Sicherheitsrecht des Bundes – Recht der Nachrichtendienste in Deutschland

von

Prof. Dr. Kurt Graulich
Richter am Bundesverwaltungsgericht a.D.

Humboldt-Universität zu Berlin – Sommersemester 2018
Raum UL9 E 25
Donnerstag, d. 14.06.2018 von 10.00 bis 12.00 Uhr
Schwerpunkt 5
Veranstaltungsnummer 10733

Skizze und Materialien

Gliederung:

Einzelheiten:

Gliederung:

d) Fernmeldeaufklärung

Zur Kerntätigkeit eines Auslandsnachrichtendienstes gehört die Fernmeldeaufklärung. Aus Gründen, die im Verfassungsrecht und der Gesetzgebungsgeschichte zum Bundesnachrichtendienst liegen, finden sich dazu in Deutschland zwei verschiedene Regelungssysteme. Neben der Notstandsgesetzgebung sind 1968 Art. 10 GG geändert und das „Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10)“ verabschiedet worden; darin wird u.a. die Überwachung von Telekommunikation durch deutsche Nachrichtendienste geregelt, die einen technischen Bezug zur Bundesrepublik hat (aa)). Die daneben bestehende sog. Ausland-Ausland-Fernmeldeüberwachung ist nicht Gegenstand des G10, sondern wird seit 2016 detailliert im BNDG geregelt (bb)).

aa) Fernmeldeaufklärung nach dem G10

aaa) Gegenstand des G10

Normativer Kern der Aufklärung von Fernmeldeverkehren mit technischem Bezug zur Bundesrepublik durch den BND ist das Gesetz zu Art. 10 GG (G 10). Auf seiner Grundlage sind die individuelle Überwachung nach § 3 G 10, die sog. strategische Überwachung als anlasslose Rasterfahndung nach § 5 G 10 sowie die strategische Fernmeldeaufklärung nach § 8 G 10 als anlassbezogene Rasterfahndung möglich. Die rechtliche Verfassung der Fernmeldeaufklärung zeigte bis 2016 die deutlichsten systematischen und regelungstechnischen Defizite beispielsweise im Vergleich zum Polizeirecht. Aufgabenbeschreibungen und Befugnisnormen wurden nicht genügend unterschieden bzw. sind durch die Verteilung auf BNDG, G 10 und BVerfSchG teilweise undeutlich. Dies traf zusammen mit gegensätzlichen Auffassungen über die rechtliche Bewertung eines erheblichen Teils der Fernmeldeaufklärung, insbesondere der Überwachung der Ausland-Ausland-Kommunikation. Keine Zuständigkeit besitzt der BND für die Überwachung ausschließlich in Deutschland stattfindender Telekommunikation. Sämtliche rechtlichen Streitfragen betreffen daher entweder die Überwachung der grenzüberschreitenden oder der ausschließlich im Ausland stattfindenden Fernmeldeverkehrs.

Das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz) (G 10) vom 13. August 1968 (BGBl I S. 949), das in Geltung trat, nachdem zuvor im Zug der verfassungsrechtlichen Notstandsvorkehrungen Art. 10 GG geändert worden war (Siebzehntes Gesetz zur Ergänzung des Grundgesetzes vom 24. Juni 1968, BGBl I S. 709), sah von Anfang an die Möglichkeit der Fernmeldeüberwachung vor (§ 1). Sie war in zwei Formen zulässig. § 2 G 10 regelte die individuelle Aufklärung. Personenbezogene Überwachungen waren danach zulässig, wenn Anhaltspunkte für den Verdacht bestanden, dass jemand näher bezeichnete, besonders schwere Straftaten plante, beging oder begangen hatte, die den Bestand der

Bundesrepublik Deutschland oder ihrer demokratischen Ordnung bedrohten. § 3 G 10 regelte die sogenannte strategische Aufklärung, die vor allem der Gewinnung von Lagebildern über bestimmte der Bundesrepublik drohende Gefahren diente (BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95 –, BVerfGE 100, 313-403, Rn. 2). Beim Verständnis von Rechtsprechung und Literatur ist genau zu beachten, auf welche Gesetzesfassung sie sich beziehen. Der Grundfall der strategischen Fernmeldeaufklärung war nämlich ursprünglich in § 3 G 10 a.F. geregelt und findet sich nunmehr in § 5 G 10. Individualmaßnahmen waren ursprünglich in § 2 G 10 a.F. enthalten und finden sich nunmehr in § 3 G 10.

Gemäß § 3 Abs. 1 Satz 2 G 10 a.F. war die strategische Überwachung ursprünglich nur zur Früherkennung und Abwehr der Gefahr eines bewaffneten Angriffs auf die Bundesrepublik zulässig. Sie beschränkte sich daher geographisch auf Gebiete, aus denen eine Kriegsgefahr drohte. Die Bestimmung dieser Gebiete traf nach § 3 Abs. 1 Satz 1 G 10 a.F. der zuständige Bundesminister mit Zustimmung des in § 9 Abs. 1 G 10 vorgesehenen Abgeordnetengremiums. Dieser ordnete gemäß § 5 Abs. 1 bis 3 G 10 auch an, welche Fernmeldeverkehrsbeziehungen im einzelnen Beschränkungen des Geheimnisses unterlagen. Unter einer Fernmeldeverkehrsbeziehung wurde dabei ein planmäßig festgelegter Fernmeldeverkehr zwischen zwei bestimmten Endpunkten in beiden Richtungen verstanden, zum Beispiel ein bestimmtes grenzüberschreitendes Sammelkabel zwischen zwei Fernsprechknotenämtern, das in der Regel mit einer konkreten Kennnummer bezeichnet war (vgl. BVerfGE 67, 157 <174>). Über die Zulässigkeit und Notwendigkeit der Beschränkungsmaßnahmen entschied gemäß § 9 Abs. 2 Satz 2 G 10 a.F. die G 10-Kommission (BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95 –, BVerfGE 100, 313-403, Rn. 3)

Wesentliches Merkmal der Beschränkungsmaßnahmen nach § 3 G 10 a.F. war es, dass sie sich **gegen einzelne Personen weder richteten noch aus technischen Gründen richten konnten, sondern der Gewinnung nicht personenbezogener Nachrichten dienten,** die der Bundesregierung Informationen über außen- und verteidigungspolitische Sachverhalte verschafften. Soweit bei der strategischen Überwachung personenbezogene Daten anfielen, etwa weil die Kommunikationspartner selbst ihre Identität lüfteten, durften die Daten gemäß § 3 Abs. 2 Satz 1 G 10 a.F. nicht zum Nachteil der Betroffenen verwendet werden. Von dieser Regel sah das Gesetz zwei Ausnahmen vor. Das Nachteilsverbot galt gemäß Satz 2 der Vorschrift nicht, wenn gegen die betroffene Person Fernmeldebeschränkungen nach § 2 G 10 angeordnet worden waren oder wenn tatsächliche Anhaltspunkte für den Verdacht bestanden, dass eine der in § 2 G 10 oder in § 138 StGB genannten Handlungen geplant oder begangen wurde (BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95 –, BVerfGE 100, 313-403, Rn. 4).

Das Gesetz zur Änderung des Strafgesetzbuchs, der Strafprozessordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz) vom 28. Oktober 1994 (BGBl I S. 3186) hat das G 10 in verschiedener Hinsicht geändert. Die Novellierung wurde damit begründet, dass die Überwachung des internationalen Fernmeldeverkehrs auch ermöglicht werden sollte, um Erkenntnisse auf den Gebieten des internationalen

Terrorismus, des Rauschgiftschmuggels nach Deutschland, des illegalen Handels mit Kriegswaffen und der internationalen Geldwäsche- und Geldfälschungsaktivitäten zu gewinnen, die in zunehmendem Maße die Sicherheit und Funktionsfähigkeit des Staates und die Sicherheit der Bürger bedrohten. Die Erkenntnisse sollten den zuständigen Sicherheitsbehörden zur Verhinderung, Aufklärung und Verfolgung von Straftaten zur Verfügung gestellt werden können (vgl. die Begründung des Gesetzentwurfs der Fraktionen der CDU/CSU und F.D.P., BT-Drs. 12/6853, S. 42). (BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95 –, BVerfGE 100, 313-403, Rn. 6)

§ 1 Gegenstand des Gesetzes

(1) Es sind
1. die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages,
2. der Bundesnachrichtendienst im Rahmen seiner Aufgaben nach § 1 Abs. 2 des BND-Gesetzes auch zu den in § 5 Abs. 1 Satz 3 Nr. 2 bis 8 und § 8 Abs. 1 Satz 1 bestimmten Zwecken
berechtigt, die Telekommunikation zu überwachen und aufzuzeichnen, in den Fällen der Nummer 1 auch die dem Brief- oder Postgeheimnis unterliegenden Sendungen zu öffnen und einzusehen.
(2) Soweit Maßnahmen nach Absatz 1 von Behörden des Bundes durchgeführt werden, unterliegen sie der Kontrolle durch das Parlamentarische Kontrollgremium und durch eine besondere Kommission (G 10-Kommission).

Die Regelung in § 1 G 10 enthält keine Aufgabenumschreibung für die Tätigkeit der Nachrichtendienste. Diese ergibt sich vielmehr jeweils aus dem Fachgesetz, nämlich BVerfSchG, BNDG und MADG. § 1 G 10 umschreibt den „Gegenstand des Gesetzes“ Huber a.a.O. G 10 § 1 Rn. 1). Die Aufgabenbeschreibung des BND enthält weitgehend § 1 Abs. 2 BNDG (vgl. Gusy a.a.O. BNDG § 1 Rn. 23).

bb) Maßnahmen nach dem G10

bbb) Befugnisse

Dem Grunde nach ergibt sich die Befugnis des BND – und auch der anderen Nachrichtendienste des Bundes - zur Überwachung und Aufzeichnung der Telekommunikation aus § 1 Abs. 1 G 10. Er lautet in der Fassung des Begleitgesetzes zum Telekommunikationsgesetz vom 17. Dezember 1997 (BGBl I S. 3108):
Es sind
1. die Verfassungsschutzbehörden des Bundes und der Länder, das Amt für den Militärischen Abschirmdienst und der Bundesnachrichtendienst zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den

Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantik-Vertrages,
2. der Bundesnachrichtendienst im Rahmen seiner Aufgaben nach § 1 Abs. 2 des BND-Gesetzes auch zu den in § 3 Abs. 1 Satz 2 Nr. 2 bis 6 bestimmten Zwecken
berechtigt, die Telekommunikation zu überwachen und aufzuzeichnen, in den Fällen der Nummer 1 auch die dem Brief- oder Postgeheimnis unterliegenden Sendungen zu öffnen und einzusehen (BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95 –, BVerfGE 100, 313-403, Rn. 16). Das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl. I S. 1938) hat die Befugnisnormen des G 10 in einigen Punkten geändert. Das Gesetz nimmt die Cyberabwehr zu den aufzuklärenden Gefahrenbereichen hinzu und berücksichtigt dies an den erforderlichen Stellen durch Erweiterung von Eingriffsbefugnissen.

bbb) Individualmaßnahmen nach dem § 3 G10

a1) Gesetzliche Grundlage

§ 3 Voraussetzungen

(1) Beschränkungen nach § 1 Abs. 1 Nr. 1 dürfen unter den dort bezeichneten Voraussetzungen angeordnet werden, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand
1. Straftaten des Friedensverrats oder des Hochverrats (§§ 80 bis 83 des Strafgesetzbuches),
2. Straftaten der Gefährdung des demokratischen Rechtsstaates (§§ 84 bis 86, 87 bis 89b, 89c Absatz 1 bis 4 des Strafgesetzbuches, § 20 Abs. 1 Nr. 1 bis 4 des Vereinsgesetzes),
3. Straftaten des Landesverrats und der Gefährdung der äußeren Sicherheit (§§ 94 bis 96, 97a bis 100a des Strafgesetzbuches),
4. Straftaten gegen die Landesverteidigung (§§ 109e bis 109g des Strafgesetzbuches),
5. Straftaten gegen die Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages (§§ 87, 89, 94 bis 96, 98 bis 100, 109e bis 109g des Strafgesetzbuches in Verbindung mit § 1 des NATO-Truppen-Schutzgesetzes),
6. Straftaten nach
a) den §§ 129a bis 130 des Strafgesetzbuches sowie
b) den §§ 211, 212, 239a, 239b, 306 bis 306c, 308 Abs. 1 bis 3, § 315 Abs. 3, § 316b Abs. 3 und § 316c Abs. 1 und 3 des Strafgesetzbuches, soweit diese sich gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes richten,
7. Straftaten nach § 95 Abs. 1 Nr. 8 des Aufenthaltsgesetzes oder
8. Straftaten nach den §§ 202a, 202b und 303a, 303b des Strafgesetzbuches, soweit sich die Straftat gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland, insbesondere gegen sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen richtet,

plant, begeht oder begangen hat. Gleiches gilt, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand Mitglied einer Vereinigung ist, deren Zwecke oder deren Tätigkeit darauf gerichtet sind, Straftaten zu begehen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind.
(1a) Beschränkungen nach § 1 Abs. 1 Nr. 1 dürfen unter den dort bezeichneten Voraussetzungen für den Bundesnachrichtendienst auch für Telekommunikationsanschlüsse, die sich an Bord deutscher Schiffe außerhalb deutscher Hoheitsgewässer befinden, angeordnet werden, wenn tatsächliche Anhaltspunkte bestehen, dass jemand eine der in § 23a Abs. 1 und 3 des Zollfahndungsdienstgesetzes genannten Straftaten plant, begeht oder begangen hat.
(2) Die Anordnung ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Sie darf sich nur gegen den Verdächtigen oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Verdächtige ihren Anschluss benutzt. Maßnahmen, die sich auf Sendungen beziehen, sind nur hinsichtlich solcher Sendungen zulässig, bei denen Tatsachen die Annahme rechtfertigen, dass sie von dem, gegen den sich die Anordnung richtet, herrühren oder für ihn bestimmt sind. Abgeordnetenpost von Mitgliedern des Deutschen Bundestages und der Parlamente der Länder darf nicht in eine Maßnahme einbezogen werden, die sich gegen einen Dritten richtet.

b1) Gesetzliche Voraussetzungen

Mit § 1 Abs. 1, § 3 G 10 hat der Gesetzgeber eine Regelung getroffen, nach der auch bisher schon Eingriffe in Art. 10 Abs. 1 GG seitens der Verfassungsschutzbehörden zulässig waren. Erlaubt sind danach Maßnahmen zur Abwehr von drohenden Gefahren für die freiheitlich demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages, soweit tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine der in § 3 G 10 näher aufgezählten Katalogtaten begangen hat. Zwar unterscheidet sich die im Artikel 10-Gesetz geregelte Überwachung der Telekommunikation grundlegend von der hier in Frage stehenden Nutzung anlasslos gespeicherter Verkehrsdaten, so dass beide Maßnahmen verfassungsrechtlich je eigens beurteilt werden müssen. Jedoch lässt sich den auch für die Landesbehörden geltenden Vorschriften des Artikel 10-Gesetzes entnehmen, dass es qualifizierte Bedrohungen gibt, hinsichtlich derer der Gesetzgeber den Verfassungsschutzbehörden auch bisher besondere Befugnisse einzuräumen bereit war und die dabei die Kernaufgaben der Verfassungsschutzbehörden betreffen. Der Gesetzgeber definiert hier Aufgaben von besonderer Dringlichkeit, die in qualifiziert begrenzter Weise auch in anderer Hinsicht betroffenen Bürgern Nachteile in Form eines Eingriffs in ihre durch Art. 10 GG geschützte Kommunikation zumuten (BVerfG, Ablehnung einstweilige Anordnung vom 28. Oktober 2008 – 1 BvR 256/08 –, BVerfGE 122, 120-151, Rn. 110).

Voraussetzung für eine Maßnahme nach § 3 G 10 ist das Erfordernis „tatsächlicher Anhaltspunkte“. Dies müssen mehr als nur vage Anhaltspunkte und bloße Vermutungen sein. Ein Verstoß gegen die Anforderung liegt vor, wenn sich sachlich zureichende plausible Gründe für eine Beschränkungsmaßnahme nach dem G 10 nicht mehr finden lassen. Auch darf nicht die gesetzliche Voraussetzung umgedreht und mit der Beschränkungsmaßnahme erst nach den Umständen gesucht werden, die diese möglicherweise rechtfertigen. Es muss also so etwas wie ein auf Tatsachen beruhender konkreter Verdacht für das Vorliegen der Voraussetzungen vorhanden sein. (Huber a.a.O. G 10 § 3 Rn. 5). GG Art 10 Abs. 2 S 2 fordert in Rücksicht auf den Grundsatz der Verhältnismäßigkeit, daß das Gesetz zu GG Art 10 die Zulässigkeit des das Eingriffs in das Brief-, Post- und Fernmeldegeheimnis beschränken muß auf den Fall, daß konkrete Umstände den Verdacht eines verfassungsfeindlichen Verhaltens rechtfertigen und daß dem verfassungsfeindlichen Verhalten im konkreten Fall nach Erschöpfung anderer Möglichkeiten der Aufklärung nur durch den Eingriff in das Brief-, Post- und Fernmeldegeheimnis beigekommen werden kann (BVerfG, Entscheidung vom 15. Dezember 1970 – 2 BvF 1/69, 2 BvR 629/68, 2 BvR 308/69 –, BVerfGE 30, 1 -).

Die für die Feststellung einer konkreten Gefahr erforderliche Wahrscheinlichkeitsprognose muss sich auf Tatsachen beziehen. Vage Anhaltspunkte oder bloße Vermutungen ohne greifbaren, auf den Einzelfall bezogenen Anlass reichen nicht aus (BVerfG, Beschluss vom 04. April 2006 – 1 BvR 518/02 –, BVerfGE 115, 320-381, Rn. 145).

