Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Andrea Voßhoff
Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

POSTANSCHRIFT Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Postfach 1468, 53004 Bonn

An den
Vorsitzenden des Innenausschusses
des Deutschen Bundestages
Herrn Ansgar Heveling, MdB
Platz der Republik 1
11011 Berlin

Wegen Eilbedürftigkeit nur per E-Mail.

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-100
TELEFAX (0228) 997799-550
E-MAIL referat22@bfdi.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 20.06.2016
GESCHÄFTSZ. **22-620/069#0263**

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Entwurf eines Gesetzes zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus - BT-Drs. 18/8702**
HIER Öffentliche Anhörung am 20. Juni 2016
ANLAGEN - 1 -

Sehr geehrter Herr Vorsitzender,

ich danke dem Innenausschuss des Deutschen Bundestages für die Gelegenheit, zu dem Gesetzentwurf Stellung nehmen zu können.

Ihrer Bitte entsprechend, übersende ich anliegend vorab meine schriftlichen Anmerkungen.

Mit freundlichen Grüßen

Andrea Voßhoff

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Öffentliche Anhörung des Innenausschusses des Deutschen Bundestages am 20.06.2016

Stellungnahme der

Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zu dem

Entwurf eines Gesetzes zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus – BT-Drs. 18/8702

Zur Verbesserung der Terrorismusbekämpfung sollen mit diesem Gesetzentwurf die Erkenntnisse einer „Vielzahl von Behörden – national und insbesondere auch international (...) zusammengeführt und übergreifend analysiert werden" (Gesetzentwurf, S. 1).

Der Gesetzentwurf hat erhebliche Auswirkungen. Er tangiert unmittelbar die Grundaussagen, die das Bundesverfassungsgericht (BVerfG) - zuletzt in seiner Entscheidung vom 20. April 2016 (1 BvR 966/09) - getroffen hat.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) befürwortet eine verfassungskonforme Intensivierung der informationellen Zusammenarbeit zur Bekämpfung des internationalen Terrorismus. Von herausragender Bedeutung ist insoweit die Beachtung der Vorgaben des Bundesverfassungsgerichts. Bereits die Ressortberatung erfolgte mit großer Eile. Auch die Fristsetzung in diesem Anhörungsverfahren ist – ausweislich des Einladungsschreibens – ungewöhnlich kurz bemessen. Deshalb bitte ich um Verständnis, dass möglicherweise nicht alle durch den Gesetzentwurf betroffenen Fragen angesprochen werden.

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße

A. Grundsätzliches

I. Verfassungsrechtliche Vorgaben

Der Gesetzentwurf setzt die verfassungsgerichtlichen Vorgaben nicht hinreichend um, so dass erhebliche verfassungsrechtliche Risiken bestehen.

Das Bundesverfassungsgericht hat in einer Reihe aktueller Entscheidungen grundlegende verfassungsrechtliche Anforderungen an Eingriffsschwellen, Eingrenzung des betroffenen Personenkreises sowie an Transparenz und Kontrolle aufgestellt (zuletzt in den Entscheidungen zum Bundeskriminalamtgesetz und zum Antiterrordateigesetz, BVerfG, Urt. v. 20. April 2016, 1 BvR 966/09; Urt. v. 24. April 2013, 1 BvR 1215/07). In seinem Urteil vom 20. April 2016 hat das Gericht beispielsweise ausgeführt: „Für die in die Privatsphäre eingreifenden Ermittlungs- und Überwachungsbefugnisse (...) hat das Bundesverfassungsgericht aus dem Verhältnismäßigkeitsgrundsatz im engeren Sinne übergreifende Anforderungen abgeleitet. Diese betreffen spezifisch breitenwirksame Gefährdungspotentiale, insbesondere solche der elektronischen Datenverarbeitung" (Abs. Nr. 103, m.w.N.).

Im Lichte dieser Rechtsprechung ist eine grundlegende Überarbeitung des Sicherheitsrechts des Bundes und der Länder erforderlich.

II. Keine umfassende, effektive Datenschutzkontrolle

Die nicht hinreichend erfolgte Umsetzung der verfassungsgerichtlichen Vorgaben für wirksame und effiziente Datenschutzkontrollen verletzt das Grundrecht der Betroffenen auf informationelle Selbstbestimmung.

Das Bundesverfassungsgericht hat der BfDI eine **Kompensationsfunktion** zum Schutz der Grundrechte der Betroffenen zugewiesen (Urt. v. 20. April 2016, Abs. Nr. 141; Urt. v. 24. April 2013, Abs. Nr. 217). Insbesondere im Bereich der Nachrichtendienste ist der schwach ausgestaltete Individualrechtsschutz durch effiziente, wirksame und regelmäßige (Datenschutz-) Kontrollen zu kompensieren. Denn Nachrichtendienste operieren grundsätzlich geheim, d.h. der Grundsatz der Offenheit der Datenerhebung gilt für sie grundsätzlich nicht (vgl. BVerfG, Urt. v. 24. April 2013, Abs. Nr. 117, 217).

In seinem Urteil vom 20. April 2016 hat das Bundesverfassungsgericht diese Kompensationsfunktion erneut betont. Es hat hervorgehoben, es obliege dem Gesetzgeber und den Behörden gemeinsam, die verfassungsrechtlichen Anforderungen einer wirksamen Kontrolle sowohl „auf der Ebene des Gesetzes als auch in der Verwaltungspraxis" (a.a.O, Abs. Nr. 214) zu gewährleisten (a.a.O., Abs. Nr. 218). Den Gesetzgeber treffe auch die Verpflichtung, die Kontrollbehörden zur Erfüllung dieser Aufgabe angemessen auszustatten (a.a.O., Abs. Nr. 217).

