundespolizei zu erfüllen. Die Vorschrift differenziert nicht näher und schränkt die Bestandsdatenabfrage nicht auf bestimmte Aufgaben ein. Daher entstehen Unklarheiten, die durch Auslegung in der Anwendungspraxis gelöst werden müssen. So ist beispielhaft die Frage zu stellen, wie der Verweis auf die Aufgabe der Grenzüberwachung gemäß § 2 BPolG zu verstehen ist. Die Datenerhebung gemäß § 21 Abs. 1 BPolG zum Beispiel ist für die polizeiliche Kontrolle des grenzüberschreitenden Verkehrs zulässig. Es ist unklar, in welchen Zusammenhängen hier eine Bestandsdatenabfrage, einschließlich der Abfrage von IP-Adressen und Zugangscodes, in Betracht kommen kann. Durch die pauschale Verweisung entstehen daher Unklarheiten, die angesichts der Eingriffsintensität nicht hinnehmbar sind.

Gemäß § 21 Abs. 2 Nr. 1 BPolG ist die Datenerhebung zur Verhütung von Straftaten zulässig, soweit Tatsachen die Annahme rechtfertigen, dass die betroffene Person Straftaten im Sinne des § 12 Abs. 1 BPolG mit erheblicher Bedeutung begehen will und die Daten zur Verhütung solcher Straftaten erforderlich sind. Diese Formulierung entspricht in ihren tatbestandlichen Voraussetzungen weitgehend dem verfassungswidrigen § 20g Abs. 1 Nr. 2 BKAG (vgl. dazu BVerfG NJW 2016, 1781, 1791, Abs. Nr. 165 ff.). Anders als § 20g Abs. 1 Nr. 2 BKAG beschränkt sich § 22a Abs. 1 i.V.m. § 21 Abs. 2 Nr. 1 BPolG nicht auf terroristische Straftaten. Beiden Vorschriften ist aber gemein, dass sie nicht ausschließen,

*„... dass sich die Prognose allein auf allgemeine Erfahrungssätze stützt. Sie enthält weder die Anforderung, dass ein wenigstens seiner Art nach konkretisiertes und absehbares Geschehen erkennbar sein muss, noch*



*die alternative Anforderung, dass das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründen muss, dass sie in überschaubarer Zukunft (...) Straftaten begeht.“ (BVerfG a.a.O.).*

Das Eingriffsgewicht des § 22a BPolG ist zwar mit den in § 20g Abs. 2 BKAG vorgesehenen Maßnahmen hinsichtlich des Eingriffsgewichts nicht gleichzusetzen, insbesondere im Hinblick auf das Abhören des nicht öffentlich gesprochenen Wortes. § 22a BPolG verbindet aber die weite tatbestandliche Formulierung des Vorfeldbereichs mit einer Anknüpfung an weniger gewichtige und unklar beschriebene Rechtsgüter.

§ 21 Abs. 2 Nr. 2 BPolG lässt darüber hinaus die Maßnahme unter wenig bestimmten Eingrenzungen auch gegen einen Dritten zu, der mit der Zielperson in Verbindung steht.

Daher ist im Ergebnis zweifelhaft, ob § 22a BPolG die Bestandsdatenabfrage hinreichend normenklar auf den Bereich des Verhältnismäßigen beschränkt.

Soweit § 22a BPolG zusätzlich bestimmt, die Datenerhebung müsse zur Erforschung des Sachverhalts oder des Aufenthaltsorts einer Person erforderlich sein, führt dies nicht zu einer hinreichenden zusätzlichen Begrenzung. Der Sinn dieses Zusatzes ist seinerseits unklar und führt nicht zu einer nennenswerten Verengung des Tatbestandes (dazu zutreffend Bäcker, A-Drs. 17(4)680C, S. 7f.).

