Leitsätze

zum Urteil des Ersten Senats vom 19. Mai 2020

- 1 BvR 2835/17 -

1. **Die Bindung der deutschen Staatsgewalt an die Grundrechte nach Art. 1 Abs. 3 GG ist nicht auf das deutsche Staatsgebiet begrenzt.**

   Der Schutz der einzelnen Grundrechte kann sich im Inland und Ausland unterscheiden.

   Jedenfalls der Schutz des Art. 10 Abs. 1 und des Art. 5 Abs. 1 Satz 2 GG als Abwehrrechte gegenüber einer Telekommunikationsüberwachung erstreckt sich auch auf Ausländer im Ausland.

2. **Die derzeitigen Regelungen zur Ausland-Ausland-Telekommunikationsüberwachung, zur Übermittlung der hierdurch gewonnenen Erkenntnisse und zur Zusammenarbeit mit ausländischen Nachrichtendiensten verletzen das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG; der Gesetzgeber hat die Grundrechte bewusst als nicht betroffen erachtet, obwohl sie auch hier anwendbar sind. Sie genügen auch zentralen materiellen Anforderungen der Grundrechte nicht.**

3. **Art. 10 Abs. 1 GG schützt die Vertraulichkeit individueller Kommunikation als solche. Personen, die geltend machen, in ihren eigenen Grundrechten verletzt zu sein, sind nicht deshalb vom Grundrechtsschutz des Grundgesetzes ausgeschlossen, weil sie als Funktionsträger einer ausländischen juristischen Person handeln.**

4. **Die Regelung der Auslandsaufklärung fällt unter die auswärtigen Angelegenheiten im Sinne von Art. 73 Abs. 1 Nr. 1 GG. Dem Bundesnachrichtendienst kann auf dieser Kompetenzgrundlage über die Aufgabe einer außen- und sicherheitspolitischen Unterrichtung der Bundesregierung hinaus als eigene, nicht operativ wahrzunehmende Aufgabe die Früherkennung von aus dem Ausland drohenden Gefahren von internationaler Dimension übertragen werden. Es muss sich um Gefahren handeln, die sich ihrer Art und ihrem Gewicht nach auf die Stellung der Bundesrepublik in der Staatengemeinschaft auswirken können und gerade in diesem Sinne von außen- und sicherheitspolitischer Bedeutung sind.**

5. **Die strategische Auslandstelekommunikationsüberwachung ist mit Art. 10 Abs. 1 GG nicht grundsätzlich unvereinbar. Als anlasslose, im Wesentlichen nur final angeleitete und begrenzte Befugnis ist sie jedoch eine Ausnahmebefugnis, die auf die Auslandsaufklärung durch eine Behörde, welche selbst keine operativen Befugnisse hat, begrenzt bleiben muss und nur durch deren besonderes Aufgabenprofil gerechtfertigt ist.**

   Erforderlich sind danach insbesondere Maßgaben zur Aussonderung der Telekommunikationsdaten von Deutschen und Inländern, eine Begrenzung der zu erhebenden Daten, die Festlegung qualifizierter Überwachungszwecke, die Strukturierung der Überwachung auf der Grundlage eigens festgelegter Maßnahmen, besondere Anforderungen an gezielt personenbezogene Überwachungsmaßnahmen, Grenzen für die bevorratende Speicherung von Verkehrsdaten, Rahmenbestimmungen zur Datenauswertung, Vorkehrungen zum Schutz von Vertraulichkeitsbeziehungen, die Gewährleistung eines Kernbereichsschutzes und Löschungspflichten.

6. **Die Übermittlung personenbezogener Daten aus der strategischen Überwachung ist nur zum Schutz besonders gewichtiger Rechtsgüter zulässig und setzt eine konkretisierte Gefahrenlage oder einen hinreichend konkretisierten Tatverdacht voraus. Ausgenommen sind hiervon Berichte an die Bundesregierung, soweit diese ausschließlich der politischen Information und Vorbereitung von Regierungsentscheidungen dienen.**

   Die Übermittlung setzt eine förmliche Entscheidung des Bundesnachrichtendienstes voraus und bedarf der Protokollierung unter Nennung der einschlägigen Rechtsgrundlage. Vor der Übermittlung an ausländische Stellen ist eine Vergewisserung über den rechtsstaatlichen Umgang mit den Daten geboten; hierbei bedarf es einer auf die betroffene Person bezogenen Prüfung, wenn es Anhaltspunkte gibt, dass diese durch die Datenübermittlung spezifisch gefährdet werden kann.