Nach § 3 Absatz 1 Nr. 8 G10 sind Beschränkungen in Einzelfällen bei Vorliegen von tatsächlichen Anhaltspunkten für den Verdacht, dass jemand Straftaten im Zusammenhang mit Cyberbedrohungen plant, begeht oder begangen hat, möglich sein. Die Regelung ist durch Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl. I S. 1938) eingeführt worden. Für den BND ergänzt die Erweiterung des § 3 G10 um „cyberbezogene“ Straftatbestände die entsprechende Befugnis des BND für die strategische Fernmeldeaufklärung gemäß § 5 G10. Für das BfV werden dadurch elektronische Spionage- oder Sabotageangriffe fremder Mächte verbessert aufklärbar. Mit der allgemeinen Verweisung in § 3 Absatz 1 Satz 1 auf die Voraussetzungen des § 1 Abs. 1 Nr. 1 G10 ist auch die neue Befugnis nur zur Abwehr drohender Gefahren für herausragend wichtige Schutzgüter der Allgemeinheit zulässig. Ebenso wie bei Nummer 6 Buchstabe b) wird dieser Bezug in der neuen Nummer ausdrücklich aufgegriffen und hier auch konkretisiert. Damit wird normenklar verdeutlicht, dass es bei dieser Aufgabe nicht originär um Strafverfolgung, sondern die Abwehr besonders schwerer Gefahren geht. Bei der Verhältnismäßigkeitswürdigung der Katalogergänzung steht dementsprechend nicht der staatliche Strafanspruch und das Strafverfolgungsinteresse, dessen Bedeutung im Strafrahmen einen objektivierten Ausdruck findet (BVerfGE 125, 260, 329), im Vordergrund. Bei den vorliegenden Sachverhalten ist der Straftatbezug nicht hinreichend, sondern nur ein notwendiger Indikator, der die spezifische Art eines Modus Operandi bezeichnet, der wesentlich höherwertige Rechtsgüter bedroht. Mögliche Angriffsziele für das Ausspähen und Abfangen von Daten sowie Datenveränderung und -sabotage nach §§ 202a, 202b und 303a, 303b StGB können u.a.

x Unternehmen der Rüstungs- und Raumfahrtindustrie,
x Betreiber von kritischer Infrastruktur,
x Telekommunikationsunternehmen oder
x Staatliche Einrichtungen, z. B. Sicherheitsbehörden,
mit dem Ziel der Beschaffung von Verschlusssachen sein. Der mögliche Täterkreis ist hierbei nicht auf staatliche Stellen beschränkt, grundsätzlich dürfen Maßnahmen nach § 3 G10 auch bei Straftaten etwa mit terroristischem Hintergrund durchgeführt werden. Eine Einschränkung auf einen vorab benannten möglichen Täterkreis entspricht daher weder der Gesetzessystematik, noch der Ratio von Beschränkungen im Einzelfall. Allerdings ergeben sich aus den Aufgaben der verschiedenen Behörden entsprechende Einschränkungen. Während der BND die Aufgabe hat, Vorgänge von außen- und sicherheitspolitischer Bedeutung unabhängig davon aufzuklären, was auch kriminelle Angriffe entsprechender Dimension einschließt, sind für das BfV nur Bestrebungen oder Tätigkeiten mit den in § 3 Absatz 1 BVerfSchG bezeichneten Zielrichtungen relevant. Insoweit stehen Angriffe fremder Mächte im Vordergrund, gleichwohl ist auch mit elektronischen Angriffen terroristischer Vereinigungen zu rechnen (BT-Drs. 18/4654 S. 40).

c1) Kernbereichsschutz

§ 3a G 10 regelt den Kernbereichsschutz bei Einzeleingriffen nach § 3 G 10. Er ist ein interessantes Beispiel dafür, wie der Gesetzgeber die Anforderungen des BVerfG (BVerfGE 120, 274) umgesetzt hat:

§ 3a Schutz des Kernbereichs privater Lebensgestaltung

Beschränkungen nach § 1 Abs. 1 Nr. 1 sind unzulässig, soweit tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch sie allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erfasst würden. Soweit im Rahmen von Beschränkungen nach § 1 Abs. 1 Nr. 1 neben einer automatischen Aufzeichnung eine unmittelbare Kenntnisnahme erfolgt, ist die Maßnahme unverzüglich zu unterbrechen, soweit sich während der Überwachung tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Bestehen insoweit Zweifel, darf nur eine automatische Aufzeichnung fortgesetzt werden. Automatische Aufzeichnungen nach Satz 3 sind unverzüglich einem bestimmten Mitglied der G10-Kommission oder seinem Stellvertreter zur Entscheidung über die Verwertbarkeit oder Löschung der Daten vorzulegen. Das Nähere regelt die Geschäftsordnung. Die Entscheidung des Mitglieds der Kommission, dass eine Verwertung erfolgen darf, ist unverzüglich durch die Kommission zu bestätigen. Ist die Maßnahme nach Satz 2 unterbrochen worden, so darf sie für den Fall, dass sie nicht nach Satz 1 unzulässig ist, fortgeführt werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Beschränkung nach § 1 Abs. 1 Nr. 1 erlangt worden sind, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese

Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

ccc) Strategische Fernmeldeaufklärung nach § 5 G10

a1) Gesetzliche Grundlage

§ 5 Voraussetzungen

(1) Auf Antrag des Bundesnachrichtendienstes dürfen Beschränkungen nach § 1 für internationale Telekommunikationsbeziehungen, soweit eine gebündelte Übertragung erfolgt, angeordnet werden. Die jeweiligen Telekommunikationsbeziehungen werden von dem nach § 10 Abs. 1 zuständigen Bundesministerium mit Zustimmung des Parlamentarischen Kontrollgremiums bestimmt. Beschränkungen nach Satz 1 sind nur zulässig zur Sammlung von Informationen über Sachverhalte, deren Kenntnis notwendig ist, um die Gefahr
1. eines bewaffneten Angriffs auf die Bundesrepublik Deutschland,
2. der Begehung internationaler terroristischer Anschläge mit unmittelbarem Bezug zur Bundesrepublik Deutschland,
3. der internationalen Verbreitung von Kriegswaffen im Sinne des Gesetzes über die Kontrolle von Kriegswaffen sowie des unerlaubten Außenwirtschaftsverkehrs mit Waren, Datenverarbeitungsprogrammen und Technologien in Fällen von erheblicher Bedeutung,
4. der unbefugten gewerbs- oder bandenmäßig organisierten Verbringung von Betäubungsmitteln in das Gebiet der Europäischen Union in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland,
5. der Beeinträchtigung der Geldwertstabilität im Euro-Währungsraum durch im Ausland begangene Geldfälschungen,
6. der international organisierten Geldwäsche in Fällen von erheblicher Bedeutung,
7. des gewerbs- oder bandenmäßig organisierten Einschleusens von ausländischen Personen in das Gebiet der Europäischen Union in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland
a) bei unmittelbarem Bezug zu den Gefahrenbereichen nach Nr. 1 bis 3 oder
b) in Fällen, in denen eine erhebliche Anzahl geschleuster Personen betroffen ist, insbesondere wenn durch die Art der Schleusung von einer Gefahr für ihr Leib oder Leben auszugehen ist, oder
c) in Fällen von unmittelbarer oder mittelbarer Unterstützung oder Duldung durch ausländische öffentliche Stellen oder
8. 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
rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen. In den Fällen von Satz 3 Nr. 1 dürfen Beschränkungen auch für Postverkehrsbeziehungen angeordnet werden; Satz 2 gilt entsprechend.
(2) Bei Beschränkungen von Telekommunikationsbeziehungen darf der Bundesnachrichtendienst nur Suchbegriffe verwenden, die zur Aufklärung von

Sachverhalten über den in der Anordnung bezeichneten Gefahrenbereich bestimmt und geeignet sind. Es dürfen keine Suchbegriffe verwendet werden, die
1. Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung bestimmter Telekommunikationsanschlüsse führen, oder
2. den Kernbereich der privaten Lebensgestaltung betreffen.
Dies gilt nicht für Telekommunikationsanschlüsse im Ausland, sofern ausgeschlossen werden kann, dass Anschlüsse, deren Inhaber oder regelmäßige Nutzer deutsche Staatsangehörige sind, gezielt erfasst werden. Die Durchführung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden. Sie sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen.

b1) Funktion der strategischen Überwachung

Zweck der strategischen Überwachung ist die Gewinnung einer bestimmten Art prinzipiell nicht personenbezogener Nachrichten, die zur Information der Bundesregierung über verteidigungspolitische Tatsachen dienen (Claus Arndt, a.a.O.). Ziel ist die Sammlung von sachbezogenen Informationen, nicht aber von personenbezogenen Daten (Claus Arndt a.a.O.; unzutreffend Schwan, NJW 1980, S. 1992 (1997)). Es geht darum, aus Nachrichten (Mosaiksteinchen) über Sachverhalte im Sinne des § 5 G10 (im Zeitpunkt der Entscheidung des BVerfG noch: § 3 G 10) - etwa auch in der Zusammenschau mit Erkenntnissen aus anderen Quellen - verteidigungspolitisch relevante Tatsachen zu gewinnen, also um die nachrichtendienstliche Erkenntnis von Tatsachen zur rechtzeitigen Aufklärung bewaffneter Angriffe auf die Bundesrepublik Deutschland (vgl. BT-Drs. V/1880 S. 9; BVerfG, Beschluss vom 20. Juni 1984 – 1 BvR 1494/78 –, BVerfGE 67, 157-185, Rn. 51).

In thematischer Hinsicht wurden aufgrund der Novellierung die Zwecke, die nach § 3 Abs. 1 Satz 2 G 10 Beschränkungen des Fernmeldegeheimnisses erlauben, ausgeweitet. Neben die Gefahr eines bewaffneten Angriffs (Nr. 1) sind fünf weitere von verschiedenen strafrechtlich relevanten Verhaltensweisen mit Auslandsbezug ausgehende Gefahren getreten. Im Einzelnen handelt es sich um die Gefahr der Begehung internationaler terroristischer Anschläge (Nr. 2), der internationalen Verbreitung von Kriegswaffen und des konventionellen Rüstungshandels (Nr. 3), des Drogenexports in die Bundesrepublik (Nr. 4), der im Ausland begangenen Geldfälschungen (Nr. 5) und der Geldwäsche im Zusammenhang mit den in Nummern 3 bis 5 genannten Handlungen (Nr. 6) (BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95 –, BVerfGE 100, 313-403, Rn. 7).

Dagegen erstreckt sich die Überwachung hinsichtlich der neu aufgenommenen Erkenntniszwecke nur auf den - bei Erlass des G 10 technisch noch unentwickelten - nicht leitungsgebundenen internationalen Telekommunikationsverkehr (§ 3 Abs. 1 Satz 1 G 10). Leitungsgebundene Telekommunikationsbeziehungen dürfen nur überwacht werden, soweit es um die Gefahr eines Angriffskriegs geht (§ 3 Abs. 1 Satz 3 G 10). Andererseits vergrößert sich die geographische Reichweite der Überwachung durch die neu eingeführten Gefahrentatbestände der Nummern 2 bis 6. Während eine Kriegsgefahr seinerzeit nur aus dem Gebiet des Warschauer Paktes befürchtet wurde,

sind die neuen Gefahren nicht auf ein einziges Gebiet beschränkt (BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95 –, BVerfGE 100, 313-403, Rn. 8).

Ferner führt die Neuregelung zu einer Ausweitung in personeller Hinsicht. Zwar ist die gezielte Erfassung bestimmter Telekommunikationsanschlüsse gemäß § 3 Abs. 2 Satz 2 G 10 ausgeschlossen. Die Selektion erfolgt vielmehr gemäß § 3 Abs. 2 Satz 1 G 10 über Suchbegriffe, die zur Aufklärung von Sachverhalten über den in der Anordnung bezeichneten Gefahrenbereich bestimmt und geeignet sind. Doch gilt dies nach Satz 3 der Vorschrift nicht für Telekommunikationsanschlüsse von Ausländern im Ausland. Deren Anschlussnummern dürfen als sogenannte formale Suchbegriffe verwendet werden. Faktisch weitet sich der Personenbezug dadurch aus, dass es im Gegensatz zu früher heute technisch grundsätzlich möglich ist, die an einem Fernmeldekontakt beteiligten Anschlüsse zu identifizieren (BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95 –, BVerfGE 100, 313-403, Rn. 9).

Soweit personenbezogene Daten bei der Überwachung erlangt werden, gilt das Nachteilsverbot nicht mehr. Vielmehr sind die Daten gemäß § 3 Abs. 3 Satz 1, Abs. 5 Satz 1 G 10 zur Verhinderung, Aufklärung oder Verfolgung bestimmter Straftaten den Verfassungsschutzbehörden des Bundes und der Länder, dem Amt für den Militärischen Abschirmdienst, dem Zollkriminalamt, dem Bundesausfuhramt, den Staatsanwaltschaften und den Polizeibehörden vollständig zu übermitteln, soweit es zur Erfüllung ihrer Aufgaben erforderlich ist. Der Katalog der Straftaten, die eine Verwendung personenbezogener Daten rechtfertigen, ist gegenüber der Ursprungsfassung erheblich erweitert worden (§ 3 Abs. 3 Satz 1 G 10). Die Verwendung setzt aber weiterhin voraus, dass gegen die Person eine Beschränkung nach § 2 G 10 angeordnet ist oder tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine der aufgezählten Straftaten plant, begeht oder begangen hat (BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95 –, BVerfGE 100, 313-403, Rn. 10).

Durch das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl. I S. 1938) ist in § 5 Abs. 1 Satz 3 G 10 eine Nr. 8 eingeführt worden. Dazu sind der Gesetzesbegründung die nachfolgenden Erwägungen zu entnehmen: Zur Erkennung und Begegnung bestimmter Gefahrenbereiche ist der BND berechtigt im Rahmen seiner Aufgaben nach § 1 Absatz 2 BNDG, strategische Fernmeldeaufklärung zu betreiben. Die in § 5 G10 genannten Bereiche (Ziff. 1 bis 7) erweisen sich im Hinblick auf die neuen Gefahren des Cyberraums als defizitär. Hier bedarf es einer Anpassung an neue Bedrohungsszenarien. Cyberbedrohungen sind kein nationales Phänomen. Dem BND eine entsprechende gesetzliche Befugnis zur Aufklärung schadbehafteter internationaler Telekommunikationsverkehre einzuräumen, vervollständigt daher das Bestreben der Sicherheitsbehörden, diesen Gefahren, also insbesondere Cyber-Angriffen in Form von Cyber-Spionage, Cyber-Ausspähung oder Cyber-Sabotage, wirkungsvoll zu begegnen. Bei der Aufnahme des Gefahrenbereichs „Cyber“ geht es um keinen grundsätzlich neuen technischen Aufklärungsansatz. Der Einsatz des bestehenden technischen Mittels der strategischen Fernmeldeaufklärung soll inhaltlich

vielmehr an neu entstandene Gefahrenlagen angepasst werden. Auch die Aufklärung des Gefahrenbereichs „Cyber“ durch den BND erfolgt ausschließlich im Rahmen seines gesetzlichen Auftrags nach § 1 Absatz 2 BNDG. Danach sammelt er die erforderlichen Informationen zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind und wertet diese aus. Der BND soll mit dem in Nr. 8 genannten Gefahrenbereich in die Lage versetzt werden, die technisch (nur) durch ihn generierbaren Erkenntnisse zur Cyber-Bedrohungslage und -Abwehr beizusteuern. Der BND trägt dadurch dazu bei, die Sicherheit von IT-Systemen zu verbessern. Vertraulichkeit, Integrität und Verfügbarkeit von IT-Systemen – insbesondere solchen Kritischer Infrastruktur – werden u.a. hierdurch gegen die neuen Gefahren gehärtet. Eine Kritische Infrastruktur kann u.a. das IT-System eines Energieversorgers oder eines Flughafens sein. Mit dem neuen Gefahrenbereich leistet der BND seinen Beitrag zum Ausbau der IT-Sicherheit der Bundesverwaltung, der Verbesserung der IT-Sicherheit bei Unternehmen sowie für einen verstärkten Schutz der Bürgerinnen und Bürger in einem sicheren Netz. Der Gefahrenbereich „Cyber“ unterliegt den gleichen gesetzlichen Beschränkungen wie die übrigen Gefahrenbereiche, so gilt insbesondere der Höchstanteil überwachbarer Kommunikation gemäß § 10 Absatz 4 Satz 4 G10. Mit dem Begriff vergleichbar schädlich wirkende informationstechnische Mittel sind Maßnahmen umfasst, die keinen eindeutigen/direkten Bezug zu Cyberangriffen mittels Schadsoftware aufweisen, allerdings auch zum Themenfeld Cyber-Angriff gehören. Vergleichbar schädlich wirkende informationstechnische Mittel können u.a. sein: x Angriffe gegen die Verfügbarkeit von IT-Systemen mittels Überlastungsangriffe mit dem Ziel der Sabotage x Vortäuschen einer Identität, um beispielsweise an Zugangsinformationen zu gelangen x Angriffe auf IT-Systeme unter Umgehung von physikalischen Grenzen (Abzug von Informationen von Systemen ohne Netzwerkanbindung unter Ausnutzung der Abstrahlung u.ä.) x Hardwaremanipulation von Netzwerkgeräten. Eine Verschlüsselung von Kommunikationsinhalten ist hiervon nicht betroffen (BT-Drs. 18/4654 S. 40 ff.).

c1) Gesetzliche Voraussetzungen der strategischen Überwachung

Die Anordnung der strategischen Telefonüberwachung gemäß § 5 des Artikel 10-Gesetzes (juris: G10 2001) durch das Bundesministerium des Innern ist kein Verwaltungsakt gegenüber den Betroffenen, sondern eine innerdienstliche Weisung an den für diese Maßnahme zuständigen Bundesnachrichtendienst. Die strategische Überwachung beruht auf § 5 Abs. 1 Satz 1 i.V.m. Satz 3 Nr. 2 G 10. Danach ist die strategische Telefonüberwachung u.a. zulässig zur Sammlung von Informationen über Sachverhalte, deren Kenntnis notwendig ist, um die Gefahr der Begehung internationaler terroristischer Anschläge mit unmittelbarem Bezug zur Bundesrepublik Deutschland rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen. Diese Voraussetzungen waren im vorliegenden Fall erfüllt (BVerwG, Urteil vom 23. Januar 2008 – 6 A 1/07 –, BVerwGE 130, 180-197, Rn. 27). Die Erweiterung der strategischen Aufklärungsbefugnisse des Bundesnachrichtendienstes auf die Gefahren des internationalen Terrorismus "mit unmittelbarem Bezug zur Bundesrepublik Deutschland" im Jahre 2001 ist verfassungsrechtlich nicht zu beanstanden. (a.a.O. Rn.28).