#### **b) § 15 ZFdG**

Ebenso wie vorstehende Vorschrift knüpft auch § 15 ZFdG allgemein an die Erforderlichkeit zur Aufgabenerfüllung an. Im Einzelnen betrifft dies die Aufgabe bei der Überwachung des Außenwirtschaftsverkehrs und des grenzüberschreitenden Warenverkehrs. Gegenstand sind alle Maßnahmen zur Verhütung von Straftaten oder Ordnungswidrigkeiten, zur Aufdeckung unbekannter Straftaten sowie zur Vorsorge für künftige Strafverfahren im Zuständigkeitsbereich der Zollverwaltung. Umfasst ist auch, bei der Bekämpfung der international organisierten Geldwäsche nach den §§ 1, 12a bis 12c, 31a und 31b des Zollverwaltungsgesetzes mitzuwirken. Diese Tatbestände knüpfen weder an einen Anfangsverdacht noch an eine konkrete Gefahr an, sondern umfassen allgemein alle Tätigkeiten zur „Mitwirkung“ bei der „Vorsorge für künftige Straftaten im Zuständigkeitsbereich der Zollverwaltung“.



Damit sind die tatbestandlichen Anforderungen geringstmöglich ausgestaltet, zumal der Tatbestand nicht an tatsächliche Anhaltspunkte irgendeiner Art anknüpft.

### **c) § 20b Abs. 3 bis 5 BKAG**

Soweit § 20b Abs. 3 BKAG auf die Voraussetzungen der Absätze 1 und 2 verweist, bestehen durchaus Bedenken. Absatz 1 verweist lediglich auf die Aufgabenerfüllung, Absatz 2 verweist auf die Straftatenverhütung, ohne auf „ein wenigstens seiner Art nach konkretisiertes und absehbares Geschehen oder die auf einem individuellen Verhalten einer Person basierende konkrete Wahrscheinlichkeit eines Gefahreneintritts“ abzustellen (vgl. zu § 20g BKAG BVerfG NJW 2016, 1781, 1791, Abs. Nr. 165 ff.). Wie bereits oben dargelegt, ist die allgemeine Bestandsdatenabfrage allerdings nicht mit Maßnahmen nach dem bisherigen § 20g Abs. 2 BKAG vergleichbar, zumindest soweit es nicht darum geht, Nutzungsprofile zu erstellen oder Zugangscodes zu erlangen. Da die Vorschrift gleichzeitig auf besonders gewichtige Rechtsgüter abstellt, bestehen insoweit nicht dieselben Bedenken, wie bei den oben genannten Rechtsvorschriften.

### **d) § 100j StPO**

§ 100j StPO setzt für die Bestandsdatenabfrage den qualifizierten Anfangsverdacht einer Straftat voraus. Grundlage des Anfangsverdachts müssen bestimmte Tatsachen sein (Günther in: MüKo StPO, 1. Aufl. 2014, § 100j Rn. 12). Das Gewicht der Straftat ist dabei unerheblich (a.a.O. Rn. 10). Damit unterscheidet sich die Vorschrift im Grundtatbestand wesentlich von §§ 7 BKAG, 7 ZFdG. Der in § 100j StPO geregelte Anlass der Datenerhebung dürfte insoweit den verfassungsrechtlichen Vorgaben genügen.

Problematisch ist allerdings, wie der Zugriff auf Zugangscodes gemäß § 100j Abs. 1 S. 2 StPO konkret ausgestaltet ist. Denn die Vorschrift bestimmt nicht hinreichend klar, in welchen Fällen die Zugangscodes genutzt werden dürfen. Insbesondere ist unklar, mit welcher Reichweite die Ermittlungsbehörden die Zugangsdaten nutzen dürfen.

