Prof. Dr. Matthias Bäcker, LL.M. Mannheim, den 11. November 2016

Bundesverfassungsgericht
Schlossbezirk
76131 Karlsruhe

Verfassungsbeschwerde

1. des Amnesty International – Sektion der Bundesrepublik Deutschland e.V.,
2. der Frau H. (Deutschland),
3. der Frau K. (Deutschland),
4. des Herrn B. (Deutschland),
5. der Frau S. (USA),
6. des Herrn H. (USA),

g e g e n

§ 5 Abs. 1 Satz 3 Nr. 8, Abs. 2 Sätze 3 und 6,

§ 5a Satz 7,

§ 6 Abs. 1 Satz 5,

§ 7 Abs. 2, Abs. 4, Abs. 4a, Abs. 5 Satz 4,

§ 7a Abs. 1 Satz 1, Abs. 2, Abs. 3 Satz 4,

§ 12 Abs. 1 Satz 2 i.V.m. Abs. 2 Satz 1,

§ 15 Abs. 5 Satz 2

des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) in der Fassung des Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl I S. 1938)

und

§ 24 Abs. 2 Satz 3 des Bundesdatenschutzgesetzes.

Namens und in Vollmacht der Beschwerdeführerinnen und Beschwerdeführer erhebe ich Verfassungsbeschwerde. Ich rüge Verletzungen der Menschenwürdegarantie (Art. 1 Abs. 1 GG), des allgemeinen Gleichheitssatzes (Art. 3 Abs. 1 GG), des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG) und der Rechtsschutzgarantie (Art. 19 Abs. 4 Satz 1 GG).

Gliederung

A. Sachverhalt

Die Verfassungsbeschwerde richtet sich gegen die Ermächtigung des Bundesnachrichtendienstes, die internationale Telekommunikation zur Frühaufklärung internationaler IT-bezogener Straftaten strategisch zu überwachen. Sie erstreckt sich auf damit zusammenhängende gesetzliche Regelungen zum Verfahren der strategischen Telekommunikationsüberwachung, zur Übermittlung der durch eine strategische Telekommunikationsüberwachung gewonnenen Daten an andere Behörden im In- und Ausland sowie zur Dokumentation und Kontrolle strategischer Telekommunikationsüberwachungen.

I. Gegenstand, Inhalt und Kontext der angegriffenen Regelungen

Die strategische Telekommunikationsüberwachung ist eine Maßnahme der Verdachtsgewinnung. Sie unterscheidet sich hierin von herkömmlichen Telekommunikationsüberwachungen, wie sie in der Strafprozessordnung oder in den Polizeigesetzen von Bund und Ländern geregelt sind. Eine herkömmliche Telekommunikationsüberwachung soll einen bestimmten Sachverhalt aufklären oder die Kommunikation einer bestimmten, aus behördlicher Sicht verdächtigen Person erfassen. Sie beruht damit auf einem konkreten Anlass und wird durch diesen Anlass sachlich und zeitlich begrenzt. Eine strategische Telekommunikationsüberwachung wird hingegen ohne konkreten Anlass, allenfalls aufgrund einer kaum konturierten allgemeinen Bedrohungslage durchgeführt. Sie findet ihre Grenze im Wesentlichen nur in dem Erkenntnisziel, das mit der Überwachung verfolgt wird.

Das Artikel 10-Gesetz (im Folgenden: G 10) ermöglicht strategische Telekommunikationsüberwachungen allein der internationalen Telekommunikation. Internationale Telekommunikation zeichnet sich dadurch aus, dass sich (mindestens) ein Teilnehmer in der Bundesrepublik aufhält oder deutscher Staatsangehöriger ist und (mindestens) ein Teilnehmer als Ausländer vom Ausland aus kommuniziert. Abzugrenzen sind hiervon die rein inländische und die rein ausländische Telekommunikation. Eine strategische Überwachung rein inländischer Telekommunikation ist keiner deutschen Behörde erlaubt. Die strategische Überwachung rein ausländischer Telekommunikation (sogenannte Ausland-Ausland-Fernmeldeaufklärung) führte der Bundesnachrichtendienst bislang ohne besondere gesetzliche Ermächtigung durch,

näher Bäcker, K&R 2014, S. 556 (559 f.).

Nunmehr soll die Ausland-Ausland-Fernmeldeaufklärung hingegen im BND-Gesetz ausdrücklich verankert werden,

> vgl. §§ 6 ff. BNDG in der Fassung des Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes. Dieses Gesetz wurde vom Bundestag und vom Bundesrat bereits verabschiedet, jedoch noch nicht ausgefertigt und verkündet. Die angenommene Gesetzesfassung entspricht unverändert dem in BT-Drs. 18/9041 enthaltenen Entwurf.

Die Ausland-Ausland-Fernmeldeaufklärung ist als solche nicht Gegenstand dieser Verfassungsbeschwerde. Sie ist hier nur mittelbar bedeutsam. Da die Übertragungswege der Telekommunikation heute in aller Regel gleichermaßen inländische, internationale und ausländische Telekommunikation vermitteln, erfasst der Bundesnachrichtendienst im Rahmen einer strategischen Überwachung nach dem G 10 praktisch immer auch Telekommunikation, deren Überwachung dieses Gesetz nicht regelt. Der Bundesnachrichtendienst trennt die unterschiedlichen Telekommunikationsformen daher bei der Erfassung zunächst mit Hilfe eines technischen Verfahrens, das als Daten-Filter-System (DAFIS) bezeichnet wird. Die dabei erkannten inländischen Telekommunikationsverkehre werden gelöscht. Die ausländischen Verkehre wurden hingegen zumindest bisher als sogenannte „Routineverkehre“ weiterverarbeitet, und zwar nicht mehr nach Maßgabe des G 10, sondern auf der Grundlage der Aufgabe des Bundesnachrichtendienstes zur Auslandsaufklärung (§ 1 Abs. 2 BNDG),

> vgl. zur gleichläufigen Behördenpraxis in den 1990er Jahren bereits BVerfGE 100, 313 (380).

Ob diese Praxis nach der ausdrücklichen gesetzlichen Regulierung der Ausland-Ausland-Fernmeldeaufklärung anhalten wird, ist allerdings unklar.

Das G 10 enthält für strategische Überwachungen des internationalen Telekommunikationsverkehrs die folgenden Vorgaben und Begrenzungen:

§ 5 Abs. 1 Satz 3 G 10 definiert die zulässigen Ziele strategischer Telekommunikationsüberwachungen, indem er bestimmte Gefahrbereiche aufzählt, zu deren Aufklärung eine solche Überwachung durchgeführt werden darf. Neben der Gefahr eines bewaffneten Angriffs auf die Bundesrepublik handelt es sich dabei seit einer Gesetzesänderung im Jahr 1994 um den internationalen Terrorismus sowie bestimmte Erscheinungsformen der grenzüber-

schreitenden organisierten Kriminalität. Das angerufene Gericht hat diese Erweiterung der Überwachungsziele mit Urteil vom 14. Juli 1999 grundsätzlich gebilligt,

BVerfGE 100, 313 (373 ff.).

Durch das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 wurden die Gefahrbereiche des § 5 Abs. 1 Satz 3 G 10 um einen weiteren Bereich ergänzt, der sich in Nr. 8 dieser Vorschrift findet. Diese Norm benennt als Überwachungsziel die rechtzeitige Erkennung der Gefahr

> „des internationalen kriminellen, terroristischen oder staatlichen Angriffs mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland“.

Gegen diese Erweiterung des Katalogs zulässiger Überwachungsziele richtet sich die Verfassungsbeschwerde.

Das G 10 sieht ein zweistufiges Verfahren vor, um den Gegenstand einer strategischen Telekommunikationsüberwachung zu konkretisieren. Auf der ersten Stufe bestimmt der Bundesminister des Innern gemäß § 5 Abs. 1 Satz 2 G 10 die Telekommunikationsbeziehungen, die überwacht werden sollen. Diese Bestimmung kann sehr weit gefasst werden. In der Praxis werden in der Regel ganze Staaten oder geografische Regionen zu Zielgebieten der Überwachung erklärt. Die Auswahl ist dabei breit gestreut. So ergibt sich aus einem jüngeren Urteil des Bundesverwaltungsgerichts, dass im Jahr 2010 die Bestimmung für den Gefahrbereich „internationaler Terrorismus“ insgesamt 150 Staaten und weitere 46 Regionen umfasste,

vgl. BVerwG, Urteil vom 28. Mai 2014 – 6 A 1.13 –, juris, Rn. 30.

Auf der zweiten Stufe sind in der eigentlichen Überwachungsanordnung die Übertragungswege zu bezeichnen, auf die sich die Überwachung bezieht. Darunter sind einzelne physikalische Verbindungen zu verstehen. Die Begründung zu der Änderung des G 10, welche das Gesetz in die bis heute weitgehend gleich gebliebene Fassung brachte, nennt beispielhaft „konkrete Satellitenverbindungen (z.B. die über den Satelliten X)“ sowie „konkrete internationale Kabelverbindungen (z.B. das Lichtwellenleiterkabel von A nach B)“,

BT-Drs. 14/5655, S. 23.

Die Beschränkung selbst ist im Gesetz gleichfalls als gestufter Geschehensablauf konzipiert. Der Bundesnachrichtendienst beschafft sich – mittels eigener Überwachungseinrichtungen (vgl. § 10 Abs. 6 Satz 2 G 10) oder bei einem Telekommunikationsunternehmen, das zur Mitwirkung verpflichtet ist (vgl. § 2 G 10) – zunächst einen Rohdatenstrom. Diesen Rohdatenstrom unterzieht der Bundesnachrichtendienst zunächst der gesetzlich nicht ausdrücklich geregelten DAFIS-Filterung. Anschließend wertet der Dienst den Datenstrom gemäß § 5 Abs. 2 G 10 mit Suchbegriffen aus. Dabei wird zwischen inhaltlichen und formellen Suchbegriffen unterschieden: Inhaltliche Suchbegriffe sondern Telekommunikationsverkehre aus, deren Gegenstand einen Bezug zu den Gefahrbereichen des § 5 Abs. 1 Satz 3 G 10 aufweist. Beispiele bilden die Bezeichnungen bestimmter Stoffe oder technischer Einrichtungen sowie bekannte Codewörter. Mit formellen Suchbegriffen sucht der Bundesnachrichtendienst nach Telekommunikationsverkehren zu Personen oder Einrichtungen, die mit einem Gefahrbereich in Verbindung stehen, etwa als „Gefährder“. Hierbei handelt es sich um Kommunikationskennungen wie Telefonnummern oder E-Mail-Adressen,

Huber*,* in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2014, § 5 G 10 Rn. 33.

In der Praxis werden überwiegend formelle Suchbegriffe eingesetzt, da sie eine höhere Treffgenauigkeit aufweisen,

vgl. etwa BT-Drs. 17/12773, S. 7; BT-Drs. 18/218, S. 7; wohl auch BT-Drs. 17/9640, S. 7.

Allerdings darf der Bundesnachrichtendienst gemäß § 5 Abs. 2 Satz 2 Nr. 1 G 10 keine Suchbegriffe verwenden, welche Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung bestimmter Telekommunikationsanschlüsse führen. Je nachdem, wie der Begriff des Telekommunikationsanschlusses zu verstehen ist (näher unten C II 1 a dd), ist im Anwendungsbereich dieser Regelung die Verwendung formeller Suchbegriffe ganz oder teilweise unzulässig. Die umfangreiche Nutzung formeller Suchbegriffe in der Praxis beruht hingegen auf § 5 Abs. 2 Satz 3 G 10. Danach gilt das Verbot einer gezielten Identifikation von Telekommunikationsanschlüssen nicht für Telekommunikationsanschlüsse im Ausland, sofern eine gezielte Erfassung von Anschlüssen ausgeschlossen werden kann, deren Inhaber oder regel-

mäßige Nutzer deutsche Staatsangehörige sind. Die Verfassungsbeschwerde der Beschwerdeführerin zu 5 und des Beschwerdeführers zu 6 richtet sich auch gegen diese Ausnahmeregelung. Das angerufene Gericht hat in seinem Urteil vom 14. Juli 1999 ausdrücklich offengelassen, ob die Vorgängerregelung von § 5 Abs. 2 Satz 3 G 10 verfassungsgemäß war, da diese Norm seinerzeit nicht zulässigerweise angegriffen worden war,

vgl. BVerfGE 100, 313 (384).

Die Treffer, die sich bei der Rasterung der erfassten Telekommunikationsverkehre mittels der Suchbegriffe ergeben, werden auf ihre nachrichtendienstliche Relevanz untersucht. Relevante Daten darf der BND anschließend gemäß § 6 Abs. 1 G 10 weiterverarbeiten.

Das G 10 enthält weitere Regelungen für die Durchführung der Überwachung, den Umgang mit den gewonnenen personenbezogenen Daten und die Kontrolle des Bundesnachrichtendienstes, die teilweise gleichfalls Gegenstand der Verfassungsbeschwerde sind:

Die Benachrichtigung betroffener Person richtet sich nach § 12 Abs. 1 i.V.m. Abs. 2 Satz 1 G 10. Gegenstand der Verfassungsbeschwerde sind die weitreichenden Ausnahmen von der grundsätzlichen Benachrichtigungspflicht, die sich in § 12 Abs. 1 Satz 2 G 10 finden.

§ 7 und § 7a G 10 enthalten Ermächtigungen zur Übermittlung personenbezogener Daten, die durch eine strategische Telekommunikationsüberwachung gewonnen wurden, an andere Behörden im In- und Ausland. Gegenstand der Verfassungsbeschwerde sind die Übermittlungsermächtigungen in § 7 Abs. 2, Abs. 4 und Abs. 4a sowie in § 7a Abs. 1 und Abs. 2 G 10.

Verschiedene Regelungen des G 10 sehen vor, bestimmte Schritte der Überwachung und der Weiterverarbeitung der erhobenen Daten zu Kontrollzwecken zu dokumentieren. Die Verfassungsbeschwerde richtet sich gegen einzelne dieser Dokumentationsvorschriften, die sich in § 5 Abs. 2 Satz 6, § 5a Satz 7, § 6 Abs. 1 Satz 5, § 7 Abs. 5 Satz 4 und § 7a Abs. 3 Satz 4 G 10 finden. Hierbei geht es teilweise um die zulässigen Nutzungen der Dokumentation und überwiegend um Löschungsfristen für die Dokumentationen.

Schließlich errichtet das G 10 mit der G 10-Kommission eine besondere Kontrollinstanz, welche sowohl – ähnlich wie ein Vorbehaltsrichter – die Anordnung der Überwachung vorab zu prüfen hat als auch – ähnlich wie eine Datenschutzbehörde – alle Schritte der Überwachung und der Weiterverarbei-

tung der erlangten Daten kontrollieren darf. Hingegen hat der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, der oder die grundsätzlich zur Kontrolle des Bundesnachrichtendienstes berufen ist, im Anwendungsbereich des G 10 prinzipiell keine Kontrollzuständigkeit. Die Verfassungsbeschwerde richtet sich gegen diese Zweiteilung der Kontrolle des Bundesnachrichtendienstes.

Die Vorgängerregelungen dieser Verfahrens- und Kontrollvorgaben waren zum Teil Gegenstand des Urteils vom 14. Juli 1999,

> vgl. zur Benachrichtigung des Betroffenen BVerfGE 100, 313 (397 ff.); zu Datenübermittlungen BVerfGE 100, 313 (388 ff.); zur Kontrolle der Überwachung BVerfGE 100, 313 (401 f.).

Jedoch unterscheiden sich die nunmehr angegriffenen Regelungen erheblich von den seinerzeit überprüften Normen. Die vorliegende Verfassungsbeschwerde enthält dementsprechend anders gelagerte Rügen als die, über welche das angerufene Gericht seinerzeit zu entscheiden hatte.

II. Die Beschwerdeführerinnen und Beschwerdeführer

Der Beschwerdeführer zu 1 ist der deutsche Ableger einer internationalen Bewegung, die sich für den Schutz der Menschenrechte einsetzt, wie sie in der Allgemeinen Erklärung der Menschenrechte und anderen internationalen Menschenrechtsstandards festgeschrieben sind. Die Tätigkeit der jeweils eigenständigen nationalen Organisationen wird von einem Internationalen Sekretariat koordiniert, das seinen Hauptsitz in London hat, aber über Mitarbeiter weltweit verfügt. Ein Tätigkeitsschwerpunkt zahlreicher Ableger der Bewegung und auch des Beschwerdeführers zu 1 liegt auf der Ausweitung staatlicher Überwachungsmaßnahmen, insbesondere der Massenerfassung elektronischer Kommunikation durch Sicherheitsbehörden.

So ist die US-amerikanische Schwesterorganisation des Beschwerdeführers zu 1 vor dem Supreme Court der Vereinigten Staaten gegen die erweiterten Überwachungsermächtigungen des Foreign Intelligence Surveillance Act vorgegangen,

> vgl. Supreme Court of the United States, Urteil vom 26. Februar 2013, Clapper v. Amnesty International USA, 568 U.S. ___ (2013).

Derzeit ist bei dem Europäischen Gerichtshof für Menschenrechte eine unter anderem von dem Internationalen Sekretariat eingelegte Individualbe-

schwerde gegen die Überwachungspraxis der Nachrichtendienste des Vereinigten Königreichs anhängig (Beschwerdenr. 24960/15).

Der Beschwerdeführer zu 1 koordiniert die Arbeit von über 120.000 deutschen Mitgliedern und Unterstützern und vernetzt sie mit anderen Ablegern sowie mit dem Internationalen Sekretariat. Hierzu beschäftigt er an den Standorten Berlin und München etwa 70 Teil- und Vollzeitkräfte. Diese Beschäftigten unterhalten über verschiedene Telekommunikationsdienste (wie Sprachtelefonie, Fax, E-Mail oder Instant Messaging) für den Beschwerdeführer zu 1 laufend Telekommunikationsverkehre mit zahlreichen Stellen im Ausland. Hierzu zählen Mitarbeiter und Mitglieder des Internationalen Sekretariats sowie der ausländischen Schwesterorganisationen des Beschwerdeführers zu 1, Personen und Gruppierungen, deren Menschenrechte durch ausländische Staaten verletzt werden, sowie deren Repräsentanten und schließlich auch hoheitliche Stellen ausländischer Staaten.

Die Beschwerdeführerin zu 2…

Die Beschwerdeführerin zu 3…

Der Beschwerdeführer zu 4…

Die Beschwerdeführerin zu 5…

Der Beschwerdeführer zu 6…

B. Zulässigkeit der Verfassungsbeschwerde

Die Verfassungsbeschwerde ist zulässig. Die Beschwerdeführerinnen und Beschwerdeführer rügen eine Verletzung ihrer Grundrechte durch die angegriffenen Regelungen (unten I). Sie sind hierzu befugt (unten II). Die Beschwerdefrist ist hinsichtlich aller angegriffenen Regelungen gewahrt (unten III).

I. Verfassungsrechtliche Rügen

Die Beschwerdeführerinnen und Beschwerdeführer rügen folgende Grundrechtsverletzungen:

Alle Beschwerdeführerinnen und Beschwerdeführer rügen, dass die Erweiterung der strategischen Telekommunikationsüberwachung auf den Gefahrbereich der IT-Kriminalität durch § 5 Abs. 1 Satz 3 Nr. 8 G 10 das Fernmeldegeheimnis des Art. 10 Abs. 1 GG verletzt.

Weitere Verletzungen des Grundrechts aus Art. 10 Abs. 1 GG, auf die sich alle Beschwerdeführerinnen und Beschwerdeführer berufen, ergeben sich aus den Ermächtigungen zu Datenübermittlungen in § 7 Abs. 2, Abs. 4 und Abs. 4a G10 und § 7a Abs. 1 Satz 1, Abs. 2 G 10 sowie aus der unzureichenden Ausgestaltung der aufsichtlichen Kontrolle in § 15 Abs. 5 Satz 2 G 10 und § 24 Abs. 2 Satz 3 BDSG.