Die strategische Telefonüberwachung dient nach ihrem gesetzlich umschriebenen Zweck der Gewinnung von Erkenntnissen über bestimmte von außen auf die Bundesrepublik Deutschland zukommende Gefahren, zu denen auch die Gefahren des internationalen Terrorismus gehören. Sie ist ein Hilfsmittel des Bundesnachrichtendienstes, um diese Gefahren aufzuklären und die gewonnenen Erkenntnisse in Lageberichte, Analysen und Berichte über Einzelvorkommnisse umzusetzen, deren Adressat die Bundesregierung ist; diese soll in den Stand versetzt werden, die Gefahrenlagen rechtzeitig zu erkennen und ihnen (politisch) zu begegnen (s. § 1 Abs. 2 des Gesetzes über den Bundesnachrichtendienst <BND-Gesetz> vom 20. Dezember 1990 <BGBl I S. 2954, 2979> i.V.m. § 1 Abs. 1, § 5 Abs. 1 G 10 sowie BVerfG, Urteil vom 14. Juli 1999 a.a.O. S. 371, 383). Da es um die frühzeitige Erkennung von Gefahren geht, bedarf es zur Anordnung der strategischen Telefonüberwachung keiner Gefahr, die sich bereits konkret abzeichnet, und nicht einmal eines bestimmten Verdachts; es reicht vielmehr aus, dass bei Durchführung der Überwachungsmaßnahme Erkenntnisse über bestehende Gefahrenlagen - hier die Gefahr terroristischer Anschläge - zu erwarten sind (BVerfG, Urteil vom 14. Juli 1999 a.a.O. S. 383, 389 sowie Beschluss vom 4. April 2006 - 1 BvR 518/02 - BVerfGE 115, 320 <359>). Die hier umstrittene Maßnahme ist im unmittelbaren zeitlichen Zusammenhang mit den Terroranschlägen in den USA am 11. September 2001 angeordnet worden; dabei wiesen bestimmte, vom Bundesnachrichtendienst in der Antragsbegründung aufgezählte Umstände, insbesondere Informationen über die Existenz von sog. Schläfern aus dem Umkreis Usama Bin Ladens in der Bundesrepublik Deutschland, auf die Gefahr weiterer Anschläge hin. Dass das Bundesministerium des Innern die strategische Überwachung des Telefonverkehrs nach Afghanistan auf der Grundlage von hinreichend aussagekräftigen Indizien angeordnet hat und dass kein anderes, ebenso erfolgversprechendes, aber die Grundrechtsträger weniger belastendes Erkenntnismittel zur Verfügung stand, wird auch vom Kläger nicht in Abrede gestellt (BVerwG, Urteil vom 23. Januar 2008 – 6 A 1/07 –, BVerwGE 130, 180-197, Rn. 29).

d1) Kritische Fragen

- Die strategische Überwachung soll durch die Verwendung bestimmter von der G 10-Kommission genehmigter Suchbegriffe sowie der Auswahl von Ländern bzw. Zielregionen begrenzt werden. Weshalb kam es im Jahr 2010 trotzdem zu 37 Millionen „e-mail-Treffern“? (Lüders a.a.O. S. 10)

- Die strategische Überwachung verlangt keine „konkrete Gefahr“, sondern eine „allgemeine Bedrohungslage“. Ermöglicht das G10 daher für die meisten Gefahrenbereiche eine permanente Überwachungstätigkeit? (Lüders S. 10)

- Nach dem Gesetz darf der BND nur grenzüberschreitende, internationale Kommunikationsvorgänge überwachen. Ist diese Begrenzung angesichts der bestehenden Routing-Regeln wirklich einzuhalten? (Lüders S. 11)

- Greift die gesetzliche Einschränkung der strategischen Überwachung auf „gebündelte Übertragung“ noch, wenn praktisch sämtliche Übertragungswege – abzüglich der sog. letzten Meile – heute gebündelt sind? (Lüders S. 11)

- Greift die 20-Prozent-Begrenzung auf die Übertragungskapazitäten wirklich angesichts von Überkapazitäten? (Lüders S. 11)

- Inwiefern greift das Verbot der Verwendung formaler Suchbegriffe, wenn bei allen internetgestützten Kommunikationsformen die Teilnehmer durch Benutzerkennungen auf Dienstebene identifiziert werden? (S. 11)

ddd) Strategische Fernmeldeaufklärung nach § 8 G10

§ 8 G10 regelt die Überwachung internationaler Telekommunikationsbeziehungen bei Gefahr für Leib und Leben einer Person im Ausland. Es handelt sich im Ergebnis um eine Individualmaßnahme, auch wenn sich der BND den Mitteln einer strategischen Beschränkungsmaßnahme bedient. Daher ist es auch nicht ausgeschlossen, eine dem Ziel des § 8 G10 dienende Maßnahme als klassische Beschränkungsmaßnahme nach § 3 G10 anzuordnen, sofern die qualifizierten Voraussetzungen dieser Vorschrift (z.B. Terrorismusbezug) vorliegen (Huber a.a.O. BNDG § 8 Rn. 1).

eee) Übermittlungen durch den BND

Die aufgrund strategischer Aufklärungsmaßnahmen gewonnenen Daten dürfen durch den BND nach Maßgabe von §§ 7 und 7a G 10 an andere Stellen übermittelt werden. Die Datenübermittlung durch den BND ist essentieller Teil der deutschen Sicherheitsarchitektur. Denn es gibt keine andere Behörde als den BND, die Daten durch Auslandsaufklärung generiert. Gerade die Bekämpfung von Gefahren des internationalen Terrorismus ist ohne die Möglichkeit der Weiterleitung solcher Daten an nationale Sicherheitsbehörden kaum denkbar. Die Übermittlung personenbezogener Daten stellt einen Eingriff in das informationelle Selbstbestimmungsrecht dar, die einer verfassungsgemäßen gesetzlichen Befugnis bedarf. Diese liegt hinsichtlich der durch strategische Überwachungsmaßnahmen gewonnenen Daten – für die Übermittlung an inländische Stellen – in § 7 G 10 und – für die Übermittlung an ausländische öffentliche Stellen – in § 7 G 10. Die nachfolgenden Erwägungen stehen unter dem Vorbehalt, dass der gegenwärtige Gesetzgebungsstand noch nicht die Ausführungen des BVerfG in seinem Urteil zu den heimlichen Überwachungsbefugnissen durch das BKAG berücksichtigt. Diese haben notwendige Auswirkungen auf die §§ 7 und 7a G 10.

Dies betrifft in beiden Regelungen den Grundsatz der Zweckbindung und Zweckänderung, der im Lichte dieses Urteils besser formuliert werden muss: „Die Reichweite der Zweckbindung richtet sich nach der jeweiligen Ermächtigung für die Datenerhebung; die Datenerhebung bezieht ihren Zweck zunächst aus dem jeweiligen Ermittlungsverfahren. Der Gesetzgeber kann eine Datennutzung über das für die Datenerhebung maßgebende Verfahren hinaus im Rahmen der ursprünglichen Zwecke dieser Daten erlauben (weitere Nutzung). Dies setzt voraus, dass es sich um eine

Verwendung der Daten durch dieselbe Behörde zur Wahrnehmung derselben Aufgabe und zum Schutz derselben Rechtsgüter handelt (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, juris)".

„Der Gesetzgeber kann darüber hinaus eine Nutzung der Daten auch zu anderen Zwecken als denen der ursprünglichen Datenerhebung erlauben (Zweckänderung) (Rn.284). Die Verhältnismäßigkeitsanforderungen für eine solche Zweckänderung orientieren sich am Grundsatz der hypothetischen Datenneuerhebung. Danach muss die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Eine konkretisierte Gefahrenlage wie bei der Datenerhebung ist demgegenüber grundsätzlich nicht erneut zu verlangen; erforderlich aber auch ausreichend ist in der Regel das Vorliegen eines konkreten Ermittlungsansatzes (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, juris)."

Die Übermittlung an ausländische öffentliche Stellen nach § 7a G 10 unterliegt zusätzlichen Anforderungen, wenn man das Urteil des BVerfG zum BKAG überträgt, was unvermeidlich ist: „Die Übermittlung von Daten an staatliche Stellen im Ausland unterliegt den allgemeinen verfassungsrechtlichen Grundsätzen von Zweckänderung und Zweckbindung. Bei der Beurteilung der neuen Verwendung ist die Eigenständigkeit der anderen Rechtsordnung zu achten. Eine Übermittlung von Daten ins Ausland verlangt eine Vergewisserung darüber, dass ein hinreichend rechtsstaatlicher Umgang mit den Daten im Empfängerstaat zu erwarten ist. (Rn.324) (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, juris)."

a1) Übermittlungen an inländische Stellen (§ 7 G 10)

§ 7 Übermittlungen durch den Bundesnachrichtendienst

(1) Durch Beschränkungen nach § 5 erhobene personenbezogene Daten dürfen nach § 12 des BND-Gesetzes zur Unterrichtung über die in § 5 Abs. 1 Satz 3 genannten Gefahren übermittelt werden.
(2) Durch Beschränkungen nach § 5 erhobene personenbezogene Daten dürfen an die Verfassungsschutzbehörden des Bundes und der Länder sowie an den Militärischen Abschirmdienst übermittelt werden, wenn
1. 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,
2. bestimmte Tatsachen den Verdacht sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten für eine fremde Macht begründen oder
3. im Falle des § 5 Absatz 1 Satz 1 in Verbindung mit Satz 3 Nummer 8 tatsächliche Anhaltspunkte dafür bestehen, dass die Angriffe von Bestrebungen oder Tätigkeiten nach § 3 Absatz 1 des Bundesverfassungsschutzgesetzes ausgehen.

(3) Durch Beschränkungen nach § 5 Abs. 1 Satz 1 in Verbindung mit Satz 3 Nr. 3 erhobene personenbezogene Daten dürfen an das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) übermittelt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Kenntnis dieser Daten erforderlich ist
1. zur Aufklärung von Teilnehmern am Außenwirtschaftsverkehr über Umstände, die für die Einhaltung von Beschränkungen des Außenwirtschaftsverkehrs von Bedeutung sind, oder
2. im Rahmen eines Verfahrens zur Erteilung einer ausfuhrrechtlichen Genehmigung oder zur Unterrichtung von Teilnehmern am Außenwirtschaftsverkehr, soweit hierdurch eine Genehmigungspflicht für die Ausfuhr von Gütern begründet wird.
(4) Durch Beschränkungen nach § 5 erhobene personenbezogene Daten dürfen zur Verhinderung von Straftaten an die mit polizeilichen Aufgaben betrauten Behörden übermittelt werden, wenn
1. tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand
a) Straftaten nach den §§ 89a, 89b, 89c Absatz 1 bis 4 oder § 129a, auch in Verbindung mit § 129b Abs. 1, sowie den §§ 146, 151 bis 152a oder § 261 des Strafgesetzbuches,
b) vorsätzliche Straftaten nach den §§ 17 und 18 des Außenwirtschaftsgesetzes, §§ 19 bis 21 oder § 22a Abs. 1 Nr. 4, 5 und 7 des Gesetzes über die Kontrolle von Kriegswaffen oder
c) Straftaten nach § 29a Abs. 1 Nr. 2, § 30 Abs. 1 Nr. 1, 4 oder § 30a des Betäubungsmittelgesetzes
plant oder begeht oder
2. bestimmte Tatsachen den Verdacht begründen, dass jemand eine der in § 3 Absatz 1 Satz 1 Nummer 1, 2, 5 und 7, Satz 2 oder Absatz 1a dieses Gesetzes oder eine sonstige der in § 100a Absatz 2 der Strafprozessordnung genannten Straftaten plant oder begeht.
(4a) Durch Beschränkungen nach § 5 Absatz 1 Satz 1 in Verbindung mit Satz 3 Nummer 8 erhobene personenbezogene Daten dürfen an das Bundesamt für Sicherheit in der Informationstechnik übermittelt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Daten erforderlich sind zur Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes oder zur Sammlung und Auswertung von Informationen über Sicherheitsrisiken auch für andere Stellen und Dritte.
(5) Die Übermittlung ist nur zulässig, soweit sie zur Erfüllung der Aufgaben des Empfängers erforderlich ist. Sind mit personenbezogenen Daten, die übermittelt werden dürfen, weitere Daten des Betroffenen oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, ist die Übermittlung auch dieser Daten zulässig; eine Verwendung dieser Daten ist unzulässig. Über die Übermittlung entscheidet ein Bediensteter des Bundesnachrichtendienstes, der die Befähigung zum Richteramt hat. Die Übermittlung ist zu protokollieren.
(6) Der Empfänger darf die Daten nur für die Zwecke verwenden, zu deren Erfüllung sie ihm übermittelt worden sind. Er prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die übermittelten Daten für diese Zwecke erforderlich sind. § 4 Abs. 6 Satz 4 und § 6 Abs. 1 Satz 2 und 3 gelten entsprechend.

Auch § 7 G 10 ist durch das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl. I S. 1938) geändert worden.

Als Folge des in § 5 Absatz 1 Satz 3 Nummer 8 ergänzten Gefahrenbereichs der internationalen Cybergefahren wird in Buchstabe a eine Befugnis zur Übermittlung personenbezogener Daten an die Verfassungsschutzbehörden und den MAD aufgenommen, soweit die Cyber-Gefahren von Bestrebungen oder Tätigkeiten ausgehen, die der Aufklärung des BfV nach § 3 Absatz 1 BVerfSchG unterliegen. Die Übermittlung dient der weiteren Aufklärung zur Abwehr dieser drohenden Gefahren. Eine Anwendung des geltenden § 7 Absatz 2 wäre für Informationen aus Aufklärungsmaßnahmen nach § 5 Absatz 1 Satz 3 Nummer 8 unpassend: x Falls der Angriff von extremistischen Bestrebungen ausgeht, wäre eine Übermittlung faktisch ausgeschlossen, da § 7 Absatz 2 Nummer 1 einen Gewaltbezug voraussetzt, der bei Cyberangriffen typischerweise fehlt. Auch ohne Gewaltbezug sind solche Angriffe ihrer Art nach aber so gefährlich, dass eine Übermittlung zur weiteren Aufklärung durch die dafür zuständigen Nachrichtendienste angemessen und geboten ist. x Falls der Angriff von fremden Mächten ausgeht, würde eine Übermittlung nach § 7 Absatz 2 Nummer 2 eine bereits erhöhte Erkenntnisdichte („bestimmte Tatsachen“) voraussetzen. Diese Voraussetzung soll dem Umstand einer zweckändernden Weitergabe Rechnung tragen (Bundestagsdrucksache 14/5655, S. 20f.). Die neue Befugnis nach § 5 Absatz 1 Satz 3 Nummer 8 dient dagegen bereits originär auch der Aufklärung von Cyberangriffen fremder Mächte, so dass eine Übermittlung zur Aufklärung sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten keine Zweckänderung beinhaltet. Daher wird mit Nummer 3 eine neue Regelung getroffen, die für den speziellen Fall der mit Maßnahmen § 5 Absatz 1 Satz 3 Nummer 8 gewonnenen Daten den allgemeinen Regelungen der Nummern 1 und 2 vorgeht. Die Änderung unter Buchstabe b greift eine Empfehlung der BLKR (Abschlussbericht Randnummer 559) auf, die Übermittlung zum Zweck der Strafverfolgung für alle Katalogtaten des § 100a StPO zu ermöglichen. Die Empfehlung bezieht sich unmittelbar auf die Übermittlung von Erkenntnissen aus Maßnahmen der Individualüberwachung nach § 4 G10, da die BLKR nur die Zusammenarbeit der Verfassungsschutzbehörden mit der Polizei – nicht auch des BND – zum Thema hatte. Sie ist aber ebenso für Übermittlungen nach § 7 G10 sachgerecht und begegnet angesichts der jeweiligen Verdachtsschwelle auch keinen verfassungsrechtlichen Bedenken. Sie wird daher aus systematischen Gründen in § 7 G10 aufgegriffen, auf den § 4 Absatz 4 Nummer 1 Buchstabe b verweist. Zudem wird die Übermittlung bereits zur Verhinderung solcher Straftaten zugelassen, was rechtspolitisch geboten ist, da inakzeptabel wäre, wenn der Nachrichtendienst sehenden Auges erst die Begehung der Straftat abwarten müsste. Auch insoweit ist mit der Verdachtsschwelle „bestimmte Tatsachen“ die Verhältnismäßigkeit gewahrt. Die Änderungen unter Buchstabe c erfassen Übermittlungen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) für dessen Aufgaben nach § 3 Absatz 1 Nummern 1 und 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). Das BSI ist zentrale Meldestelle für die Sicherheit in der Informationstechnik und dient der umfassenden Information aller Akteure über die aktuelle Cybergefährdungslage. Um dieser Aufgabe nachzukommen, bedarf es einer Kenntnis sämtlicher hierfür relevanter Informationen (BT-Drs. 18/4654 S. 41 ff.).

b1) Übermittlungen an ausländische Stellen (§ 7a G 10)

§ 7a Übermittlungen durch den Bundesnachrichtendienst an ausländische öffentliche Stellen

(1) Der Bundesnachrichtendienst darf durch Beschränkungen nach § 5 Abs. 1 Satz 3 Nr. 2, 3, 7 und 8 erhobene personenbezogene Daten an die mit nachrichtendienstlichen Aufgaben betrauten ausländischen öffentlichen Stellen übermitteln, soweit
1. die Übermittlung zur Wahrung außen- oder sicherheitspolitischer Belange der Bundesrepublik Deutschland oder erheblicher Sicherheitsinteressen des ausländischen Staates erforderlich ist,
2. überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen, insbesondere in dem ausländischen Staat ein angemessenes Datenschutzniveau gewährleistet ist sowie davon auszugehen ist, dass die Verwendung der Daten durch den Empfänger in Einklang mit grundlegenden rechtsstaatlichen Prinzipien erfolgt, und
3. das Prinzip der Gegenseitigkeit gewahrt ist.
Die Übermittlung bedarf der Zustimmung des Bundeskanzleramtes.
(2) Der Bundesnachrichtendienst darf unter den Voraussetzungen des Absatzes 1 durch Beschränkungen nach § 5 Abs. 1 Satz 3 Nr. 2, 3, 7 und 8 erhobene personenbezogene Daten ferner im Rahmen von Artikel 3 des Zusatzabkommens zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen hinsichtlich der in der Bundesrepublik Deutschland stationierten ausländischen Truppen vom 3. August 1959 (BGBl. 1961 II S. 1183, 1218) an Dienststellen der Stationierungsstreitkräfte übermitteln, soweit dies zur Erfüllung der in deren Zuständigkeit liegenden Aufgaben erforderlich ist.
(3) Über die Übermittlung entscheidet ein Bediensteter des Bundesnachrichtendienstes, der die Befähigung zum Richteramt hat. Die Übermittlung ist zu protokollieren. Der Bundesnachrichtendienst führt einen Nachweis über den Zweck, die Veranlassung, die Aktenfundstelle und die Empfänger der Übermittlungen nach Absatz 1 und 2. Die Nachweise sind gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr ihrer Erstellung folgt, zu vernichten.
(4) Der Empfänger ist zu verpflichten,
1. die übermittelten Daten nur zu dem Zweck zu verwenden, zu dem sie ihm übermittelt wurden,
2. eine angebrachte Kennzeichnung beizubehalten und
3. dem Bundesnachrichtendienst auf Ersuchen Auskunft über die Verwendung zu erteilen.
(5) Das zuständige Bundesministerium unterrichtet monatlich die G10-Kommission über Übermittlungen nach Absatz 1 und 2.
(6) Das Parlamentarische Kontrollgremium ist in Abständen von höchstens sechs Monaten über die vorgenommenen Übermittlungen nach Absatz 1 und 2 zu unterrichten.

