Sicherheitsrecht des Bundes – Recht der Nachrichtendienste in Deutschland

von

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

Humboldt-Universität zu Berlin – Sommersemester 2019
Raum UL9 E 25
Donnerstag, d. 06.06.2019 von 13.00 bis 15.00 Uhr
Schwerpunkte 2 und 5
Veranstaltungsnummer 10727

Skizze und Materialien

Gliederung:

b) Organisation und Aufgaben
aa) Stellung des BND im Behördenaufbau (§ 1 Abs. 1 Satz 1 BNDG)
bb) Organisatorisches Trennungsgebot (§ 1 Abs. 1 Satz 2 BNDG)
cc) Aufgabe der Auslandsaufklärung (§ 1 Abs. 2 BNDG)
dd) Aufgaben und Befugnisse
c) Allgemeine Befugnisse
aa) Generalermächtigung (§ 2 BNDG)
aaa) Generalbefugnis für Eingriffe in personenbezogene Daten (§ 2 Abs. 1 BNDG)
a1) Eigensicherung (Nr. 1)
b1) Sicherheitsüberprüfung von Personen (Nr. 2)
c1) Überprüfung von Nachrichtenzugängen (Nr. 3)
d1) Vorgänge im Ausland (Nr. 4)
bbb) Umgang mit einverständlich erhobenen Daten (§ 2 Abs. 2 BNDG)
ccc) Materielles Trennungsgebot (§ 2 Abs. 3 BNDG)
ddd) Verhältnismäßigkeitsgrundsatz (§ 2 Abs. 4 BNDG)
bb) Besondere Auskunftsverlangen nach § 3 BNDG i.V.m. §§ 8a und 8b BVerfSchG
cc) Weitere Auskunftsverlangen nach § 4 BNDG i.V.m. § 8d BVerfSchG (Bestandsdatenauskunft)
dd) Besondere Formen der Datenerhebung nach § 5 BNDG i.V.m. §§ 8 Abs. 2, 9, 9a und 9b BVerfSchG
d) Fernmeldeaufklärung
aa) Fernmeldeaufklärung nach dem G10
aaa) Gegenstand des G10
bbb) Individualmaßnahmen nach dem § 3 G10

Einzelheiten:

b) Organisation und Aufgaben

§ 1 Organisation und Aufgaben
(1) Der Bundesnachrichtendienst ist eine Bundesoberbehörde im Geschäftsbereich des Bundeskanzleramtes. Einer polizeilichen Dienststelle darf er nicht angegliedert werden.

aa) Stellung des BND im Behördenaufbau (§ 1 Abs. 1 Satz 1 BNDG)

bb) Organisatorisches Trennungsgebot (§ 1 Abs. 1 Satz 2 BNDG)

cc) Aufgabe der Auslandsaufklärung (§ 1 Abs. 2 BNDG)

(2) Der Bundesnachrichtendienst sammelt zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen und wertet sie aus. Werden dafür im Geltungsbereich dieses Gesetzes Informationen einschließlich personenbezogener Daten erhoben, so richtet sich ihre Erhebung, Verarbeitung und Nutzung nach den §§ 2 bis 15, 19 bis 21 sowie 23 bis 32.

dd) Aufgaben und Befugnisse

c) Allgemeine Befugnisse

aa) Generalermächtigung (§ 2 BNDG)

aaa) Generalbefugnis für Eingriffe in personenbezogene Daten (§ 2 Abs. 1 BNDG)

§ 2 Befugnisse
(1) Der Bundesnachrichtendienst darf die erforderlichen Informationen einschließlich personenbezogener Daten erheben, verarbeiten und nutzen, soweit nicht die anzuwendenden Bestimmungen des Bundesdatenschutzgesetzes oder besondere Regelungen in diesem Gesetz entgegenstehen,
1. zum Schutz seiner Mitarbeiter, Einrichtungen, Gegenstände und Quellen gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten,
2. für die Sicherheitsüberprüfung von Personen, die für ihn tätig sind oder tätig werden sollen,
3. für die Überprüfung der für die Aufgabenerfüllung notwendigen Nachrichtenzugänge und
4. über Vorgänge im Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, wenn sie nur auf diese Weise zu erlangen sind und für ihre Erhebung keine andere Behörde zuständig ist.