Alle Beschwerdeführerinnen und Beschwerdeführer rügen zudem eine Verletzung von Art. 10 Abs. 1 und Art. 19 Abs. 4 GG durch die Dokumentationsregelungen in § 5 Abs. 2 Satz 6, § 5a Satz 7, § 6 Abs. 1 Satz 5, § 7 Abs. 5 Satz 4 und § 7a Abs. 3 Satz 4 G 10. Die Beschwerdeführerinnen und Beschwerdeführer zu 2 bis 6 rügen darüber hinaus, dass § 5a Satz 7 G 10 auch die Menschenwürdegarantie des Art. 1 Abs. 1 GG verletzt.

Die Beschwerdeführerinnen und Beschwerdeführer zu 1 bis 4 rügen eine weitere Verletzung von Art. 10 Abs. 1 und Art. 19 Abs. 4 GG durch die in § 12 Abs. 1 Satz 2 i.V.m. Abs. 2 Satz 1 G 10 enthaltene Ausnahme von der Pflicht zur Benachrichtigung des oder der Betroffenen einer strategischen Telekommunikationsüberwachung.

Die Beschwerdeführerin zu 5 und der Beschwerdeführer zu 6 rügen schließlich eine Verletzung von Art. 1 Abs. 1, Art. 3 Abs. 1 und Art. 10 Abs. 1 GG durch § 5 Abs. 2 Satz 3 G 10, der eine Ausnahme von dem grundsätzlichen

Verbot gezielt personenbezogener Überwachungen für Anschlüsse ausländischer Kommunikationsteilnehmer im Ausland errichtet.

Zur näheren Begründung dieser Rügen wird auf die Ausführungen zur Begründetheit der Verfassungsbeschwerde (unten C) verwiesen.

II. Beschwerdebefugnis

Die Beschwerdeführerinnen und Beschwerdeführer sind im Sinne von § 90 Abs. 1 BVerfGG beschwerdebefugt. Insbesondere sind sie durch die angegriffenen Vorschriften selbst, gegenwärtig und unmittelbar in ihren Grundrechten aus Art. 1 Abs. 1, Art. 10 Abs. 1 und Art. 19 Abs. 4 GG, die Beschwerdeführerin zu 5 und der Beschwerdeführer zu 6 darüber hinaus auch in ihrem Grundrecht aus Art. 3 Abs. 1 GG betroffen.

Die Beschwerdeführerinnen und Beschwerdeführer sind durch die angegriffenen Vorschriften unmittelbar betroffen. Zwar bedürfen diese Vorschriften einer Umsetzung durch weitere Vollzugsakte. Von einer unmittelbaren Betroffenheit durch ein Gesetz ist jedoch auch dann auszugehen, wenn potenziell betroffene Personen den Rechtsweg nicht beschreiten können, weil sie keine Kenntnis von der betreffenden Vollziehungsmaßnahme erhalten,

> BVerfGE 133, 277 (311); BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 82.

Strategische Telekommunikationsüberwachungen nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 werden verdeckt durchgeführt. Die in § 12 Abs. 1 i.V.m. Abs. 2 G 10 vorgesehene Benachrichtigungspflicht gleicht dies nur teilweise aus, weil sie vielfach erst spät greift und weitreichende Ausnahmen vorgesehen sind. Auch von der Übermittlung der durch eine strategische Telekommunikationsüberwachung gewonnenen Erkenntnisse erhalten die Betroffenen in der Regel keine Kenntnis. Sie können entsprechende Vollzugsakte daher nicht abwarten, um dann dagegen vorzugehen.

Die Beschwerdeführerinnen und Beschwerdeführer sind durch die angegriffenen Vorschriften selbst und gegenwärtig betroffen. Erforderlich, aber auch ausreichend ist hierfür bei gesetzlichen Ermächtigungen zu verdeckten Überwachungsmaßnahmen die Darlegung, zukünftig mit einiger Wahrscheinlichkeit von einer solchen Maßnahme betroffen und dadurch einem Grundrechtseingriff ausgesetzt zu sein,

vgl. BVerfGE 100, 313 (354); BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 84; BVerfG, Beschluss vom 20. September 2016 – 2 BvE 5/15 –, Rn. 60.

Dies ist hier für alle Beschwerdeführerinnen und Beschwerdeführer der Fall. Die Beschwerdeführerinnen und Beschwerdeführer zu 1 bis 4 unterhalten regelmäßige Telekommunikationsverkehre zu ausländischen Kommunikationsteilnehmern im Ausland, die Beschwerdeführerin zu 5 und der Beschwerdeführer zu 6 unterhalten vom Ausland aus regelmäßige Telekommunikationsverkehre in die Bundesrepublik. Es ist wahrscheinlich, dass die internationale Telekommunikation der Beschwerdeführerinnen und Beschwerdeführer geografisch einer Bestimmung im Sinne von § 5 Abs. 1 Satz 1 G 10 für den Gefahrbereich des § 5 Abs. 1 Satz 3 Nr. 8 G 10 unterfallen wird…

Ohnehin kann die Bestimmung der Zielgebiete einer strategischen Telekommunikationsüberwachung sehr viele Staaten und Regionen umfassen, wie die von dem Bundesverwaltungsgericht für 2010 genannte Zahl von 150 Staaten und weiteren 46 Regionen allein für den Gefahrbereich „internationaler Terrorismus“ zeigt.

Selbst wenn davon ausgegangen wird, dass für jeden einzelnen Telekommunikationsverkehr der Beschwerdeführerinnen und Beschwerdeführer nur eine geringe Wahrscheinlichkeit besteht, durch eine strategische Überwachung erfasst zu werden, ist wegen der Vielzahl der Telekommunikationsverkehre anzunehmen, dass zukünftig einzelne Kontakte der Beschwerdeführerinnen und Beschwerdeführer von einer strategischen Telekommunikationsüberwachung erfasst werden. Dies lässt sich beispielhaft veranschaulichen: Geht man davon aus, dass ein einzelner internationaler Telekommunikationsverkehr mit dem Zielgebiet einer strategischen Überwachung lediglich mit einer Wahrscheinlichkeit von 0,01 erfasst wird, beträgt etwa bei 100 Telekommunikationsverkehren die Wahrscheinlichkeit, dass mindestens einer davon erfasst wird, $1 - 0{,}99^{100} \approx 0{,}63$.

Dieser Befund reicht aus, um die eigene und gegenwärtige Betroffenheit der Beschwerdeführerinnen und Beschwerdeführer zu begründen, da bereits die Erfassung eines Telekommunikationsverkehrs in das Grundrecht aus Art. 10 Abs. 1 GG eingreift. Denn diese Erfassung macht die Kommunikation für den Bundesnachrichtendienst verfügbar und bildet die Basis für einen Abgleich mit den angeordneten Suchbegriffen. Insbesondere ist ein Grundrechtseingriff mithin nicht etwa erst anzunehmen, wenn sich bei dem Abgleich ein

Treffer ergibt. Vielmehr scheidet ein solcher Eingriff nur aus, wenn die erfasste Telekommunikation bereits vor dem Abgleich aufgrund der Ausfilterung innerdeutscher Telekommunikation ausgesondert und unmittelbar anschließend spurenlos gelöscht wird. Dies hat das angerufene Gericht in seinem Urteil vom 14. Juli 1999 ausdrücklich ausgeführt,

> BVerfGE 100, 313 (366); daran anschließend BVerwG, Urteil vom 28. Mai 2014 – 6 A 1.13 –, juris, Rn. 23 f.

Der Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG, der in der Erfassung durch eine strategische Telekommunikationsüberwachung aufgrund von § 5 Abs. 1 Satz 3 Nr. 8 G 10 liegt, bedarf der verfassungsrechtlichen Rechtfertigung. Da die Beschwerdeführer zukünftig sogar mit hoher Wahrscheinlichkeit einem solchen Eingriff ausgesetzt sein werden, können sie mit der Verfassungsbeschwerde rügen, dass die gesetzliche Ermächtigung zu diesem Eingriff die verfassungsrechtlichen Anforderungen verfehlt. Es kommt nicht darauf an, ob es auch wahrscheinlich ist, dass sich bei dem Abgleich ein Treffer ergibt und deshalb die Kommunikation der Beschwerdeführer als potenziell nachrichtendienstlich relevant behandelt wird.

Selbst wenn dies anders zu sehen und die konkrete Wahrscheinlichkeit eines solchen Treffers zu fordern wäre, wären zumindest der Beschwerdeführer zu 1 und die Beschwerdeführerin zu 5 durch die angegriffenen Vorschriften selbst und gegenwärtig betroffen.

Der Beschwerdeführer zu 1 unterhält ständige Telekommunikationskontakte zu zahlreichen Personen weltweit. Da sich der Beschwerdeführer zu 1 satzungsmäßig weltweit für den Schutz der Menschenrechte gegen staatliche Übergriffe einsetzt, finden sich darunter zum einen Kontakte zu Personen, die einer Straftat beschuldigt werden, sowie zu Personen und Gruppierungen, die zumindest im Ausland als potenziell gefährlich angesehen werden und darum staatlichen Repressionen ausgesetzt sind. Zum anderen unterhält der Beschwerdeführer zu 1 auch Kontakte zu hoheitlichen Stellen im Ausland. Dies schließt Repräsentanten von Staaten ein, bei denen zumindest nicht fernliegt, dass von ihnen IT-basierte Angriffe auf informationstechnische Systeme in der Bundesrepublik ausgehen. Wegen der Vielzahl einschlägiger Telekommunikationskontakte des Beschwerdeführers zu 1 ist wahrscheinlich, dass sich unter seinen Kontakten auch Personen, Gruppierungen oder hoheitliche Stellen finden, denen der Bundesnachrichtendienst eine nachrichtendienstliche Relevanz im Zusammenhang mit dem Gefahrbereich des § 5

Abs. 1 Satz 3 Nr. 8 G 10 zumisst und deren Kontaktdaten daher bei einer strategischen Telekommunikationsüberwachung auf der Grundlage dieser Vorschrift als formelle Suchbegriffe genutzt werden.

Zudem besteht auch die konkrete Wahrscheinlichkeit, dass Telekommunikationsverkehre des Beschwerdeführers zu 1 nach einem Abgleich mit inhaltlichen Suchbegriffen bei einer strategischen Telekommunikationsüberwachung nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 als Treffer weiterverarbeitet werden. Zu den thematischen Schwerpunkten des Beschwerdeführers zu 1 gehört gerade in jüngerer Zeit die weltweite Zunahme staatlicher Überwachungen, die sich auf die elektronische Kommunikation beziehen. Aus technischer Sicht gleichen sich illegale Angriffe auf informationstechnische Systeme und bestimmte staatliche Überwachungen mit Bezug zu solchen Systemen (wie „Online-Durchsuchungen“ oder „Quellen-Telekommunikationsüberwachungen“) weitgehend. In der Folge ist es wahrscheinlich, dass die Kommunikation des Beschwerdeführers zu 1 über staatliche Überwachungsmaßnahmen Begriffe enthält, die auch für die Aufklärung des in § 5 Abs. 1 Satz 3 Nr. 8 G 10 geregelten Gefahrbereichs bedeutsam sein können und daher als inhaltliche Suchbegriffe in Betracht kommen.

Die Beschwerdeführerin zu 5…

Eine noch konkretere Darlegung ihrer voraussichtlichen Betroffenheit ist den Beschwerdeführerinnen und Beschwerdeführern aufgrund des extrem breit streuenden Überwachungsansatzes strategischer Telekommunikationsüberwachungen, aufgrund der verdeckten Durchführung der Überwachung selbst sowie aufgrund der Geheimhaltung der verwendeten Filterkriterien und Suchbegriffe nicht möglich und darum zur Begründung ihrer Beschwerdebefugnis auch nicht zumutbar.

III. Beschwerdefrist

Die Jahresfrist des § 93 Abs. 3 BVerfGG ist gewahrt. Das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes, welches die hier angegriffenen Regelungen in § 5 Abs. 1 Satz 3 Nr. 8, § 7 Abs. 2 Nr. 3 und § 7 Abs. 4a G 10 in das Artikel 10-Gesetz eingefügt und § 7 Abs. 4 Satz 1 Nr. 2 G 10 neu gefasst hat, ist gemäß Art. 12 Satz 1 dieses Gesetzes am Tag nach seiner Verkündung und damit am 21. November 2015 in Kraft getreten.

Die Verfassungsbeschwerde ist darüber hinaus auch hinsichtlich der anderen angegriffenen Vorschriften über die Auswahl der Suchbegriffe, die Benachrichtigung der betroffenen Person, Datenübermittlungen sowie die Dokumentation und Kontrolle strategischer Überwachungen fristgemäß erhoben. Zwar wurden diese Vorschriften nicht durch das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes geändert. Jedoch wurden sie durch die Einfügung des neuen Gefahrbereichs in § 5 Abs. 1 Satz 3 Nr. 8 G 10 in einen neuen Regelungskontext gestellt, da sie nunmehr auch auf strategische Überwachungen im Rahmen dieses Gefahrbereichs und auf die daraus gewonnenen Erkenntnisse anzuwenden sind. Infolgedessen können diese Vorschriften im Vergleich mit dem früheren Rechtszustand neue und zusätzliche Belastungen bewirken. Die Einfügung von § 5 Abs. 1 Satz 3 Nr. 8 G 10 hat daher hinsichtlich der mit dem neuen Gefahrbereich im Kontext stehenden Verfahrensregelungen die Beschwerdefrist neu in Gang gesetzt,

> vgl. zu dem ähnlich gelagerten Fall der Übermittlungsermächtigungen des BKA-Gesetzes BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 85; ferner BVerfGE 100, 313 (356).

C. Begründetheit der Verfassungsbeschwerde

Die angegriffenen Regelungen sind primär an der Garantie des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG zu messen, zu der weitere Gewährleistungen hinzutreten. Auf diese Grundrechte können sich vollumfänglich auch die Beschwerdeführerin zu 5 und der Beschwerdeführer zu 6 berufen (unten I).

Die verfassungsrechtlichen Defizite der strategischen Telekommunikationsüberwachung nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 lassen sich wie folgt zusammenfassen: Das Gesetz ermöglicht solche Überwachungen zu einem übermäßig weit gefassten Ziel und ohne hinreichenden Anlass (unten II). Der verfassungsrechtlich gebotene Schutz vor einer gezielt personenbezogenen Überwachung wird ausländischen Kommunikationsteilnehmern im Ausland wie der Beschwerdeführerin zu 5 und dem Beschwerdeführer zu 6 ohne tragfähigen Grund vorenthalten (unten III). Die Transparenz strategischer Telekommunikationsüberwachungen ist nicht hinreichend sichergestellt, da zu weitreichende Ausnahmen von der Pflicht zur nachträglichen Benachrichtigung betroffener Personen bestehen (unten IV). Der Bundesnachrichtendienst darf die durch eine strategische Telekommunikationsüberwachung erlangten personenbezogenen Daten in zu weitem Umfang an andere Behörden im In- und Ausland weitergeben (unten V). Schließlich ist eine wirksame gerichtliche und aufsichtliche Kontrolle strategischer Telekommunikationsüberwachungen nicht gewährleistet (unten VI).

I. Maßstäbliche Grundrechte, insbesondere grundrechtliche Stellung der Beschwerdeführerin zu 5 und des Beschwerdeführers zu 6

Die mit der Verfassungsbeschwerde angegriffenen Regelungen sind primär an der Garantie des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG zu messen. Die Erfassung internationaler Telekommunikation im Rahmen einer strategischen Telekommunikationsüberwachung greift in dieses Grundrecht ein. Der grundrechtliche Schutz des Fernmeldegeheimnisses erstreckt sich auf die gesamte Weiterverarbeitung der erfassten Daten. Insoweit wirkt Art. 10 Abs. 1 GG teilweise mit anderen Grundrechten zusammen, insbesondere zum Schutz des Kernbereichs privater Lebensgestaltung mit der Garantie der Unverletzlichkeit der Menschenwürde aus Art. 1 Abs. 1 GG sowie zur Gewährleistung eines effektiven Rechtsschutzes gegen Überwachungsmaßnahmen mit der Rechtsschutzgarantie des Art. 19 Abs. 4 GG,

vgl. BVerfGE 100, 313 (358 ff.).

Diese Grundrechte schützen vollumfänglich auch die Beschwerdeführerin zu 5 und den Beschwerdeführer zu 6, die US-amerikanische Staatsangehörige sind und in den Vereinigten Staaten leben, wenn der Bundesnachrichtendienst ihre Telekommunikation mit Personen und Einrichtungen in der Bundesrepublik im Rahmen einer strategischen Überwachung erfasst und auswertet.

1. Grundrechtsberechtigung der Beschwerdeführerin zu 5 und des Beschwerdeführers zu 6

Art. 10 Abs. 1 GG garantiert das Fernmeldegeheimnis neben den Beschwerdeführerinnen sowie dem Beschwerdeführer zu 2-4 als inländischen natürlichen Personen und dem Beschwerdeführer zu 1 als inländischer juristischer Person (Art. 19 Abs. 3 GG),

vgl. BVerfGE 100, 313 (356),

auch der Beschwerdeführerin zu 5 und dem Beschwerdeführer zu 6.

Das angerufene Gericht hat bislang offengelassen, ob Art. 10 Abs. 1 GG auch ausländische Kommunikationsteilnehmer schützt, die sich zum Zeitpunkt der Kommunikation im Ausland aufhalten,

vgl. BVerfGE 100, 313 (364); BVerfG, Beschluss vom 20. September 2016 – 2 BvE 5/15 –, Rn. 58.

Die Bundesregierung und der Bundesnachrichtendienst vertreten demgegenüber seit langem die Auffassung, der Schutz des Art. 10 Abs. 1 GG beschränke sich auf deutsche Staatsangehörige und Personen, die sich im Bundesgebiet aufhalten,

vgl. BVerfGE 100, 313 (338 f.); in jüngerer Zeit wird dies vor allem daraus deutlich, dass nach Auffassung der Bundesregierung der Bundesnachrichtendienst zu einer strategischen Überwachung des ausländischen Fernmeldeverkehrs ohne ausdrückliche gesetzliche Ermächtigung befugt sein soll, vgl. etwa BT-Drs. 17/9640, S. 6, 10; BT-Drs. 17/14739, S. 14; andeutungsweise auch BT-Drs. 17/14560, S. 2.

Diese Auffassung überzeugt nicht.

Der Text des Grundgesetzes bietet keinen Anhaltspunkt dafür, Ausländer im Ausland vom Schutz des Fernmeldegeheimnisses auszunehmen. Art. 1 Abs. 3 GG bindet die gesamte öffentliche Gewalt der Bundesrepublik an die Grundrechte des Grundgesetzes. Zudem enthält Art. 10 Abs. 1 GG ein Jedermannsgrundrecht,

hierauf verweist auch Papier, NVwZ-Extra 1/2016, S. 1 (5).

Diese Befunde schließen nicht aus, aus funktionalen Erwägungen den Schutz des Fernmeldegeheimnisses gleichwohl auf bestimmte Personengruppen zu beschränken. Jedoch gibt es keinen einleuchtenden Grund dafür, ausländischen Kommunikationsteilnehmern im Ausland den Schutz des Fernmeldegeheimnisses bereits auf der Ebene des Schutzbereichs und damit vollständig zu versagen.

Das angerufene Gericht hat in seinem Urteil vom 14. Juli 1999 zwei Anknüpfungspunkte für funktionale Grenzen des Grundrechtsschutzes bei einem extraterritorial wirkenden Handeln der deutschen Staatsgewalt genannt: die Grenzen der Verantwortung der deutschen Staatsgewalt sowie die Völkerrechtsfreundlichkeit des Grundgesetzes,

BVerfGE 100, 313 (362 f.).