§ 7a G 10 ist ebenfalls durch das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl. I S. 1938) geändert worden. Cybergefahren sind Gefahren im internationalen Raum. Die Bundesrepublik kann aufgrund der Komplexität und der internationalen Durchdringung Cyberbedrohungen nicht allein entgegentreten. Eine Übermittlung von Daten, die

mittels strategischer Fernmeldeaufklärung gemäß § 5 G10 erlangt wurden, kann daher auch an ausländische öffentliche Stellen geboten sein. Durch die entsprechende Ergänzung des § 7a G10 kann dies unter den genannten hohen Anforderungen im Einzelfall in Betracht kommen (BT-Drs. 18/4654 S. 42).

bb) Ausland-Ausland-Fernmeldeaufklärung

Vorbemerkung: In die nachfolgenden Ausführungen zur Ausland-Ausland-Fernmeldeaufklärung werden weitgehend die Gesetzesmaterialien eingearbeitet (Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BT-Drs. 18/9041)). Zur ergänzenden Lektüre wird das über Internet abrufbare Dokument empfohlen: Graulich, Gutachtliche Stellungnahme zum Entwurf der Fraktionen der CDU/CSU und SPD eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BT-Drs.18/9041) (Deutscher Bundestag Innenausschuss, Ausschussdrucksache 18(4)653 B vom 19. September 2016

Der gesetzliche Auftrag des Bundesnachrichtendienstes (BND) ist die Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind. Hierdurch leistet der BND einen wichtigen Beitrag zur Sicherheit der Bundesrepublik Deutschland. Ein wesentliches Instrument zur Erfüllung dieses gesetzlichen Auftrags ist **die strategische Fernmeldeaufklärung von Ausländerinnen und Ausländern im Ausland vom Inland aus** (sogenannte **„Ausland-Ausland-Fernmeldeaufklärung“**). Durch die Ausland-Ausland-Fernmeldeaufklärung kann der BND ohne Zeitverzug aktuelle und authentische Informationen erlangen und damit besonders wichtige auftragsrelevante Erkenntnisse aus internationalen Datenströmen gewinnen. Inhaltlich geht es dabei um die strategische, das heißt an internationalen und übergeordneten, für die Außen- und Sicherheitspolitik der Bundesrepublik Deutschland bedeutsamen Themen wie zum Beispiel internationaler Terrorismus, Proliferation von Massenvernichtungswaffen und Trägersystemen, internationale organisierte Kriminalität sowie politische Lageentwicklung in bestimmten Ländern ausgerichtete Aufklärung. Der BND stützt sich bislang bei der Durchführung der Ausland-Ausland-Fernmeldeaufklärung auf § 1 Abs. 2 des BND-Gesetzes (BNDG). Als Konsequenz aus der aktuellen rechtspolitischen Debatte sollen im Interesse der Rechtssicherheit – nicht zuletzt für die mit der Aufgabe der strategischen Fernmeldeaufklärung betrauten Mitarbeiterinnen und Mitarbeiter des BND – die bestehende Rechtslage präzisiert und spezielle rechtliche Grundlagen für die Ausland-Ausland-Fernmeldeaufklärung sowie eine diesbezügliche Kooperation mit ausländischen öffentlichen Stellen anderer Staaten geschaffen werden. Auch die gemeinsame Datenhaltung mit ausländischen öffentlichen Stellen soll auf eine spezielle Rechtsgrundlage gestellt werden.

In der Fachliteratur und im Zuge des 1. Untersuchungsausschusses der 18. Wahlperiode des Deutschen Bundestages („NSA-Untersuchungsausschuss“) wurde kontrovers diskutiert, ob für die Ausland-Ausland-Fernmeldeaufklärung vom Inland aus über die bestehende Aufgabenzuweisung in § 1 Absatz 2 des BND-Gesetzes (BNDG) hinaus eine spezialgesetzliche Regelung erforderlich sei. Mit der Neuregelung soll vor diesem Hintergrund eine klarstellende Regelung auf gesetzlicher Ebene für

dieses Mittel geschaffen werden, welches für die Aufgabenerfüllung des Bundesnachrichtendienstes (BND) unverzichtbar ist. Auch werden Kooperationen des BND mit ausländischen öffentlichen Stellen sowie die gemeinsame Datenhaltung des BND mit ausländischen öffentlichen Stellen spezialgesetzlich geregelt. Ziel des Gesetzes ist es insbesondere, eine ausdrückliche Rechtsgrundlage für die Ausland-Ausland-Fernmeldeaufklärung vom Inland aus zu schaffen.

In einem neuen Abschnitt 2 wird die strategische Fernmeldeaufklärung des BND gegenüber Ausländerinnen und Ausländern im Ausland klarstellend geregelt, soweit die Fernmeldeaufklärung vom Inland aus erfolgt (sogenannte Ausland-Ausland-Fernmeldeaufklärung). Die Fernmeldeaufklärung erfolgt vom Inland aus, wenn sich die Erfassungssysteme in Deutschland befinden. Die §§ 6 ff. BNDG-E sind lex specialis zu § 5 BNDG-E (bisher § 3 BNDG) und enthalten besondere Regelungen für die sogenannte Ausland-Ausland-Fernmeldeaufklärung. Ziel ist es, Rechtsklarheit und Rechtssicherheit beim Einsatz dieses Mittels zu gewährleisten. **Die Fernmeldeaufklärung vom Ausland aus stützt sich weiterhin auf § 1 Absatz 2 BNDG**. Eine Ausnahme stellt insoweit § 7 BNDG-E dar, der eine Verwendungsbeschränkung für die mit Mitteln der Fernmeldeaufklärung vom Ausland aus erhobenen Daten regelt. **Das Artikel 10-Gesetz bleibt unberührt.**

aaa) Voraussetzungen für die Erhebung und Verarbeitung von Daten (§ 6 BNDG)

Für die Ausland-Ausland-Fernmeldeaufklärung wird mit § 6 des BND-Gesetzes in der Entwurfsfassung (BNDG-E) eine ausdrückliche gesetzliche Grundlage geschaffen, die den rechtlichen Rahmen der Maßnahme klar absteckt und ein angemessenes Schutzniveau für die Betroffenen sichert. § 9 BNDG-E sieht ein Anordnungsverfahren für die Ausland-Ausland-Fernmeldeaufklärung mit entsprechenden Kontrollrechten einer neu zu schaffenden Kommission (Unabhängiges Gremium) vor. Die Pflichten der Telekommunikationsdienstleister werden analog zu den bereits nach dem Artikel 10-Gesetz (G10) geltenden Pflichten auch für die Ausland-Ausland-Fernmeldeaufklärung normiert. Die Kooperation des BND mit ausländischen öffentlichen Stellen wird in den §§ 13 ff. BNDG-E für den Bereich

§ 6 Voraussetzungen für die Erhebung und Verarbeitung von Daten

(1) Der Bundesnachrichtendienst darf zur Erfüllung seiner Aufgaben vom Inland aus mit technischen Mitteln Informationen einschließlich personenbezogener Daten aus Telekommunikationsnetzen, über die Telekommunikation von Ausländern im Ausland erfolgt (Telekommunikationsnetze), erheben und verarbeiten (Ausland-Ausland-Fernmeldeaufklärung), wenn diese Daten erforderlich sind, um
1. frühzeitig Gefahren für die innere oder äußere Sicherheit der Bundesrepublik Deutschland erkennen und diesen begegnen zu können,
2. die Handlungsfähigkeit der Bundesrepublik Deutschland zu wahren oder
3. sonstige Erkenntnisse von außen- und sicherheitspolitischer Bedeutung über Vorgänge zu gewinnen, die in Bezug auf Art und Umfang durch das Bundeskanzleramt im Einvernehmen mit dem Auswärtigen Amt, dem

Bundesministerium des Innern, dem Bundesministerium der Verteidigung, dem Bundesministerium für Wirtschaft und Energie und dem Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung bestimmt werden.
Die Datenerhebung darf nur aus denjenigen Telekommunikationsnetzen erfolgen, die das Bundeskanzleramt zuvor durch Anordnung bestimmt hat.

Absatz 1 bildet die zentrale Norm für die Ausland-Ausland-Fernmeldeaufklärung. Danach darf der BND zur Erfüllung seiner gemäß § 1 Absatz 2 Satz 1 BNDG auslandsbezogenen Aufgaben Informationen einschließlich personenbezogener Daten mit technischen Mitteln aus Telekommunikationsnetzen erheben und verarbeiten, wenn diese Daten erforderlich sind, um frühzeitig Gefahren für die innere oder äußere Sicherheit der Bundesrepublik Deutschland zu erkennen und diesen begegnen zu können (Nummer 1), um die Handlungsfähigkeit der Bundesrepublik Deutschland zu wahren (Nummer 2) oder um sonstige Erkenntnisse von außen- und sicherheitspolitischer Bedeutung zu gewinnen (Nummer 3). Absatz 1 konkretisiert damit den gesetzlichen Aufklärungsauftrag nach § 1 Absatz 2 Satz 1 BNDG, engt ihn aber nicht ein. Die Ausland-Ausland-Fernmeldeaufklärung ist und bleibt ein wesentliches und unverzichtbares Instrument, um eine Grundaussagefähigkeit des BND zu allen in sein Aufgabenspektrum fallende Bereiche sicherzustellen. Hierzu gehört neben der Aufklärung von Gefahren für die innere oder äußere Sicherheit der Bundesrepublik Deutschland die Gewinnung von Erkenntnissen zur Wahrung der – auch außenpolitischen – Handlungsfähigkeit der Bundesrepublik Deutschland. Auch die Aufklärung von wirtschaftspolitisch bedeutsamen Vorgängen kann erforderlich sein, soweit es sich nicht um unzulässige Wirtschaftsspionage handelt. Eine Erforderlichkeit zur Gewinnung von sonstigen Erkenntnissen von außen- und sicherheitspolitischer Bedeutung im Sinne von Nummer 3 kann angenommen werden, wenn die Aufklärungstätigkeit im Einklang mit dem sogenannten Auftragsprofil der Bundesregierung (APB) steht, das das Bundeskanzleramt im Einvernehmen mit den zuständigen Bundesministerien festgelegt. Die für Sicherheitsbelange zuständigen Bundesministerien sind das Auswärtige Amt, das Bundesministerium für Wirtschaft und Energie, das Bundesministerium des Innern, das Bundesministerium der Verteidigung sowie das Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung. In dem APB werden die Prioritäten, nach denen der BND gemäß seinem Auftrag außen- und sicherheitspolitisch relevante Informationen über das Ausland zu beschaffen und auszuwerten hat, festgelegt. Das mittel- und langfristig steuernde APB wird regelmäßig überprüft und kann zur schnellen Reaktion auf krisen- und krisenähnliche Szenarien auch kurzfristig aktualisiert werden. Die Bestimmung der auch mit den Mitteln der Ausland-Ausland-Fernmeldeaufklärung aufzuklärenden Vorgänge von außen- und sicherheitspolitischer Bedeutung unterliegt folglich wie die außen- und sicherheitspolitischen Gegebenheiten selbst gewissen Veränderungen. Die Datenerhebung erfolgt bei der Ausland-Ausland-Fernmeldeaufklärung aus Telekommunikationsnetzen. Der Begriff des Telekommunikationsnetzes wird in § 3 Nummer 27 des Telekommunikationsgesetzes (TKG) legaldefiniert: Ein Telekommunikationsnetz ist demnach „die Gesamtheit von Übertragungssystemen und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitigen Ressourcen, einschließlich der nicht aktiven Netzbestandteile, die die Übertragung von Signalen über Kabel, Funk, optische und andere elektromagnetische Einrichtungen

ermöglichen, einschließlich Satellitennetzen, festen, leitungs- und paketvermittelten Netzen, einschließlich des Internets, und mobilen terrestrischen Netzen, Stromleitungssystemen, soweit sie zur Signalübertragung genutzt werden, Netzen für Hör- und Fernsehfunk sowie Kabelfernsehnetzen, unabhängig von der Art der übertragenen Information“. Im Jahr 2004 wurde das Telekommunikationsgesetz neugefasst, um fünf europäische Richtlinien in nationales Recht umzusetzen. Eine dieser Richtlinien ist die Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (ABl. EG Nr. L 108 vom 24.4.2002 S. 33). Die Definition von Telekommunikationsnetzen entspricht Artikel 2 Buchstabe a dieser Richtlinie. Telekommunikationsnetze enthalten neben nicht leitungsgebundenen Strecken (u.a. Satellitenverkehre, Richtfunkverkehre, Kurzwellenverkehre) auch leitungsgebundene Strecken (u.a. Kabel, wie Lichtwellenleiter-Kabel). Mit der Aufnahme des Begriffs Telekommunikationsnetze in die §§ 6 ff. BNDG-E anstelle des im Artikel 10-Gesetzes verwendeten Begriffs der Übertragungswege werden die vielfältigen Möglichkeiten der Kommunikationsübertragung berücksichtigt. Es erfolgt mit der Aufnahme des Begriffs auch eine Angleichung an die im Telekommunikationsgesetz sowie im europäischen Raum genutzten Begrifflichkeiten. Telekommunikationsnetze, die ausschließlich der Anbindung eines einzelnen, individuellen Anschlusses dienen, sind nicht Gegenstand der strategischen Fernmeldeaufklärung. Für eine Anordnung einer Maßnahme im Rahmen der Ausland-Ausland-Fernmeldeaufklärung kommen nur solche Telekommunikationsnetze in Betracht, die auch ausländische Telekommunikation – also Telekommunikation von Ausländern im Ausland – führen, unabhängig davon, ob sie über deutsches Territorium geführt werden; beispielsweise sind dies Telekommunikationsnetze, die a) der Telekommunikation zwischen Endnutzern im Ausland, b) der Verbindung von Telekommunikationsnetzen nach Buchstabe a, oder c) der Steuerung von Telekommunikation in den unter Buchstaben a und b genannten Netzen dienen. Darunter fallen ebenso Telekommunikationsnetze im Ausland, die nur einem Land zugeordnet sind. Dass über ein Telekommunikationsnetz auch nationale Verkehre geführt werden, steht einer Anordnung nach § 6 BNDG-E nicht entgegen. Absatz 1 Satz 2 sieht vor, dass für die Ausland-Ausland-Fernmeldeaufklärung nur solche Telekommunikationsnetze genutzt werden dürfen, die durch das Bundeskanzleramt angeordnet wurden. Durch die Einführung eines speziellen Anordnungsverfahrens für die Ausland-Ausland-Fernmeldeaufklärung wird zum einen eine klare Trennung der Fernmeldeaufklärung nach dem BND-Gesetz von der Fernmeldeaufklärung nach dem Artikel 10-Gesetz erreicht. Gleichzeitig wird auf diese Weise sowohl die interne als auch die externe Kontrolle (durch das Bundeskanzleramt als anordnende Stelle und das neu einzuführende Unabhängige Gremium als zusätzliche Kontrollinstanz) der Ausland-Ausland-Fernmeldeaufklärung des BND verstärkt.

(2) Der Bundesnachrichtendienst darf die Erhebung von Inhaltsdaten im Rahmen der Ausland-Ausland-Fernmeldeaufklärung nur anhand von Suchbegriffen durchführen. Diese müssen für die Aufklärung von Sachverhalten nach Absatz 1 Satz 1 bestimmt und geeignet sein und ihre Verwendung muss im Einklang mit den außen- und sicherheitspolitischen Interessen der Bundesrepublik Deutschland stehen.

Die Erhebung von Inhaltsdaten ist im Rahmen der Ausland-Ausland-Fernmeldeaufklärung nur anhand von Suchbegriffen zulässig. Hierbei bleiben die Befugnisse aus § 12 BNDG-E unberührt. Es dürfen dabei nur solche Suchbegriffe verwendet werden, die zur Erhebung von auftragsrelevanten Informationen führen, das heißt die für die Aufklärung der nach Absatz 1 bestimmten Vorgänge geeignet sind. Suchbegriffe können u.a. Anschlusskennungen, Signaturen von Übertragungen (das heißt bestimmte technische Parameter) oder ein bestimmtes Telekommunikationsnetz einer geschlossenen Nutzergruppe sein. Darüber hinaus muss die Verwendung des Suchbegriffs im Einklang mit den außen- und sicherheitspolitischen Interessen der Bundesregierung stehen. Beispielsweise dürfen demnach grundsätzlich keine Suchbegriffe genutzt werden, die zur gezielten Erhebung von Verkehren von Staatsoberhäuptern führen, mit denen Deutschland enge und gute partnerschaftliche Beziehungen führt. Dies gilt auch dann, wenn dies auf die Erlangung von auftragsrelevanten Informationen gerichtet ist.