Nach dem aktuellen Stand des Gesetzentwurfs kann die BfDI diese Kompensationsfunktion nicht adäquat erfüllen. Ursächlich hierfür ist nicht nur die fehlende Zuweisung ausreichender personeller Mittel für den aus diesem Gesetzentwurf resultierenden Mehraufwand, sondern auch die Beschränkung bzw. nicht hinreichende Ausgestaltung der Kontrollbefugnisse der BfDI (vgl. § 22 b, c BVerfSchG-E).
Sind die aus der Kompensationsfunktion resultierenden „qualifizierten Anforderungen an die Kontrolle" (a.a.O., Abs. Nr. 134) nicht angemessen zu erfüllen, begründet dies einen Verstoß gegen den „Verhältnismäßigkeitsgrundsatz im engeren Sinne" (a.a.0. Abs. Nr. 134) und damit eine Verletzung des Grundrechts der Betroffenen auf informationelle Selbstbestimmung, den die Betroffenen mit einer Verfassungsbeschwerde rügen können (vgl. a.a.O., sowie Abs. Nr. 207).

B. Im Einzelnen

I. Zum Erfüllungsaufwand der Verwaltung

Aus der Umsetzung des Gesetzentwurfs resultiert für die BfDI ein Mehrbedarf an Personal- und Sachmitteln in Höhe von vier (Plan-)stellen (zwei höherer und zwei gehobener Dienst). Diesen Bedarf hat die BfDI in den Ressortberatungen detailliert konkretisiert und begründet.

Der (Plan-)Stellenbedarf des Bundesamtes für Verfassungsschutz (BfV) und der Bundespolizei (BPol) ist in der Begründung des Gesetzentwurfs (vgl. S. 18 f) enthalten, nicht jedoch der vorgenannte Mehrbedarf der BfDI.

Insbesondere die Errichtung gemeinsamer Dateien mit ausländischen Nachrichtendiensten (AND), die Teilnahme an gemeinsamen Dateien mit AND sowie die Befugniserweiterungen zugunsten der Bundespolizei führen zu einem erheblichen Mehrbedarf an Kontrollen. Dieser ist mit den vorhandenen Ressourcen nicht zu erfüllen.

Diese Kontrollen sind zwingend erforderlich. Der BfDI obliegt eine verfassungsgerichtlich vorgegebene „Kompensationsfunktion", die insbesondere bei heimlichen Grundrechtseingriffen von herausragender Bedeutung ist (s.o. A. II).

II. Zu Artikel 1: Änderung des Bundesverfassungsschutzgesetzes

1. Zu Nummer 1: § 22 a Absatz 4 Satz 2 BVerfSchG-E

Mit dieser „Änderung wird die Höchstdauer einer gemeinsamen Projektdatei um ein Jahr auf dann maximal für Jahre verlängert." (Gesetzentwurf, S. 19). Zur Begründung verweist der Gesetzentwurf auf „die technisch vereinfachte Durchführung, die insbesondere auch die Datenpflege erleichtert" (a.a.O.).

Die Erhöhung der maximalen Speicherdauer ist ein wesentlicher Eingriff in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung. Bereits die Aufnahme in eine solche Datei „kann für die Betreffenden erheblich belastende Wirkung haben" (BVerfG, Urt. v. 24. April 2013, Abs. Nr. 128).
Nach dem Verhältnismäßigkeitsgebot muss jede Maßnahme, die in Grundrechte eingreift, geeignet, erforderlich und verhältnismäßig im engeren Sinne, d.h. angemessen, sein. Das Vorliegen dieser Voraussetzungen ist qualifiziert zu begründen.

Der Hinweis in der Gesetzesbegründung auf eine technische Vereinfachung ist insoweit nicht ausreichend. Erforderlich ist eine weitergehende, qualifizierte Begründung. Ausreichen könnte beispielsweise, wenn auf der Grundlage konkret nachgewiesener Fälle ein zwingendes, anderweitig nicht regelbares fachliches Bedürfnis für diesen Grundrechtseingriff nachgewiesen würde.

2. Zu Nummer 2: § 22 b BVerfSchG-E

„§ 22 b schafft eine spezifische Rechtsgrundlage für die Errichtung von gemeinsamen Dateien unter Federführung des BfV mit ausländischen öffentlichen Stellen, die mit nachrichtendienstlichen Aufgaben betraut sind." (Gesetzentwurf, S. 20).

Die Kooperationsbefugnis erstreckt sich allgemein auf ausländische Nachrichtendienste, d.h. nicht nur auf Partnerdienste in den Nachbarstaaten, in der EU und der NATO (vgl. Entwurfsbegründung, S. 20). In Bezug auf die Prämisse des Gesetzentwurfs, wonach die NATO-Partner über ein angemessenes Daten-

schutzniveau verfügen bzw. bei NATO-Staaten „das Vertrauen in die Zuverlässigkeit von Zusicherungen grundsätzlich begründet ist" (Gesetzentwurf, S. 20 f.) erscheint eine differenzierte Bewertung der Angemessenheit des Datenschutzniveaus der NATO-Staaten erforderlich.

a) *Absätze 1 und 2*

Nach der Begründung des Gesetzentwurfs soll die Tatbestandsvoraussetzung „bestimmte Ereignisse oder Personenkreise" ausschließen, „eine gemeinsame Datei über die gesamte Aufgabenbreite des BfV – gleichermaßen als internationales NADIS – einzurichten" (S. 20).