a1) Eigensicherung (Nr. 1)

b1) Sicherheitsüberprüfung von Personen (Nr. 2)

c1) Überprüfung von Nachrichtenzugängen (Nr. 3)

d1) Vorgänge im Ausland (Nr. 4)

bbb) Umgang mit einverständlich erhobenen Daten (§ 2 Abs. 2 BNDG)

(2) Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist der Erhebungszweck anzugeben. Der Betroffene ist auf die Freiwilligkeit seiner Angaben und bei einer Sicherheitsüberprüfung nach Absatz 1 Nr. 2 auf eine dienst- und arbeitsrechtliche oder sonstige vertragliche Mitwirkungspflicht hinzuweisen. Bei Sicherheitsüberprüfungen ist das Sicherheitsüberprüfungsgesetz vom 20. April 1994 (BGBl. I S. 867) anzuwenden.

ccc) Materielles Trennungsgebot (§ 2 Abs. 3 BNDG)

(3) Polizeiliche Befugnisse oder Weisungsbefugnisse stehen dem Bundesnachrichtendienst nicht zu. Er darf die Polizei auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen, zu denen er selbst nicht befugt ist.

ddd) Verhältnismäßigkeitsgrundsatz (§ 2 Abs. 4 BNDG)

(4) Von mehreren geeigneten Maßnahmen hat der Bundesnachrichtendienst diejenige zu wählen, die den Betroffenen voraussichtlich am wenigsten beeinträchtigt. Eine Maßnahme darf keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht.

bb) Besondere Auskunftsverlangen nach § 3 BNDG i.V.m. §§ 8a und 8b BVerfSchG

§ 3 Besondere Auskunftsverlangen
(1) Der Bundesnachrichtendienst darf Auskünfte entsprechend den §§ 8a und 8b des Bundesverfassungsschutzgesetzes einholen, soweit dies im Einzelfall erforderlich ist
1. zur Erfüllung seiner Aufgaben nach § 1 Absatz 2 oder
2. zum Schutz seiner Mitarbeiter, Einrichtungen, Gegenstände oder Quellen gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten.
§ 8a Absatz 2 und 2a des Bundesverfassungsschutzgesetzes ist mit der Maßgabe anzuwenden, dass an die Stelle der schwerwiegenden Gefahren für die in § 3 Absatz 1 des Bundesverfassungsschutzgesetzes genannten Schutzgüter
1. im Falle des Satzes 1 Nummer 1 schwerwiegende Gefahren für die in § 5 Absatz 1 Satz 3 Nummer 1 bis 4 und 6 des Artikel 10-Gesetzes genannten Gefahrenbereiche und
2. im Falle des Satzes 1 Nummer 2 schwerwiegende Gefahren im Sinne des § 3 Absatz 1 Nummer 2 des Bundesverfassungsschutzgesetzes

treten. § 8b Absatz 1 bis 9 des Bundesverfassungsschutzgesetzes ist mit der Maßgabe anzuwenden, dass an die Stelle des Bundesministeriums des Innern das Bundeskanzleramt tritt.
(2) Anordnungen nach § 8a Absatz 2 und 2a des Bundesverfassungsschutzgesetzes dürfen sich nur gegen Personen richten, bei denen auf Grund tatsächlicher Anhaltspunkte davon auszugehen ist, dass sie an der Schaffung oder Aufrechterhaltung einer in Absatz 1 Satz 2 genannten Gefahr beteiligt sind, sowie gegen die in § 8a Absatz 3 Nummer 2 des Bundesverfassungsschutzgesetzes bezeichneten Personen.
(3) Das Grundrecht des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird insoweit eingeschränkt.