Unter beiden Gesichtspunkten ist kein Grund dafür ersichtlich, ausländischen Kommunikationsteilnehmern im Ausland den Schutz des Fernmeldegeheimnisses vorzuenthalten: Der Bundesnachrichtendienst führt strategische Telekommunikationsüberwachungen nach § 5 G 10 aufgrund eigener strategischer Entscheidungen selbstständig und eigenverantwortlich durch. Ein Ausschluss des Grundrechtsschutzes ist auch nicht erforderlich, um einen Verstoß gegen das Völkerrecht zu vermeiden. Völkerrechtlich ist die strategische Überwachung internationaler Telekommunikationsverbindungen bestenfalls nicht verboten, jedenfalls aber weder geboten noch auch nur erwünscht.

Ein in der Rechtsprechung des angerufenen Gerichts bislang nicht anerkanntes, aber näher erörterungsbedürftiges Argument für eine funktionale Grenze des Fernmeldegeheimnisses wird in der jüngeren Diskussion um die Ausland-Ausland-Fernmeldeaufklärung angeführt. Danach gehen

> „die Grundrechtsgarantien unausgesprochen von den Gestaltungsmöglichkeiten [aus], die die deutsche Staatsgewalt typischerweise nur auf ihrem eigenen Hoheitsgebiet hat“,

so im Kontext der Neuregelung der Ausland-Ausland-Fernmeldeaufklärung Wolff, BT-Ausschussdrs. 18(4)653 F, S. 2.

Dieses Argument lässt sich so reformulieren: Weil Ausländer, die sich im Ausland aufhalten, der deutschen Hoheitsgewalt nicht in vergleichbarem Maße unterworfen sind wie Personen im Inland oder deutsche Staatsangehörige im Ausland, unterliegen sie auch nicht dem Schutz des Fernmeldegeheimnisses, das ein solches Unterworfensein kompensieren soll.

Nicht überzeugend wäre es dabei, pauschal die Einwirkungsmöglichkeiten der deutschen Staatsgewalt auf Personen im Inland, deutsche Staatsangehörige im Ausland und Ausländer im Ausland zu vergleichen. Es trifft sicher zu, dass Personen im Inland generell in stärkerem Maße der deutschen Staatsgewalt unterworfen sind als Ausländer im Ausland. So müssen sie Einkommensteuer an die deutschen Finanzbehörden bezahlen, unterliegen bei der Teilnahme am Straßenverkehr dem deutschen Straßenverkehrsrecht oder haben unter bestimmten Voraussetzungen Ansprüche auf Sozialleistungen gegen deutsche Sozialleistungsträger. All dies sind grundrechtlich relevante Vorgänge, die Ausländer im Ausland zumindest in aller Regel nicht betreffen.

Hier geht es jedoch um eine Schutzgrenze des Fernmeldegeheimnisses und nicht der deutschen Grundrechte allgemein. Die territoriale und personale Reichweite des Grundrechtsschutzes lässt sich sinnvoll nur grundrechtsspezifisch diskutieren. So steht die territoriale Beschränkung der Freizügigkeitsgarantie des Art. 11 GG auf das Bundesgebiet nicht der unstreitigen Annahme entgegen, dass zumindest deutsche Staatsbürger auch im Ausland durch das Fernmeldegeheimnis geschützt sind. Die von der Bundesregierung und dem Bundesnachrichtendienst vertretene Begrenzung des Fernmeldegeheimnisses sagt nichts darüber aus, ob sich Ausländer im Ausland gegenüber der deutschen Staatsgewalt auf die durch Art. 2 Abs. 2 GG gewährleisteten Rechte auf Leben, körperliche Unversehrtheit und Freiheit der Person oder auf die durch Art. 5 Abs. 1 GG garantierten Kommunikationsfreiheiten berufen können.

Um zu beurteilen, ob das Fernmeldegeheimnis aus funktionalen Gründen in territorialer und personaler Hinsicht begrenzt ist, muss daher auf solche Einwirkungsmöglichkeiten der deutschen Staatsgewalt abgestellt werden, die gerade im Zusammenhang mit Eingriffen in dieses Grundrecht, also mit Überwachungen der Telekommunikation stehen.

Hinsichtlich der Überwachung als solcher sind sachliche Unterschiede zwischen deutschen Staatsangehörigen, Personen im Inland und Ausländern im Ausland von vornherein nicht erkennbar, wenn die Überwachung vom Inland ausgeht. Die durch die Bundesrepublik verlaufende Telekommunikation ist stets dem Zugriff deutscher staatlicher Stellen ausgesetzt, einerlei wo sich die kommunizierenden Personen befinden. In jedem Fall werden dieselben hoheitlichen Mittel eingesetzt, um die Überwachung zu ermöglichen. Namentlich werden im Fall der strategischen Telekommunikationsüberwachung die Telekommunikationsunternehmen durch § 2 G 10 verpflichtet, an der Überwachung mitzuwirken. Hinsichtlich der Vertraulichkeit ihrer Fernkommunikation sind daher Ausländer im Ausland, die mit einem Partner in der Bundesrepublik kommunizieren, der deutschen Staatsgewalt in gleicher Weise unterworfen wie Personen im Inland. Das Argument der unterschiedlichen Betroffenheit von staatlichen Eingriffen ist mithin unzutreffend, soweit es um die Datenerhebung und anschließende Datenauswertung geht. Diese betreffen alle genannten Personenkreise gleichermaßen.

Damit das angeführte Argument überhaupt Sinn ergeben kann, kann es darum nicht auf die Überwachung selbst, sondern nur auf mögliche Folgemaßnahmen bezogen werden. Der grundrechtliche Schutz des Fernmeldegeheimnisses entfiele demnach für ausländische Kommunikationsteilnehmer im Ausland deshalb, weil sie im Anschluss an die Überwachung nicht oder zumindest nicht annähernd im selben Ausmaß wie Personen im Inland oder wie deutsche Staatsangehörige im Ausland mit weiteren Grundrechtseingriffen durch staatliche Stellen der Bundesrepublik zu rechnen haben.

Für diesen Ansatz lässt sich vorbringen, dass das Fernmeldegeheimnis als besondere Garantie der informationellen Privatheit auch einen Schutz vor Grundrechtsgefährdungen enthält. Ähnlich wie das Recht auf informationelle Selbstbestimmung verlagert das Fernmeldegeheimnis den grundrechtlichen Schutz der (äußeren) Verhaltensfreiheit vor, weil sich der Einzelne gegen belastende Folgemaßnahmen, die an einen Eingriff in dieses Grundrecht anschließen, ansonsten nicht durchweg wirksam wehren könnte,

vgl. etwa BVerfGE 118, 168 (184 f.); 120, 378 (397).

Es ist darum plausibel, bei der Interpretation von Art. 10 Abs. 1 GG zu berücksichtigen, ob und welche Folgeeingriffe dem Betroffenen im Anschluss an eine Beschränkung des Fernmeldegeheimnisses bei typisierender Betrachtung drohen,

so im Zusammenhang mit der Frage der Eingriffsintensität etwa BVerfGE 100, 313 (376); 107, 299 (320); 125, 260 (320).

Unplausibel ist es jedoch, auf dieser Grundlage Ausländern im Ausland den Schutz des Fernmeldegeheimnisses vollständig zu versagen, indem bei Telekommunikationsüberwachungen ihnen gegenüber schon ein Eingriff in dieses Grundrecht verneint wird. Denn diesem Personenkreis drohen aufgrund einer Überwachung partiell andere, in vielen Überwachungskonstellationen tendenziell seltenere, nicht aber nur unerhebliche Nachteile.

Aufklärungsmaßnahmen einer deutschen staatlichen Stelle, die sich auf die Telekommunikation von Ausländern im Ausland beziehen, bleiben für die einzelnen Betroffenen nicht von vornherein typischerweise ohne nachteilige Folgen. Solche Maßnahmen können nicht nur zu außenpolitischen Entscheidungen führen, welche die Lebensgestaltung der Betroffenen mittelbar massiv beeinträchtigen können, etwa Entscheidungen über wirtschaftliche Sanktionen oder über einen Auslandseinsatz der Bundeswehr. Sie können auch zu unmittelbar gegen bestimmte Einzelpersonen oder Personengruppen gerichteten Folgemaßnahmen führen, die als Grundrechtseingriffe erheblicher Intensität anzusehen sind. Beispielhaft seien genannt Einreiseverbote, gezielte Finanzsanktionen (*smart sanctions*) oder Strafverfolgungsmaßnahmen wegen Auslandstaten, die gemäß §§ 5 ff. StGB dem deutschen Strafrecht unterfallen. Im Extremfall ist denkbar, Erkenntnisse aus einer Telekommunikationsüberwachung mit Auslandsbezug zu nutzen, um konkrete Kampfeinsätze der Bundeswehr zu planen. Dabei ginge es um Folgeeingriffe, die im innerstaatlichen Bereich außerhalb des Notstandsfalls keine Entsprechung finden. Schließlich können Telekommunikationsüberwachungen für ausländische Betroffene im Ausland schwerwiegende Folgen haben, wenn die erhobenen Daten an ausländische Stellen weitergeleitet werden.

Diese Risiken sind gerade bei strategischen Telekommunikationsüberwachungen nach § 5 G 10 besonders stark ausgeprägt, da diese Überwachungen entsprechend der Aufgabe des Bundesnachrichtendienstes auf die Gewinnung von Erkenntnissen über das Ausland angelegt sind. Fallen dabei sicherheitsbehördlich relevante Erkenntnisse über das Inland an, so handelt es sich hingegen um Zufallsfunde, die nicht dem Überwachungszweck entstammen. Eine strategische Telekommunikationsüberwachung gefährdet daher nach ihrem Erkenntnisziel sogar *primär* Ausländer im Ausland.

Zudem soll das Fernmeldegeheimnis nicht nur als grundrechtlicher Vorfeldschutz Gefährdungen der äußeren Freiheit des Einzelnen abschirmen. Dieses Grundrecht dient – wiederum ähnlich wie das Recht auf informationelle Selbstbestimmung – auch dazu, die innere Freiheit zu schützen und die Unbefangenheit der Fernkommunikation zu bewahren. Das angerufene Gericht hat dementsprechend in seiner jüngeren Rechtsprechung die Einschüchterungseffekte hervorgehoben, die gerade breit streuende Eingriffe in das Fernmeldegeheimnis bewirken können,

BVerfGE 100, 313 (381); 125, 260 (320).

Dass solche Einschüchterungseffekte auch von der Erwartung ausgehen können, durch ausländische Nachrichtendienste überwacht zu werden, zeigt die weltweite Diskussion um die Überwachungstätigkeit von Nachrichtendiensten aus dem angelsächsischen Sprachraum seit den Enthüllungen Edward Snowdens. Insbesondere die Überwachungstätigkeit des Bundesnachrichtendienstes dürfte wegen dessen Aufgabe als Auslandsnachrichtendienst und wegen der Beschränkung strategischer Überwachungen auf die internationale und ausländische Kommunikation die innere Freiheit von Ausländern im Ausland sogar deutlich schwerwiegender beeinträchtigen als die innere Freiheit von Personen, die sich in der Bundesrepublik aufhalten.

Insgesamt sprechen daher die besseren Gründe gegen eine territoriale und personale Begrenzung des Fernmeldegeheimnisses. Staatliche Stellen der Bundesrepublik haben dieses Grundrecht vielmehr unabhängig vom Ort ihres Handelns wie auch vom Ort der betroffenen Fernkommunikation zu beachten. Strategische Telekommunikationsüberwachungen nach § 5 G 10 bewirken dementsprechend auch für die betroffenen ausländischen Kommunikationsteilnehmer im Ausland Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG,

mit Blick auf die Einordnung der Ausland-Ausland-Fernmeldeaufklärung entspricht diese Position mittlerweile der wohl überwiegenden Auffassung in der juristischen Literatur, wie hier etwa Becker, NVwZ 2015, S. 1335 (1339); Heidebach, DÖV 2015, S. 593 (596); Lachenmann, DÖV 2016, S. 501 (505); Huber, ZRP 2016, S. 162 (163); Payandeh, DVBl 2016, S. 1073 (1076); Durner, in: Maunz/Dürig, GG, Art. 10 Rn. 64 f.; Baldus, in: BeckOK GG, Art. 10 Rn. 21. Nach Papier, NVwZ-Extra 1/2016, S. 1 (3) wird die Rechtsauffassung der Bundesregierung und des Bundes-

nachrichtendienstes „in der rechtswissenschaftlichen Literatur nahezu einhellig abgelehnt“.

2. Grundrechtlicher Schutz der beruflichen Telekommunikation der Beschwerdeführerin zu 5 und des Beschwerdeführers zu 6

Die Telekommunikation der Beschwerdeführerin zu 5 und des Beschwerdeführers zu 6 wird durch das Fernmeldegeheimnis unabhängig davon geschützt, ob sie hierzu ihre privaten Telekommunikationsanschlüsse oder berufliche Anschlüsse nutzen, die sie von ihren Arbeitgebern zur Verfügung gestellt bekommen. Auch auf den beruflichen oder privaten Inhalt der Kommunikation kommt es nicht an.

Allerdings können sich die Arbeitgeber der Beschwerdeführerin zu 5 und des Beschwerdeführers zu 6 selbst als juristische Personen des US-amerikanischen Rechts gemäß Art. 19 Abs. 3 GG nicht auf das Fernmeldegeheimnis des Art. 10 Abs. 1 GG berufen,

vgl. BVerfGE 100, 313 (364).

Hieraus schließt der Bundesnachrichtendienst in seiner Überwachungspraxis, Beschäftigte ausländischer juristischer Personen seien bei ihrer beruflichen Telekommunikation nicht durch Art. 10 Abs. 1 GG geschützt, da sie als bloße „Funktionsträger“ ihres Arbeitgebers handelten,

vgl. Graulich, Bericht für den NSA-Untersuchungsausschuss, öffentliche Version, S. 44.

Diese Auffassung überzeugt nicht. Wenn die Beschwerdeführerin zu 5 und der Beschwerdeführer zu 6 dienstliche Telefongespräche führen oder dienstliche E-Mails absenden oder empfangen, kommunizieren unmittelbar sie und nicht ihre Arbeitgeber. Da die Beschwerdeführerin zu 5 und der Beschwerdeführer zu 6 ohne Einschränkung Träger des Grundrechts aus Art. 10 Abs. 1 GG sind, erstreckt sich der Schutz des Fernmeldegeheimnisses auf ihre gesamte, auch die berufliche Telekommunikation,

dass Träger des Grundrechts aus Art. 10 Abs. 1 GG primär die unmittelbar kommunizierenden Teilnehmer sind, betont etwa Durner, in: Maunz/Dürig, GG, Art. 10 Rn. 100.

Die Frage der Grundrechtsberechtigung der Arbeitgeber ist hiervon unabhängig zu beantworten – weder leitet sich der grundrechtliche Schutz der Beschwerdeführerin zu 5 und des Beschwerdeführers zu 6 vom Schutz ihrer

Arbeitgeber ab noch umgekehrt der Schutz ihrer Arbeitgeber vom individuellen Schutz der Beschwerdeführerin zu 5 und des Beschwerdeführers zu 6. Dementsprechend machen die Beschwerdeführerin zu 5 und der Beschwerdeführer zu 6 nicht etwa geltend, ihre Arbeitgeber würden durch die Ermächtigung des Bundesnachrichtendienstes zu strategischen Telekommunikationsüberwachungen übermäßig in ihrer Tätigkeit gestört. Sie fordern allein die kommunikative Privatheit der Telekommunikationsvorgänge ein, an denen sie selbst beteiligt sind.

Eine Ausnahme vom Grundrechtsschutz für die unmittelbar kommunizierenden natürlichen Personen muss vielmehr an deren eigene Stellung anknüpfen. Zu nennen sind insbesondere die Angehörigen ausländischer Staatsorgane oder andere öffentlich Bedienstete, soweit sie selbst hoheitliche Gewalt ausüben oder zumindest zur Ausübung hoheitlicher Gewalt beitragen. Im Privatsektor, in dem die Beschwerdeführerin zu 5 und der Beschwerdeführer zu 6 tätig sind, lässt sich eine solche Ausnahme hingegen nicht begründen.

Hinzu kommt, dass eine Abgrenzung von geschützter privater und nicht geschützter beruflicher Telekommunikation von „Funktionsträgern“ vielfach faktisch kaum möglich ist. Dies zeigt sich beispielhaft darin, dass die Beschwerdeführerin zu 5 ihr berufliches Mobiltelefon auch – erlaubtermaßen – für Privatgespräche mit Personen in der Bundesrepublik nutzt.

3. Grundrechtliches Schutzniveau hinsichtlich der Beschwerdeführerin zu 5 und des Beschwerdeführers zu 6

Das Fernmeldegeheimnis des Art. 10 Abs. 1 GG schützt die Beschwerdeführerin zu 5 und den Beschwerdeführer zu 6 gegen strategische Überwachungen des internationalen Telekommunikationsverkehrs durch den Bundesnachrichtendienst grundsätzlich in derselben Weise wie deutsche Staatsangehörige und Ausländer, die sich im Inland aufhalten. Für eine generelle Absenkung des grundrechtlichen Schutzniveaus zulasten ausländischer Kommunikationsteilnehmer im Ausland besteht entgegen einer im Zusammenhang mit der Ausland-Ausland-Fernmeldeaufklärung vertretenen Auffassung kein Grund. Angezeigt sind lediglich punktuelle Anpassungen, soweit sachliche Unterschiede zwischen den betroffenen Personenkreisen sie gebieten.

Das Fernmeldegeheimnis errichtet unterschiedliche Anforderungen an unterschiedliche Eingriffsmaßnahmen unterschiedlicher Behörden zu unterschiedlichen Zwecken. Bei der Konkretisierung dieser Anforderungen sind auch die

spezifischen Schutzbedarfe unterschiedlicher betroffener Personengruppen zu berücksichtigen.

Das angerufene Gericht hat zu den grundrechtlichen Auswirkungen des spezifischen Erkenntnisziels strategischer Telekommunikationsüberwachungen durch den Bundesnachrichtendienst in seinem Urteil vom 14. Juli 1999 Stellung bezogen. Es hat darin diese Überwachungsmaßnahme im Aufgabenbereich des Bundesnachrichtendienstes grundsätzlich gebilligt, obwohl eine breit gestreute verdachtslose Telekommunikationsüberwachung zur Verdachtsgewinnung etwa im Polizei- oder Strafprozessrecht von Verfassungs wegen nicht erlaubt werden dürfte. Zugleich hat das angerufene Gericht aus Art. 10 Abs. 1 GG spezifische verfassungsrechtliche Anforderungen an strategische Telekommunikationsüberwachungen abgeleitet,

vgl. BVerfGE 100, 313 (382 ff.).

Unabhängig von der Frage, ob die seinerzeit formulierten Anforderungen aufgrund des technischen und sozialen Wandels angepasst werden sollten (siehe hierzu unten II 1), sind die Anforderungen jedenfalls gegenüber allen Kommunikationspartnern gleichermaßen zu beachten. Das angerufene Gericht hat die Besonderheiten der Aufgabe des Bundesnachrichtendienstes zur Auslandsaufklärung in seinem Urteil bereits berücksichtigt. Tragfähige Gründe für eine weitere grundsätzliche Differenzierung im grundrechtlichen Schutzniveau je nachdem, ob der in- oder der ausländische Kommunikationspartner betrachtet wird, sind nicht erkennbar. Das strategische Erkenntnisziel birgt für alle betroffenen Personengruppen vergleichbare Risiken. Hinsichtlich des Primärziels der strategischen Aufklärung, außenpolitische Maßnahmen der Bundesregierung vorzubereiten, sind die Risiken für ausländische Telekommunikationsteilnehmer im Ausland sogar typischerweise am höchsten.