(3) Suchbegriffe, die zur gezielten Erfassung von Einrichtungen der Europäischen Union, von öffentlichen Stellen ihrer Mitgliedstaaten oder von Unionsbürgerinnen oder Unionsbürgern führen, dürfen nur verwendet werden, wenn dies erforderlich ist,
1. um Gefahren im Sinne des § 5 Absatz 1 Satz 3 des Artikel 10-Gesetzes zu erkennen und zu begegnen oder
2. um Informationen im Sinne des Absatzes 1 Satz 1 Nummer 1 bis 3 zu gewinnen, soweit ausschließlich Daten über Vorgänge in Drittstaaten gesammelt werden sollen, die von besonderer Relevanz für die Sicherheit der Bundesrepublik Deutschland sind.
Suchbegriffe, die zur gezielten Erfassung von Unionsbürgerinnen und Unionsbürgern führen, dürfen darüber hinaus verwendet werden, wenn dies erforderlich ist zur Erkennung und Begegnung von Straftaten im Sinne des § 3 Absatz 1 des Artikel 10-Gesetzes.

Absatz 3 regelt die konkreten Voraussetzungen für die Nutzung von Suchbegriffen, die zu einer gezielten Erfassung von Einrichtungen der Europäischen Union, öffentlicher Stellen ihrer Mitgliedsstaaten oder von Unionsbürgerinnen und Unionsbürgern führen. Eine gezielte Erfassung in diesem Sinne liegt vor, wenn die Verwendung eines bestimmten Suchbegriffs (zum Beispiel E-Mail-Adresse) dazu dienen soll, Telekommunikationsverkehre von Einrichtungen der Europäischen Union, öffentlichen Stellen ihrer Mitgliedsstaaten oder Unionsbürgerinnen und Unionsbürgern zu erheben. Ein Suchbegriff wird in diesem Sinne verwendet, wenn er in die Erfassungssysteme eingespeist wird, um Verkehre, die diesen Suchbegriff enthalten, zu erkennen und auszuleiten. Der BND setzt zur Prüfung der eingesetzten Suchbegriffe sowie auch zur Prüfung der erfassten Verkehre bzw. Suchbegriffe ein mehrstufiges Filtersystem ein. Dieses System wird regelmäßig aktualisiert und ergänzt. Gleichwohl können geschützte Verkehre zum Teil nicht unverzüglich als solche erkannt bzw. Anschlusskennungen nicht eindeutig einer Person zugeordnet werden. Telefoniert beispielsweise ein französischer Staatsangehöriger in Syrien mit einem syrischen Mobiltelefon mit einer anderen Person in Syrien, so kann seine französische Staatsangehörigkeit unter Umständen erst dann erkannt werden, wenn er in dem Telefonat erkennbar macht, dass er französischer Staatsangehöriger sein könnte. Suchbegriffe nach Absatz 3 dürfen nur in eng umgrenzten Ausnahmefällen verwendet

werden. Absatz 3 regelt die Voraussetzungen hierfür: Die Verwendung des Suchbegriffs muss entweder nach Satz 1 Nummer 1 zur Aufklärung von Gefahren im Sinne des § 5 G10 erforderlich sein, wobei anders als bei der Fernmeldeaufklärung nach § 5 G10 kein konkreter Inlandsbezug vorliegen muss. Nach Nummer 2 ist eine Verwendung von Suchbegriffen, die einer Einrichtung der Europäischen Union, einer öffentlichen Stelle eines Mitgliedstaates oder einer Unionsbürgerin oder einem Unionsbürger zugeordnet sind, außerdem zulässig, wenn dies erforderlich ist, um Informationen zur Erkennung und Begegnung von Gefahren für die innere oder äußere Sicherheit der Bundesrepublik Deutschland, zur Wahrung der Handlungsfähigkeit der Bundesrepublik Deutschland oder zur Gewinnung von sonstigen Erkenntnissen von außen- und sicherheitspolitischer Bedeutung zu erlangen. Weitere Voraussetzung ist, dass ausschließlich Daten über Vorgänge in Drittstaaten gesammelt werden sollen, die von besonderer Relevanz für die Sicherheit der Bundesrepublik Deutschland sind. Eine darüber hinausgehende Verwendung von Suchbegriffen, die zur gezielten Erfassung von Unionsbürgerinnen und Unionsbürgern führen, ist nur zulässig, wenn dies zur Erkennung und Begegnung von Straftaten im Sinne des § 3 Absatz 1 G10 erforderlich ist.

(4) Eine Erhebung von Daten aus Telekommunikationsverkehren von deutschen Staatsangehörigen, von inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen ist unzulässig.

Die Erhebung von Inhalts- und Verkehrsdaten von deutschen Staatsangehörigen, inländischen juristischen Personen oder sich im Bundesgebiet aufhaltenden Personen richtet sich nach dem Artikel 10-Gesetz. Der BND setzt hierfür ein mehrstufiges automatisiertes Filtersystem ein, um solche Verkehre zu erkennen und unverzüglich und unwiederbringlich zu löschen, wenn keine Beschränkungsmaßnahme nach dem Artikel 10-Gesetz vorliegt. Die Erhebung von sonstigen personenbezogenen Daten (also solche, die nicht Artikel 10 GG unterfallen) von deutschen Staatsangehörigen, inländischen juristischen Personen oder sich im Bundesgebiet aufhaltenden Personen mit Mitteln der Ausland-Ausland-Fernmeldeaufklärung ist nicht ausgeschlossen.

(5) Eine Ausland-Ausland-Fernmeldeaufklärung zum Zwecke der Erzielung von Wettbewerbsvorteilen (Wirtschaftsspionage) ist unzulässig.

Absatz 5 legt fest, dass die Informationsgewinnung und -nutzung zur Erzielung von Wettbewerbsvorteilen (Wirtschaftsspionage) – wie bei der Auftragserfüllung durch den BND insgesamt – auch bei der Ausland-Ausland-Fernmeldeaufklärung unzulässig ist.

(6) Verkehrsdaten werden höchstens sechs Monate gespeichert. Die §§ 19 und 20 bleiben im Übrigen unberührt.

Die Speicherdauer für die erhobenen Verkehrsdaten beträgt höchstens sechs Monate. Eine längere Speicherung setzt eine Prüfung im Einzelfall voraus, ob die weitere Speicherung nach § 19 Absatz 1 BNDG-E (bislang § 4 BNDG) für die Erfüllung der Aufgaben des BND erforderlich ist. Die §§ 19 und 20 BNDG-E (bislang § 5 BNDG)

finden nur dann Anwendung. Absatz 6 Satz 1 ist insofern lex specialis zu den §§ 19 und 20 BNDG-E. Die sechsmonatige Speicherfrist dient insbesondere der frühzeitigen Erkennung neuer für den BND auftragsrelevanter Teilnehmer im Ausland durch eine Analyse der erhobenen Verkehrsdaten. Darüber hinaus können beispielsweise nach einem Terroranschlag die gespeicherten Verkehrsdaten auf mögliche Verkehre der von den Tätern genutzten, bislang unbekannten Anschlusskennungen, geprüft werden. Auf diese Weise könnten das Umfeld der Täter oder auch weitere Täter schnell identifiziert werden, um möglicherweise sogar Folgeanschläge rechtzeitig zu erkennen und zu verhindern. Zudem können in den Bereichen organisierte Kriminalität und Terrorismus auch Aufenthaltsorte oder Reisetätigkeiten Hinweise auf auftragsrelevante Aktivitäten geben. Mit der sechsmonatigen Speicherdauer wird ein angemessener Ausgleich der Interessen der ausländischen Betroffenen im Ausland mit den nachrichtendienstlichen Erfordernissen gefunden.

(7) Die technische und organisatorische Umsetzung von Maßnahmen nach Absatz 1 sowie die Kontrollzuständigkeiten innerhalb des Bundesnachrichtendienstes sind in einer Dienstvorschrift festzulegen, die auch das Nähere zu dem Anordnungsverfahren regelt. Die Dienstvorschrift bedarf der Zustimmung des Bundeskanzleramtes. Das Bundeskanzleramt unterrichtet das Parlamentarische Kontrollgremium.

Die Einzelheiten der Umsetzung der Ausland-Ausland-Fernmeldeaufklärung, u.a. die BND-internen Abläufe und Zuständigkeiten, Prüf- und Unterrichtungsvorgaben sowie technische Details der Ausland-Ausland-Fernmeldeaufklärung, sind in einer Dienstvorschrift zu regeln. Die Dienstvorschrift bedarf der Zustimmung des Bundeskanzleramtes, das das Parlamentarische Kontrollgremium unterrichtet.

bbb) Verarbeitung und Nutzung der vom Ausland aus erhobenen Daten (§ 7 BNDG)

§ 7 Verarbeitung und Nutzung der vom Ausland aus erhobenen Daten
(1) Für die Verarbeitung und Nutzung der vom Bundesnachrichtendienst mit Mitteln der Fernmeldeaufklärung vom Ausland aus erhobenen Daten gilt § 6 Absatz 1 Satz 1, Absatz 3 bis 6 entsprechend.

Absatz 1 stellt klar, dass für die Verarbeitung und Nutzung der mit Mitteln der Fernmeldeaufklärung vom Ausland aus erhobenen Daten im Inland trotz der an sich von § 1 Absatz 2 Satz 2 BNDG vorgesehenen Beschränkung des BNDG auf Fälle von Datenerhebungen im Inland die materiellen Beschränkungen des § 6 Absatz 1 Satz 1, Absatz 3 bis 6 BNDG-E gelten, also unabhängig vom Standort der Datenerhebung durch den BND. Eine Datenerhebung im Sinne von Absatz 1 liegt auch vor, wenn dem BND die Daten im Ausland durch einen Telekommunikationsanbieter ausgeleitet werden. Bei der Verwendung ist mithin zu beachten, dass die Daten nur zu den in § 6 Absatz 1 Satz 1 BNDG-E benannten Zwecken verwendet werden dürfen. Bei der Verwendung solcher Daten ist der Schutz von Einrichtungen der Europäischen Union und öffentlichen Stellen ihrer Mitglieder sowie von Unionsbürgerinnen und Unionsbürgern nach § 6 Absatz 3 BNDG-E, der Schutz von deutschen Staatsangehörigen, von inländischen juristischen Personen sowie sich im Bundesgebiet

aufhaltenden Personen nach § 6 Absatz 4 BNDG-E sowie das Verbot der Wirtschaftsspionage nach § 6 Absatz 5 BNDG-E zu beachten. Ferner gelten die Regelungen des § 6 Absatz 6 BNDG-E zur Speicherdauer für Verkehrsdaten entsprechend.

(2) Eine gezielte Erfassung von Einrichtungen der Europäischen Union, von öffentlichen Stellen ihrer Mitgliedstaaten oder von Unionsbürgerinnen oder Unionsbürgern durch ausländische öffentliche Stellen vom Ausland aus darf durch den Bundesnachrichtendienst nur unter den Voraussetzungen des § 6 Absatz 3 veranlasst werden.

Mit Absatz 2 wird der sogenannte Ringtausch ausgeschlossen. Erfolgt die Datenerhebung für den BND zum Beispiel im Rahmen einer Kooperation durch eine ausländische öffentliche Stelle im Ausland, dürfen Suchbegriffe zu Unionsbürgerinnen und Unionsbürgern, Einrichtungen der Europäischen Union oder von öffentlichen Stellen ihrer Mitgliedstaaten nur dann verwendet werden, wenn die Voraussetzungen des § 6 Absatz 3 BNDG-E vorliegen. Eine Umgehung des Schutzes für europäische Stellen und Unionsbürger ist ausgeschlossen.

ccc) Pflichten der Anbieter von Telekommunikationsdiensten (§ 8 BNDG)

§ 8 regelt die Pflichten der Anbieter von Telekommunikationsdiensten. Diese sind parallel zu dem Verfahren bei Maßnahmen nach dem Artikel 10-Gesetz ausgestaltet.

§ 8 Pflichten der Anbieter von Telekommunikationsdiensten
(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt, hat dem Bundesnachrichtendienst auf Anordnung Auskunft über die näheren Umstände der nach Wirksamwerden der Anordnung durchgeführten Telekommunikation zu erteilen, Sendungen, die ihm zur Übermittlung auf dem Telekommunikationsweg anvertraut sind, auszuhändigen sowie die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen. Die §§ 3 und 4 bleiben unberührt. Ob und in welchem Umfang das verpflichtete Telekommunikationsunternehmen Vorkehrungen für die technische und organisatorische Umsetzung der Überwachungsmaßnahmen zu treffen hat, bestimmt sich nach § 110 des Telekommunikationsgesetzes und der dazu erlassenen Rechtsverordnung.

Anbieter von Telekommunikationsdiensten sind verpflichtet, an der Durchführung der Ausland-Ausland-Fernmeldeaufklärung mitzuwirken. Die hierfür erforderlichen Mitwirkungspflichten werden in Absatz 1 bestimmt: Sie haben auf Anordnung des BND Auskunft über die näheren Umstände der Telekommunikation zu erteilen, Sendungen sind dem BND auszuhändigen sowie die Überwachung und Aufzeichnung zu ermöglichen. Die Pflichten der Anbieter von Telekommunikationsdiensten sind im Näheren im Telekommunikationsgesetz und in der Telekommunikations-Überwachungsverordnung geregelt.

(2) Das nach Absatz 1 verpflichtete Unternehmen hat vor Durchführung einer beabsichtigten Maßnahme unverzüglich die Personen, die mit der Durchführung der Maßnahme betraut werden sollen,
1. auszuwählen,
2. einer einfachen Sicherheitsüberprüfung unterziehen zu lassen und
3. über Mitteilungsverbote nach § 17 sowie die Strafbarkeit eines Verstoßes nach § 34 zu belehren; die Belehrung ist aktenkundig zu machen.
Mit der Durchführung einer Maßnahme dürfen nur Personen betraut werden, die nach Maßgabe des Satzes 1 überprüft und belehrt worden sind. Nach Zustimmung des Bundeskanzleramtes kann die Behördenleiterin oder der Behördenleiter des Bundesnachrichtendienstes oder eine Vertreterin oder ein Vertreter die nach Absatz 1 verpflichteten Unternehmen schriftlich auffordern, die Maßnahme bereits vor Abschluss der Sicherheitsüberprüfung durchzuführen. Die nach Absatz 1 verpflichteten Unternehmen haben sicherzustellen, dass die Geheimschutzmaßnahmen nach der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen vom 31. März 2006 (GMBl S. 803), die zuletzt durch die Allgemeine Verwaltungsvorschrift vom 26. April 2010 (GMBl S. 846) geändert worden ist, in der jeweils geltenden Fassung getroffen werden.

Verpflichtete Anbieter von Telekommunikationsdiensten haben die erforderlichen Geheimschutzvorkehrungen zu treffen. Dazu gehört u.a., dass die hiermit betrauten Mitarbeiterinnen und Mitarbeiter einer Sicherheitsüberprüfung unterzogen werden müssen und sie über die Mitteilungsverbote nach § 17 BNDG-E sowie die Folgen eines Verstoßes nach § 34 BNDG-E zu belehren sind. Darüber hinaus sind alle Geheimschutzmaßnahmen nach der Verschlusssachenanweisung des Bundesministeriums des Innern zu treffen.

(3) Die Sicherheitsüberprüfung nach Absatz 2 Satz 1 Nummer 2 ist entsprechend dem Sicherheitsüberprüfungsgesetz durchzuführen. Zuständig ist das Bundesministerium des Innern. Soll mit der Durchführung einer Maßnahme eine Person betraut werden, für die innerhalb der letzten fünf Jahre bereits eine gleich- oder höherwertige Sicherheitsüberprüfung nach Bundes- oder Landesrecht durchgeführt worden ist, soll von einer erneuten Sicherheitsüberprüfung abgesehen werden.

Absatz 3 regelt die Durchführung der Sicherheitsüberprüfung. Diese richtet sich nach dem Sicherheitsüberprüfungsgesetz.

ddd) Anordnung und Unterrichtung (§ 9 BNDG)

(1) Die Anordnung nach § 6 Absatz 1 ergeht schriftlich auf Antrag der Behördenleiterin oder des Behördenleiters des Bundesnachrichtendienstes oder einer Vertreterin oder eines Vertreters. Der Antrag sowie die Anordnung müssen bezeichnen:
1. den Grund und die Dauer der Maßnahme,
2. das betroffene Telekommunikationsnetz sowie
3. das nach § 8 verpflichtete Unternehmen.

Der Antrag zur Durchführung der Ausland-Ausland-Fernmeldeaufklärung ist durch die Präsidentin oder den Präsidenten des BND oder eine Vertreterin oder einen Vertreter zu stellen. Die Präsidentin oder der Präsident des BND kann mithin die Antragsbefugnis auch dauerhaft auf einen von ihr oder ihm bestimmte Vertreterin oder bestimmten Vertreter delegieren. Für die Beantragung gilt das Schriftformerfordernis und die anzuordnenden Telekommunikationsnetze sind zu benennen. Zur Ermöglichung einer Prüfung der Anträge ist der Grund der beantragten Maßnahme darzustellen. Häufig leiten Telekommunikationsdienstleister Verkehre dynamisch auf ihren Strecken. Um diesen dynamischen Leitweglenkungen folgen zu können, kann es erforderlich sein, auch übergeordnete Telekommunikationsnetze anordnen zu können. Dadurch kann der BND wechselnde Anteile aus diesen angeordneten Telekommunikationsnetzen für die Erhebung nutzen. Sofern für die Durchführung der Maßnahme die Mitwirkung des Telekommunikationsdienstleisters erforderlich ist (zum Beispiel Kabelverkehre), ist der zu verpflichtende Telekommunikationsdienstleister in der Anordnung sowie das angeordnete Telekommunikationsnetz zu benennen. Eine Kapazitätsbeschränkung ist – anders als im Artikel 10-Gesetz – nicht erforderlich. Der BND kann bereits aus tatsächlichen Gründen nur einen sehr geringen Anteil der weltweiten Telekommunikation erfassen. Einer Kapazitätsbeschränkung, die eine flächendeckende Überwachung ausschließen soll, bedarf es daher nicht.

(2) Der Anordnung durch die Behördenleiterin oder den Behördenleiter oder durch eine Vertreterin oder einen Vertreter bedarf die Bestimmung der Suchbegriffe
1. nach § 6 Absatz 3 Satz 1 Nummer 1, soweit sich diese auf Einrichtungen der Europäischen Union oder auf öffentliche Stellen ihrer Mitgliedstaaten beziehen sowie
2. nach § 6 Absatz 3 Satz 1 Nummer 2.
Das Bundeskanzleramt ist über Anordnungen nach Satz 1 zu unterrichten.