Denkbar ist einerseits, beispielsweise Zugang zum gesperrten Mobiltelefon des Beschuldigten zu erhalten. Ebenfalls ist denkbar, umfangreich auf räumlich ge-



trennte Speichermedien zuzugreifen. Dies betrifft etwa Daten, die die betroffene Person – nicht notwendig der Beschuldigte – bei Cloud-Diensten im Internet gespeichert hat. Dies kann Daten von sehr unterschiedlicher Sensibilität betreffen. Es kann sich um vergleichsweise harmlose Daten handeln, wie einfache Geschäftsbriefe, ebenso kann es sich aber um Unterlagen zu Gesundheitsfragen, persönliche Tagebücher oder sonstige Notizen aus dem Bereich der innersten Privatsphäre handeln. Auch der Zugang zum Online-Banking kann beispielsweise umfasst sein. Ein Zugriff auf solche Daten kommt etwa gemäß § 110 Abs. 3 StPO in Betracht. Es ist allerdings ausgeschlossen, dies als heimliche Maßnahme durchzuführen (Hauschild in MüKo StPO, § 110, Rn. 16). Dazu passt allerdings nicht, dass § 100j StPO als heimliche Maßnahme ausgestaltet ist, der lediglich die nachträgliche Benachrichtigung des Betroffenen vorsieht. Dies zeigt beispielhaft, dass es zu gesetzlichen Unstimmigkeiten führt, die Regeln zum Zugriff auf Zugangscodes von den Regeln zu trennen, die es ermöglichen sollen, mithilfe dieser Zugangscodes Daten zu erheben.

Aus rein technischer Sicht wäre es mit Hilfe der Zugangsdaten ohne weiteres möglich, auf die in der Cloud gespeicherten Daten der betroffenen Person zuzugreifen. Dies würde in der Eingriffsintensität einer heimlichen Online-Durchsuchung gleichkommen, ohne dass die Ermittlungsbehörde den dafür sonst notwendigen sehr hohen Aufwand betreiben müsste, mit einer Überwachungssoftware in das System des Betroffenen einzudringen. Der Aufwand beschränkt sich auf die Eingabe des Zugangscodes beim jeweiligen Anbieter des Clouddienstes. Zulässig wäre ein solches Vorgehen indes nach derzeitiger Rechtslage nicht (siehe allerdings den Gesetzesbeschluss des Deutschen Bundestages in Form der Beschlussempfehlung BT-Drs.18/12785).

Deshalb ist sowohl rechtlich als auch technisch-organisatorisch auszuschließen, dass Zugangscodes in unzulässiger Weise genutzt werden. Es ist jedoch nicht näher festgelegt, wie die Ermittlungsbehörde mit den Daten umzugehen hat. Es wäre insofern denkbar – auch angesichts des Grundsatzes der Aktenvollständigkeit und der Aktenwahrheit – die Zugangsdaten in Ermittlungsakten oder ggf. Beiakten aufzunehmen. Sie sind dann für alle mit der Sache in Berührung kommenden Ermittlungs- und Justizbeamte, Registratoren, Schreibkräfte etc. sichtbar.

Die Polizeibehörden können die Daten in Strafverfolgungsdateien nach § 483 StPO speichern. Diese Vorschrift enthält keinerlei Begrenzungen zum Inhalt der Datei. In der Praxis ist die Reichweite dieser Vorschrift streitig. So vertrete ich die Auffassung, nach der in Dateien gemäß § 483 StPO nur Daten zu einem bestimmten Strafverfahren gespeichert werden dürfen, nicht jedoch zu einer



Vielzahl nicht zusammenhängender Verfahren (siehe meinen 26. Tätigkeitsbericht, Nr. 10.2.9.3).

Ebenfalls können sie die Daten in polizeiliche Dateien gemäß § 481 Abs. 1 S. 1 StPO übernehmen.

Ebenfalls ist denkbar, dass die Zugangsdaten über Akteneinsichtsrechte an weitere Personen gelangen, zumindest innerhalb des Behördenverkehrs, ggf. aber auch gegenüber Dritten oder Nachrichtendiensten, siehe z.B. §§ 474, 406e StPO.