Die Begriffe „Ereignisse" und „Personenkreise" sind jedoch extensiv auslegbar (allgemein zur geringen Eingrenzung des betroffenen Personenkreises im Recht der Nachrichtendienste vgl. Bergemann in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Auflage 2012, Kap. H Rn. 44 ff.). Insoweit bestehen erhebliche Bedenken im Hinblick auf das verfassungsrechtliche Gebot hinreichender Normenklarheit und –bestimmtheit. Dieses Gebot soll sicherstellen, dass die „Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte eine wirksame Rechtskontrolle durchführen können. Ferner erlauben die Bestimmtheit und Klarheit der Norm, dass die betroffenen Bürgerinnen und Bürger sich auf mögliche belastende Maßnahmen einstellen können (BVerfG, Urt. v. 24. April 2013, Abs. Nr. 140 m.w.N.).

Entsprechende Bedenken bestehen auch in Bezug auf das Tatbestandsmerkmal „erhebliche Sicherheitsinteressen". Dieses Tatbestandsmerkmal steht in inhaltlicher Relation zu der in § 22 b Abs. 2 Satz 1 BVerfSchG-E normierten qualifizierten Tatbestandsvoraussetzung „besondere Sicherheitsinteressen". Diese Sicherheitsinteressen werden in § 22 b Abs. 2 Satz 2 BVerfSchG-E definiert. Danach liegen besondere Sicherheitsinteressen vor, „wenn Bestrebungen oder Tätigkeiten erforscht werden, die auf die Begehung schwerwiegender Straftaten gegen den Bestand oder die Sicherheit eines Staates oder einer internationalen Organisation gerichtet sind." Nach § 22 b Abs. 2 Satz 3 BVerfSchG-E sind dies die in § 3 Abs. 1 des Artikel 10-Gesetzes genannten Straftaten.

Die inhaltliche Konnexität der vorgenannten Regelungen indiziert, dass die Schwelle für die Annahme erheblicher Sicherheitsinteressen vergleichsweise niedriger ausgestaltet ist, d.h. hierfür nicht die Begehung schwerwiegender Straftaten erforderlich ist.
Mithin könnten unter den Begriff „erhebliche" Sicherheitsinteressen auch Bestrebungen oder Tätigkeiten gefasst werden, die auf die Begehung von Ordnungs-

widrigkeiten oder Alltagsdelikten, d.h. Vergehen mittlerer Schwere, gerichtet sind. Insofern bedarf es einer gesetzgeberischen Präzisierung bzw. Klarstellung, die eine derartige Auslegung des Tatbestandsmerkmals ausschließt.

b) *Absätze 3 und 4*

„Absatz 3 regelt die Basisnutzung als bloße Indexdatei, die lediglich der Kontaktanbahnung – zum nachfolgend gezielten Informationsaustausch außerhalb der Datei – dient und in Datenkranz und Nutzung entsprechend beschränkt ist" (Gesetzentwurf, S. 21).

Demgegenüber regelt Absatz 4 die „analytische Nutzung" (Gesetzentwurf, S. 22). Diese sei von „höherer Praxisbedeutung wegen des höheren Eingriffsgewichts."

Die gemeinsame Datei mit AND dient mithin unterschiedlichen Zwecken (Indexfunktion und Analysefunktion). Die aus der analytischen Verwendung personenbezogener Daten gewonnenen Erkenntnisse können – ausweislich der Begründung des Gesetzentwurfs – „womöglich auch Folgemaßnahmen anstoßen" (vgl. S. 22). Sie haben also weit reichende Folgen für die Betroffenen.

Nach der Rechtsprechung des Bundesverfassungsgerichts zur Angemessenheit, d.h. der Verhältnismäßigkeit von Grundrechtseingriffen im engeren Sinne, ist für die Beurteilung der Verhältnismäßigkeit einer Norm von Bedeutung, welche (potentiellen) Folgen ein Grundrechtseingriff für den Betroffenen hat bzw. welche Folgen die Betroffenen befürchten. Wie oben ausgeführt, greift die Datenanalyse im Vergleich zur Datenspeicherung intensiver in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung ein. Nach dem Verhältnismäßigkeitsgebot muss jede Maßnahme, die in Grundrechte eingreift, geeignet, erforderlich und verhältnismäßig im engeren Sinne, d.h. angemessen, sein. Die Angemessenheit ist zu bejahen, sofern der Grundrechtseingriff nicht außer Verhältnis zu dem verfolgten Zweck steht. Insofern bestehen erhebliche Bedenken, ob die Angemessenheit des Grundrechtseingriffs durch das Vorliegen von „besonderen Sicherheitsinteressen", d.h. dieser alleinigen qualifizierten Tatbestandsvoraussetzung, begründet werden kann.

c) Absatz 5

Diese Regelung berücksichtigt nicht ausreichend die aktuellen verfassungsgerichtlichen Voraussetzungen für die Übermittlung personenbezogener Daten an ausländische öffentliche Stellen. Die Beachtung dieser Voraussetzungen ist von zentraler Bedeutung, da das BfV nach § 22 b Absatz 6 Satz 1 BVerfSchG-E personenbezogene Daten in die gemeinsamen Dateien nur eingeben darf, wenn es die Daten allen teilnehmenden AND übermitteln darf.

Ausweislich der Begründung des Gesetzentwurfs dient die Regelung des Absatzes 5 der Gewährleistung rechtsstaatlicher und datenschutzrechtlicher Garantien (vgl. Gesetzentwurf, S. 21 f.).