Gegen unterschiedliche Schutzniveaus des Fernmeldegeheimnisses für Personen im Inland und deutsche Staatsangehörige einerseits und Ausländer im Ausland andererseits spricht zudem, dass sich diese Personengruppen beim heutigen Stand der Technik im Rahmen einer Überwachung nicht mehr zuverlässig auseinanderhalten lassen (näher hierzu unten II 1 a bb). Selbst wenn man daher auf der rein normativen Ebene davon ausginge, dass sich eine generelle Differenzierung im grundrechtlichen Schutzniveau zwischen den unterschiedlichen Personengruppen begründen lässt, wäre diese Wertung gleichwohl aus technischen Gründen tatsächlich nicht durchzuhalten.

Vielmehr ist davon auszugehen, dass sich eine Überwachung des (vermeintlich) internationalen Telekommunikationsverkehrs faktisch aus strukturellen Gründen stets in durchaus erheblichem Ausmaß auf rein inländische und rein ausländische Telekommunikationsverkehre erstreckt. Beispielsweise wird sich Telekommunikationsverkehren der Beschwerdeführerin zu 5 und des Beschwerdeführers zu 6 vielfach nicht ansehen lassen, wo sie sich gerade aufhalten, obwohl dies nach der Auffassung der Bundesregierung und des Bundesnachrichtendienstes maßgeblich für ihren Grundrechtsschutz sein soll. Daher müssen die grundrechtlichen Anforderungen im Sinne eines grundrechtlichen Schutzes vor absehbaren und unvermeidbaren Kollateralschäden grundsätzlich für alle Beteiligten gleich bestimmt werden.

Hingegen können Differenzierungen im grundrechtlichen Schutzniveau zwischen Personen im Inland beziehungsweise deutschen Staatsangehörigen einerseits und Ausländern im Ausland andererseits punktuell begründet sein. Es ist denkbar, dass bestimmte grundrechtliche Anforderungen, die für Personen im Inland entwickelt worden sind, auf Ausländer im Ausland nicht passen oder sich ihnen gegenüber sogar kontraproduktiv erweisen. Für die strategische Telekommunikationsüberwachung sind insbesondere die Anforderungen an die Transparenz von Überwachungen zu nennen, die im Inland grundsätzlich gebieten, eine nachträgliche Benachrichtigung der Betroffenen einer Überwachung zu gewährleisten (siehe unten IV). Eine Benachrichtigung von Ausländern im Ausland könnte jedoch in Konflikt mit den territorialen Hoheitsrechten des Aufenthaltsstaats einer betroffenen Person geraten und – vor allem – Betroffene in manchen Staaten sogar massiv gefährden. Angesichts dessen ist das grundrechtliche Transparenzgebot für Ausländer im Ausland zurückzunehmen. Dies hat wiederum gleichfalls hinzunehmende Folgen für die faktischen Rechtsschutzmöglichkeiten der Betroffenen.

II. Ziel der strategischen Beschränkung (§ 5 Abs. 1 Satz 3 Nr. 8 G 10)

Das angerufene Gericht hat in seinem Urteil vom 14. Juli 1999 die anlasslose und großflächige Telekommunikationsüberwachung zur Verdachtsgewinnung, die § 5 G 10 ermöglicht, grundsätzlich auch zur Aufklärung von Gefahren der grenzüberschreitenden organisierten Kriminalität für verfassungskonform gehalten. Es hat zur Begründung auf die Spezifika der Aufklärungstätigkeit des Bundesnachrichtendienstes sowie auf die rechtlichen und faktischen Begrenzungen der strategischen Telekommunikationsüberwachung verwiesen,

vgl. BVerfGE 100, 313 (368 ff.).

Diese Ausführungen bedürfen heute angesichts einer veränderten Rechtslage und andersartiger technischer und sozialer Rahmenbedingungen der kritischen Evaluation. Die verfassungsrechtlichen Anforderungen an Voraussetzungen und Ziele strategischer Telekommunikationsüberwachungen müssen heute strenger gefasst werden als im Urteil vom 14. Juli 1999. Selbst wenn allerdings die damals aus Art. 10 Abs. 1 GG abgeleiteten Maßstäbe unverändert herangezogen werden, verletzt die neue Überwachungsermächtigung des § 5 Abs. 1 Satz 3 Nr. 8 G 10 das Fernmeldegeheimnis.

1. Zur Neubestimmung der verfassungsrechtlichen Anforderungen an die Ziele strategischer Telekommunikationsüberwachungen

Es ist angezeigt, die verfassungsrechtlichen Anforderungen an Voraussetzungen und Ziele strategischer Telekommunikationsüberwachungen heute strenger zu fassen als im Urteil vom 14. Juli 1999. Denn die Eingriffsintensität solcher Überwachungen hat seitdem erheblich zugenommen. Hierfür gibt es zwei Gründe: Erstens hat sich das angerufene Gericht seinerzeit auf rechtliche und tatsächliche Grenzen der Überwachung berufen, welche ihre potenziell enorme Streubreite kompensierten. Diese Grenzen bestehen heute teils nicht mehr, teils lassen sie sich faktisch kaum noch operationalisieren. Zweitens hat seit 1999 die Sensibilität von Telekommunikationsdaten stark zugenommen. In der Folge ist zweifelhaft, ob Ermächtigungen zu strategischen Überwachungen *überhaupt je* dem Verhältnismäßigkeitsgrundsatz genügen können. Zumindest aber müssen die Anforderungen an das Überwachungsziel deutlich verschärft werden.

a) Rechtliche und faktische Begrenzungen der Überwachung

Das angerufene Gericht hat in seinem Urteil vom 14. Juli 1999 die damals angegriffenen Überwachungsermächtigungen in § 3 G 10-a.F. auch deshalb überwiegend für verfassungsgemäß gehalten, weil sie einschränkende Vorgaben enthielten, die Gegenstand, Ausmaß und Modalitäten der Überwachung begrenzten, und weil die Überwachung zudem faktisch begrenzt war.

Diese Ausführungen sind heute überholt. Teils existieren die damals herangezogenen einschränkenden Vorgaben nicht mehr, teils lassen sie sich kaum noch trennscharf handhaben. Ob die zwischenzeitlich hinzugetretenen Vorgaben eine tatsächlich wirksame Begrenzung leisten, ist sehr zweifelhaft.

aa) Gegenstand der Überwachung: Wegfall der Beschränkung auf nicht leitungsgebundene Kommunikation

Dies gilt zunächst für die Vorgaben zum *Gegenstand* der Überwachung. Gemäß § 5 Abs. 1 Satz 1 G 10 darf der Bundesnachrichtendienst die Telekommunikation unabhängig vom technischen Übertragungsweg erfassen. Die Norm setzt lediglich voraus, dass eine gebündelte Übertragung erfolgt, was praktisch so gut wie immer der Fall ist.

Darin liegt ein erheblicher Unterschied zu § 3 G 10-a.F. Seinerzeit durfte nur die nicht leitungsgebundene Telekommunikation überwacht werden. Dadurch wurde die Überwachung im Wesentlichen auf Kommunikation begrenzt, die über Satelliten verläuft. Dies schränkte die Reichweite der Überwachungsbefugnis deutlich ein,

> vgl. BVerfGE 100, 313 (376 f.).

bb) Gegenstand der Überwachung: Untauglichkeit der Beschränkung auf internationale Telekommunikation

Allerdings darf der Bundesnachrichtendienst nach wie vor allein die internationale Telekommunikation zwischen der Bundesrepublik und dem Ausland auswerten. Rein inländische Telekommunikation darf nicht strategisch überwacht werden,

> hierauf bezieht sich BVerfGE 100, 313 (376 f.).

Diese Begrenzung ist jedoch praktisch nicht mehr trennscharf handhabbar. Die Endpunkte eines Telekommunikationsvorgangs lassen sich auf der Übertragungsstrecke nicht mehr zuverlässig verorten.

Telekommunikation wird je nach dem genutzten Dienst (wie Sprachtelefonie, E-Mail, Instant Messaging usw.) heute vielfach und zunehmend bzw. ausschließlich über das Internet vermittelt. Dabei werden die Inhalte der Telekommunikation in Datenpakete zerlegt, die separat anhand von IP-Adressen zugestellt werden. Die IP-Adressen von Quelle und Ziel eines Datenpakets lassen Rückschlüsse auf die Standorte der beteiligten Rechner zu, wenngleich bereits diese Rückschlüsse nicht völlig zuverlässig sind,

> eingehend hierzu die von dem NSA-Untersuchungsausschuss des Deutschen Bundestags eingeholten Gutachten des Chaos Computer Club und von Prof. Dr. Gabi Dreo Rodosek, abrufbar unter https://netzpolitik.org/2016/bnd-kann-internetverkehr-nicht-

zuverlaessig-nach-in-und-ausland-filtern-und-verstoesst-so-gegen-gesetze (letzter Abruf am 10. November 2016).

Für die Abgrenzung inländischer, internationaler und ausländischer Telekommunikation kommt es jedoch nicht durchweg auf die Verortung von Quellrechner und Zielrechner eines Datenpakets an. Entscheidend sind die natürlichen Personen an den Netzenden, die miteinander kommunizieren. Viele Kommunikationsdienste – und zwar gerade Dienste von hoher Relevanz für die nachrichtendienstliche Aufklärung – werden aber durch Intermediäre vermittelt. Dies führt dazu, dass die interpersonale Kommunikation mehrere technische Kommunikationsvorgänge durchläuft, die aneinander anschließen und bei denen jeweils Datenpakete zwischen unterschiedlichen Rechnern an den Netzenden und/oder bei den Intermediären ausgetauscht werden. In der Folge gibt keines der versandten Datenpakete Aufschluss über die Standorte sämtlicher Beteiligter an den Netzenden. Viele Pakete sagen über diese Standorte vielmehr überhaupt nichts aus.

Dies lässt sich an einem Beispiel illustrieren: Die allermeisten Privatpersonen und auch viele kleinere Organisationen oder Unternehmen nutzen für Versand und Empfang von E-Mails Dienstleister, die Mailserver mit ihrer eigenen Rechnerinfrastruktur betreiben. Verschickt A aus Augsburg eine E-Mail an B aus Berlin und nutzen sie verschiedene E-Mail-Dienstleister, so umfasst der grundrechtlich geschützte Telekommunikationsvorgang zwischen A und B (mindestens) drei technisch separate Datenflüsse: Zunächst verschickt A Datenpakete an seinen E-Mail-Dienstleister. Der E-Mail-Dienstleister von A verschickt Datenpakete an den E-Mail-Dienstleister von B. Schließlich verschickt der E-Mail-Dienstleister von B Datenpakete an B.

Diese Datenflüsse können zeitlich erheblich auseinanderliegen und werden typischerweise völlig unterschiedliche Übertragungsstrecken nehmen, die nicht alle durch die Bundesrepublik laufen müssen, insbesondere wenn sich beide E-Mail-Dienstleister im Ausland befinden. Es ist darum davon auszugehen, dass im Rahmen einer strategischen Telekommunikationsüberwachung oftmals oder sogar in der Regel nur einer der drei Datenflüsse erfasst wird. Je nachdem, welche Datenpakete auf der Übertragungsstrecke erfasst werden, sind Rückschlüsse auf den Standort von A, auf den Standort von B oder nur auf die – für die Unterscheidung von inländischer, internationaler und ausländischer Telekommunikation irrelevanten – Standorte der Dienst-

leister von A und B möglich. In keinem Fall können sowohl A als auch B anhand der IP-Adressen der erfassten Datenpakete lokalisiert werden.

Unter den heutigen technischen Bedingungen lässt sich darum das Tatbestandsmerkmal der internationalen Telekommunikation nur mit Hilfe von groben Faustregeln handhaben, die das Gesetz nicht konturiert. Der kürzlich vorgelegte Bericht über die tatsächliche Überwachungspraxis des Bundesnachrichtendienstes bestätigt dies. Danach arbeitet das vom Bundesnachrichtendienst eingesetzte DAFIS-Filtersystem – soweit es internationale Telekommunikationsverkehre erkennen soll[1] – zweistufig: Auf der ersten Stufe werden Telekommunikationsverkehre aufgrund zuordenbarer technischer Parameter vorgefiltert. Für die Telefonie wird die Landesvorwahl, für paketvermittelte Kommunikation die Top-Level-Domain (also Kennungen wie „de“, „com“ oder „uk“) genannt. Auf der zweiten Stufe werden die Verkehre mit einer Positivliste abgeglichen. Diese enthält Telekommunikationskennungen, die bekanntermaßen deutschen Staatsangehörigen zugeordnet sind, ohne dass dies aufgrund technischer Merkmale erkennbar wäre. Die Positivliste wird lediglich anlassbezogen ergänzt, nicht aber routinemäßig befüllt. Sie ist anscheinend auch nicht sehr umfangreich,

> vgl. Graulich, Bericht für den NSA-Untersuchungsausschuss, öffentliche Fassung, 2015, S. 27 ff.

Es liegt auf der Hand, dass die Filterkriterien auf der ersten Stufe nur äußerst grob zugeschnitten sind. Beispielsweise lässt der Umstand, dass eine E-Mail von einer E-Mail-Adresse der Domain outlook.com an eine E-Mail-Adresse der Domain gmail.com versendet wurde, keine Schlüsse auf Staatsangehörigkeiten und Aufenthaltsorte von Sender und Empfänger zu. Dies gälte selbst dann noch, wenn weitere Metadaten wie die Zeichencodierung einbezogen würden. Beispielsweise kommunizieren zahlreiche deutsche Staatsbürger innerhalb der Bundesrepublik miteinander auf Arabisch. Selbst nach der Auswertung werden sich erhobene Telekommunikationsverkehre vielfach nicht klar verorten lassen.

Die Positivliste auf der zweiten Stufe könnte allenfalls dann einen nennenswerten zusätzlichen Filterertrag erbringen, wenn sie fortlaufend aktualisiert und proaktiv erweitert würde. Dies würde – selbst wenn man von den nicht unerheblichen datenschutzrechtlichen Bedenken absieht, die gegen die Füh-

[1] Der auf der dritten Stufe eingesetzte Filter zum Schutz deutscher Interessen dient nicht dem Grundrechtsschutz und bleibt hier außer Betracht.

rung einer solchen Liste ohne besondere gesetzliche Grundlage sprächen – einen praktisch nicht zu leistenden Aufwand erfordern, zumal es kein zentrales Verzeichnis der Kommunikationskennungen im Netz und ihrer Inhaber gibt.

Somit ist davon auszugehen, dass im Rahmen von strategischen Beschränkungen nach §§ 5 ff. G 10 in weitem Umfang auch rein inländische (oder rein ausländische) Telekommunikationsverkehre erfasst und ausgewertet werden,

> nach einem als geheim eingestuften, aber gleichwohl jüngst an die Öffentlichkeit gelangten Prüfbericht der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit weist das DAFIS-Filtersystem „erhebliche systemische Defizite“ auf; der Bericht ist abrufbar unter https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling (letzter Abruf am 10. November 2016).

Das Tatbestandsmerkmal der internationalen Telekommunikation birgt insgesamt so erhebliche Anwendungsprobleme, dass seine Begrenzungswirkung als sehr gering zu veranschlagen ist,

> kritisch auch etwa Caspar, PinG 2014, S. 1 (2 f.).

cc) Ausmaß der Überwachung: Zweifelhafte Wirksamkeit der 20%-Grenze

Auch das *Ausmaß* der Überwachung wird durch das Gesetz allenfalls begrenzt wirksam eingeschränkt. Eine Obergrenze hierfür enthält § 10 Abs. 4 Sätze 3 und 4 G 10. Danach muss die Überwachungsanordnung festlegen, welcher Anteil der Übertragungskapazität überwacht werden darf, die auf den betroffenen Übertragungswegen zur Verfügung steht. Dieser Anteil darf höchstens 20% betragen.

Nach der Begründung dieser Norm soll die Obergrenze die Ausdehnung der strategischen Telekommunikationsüberwachung auf den leitungsgebundenen Telekommunikationsverkehr kompensieren,

> BT-Drs. 14/5655, S. 18.

Ob die Obergrenze das Ausmaß der Überwachung tatsächlich vergleichbar wirksam begrenzt wie die frühere Beschränkung der Überwachung auf den nicht-leitungsgebundenen Verkehr, ist jedoch zweifelhaft.

In der Praxis wird die Obergrenze nach der Gesamtkapazität aller Übertragungswege bemessen, auf die sich eine Überwachungsanordnung bezieht. Der Bundesnachrichtendienst muss danach aus den angeordneten Übertragungswegen eine Auswahl treffen,

vgl. BVerwG, Urteil vom 28. Mai 2014 – 6 A 1.13 –, juris, Rn. 29

Damit verhindert § 10 Abs. 4 Sätze 3 und 4 G 10 zwar immerhin eine Totalüberwachung des internationalen Telekommunikationsverkehrs zur Aufklärung eines bestimmten Gefahrbereichs. Allerdings setzt die Norm einen Anreiz, in die Anordnung möglichst viele Übertragungswege aufzunehmen, um eine möglichst hohe Gesamtkapazität zu erreichen, nach der sich die Obergrenze bemisst. Zudem kann der Bundesnachrichtendienste danach eine Überwachungsdichte von mehr als 20% des tatsächlichen Übertragungsvolumens auf den betreffenden Übertragungswegen erzielen, indem er für die Überwachung solche Übertragungswege auswählt, die besonders intensiv genutzt werden. Schließlich ergehen jeweils eigenständige Anordnungen für die unterschiedlichen Gefahrbereiche des § 5 Abs. 1 G 10. Diese Anordnungen setzt das G 10 nicht zueinander in Bezug. Der Bundesnachrichtendienst ist also rechtlich nicht gehindert, aufgrund mehrerer Überwachungsanordnungen insgesamt einen erheblichen Anteil aller internationalen Übertragungswege strategisch zu überwachen, der deutlich über der Kapazitätsobergrenze liegen könnte.

dd) Modalitäten der Überwachung: Unvollständiger Schutz vor einer personengerichteten Überwachung

Hinsichtlich der *Modalitäten* der Überwachung hat das angerufene Gericht in seinem Urteil vom 14. Juli 1999 das in § 3 Abs. 2 Satz 2 G 10-a.F. (heute § 5 Abs. 2 Satz 2 G 10) enthaltene Verbot hervorgehoben, mittels formeller Suchbegriffe bestimmte individuelle Anschlüsse gezielt zu überwachen. Dieses Verbot sei verfassungsrechtlich unabdingbar,

BVerfGE 100, 313 (384).

Ob § 5 Abs. 2 Satz 2 G 10 den Zweck, eine gezielte Überwachung bestimmter Personen zu verhindern, heute noch vollumfänglich erfüllt, ist jedoch zweifelhaft. Grund hierfür ist, dass das Verbot bestimmter Suchbegriffe sich auf Telekommunikations*anschlüsse* bezieht. Dieses Verbot schützt vor der gezielten Erfassung bestimmter Telekommunikations*teilnehmer* nur dann

umfassend, wenn Telekommunikationsverkehre stets durch solche Anschlüsse zugeordnet werden.

Das G 10 definiert selbst nicht, was ein Telekommunikationsanschluss ist. Es liegt nahe, zur Interpretation dieses Begriffs § 2 Nr. 10 TKÜV heranzuziehen, der einem verwandten Regelungskontext entstammt. Danach ist ein Telekommunikationsanschluss der durch eine Adressierungsangabe bezeichnete Zugang zu einer Telekommunikationsanlage, der es einem Nutzer ermöglicht, Telekommunikationsdienste zu nutzen. Eine Telekommunikationsanlage ist nach § 3 Nr. 23 TKG eine technische Einrichtung, die als Nachrichten identifizierbare Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren kann.