Es wäre daher erheblich klarer und sicherer, den Zugriff auf Zugangscodes gemeinsam mit den Vorschriften zu regeln, die den Zugriff auf die beweiserheblichen Daten selbst betreffen. Zudem wäre es klarer und sicherer, die Verwendung der erhobenen Zugangscodes auf diese gekoppelte Maßnahme zu beschränken. Es wäre gesetzlich festzulegen, dass die Daten nur einem besonders beschränkten Personenkreis zur Kenntnis gegeben werden dürfen. Da dies gesetzlich nicht geregelt ist, bestehen insoweit Zweifel, ob die Verhältnismäßigkeit durch eine hinreichend normenklare Formulierung des Gesetzestextes sichergestellt ist.

#### **4. Nachrichtendienstliche Befugnisse**

##### **a) § 8d BVerfSchG**

###### **(1) Auskunft über Bestandsdaten**

Als Voraussetzung zur Annahme der Daten auf Seiten der Nachrichtendienste muss die Auskunft zur Erfüllung ihrer Aufgaben erforderlich sein (§ 8d Abs. 1 Satz 1 BVerfSchG, § 4b Satz 1 MADG, § 4 Satz 1 BNDG).

Diese Voraussetzung schränkt die Annahme der fraglichen Daten faktisch nicht ein. Denn die Erforderlichkeit zur Aufgabenerfüllung ist grundsätzliche Voraussetzung für die Verarbeitung personenbezogener Daten durch Nachrichtendienste. Mit der Schaffung einer eigenständigen Rechtsgrundlage (das Auskunftsverlangen wurde vorher auf die allgemeine Befugnisnorm des § 8 BVerfSchG gestützt) hat der Gesetzgeber die Vorgabe des Bundesverfassungsgerichtes nur formal erfüllt. Es fehlt aber an der notwendigen Bestimmtheit, weil die Auskunft unterschiedslos für jegliche Aufgabe des Bundesamtes für Verfassungsschutz (BfV) nach § 3 BVerfSchG verlangt werden kann und damit nach §



8d BVerfSchG im Ergebnis keine strengeren Anforderungen für die Datenerhebung gelten als nach § 8 BVerfSchG.

Aufgabe der Verfassungsschutzbehörden ist die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen über

- Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane oder ihrer Mitglieder zum Ziel haben,
- sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht,
- Bestrebungen im Geltungsbereich dieses Gesetzes, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden,
- Bestrebungen im Geltungsbereich dieses Gesetzes, die gegen den Gedanken der Völkerverständigung, insbesondere gegen das friedliche Zusammenleben der Völker gerichtet sind (§ 3 Abs. 1 BVerfSchG).

Die Erforderlichkeit der Erhebung und Speicherung von Bestandsdaten nach §§ 95, 111 TKG lässt sich unter dieser Aufgabenstellung grundsätzlich recht leicht begründen. Insbesondere um einschätzen zu können, mit welchen anderen Personen, die ggf. ebenfalls einer bestimmten Gruppierung zugerechnet werden können, eine bestimmte Person kommuniziert, können Bestandsdaten hilfreich sein. Diese Daten können in der Zusammenschau mit weiteren Informationen ein Bild von einer Person entstehen lassen, welches eine Einschätzung ermöglicht. Das bedeutet aber letztlich, dass das BfV praktisch ohne tatbestandliche Begrenzungen beliebig Daten zu Personen „anreichern“ kann, die im Kontext anderer Personen bereits aufgetaucht und deshalb gespeichert sind, und zu denen derzeit eine Einschätzung nicht möglich ist bzw. sich ein Verdacht von Handlungen nach § 3 Abs. 1 BVerfSchG bislang nicht erhärtet hat. Aus meiner Prüfungspraxis ist mir bekannt, wie leicht man als bloße undolose Kontaktperson zumindest in Akten, ggf. auch in Dateien des BfV zu einer anderen Person hinzu gespeichert werden kann. Damit wird deutlich, dass auch deren TK-Bestandsdaten gespeichert und genutzt werden können.

Im Ergebnis beschränkt die Vorschrift weder den Anlass, noch den Umfang, noch den betroffenen Personenkreis. Dies verstößt gegen das Bestimmtheitsgebot und den Grundsatz der Verhältnismäßigkeit.