Hinsichtlich der Kooperation mit AND aus Drittstatten bezieht sich der Gesetzentwurf ausdrücklich auf das Urteil des Bundesverfassungsgerichts vom 20. April 2016. Danach kommt der Voraussetzung, dass ein hinreichend rechtsstaatlicher Umgang mit den vom BfV in die Datei eingestellten Daten im Teilnehmerstaat zu erwarten ist, „speziell bei der Teilnahme von Drittstaaten (...) besondere Bedeutung zu" (Gesetzentwurf, S. 21). Die nach Absatz 5 notwendige Verlässlichkeit muss auf der Grundlage „typischerweise gefestigter Zusammenarbeitserfahrungen" „konkret gewürdigt" (a.a.O.) werden.

Für die informationelle Kooperation mit Drittstaaten hat das Bundesverfassungsgericht in seinem vorgenannten Urteil dezidierte Vorgaben gemacht (BVerfG Urt. v. 20. April 2016, Abs. Nr. 323 ff). Diese setzt der Gesetzentwurf nicht hinreichend um. Bedeutsam sind insoweit u.a. das „Kriterium der hypothetischen Datenneuerhebung" (a.a.O., Abs. Nr. 330), die „mit Tatsachen unterlegte Einzelfallprüfung" (a.a.O., Abs. Nr. 338), die geforderte gehaltvolle wie realitätsbezogene Informationsgrundlage (vgl. a.a.O., Abs. Nr. 339), deren regelmäßiger Aktualisierung (vgl. a.a.O.), die nachvollziehbare Dokumentation der Gründe (a.a.O.) sowie die – auch insoweit erforderliche – wirksame inländische aufsichtliche Kontrolle bzw. Überprüfbarkeit durch die Datenschutzbeauftragten (a.a.O., Abs. Nr. 330, 340).

d) Absatz 7

Absatz 7 gewährleistet die vom Bundesverfassungsgericht geforderte Datenschutzkontrolle nicht in ausreichendem Maße bzw. schränkt diese ein.

Absatz 7 Satz 2 beschränkt die Kontrollkompetenz der BfDI auf die vom BfV eingegebenen Daten sowie dessen Abrufe. Dies steht nicht in Einklang mit dem Verhältnismäßigkeitsgebot.

Wie oben ausgeführt, ist die in Absatz 4 geregelte „analytische Nutzung" (Gesetzentwurf, S. 22) im Gegensatz zur bloßen Speicherung der Daten nicht nur von „höherer Praxisbedeutung" (a.a.O.), sondern auch mit einem „höheren Eingriffsgewicht" (a.a.O.) verbunden. Mithin ist die datenschutzrechtliche Kontrolle des Analyseverfahrens (auch des technischen Systems) und der hieraus gewonnenen Erkenntnisse von zentraler Bedeutung. Die in Absatz 7 Satz 2 der BfDI zugewiesene Kontrollkompetenz erstreckt sich lediglich auf Eingaben und Abrufe. Im Hinblick auf die Kontrolle des (technischen) Analyseverfahrens und der –ergebnisse besteht somit Ergänzungs- bzw. zumindest Klärungsbedarf – erst recht wenn man von der Zielsetzung des Gesetzentwurfs ausgeht, wonach die Erkenntnisse der Behörden „zusammengeführt und übergreifend analysiert werden müssen" (Gesetzentwurf, S. 1).

Bedeutsam und zugleich Wesensmerkmal einer gemeinsamen Datei ist zudem, dass alle Teilnehmer einer gemeinsamen Datei alle von den jeweils anderen Teilnehmern in dieser Datei offen gespeicherten Daten mit dem Zeitpunkt der Speicherung zur Kenntnis nehmen und - auch rechtsfehlerhaft - verwenden können. Diese Besonderheit ist bei der Ausgestaltung der Kontrollkompetenz der BfDI ebenfalls zu berücksichtigen.

Darüber hinaus ist auch in diesem Zusammenhang die Funktion des BfV als Betreiberin der gemeinsamen Datei, d.h. als verantwortliche Behörde für die technischen und organisatorischen Maßnahmen nach § 9 BDSG, von Bedeutung. Zur Erfüllung dieser Funktion hat das BfV jederzeit umfassende technische Zugriffsrechte auf alle Dateninhalte dieser Datei sowie auf alle IT-technischen Systemparameter.

Die in Absatz 7 Satz 2 geregelte Beschränkung der Kontrollkompetenz der BfDI steht auch aus folgendem Grund in Widerspruch zu verfassungsgerichtlichen Vorgaben: Hinsichtlich der gemeinsamen Dateien nach § 22 b BVerfSchG-E besteht in Bezug auf die Gewährleistung einer effektiven Datenschutzkontrolle ein zentraler Unterschied zu gemeinsamen projektbezogenen Dateien nach § 22 a

BVerfSchG. Bei diesen Projektdateien kooperieren – verbundübergreifend – nationale Sicherheitsbehörden des Bundes und der Länder. Die Kontrollkompetenz der BfDI erstreckt sich insoweit zwar nur auf die beteiligten Behörden des Bundes. Dennoch besteht ein zentraler Unterschied zu den gemeinsamen Dateien des BfV mit AND.
Nach der Rechtsprechung des Bundesverfassungsgerichts ist bei den nationalen, gemeinsamen Datei dafür „Sorge (...) zu tragen, dass deren Kontrolle nicht aufgrund föderaler Zuständigkeitsunklarheiten hinter der Effektivierung des Datenaustauschs zurückbleibt" (BVerfG, Urt. v. 24. April 2013, Abs. Nr. 216). Das „Zusammenspiel der verschiedenen Aufsichtsinstanzen" (a.a.O.) muss „praktisch wirksam sichergestellt" (a.a.O) sein. Es obliegt dem Gesetzgeber, diese Vorgaben umzusetzen (s.o., Abs. Nr. 220).