cc) Weitere Auskunftsverlangen nach § 4 BNDG i.V.m. § 8d BVerfSchG (Bestandsdatenauskunft)

§ 4 Weitere Auskunftsverlangen
Soweit dies zur Erfüllung der Aufgaben des Bundesnachrichtendienstes nach § 1 Absatz 2 erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten entsprechend § 8d des Bundesverfassungsschutzgesetzes verlangt werden. § 8b Absatz 1 Satz 2 ist mit der Maßgabe anzuwenden, dass an die Stelle des Bundesministeriums des Innern das Bundeskanzleramt tritt. Die Auskunftserteilung ist nach § 8d Absatz 5 des Bundesverfassungsschutzgesetzes zu entschädigen. Das Grundrecht des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird nach Maßgabe des § 8d Absatz 2 des Bundesverfassungsschutzgesetzes eingeschränkt.

dd) Besondere Formen der Datenerhebung nach § 5 BNDG i.V.m. §§ 8 Abs. 2, 9, 9a und 9b BVerfSchG

§ 5 Besondere Formen der Datenerhebung
Der Bundesnachrichtendienst darf zur heimlichen Beschaffung von Informationen einschließlich personenbezogener Daten die Mittel gemäß § 8 Abs. 2 des Bundesverfassungsschutzgesetzes anwenden, wenn Tatsachen die Annahme rechtfertigen, daß dies zur Erfüllung seiner Aufgaben erforderlich ist. Die §§ 9, 9a und 9b des Bundesverfassungsschutzgesetzes sind entsprechend anzuwenden.

§ 9 Abs. 1 Sätze 2 bis 4 BVerfSchG begründen jedoch eine besonders hohe Schwelle der Verhältnismäßigkeit: „Die Erhebung nach (§ 9 Abs. 1) Satz 1 ist unzulässig, wenn die Erforschung des Sachverhalts auf andere, den Betroffenen weniger beeinträchtigende Weise möglich ist; eine geringere Beeinträchtigung ist in der Regel anzunehmen, wenn die Information aus allgemein zugänglichen Quellen oder durch eine Auskunft nach § 18 Abs. 3 gewonnen werden kann. Die Anwendung eines Mittels gemäß § 8 Abs. 2 darf nicht erkennbar außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhaltes stehen. Die Maßnahme ist unverzüglich zu beenden, wenn ihr Zweck erreicht ist oder sich Anhaltspunkte dafür ergeben, daß er nicht oder nicht auf diese Weise erreicht werden kann.“

Durch das Gesetz zur Verbesserung der Zusammenarbeit Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl. I S. 1938) ist § 5 Satz 2 BND (damals § 3 BNDG) geändert worden durch die **erweiterte Bezugnahme auf §§ 9a, 9b BVerfSchG**. Die §§ 9a und 9b BVerfSchG regeln Einsatzvoraussetzungen und Rahmenbedingungen von **verdeckten Mitarbeitern und Vertrauensleuten**. Nach der Absicht des Gesetzgebers sollte die für das BfV in diesem Bereich angestrebte Rechtssicherheit soll auch für den Bundesnachrichtendienst (BND) gelten. Auch der BND betreibt im Rahmen seiner Aufgabenerfüllung nach § 1 Absatz 2 BNDG organisationsbezogene Aufklärung, wie sie Regelungsgegenstand der §§ 9a und 9b BVerfSchG ist, durch heimlich eingesetzte Personen. Die §§ 9a und 9b BVerfSchG sollen daher entsprechende Anwendung finden (BT-Dr. 18/4654 S. 36).

d) Fernmeldeaufklärung

aa) Fernmeldeaufklärung nach dem G10

aaa) Gegenstand des G10

§ 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).

bb) Maßnahmen nach dem G10

bbb) Befugnisse

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

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 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

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

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

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.

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).