Die Begriffe der Telekommunikationsanlage und des damit verbundenen Telekommunikationsanschlusses beziehen sich danach auf die technische Schicht der Signalübertragung, nicht aber auf die Dienstschicht, die auf der Signalübertragung aufsitzt. Damit sind Teilnehmerkennungen auf der Dienstschicht vom Begriff des Telekommunikationsanschlusses nicht umfasst. Sie dürfen gemäß § 5 Abs. 2 Satz 2 G 10 unbeschränkt als formale Suchbegriffe genutzt werden.

Dies ist insbesondere für die Internetkommunikation bedeutsam. Beispielsweise beziehen sich E-Mail-Adressen auf E-Mail-Postfächer und nicht auf Telekommunikationsanschlüsse wie einen DSL-Anschluss oder einen Mobilfunkzugang. E-Mail-Postfächer und Telekommunikationsanschlüsse sind technisch auch nicht miteinander verknüpft. Ein E-Mail-Postfach kann vielmehr grundsätzlich von jedem Telekommunikationsanschluss weltweit aus angesteuert werden. Folgerichtig regelt etwa § 111 Abs. 1 Satz 3 TKG die Verpflichtung von E-Mail-Anbietern zur Speicherung bestimmter Bestandsdaten zusätzlich zu der entsprechenden Verpflichtung der Anbieter von Telekommunikationsanschlüssen. Wird der Wortlaut von § 5 Abs. 2 Satz 2 G 10 ernst genommen, so darf der BND den Datenstrom anhand beliebiger E-Mail-Adressen auswerten und so personenbezogene Überwachungen durchführen. Dabei wiegt die grundrechtliche Gefährdungslage nicht weniger schwer als etwa bei einer Auswertung anhand von Telefonnummern.

Demgegenüber versteht der Bundesnachrichtendienst den Begriff des Telekommunikationsanschlusses in der Praxis anscheinend derzeit weiter und fasst darunter jegliche Teilnehmerkennungen. Für die verfassungsrechtliche Beurteilung der rechtlichen Grenzen, die das G 10 der strategischen Tele-

kommunikationsüberwachung setzt, ist dies jedoch nicht entscheidend. Hierfür kommt es nicht darauf an, wie der Bundesnachrichtendienst auf der Grundlage des Gesetzes faktisch vorgeht. Maßgeblich ist, wie er vorgehen könnte, ohne gegen das Gesetz zu verstoßen.

b) Gestiegene Sensibilität von Telekommunikationsdaten

Zu diesen rechtlichen und faktischen Entgrenzungen der Überwachung kommt hinzu, dass sich seit dem Urteil vom 14. Juli 1999 die Sensibilität von Telekommunikationsdaten erheblich gesteigert hat. Hierfür gibt es mehrere Gründe:

Erstens sind ein quantitativer Anstieg und ein qualitativer Wandel der Telekommunikation zu verzeichnen. Eine erhebliche Zunahme ist bereits für die Individualkommunikation zu beobachten, die in immer größerem Ausmaß über Telekommunikationsnetze vermittelt wird. So ist heute davon auszugehen, dass eine große Mehrheit der Bevölkerung neben einem Festnetzanschluss auch über ein Mobiltelefon verfügt. Zudem haben sich im Internet zahlreiche Kommunikationsdienste mit unterschiedlichen kommunikativen Eigenschaften ausdifferenziert, etwa E-Mail, Instant Messaging, Diskussionsforen oder Soziale Netzwerke. Hinzu kommt, dass Telekommunikationsnetze immer mehr genutzt werden, um Dienstleistungen ohne unmittelbaren kommunikativen Bezug zu erbringen. Hierdurch wandelt sich die Telekommunikation von einer immerhin noch auf bestimmte kommunikative Zwecke bezogenen Technologie zu einer allgegenwärtigen Basisinfrastruktur, die große Teile der Lebenswelt durchdringt. Beispielhaft sei die zunehmende Ausstattung von Alltagsgegenständen wie Kraftfahrzeugen oder haustechnischen Anlagen mit vernetzten informationstechnischen Komponenten genannt.

Zweitens ist die Aussagekraft von Telekommunikationsdaten seit 1999 erheblich gestiegen. Während damals insbesondere die Möglichkeiten des Bundesnachrichtendienstes zur Erfassung und zur automatisierten Analyse der erfassten Telekommunikation relativ eng begrenzt waren,

> vgl. zu den damaligen – heute nahezu archaisch anmutenden – technischen Verhältnissen BVerfGE 100, 313 (379 ff.): so wurde damals gerade eine „Ausdehnung der Beobachtung auf E-Mail angestrebt“, und nur Telex-Verkehre waren „maschinell vollständig abgleichbar“,

lassen sich heute Telekommunikationsdaten in vollkommen anderer Quantität erfassen, und aus den erfassten Daten kann der Bundesnachrichtendienst mit heutiger Analysetechnologie automatisch zahlreiche hochsensible Informationen gewinnen. Deutlich aussagekräftiger als 1999 sind etwa Telekommunikations-Verkehrsdaten (in der sicherheitspolitischen Diskussion in der Regel als „Metadaten“ bezeichnet). Aus ihnen können weitreichende Rückschlüsse auf das Verhalten und die sozialen Beziehungen Einzelner gezogen werden, da sie sich – anders als manche Inhaltsdaten – inzwischen sehr weitgehend automatisiert auswerten und so beispielsweise zu Bewegungs- und Kommunikationsprofilen einzelner Personen oder zu komplexen Beziehungsnetzwerken aggregieren lassen,

> ein instruktives Auswertungsbeispiel findet sich unter https://netzpolitik.org/2014/metadaten-wie-dein-unschuldiges-smartphone-fast-dein-ganzes-leben-an-den-geheimdienst-uebermittelt (letzer Abruf am 10. November 2016).

Das angerufene Gericht ist hierauf bereits in seinem Vorratsdatenurteil vom 2. März 2010 näher eingegangen,

> vgl. BVerfGE 125, 260 (319).

Diese Entwicklung hält weiter an, zumal auch viele Inhalte der Telekommunikation – wie Beiträge in Sozialen Netzwerken und deren Metadaten oder die Texte von E-Mails oder Kurznachrichten – mittlerweile automatisch analysiert werden können. Die anhaltende Tendenz zur Vernetzung von Gegenständen ohne kommunikative Funktion steigert die Aussagekraft von Telekommunikationsdaten nochmals. So lassen sich aus den Daten, die vernetzte informationstechnische Komponenten in Fahrzeugen oder haustechnischen Anlagen erzeugen und übermitteln, zahlreiche sensible Informationen über Einzelne gewinnen.

Die technische und soziale Entwicklung hat insgesamt zur Folge, dass die Sensibilität von Telekommunikationsdaten gegenüber breit streuenden Erfassungen und Auswertungen fundamental anders zu beurteilen ist als im Jahr 1999. Unter den heutigen Bedingungen ist deshalb eine anlasslose strategische Überwachung der Telekommunikation unabhängig von dem damit verfolgten behördlichen Zweck in jedem Fall als Grundrechtseingriff von sehr hoher Intensität anzusehen.

c) Folgerungen aus der gestiegenen Eingriffsintensität

Angesichts der stark gestiegenen Eingriffsintensität strategischer Telekommunikationsüberwachungen erscheint zweifelhaft, ob solche Überwachungen überhaupt dem Verhältnismäßigkeitsgrundsatz genügen können. Aufgrund der technischen und ermittlungstaktischen Nähe zwischen strategischen Telekommunikationsüberwachungen und Rasterfahndungen liegt es näher, als verfassungsrechtliche Mindestschwelle für eine großflächige Erfassung und Auswertung der Telekommunikation wenigstens eine konkrete Gefahr für ein gewichtiges Rechtsgut zu fordern,

> vgl. zur konkreten Gefahr als Mindestschwelle für präventivpolizeiliche Rasterfahndungen BVerfGE 115, 320 (357 ff.).

Um den Einsatz formeller Suchbegriffe zu legitimieren, mag hierunter auch noch ein konkreter, durch hinreichend spezifische Anknüpfungstatsachen begründeter „Gefährlichkeitsverdacht“ gegen die durch einen Suchbegriff bezeichneten Personen oder Gruppierungen zu verstehen sein,

> vgl. zur Konturierung des verfassungsrechtlichen Gefahrbegriffs, wenngleich zumindest primär mit Bezug auf Ermittlungsmaßnahmen geringerer Streubreite BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 109 ff.

Das Erfordernis einer konkreten Gefahr oder eines konkreten „Gefährlichkeitsverdacht“ kann die extreme Streubreite der großflächigen Telekommunikationsüberwachung kompensieren, da es Dauer und Ausmaß der Überwachung wirksam begrenzt. Aufgrund eines solchen konkreten Anlasses ist auch die Erfassung und Auswertung hochsensibler Datenbestände grundrechtlich hinnehmbar, wie sie bei der Telekommunikation anfallen. Die weitgehend anlasslose, nur durch ein Aufklärungsziel programmierte strategische Überwachung, welche § 5 G 10 ermöglicht, lässt sich hingegen heute nicht mehr legitimieren.

Dieser Neubestimmung der verfassungsrechtlichen Mindestschwelle lässt sich die besondere Aufgabe des Bundesnachrichtendienstes zur Auslandsaufklärung nicht entgegenhalten. Zwar hat das angerufene Gericht mehrfach ausgeführt, dass die Aufgaben der Nachrichtendienste im Vergleich mit Gefahrenabwehr- und Strafverfolgungsbehörden weitergehende Überwachungsbefugnisse im Vorfeld der hergebrachten Eingriffsschwellen der konkreten Gefahr und des Anfangsverdachts einer Straftat rechtfertigen,

eingehend zu den unterschiedlichen Aufgaben und ihren Implikationen BVerfGE 133, 277 (324 ff.); niedrigere Eingriffsschwellen in nachrichtendienstlichen Eingriffsermächtigungen werden ausdrücklich für verfassungskonform befunden in BVerfGE 100, 313 (383); 130, 151 (206).

Hingegen für eine weitgehende „Deprivilegierung der Geheimdienste“ jüngst Wegener, VVDStRL 75 (2016), S. 293 (312 ff.).

Dies gilt jedoch nicht für Überwachungsmaßnahmen von besonders hoher Eingriffsintensität wie die strategische Telekommunikationsüberwachung. Vielmehr hat das angerufene Gericht für solche Maßnahmen in seiner jüngeren Rechtsprechung deutlich gemacht, dass die verfassungsrechtlichen Maßstäbe für alle präventiv tätigen Behörden gleich zu bestimmen sind,

vgl. für „Online-Durchsuchungen“ BVerfGE 120, 274 (329 ff.); für den Abruf bevorrateter Telekommunikations-Verkehrsdaten BVerfGE 125, 260 (331 f.); für Wohnraumüberwachungen im Zusammenhang mit Datenübermittlungen an die Nachrichtendienste BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 320.

Selbst wenn jedoch strategische Telekommunikationsüberwachungen im Sinne von § 5 G 10 verfassungsrechtlich überhaupt noch hinzunehmen sein sollten, müssen zumindest die verfassungsrechtlichen Anforderungen an die Ziele solcher Überwachungen ihrer deutlich erhöhten Eingriffsintensität angepasst werden.

Das Überwachungsziel ist nach dem Urteil des angerufenen Gerichts vom 14. Juli 1999 maßgeblicher Anknüpfungspunkt für eine Neubestimmung der materiellen verfassungsrechtlichen Anforderungen an strategische Telekommunikationsüberwachungen, da solche Überwachungen ohne konkreten Anlass durchgeführt werden,

vgl. BVerfGE 100, 313 (384).

Anders als das angerufene Gericht seinerzeit angenommen hat,

BVerfGE 100, 313 (382),

reicht die Früherkennung gewichtiger Kriminalität von außenpolitischer Bedeutung angesichts der erheblich gesteigerten Eingriffstiefe strategischer Telekommunikationsüberwachungen nicht mehr generell aus, um solche Über-

wachungen zu legitimieren. Allenfalls zur Aufklärung existenzieller Gefahren für die Sicherheit der Bundesrepublik kann dieser Eingriff möglicherweise noch hingenommen werden.

Diesen modifizierten verfassungsrechtlichen Maßstab verfehlt § 5 Abs. 1 Satz 3 Nr. 8 G 10. Die Norm beschränkt die strategische Telekommunikationsüberwachung nicht auf existenzielle Gefährdungen. Sie ermöglicht sie vielmehr zur Früherkennung aller erheblichen Erscheinungsformen internationaler IT-Kriminalität, sofern die Täter informationstechnische Mittel einsetzen. Dies schließt Handlungen ein, die erhebliche Schäden verursachen mögen, die Sicherheit der Bundesrepublik insgesamt jedoch nicht ansatzweise in Frage stellen. Selbst Angriffe auf informationstechnische Systeme in der Bundesrepublik, die von fremden Staaten ausgehen, erreichen diese Schwelle nicht quasi automatisch.

2. Verfassungswidrigkeit von § 5 Abs. 1 Satz 3 Nr. 8 G 10 auf der Grundlage der bisherigen Maßstäbe

Im Übrigen verfehlt die neue Überwachungsermächtigung in § 5 Abs. 1 Satz 3 Nr. 8 G 10 die verfassungsrechtlichen Anforderungen selbst dann, wenn die im Urteil vom 14. Juli 1999 entwickelten Maßstäbe unmodifiziert herangezogen werden.

Bereits nach diesem Urteil darf die strategische Telekommunikationsüberwachung nicht zur Früherkennung jeglicher Erscheinungsformen der erheblicheren grenzüberschreitenden Kriminalität eingesetzt werden. Die betreffenden Kriminalitätsfelder müssen sich vielmehr durch ein besonderes Gefahrenpotenzial für Bestand oder Sicherheit der Bundesrepublik auszeichnen. Dies wurde insbesondere bejaht für Deliktsbereiche, die in besonderem Maße Kollektivgüter gefährden. So bedrohen Schleusungsdelikte die territoriale Integrität der Bundesrepublik. Proliferationsstraftaten bergen das Risiko eines mit Kriegswaffen geführten Konflikts. Betäubungsmittelstraftaten großen Ausmaßes können mittelbar aufgrund von Geldwäschehandlungen den legalen Wirtschaftskreislauf bedrohen,

> vgl. zu der sicherheitspolitisch vor allem in den 1990er Jahren geführten Auseinandersetzung über das Bedrohungspotenzial der organisierten Kriminalität Bäcker, Kriminalpräventionsrecht, 2015, S. 36 ff., m.w.N.

Demgegenüber hat das angerufene Gericht den in § 3 Abs. 1 Satz 2 Nr. 5 G 10-a.F. benannten Gefahrbereich der im Ausland begangenen Geldfälschung nicht für hinreichend gewichtig gehalten, um strategische Telekommunikationsüberwachungen zu legitimieren. Insbesondere begrenzte die Norm das Überwachungsziel nicht auf erhebliche Gefahren für Kollektivgüter, die etwa entstehen können, wenn durch Geldfälschungen großen Stils die Geldwertstabilität der Bundesrepublik und damit die Wirtschaftskraft des Landes in gewichtigem Maß bedroht werden,

BVerfGE 100, 313 (384 f.).

Die Überwachungsermächtigung in § 5 Abs. 1 Satz 3 Nr. 8 G 10 ist in vergleichbarer Weise zu weit gefasst. Sie ermöglicht strategische Telekommunikationsüberwachungen generell mit dem Ziel, erhebliche illegale Angriffe auf IT-Systeme mit informationstechnischen Mitteln aufzudecken, wenn sie einen Bezug zur Bundesrepublik aufweisen. Hierunter fallen nicht nur Angriffe, die in ihrem Gewicht einem bewaffneten Angriff oder einem terroristischen Anschlag nahekommen, wie etwa gezielte Manipulationen kritischer Infrastrukturen. Vielmehr kann die strategische Überwachung nach dem Gesetzeswortlaut zur Früherkennung jeglicher Form schwerer wiegender IT-Kriminalität dienen. Hierunter ließe sich auch etwa der Betrieb eines größeren sogenannten Botnetzes durch eine kriminelle Gruppierung subsumieren, mit dessen Hilfe Bankdaten ausspioniert und zu unbefugten Transaktionen missbraucht werden sollen. Dabei handelt es sich um gewichtige Kriminalität, die jedoch nicht das Bedrohungspotenzial für das Gemeinwesen aufweist, welches das angerufene Gericht in seinem Urteil vom 14. Juli 1999 zur Legitimation strategischer Telekommunikationsüberwachungen gefordert hat.

III. Verwendung formeller Suchbegriffe zulasten von Ausländern im Ausland (§ 5 Abs. 2 Satz 3 G 10)

§ 5 Abs. 2 Satz 3 G 10 enthält eine Ausnahme von dem in § 5 Abs. 2 Satz 2 Nr. 1 G 10 enthaltenen Verbot der gezielten Überwachung bestimmter individueller Anschlüsse. Diese Ausnahme gilt für Anschlüsse im Ausland, deren Inhaber und regelmäßige Nutzer Ausländer sind. Sie ermöglicht gegenüber diesem Personenkreis die Verwendung formeller Suchbegriffe, die sich gerade dadurch auszeichnen, dass sie individuelle Kennungen von Telekommunikationsteilnehmern enthalten.

Das angerufene Gericht hat in seinem Urteil vom 14. Juli 1999 die Vorgängerregelung von § 5 Abs. 2 Satz 2 Nr. 1 G 10 als unabdingbare Voraussetzung einer verhältnismäßigen strategischen Telekommunikationsüberwachung bezeichnet,

> BVerfGE 100, 313 (384).

Dies muss auch für Anschlüsse von ausländischen Kommunikationsteilnehmern im Ausland gelten, da dieser Personenkreis materiell gleichermaßen durch das Fernmeldegeheimnis geschützt wird wie Personen im Inland und deutsche Staatsangehörige im Ausland (siehe oben C I 3). § 5 Abs. 2 Satz 3 G 10 ermöglicht daher unverhältnismäßige Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG. Zudem verstößt er wegen der sachwidrigen Schlechterstellung von ausländischen Kommunikationsteilnehmern im Ausland gegen den Gleichheitssatz des Art. 3 Abs. 1 GG,

> für verfassungswidrig halten § 5 Abs. 2 Satz 3 G 10 etwa Müller-Terpitz, Jura 2000, S. 296 (302); Huber, NJW 2013, S. 2572 (2573 f.); Caspar, PinG 2014, S. 1 (5); Durner, in: Maunz/Dürig, GG, Art. 10 Rn. 186; Gusy, in: v. Mangoldt/Klein/Starck (Hrsg.), GG, 6. Aufl. 2010, Art. 10 Rn. 99; Roggan, G 10, 2012, § 5 Rn. 22; Hermes, in: Dreier (Hrsg.), GG, 3. Aufl. 2013, Art. 10 Rn. 43.

Selbst wenn das materiell-grundrechtliche Schutzniveau des Art. 10 Abs. 1 GG für Ausländer im Ausland niedriger als für deutsche Staatsangehörige anzusetzen wäre, wäre § 5 Abs. 2 Satz 3 G 10 im Ergebnis verfassungsrechtlich nicht zu halten. Mindestens ist auch für Überwachungen von Ausländern im Ausland zu fordern, dass dem Einsatz formeller Suchbegriffe Auswahlkriterien zugrunde liegen, die gewährleisten, dass die gezielte Suche nach bestimmten Personen auf einer hinreichenden Tatsachengrundlage und einem hinreichenden Näheverhältnis zu dem aufzuklärenden Gefahrbereich beruht. Hierzu müssen qualifizierte Anforderungen an die „Gefährlichkeit“ derjenigen formuliert werden, nach denen gesucht wird. Es ist Aufgabe des Gesetzgebers, diese Kriterien vorzugeben und so das personen- oder gruppenbezogene Prognoseurteil, das dem Einsatz eines formellen Suchbegriffs zugrunde liegt, rechtsstaatlich handhabbar und kontrollierbar zu gestalten,

> näher zu denkbaren normativen Vorgaben für solche Gefährlichkeitsurteile Bäcker, Kriminalpräventionsrecht, 2015, S. 205 ff.