Zusätzlich zu der Anordnung der Telekommunikationsnetze nach Absatz 1 in Verbindung mit § 6 Absatz 1 BNDG-E bedarf die Bestimmung der Suchbegriffe in den in Absatz 2 benannten Fällen einer Anordnung durch die Präsidentin oder den Präsidenten des BND oder einer Vertreterin oder einen Vertreter. Die Steuerung von Suchbegriffen von Einrichtungen der Europäischen Union sowie ihrer Mitgliedstaaten bedarf danach immer einer entsprechenden Anordnung. Die Nutzung von Suchbegriffen, die Unionsbürgerinnen und Unionsbürger zugeordnet sind, bedarf nur dann einer Anordnung durch die Präsidentin oder den Präsidenten des BND oder einer Vertreterin oder einen Vertreter, wenn ein Fall des § 6 Absatz 3 Satz 1 Nummer 2 BNDG-E vorliegt. Danach dürfen Suchbegriffe verwendet werden, wenn bestimmte Informationen (Gefahren für die innere und äußere Sicherheit Deutschlands, für die Handlungsfähigkeit Deutschlands und sonstige Erkenntnisse von außen- und sicherheitspolitischer Bedeutung) gewonnen werden sollen und soweit ausschließlich Daten über Vorgänge in Drittstaaten gesammelt werden sollen, die von besonderer Relevanz für die Sicherheit der Bundesrepublik Deutschland sind.

(3) Die Anordnungen nach Absatz 2 und § 6 Absatz 1 sind auf höchstens neun Monate zu befristen. Verlängerungen um jeweils bis zu neun Monate sind zulässig, soweit die Voraussetzungen der Anordnung fortbestehen.

Die Anordnung sowohl der Telekommunikationsnetze nach § 6 Absatz 1 BNDG-E als auch der Suchbegriffe nach § 6 Absatz 3 BNDG-E ist auf höchstens neun Monate zu befristen. Beide Arten der Anordnung können – gegebenenfalls mehrfach – verlängert werden. Die Anordnungsfähigkeit ist bei einer beantragten Verlängerung stets erneut zu prüfen.

(4) Das Bundeskanzleramt unterrichtet das Unabhängige Gremium über die von ihm getroffenen Anordnungen nach § 6 Absatz 1 vor deren Vollzug. Das Unabhängige Gremium prüft die Zulässigkeit und Notwendigkeit der Anordnung. Die Anordnung kann auch ohne vorherige Unterrichtung des Unabhängigen Gremiums vollzogen werden, wenn das Ziel der Maßnahme ansonsten vereitelt oder wesentlich erschwert würde. In diesem Fall ist die Unterrichtung des Unabhängigen Gremiums unverzüglich nachzuholen. Anordnungen, die das Unabhängige Gremium für unzulässig oder nicht notwendig erklärt, sind unverzüglich aufzuheben.

Absatz 4 enthält eine Verpflichtung zur Unterrichtung des Unabhängigen Gremiums durch das Bundeskanzleramt über die von ihm angeordneten Maßnahmen nach § 6 Absatz 1 BNDG-E vor deren Vollzug. Die Möglichkeit des Vollzugs der Anordnung einer Maßnahme schon vor der Unterrichtung des Unabhängigen Gremiums ist vorgesehen, wenn die Gefahr besteht, dass das Ziel der Maßnahme durch die Verzögerung aufgrund des zusätzlichen Verfahrens ansonsten vereitelt oder wesentlich erschwert wird. Um der Bundesregierung beispielsweise bei Entführungsfällen im Ausland, bei denen Kommunikation erhoben werden soll, die nicht dem Artikel 10-Gesetz unterfällt, oder in anderen Ausnahmesituationen unverzüglich Informationen über neue krisenhafte Entwicklungen zur Verfügung stellen zu können, müssen die strategischen Beschaffungsmöglichkeiten des BND kurzfristig angepasst werden können. Das Unabhängige Gremium ist in diesem Fall spätestens im Rahmen der nächsten Sitzung zu unterrichten.

(5) Das Bundeskanzleramt unterrichtet das Unabhängige Gremium über die vom Bundesnachrichtendienst getroffenen Anordnungen nach Absatz 2, soweit sich diese auf Einrichtungen der Europäischen Union oder auf öffentliche Stellen ihrer Mitgliedstaaten beziehen. Anordnungen, die das Unabhängige Gremium für unzulässig oder nicht notwendig erklärt, sind unverzüglich aufzuheben. Das Unabhängige Gremium ist im Übrigen befugt, die Einhaltung der Vorgaben des § 6 Absatz 3 jederzeit stichprobenartig zu kontrollieren. Die Kontrollrechte des Parlamentarischen Kontrollgremiums bleiben unberührt.

Nach Absatz 5 ist das Unabhängige Gremium über Anordnungen der Behördenleiterin oder des Behördenleiters oder ihrer oder seiner Vertretung zur Bestimmung von Suchbegriffen zu unterrichten soweit sich diese auf Einrichtungen der Europäischen Union oder auf öffentliche Stellen ihrer Mitgliedstaaten beziehen. Die sonstigen Suchbegriffe kann das Unabhängige Gremium stichprobenartig auf die Einhaltung der Vorgaben des § 6 Absatz 3 BNDG-E hin überprüfen. Bei der Prüfung kann das Unabhängige Gremium beispielsweise eine Erläuterung zu ausgewählten

Suchbegriffen verlangen. Die Kontrollrechte des Parlamentarischen Kontrollgremiums bleiben unberührt.

eee) Kennzeichnung und Löschung (§ 10 BNDG)

§ 10 regelt Löschpflichten und Kennzeichnungspflichten. Mit den Löschpflichten wird berücksichtigt, dass besonders geschützte Personen zum Teil nicht bereits zum Zeitpunkt der Erhebung des Verkehrs oder unverzüglich nach Erhebung erkannt werden können. Sobald dem BND hinreichende Hinweise vorliegen, dass ein Verkehr einem besonderen Schutz unterliegt, ist dieser zu löschen bzw. zu sperren, sofern die gesetzlichen Vorgaben für die Erfassung solcher Verkehre nicht erfüllt sind.

(1) Die nach § 6 erhobenen Daten sind zu kennzeichnen.

Die Kennzeichnung der nach § 6 Absatz 1 BNDG-E erhobenen Daten dient insbesondere der Wahrung der Unterrichtungspflichten. Dies wird durch eine Implementierung in den Erfassungssystemen gewährleistet. Die Kennzeichnungspflicht beschränkt sich auf die erhobenen Verkehre. Wird eine Einzelinformation aus einem Verkehr zum Beispiel für einen Bericht des BND genutzt, so unterliegt der Bericht keiner Kennzeichnungspflicht.

(2) Wird eine Anordnung nach § 9 Absatz 5 Satz 2 aufgehoben, so sind die aufgrund dieser Anordnung bereits erhobenen Daten unverzüglich zu löschen.

Sofern eine Anordnung nach § 9 Absatz 5 Satz 2 BNDG-E durch das Unabhängige Gremium aufgehoben wird, sind die aufgrund der Anordnung bereits erhobenen Verkehre unverzüglich zu löschen. Für die Berichtigung, Sperrung und Löschung von Daten gilt im Übrigen § 20 BNDG-E (bislang § 5 BNDG).

(3) Werden Daten entgegen § 6 Absatz 3 oder § 9 Absatz 2 erhoben, sind diese unverzüglich zu löschen. Das Unabhängige Gremium ist hierüber zu unterrichten. Wird nachträglich erkannt, dass ein Suchbegriff einer Einrichtung der Europäischen Union, einer öffentlichen Stelle eines Mitgliedstaates oder einer Unionsbürgerin oder einem Unionsbürger zuzuordnen ist, sind die mittels dieses Suchbegriffs erhobenen Telekommunikationsverkehre ebenfalls unverzüglich zu löschen, es sei denn, eine gezielte Erfassung nach § 6 Absatz 3 wäre zulässig gewesen.

Wird nach Erhebung eines Verkehrs erkannt, dass der Suchbegriff, der zu der Erhebung des Verkehrs geführt hat, einer Einrichtung der Europäischen Union, einer öffentlichen Stelle eines Mitgliedstaates oder einer Unionsbürgerin oder einem Unionsbürger zugeordnet ist, so sind die Verkehre zu löschen, die aufgrund dieses Suchbegriffs erhoben wurden. Die Löschung muss unverzüglich erfolgen. Eine Löschung unterbleibt, wenn die materiellen Voraussetzungen für eine gezielte Erfassung des Verkehrs nach § 6 Absatz 3 BNDG-E vorliegen.

(4) Werden Daten entgegen § 6 Absatz 4 erhoben, sind diese unverzüglich zu löschen. Werden die Daten nicht unverzüglich gelöscht, ist die G10-Kommission in der

folgenden Sitzung zu unterrichten und der betroffenen Person ist die Erhebung der Daten mitzuteilen, sobald
1. ausgeschlossen werden kann, dass hierdurch der Zweck der Maßnahme gefährdet ist und
2. kein überwiegender Nachteil für das Wohl des Bundes oder eines Landes absehbar ist.
Erfolgt die Mitteilung nicht binnen zwölf Monaten nach Erhebung der Daten, bedarf die weitere Zurückstellung der Zustimmung der G10-Kommission. Die G10-Kommission bestimmt die weitere Dauer der Zurückstellung. Fünf Jahre nach Erhebung der Daten kann mit Zustimmung der G10-Kommission endgültig von der Mitteilung abgesehen werden, wenn die Voraussetzungen für die Mitteilung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden. Solange die personenbezogenen Daten für eine Mitteilung oder für eine gerichtliche Nachprüfung der Datenerhebung von Bedeutung sein können, wird die Löschung zurückgestellt und die personenbezogenen Daten werden gesperrt; sie dürfen nur zu diesen Zwecken verwendet werden.

Werden durch die Ausland-Ausland-Fernmeldeaufklärung Verkehre erhoben, an denen eine deutsche Staatsangehörige oder ein deutscher Staatsangehöriger, eine inländische juristische Person oder eine sich im Bundesgebiet aufhaltende Person beteiligt ist, und wird dieser Verkehr nicht unverzüglich gelöscht, ist dies der betroffenen Person grundsätzlich mitzuteilen. Eine Mitteilung kommt jedoch nur in Betracht, wenn ausgeschlossen ist, dass der Zweck der Maßnahme (zum Beispiel Aufklärung eines bestimmten Terrornetzwerks) hierdurch gefährdet wird und kein übergreifender Nachteil für das Wohl des Bundes oder eines Landes absehbar ist (zum Beispiel wenn durch die Mitteilung besondere Aufklärungsfähigkeiten des BND bekannt würden). Die Zuständigkeit in diesen Mitteilungsfällen liegt wie der bisherigen Praxis entsprechend bei der G10-Kommission. Sofern die Mitteilung nicht innerhalb von zwölf Monaten nach dem Datum der Erhebung erfolgt, entscheidet die G10-Kommission über die weitere Zurückstellung der Mitteilung. Auch die Entscheidung über die endgültige Nichtmitteilung obliegt der G10Kommission. Die Entscheidung über die endgültige Nichtmitteilung darf erst fünf Jahre nach Erhebung des Verkehrs erfolgen und die Voraussetzungen für die Mitteilungen müssen mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten. Solange die Daten noch für eine Mitteilung oder eine gerichtliche Überprüfung der Erhebung erforderlich sind, darf keine Löschung erfolgen. Die Löschung erfolgt daher erst nach einer endgültigen Nichtmitteilung oder – bei Mitteilung – nach Ablauf der Rechtsmittelfrist. Die Daten werden gesperrt, um eine weitere Nutzung der Daten durch den BND auszuschließen.

(5) Werden Daten entgegen § 6 Absatz 5 erhoben, sind diese unverzüglich zu löschen.

Werden durch die Ausland-Ausland-Fernmeldeaufklärung (ungezielt) Informationen erhoben, die zur Erzielung von Wettbewerbsvorteilen geeignet wären (entgegen § 6 Absatz 5 BNDG-E), dürfen diese durch den BND nicht genutzt werden und sind unverzüglich zu löschen.

(6) Löschungen nach den Absätzen 2 bis 5 sind zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung der Datenschutzkontrolle verwendet werden. Die Protokolldaten sind bis zum Ablauf des zweiten auf die Protokollierung folgenden Kalenderjahres aufzubewahren und danach unverzüglich zu löschen.

Die Löschungen nach den Absätzen 2 bis 5 sind zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Datenschutzkontrolle durch den oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) bzw. den behördlichen Datenschutz des BND verwendet werden und sind bis zum Ablauf des zweiten auf die Protokollierung folgenden Jahres aufzubewahren und danach unverzüglich zu löschen. Durch diese Pflicht zur Aufbewahrung der Protokolldaten wird eine angemessene Datenschutzkontrolle sichergestellt.

fff) Kernbereichsschutz (§ 11 BNDG)

§ 11 Kernbereichsschutz
Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach § 6 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Sofern durch eine Maßnahme nach § 6 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt wurden, dürfen diese nicht verwertet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen. Sowohl ihre Erlangung als auch ihre Löschung sind aktenkundig zu machen.

Die Vorschrift regelt den Schutz des Kernbereichs privater Lebensgestaltung im Rahmen der Ausland-Ausland-Fernmeldeaufklärung. Die Vorschrift sieht ebenso wie andere Regelungen (vgl. etwa § 100a Absatz 4 der Strafprozessordnung sowie § 5a G10) zum Kernbereichsschutz im Bereich der Telekommunikationsüberwachung ein zweistufiges Schutzkonzept vor, um den Betroffenen vor Eingriffen in den absolut geschützten Kernbereich privater Lebensgestaltung zu bewahren. Auf Ebene der Datenerhebung bestimmt Satz 1, dass eine zielgerichtete Erhebung kernbereichsrelevanter Daten zu unterbleiben hat. Eine Maßnahme der strategischen Fernmeldeaufklärung ist danach unzulässig, sofern tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden. Kommt es dennoch zur Erhebung kernbereichsrelevanter Daten, schreibt Satz 2 ein umfassendes Verwertungsverbot, ein unverzügliches Löschungsgebot sowie eine entsprechende Pflicht zur Protokollierung der Löschung vor.

ggg) Eignungsprüfung (§ 12 BNDG)

Im Rahmen der Eignungsprüfung wird der Datenstrom durch den BND auf zwei Kriterien hin geprüft: Zum einen wird der Datenstrom genutzt, um neue Suchbegriffe für die Ausland-Ausland-Fernmeldeaufklärung zu generieren. Durch die Sichtung des Datenstroms können zum Beispiel neue Kommunikationsmittel erkannt werden, die zur Generierung neuer Suchbegriffe genutzt werden können. Würde ausschließlich der bereits selektierte Datenstrom durch den BND betrachtet, würden die

Erfassungsmöglichkeiten des BND massiv eingeschränkt werden. Der Datenstrom wird zum anderen daraufhin geprüft, ob sich bestimmte Strecken für die Ausland-Ausland-Fernmeldeaufklärung eignen.

§ 12 Eignungsprüfung
(1) Der Bundesnachrichtendienst darf Informationen einschließlich personenbezogener Daten aus Telekommunikationsnetzen erheben und auswerten, soweit dies zur Bestimmung
1. geeigneter Suchbegriffe oder
2. geeigneter Telekommunikationsnetze
für Maßnahmen nach § 6 erforderlich ist (Eignungsprüfung).

In Absatz 1 wird festgelegt, zu welchen Zwecken die Eignungsprüfung erfolgen darf. Bei der Eignungsprüfung werden aus Telekommunikationsnetzen ohne Einsatz von Suchbegriffen Daten erhoben, um geeignete Suchbegriffe oder geeignete Telekommunikationsnetze für Maßnahmen der Ausland-Ausland-Fernmeldeaufklärung zu bestimmen.

(2) Die Eignungsprüfung ist durch die Behördenleiterin oder den Behördenleiter oder durch eine Vertreterin oder einen Vertreter anzuordnen. Sie darf nur angeordnet werden, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass in dem zu prüfenden Telekommunikationsnetz geeignete Daten übertragen werden. Die Anordnung ist auf sechs Monate zu befristen. Ist für die Durchführung der Eignungsprüfung die Mitwirkung eines Unternehmens, das Telekommunikationsdienste anbietet, erforderlich, gelten § 6 Absatz 1 Satz 2 sowie die §§ 8 und 9 Absatz 1 entsprechend.

Die Eignungsprüfung muss vorab durch die Präsidentin oder den Präsidenten des BND oder ihrer oder seiner Vertretung angeordnet werden. Voraussetzung der Anordnung ist, dass tatsächliche Anhaltspunkte dafür vorliegen, dass in dem jeweiligen Telekommunikationsnetz Daten übertragen werden, die für die Auftragserfüllung des BND relevant sind. Sofern für die Eignungsprüfung die Mitwirkung eines Anbieters eines Telekommunikationsdienstes erforderlich ist, bedarf es der Anordnung durch das Bundeskanzleramt. Es wird auf die entsprechenden Regelungen für das Anordnungsverfahren verwiesen.

(3) Die im Rahmen einer Eignungsprüfung erhobenen personenbezogenen Daten dürfen nur zum Zweck der Eignungsprüfung verwendet werden. § 5 Absatz 7 Satz 2 bis 8 des BSI-Gesetzes gilt entsprechend. Der Bundesnachrichtendienst darf die erhobenen personenbezogenen Daten speichern, soweit dies zur Durchführung der Eignungsprüfung erforderlich ist. Die Auswertung ist unverzüglich nach der Erhebung durchzuführen.

Absatz 3 regelt die Zweckbindung für die erhobenen personenbezogenen Daten. Eine anderweitige Nutzung als in Absatz 1 benannt, ist nur in Ausnahmefällen zulässig. Der Kernbereichsschutz wird durch einen Verweis auf eine Regelung im BSIGesetz sichergestellt. Danach gilt auch für Daten, die im Rahmen der Eignungsprüfung erhoben wurden, entsprechend § 5 Absatz 7 Satz 2 bis 8 BSI-Gesetz: „Soweit möglich, ist technisch

sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Werden aufgrund der Maßnahmen der Absätze 1 bis 3 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder Daten im Sinne des § 3 Absatz 9 des Bundesdatenschutzgesetzes erlangt, dürfen diese nicht verwendet werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung sind unverzüglich zu löschen. Dies gilt auch in Zweifelsfällen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.“ Eine Speicherung der erhobenen personenbezogenen Daten ist im Rahmen der Eignungsprüfung zulässig, die Speicherdauer wird in Absatz 4 geregelt. Die Auswertung der erhobenen Daten hat unverzüglich zu erfolgen.