Auf nationaler Ebene, d.h. in Bezug auf gemeinsame Dateien nationaler Sicherheitsbehörden, ist diese Vorgabe umsetzbar. In Bezug auf die gemeinsamen Dateien des BfV mit AND besteht jedoch keine diesbezügliche Regelungsbefugnis des nationalen Gesetzgebers im Hinblick auf die für diese AND zuständigen Kontrollorgane (sofern derartige Kontrollorgane in Drittstaaten überhaupt existieren). D.h.: Ein „Zusammenspiel der verschiedenen Aufsichtsinstanzen" im Sinne des Bundesverfassungsgerichts ist nach dem Gesetzentwurf nicht gewährleistet. Dies ist insbesondere im Hinblick auf die intendierte übergreifende Datenanalyse und die daraus (potentiell) resultierenden „Folgemaßnahmen" (Gesetzentwurf, S. 22) kritisch zu bewerten.

Nach Absatz 7 Satz 1 trifft das BfV für die gemeinsamen Dateien die technischen und organisatorischen Maßnahmen nach § 9 Bundesdatenschutzgesetz (BDSG). Demnach obliegt dem BfV zur Gewährleistung einer effektiven Datenschutzkontrolle nach der Rechtsprechung des Bundesverfassungsgerichts auch eine „umfassende Protokollierungspflicht" (BVerfG, Urt. v. 20. April 2016, Abs. Nr. 267; vgl. auch: a.a.O, Abs. Nr. 322, 340, 354; 1 BVerfG, Urt. v. 24. April 2013, Abs. Nr. 215).

3. *Zu Nummer 2: § 22 c BVerfSchG-E*

Für die Teilnahme des BfV an gemeinsamen Dateien, die von AND errichtet sind, stellt sich die o.g. Problematik der Gewährleistung einer effektiven Datenschutzkontrolle in besonderer Weise. So muss es der BfDI auch möglich sein, Dateneingaben und –abrufe des BfV nicht nur beim BfV, sondern auch in der vom AND geführten Datei überprüfen zu können. Dies ist u.a. notwendig um festzustellen, ob die vom BfV in diese gemeinsame Datei eingegebenen Daten identisch mit

dem Quelldatenbestand des BfV sind und Verfahrenssicherungen (z.B. die Kennzeichnung von Daten, die nach § 8 a BVerfSchG oder dem Artikel 10-Gesetz erhoben worden sind) dort enthalten sind. Insoweit besteht auf nationaler Ebene eine Vergleichbarkeit zwischen der Antiterrordatei und den Quelldateien des BfV. Im Rahmen meiner Kontrollen dieser Dateien habe ich beispielsweise festgestellt, dass gesetzliche Datenkennzeichnungen in den Quelldateien des BfV zwar vorhanden waren, nicht jedoch in dem entsprechenden – gespiegelten – Datenbestand der Antiterrordatei. Dies verdeutlicht die Notwendigkeit, die Daten des BfV auch in einer vom AND geführten Datei zu kontrollieren. Bei einer Datenübermittlung des BfV an einen AND endet die datenschutzrechtliche Verantwortlichkeit des BfV gemäß § 27 BVerfSchG i.V.m. § 3 Abs. 7 BDSG mit der rechtskonformen Übermittlung der Daten. Bei der Eingabe von Daten des BfV in die von einem AND geführte gemeinsame Datei besteht die datenschutzrechtliche Verantwortlichkeit des BfV für diese Daten uneingeschränkt fort – und damit auch meine Kontrollkompetenz in Bezug auf diese Daten.

Im Übrigen wird auf die Ausführungen zu § 22 b BVerfSchG-E verwiesen.

III. Zu Artikel 2 Nr. 1: Änderung des BND-Gesetzes

Die Begründung für die durch § 2a Abs. 1 Nr. 2 BNDG-E erfolgte erhebliche Ausweitung dieser Befugnis ist kritisch zu bewerten.
Die Anwendung dieser neuen Befugnis führt zu erheblichen Grundrechtseingriffen nicht nur gegenüber den Zielpersonen dieser Maßnahme, sondern auch gegenüber unbeteiligten Dritten, die mit den Zielpersonen in – rechtlich zulässigem bzw. sozialüblichen – Kontakt stehen, z.B. als Gläubiger (Handwerker, Rechtsanwalt, Steuerberater, Arzt, Darlehensgeber etc.) und rechtmäßiger Empfänger einer von der Zielperson veranlassten Banküberweisung.
Nach dem Verhältnismäßigkeitsgebot muss jede Maßnahme, die in Grundrechte eingreift, geeignet, erforderlich und verhältnismäßig im engeren Sinne, d.h. angemessen, sein. Das Vorliegen dieser Voraussetzungen ist qualifiziert zu begründen.
Angesichts der Intensität und Streubreite dieser Grundrechtseingriffe erscheint die Gesetzesbegründung mit dem Hinweis auf die Notwendigkeit zur Beseitigung eines vermeintlich bestehenden „Wertungswiderspruchs“ (Gesetzentwurf, S. 24) und der Herstellung eines „Gleichklangs der Befugnisse von BND und BfV“ (a.a.O.) nicht ausreichend.

IV. Zu Artikel 3: Änderung des Bundespolizeigesetzes

Die erweiterten Befugnisse der Bundespolizei entsprechen nicht den Vorgaben der aktuellen Rechtsprechung des Bundesverfassungsgerichts (s.o. A).