## (2) Auskunft über Zugangscodes

Wie bereits bei § 100j StPO sind auch bei § 8d BVerfSchG die Anforderungen für den Zugriff auf Zugangssicherungscodes nicht konkret genug. Denn aus dem BVerfSchG ergeben sich nur ganz allgemeine Angaben, wozu das BfV die empfangenen Daten nutzen darf.

Die Aufgaben des BfV bestehen in der Sammlung und Auswertung von Informationen über Bestrebungen nach § 3 Abs. 1 Nr. 1, 3 und 4 BVerfSchG sowie über sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich des Gesetzes (§ 3 Abs. 1 Nr. 2 BVerfSchG). Um diese Aufgaben erledigen zu können, hat der Gesetzgeber dem BfV im BVerfSchG verschiedene Ermächtigungen zur Verarbeitung personenbezogener Daten zugewiesen. Neben der allgemeinen Befugnisnorm des § 8 BVerfSchG stehen § 8a BVerfSchG als Auskunftsverlangen gegenüber Telemediendiensten, Luftfahrtunternehmen, Kreditinstituten und weiteren, in § 8a Abs. 2 BVerfSchG genannten Einrichtungen, sowie der hier in Rede stehende § 8d BVerfSchG als Ermächtigungsgrundlage zur Verfügung.

§ 8a Abs. 2 Nr. 4 BVerfSchG ermächtigt das BfV zur Entgegennahme von Verkehrsdaten, soweit dies zur Sammlung und Auswertung von Informationen erforderlich ist und Tatsachen die Annahme rechtfertigen, dass schwerwiegende Gefahren für die in § 3 Abs. 1 genannten Schutzgüter vorliegen, wobei für Schutzgüter nach § 3 Abs. 1 Nr. 1 BVerfSchG weitere Einschränkungen gemacht werden. Vergleicht man diese Ermächtigung mit § 8d Abs. 1 Satz 2 BVerfSchG, fällt auf, dass das Gesetz letztlich höhere Anforderungen an die Erhebung von Verkehrsdaten (also z.B. mit wem, wann und wie lange hat ein bestimmter Anschlussinhaber telefoniert) stellt, als an die Erhebung von Inhaltsdaten. Denn der Zugriff auf Zugangssicherungscodes als Bestandsdaten führt ja im Ergebnis dazu, dass auf Inhalte zugegriffen werden kann. § 8d BVerfSchG enthält keine Forderung nach dem Vorliegen schwerwiegender Gefahren für Schutzgüter nach § 3 Abs. 1 BVerfSchG. Hier fehlt es also an der Verhältnismäßigkeit der Norm.

Mit der „Nutzung“ der Daten ist offenbar gemeint, dass die Behörde die Daten, auf die sie durch die Zugangscodes zugreifen will (z.B. Inhalte von Email-Accounts, Endgeräten oder Clouddiensten), auch für eine weitergehende Maßnahme nutzen darf. Dies kann sich wiederum nur aus anderen Befugnisnormen im Fachgesetz ergeben. Die allgemeine Befugnisnorm des § 8 BVerfSchG ist



bewusst weit gehalten und bemisst sich an den Aufgaben des BfV nach § 3 BVerfSchG. Aus Gründen der Verhältnismäßigkeit kann aber nicht jede Maßnahme, zu der das BfV theoretisch befugt ist, auch direkt (ggf. sogar kumulativ) durchgeführt werden. Vielmehr muss abgewogen werden, welche Maßnahme nach den konkreten Umständen (z.B. aktuelles Geschehen, bereits aus anderen Quellen vorhandene Daten) zum Einsatz kommen soll. Nicht jede vom BfV beobachtete Person wird z.B. dauerhaft oder unmittelbar, sobald sie in den Fokus des Verfassungsschutzes gerät, observiert oder ihre Kommunikation aufgezeichnet. Dementsprechend wäre es z.B. unverhältnismäßig, wenn das BfV sich die Zugangscodes im Sinne von § 113 Abs. 1 Satz 2 TKG von einer Person, die nur Kontakte zu einer bereits beobachteten Person hat, besorgen würde, um herauszufinden, ob diese Person beispielsweise ebenfalls Bestrebungen nach § 3 Abs. 1 Nr. 1, 3 oder 4 BVerfSchG unternimmt oder unterstützt. Dies ergibt sich auch aus § 8 Abs. 5 BVerfSchG, wonach das BfV von mehreren geeigneten Maßnahmen diejenige wählen muss, die den Betroffenen voraussichtlich am wenigsten beeinträchtigt, und wonach die Maßnahme zu keinem Nachteil führen darf, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht.