(4) Personenbezogene Daten für eine Eignungsprüfung nach Absatz 1 Nummer 1 sind spätestens zwei Wochen, personenbezogene Daten für eine Eignungsprüfung nach Absatz 1 Nummer 2 spätestens vier Wochen nach ihrer Erhebung spurenlos zu löschen. Die Löschung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung der Datenschutzkontrolle verwendet werden. Die Protokolldaten sind bis zum Ablauf des zweiten auf die Protokollierung folgenden Kalenderjahres aufzubewahren und danach unverzüglich zu löschen.

Absatz 4 legt die Speicherdauer für die personenbezogenen Daten fest, die im Rahmen der Eignungsprüfung erhoben wurden. Soweit die personenbezogenen Daten für die Bestimmung geeigneter Suchbegriffe ausgewertet werden sollen, dürfen diese für zwei Wochen gespeichert werden. Dienen die personenbezogenen Daten zur Bestimmung geeigneter Telekommunikationsnetze, darf die Speicherung für höchstens vier Wochen erfolgen. Für die Löschung der personenbezogenen Daten gelten die bereits in § 10 Absatz 6 BNDG-E geregelten Protokollierungspflichten.

(5) Eine über Absatz 3 Satz 1 hinausgehende Verwendung der erhobenen personenbezogenen Daten ist nur zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dadurch eine erhebliche Gefahr abgewendet werden kann für
1. Leib, Leben oder Freiheit einer Person oder
2. die Sicherheit der Bundesrepublik Deutschland.

Absatz 5 ermöglicht eine zweckändernde Nutzung von Daten für den Fall, dass tatsächliche Anhaltspunkte dafür vorliegen, dass hierdurch eine erhebliche Gefahr für Leib, Leben oder Freiheit einer Person oder für die Sicherheit Deutschlands abgewendet werden kann.

(6) Daten aus laufenden Maßnahmen nach § 6 können auch für Eignungsprüfungen verwendet werden; die Absätze 1 und 3 bis 5 gelten entsprechend.

Eine Eignungsprüfung darf auch bei Telekommunikationsnetzen erfolgen, die bereits durch das Bundeskanzleramt angeordnet wurden. Das heißt auch hier können Inhaltsdaten ausnahmsweise und streng zweckgebunden ohne den Einsatz von Suchbegriffen verwendet werden.

hhh) Kooperation im Rahmen der Ausland-Ausland-Fernmeldeaufklärung (§ 13 BNDG)

Der BND ist zur Erfüllung seines Auftrags nach § 1 Absatz 2 Satz 1 BNDG auf die Kooperation mit ausländischen Nachrichtendiensten angewiesen. Insbesondere auch infolge der deutschen Mitgliedschaft in der EU und der NATO hat die Bundesrepublik Deutschland eine Verantwortung, sicherheitspolitisch relevante Informationen insbesondere mit anderen EU-Partnern oder NATO-Mitgliedsstaaten zeitnah zu teilen. Nicht zuletzt aufgrund von beschränkten personellen und finanziellen Ressourcen ist ein Datenaustausch zur gemeinsamen Erkennung von Gefahren für die Bundesrepublik Deutschland von großer Bedeutung. Dies gilt insbesondere auch im Bereich der Ausland-Ausland-Fernmeldeaufklärung. Die immer stärkere Vernetzung der Welt mit dem dieser Entwicklung innewohnenden stark steigenden Kommunikationsaufkommen stellt die Fernmeldeaufklärung vor erhebliche Herausforderungen. Angesichts vielfältiger, komplexer Bedrohungen und knapper Ressourcen bietet eine Arbeitsteilung und Zusammenarbeit mit anderen Nachrichtendiensten erhebliche Vorteile für beide Seiten. Kooperationen mit ausländischen Nachrichtendiensten im Sinne eines „Burden-Sharing“ sind daher unabdingbar. § 13 BNDG-E trifft für die Kooperation auf dem Gebiet der Ausland-Ausland-Fernmeldeaufklärung mit ausländischen öffentlichen Stellen spezielle Regelungen und geht insoweit den §§ 6 ff. BNDG-E vor. Diese Kooperationen sind nur unter den normierten Voraussetzungen statthaft. Eine Umgehung dieser Vorschriften (sogenannter Ringtausch) ist unzulässig.

§ 13 Kooperation im Rahmen der Ausland-Ausland-Fernmeldeaufklärung
(1) Soweit der Bundesnachrichtendienst im Rahmen der Ausland-Ausland-Fernmeldeaufklärung (§ 6) mit ausländischen öffentlichen Stellen, die nachrichtendienstliche Aufgaben wahrnehmen (ausländische öffentliche Stellen) kooperiert, dürfen dabei auch Informationen einschließlich personenbezogener Daten nach § 14 erhoben und nach § 15 ausgetauscht werden.

Der BND darf Daten erheben und mit ausländischen öffentlichen Stellen, die mit nachrichtendienstlichen Aufgaben betraut sind, austauschen, um seine Aufgaben auf dem Gebiet der Ausland-Ausland-Fernmeldeaufklärung zu erfüllen. Ein Austausch ist auch dann gegeben, wenn eine Gegenseitigkeit der Leistungen in anderer Form sichergestellt wird.

(2) Eine Kooperation nach Absatz 1 mit einer ausländischen öffentlichen Stelle ist zulässig, wenn
1. sie den Zielen des § 6 Absatz 1 Satz 1 Nummer 1 bis 3 dient und
2. die Aufgabenerfüllung durch den Bundesnachrichtendienst ohne eine solche Kooperation wesentlich erschwert oder unmöglich wäre.

Absatz 2 regelt, unter welchen Voraussetzungen Kooperationen auf dem Gebiet der Ausland-Ausland-Fernmeldeaufklärung im Sinne des § 6 BNDG-E zulässig sind. Demnach müssen Kooperationen den in § 6 Absatz 1 Nummer 1 bis 3 BNDG-E

genannten Zielen dienen und die mit der Kooperation angestrebte Aufgabenerfüllung muss für den BND ohne eine solche Kooperation wesentlich erschwert oder unmöglich sein.

(3) Einzelheiten der Kooperation sind vor ihrem Beginn zwischen dem Bundesnachrichtendienst und der ausländischen öffentlichen Stelle in einer Absichtserklärung schriftlich niederzulegen. In die Absichtserklärung sind insbesondere aufzunehmen:
1. Kooperationsziele,
2. Kooperationsinhalte,
3. Kooperationsdauer,
4. eine Absprache, dass die im Rahmen der Kooperation erhobenen Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie erhoben wurden, und die Verwendung mit grundlegenden rechtstaatlichen Prinzipien vereinbar sein muss,
5. eine Absprache, nach der sich die ausländische öffentliche Stelle bereit erklärt, auf Ersuchen des Bundesnachrichtendienstes Auskunft über die vorgenommene Verwendung der Daten zu erteilen, sowie
6. eine Zusicherung der ausländischen öffentlichen Stelle, einer Löschungsaufforderung des Bundesnachrichtendienstes Folge zu leisten.

Die Art und Weise der Durchführung einer solchen Kooperation mit ausländischen öffentlichen Stellen ist vorab detailliert niederzulegen. Die Absichtserklärung muss schriftlich erfolgen und u.a. Kooperationsziele und -inhalte bezeichnen. Darüber hinaus muss sie die Bereitschaft der Kooperationspartner enthalten, die Daten nur zu dem festgelegten Zweck zu verwenden und sie auf Aufforderung des BND zu löschen, sollte der BND im Nachhinein feststellen, dass die Übermittlung unzulässig war. Der BND muss sich zudem das Recht vorbehalten, um Auskunft über die tatsächliche Verwendung der Daten zu bitten, um die Einhaltung der Kooperationsziele überprüfen zu können.

(4) Die Kooperationsziele und -inhalte müssen gerichtet sein auf die Gewinnung von Informationen
1. zur Erkennung und Begegnung von Gefahren durch den internationalen Terrorismus,
2. zur Erkennung und Begegnung von Gefahren durch die illegale Verbreitung von Massenvernichtungs- und Kriegswaffen,
3. zur Unterstützung der Bundeswehr und zum Schutz der Streitkräfte der an der Kooperation beteiligten Staaten,
4. zu krisenhaften Entwicklungen im Ausland,
5. über die Gefährdungs- und Sicherheitslage von deutschen Staatsangehörigen sowie von Staatsangehörigen der an der Kooperation beteiligten Staaten im Ausland,
6. zu politischen, wirtschaftlichen oder militärischen Vorgängen im Ausland, die von außen- und sicherheitspolitischer Bedeutung sind oder
7. in vergleichbaren Fällen.

Die in der Absichtserklärung niederzulegenden Ziele und Inhalte der Kooperation müssen auf die Gewinnung bestimmter Informationen gerichtet sein, diese werden in Absatz 4 genannt.

(5) Die Absichtserklärung bedarf der Zustimmung des Bundeskanzleramtes, wenn die Kooperation mit ausländischen öffentlichen Stellen von Mitgliedstaaten der Europäischen Union, des Europäischen Wirtschaftsraumes oder des Nordatlantikvertrages erfolgt; im Übrigen bedarf sie der Zustimmung der Chefin oder des Chefs des Bundeskanzleramtes. Das Parlamentarische Kontrollgremium ist über die Absichtserklärung zu unterrichten.

Die Absichtserklärung über eine Kooperation mit Mitgliedsstaaten der EU, des Europäischen Wirtschaftsraumes oder der NATO bedarf der der Zustimmung des Bundeskanzleramtes. Für Kooperationen mit sonstigen Staaten bedarf die Absichtserklärung als zusätzliche formale Hürde der Zustimmung der Chefin oder des Chefs des Bundeskanzleramtes. Das Parlamentarische Kontrollgremium wird über den Abschluss einer Absichtserklärung unterrichtet.

Exkurs: NSA-Selektoren vor dem Untersuchungsausschuss im Deutschen Bundestag, 18. Wahlperiode

Es wird verwiesen auf
Graulich, Nachrichtendienstliche Fernmeldeaufklärung mit Selektoren in einer transnationalen Kooperation. Prüfung und Bewertung von NSA-Selektoren nach Maßgabe des Beweisbeschlusses BND-26, Bericht im Rahmen des 1. Untersuchungsausschusses des 18. Deutschen Bundestags; abrufbar unter: http://www.bundestag.de/blob/393598/b5d50731152a09ae36b42be50f283898/mat_a_sv-11-2-data.pdf.

iii) Erhebung von Informationen einschließlich personenbezogener Daten im Rahmen einer Kooperation (§ 14 BNDG)

§ 14 Erhebung von Informationen einschließlich personenbezogener Daten im Rahmen einer Kooperation

Während § 13 BNDG-E die Voraussetzungen der Kooperationen im Rahmen der Ausland-Ausland-Fernmeldeaufklärung als solche regelt, werden in § 14 die Voraussetzungen der Erhebung von Informationen im Rahmen einer Kooperation festgelegt.

(1) Die Erhebung von Informationen einschließlich personenbezogener Daten im Rahmen einer Kooperation nach § 13 durch den Bundesnachrichtendienst ist zulässig,
1. um die vereinbarten Kooperationsziele zu erreichen,
2. wenn bei der Erhebung von Inhaltsdaten nur solche Suchbegriffe verwendet werden, die zur Erreichung der vereinbarten Kooperationsziele geeignet sind.

Die Erhebung der Informationen einschließlich personenbezogener Daten und die Verwendung der Suchbegriffe müssen zudem in Einklang mit den außen- und sicherheitspolitischen Interessen der Bundesrepublik Deutschland stehen.

Die Informationen sind zur Erreichung der schriftlich niedergelegten Kooperationsziele zu erheben. Weiterhin dürfen bei der Erhebung von Inhaltsdaten nur solche Suchbegriffe verwendet werden, die zur Erreichung der in der schriftlich niedergelegten Kooperationsziele und -inhalte geeignet sind. Zudem muss die Erhebung der jeweiligen Information in Einklang mit den außen- und sicherheitspolitischen Interessen der Bundesrepublik Deutschland stehen. Hierbei ist zu berücksichtigen, dass die Geeignetheit eines Suchbegriffs im Rahmen der Kooperation auch dann gegeben sein kann, wenn nur einer der Kooperationspartner den Suchbegriff benennt.

(2) Im Übrigen gelten § 6 Absatz 1 Satz 2, Absatz 3 bis 7 sowie die §§ 8 bis 12 entsprechend.

Absatz 2 verweist auf die entsprechend geltenden Vorschriften. Die für die Kooperation zu nutzenden Telekommunikationsnetze müssen durch das Bundeskanzleramt angeordnet werden. Die Vorgaben für das Anordnungsverfahren gelten entsprechend. Darüber hinaus gilt auch der besondere Schutz von Einrichtungen der Europäischen Union, öffentliche Stellen ihrer Mitgliedsstaaten und Unionsbürgerinnen und Unionsbürger. Deutsche Staatsangehörige, inländische juristische Personen oder sich im Bundesgebiet aufhaltende Personen werden umfassend geschützt. U.a. müssen technische Vorkehrungen getroffen werden, dass es bei Kooperationen zu keinen Eingriffen in Artikel 10 GG kommt. Wirtschaftsspionage ist auch im Rahmen von Kooperationen unzulässig. Vorabfassung

(3) Die Ausland-Ausland-Fernmeldeaufklärung darf im Rahmen einer Kooperation nach § 13 nur durch den Bundesnachrichtendienst selbst erfolgen.

Absatz 3 stellt klar, dass die Datenerfassung nur durch den BND und nicht durch den jeweiligen Kooperationspartner erfolgt. Damit wird ausgeschlossen, dass der Kooperationspartner vom deutschen Territorium aus Fernmeldeaufklärung durchführt.

jjj) Automatisierte Datenübermittlung; Speicherung; Prüfung (§ 15 BNDG)

§ 15 Automatisierte Datenübermittlung; Speicherung; Prüfung

(1) Die im Rahmen der Kooperation erhobenen Informationen einschließlich personenbezogener Daten dürfen der ausländischen öffentlichen Stelle automatisiert übermittelt werden, wenn
1. vorab durch eine automatisierte Prüfung erkannte
a) Daten nach § 10 Absatz 3 und 4 oder
b) Daten, deren Übermittlung nationalen Interessen der Bundesrepublik Deutschland entgegenstehen würden,

gelöscht wurden und
2. die sofortige Übermittlung erforderlich ist, um die Kooperationsziele zu erreichen.

Die im Rahmen der Kooperation erhobenen Daten können dem Kooperationspartner auch automatisiert zur Verfügung gestellt werden. In Absatz 1 wird für Kooperationen eine ergänzende Übermittlungsmöglichkeit geregelt. Das Artikel 10Gesetz bleibt auch bei Kooperationen unberührt, die erhobenen Daten sind daher vor Weiterleitung automatisiert in einem mehrstufigen Verfahren zu prüfen, um u.a. nach G10 geschützte Daten zu erkennen. Auch gezielt gesteuerte Verkehre von Unionsbürgerinnen und Unionsbürgern, Einrichtungen der EU und öffentlichen Stellen ihrer Mitgliedstaaten sowie Daten, deren Übermittlung nationalen Interessen Deutschlands entgegenstehen würde, sind automatisiert auszufiltern. Weiterhin muss die sofortige Übermittlung erforderlich sein, um die vereinbarten Kooperationsziele zu erreichen.

(2) Die Übermittlung der Daten ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung der Datenschutzkontrolle verwendet werden. Die Protokolldaten sind bis zum Ablauf des zweiten auf die Protokollierung folgenden Kalenderjahres aufzubewahren und danach unverzüglich zu löschen.

Die Übermittlung der Daten ist zu protokollieren. Die Protokollierung dient der datenschutzrechtlichen Kontrolle.

(3) Die Einhaltung der Vorgaben nach Absatz 1 und § 11 wird stichprobenartig überprüft. Die Prüfung erfolgt unter Aufsicht einer Bediensteten oder eines Bediensteten des Bundesnachrichtendienstes, die oder der die Befähigung zum Richteramt hat. Sofern nachträglich erkannt wird, dass Daten entgegen dieser Vorgaben erhoben und an die ausländische öffentliche Stelle weitergegeben wurden, wird die ausländische öffentliche Stelle zur Löschung der Daten aufgefordert. Der Bundesnachrichtendienst unterrichtet das Bundeskanzleramt in Abständen von höchstens sechs Monaten über die Durchführung der Prüfung nach Satz 1. Einzelheiten sind in einer Dienstvorschrift zu regeln, die der Zustimmung des Bundeskanzleramtes bedarf. Das Bundeskanzleramt unterrichtet das Parlamentarische Kontrollgremium. Das Unabhängige Gremium darf die Einhaltung der Vorgaben nach Absatz 1 und § 11 jederzeit stichprobenartig kontrollieren.

Der BND ist gehalten, die erhobenen und automatisiert weitergegebenen Daten stichprobenartig zu sichten, um erkennen zu können, ob dem Kooperationspartner ungeachtet der vorgenannten mehrstufigen Prüfung unbeabsichtigt Daten von Einrichtungen der Europäischen Union, von öffentlichen Stellen ihrer Mitgliedsstaaten oder Unionsbürger sowie nach G10 geschützte Daten und kernbereichsrelevante Daten automatisiert zur Verfügung gestellt wurden. Sofern dies der Fall sein sollte, wäre der BND verpflichtet, die ausländische öffentliche Stelle zur Löschung dieser Daten aufzufordern. Diese muss sich vorab in der Absichtserklärung nach § 13 BNDG-E bereit erklärt haben, der Löschaufforderung umgehend nachzukommen.

(4) Die im Rahmen der Kooperation auf Grundlage der von der ausländischen öffentlichen Stelle benannten Suchbegriffe erhobenen Daten werden durch den

Bundesnachrichtendienst für die Dauer von zwei Wochen gespeichert. Die §§ 19 und 20 bleiben im Übrigen unberührt.