Wenn gerade die Bundespolizei zur Abwehr terroristischer Gefahren oder zur Bekämpfung anderer schwerwiegender Gefahren innerhalb ihres durch Art. 73 Abs. 1 Nr. 5 GG begrenzten Auftrags derartige Befugnisse benötigt, kann dies verfassungsrechtlich möglicherweise auch unter Datenschutzgesichtspunkten gerechtfertigt sein, wenn der Gesetzgeber die Erforderlichkeit begründen kann. Darauf müssen die gesetzlichen Befugnisse dann aber entsprechend genau mit normenklaren und verhältnismäßigen Eingriffsschwellen zugeschnitten sein. Dies ist hier nicht hinreichend der Fall. Die vorgeschlagene Regelung erfasst nicht nur die in der Begründung zu § 28a BPolG-E genannten Fälle der Schleuserkriminalität. Vielmehr umfasst der zu unbestimmte Gesetzestext auch weit weniger schwerwiegende Fälle und auch diesbezüglich nur ein unklares Gefahrenvorfeld.

Darüber hinaus ist auch der Charakter der Bundespolizei als einer Sonderpolizei zur Sicherung der Grenzen und zur Abwehr bestimmter, das Gebiet oder die Kräfte eines Landes überschreitender Gefahrenlagen zu wahren (vgl. Uhle in: Maunz/Dürig, GG, Art. 73 Rn. 124 m.w.N.).

1. zu Artikel 3 Nr. 1 (§ 28 BPolG, verdeckter Ermittler)

Die vorgeschlagene Regelung ist verfassungswidrig, soweit sie sich auf den Bereich des Gefahrenvorfelds bezieht. In ihrer tatbestandlichen Grundstruktur entspricht sie insoweit dem vom Bundesverfassungsgericht für unvereinbar mit der Verfassung eingestuften § 20g Abs. 1 Nr. 2 BKAG. Verfassungsrechtliche Zweifel bestehen darüber hinaus, soweit sie Kontakt- und Begleitpersonen in ihren Anwendungsbereich einbezieht.

Zwar ergänzt die vorgeschlagene Änderung den bestehenden § 28 BPolG „nur" um ein weiteres Einsatzmittel, nämlich den verdeckten Ermittler. Aber bereits die bestehende Regelung ist wegen der unzureichenden Eingriffsschwellen und Verfahrenssicherungen verfassungsrechtlich nicht zulässig. Deshalb verbietet es sich, sie um ein besonders eingriffsintensives Mittel der Datenerhebung zu ergänzen.

a) Eingriffsschwelle Straftatenverhütung (Buchstabe a, § 28 Abs. 2 Nr. 4 PBolG-E)

Die neue Regelung erweitert die bestehenden Befugnisse auch für Fälle des § 28 Abs. 1 Nr. 2 BPolG. Die Eingriffsschwellen des § 28 Abs. 1 Nr. 2 BPolG entsprechen in der tatbestandlichen Struktur weitgehend dem vom BVerfG verworfenen § 20g Abs. 1 Nr. 2 BKAG (dazu BVerfG, Urt. v. 20. April 2016, Abs. Nr. 162 ff.).

Allerdings liegt die Eingriffsschwelle hier im Falle des BPolG noch niedriger als in der verworfenen Vorschrift. Denn anders als § 20g Abs. 1 Nr. 2 BKAG bezieht sich § 28 Abs. 1 Nr. 2 BPolG nicht auf terroristische Straftaten nach § 4a BKAG, sondern auf alle gewerbs-, gewohnheits-, bandenmäßig oder von einer kriminellen Vereinigung begangenen Straftaten von erheblicher Bedeutung, die in § 12 BPolG genannt sind.

§ 20g Abs. 1 Nr. 2 BKAG ***verfassungswidrig***	**§ 28 Abs. 1 Nr. 2 BPolG (i.V.m. § 21 Abs. 2).**
Wortlaut: „Das Bundeskriminalamt kann personenbezogene Daten mit den besonderen Mitteln nach Absatz 2 erheben über (...) ***2. die Person, bei der Tatsachen die Annahme rechtfertigen, dass sie Straftaten gemäß § 4a Abs. 1 Satz 2 begehen wird,*** (...) wenn die Abwehr der Gefahr oder die Verhütung der Straftaten auf andere Weise aussichtslos ist oder wesentlich erschwert wäre..."	„(1) Die Bundespolizei kann unter Beachtung des § 70 Satz 2 personenbezogene Daten mit den besonderen Mitteln nach Absatz 2 erheben über (...) 2. die in § 21 Abs. 2 bezeichneten Personen zur Verhütung von Straftaten im Sinne des § 12 Abs. 1 mit erheblicher Bedeutung, ***wenn Tatsachen die Annahme rechtfertigen, daß eine solche Straftat gewerbs-, gewohnheits-, bandenmäßig oder von einer kriminellen Vereinigung begangen werden soll...***" § 21 Abs. 2 Nr. 1 BPolG: Zur Verhütung von Straftaten ist eine Erhebung personenbezogener Daten nur zulässig, soweit ***Tatsachen die Annahme rechtfertigen, daß*** ***1. die Person Straftaten im Sinne des § 12 Abs. 1 mit erheblicher Bedeutung begehen will und die Daten zur Verhütung solcher Straftaten erforderlich sind ...***

§ 28 Abs. 1 Nr. 2 BPolG sollte gestrichen oder durch eine andere Regelung ersetzt werden, die den verfassungsrechtlichen Vorgaben entspricht. Eine Erweiterung der bestehenden Regelung ohne eine entsprechende verfassungskonforme Änderung ist nicht zu legitimieren.