Wegen der hohen Eingriffsintensität der strategischen Telekommunikationsüberwachung ist es nicht hinnehmbar, daneben auch eine gezielte Suche nach Personen oder Organisationen zu ermöglichen, von denen selbst keine Schäden befürchtet werden, die aber mit „Gefährdern“ in – möglicherweise nur losem oder über Dritte vermittelten – Kontakt stehen. Wäre dies anders zu sehen, müsste die Überwachungsermächtigung zumindest Kriterien für die Auswahl der Suchbegriffe vorgeben, die gewährleisten, dass die Inanspruchnahme dieser Betroffenen die grundrechtliche Opfergrenze wahrt,

> vgl. allgemein zu den verfassungsrechtlichen Grenzen einer gezielten Inanspruchnahme Dritter BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 114 ff.

Demgegenüber enthält § 5 Abs. 2 Satz 3 G 10 überhaupt keine Kriterien für die Auswahl formeller Suchbegriffe, die sich auf die Anschlüsse von Ausländern im Ausland beziehen. Dem Bundesnachrichtendienst wird so ermöglicht, aus diesem Personenkreis nach nachrichtendienstlichen Kriterien eine Auswahl zu treffen, die gesetzlich nur insoweit angeleitet wird, als gemäß § 5 Abs. 2 Satz 1 G 10 überhaupt ein Bezug zu dem Gefahrbereich bestehen muss. Dies ermöglicht letztlich eine personengerichtete Überwachung annähernd nach Gutdünken. Eine so weitgehende Freigabe der gezielten Suche nach Personen und Gruppierungen kann auch mit abgesenkten grundrechtlichen Anforderungen nicht vereinbar sein.

Unklar ist schließlich, ob sich die Ausnahmeregelung des § 5 Abs. 2 Satz 3 G 10 auch auf das in § 5 Abs. 2 Satz 2 Nr. 2 G 10 enthaltene Verbot von Suchbegriffen bezieht, die den Kernbereich privater Lebensgestaltung betreffen. Eine Ausnahme von diesem Verbot ließe sich jedenfalls nicht rechtfertigen. Der prozedurale Schutz des Kernbereichs privater Lebensgestaltung, zu dem § 5 Abs. 2 Satz 2 Nr. 2 G 10 beiträgt, wurzelt unmittelbar in der durch Art. 1 Abs. 1 GG garantierten Unverletzlichkeit der Menschenwürde,

> vgl. zuletzt BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 120.

Zumindest der elementare grundrechtliche Schutzstandard, den Art. 1 Abs. 1 GG vermittelt, muss unmodifiziert allen Menschen unabhängig von Staatsangehörigkeit und Aufenthaltsort zugutekommen. Im Übrigen ist auch nicht nachvollziehbar, inwieweit eine gezielte Ausforschung des Kernbereichs privater Lebensgestaltung von Ausländern im Ausland durch entsprechende

Suchbegriffe zur Aufgabenerfüllung des Bundesnachrichtendienstes beitragen könnte.

IV. Benachrichtigung des Betroffenen (§ 12 Abs. 1 Satz 2 i.V.m. Abs. 2 Satz 1 G 10)

Nach der Rechtsprechung des angerufenen Gerichts gehört zu den Anforderungen an die verfassungskonforme Regulierung verdeckter Überwachungsmaßnahmen die gesetzliche Anordnung von Benachrichtigungspflichten. Dies ergibt sich aus dem Grundrecht, in das die Überwachung eingreift (hier also Art. 10 Abs. 1 GG), sowie aus Art. 19 Abs. 4 GG. Ausnahmen von der Benachrichtigung kann der Gesetzgeber in Abwägung mit verfassungsrechtlich geschützten Rechtsgütern Dritter vorsehen. Ausnahmeregelungen sind jedoch auf das unbedingt Erforderliche zu beschränken und müssen dem Gebot der Normenklarheit und Bestimmtheit genügen,

> vgl. zuletzt BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 136.

Diese Grundsätze sind auf Überwachungsmaßnahmen gemäß § 5 Abs. 1 Satz 3 Nr. 8 G 10 vollumfänglich zu übertragen. Insbesondere erfasst Art. 10 Abs. 2 Satz 2 GG, der eine weitergehende Beschränkung der Benachrichtigungspflicht ermöglicht, diese Maßnahmen nicht. Die geregelten Ausnahmen von der Benachrichtigungspflicht sind vielmehr an Art. 10 Abs. 2 Satz 1 GG sowie an Art. 19 Abs. 4 GG zu messen,

> vgl. BVerfGE 100, 313 (397).

Für strategische Telekommunikationsüberwachungen nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 sieht zwar § 12 Abs. 1 Satz 1 i.V.m. Abs. 2 Satz 1 G 10 grundsätzlich vor, die betroffenen Personen nach Einstellung der Maßnahme zu benachrichtigen. Jedoch enthält § 12 Abs. 1 Satz 2 i.V.m. Abs. 2 Satz 1 G 10 so weitreichende Ausnahmen von der Benachrichtigungspflicht, dass die Benachrichtigung annähernd ins Belieben des Bundesnachrichtendienstes gestellt wird. Dies ist mit den aus Art. 10 Abs. 2 Satz 1 und Art. 19 Abs. 4 GG folgenden Anforderungen nicht zu vereinbaren.

Bereits sehr weit geht der Ausnahmetatbestand in § 12 Abs. 1 Satz 2 Alt. 1 G 10, nach dem die Benachrichtigung unterbleibt, solange eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann. Zwar ist

die Sicherung des Überwachungszwecks grundsätzlich ein verfassungsrechtlich tragfähiger Grund, die Benachrichtigung zurückzustellen,

> vgl. etwa BVerfGE 129, 208 (254); BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 136.

Indem jedoch § 12 Abs. 1 Satz 2 Alt. 1 G 10 die Benachrichtigung generell sperrt, solange eine Gefährdung des Überwachungszwecks lediglich *nicht auszuschließen* ist, lässt die Norm ihrem Wortlaut nach bereits entfernte Risiken ausreichen, damit der Ausnahmetatbestand greift. Angesichts des großflächigen Überwachungsansatzes bei Maßnahmen nach § 5 G 10 wird sich praktisch nie mit Sicherheit ausschließen lassen, dass eine Benachrichtigung solche Risiken birgt. § 12 Abs. 1 Satz 2 Alt. 1 G 10 beschränkt die Benachrichtigungspflicht daher unverhältnismäßig weit. Zumindest bedarf die Norm einer verfassungskonformen Auslegung, nach der die Benachrichtigung nur ausgeschlossen ist, wenn konkrete Tatsachen für eine Gefährdung des Überwachungszwecks sprechen,

> implizit verlangt solche positiven Anhaltspunkte auch BVerfGE 100, 313 (397 f.); vgl. ferner die nochmals einschränkende Auslegung des ohnehin deutlich restriktiver gefassten Ausnahmetatbestands des § 20w Abs. 2 Satz 1 Hs. 2 BKAG durch BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 261.

Unverhältnismäßig und auch keiner verfassungskonformen Auslegung zugänglich ist § 12 Abs. 1 Satz 2 Alt. 2 G 10, der die Benachrichtigung ausschließt, solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist.

Sowohl der Begriff des Bundes- oder Landeswohls als auch der Begriff der übergreifenden Nachteile sind weitgehend unbestimmt und grenzen den Grund für eine Zurückstellung der Benachrichtigung praktisch nicht ein. Zudem müssen die Nachteile nach dem Wortlaut der Norm in keinem Zusammenhang mit dem Überwachungszweck stehen, so dass der Ausnahmetatbestand auch hierdurch nicht konkretisiert wird. Letztlich lässt sich unter das Wohl des Bundes oder eines Landes – anders als unter den etwa in § 20w Abs. 2 Satz 1 BKAG aufgeführten Bestand des Staates – der gesamte Aufgabenkreis des Bundesnachrichtendienstes oder auch jeder anderen Behörde subsumieren,

vgl. zur Interpretation dieses Begriffs im Rahmen von § 96 StPO Ritzert, in: BeckOK StPO, § 96 Rn. 4: „Der Begriff des Nachteils für das Staatswohl wird weit gefasst und ist bereits gegeben, wenn die Erfüllung öffentlicher Aufgaben ernstlich gefährdet oder erheblich erschwert würde."

Für die Zurückstellung und – auf der Grundlage von § 12 Abs. 1 Satz 5 i.V.m. Abs. 2 Satz 1 G 10 – den endgültigen Ausschluss der Benachrichtigung reichen damit annähernd beliebige behördliche Opportunitätserwägungen aus, solange diese aufgrund einer normativ nicht angeleiteten Abwägung wichtiger erscheinen als die Benachrichtigung.

Für die Verfassungsmäßigkeit von § 12 Abs. 1 Satz 2 Alt. 2 G 10 lässt sich nicht anführen, dass dieser Ausnahmetatbestand weitgehend wörtlich dem Urteil des angerufenen Gerichts vom 14. Juli 1999 entnommen ist,

vgl. BVerfGE 100, 313 (398).

Das Bundesverfassungsgericht ist keine Rechtsetzungsinstanz, sondern dazu berufen, grundrechtliche Grenzen der Rechtsetzung zu bestimmen. Es kann sinnvoll oder sogar angezeigt sein, im Rahmen verfassungsgerichtlicher Entscheidungen allgemeine, nicht notwendigerweise unmittelbar subsumtionsfähige Formulierungen zu wählen, um so gesetzgeberische Regelungsspielräume offenzuhalten. Hingegen besteht die originäre Aufgabe des Gesetzgebers darin, diese Regelungsspielräume durch einfaches Recht auszufüllen und so die Verfassung zu konkretisieren. Er kann sich dieser Aufgabe zumindest nicht in jedem Fall dadurch entziehen, dass er Formulierungen aus der Rechtsprechung des Bundesverfassungsgerichts schlicht abschreibt.

Insbesondere wäre es sowohl möglich als auch geboten gewesen, den Ausnahmetatbestand zum Schutz des Staatswohls näher zu spezifizieren und so auf hinreichend gewichtige Ausnahmegründe zu beschränken. Hierbei hätten auch spezifisch nachrichtendienstliche Belange wie etwa die Erhaltung von Austauschbeziehungen mit ausländischen Diensten benannt werden können, soweit diese eine Ausnahme von der Benachrichtigungspflicht rechtfertigen können,

vgl. die beispielhafte Aufzählung bei BVerfGE 100, 313 (398).

V. Ermächtigungen zu Datenübermittlungen

Auch die Ermächtigungen des Bundesnachrichtendienstes, die durch eine strategische Telekommunikationsüberwachung gemäß § 5 Abs. 1 Satz 3 Nr. 8 G 10 gewonnenen Daten an andere Behörden zu übermitteln, stehen mit den verfassungsrechtlichen Anforderungen in weitem Umfang nicht in Einklang. Dies gilt gleichermaßen für die Regelungen über Datenübermittlungen an inländische wie an ausländische Behörden.

1. Datenübermittlungen an inländische Behörden (§ 7 Abs. 2, 4 und 4a G 10)

§ 7 Abs. 2, 4 und 4a G 10 enthalten Ermächtigungen zu Datenübermittlungen an unterschiedliche inländische Behörden. Keine von ihnen steht in vollem Umfang mit Art. 10 Abs. 1 GG in Einklang.

Diese Übermittlungsermächtigungen sind an den Anforderungen zu messen, die das angerufene Gericht in seinem Urteil zum BKA-Gesetz an Befugnisse zur zweckändernden Weiterverarbeitung erhobener Daten herausgearbeitet hat. Um eine bloße weitere Nutzung im Rahmen des Erhebungszwecks geht es schon deshalb nicht, weil die Daten an andere Behörden mit anderen Aufgaben übermittelt werden sollen,

> vgl. zur Abgrenzung von weiterer Nutzung und Zweckänderung BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 279.

Zweckänderungsermächtigungen ermöglichen erneute Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG. Sie müssen sicherstellen, dass dem Eingriffsgewicht der Datenerhebung auch hinsichtlich der Weiterverarbeitung Rechnung getragen wird, die an die Zweckänderung anschließen soll. Insbesondere verlangt der Verhältnismäßigkeitsgrundsatz, dass Daten, die durch besonders eingriffsintensive Maßnahmen erlangt wurden, auch nur zu besonders gewichtigen Zwecken genutzt werden dürfen. Als Kriterium hierfür dient die Prüfung einer hypothetischen Datenneuerhebung: Daten aus eingriffsintensiven Überwachungsmaßnahmen dürfen danach nur für solche geänderten Zwecke weiterverarbeitet werden, für die entsprechende Daten mit vergleichbar schwerwiegenden Mitteln erhoben werden dürften,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 284 ff.

Dies bedeutet nicht, dass der Bundesnachrichtendienst Daten, die er durch eine strategische Telekommunikationsüberwachung nach § 5 G 10 gewonnen hat, überhaupt nicht an andere Behörden übermitteln dürfte. Zwar dürften solche Telekommunikationsüberwachungen insbesondere Behörden mit Zwangsbefugnissen im Inland nicht erlaubt werden. Jedoch wird durch eine gezielte Datenübermittlung zu bestimmten behördlichen Zwecken nicht der gesamte Datenbestand des Bundesnachrichtendienstes offengelegt. Eine Datenübermittlung, die sich auf punktuelle relevante Informationen beschränkt, ist daher nicht von vornherein ausgeschlossen,

> BVerfGE 100, 313 (390); BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 287.

Die gesetzliche Übermittlungsschwelle muss jedoch der besonders hohen, in den letzten Jahren erheblich gestiegenen Eingriffsintensität der strategischen Telekommunikationsüberwachung Rechnung tragen (siehe oben II 1). Wegen der extremen Streubreite und der wenig effektiven rechtlichen und faktischen Begrenzungen dieser Überwachung geht ihre Eingriffsintensität insbesondere über die einer anlassbezogenen und auf bestimmte Zielpersonen beschränkten Telekommunikationsüberwachung noch deutlich hinaus. Das Urteil des angerufenen Gerichts vom 14. Juli 1999, das als Referenzmaßnahme für die hypothetische Datenneuerhebung eine solche Telekommunikationsüberwachung herkömmlichen Typs herangezogen hat,

> BVerfGE 100, 313 (394 f.),

ist auch hinsichtlich der verfassungsrechtlichen Mindestschwelle für Datenübermittlungen überholt.

Es liegt vielmehr nahe, für die verfassungsrechtliche Übermittlungsschwelle die Maßstäbe heranzuziehen, die das angerufene Gericht in seinem Urteil zum BKA-Gesetz für die Übermittlung von Daten entwickelt hat, die durch Wohnraumüberwachungen oder „Online-Durchsuchungen“ gewonnen wurden. Eine solche Übermittlung ist verfassungsrechtlich nur zulässig, wenn sie dazu dient, eine konkrete Gefahr für ein besonders bedeutsames Rechtsgut abzuwehren oder den Verdacht einer besonders schweren Straftat aufzuklären,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 291.

Diese Anforderungen verfehlen die gesetzlichen Übermittlungsermächtigungen weit, wie im Folgenden zu zeigen ist.

a) Datenübermittlungen zur Strafverfolgung (§ 7 Abs. 4 Satz 2 G 10)

§ 7 Abs. 4 Satz 2 G 10, der Datenübermittlungen an Strafverfolgungsbehörden regelt, verfehlt die verfassungsrechtlichen Anforderungen in erheblichem Umfang.

Diese Regelung knüpft die Übermittlung an den Verdacht, dass jemand eine Straftat aus dem in § 7 Abs. 4 Satz 1 G 10 enthaltenen Straftatenkatalog, der teils auf § 3 Abs. 1 G 10 und § 100a Abs. 2 StPO weiterverweist, begeht oder begangen hat. Der tatsächliche Übermittlungsanlass deckt sich mit dem strafprozessualen Verdachtsbegriff und begegnet keinen verfassungsrechtlichen Bedenken. § 7 Abs. 4 Satz 2 G 10 ermöglicht die Übermittlung jedoch auch zur Verfolgung von Straftaten, die kein hinreichendes Gewicht haben, um die Übermittlung verfassungsrechtlich zu legitimieren.

Hierzu ist analog zur Übermittlung von Daten, die aus Wohnraumüberwachungen oder „Online-Durchsuchungen“ stammen, zu fordern, dass die Anlasstat der Übermittlung eine besonders schwere Straftat ist. Maßgeblicher Anhaltspunkt hierfür ist der gesetzliche Strafrahmen. Eine besonders schwere Straftat liegt erst vor, wenn die Tat im Höchstmaß mit einer Freiheitsstrafe über fünf Jahren bedroht ist,

> BVerfGE 109, 279 (347 f., 377); BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 316.

Die in § 7 Abs. 4 Satz 2 G 10 in Bezug genommenen Straftatenkataloge gewährleisten nicht durchweg, dass Daten aus strategischen Telekommunikationsüberwachungen nur zur Verfolgung besonders schwerer Straftaten übermittelt werden. Diese Kataloge enthalten vielmehr in weitem Umfang Taten, die lediglich der mittleren Kriminalität zuzuordnen sind oder bei denen es sich sogar um Bagatelldelikte handelt. Insbesondere können zumindest die folgenden Anlasstaten die Datenübermittlung nach dem zugrunde zu legenden strengen Maßstab nicht legitimieren:

Straftatbestand	Katalogtat nach	Strafrahmen (Freiheitsstrafe)
§ 84 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 i.V.m. § 3 Abs. 1 Satz 1	(Drei Monate bis) fünf Jahre

	Nr. 2 G 10	
§ 85 Abs. 1 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 i.V.m. § 3 Abs. 1 Satz 1 Nr. 2 G 10	Bis fünf Jahre
§ 85 Abs. 2 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 i.V.m. § 3 Abs. 1 Satz 1 Nr. 2 G 10	Bis drei Jahre
§ 86 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 i.V.m. § 3 Abs. 1 Satz 1 Nr. 2 G 10	Bis drei Jahre
§ 87 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 i.V.m. § 3 Abs. 1 Satz 1 Nr. 2 G 10	Bis fünf Jahre
§ 88 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 i.V.m. § 3 Abs. 1 Satz 1 Nr. 2 G 10	Bis fünf Jahre
§ 89 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 i.V.m. § 3 Abs. 1 Satz 1 Nr. 2 G 10	Bis fünf Jahre
§ 89b StGB	§ 7 Abs. 4 Satz 1 Nr. 1 lit. a G 10	Bis drei Jahre
§ 95 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. a StPO	Sechs Monate bis fünf Jahre
§ 97 Abs. 1 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. a StPO	Bis fünf Jahre
§ 97 Abs. 2 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. a StPO	Bis drei Jahre
§ 98 Abs. 1 Satz 1 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. a StPO	Bis fünf Jahre
§ 99 Abs. 1 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. a StPO	Bis fünf Jahre
§ 100a StGB	§ 7 Abs. 4 Satz 1 Nr. 2	Sechs Monate bis fünf

	G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. a StPO	Jahre
§ 108e StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. b StPO	Bis fünf Jahre
§ 109d StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. c stopp	Bis fünf Jahre
§ 109e StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. c StPO	Drei Monate bis fünf Jahre
§ 109f StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. c StPO	Bis fünf Jahre

§ 109g Abs. 1 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. c StPO	Bis fünf Jahre
§ 109g Abs. 2 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. c StPO	Bis zwei Jahre
§ 109h StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. c StPO	Drei Monate bis fünf Jahre
§ 129 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. d StPO	Bis fünf Jahre
§ 184b Abs. 1 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. g StPO	Drei Monate bis fünf Jahre
§ 184c Abs. 2 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. g StPO	Drei Monate bis fünf Jahre
§ 261 Abs. 1 und 2 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. m StPO	Drei Monate bis fünf Jahre
§ 275 Abs. 2 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. p StPO	Drei Monate bis fünf Jahre
§ 276 Abs. 2 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. p StPO	Drei Monate bis fünf Jahre
§ 298 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. r StPO	Bis fünf Jahre
§ 299 i.V.m. § 300 Satz 2 StGB	§ 7 Abs. 4 Satz 1 Nr. 2 G 10 i.V.m. § 100a Abs. 2 Nr. 1 lit. r StPO	Drei Monate bis fünf Jahre
§ 95 Abs. 1 Nr. 8 AufenthaltsG	§ 7 Abs. 4 Satz 1 Nr. 2 i.V.m. § 3 Abs. 1 Satz 1 Nr. 7 G 10	Bis ein Jahr
§ 18 Abs. 1-5 AWG	§ 7 Abs. 4 Satz 1 Nr. 1	(Drei Monate bis) fünf

	lit. b G 10	Jahre

§ 20 Abs. 1 Nr. 1-4 VereinsG	§ 7 Abs. 4 Satz 1 Nr. 2 i.V.m. § 3 Abs. 1 Satz 1 Nr. 2 G 10	Bis ein Jahr

Selbst wenn als Referenzmaßnahme für die hypothetische Datenneuerhebung – wie im Urteil vom 14. Juli 1999 – lediglich eine Telekommunikationsüberwachung herkömmlicher Art herangezogen würde, verfehlte der Straftatenkatalog des § 7 Abs. 4 Satz 1 G 10 die verfassungsrechtlichen Anforderungen in weitem Umfang:

Eine Telekommunikationsüberwachung kann im Strafverfahren nur gerechtfertigt werden, wenn sie dazu dient, eine schwere Straftat zu verfolgen. Dazu ist neben einer gesetzlichen Höchststrafe von mindestens fünf Jahren zu verlangen, dass die Tat besonders bedeutsame Rechtsgüter bedroht oder schädigt und auch im Einzelfall schwer wiegt,

> vgl. BVerfGE 129, 208 (243 f.).