Die auf Grundlage von Suchbegriffen des Kooperationspartners erhobenen Daten werden für höchstens zwei Wochen gespeichert. Während dieser zweiwöchigen Speicherung hat die stichprobenartige Prüfung der Daten nach Absatz 3 zu erfolgen. Darüber hinaus ist die Speicherung auch aus technischen Gründen erforderlich. Gibt es beispielsweise bei der Übermittlung technische Schwierigkeiten, könnten die Daten erneut übermittelt werden. Eine längere Speicherfrist gilt, wenn die Erforderlichkeit der weiteren Speicherung, Nutzung oder Veränderung nach § 19 Absatz 1 BNDG-E (bislang § 4 Absatz 1 BNDG) festgestellt wurde. Bei Daten, die aufgrund von Suchbegriffen des BND erhoben wurden, gelten die §§ 19 und 20 BNDG-E (bislang §§ 4 und 5 BNDG). Die Einzelheiten der stichprobenartigen Prüfung sind in der Dienstvorschrift zu regeln.

kkk) Unabhängiges Gremium (§ 16 BNDG)

§ 16 Unabhängiges Gremium

Für die Kontrolle von Maßnahmen der Ausland-Ausland-Fernmeldeaufklärung sowie auch die in § 9 Absatz 4 BNDG-E vorgesehene Vorab-Zustimmung zu den Maßnahmen der Ausland-Ausland-Fernmeldeaufklärung ist das Unabhängige Gremium zuständig.

(1) Das Unabhängige Gremium besteht aus
1. einer Vorsitzenden oder einem Vorsitzenden,
2. zwei Beisitzerinnen oder Beisitzern sowie
3. drei stellvertretenden Mitgliedern.
Die Mitglieder des Unabhängigen Gremiums sowie die stellvertretenden Mitglieder des Unabhängigen Gremiums sind in ihrer Amtsführung unabhängig und Weisungen nicht unterworfen. Vorsitzende oder Vorsitzender und eine Beisitzerin oder ein Beisitzer sind Richterinnen am Bundesgerichtshof oder Richter am Bundesgerichtshof, die weitere Beisitzerin oder der weitere Beisitzer ist eine Bundesanwältin beim Bundesgerichtshof oder ein Bundesanwalt beim Bundesgerichtshof. Zwei stellvertretende Mitglieder sind Richterinnen am Bundesgerichtshof oder Richter am Bundesgerichtshof, ein stellvertretendes Mitglied ist eine Bundesanwältin beim Bundesgerichtshof oder ein Bundesanwalt beim Bundesgerichtshof.

Das Unabhängige Gremium setzt sich zusammen aus 1. einer Vorsitzenden oder einem Vorsitzenden, 2. zwei Beisitzerinnen oder Beisitzern sowie 3. drei stellvertretenden Mitgliedern. Die Mitglieder des Unabhängigen Gremiums sowie die stellvertretenden Mitglieder des Unabhängigen Gremiums sind in ihrer Amtsführung unabhängig und Weisungen nicht unterworfen. Vorsitzende oder Vorsitzender und eine Beisitzerin oder ein Beisitzer sind Richterinnen am Bundesgerichtshof oder Richter am Bundesgerichtshof. Dabei soll es sich um Richterinnen und Richter mit Erfahrung in Strafsachen handeln. Die weitere Beisitzerin oder der weitere Beisitzer ist eine Bundesanwältin beim Bundesgerichtshof oder ein Bundesanwalt beim

Bundesgerichtshof. Zwei stellvertretende Mitglieder sind Richterinnen am Bundesgerichtshof und Richter am Bundesgerichtshof, ein stellvertretendes Mitglied ist eine Bundesanwältin beim Bundesgerichtshof oder ein Bundesanwalt beim Bundesgerichtshof.

(2) Das Bundeskabinett beruft für die Dauer von sechs Jahren
1. auf Vorschlag der Präsidentin oder des Präsidenten des Bundesgerichtshofs die Mitglieder des Unabhängigen Gremiums, die Richterinnen am Bundesgerichtshof oder Richter am Bundesgerichtshof sind, einschließlich deren Stellvertretung und
2. auf Vorschlag der Generalbundesanwältin oder des Generalbundesanwalts das Mitglied des Unabhängigen Gremiums, das Bundesanwältin beim Bundesgerichtshof oder Bundesanwalt beim Bundesgerichtshof ist, einschließlich dessen Stellvertretung.

Das Bundeskabinett beruft für die Dauer von sechs Jahren 1. auf Vorschlag der Präsidentin oder des Präsidenten des Bundesgerichtshofs: die Mitglieder des Unabhängigen Gremiums, die Richterinnen am Bundesgerichtshofs oder Richter am Bundesgerichtshofs sind, einschließlich deren Stellvertretung, und 2. auf Vorschlag der Generalbundesanwältin oder des Generalbundesanwalts: das Mitglied des Unabhängigen Gremiums, das Bundesanwältin beim Bundesgerichtshof oder Bundesanwalt beim Bundesgerichtshof ist, einschließlich dessen Stellvertretung. Aufgrund des Vorschlagsrechts der Präsidentin oder des Präsidenten des Bundesgerichtshofs bzw. der Generalbundesanwältin oder des Generalbundesanwalts ist eine hinreichende Unabhängigkeit im Rahmen des Besetzungsverfahrens sichergestellt.

(3) Dem Unabhängigen Gremium ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen. Die Geschäftsstelle wird beim Bundesgerichtshof eingerichtet.

Dem Unabhängigen Gremium ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen. Die Geschäftsstelle wird beim Bundesgerichtshof eingerichtet.

(4) Das Unabhängige Gremium tritt mindestens alle drei Monate zusammen. Es gibt sich eine Geschäftsordnung. Das Unabhängige Gremium entscheidet mit der Mehrheit der Stimmen. Ist eines oder sind mehrere der Mitglieder verhindert, nimmt die jeweilige Stellvertreterin oder der jeweilige Stellvertreter an der Sitzung teil.

Das Unabhängige Gremium tritt mindestens alle drei Monate zusammen. Beschlussfähig ist das Unabhängige Gremium, wenn drei Mitglieder anwesend sind. Das Unabhängige Gremium entscheidet mit der Mehrheit der Stimmen. Ist eines oder sind mehrere der Mitglieder verhindert, nehmen die jeweiligen Stellvertreterinnen und Stellvertreter an der Sitzung teil. Das Unabhängige Gremium gibt sich eine Geschäftsordnung.

(5) Die Beratungen des Unabhängigen Gremiums sind geheim. Die Mitglieder sowie die stellvertretenden Mitglieder des Unabhängigen Gremiums sowie die Mitarbeiterinnen und Mitarbeiter der Geschäftsstelle sind zur Geheimhaltung der

Angelegenheiten verpflichtet, die ihnen bei oder bei Gelegenheit ihrer Tätigkeit in dem Gremium bekannt geworden sind. Dies gilt auch für die Zeit nach ihrem Ausscheiden aus dem Unabhängigen Gremium. Die Mitarbeiterinnen und Mitarbeiter der Geschäftsstelle haben sich einer erweiterten Sicherheitsüberprüfung mit Sicherheitsermittlungen (§ 7 Absatz 1 Nummer 3 des Sicherheitsüberprüfungsgesetzes) unterziehen zu lassen.

Die Beratungen des Unabhängigen Gremiums sind geheim. Die Mitglieder und die stellvertretenden Mitglieder des Unabhängigen Gremiums sowie die Mitarbeiterinnen und Mitarbeiter der Geschäftsstelle sind zur Geheimhaltung der Angelegenheiten verpflichtet, die ihnen bei oder bei Gelegenheit ihrer Tätigkeit in dem Gremium bekannt geworden sind. Dies gilt auch für die Zeit nach ihrem Ausscheiden aus dem Unabhängigen Gremium. Zur Sicherung der Geheimschutzbelange ist für Mitarbeiterinnen und Mitarbeiter der Geschäftsstelle eine erweiterte Sicherheitsüberprüfung vorgesehen.

(6) Das Unabhängige Gremium unterrichtet in Abständen von höchstens sechs Monaten das Parlamentarische Kontrollgremium über seine Tätigkeit.

Das Unabhängige Gremium berichtet mindestens einmal im halben Jahr in abstrakter Form dem Parlamentarischen Kontrollgremium über seine Tätigkeit. Die Belange des Geheimschutzes sind zu wahren.

lll) Mitteilungsverbote (§ 17 BNDG)

§ 17 Mitteilungsverbote
(1) Personen, die Telekommunikationsdienste erbringen oder die an der Erbringung solcher Dienste mitwirken, dürfen anderen nichts über Maßnahmen nach § 6 Absatz 1 auch in Verbindung mit § 12 Absatz 2 Satz 4 mitteilen.

(2) Erfolgt ein Auskunftsersuchen oder eine Auskunftserteilung nach § 8 Absatz 1 Satz 1 auch in Verbindung mit § 12 Absatz 2 Satz 4, so darf diese Tatsache oder der Inhalt des Ersuchens oder der erteilten Auskunft von Personen, die zur Beantwortung verpflichtet oder mit der Beantwortung betraut sind oder die hieran mitwirken, anderen nicht mitgeteilt werden.

Mit § 17 werden die für die Anbieter von Telekommunikationsdiensten geltenden Mitteilungsverbote geregelt. Diese Regelung entspricht derjenigen im Artikel 10-Gesetz.

mmm) Entschädigung (§ 18 BNDG)

§ 18 Entschädigung
Der Bundesnachrichtendienst vereinbart mit den nach § 8 Absatz 1 Satz 1 oder § 12 Absatz 2 Satz 4 verpflichteten Unternehmen für die dort genannten Leistungen eine Entschädigung, deren Höhe sich an den nachgewiesenen tatsächlichen Kosten orientiert.

Die Vorschrift regelt die Entschädigung der in Anspruch genommenen Anbieter von Telekommunikationsdiensten. Die Kosten werden nicht pauschal erstattet, sondern die tatsächlich entstandenen Kosten müssen durch die Verpflichteten nachgewiesen werden und werden sodann ersetzt.

Gesetzgebung, Literatur und Rechtsprechung

1. Gesetze und Materialien:

Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BT-Drs. 18/9041)

Entwurf eines Gesetzes zur weiteren Fortentwicklung der parlamentarischen Kontrolle der Nachrichtendienste des Bundes (BT-Drs. 18/9040)

Gesetz zur Änderung des Strafgesetzbuchs, der Strafprozeßordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz) vom 28. Oktober 1994 (BGBl I S. 3186)

Entwurf der Fraktionen der CDU/CSU und F.D.P. eines Gesetzes zur Änderung des Strafgesetzbuches, der Strafprozeßordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz) (BT-Drs. 12/6853)

Entwurf der Bundesregierung vom 13. Juni 1967 eines Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zur Artikel 10 Grundgesetz) (G 10) (BT-Drs. V/1880)

Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses vom 13.08.1968 – G 10 – (BGBl. I 1968 S. 949)

Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Hans-Christian Ströbele, Dr. Konstantin von Notz, Volker Beck (Köln), weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 17/14302 – Überwachung der Internet- und Telekommunikation durch Geheimdienste der USA, Großbritanniens und in Deutschland (BT-Drs. 17/14739)

2. Rechtsprechung

Europäischer Gerichtshof für Menschenrechte, Entscheidung vom 29. Juni 2006 – 54934/00 – NJW 2007 1433 - Individualbeschwerde: Strategische Überwachung sowie die Verwertung der dabei erlangten personenbezogenen Daten nach dem Verbrechensbekämpfungsgesetz

BVerfG, Urteil vom 20.04.2016 - 1 BvR 966/09, 1 BvR 1140/09 - Vorschriften des Bundeskriminalamtsgesetzes über Befugnisse im Rahmen der Abwehr von Gefahren des internationalen Terrorismus teilweise verfassungswidrig – Fortgeltung längstens bis 30.06.2018 - Anforderungen des Verhältnismäßigkeitsgrundsatzes an heimliche Überwachung und Datenerhebung - Grundsatz der Zweckbindung und Grenzen der Zweckänderung (Grundsatz der hypothetischen Datenneuerhebung) - Maßgaben für Datenübermittlung an ausländische Stellen

BVerfG, Ablehnung einstweilige Anordnung vom 28. Oktober 2008 – 1 BvR 256/08 –, BVerfGE 122, 120-151 - Teilweise Stattgabe eines erweiterten Antrags auf Erlass einer eA in Sachen Vorratsdatenspeicherung von Telekommunikations-Verkehrsdaten: hinsichtlich der Speicherungspflicht des § 113a TKG 2004 und der Nutzung der gespeicherten Daten Verlängerung der eA vom 11.03.2008 in unverändertem Umfang - Erweiterung der eA vom 11.03.2008 hinsichtlich der Übermittlung der gespeicherten Daten zur Gefahrenabwehr und zu Zwecken des Verfassungsschutzes dahingehend, dass eine Übermittlung nur unter einschränkenden Bedingungen an die ersuchende Behörde zulässig ist

BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07 –, BVerfGE 120, 274-350 - Online-Durchsuchung

BVerfG, Beschluss vom 04. April 2006 – 1 BvR 518/02 –, BVerfGE 115, 320-381 – Präventive polizeiliche Rasterfahndung nur bei hinreichend konkreter Gefahr für hochrangige Rechtsgüter mit dem informationellen Selbstbestimmungsrecht vereinbar, nicht jedoch im Vorfeld der Gefahrenabwehr - hier: ausweitende Auslegung des Begriffs der gegenwärtigen Gefahr in PolG NW 1990 § 31 Abs 1 mit GG Art 2 Abs 1 iVm Art 1 Abs 1 unvereinbar - abweichende Meinung: Rechtfertigung der vorliegenden Rasterfahndung angesichts terroristischer Bedrohungslage

BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95 –, BVerfGE 100, 313-403 - Befugnisse des BND zur Überwachung, Aufzeichnung und Auswertung des Telekommunikationsverkehrs sowie zur Übermittlung der daraus erlangten Daten an andere Behörden nicht in vollem Umfang mit dem Schutz des Fernmeldegeheimnisses und teilweise der Rechtsschutzgarantie sowie der Pressefreiheit vereinbar: Schutzumfang des Fernmeldegeheimnisses – Anforderungen des Verhältnismäßigkeitsgrundsatzes bei Grundrechtsbeschränkungen zum Schutz hochrangiger Gemeinschaftsgüter – Verpflichtung des Gesetzgebers zur Herstellung eines verfassungsmäßigen Zustandes

BVerfG, Beschluss vom 20. Juni 1984 – 1 BvR 1494/78 –, BVerfGE 67, 157-185 - Zur Frage der Verfassungsmäßigkeit der vom Bundesminister der Verteidigung angeordneten Maßnahmen zur Überwachung des Briefverkehrs und Telefonverkehrs von und nach Ländern des Warschauer Paktes

BVerfG, Entscheidung vom 15. Dezember 1970 – 2 BvF 1/69, 2 BvR 629/68, 2 BvR 308/69 –, BVerfGE 30, 1 – Abhör-Urteil

BVerwG, Urteil vom 23. Januar 2008 – 6 A 1/07 –, BVerwGE 130, 180-197 - Strategische Telefonüberwachung - internationaler Terrorismus - Mitteilungszeitpunkt

3. Literatur:

Arndt, Claus in Verfassungsschutz und Rechtsstaat, 1981, S. 43 (51)

Bäcker, Das G 10 und die Kompetenzordnung, in DÖV 2011, 840-848

Deiseroth, NSA-Ausspähungen und der demokratische Verfassungsstaat, in Vorgänge, 206/207 (2014) S. 50-65

Deiseroth, Alles legal? – Zu den rechtlichen Befugnissen und Grenzen der US-Nachrichtendienste in Deutschland, in DVBl. 2015, 197

Graulich, Reform des Gesetzes über den Bundesnachrichtendienst Ausland-Ausland-Fernmeldeaufklärung und internationale Datenkooperation, in KriPoZ 2017, 43

Graulich, Gutachtliche Stellungnahme zum Entwurf der Fraktionen der CDU/CSU und SPD eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BT-Drs.18/9041) (Deutscher Bundestag Innenausschuss, Ausschussdrucksach 18(4)653 B vom 19. September 2016

Graulich/Kutscha/Will, Massenüberwachung oder automatisches Filtern? Ein Streitgespräch zur Überwachungspraxis des BND, in Vorgänge, 206/207 (2014) S. 22-30

Graulich, Nachrichtendienstliche Fernmeldeaufklärung mit Selektoren in einer transnationalen Kooperation. Prüfung und Bewertung von NSA-Selektoren nach Maßgabe des Beweisbeschlusses BND-26, Bericht im Rahmen des 1. Untersuchungsausschusses des 18. Deutschen Bundestags; abrufbar unter: http://www.bundestag.de/blob/393598/b5d50731152a09ae36b42be50f283898/mat_a_sv-11-2-data.pdf.

Graulich, Polizeiliche Gefahrenabwehr mit heimlichen Überwachungsmaßnahmen Anm. zu BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09 – zum BKAG

Gusy in Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, BNDG

Huber in Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, Artikel 10-Gesetz

Huber, Die Fernmeldeaufklärung des Bundesnachrichtendienstes – Rechtsgrundlagen und bestehende Regelungsdefizite, in Vorgänge, 206/207 (2014) S. 42-49

Huber, Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, in NJW 2013, 2572-2577

Löffelmann, REGELUNG DER AUSLAND-AUSLAND-FERNMELDEAUFKLÄRUNG, in Recht+Politik, Ausgabe 8/2016 S. 1 ff.

Lüders, Deutsche Rechtspositionen zur Überwachungsaffäre, in Vorgänge, 206/207 (2014) S. 7-21

Roggan, G-10-Gesetz, 1. Auflage 2012

Schwan, Das Abhörurteil des Europäischen Gerichtshofes für Menschenrechte, in NJW 1980, 1992-1998

Weigelt, Die Auswirkung der Bekämpfung des internationalen Terrorismus auf die staatliche Souveränität, Berlin 2016

Will, Zur Bedeutung des nationalen Schutzregimes für transnationale Kooperationen des BND. Fragen an Kurt Graulich, den unabhängigen Sachverständigen zur Begutachtung der NSA-Selektorenliste. In: vorgänge Nr. 213 (Heft 1/2016), S. 140-152