Zwar ist der Gesetzgeber nicht grundsätzlich daran gehindert, auch für das Gefahrenvorfeld Eingriffsbefugnisse zu normieren. Auch zur Straftatenverhütung bedarf es dann aber zumindest einer auf bestimmte Tatsachen und nicht allein auf allgemeine Erfahrungssätze gestützten Prognose, die auf eine konkrete Gefahr bezogen ist. Grundsätzlich gehört hierzu, dass insoweit ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zu erwarten ist (BVerfG, Urt. v. 20. April 2016, Abs. Nr. 164 m.w.N.).

Für terroristische Straftaten könnte der Gesetzgeber darauf abstellen, ob das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft terroristische Straftaten begeht. Ob sich diese Möglichkeit auf Gefahren durch Straftaten übertragen lässt, die in ihrer Qualität deutlich unter terroristischen Straftaten liegen, bedürfte einer eingehenden Prüfung. § 12 Abs. 1 BPolG bezieht sich auch auf weniger schwere Straftaten. Die Begrenzung auf den Bereich der Straftaten von erheblicher Bedeutung führt nicht zu einer ähnlich hohen Gewichtigkeit wie im Bereich terroristischer Straftaten. In der Praxis wurden bereits Fundunterschlagungen von Mobiltelefonen als Straftat von erheblicher Bedeutung eingestuft. Festzustellen ist: Der Gesetzentwurf beschränkt sich im Gesetzestext nicht auf den in der Entwurfsbegründung angegebenen Fall besonders schwerer Schleusungskriminalität.

b) *Eingriffsschwelle bei Kontaktpersonen (Buchstabe a, § 28 Abs. 2 Nr. 4 BPolG-E)*

Eingriffe gegen Kontakt- und Begleitpersonen nach § 20g Abs. 1 Nr. 3 Bundeskriminalamtgesetz hat das Bundesverfassungsgericht wegen der möglichen verfassungskonformen Auslegung der Vorschrift akzeptiert, weil § 20b Abs. 2 Nr. 2 BKAG eine besondere Tatnähe der Kontakt- und Begleitperson verlangt. Ob der deutlich anders formulierte § 21 Abs. 2 Nr. 2 BPolG diese Kriterien ebenfalls erfüllt, ist jedenfalls zweifelhaft. Zu unbestimmt wird die Vorschrift spätestens durch den Verweis auf § 21 Abs. 1 Nr. 1 BPolG.

Hinzu kommt, dass § 28 insoweit nicht dem Schutz derselben hochrangigen Rechtsgüter dient, wie dies bei § 20g BKAG der Fall ist. § 28 BPolG ist nicht auf die Terrorismusbekämpfung begrenzt, sondern umfasst alle gewerbs-, gewohnheits- oder bandenmäßig begangenen Delikte, die in § 12 Abs. 1 BPolG genannt sind (siehe oben). Damit darf der verdeckte Ermittler nach dem geplanten Gesetz

gezielt gegen Personen eingeschleust werden, die mit einer anderen Person lediglich in Kontakt stehen, die als gewohnheitsmäßiger Taschendieb im Bereich der Bahnanlagen vage verdächtig ist (Vorfeldkompetenz!).

c) *Unzureichende Verfahrenssicherungen (Buchstabe b und c, § 28 Abs. 3a, 6 bis 9 BPolG-E)*

Die neu eingefügten Verfahrenssicherungen entsprechen nicht den Vorgaben der genannten Entscheidung des Bundesverfassungsgerichts. Sie sind schon deshalb unzureichend, weil sie sich ausdrücklich auf die neu eingefügten Befugnisse beschränken. Die bereits im § 28 Bundespolizeigesetz enthaltenen weiteren ebenfalls eingriffsintensiven Ermittlungsmethoden, wie etwa das Abhören oder Aufzeichnen des nicht öffentlich gesprochenen Wortes in § 28 Abs. 2 Nr. 2 Buchst. b BPolG oder die längerfristige Observation, werden nicht erfasst. Für diese wären jedoch ebenfalls verfahrensrechtliche Sicherungen einzufügen (vgl. BVerfG, Urt. v. 20. April 2016, Abs. Nr. 170 ff. sowie Abs. Nr. 272 ff.). Es fehlt eine Vorschrift zur Sicherung des Kernbereichs privater Lebensgestaltung (BVerfG, Urt. v. 20. April 2016, Abs. Nr. 176). Ebenso fehlen Regelungen zur Datenschutzkontrolle.

Zweifelhaft ist, ob die Regelung zur Zweckbindung in § 29 Abs. 1 Satz 5 BPolG ausreicht, um die Anforderung zur Zweckbindung – insbesondere hinsichtlich des Kriteriums der hypothetischen Datenneuerhebung – zu erfüllen (vgl. BVerfG, Urt. v. 20. April 2016, Abs. Nr. 287).

Letztlich zeigt sich hier nochmals, dass nach den jüngsten Korrekturen des Bundesverfassungsgerichts eine grundlegende Überarbeitung des Sicherheitsrechts des Bundes und der Länder erforderlich wäre.

2. zu Artikel 3 Nr. 2 (§ 28a BPolG, technische Mittel zur Eigensicherung)

Zunächst wirken sich hier die o.g. Bedenken zu § 28 Abs. 2 Nr. 4 BPolG-E aus, auf die sich die Erweiterung in § 28a BPolG bezieht.

Auf Bedenken stößt die Regelung zur weiteren Verwendung der Daten in § 28a Absatz 4 BPolG-E. Bei der Nutzung für Zwecke der Strafverfolgung handelt es sich um eine zweckändernde Nutzung. Diese ist nur unter denselben Eingriffsvoraussetzungen zulässig, wie die Ersterhebung (Grundsatz der hypothetischen Neuerhebung, vgl. BVerfG, Urt. v. 20. April 2016, Abs. Nr. 287). Die Strafprozessordnung sieht die akustische Wohnraumüberwachung zur Eigensicherung

eines verdeckten Ermittlers gerade nicht vor. Deshalb stellt sich die Frage, worauf der Verweis dann zielt.