Im Übrigen sind im Verhältnis zur allgemeinen Befugnisnorm des § 8 BVerfSchG („Das Bundesamt [...] darf die zur Erfüllung seiner Aufgaben erforderlichen [...] personenbezogene[n] Daten erheben, verarbeiten und nutzen ...“) die besonderen Befugnisse in den §§ 8a und 8d BVerfSchG gemessen an der üblichen datenschutzrechtlichen Terminologie schon sehr ungenau formuliert, weil in diesen Vorschriften nur die Ermächtigung enthalten ist, bei den genannten Institutionen „Auskunft [...] einzuholen“. Es bedarf einer Auslegung, um in dieser Empfangnahme von Daten auch die Befugnis zu weiteren Datenverarbeitungsschritten zu lesen. Man könnte der Auffassung sein, dass schon diese Formulierung einen Verstoß gegen die Normenklarheit und das Bestimmtheitsgebot darstellt.

#### **b) § 4b MADG**

Nach § 4b Satz 1 MADG darf der MAD, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und § 111 TKG erhobenen Daten entsprechend § 8d BVerfSchG verlangen.



Bei § 4b MADG handelt es sich um eine Rechtsgrundverweisung auf § 8d BVerfSchG, so dass § 4b MADG auf eine Wiederholung der Tatbestandsvoraussetzungen verzichtet. Allerdings ist fraglich, ob aus Gründen des Bestimmtheitsgebots nicht eine gesonderte Erwähnung der Zugangssicherungscodes im MADG erforderlich ist. § 113 Abs. 1 TKG erwähnt die Zugangssicherungscodes gesondert, weil sie im Vergleich zu „normalen“ Bestandsdaten Zugang zu weitaus sensibleren Daten (Verkehrs-, aber vor allem auch Inhaltsdaten) ermöglichen. Daher nimmt auch § 8d BVerfSchG in Absatz 1 Satz 2 nochmals gesondert Bezug auf § 113 Abs. 1 Satz 2 TKG. § 4b MADG nimmt dagegen nur insgesamt auf § 8d BVerfSchG Bezug. Dass dem MAD dieselben Auskunftsrechte gegenüber Telekommunikationsdienstleistern zustehen wie dem BfV, lässt sich daher meines Erachtens nur mit einer sehr extensiven Auslegung des Wortlauts erreichen. Käme man zu dem Ergebnis, dass diese Auslegung nicht möglich ist, wäre der MAD nur zur Entgegennahme von „normalen“ Bestandsdaten ermächtigt und § 4 MADG damit verfassungsrechtlich weitaus weniger problematisch als § 8d BVerfSchG.

Im Übrigen gelten die zu § 8d BVerfSchG gemachten Ausführungen entsprechend.

#### c) § 4 BNDG

§ 4 BNDG (vormals § 2b BNDG) ist die einschlägige Ermächtigungsnorm für den BND zur Entgegennahme der Daten nach dem TKG.

Nach § 4 BNDG darf der BND, soweit dies zur Erfüllung seiner Aufgaben nach § 1 Abs. 2 erforderlich ist, von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und § 111 TKG erhobenen Daten entsprechend § 8d BVerfSchG verlangen.