Wie aus der Tabelle ersichtlich, sind nicht alle Anlasstaten der Datenübermittlung mit einer Höchststrafe von mindestens fünf Jahren bedroht. Viele der Taten, für die diese Höchststrafe angedroht ist, heben sich zudem aus dem Bereich der mittleren Kriminalität nicht erkennbar heraus. Schließlich verlangt § 7 Abs. 4 Satz 2 G 10 nicht, dass die Tat auch im Einzelfall schwer wiegt.

b) Datenübermittlungen zu präventivpolizeilichen Zwecken (§ 7 Abs. 4 Satz 1 G 10)

Gleichfalls nicht in vollem Umfang verfassungsgemäß ist § 7 Abs. 4 Satz 1 G 10, der Datenübermittlungen zu präventivpolizeilichen Zwecken regelt. Wegen der besonders hohen Eingriffsintensität der strategischen Telekommunikationsüberwachung muss eine solche Datenübermittlung von Verfassungs wegen an eine konkrete Gefahr für ein besonders bedeutsames Rechtsgut gebunden werden,

> vgl. zu Datenübermittlungen im Anschluss an Wohnraumüberwachungen und „Online-Durchsuchungen“ BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 291.

Diese verfassungsrechtliche Mindesteingriffsschwelle verfehlt § 7 Abs. 4 Satz 1 G 10 in mehrfacher Hinsicht.

Die in dieser Vorschrift enthaltenen oder in Bezug genommenen Kataloge führen in erheblichem Umfang Straftatbestände auf, die keine hinreichend schwerwiegenden Rechtsgutsverletzungen beschreiben, um die Übermittlung von Daten zu legitimieren, die aus einer so eingriffsintensiven Überwachungsmaßnahme wie der strategischen Telekommunikationsüberwachung stammen. Oben wurde bereits dargelegt, dass zahlreiche Katalogtaten lediglich der mittleren Kriminalität zuzuordnen sind. Teils handelt es sich sogar lediglich um Bagatellstraftaten. Solche Straftaten können eine Datenübermittlung für präventivpolizeiliche Zwecke ebenso wenig rechtfertigen wie eine Übermittlung zum Zweck der Strafverfolgung,

> vgl. zum insoweit anzunehmenden Gleichlauf der Anforderungen an Straftatkataloge in präventiv und repressiv ausgerichteten Übermittlungsermächtigungen BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 347.

Selbst soweit die Straftatkataloge des § 7 Abs. 4 Satz 1 G 10 gewichtige Straftaten enthalten, genügt die vorgesehene Übermittlungsschwelle in tatsächlicher Hinsicht nicht durchweg den verfassungsrechtlichen Anforderungen. Die Norm bindet die Übermittlung nicht durchweg an eine hinreichend verdichtete konkrete Gefahr.

Für die verfassungsrechtliche Mindesteingriffsschwelle kommt es dabei nicht auf die Gefahr einer Straftat als solcher an, sondern auf eine Gefahr für die Rechtsgüter, deren Schutz der Straftatbestand bezweckt,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 108

Dies schließt nicht aus, auch präventivpolizeiliche Überwachungsermächtigungen an Straftatkataloge zu koppeln,

> zumindest missverständlich insoweit BVerfGE 125, 260 (329); kritisch hierzu etwa Möstl, DVBl 2010, S. 808 (811 ff.); Schwabenbauer, Heimliche Grundrechtseingriffe, 2013, S. 233 f.

Ein präventivpolizeilicher Straftatkatalog muss aber nach spezifisch präventiven Kriterien zusammengestellt werden. Zudem muss das Gesetz den Eingriffsanlass so beschreiben, dass im Zusammenwirken mit dem Straftatkatalog die verfassungsrechtliche Mindestschwelle der konkreten Gefahr immer erfüllt ist, wenn der Eingriffsanlass vorliegt. § 7 Abs. 4 Satz 1 G 10 leistet dies in zweierlei Hinsicht nicht:

Erstens knüpft dieser Übermittlungstatbestand nicht nur an die gegenwärtige Begehung einer Straftat an, die zumindest in der Regel auf eine Rechtsgutsgefahr schließen lässt, sondern ermöglicht Übermittlungen bereits im Planungsstadium. Der Umstand allein, dass jemand eine Straftat plant, begründet jedoch noch nicht zwangsläufig eine Gefahr für die Rechtsgüter, die durch diese Straftat verletzt würden. Die Planungen können sich noch in einem so frühen Stadium befinden und vor der Tatbegehung noch so erhebliche Hürden zu überwinden sein, dass eine konkrete Straftat nicht einmal grob konturiert absehbar oder ihre Begehung sehr unwahrscheinlich sein kann. § 7 Abs. 4 Satz 1 G 10 enthält keine präzisierenden Tatbestandsmerkmale, um das potenziell fast uferlose Planungsstadium einzugrenzen,

> offener für eine Einbeziehung des Planungsstadiums noch BVerfGE 100, 313 (392 f.); diese Ausführungen sind angesichts der zwischenzeitlichen Entwicklung der Rechtsprechung und der erheblich erhöhten Eingriffsintensität der strategischen Telekommunikationsüberwachung heute so nicht mehr tragfähig.

Zweitens finden sich in den Straftatkatalogen des § 7 Abs. 4 Satz 1 G 10 neben Erfolgsdelikten auch Gefährdungstatbestände, die Handlungen im Vorfeld einer Rechtsgutsverletzung kriminalisieren. Teilweise verlagern diese Tatbestände die Strafbarkeit erheblich vor.

Beispielhaft sei auf § 129a StGB verwiesen, der bereits die Gründung oder Beteiligung an einer terroristischen Vereinigung bei Strafe verbietet, also eine Tathandlung weit im Vorfeld konkreter Schädigungshandlungen beschreibt. Eine sehr weitreichende Vorverlagerung der Strafbarkeit sieht auch § 89a StGB vor. Diese Norm stellt die Vorbereitung eines terroristischen Anschlags bereits in einem sehr frühen Stadium unter Strafe, wenn noch kaum absehbar ist, ob der Täter sein Vorhaben letztlich in die Tat umsetzen können wird. Die Rechtsprechung begrenzt die sehr weit gefasste Norm vor allem, indem sie hohe Anforderungen an den subjektiven Tatbestand stellt,

> vgl. BGH, Urteil vom 8. Mai 2014 – 3 StR 243/13 –, juris, Rn. 45; BGH, Urteil vom 27. Oktober 2015 – 3 StR 218/15 –, juris, Rn. 10.

Diese Begrenzung wirkt sich jedoch im präventivpolizeilichen Handlungsfeld allenfalls schwach aus. Denn im Voraus lassen sich die genauen Absichten und die Motivation des Betroffenen kaum erschließen. Ein präventives Handeln muss darum ganz überwiegend an äußerliche, klar erkennbare Tatsa-

chen anknüpfen. Vorfeldtatbestände wie § 129a oder § 89a StGB, die auf der objektiven Seite sehr weit gefasst sind, bieten deshalb kaum Anknüpfungspunkte, um die von § 7 Abs. 4 Satz 1 G 10 geforderte Prognoseentscheidung normativ anzuleiten. Diese Entscheidung kann vielmehr in weitem Umfang an hoch ambivalente und vage Erkenntnisse anknüpfen. Sie wird weitgehend ins Belieben des Bundesnachrichtendienstes gestellt.

Ungeachtet der Einstufung der in Bezug genommenen Vorfeldtatbestände als Erscheinungsformen der Schwerkriminalität, die sich im gesetzlichen Strafrahmen zeigt, sind diese Straftatbestände daher nicht geeignet, den Anlass präventiv ausgerichteter Eingriffsmaßnahmen trennscharf zu beschreiben,

> vgl. zu einer eingehenden Kritik der Verknüpfung präventivpolizeilicher Ermächtigungen mit strafrechtlichen Vorfeldtatbeständen Bäcker, Kriminalpräventionsrecht, 2015, S. 349 ff.

Beide Defizite des gesetzlichen Übermittlungsanlasses verschärfen sich, wenn sie miteinander verbunden werden. § 7 Abs. 4 Satz 1 G 10 ermöglicht eine Datenübermittlung auch, wenn der Verdacht besteht, dass jemand eine Vorfeldstraftat plant. Materiell-strafrechtliche und prozedural-nachrichtendienstrechtliche Vorverlagerung verstärken dann einander, so dass sich der Übermittlungstatbestand nahezu auflöst und Datenübermittlungen beinahe nach Belieben ermöglicht werden.

Dies lässt sich an einem Beispiel illustrieren: Nach § 89a Abs. 1, Abs. 2 Nr. 2 StGB macht sich unter anderem strafbar, wer sich vielfältig nutzbare Gegenstände beschafft, um damit einen terroristischen Anschlag zu begehen. Den Straftatbestand erfüllt unter anderem der Kauf von Unkrautvernichtungsmittel in der Absicht, daraus Sprengstoff für einen solchen Anschlag herzustellen. In der Folge kann der Bundesnachrichtendienst gemäß § 7 Abs. 4 Satz 1 G 10 Daten, die durch eine strategische Telekommunikationsüberwachung erlangt wurden, bereits übermitteln, wenn der Verdacht besteht, dass jemand plant, mit entsprechendem Vorbereitungsvorsatz Unkrautvernichtungsmittel zu kaufen. Eine solche Schlussfolgerung wird zwangsläufig vor allem auf Faktoren wie den persönlichen Überzeugungen und sozialen Beziehungen des Betroffenen beruhen.

Zumindest aufgrund dieser doppelten materiellen und prozeduralen Vorverlagerung des tatsächlichen Eingriffsanlasses verfehlt § 7 Abs. 4 Satz 1 G 10

die verfassungsrechtlichen Anforderungen auch dann, wenn als Referenzmaßnahme der hypothetischen Datenneuerhebung mit dem Urteil vom 14. Juli 1999 lediglich eine Telekommunikationsüberwachung herkömmlichen Typs angenommen wird. Denn auch Datenübermittlungen lediglich gehobener, aber nicht höchster Eingriffsintensität setzen voraus, dass sich aus den Daten ein konkreter Ermittlungsansatz ergibt, was hier nicht der Fall ist,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 289 f., 313.

c) Datenübermittlungen an Nachrichtendienste (§ 7 Abs. 2 G 10)

Die in § 7 Abs. 2 G 10 enthaltenen Ermächtigungen zu Datenübermittlungen an andere Nachrichtendienste genügen gleichfalls nicht den verfassungsrechtlichen Anforderungen. Zumindest bedürfen sie einer einengenden verfassungskonformen Auslegung.

Zu weit gefasst ist zunächst § 7 Abs. 2 Nr. 1 G 10, der eine Übermittlung ermöglicht, wenn „tatsächliche Anhaltspunkte dafür bestehen, dass die Daten erforderlich sind zur Sammlung und Auswertung von Informationen über Bestrebungen in der Bundesrepublik Deutschland, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Abs. 1 Nr. 1, 3 und 4 des Bundesverfassungsschutzgesetzes genannten Schutzgüter gerichtet sind“. Dieser Übermittlungstatbestand gewährleistet nicht in jedem Fall, dass eine konkrete Gefahr für ein besonders bedeutsames Rechtsgut den Übermittlungsanlass bildet. Nach dem Gesetzeswortlaut werden nur tatsächliche Anhaltspunkte für die Existenz einer gewaltaffinen Bestrebung, nicht aber für konkrete, zumindest ansatzweise absehbare Gewalttaten verlangt. Auch die Anknüpfungstatsachen, aus denen auf die Gewaltneigung der Bestrebung zu schließen ist, werden nicht ansatzweise eingegrenzt. Die Norm lässt einen solchen Schluss vielmehr aus beliebigen Anhaltspunkten zu, etwa der ideologischen Ausrichtung einer Gruppierung. Ein so weit gefasster Übermittlungsanlass genügt dem (verfassungsrechtlichen) Gefahrbegriff selbst in der von dem angerufenen Gericht in seinem Urteil zum BKA-Gesetz entwickelten erweiterten Variante nicht,

> vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 112 f.

Nach § 7 Abs. 2 Nr. 2 G 10 dürfen die erlangten Daten übermittelt werden, wenn der Verdacht sicherheitsgefährdender oder geheimdienstlicher Tätig-

keiten für eine fremde Macht besteht. In einer solchen Tätigkeit kann eine Gefahr für bedeutsame Kollektivgüter liegen. Dies ist jedoch nicht notwendigerweise der Fall, da der Übermittlungstatbestand – insbesondere hinsichtlich von geheimdienstlichen Tätigkeiten – allein auf die Tätigkeit, nicht aber auf die dadurch drohenden Folgen abstellt.

Auch der spezifisch auf Überwachungen nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 zugeschnittene Übermittlungstatbestand in § 7 Abs. 2 Nr. 3 G 10 ist defizitär. Diese Norm ermöglicht eine Datenübermittlung, wenn „tatsächliche Anhaltspunkte dafür bestehen, dass die Angriffe von Bestrebungen oder Tätigkeiten nach § 3 Absatz 1 des Bundesverfassungsschutzgesetzes ausgehen“. Sie ist aus zwei Gründen verfassungsrechtlich unzureichend: Erstens setzt § 7 Abs. 2 Nr. 3 G 10 nach dem Normwortlaut zumindest nicht eindeutig voraus, dass konkrete Angriffe auf informationstechnische Systeme festgestellt oder zumindest wahrscheinlich sind. Die Regelung kann auch – parallel zu § 7 Abs. 2 Nr. 1 G 10 – so verstanden werden, dass es ausreicht, wenn eine verfassungsfeindliche Bestrebung im Sinne von § 3 Abs. 1 BVerfSchGG lediglich eine irgendwie herzuleitende Affinität zu solchen Angriffen aufweist. Zweitens lässt die Norm für eine Datenübermittlung jegliche illegalen Angriffe auf informationstechnische Systeme im Sinne von § 5 Abs. 1 Satz 3 Nr. 8 G 10 ausreichen. Sie teilt damit das Defizit dieser Ermächtigung, dass auch Angriffe umfasst sind, die zwar beträchtliche Schäden verursachen können, aber keine elementaren Rechtsgüter bedrohen (siehe oben II 1 c und II 2).

d) Datenübermittlungen an das Bundesamt für Sicherheit in der Informationstechnik (§ 7 Abs. 4a G 10)

Schließlich verfehlt auch die gleichfalls spezifisch auf strategische Telekommunikationsüberwachungen nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 zugeschnittene Übermittlungsermächtigung in § 7 Abs. 4a G 10 zumindest teilweise die verfassungsrechtlichen Anforderungen.

Bedenklich weit gefasst ist bereits der Übermittlungstatbestand in § 7 Abs. 4a Hs. 1 G 10, demzufolge der Bundesnachrichtendienst die erhobenen personenbezogenen Daten an das Bundesamt für Sicherheit in der Informationstechnik zur Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes übermitteln darf. Diese Regelung mag so auszulegen sein, dass die Datenübermittlung eine konkrete Gefahr im Sinne der Aufgabenzuweisung in § 3 Abs. 1 Satz 2 Nr. 1 BSIG voraussetzt. Der Übermittlungstatbe-

stand benennt jedoch keine konkreten Schutzgüter und bedarf insoweit zumindest einer verfassungskonformen Auslegung.

Eine solche verfassungskonforme Auslegung scheidet hingegen aus für den weiteren Übermittlungstatbestand in § 7 Abs. 4a Hs. 2 G 10. Diese Norm ermöglicht Datenübermittlungen an das Bundesamt für Sicherheit in der Informationstechnik zur Sammlung und Auswertung von Informationen über Sicherheitsrisiken, also im Anwendungsbereich der Aufgabenzuweisungen in § 3 Abs. 1 Satz 2 Nr. 2 und 3 BSIG. Diese Aufgabenzuweisungen geben dem Bundesamt auf, Informationen über Sicherheitsrisiken zusammenzutragen und auszuwerten, um so allgemein zu einem hohen Sicherheitsniveau der Informationstechnik des Bundes und anderer Stellen beizutragen. Hierbei handelt es sich um eine fortlaufende Analyseaufgabe, die gerade unabhängig von konkreten Gefahren erfüllt werden soll,

> vgl. Buchberger, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, § 3 BSIG Rn. 3 f.

Der gesetzliche Übermittlungsanlass beschränkt daher die Übermittlung in tatsächlicher Hinsicht nicht auf konkrete Gefahren. Zudem bedrohen nicht alle Risiken für die Sicherheit informationstechnischer Systeme beliebiger Dritter hinreichend gewichtige Rechtsgüter, um eine Übermittlung von Daten zu rechtfertigen, die aus einer strategischen Telekommunikationsüberwachung stammen.

2. Datenübermittlungen an ausländische öffentliche Stellen (§ 7a Abs. 1 Satz 1 Nr. 1 und Abs. 2 G 10)

Die in § 7a Abs. 1 Satz 1 Nr. 1 und Abs. 2 G 10 enthaltenen Ermächtigungen zur Übermittlung von Daten, die durch strategische Telekommunikationsüberwachungen nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 erlangt wurden, an ausländische öffentliche Stellen genügen gleichfalls nicht den verfassungsrechtlichen Anforderungen.

Das angerufene Gericht hat in seinem Urteil zum BKA-Gesetz die verfassungsrechtlichen Anforderungen an Datenübermittlungen ins Ausland im Vergleich zu Inlandsübermittlungen teils modifiziert, um der verfassungsrechtlichen Ausrichtung der deutschen öffentlichen Gewalt auf eine internationale Zusammenarbeit Rechnung zu tragen,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 325.