V. Zu Artikel 9: Änderung des Telekommunikationsgesetzes – Nummer 2: § 111 TKG

Die Notwendigkeit, bei im Voraus bezahlten Mobilfunkdiensten eine Verifikation erhobener Bestandsdaten durchzuführen, wird grundsätzlich anerkannt. Insofern bestehen gegen die in § 111 Absatz 1 Sätze 3 und 4 beabsichtigte Regelung keine Bedenken.

Die gemäß § 111 Absatz 1 Satz 5 vorgesehene Speicherungspflicht von Angaben zu Identitätsdokumenten begegnet jedoch erheblichen datenschutzrechtlichen Bedenken. Ich rege daher an, Satz 5 ersatzlos zu streichen.

De facto bedeutet diese Regelung zunächst, dass der Gesetzgeber offenbar seinen eigenen Vorgaben misstraut und davon ausgeht, dass die Erbringer von geschäftsmäßigen Telekommunikationsdiensten sowie daran Mitwirkende sich rechtswidrig verhalten und ihrer Verpflichtung zur Verifikation der von ihnen erhobenen Daten nicht ordnungsgemäß nachkommen werden, so dass eine erneute Überprüfung durch die Sicherheitsbehörden erforderlich ist.

Weiterhin bedeutet diese Regelung, dass über diese Hintertür der Überprüfung der der Verifikation dienenden Daten der Katalog der Daten nach § 111 Absatz 1 Satz 1 Nr. 1 bis 6 ergänzt wird. Dies würde zu einer massenhaften Speicherung von sensiblen Daten zu Identitätsdokumenten bei Telekommunikationsunternehmen führen, ohne dass zu dem Zeitpunkt der Speicherung überhaupt absehbar ist, ob diese Daten benötigt werden. Weiter ist zu berücksichtigen, dass es sich um Daten handelt, die von den Anbietern selbst zur Erbringung des Dienstes in keiner Weise benötigt werden. Die geplante Regelung konstituiert somit eine Pflicht, Daten zu erheben und zu speichern, die ausschließlich für sicherheitsbehördliche Zwecke verwendet werden. Sogar in der Gesetzesbegründung wird explizit ausgeführt, dass die gespeicherten Angaben zum Identitätsdokument lediglich dem Zweck dienen sollen, Sicherheitsbehörden "einen Anknüpfungspunkt für weitere Ermittlungen zur Feststellung des Anschlussinhabers zu ermöglichen".

Dies ist weder erforderlich noch steht es in Übereinstimmung mit den Vorgaben des Bundesverfassungsgerichts in seinem Beschluss vom 24. Januar 2012 (1 BvR 1299/05). Das Bundesverfassungsgericht hat zwar festgestellt, dass die Speicherpflicht des § 111 TKG zur Schaffung einer Datenbasis für die in § 112 und § 113 TKG geregelten Auskunftsverfahren verfassungsrechtlich nicht zu beanstanden ist.

Weiterhin führt das Bundesverfassungsgericht aber aus, § 111 TKG diene dazu, eine verlässliche Datenbasis für Auskünfte vorzuhalten, die es bestimmten Behörden erlaubt, Telekommunikationsnummern individuellen Anschlussinhabern zuzuordnen (Abs. Nr. . 132). An anderer Stelle heißt es, dass durch § 111 TKG eine Datenbasis geschaffen werde, um im Rahmen der §§ 112, 113 TKG Telekommunikationsnummern ihren Anschlussinhabern zuordnen zu können (Abs. Nr. . 134). Dadurch ist eindeutig der Zweck des § 111 TKG darauf begrenzt, Telekommunikationsnummern ihren Anschlussinhabern zuzuordnen. Eine hierfür valide Datenbasis kann aber bereits durch die neue Verpflichtung zur Verifizierung der angegebenen Daten durch ein Identitätsdokument erreicht werden. Jedenfalls so lange nicht durch praktische Erfahrungen belegbar ist, dass die neu einzuführende Verifikationspflicht nicht zu dem gewünschten Effekt einer Verbesserung der Datenqualität führt, geht die zusätzlich geforderte Speicherung im Sinne des § 111 Absatz 1 Satz 5 über die Vorgaben des Bundesverfassungsgerichts hinaus und ist damit weder erforderlich noch verhältnismäßig.

Schließlich ist die in § 111 Absatz 1 Satz 5 vorgesehene Ausweitung der Speicherverpflichtung auch mit Blick auf aktuelle Bestrebungen des Rates der Europäischen Union, in Zukunft ausländischen Sicherheitsbehörden – gegebenenfalls auch solchen aus Drittstaaten – unmittelbar die Möglichkeit einzuräumen, Daten bei Telekommunikationsunternehmen abfragen zu können (vgl. Presseerklärung: „Council conclusions on improving criminal justice in cyberspace" vom 09.06.2016, abrufbar unter: http://www.consilium.europa.eu/de/press/press-releases/2016/06/09-criminal-activities-cyberspace), äußerst kritisch zu sehen. Bei Umsetzung der Pläne würden solche Behörden künftig auf diesem Weg neben den ohnehin schon umfangreichen telekommunikationsbezogenen Daten zusätzlich einfachen Zugriff auf die auf Vorrat zu speichernden Daten zu Ausweis- und anderen Identitätsdokumenten erhalten.

Andrea Voßhoff