Da § 4 BNDG inhaltsgleich mit § 4b MADG ist, gelten die dort gemachten Ausführungen entsprechend.



## **Teil II: Hinweise zu verfahrenssichernden Maßnahmen**

Neben den vorstehenden Ausführungen zu einzelnen Vorschriften, gibt es zudem Defizite, bei verfahrenssichernden Maßnahmen, die unabhängig von der konkreten die Abfrage legitimierenden Vorschrift global für das Bestandsdatenauskunftsverfahren anzumerken sind.

### **1. Fehlender Richtervorbehalt für Auskunft über IP-Adressen**

Auch wenn vom Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung (BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08) nicht explizit gefordert, halte ich die Einführung eines Richtervorbehalts für die Auskunft über den Inhaber einer IP-Adresse nach § 113 Abs. 1 S. 3 TKG für datenschutzrechtlich geboten.

Diese Notwendigkeit ergibt sich zum einen aufgrund der zwischenzeitlich unstrittig feststehenden Tatsache, dass mit einer entsprechenden Auskunft immer auch ein Eingriff das Fernmeldegeheimnis nach Art. 10 GG einhergeht. Die hohe Sensibilität von Daten, die das Fernmeldegeheimnis tangieren, zieht unweigerlich das Erfordernis nach sich, den vom Grundgesetz gewährten besonderen Schutz auch auf ihre praktische Handhabung zu übertragen. Dieser Anforderung wird man aber lediglich dann gerecht, wenn – im Verhältnis zur „klassischen“ Bestandsdatenauskunft – die Auskunft über den Inhaber einer IP-Adresse unter die erhöhten Anforderungen einer richterlichen Genehmigung gestellt wird.

Zum anderen ergibt sich das Erfordernis einer entsprechenden verfahrenssichernden Maßnahme auch aus der aktuellen Entwicklung, die die Internetnutzung in den letzten Jahren vollzogen hat (vgl. auch *Teil I* bei 2 a) (2) (c)).

Dabei ist zu berücksichtigen, dass nicht nur die Quantität der Internetnutzung massiv zugenommen hat, sondern auch deren Qualität. Immer mehr werden bislang analoge Datenspeicherungen in die digitale Welt ausgelagert; seien es vermeintlich „banale“ Dinge wie die Einkaufsliste oder sensible wie das Tagebuch oder der private Kalender. Hinzu kommt die immer größere Bedeutung des „Internet of Things“, in denen Kühlschränke, Autos oder sogar medizinische Geräte mit einer IP-Adresse Verbindungen zum oder übers Internet aufnehmen. Durch die Umstellung des Internetprotokolls von der Version 4 auf die Version 6 ist es zudem möglich, in viel größerem Umfang IP-Adressen quasi-statisch zu



vergeben, da auch dort, wo bislang IP-Adressen regelmäßig spätestens nach 24 Stunden gewechselt wurden, ein solcher Wechsel zwar grundsätzlich möglich, aber aus technischer Sicht nicht zwingend erforderlich ist. Das bringt aus Datenschutzsicht jedenfalls ein weiteres erhöhtes Gefährdungspotential mit sich.

Gerade weil in den letzten Jahren in immer mehr Gesetzen die Rechtsgrundlagen zur Speicherung und Verarbeitung von IP-Adressen durch Sicherheitsbehörden geschaffen wurden, führt dieser Wandel in der Intensität der Internetnutzung zu einer mit einer entsprechenden Auskunft zumindest mittelbar verbunden Eingriffsintensität, die nicht mit der einer „gewöhnlichen“ Bestandsdatenauskunft vergleichbar ist.