Die Modifikationen betreffen indes primär die Anforderungen an den Umgang mit den einmal übermittelten Daten. Hingegen gibt es keinen Grund, die verfassungsrechtlichen Mindestschwellen für Auslandsübermittlungen im Vergleich mit Inlandsübermittlungen generell abzusenken. Auch Datenübermittlungen an ausländische Stellen können nur gerechtfertigt werden, wenn sie hinreichend gewichtigen Übermittlungszwecken dienen und für sie eine hinreichende Tatsachenbasis besteht. Die Anforderungen an das Gewicht der Übermittlungszwecke sind allerdings mit den Zweckkategorien und Wertungen der jeweiligen ausländischen Rechtsordnung abzustimmen,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 330 f.

Nach diesem Maßstab sind die in § 7a G 10 enthaltenen Ermächtigungen zu Auslandsübermittlungen verfassungswidrig, weil sie solche Übermittlungen nicht auf hinreichend gewichtige Zwecke beschränken und nicht an einen hinreichenden tatsächlichen Anlass binden. Für diesen Befund kommt es nicht entscheidend darauf an, ob – wie hier vertreten – die verfassungsrechtliche Mindestübermittlungsschwelle gleichläufig zu Daten aus Wohnraumüberwachungen und „Online-Durchsuchungen“ bestimmt wird oder ob das Kriterium der hypothetischen Datenneuerhebung lediglich auf eine Telekommunikationsüberwachung herkömmlichen Typs als Referenzmaßnahme bezogen wird. Die Übermittlungsermächtigungen in § 7a G 10 verfehlen auch die niedrigeren Anforderungen an eine Zweckänderung von Daten aus Telekommunikationsüberwachungen.

Nach § 7a Abs. 1 Satz 1 Nr. 1 G 10 dürfen Daten, die durch eine strategische Telekommunikationsüberwachung erlangt wurden, an ausländische Nachrichtendienste übermittelt werden, wenn die Übermittlung zur Wahrung außen- oder sicherheitspolitischer Belange der Bundesrepublik oder erheblicher Sicherheitsinteressen des ausländischen Staates erforderlich ist. Die außen- und sicherheitspolitischen Belange der Bundesrepublik umfassen hochrangige Rechtsgüter, erschöpfen sich jedoch nicht in deren Schutz, sondern erstrecken sich auf zahlreiche weitere, weniger gewichtige Anliegen. Demgegenüber mag es möglich sein, als erhebliches Sicherheitsinteresse eines ausländischen Staates in einengender Interpretation nur den Schutz hochrangiger Individual- und Kollektivgüter anzuerkennen. Jedoch ermöglicht § 7a Abs. 1 Satz 1 Nr. 1 G 10 eine Datenübermittlung nicht nur, wenn solche Güter konkret gefährdet sind oder eine Bedrohung zumindest ansatzweise ab-

sehbar ist. Die Übermittlungsermächtigung wird vielmehr nur durch den Erforderlichkeitsgrundsatz begrenzt. Dieser Grundsatz schließt eine vorsorgliche Übermittlung von Informationen nicht aus, die möglicherweise in zukünftigen, noch nicht näher absehbaren Bedrohungslagen einmal von Interesse sein könnten. § 7a Abs. 1 Satz 1 Nr. 1 G 10 erfordert daher als tatsächliche Basis der Übermittlung weder eine konkrete Gefahr noch einen konkreten Ermittlungsansatz.

Die weitere Übermittlungsermächtigung in § 7a Abs. 2 G 10 verweist hinsichtlich der Voraussetzungen der Übermittlung auf § 7a Abs. 1 G 10 und teilt so das verfassungsrechtliche Defizit dieser Norm. § 7a Abs. 2 G 10 enthält auch keine eigenständigen Tatbestandsmerkmale, die dieses Defizit ausgleichen könnten.

§ 7a Abs. 2 G 10 verweist für Datenübermittlungen an Dienststellen der Stationierungskräfte auf Art. 3 des Zusatzabkommens zum NATO-Truppenstatut. Diese Regelung enthält eine Kooperationspflicht zwischen deutschen Behörden und Stationierungskräften, welche eine Pflicht zum Nachrichtenaustausch einschließt. Konkrete Vorgaben für die Voraussetzungen von Datenübermittlungen enthält sie nicht. Hingegen stellt der im Jahr 1993 eingefügte Art. 3 Abs. 3 lit. b des Zusatzabkommens klar, dass die Pflicht zur informationellen Kooperation eine Grenze im innerstaatlichen Recht der Vertragsstaaten findet. Das Zusatzabkommen verpflichtet die Bundesrepublik mithin nicht, die Voraussetzungen für Datenübermittlungen so niedrig anzusetzen wie es § 7a Abs. 2 vorsieht.

Des Weiteren verlangt § 7a Abs. 2 G 10, dass die Übermittlung für die Erfüllung der Aufgaben des Übermittlungsempfängers erforderlich ist. Auch hierin liegt in materieller wie tatsächlicher Hinsicht keine Begrenzung, die den verfassungsrechtlichen Anforderungen an die Übermittlung von Daten aus eingriffsintensiven Überwachungsmaßnahmen annähernd gerecht würde.

VI. Kontrolle der strategischen Telekommunikationsüberwachung

Das Gesetz gewährleistet schließlich nicht in vollem Umfang die verfassungsrechtlich gebotene wirksame unabhängige Kontrolle der strategischen Telekommunikationsüberwachung und die Rechtsschutzmöglichkeiten der Betroffenen einer solchen Überwachung. Zum einen sind die gesetzlichen Dokumentationspflichten teils unzureichend gestaltet. Zum anderen wird die

aufsichtliche Kontrolle des Bundesnachrichtendienstes in dysfunktionaler Weise aufgespalten.

1. Dokumentationspflichten (§ 5 Abs. 2 Satz 6, § 5a Satz 7, § 6 Abs. 1 Satz 5, § 7 Abs. 5 Satz 4, § 7a Abs. 3 Satz 4 G 10)

Eine wirksame aufsichtliche Kontrolle eingriffsintensiver verdeckter Überwachungen wie auch ein effektiver Rechtsschutz der Betroffenen hiergegen setzen voraus, dass die wesentlichen Schritte eines Überwachungsvorgangs in hinreichend gehaltvoller Weise dokumentiert werden. Die verfassungsrechtlichen Dokumentationsanforderungen erfassen neben der Datenerhebung auch nachgelagerte Phasen des Datenumgangs. So sind auch Datenlöschungen, Datenübermittlungen und Zurückstellungen der Benachrichtigung des Betroffenen zu dokumentieren,

> vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 129, 141, 144, 267, 322, 340.

Zur Gewährleistung eines effektiven Rechtsschutzes und einer wirksamen Kontrolle müssen diese Dokumentationen so lange vorgehalten werden, dass sie bei typisierender Betrachtung noch vorhanden sein werden, wenn der Betroffene von einer Überwachungsmaßnahme benachrichtigt wird oder die nächste turnusmäßige Kontrolle ansteht. Die gesetzliche Protokollierungsregelung kann und muss durch eine entsprechende Zweckbindung gegebenenfalls gewährleisten, dass die Protokolle nicht zum Nachteil des Betroffenen verwendet werden dürfen,

> vgl. für Löschungsprotokolle, aber verallgemeinerbar BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 205, 226, 246, 272.

Diesen Anforderungen wird das G 10 hinsichtlich von strategischen Telekommunikationsüberwachungen gemäß § 5 Abs. 1 Satz 3 Nr. 8 G 10 nicht gerecht.

Die Dokumentationsregelungen in § 5 Abs. 2 Satz 6 G 10 für die Durchführung der Überwachung, in § 6 Abs. 1 Satz 5 G 10 für die Löschung nicht mehr benötigter Daten, in § 5a Satz 7 G 10 für die Erfassung und Löschung kernbereichsrelevanter Daten sowie in § 7a Abs. 3 Satz 4 G 10 für Datenübermittlungen ins Ausland sehen jeweils vor, dass die Dokumentationen spätestens am Ende des Kalenderjahres zu löschen sind, das dem Jahr der Protokollierung folgt. Zu diesem Zeitpunkt wird den Betroffenen vielfach

mangels Benachrichtigung noch nicht möglich gewesen sein, den Rechtsweg zu beschreiten. Es ist auch nicht gewährleistet, dass bis zur Löschung eine aufsichtliche Kontrolle durchgeführt wurde. Ein rechtfertigender Grund für die kurze Aufbewahrungsfrist ist in keinem Fall erkennbar.

§ 7a Abs. 3 Satz 4 G 10 ist zudem auch insoweit verfassungswidrig, als diese Regelung die Verwendung der Dokumentation zumindest nicht eindeutig auf den Zweck der Datenschutzkontrolle begrenzt. Gerade aus der Dokumentation einer Datenübermittlung ins Ausland könnten jedoch auch behördliche Schlussfolgerungen gezogen werden, die sich für die betroffene Person nachteilig auswirken. Die Gründe, welche die Auslandsübermittlung tragen, rechtfertigen nicht zwangsläufig, zu einem späteren Zeitpunkt den Umstand der Auslandsübermittlung zulasten der betroffenen Person zu verwenden. Um eine Aufbewahrung der Dokumentationsdaten auch für behördliche Zwecke zu legitimieren, bedürfte es daher eines eigenständigen gesetzlichen Eingriffsanlasses, den § 7a Abs. 3 Satz 4 G 10 nicht enthält.

Schließlich verfehlt auch § 7 Abs. 5 Satz 4 G 10 die verfassungsrechtlichen Anforderungen. Diese Regelung sieht vor, Datenübermittlungen an inländische Behörden zu protokollieren, regelt jedoch weder eine Zweckbindung noch eine Löschung der Protokolldaten. Auf diese Weise werden die Protokolldaten für beliebige Nutzungen auch im Eigeninteresse des Bundesnachrichtendienstes geöffnet, ohne dass hierfür in jedem Fall ein verfassungsrechtlich hinreichender Grund bestehen müsste.

2. Verhältnis von G 10-Kommission und Bundesbeauftragter für den Datenschutz (§ 15 Abs. 5 Satz 2 G 10, § 24 Abs. 2 Satz 3 BDSG)

Eine wirksame aufsichtliche Kontrolle strategischer Telekommunikationsüberwachungen nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 ist darüber hinaus wegen einer dysfunktionalen Aufspaltung der Kontrollaufgabe nicht gewährleistet.

Eine wirksame Aufsicht kann nicht nur an mangelhafter Ausstattung oder an unzureichenden Befugnissen der Aufsichtsbehörde scheitern, sondern auch daran, dass diese Behörde kein vollständiges Bild von den Tätigkeiten der kontrollierten Behörden erlangen kann. Das angerufene Gericht hat dementsprechend in seinem Urteil zur Antiterrordatei eine Kooperation der zuständigen Aufsichtsbehörden angemahnt, um eine effektive Kontrolle dieser Verbunddatei von Bund und Ländern sicherzustellen,

vgl. BVerfGE 133, 277 (370).

Zur Kontrolle strategischer Telekommunikationsüberwachungen ist die G 10-Kommission des Deutschen Bundestags zuständig. Die Tätigkeit der Kommission erschöpft sich nicht in der – mit der Aufgabe eines Vorbehaltsrichters vergleichbaren – Vorabprüfung vorgesehener Beschränkungsmaßnahmen nach § 15 Abs. 6 G 10. Die G 10-Kommission ist darüber hinaus – ähnlich wie eine Datenschutzaufsichtsbehörde – gemäß § 15 Abs. 5 Sätze 1 und 2 G 10 berufen, umfassend über die Zulässigkeit und Notwendigkeit der Telekommunikationsüberwachungen selbst wie auch aller nachfolgender Verarbeitungsschritte zu entscheiden. Hierzu räumt ihr § 15 Abs. 5 Satz 3 G 10 umfängliche Kontrollbefugnisse ein. Wird die strategische Telekommunikationsüberwachung isoliert betrachtet, so genügt der gesetzliche Kontrollmechanismus den verfassungsrechtlichen Anforderungen,

> vgl. demgegenüber zum früheren, defizitären Befugniskreis der G 10-Kommission BVerfGE 100, 313 (301).

Die Kontrolle ist gleichwohl defizitär ausgestaltet, weil sich die Aufklärungstätigkeit des Bundesnachrichtendienstes nicht in strategischen Telekommunikationsüberwachungen erschöpft. Der Dienst ist nach §§ 2 ff. BNDG vielmehr zu zahlreichen weiteren Überwachungsmaßnahmen und nachgehenden Verarbeitungen personenbezogener Daten im Inland befugt. Zur Kontrolle dieser Maßnahmen und Verarbeitungen ist die G 10-Kommission lediglich teilweise gemäß § 2a Abs. 1 Satz 3 BNDG i.V.m. § 8b BVerfSchG berufen. Nicht der Kontrolle durch die G 10-Kommission unterliegt zudem die gesamte Auslandstätigkeit des Bundesnachrichtendienstes. Dies schließt die strategische Überwachung ausländischer Telekommunikationsverkehre ein, selbst wenn der Bundesnachrichtendienst sie vom Inland aus durchführt, und sogar dann, wenn der Bundesnachrichtendienst die bei einer Überwachung nach § 5 G 10 anfallenden ausländischen „Routineverkehre“ auswertet. Hieran ändert die gesetzliche Regulierung der Ausland-Ausland-Fernmeldeaufklärung nichts. Vielmehr errichtet § 16 BNDG-neu statt einer Befassung der G 10-Kommission ein weiteres Kontrollgremium, das in diesem Bereich bestimmte Kontrollaufgaben wahrnimmt.

Die Begrenzung der Kontrollaufgabe der G 10-Kommission hat zur Folge, dass die Kommission sich kein umfassendes Bild von den Aufklärungsaktivitäten des Bundesnachrichtendienstes machen kann. Dies wäre aber erforderlich, um die Maßnahmen, zu deren Kontrolle die Kommission berufen ist, umfassend zu würdigen. So hängt die Erforderlichkeit einer strategischen

Überwachung davon ab, ob und welche Erkenntnisse der Bundesnachrichtendienst mit anderen, weniger eingriffsintensiven Maßnahmen gewinnen könnte. Der Ertrag einer solchen Überwachung und die Erforderlichkeit einer (weiteren) Speicherung der Überwachungsergebnisse lässt sich nur dann vollständig bemessen, wenn der gesamte Erkenntnisstand des Bundesnachrichtendienstes vorliegt. Auch die Entscheidung darüber, die Benachrichtigung der Betroffenen einer strategischen Telekommunikationsüberwachung zurückzustellen, kann von weiteren Erkenntnissen abhängen, auf welche die Kommission nicht aus eigener Initiative und nicht vollständig zugreifen kann. Zudem gebietet die Menschenwürdegarantie nach der Rechtsprechung des angerufenen Gerichts, das Gesamtniveau hoheitlicher Überwachungsmaßnahmen gegenüber bestimmten Betroffenen begrenzt zu halten,

> vgl. zuletzt BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1140/09 –, Rn. 130.

Diese „Überwachungs-Gesamtrechnung“

> so die griffige Bezeichnung von Roßnagel, NJW 2010, S. 1238,

setzt voraus, dass zumindest die Kontrolle einer einzelnen Behörde, die zu eingriffsintensiven Überwachungsmaßnahmen ermächtigt ist, die Gesamtheit dieser Überwachungsmaßnahmen umfassen muss. Ansonsten kann die Kontrollstelle das additive Überwachungsniveau nicht zuverlässig einschätzen.

Dieses Defizit der Kontrollaufgabe der G 10-Kommission wird nicht durch andere Vorkehrungen zur Gewährleistung einer wirksamen Kontrolle kompensiert. Insbesondere kann eine hinreichend wirksame Kontrolle nicht durch ein Zusammenwirken der G 10-Kommission mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erreicht werden.

Auch die Bundesbeauftragte ist nicht umfassend zur Kontrolle des Bundesnachrichtendienstes berufen. Ihre Kontrollaufgabe beschränkt sich gemäß § 24 Abs. 2 Satz 3 BDSG auf Verarbeitungen personenbezogener Daten, die nicht der Kontrolle durch die G 10-Kommission unterliegen. Diese Regelung führt zu einer weitgehend unverbundenen Zweiteilung der Kontrolle mit der Folge, dass keine Kontrollstelle den Erkenntnisstand und die Überwachungstätigkeit des Bundesnachrichtendienstes umfassend nachvollziehen kann.

Zwar kann die G 10-Kommission gemäß § 15 Abs. 5 Satz 4 G 10 die Bundesbeauftragte zu Fragen des Datenschutzes anhören. Darüber hinaus kann sie die Bundesbeauftragte gemäß § 24 Abs. 2 Satz 3 BDSG zu Kontrollmaßnahmen ersuchen. Diese Befugnisse der Kommission bleiben jedoch auf ihren eigenen Aufgabenbereich bezogen und ermöglichen ihr daher nicht, sich ein Gesamtbild von der Überwachungstätigkeit des Bundesnachrichtendienstes zu machen,

> vgl. zu § 15 Abs. 5 Satz 4 G 10 Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2014, § 15 G 10 Rn. 51; zu § 24 Abs. 2 Satz 3 BDSG Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2014, § 24 Rn. 9.

Umgekehrt hat die Bundesbeauftragte überhaupt keine Möglichkeit, die G 10-Kommission zur Kontrolle von Maßnahmen der strategischen Telekommunikationsüberwachungen oder von nachgelagerten Verarbeitungsschritten zu ersuchen, selbst wenn dies für ihre eigene Kontrollaufgabe bedeutsam wäre.

Schließlich führt die Aufspaltung der Kontrolle in Randbereichen zu erheblichen Abgrenzungsproblemen, welche ihre Wirksamkeit weiter vermindern. Unklar und in der Praxis zwischen den beteiligten Stellen umstritten ist etwa, ob die Bundesbeauftragte für die Kontrolle der Verarbeitung personenbezogener Daten zuständig ist, die ursprünglich aus einer G 10-Überwachung stammen und vom Bundesnachrichtendienst an eine andere Bundesbehörde übermittelt wurden,

> vgl. Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2014, § 15 G 10 Rn. 51.

Ein rechtfertigender Grund für diese dysfunktionale Aufspaltung der Kontrolle ist nicht erkennbar. Anders als im Fall der Antiterrordatei lassen sich für diese Aufspaltung keine bundesstaatlichen Gründe anführen. Es geht vielmehr hier allein um die Aufsicht über eine einzige Behörde mit einer einheitlichen gesetzlichen Aufgabe. Diese Kontrollaufgabe ließe sich ohne weiteres gleichfalls vereinheitlichen. Beispielsweise könnte die Kontrollaufgabe der G 10-Kommission auf eine richterähnliche Vorabprüfung bestimmter Überwachungsmaßnahmen beschränkt und die gesamte Ex-post-Kontrolle bei der Bundesbeauftragten konzentriert werden. Dies wäre auch im Anwendungsbereich von Art. 10 Abs. 2 Satz 2 GG möglich, da die Bundesbeauftragte

gemäß § 22 Abs. 1 Satz 1 BDSG vom Bundestag gewählt wird und damit gleichfalls ein von der Volksvertretung bestelltes Organ im Sinne dieser Norm ist,

> vgl. BVerfGE 67, 157 (185); BVerfG, Beschluss vom 20. September 2016 – 2 BvE 5/15 –, Rn. 45.

Insoweit besteht ein erheblicher Gestaltungsspielraum des Gesetzgebers, der jedoch endet, wenn – wie gegenwärtig – insgesamt eine wirksame Kontrolle des Bundesnachrichtendienstes nicht zuverlässig gewährleistet ist.

(Prof. Dr. Bäcker, LL.M.)

Anlage: Verfahrensvollmachten