Die betroffenen IP-Adressen sind in diesem Kontext nicht nur als Bestands- oder Verkehrsdaten im Sinne des TKG zu betrachten, sondern auch als Nutzungsdaten im Sinne des Telemediengesetzes betroffen. Gerade letztere vermitteln detaillierte Informationen über die im Internet genutzten Inhalte. Anhand der bei den Telemediendiensten erhobenen Nutzungsdaten können Sicherheitsbehörden im Zusammenspiel mit der Zuordnungsmöglichkeit der IP-Adressen das Surfverhalten der Internetnutzer äußerst detailliert überwachen. Im Zusammenhang mit der über § 113c Absatz 1 Nummer 3 TKG erreichten Ausweitung des Auskunftsanspruchs auf Vorratsdaten, ist dies sogar über mehrere Wochen möglich. Dass es sich bei der umfassenden Überwachung des Internetverkehrs – zumindest im nachrichtendienstlichen Bereich – mittlerweile um ein realistisches und tatsächlich praktiziertes Szenario handelt, sollte nach den Diskussionen im Zusammenhang mit dem sogenannten „NSA-Skandal“ nicht mehr bestritten werden können.

Um all diesen Problemen angemessen zu begegnen, erscheint hier die Einführung eines Richtervorbehaltes als der einzig konsequente Schritt. Diesem steht m.E. auch nicht die oben angesprochene Entscheidung des Bundesverfassungsgerichts entgegen, da sich – wie gerade dargelegt – die Voraussetzungen, unter denen das Gericht in 2010 seine Entscheidung getroffen hat, mittlerweile grundlegend geändert haben.

## **2. Partiiell fehlende Benachrichtigungspflichten im BKAG**

§ 7 Abs. 6 BKAG sieht nur für einen Teilbereich der Bestandsdatenerhebung vor, die betroffene Person zu benachrichtigen. Sie fehlt bei statischen IP-Adressen und bei allen sonstigen Bestandsdaten in den Fällen des § 7 Abs. 3



SEITE 30 VON 30

S. 1 BKAG. Es fehlt ebenso für die Fälle des § 7 Abs. 2 BKAG eine Benachrichtigungspflicht. Wenn also die Bestandsdatenabfrage auf eine vorangegangene Datenerhebung nach dieser Vorschrift aufbaut, bleibt dies daher für die betroffene Person zunächst unbekannt.

Damit ist die Bestandsdatenabfrage gemäß § 7 Abs. 3 S. 1 BKAG generell eine heimliche Maßnahme. Dies wirkt sich auf die Eingriffsintensität aus.

Hierbei ist zu berücksichtigen, dass die betroffenen Personen über eine Speicherung beim BKA in der Regel auch nicht auf anderem Wege von Amts wegen informiert werden. § 7 BKAG ist nicht Teil des Strafverfahrens, das zwingend zu einer Ermittlungsakte führt, die regelmäßig Gegenstand der anwaltlichen Akteneinsicht ist. Hiervon erfahren die Betroffenen in der Regel nur aufgrund von Zufällen oder aufgrund aktiver Auskunftsanträge. Daher erfolgt auch die weitere „Anreicherung“ der Datenbestände gemäß § 7 Abs. 3 S. 1 BKAG (zur Ergänzung vorhandener Sachverhalte und zu Zwecken der Auswertung) ohne Kenntnis der Betroffenen. Entsprechendes gilt für § 7 Abs. 8 ZFdG.

### **3. Protokollierung und datenschutzrechtliche Kontrolle**

Eine zentrale Protokollierung der Datenerhebungen ist nicht vorgesehen. Dies kann die datenschutzrechtliche Kontrolle erheblich erschweren; jedenfalls soweit anlassunabhängig Bestandsdatenerhebungen kontrolliert werden sollen. Da die Daten gegenüber dem Betroffenen nicht offen erhoben werden, ist eine solche anlassunabhängige Datenschutzkontrolle aber notwendig, um den durch die Heimlichkeit eingeschränkten Rechtsschutz zu kompensieren. Bei einer datenschutzrechtlichen Kontrolle beim BKA war es mir insoweit nicht möglich, selbst Fälle von Datenerhebungen nach § 7 Abs. 2 bis 7 BKAG herauszugreifen, sondern ich habe mich insoweit auf die Recherchen des BKA gestützt.

Mit freundlichen Grüßen  
In Vertretung

  
Gerhold