7. **Regelungen zur Kooperation mit ausländischen Nachrichtendiensten genügen grundrechtlichen Anforderungen nur, wenn sie sicherstellen, dass die rechtsstaatlichen Grenzen durch den gegenseitigen Austausch nicht überspielt werden und die Verantwortung des Bundesnachrichtendienstes für die von ihm erhobenen und ausgewerteten Daten im Kern gewahrt bleibt.**

Will der Bundesnachrichtendienst von einem Partnerdienst bestimmte Suchbegriffe nutzen, um die Treffer ohne nähere inhaltliche Auswertung automatisiert an diesen zu übermitteln, erfordert dies eine sorgfältige Kontrolle dieser Suchbegriffe sowie der hieran anknüpfenden Trefferfälle. Die bei Auslandsübermittlungen geltenden Vergewisserungspflichten gelten entsprechend. Die gesamthafte Übermittlung von Verkehrsdaten an Partnerdienste setzt einen qualifizierten Aufklärungsbedarf im Hinblick auf eine spezifisch konkretisierte Gefahrenlage voraus. Für den Umgang der Partnerdienste mit den übermittelten Daten sind gehaltvolle Zusagen einzuholen.

8. **Die Befugnisse zur strategischen Überwachung, zur Übermittlung der mit ihr gewonnenen Erkenntnisse und zur diesbezüglichen Zusammenarbeit mit ausländischen Diensten sind mit den Anforderungen der Verhältnismäßigkeit nur vereinbar, wenn sie durch eine unabhängige objektivrechtliche Kontrolle flankiert sind. Sie ist als kontinuierliche Rechtskontrolle auszugestalten, die einen umfassenden Kontrollzugriff ermöglicht.**

   Hierfür ist einerseits eine mit abschließenden Entscheidungsbefugnissen verbundene gerichtsähnliche Kontrolle sicherzustellen, der die wesentlichen Verfahrensschritte der strategischen Überwachung unterliegen, sowie anderseits eine administrative Kontrolle, die eigeninitiativ stichprobenmäßig den gesamten Prozess der Überwachung auf seine Rechtmäßigkeit prüfen kann.

   Zu gewährleisten ist eine Kontrolle in institutioneller Eigenständigkeit. Hierzu gehören ein eigenes Budget, eine eigene Personalhoheit sowie Verfahrensautonomie. Die Kontrollorgane sind personell wie sächlich so auszustatten, dass sie ihre Aufgaben wirksam wahrnehmen können. Sie müssen gegenüber dem Bundesnachrichtendienst alle für eine effektive Kontrolle erforderlichen Befugnisse haben. Dabei ist auch dafür Sorge zu tragen, dass die Kontrolle nicht durch die „Third Party Rule“ behindert wird.

BUNDESVERFASSUNGSGERICHT

- 1 BvR 2835/17 -

Verkündet
am 19. Mai 2020
Langendörfer
Tarifbeschäftigte
als Urkundsbeamtin
der Geschäftsstelle

IM NAMEN DES VOLKES

In dem Verfahren
über
die Verfassungsbeschwerde

1. der Reporters sans frontières,
   vertreten durch den Directeur général D…,
2. der Frau I…,
3. des Herrn G…,
4. des Herrn N…,
5. des Herrn Z…,
6. des Herrn O...,
7. des Herrn L…,
8. des Herrn M...,

- Bevollmächtigte: 1. Prof. Dr. Matthias Bäcker, LL.M.,
2. Rechtsanwalt Dr. Bijan Moini -

gegen § 6 Absatz 1, 2, 3 und 6,

§ 7 Absatz 1,

§ 9 Absatz 4 und 5,

§ 10 Absatz 3,

§ 13 Absatz 4,

§ 14 Absatz 1 Satz 1 und Absatz 2,

§ 15 Absatz 1,

§ 19 Absatz 1,

§ 24 Absatz 1 Satz 1, Absatz 2 und 3

des Gesetzes über den Bundesnachrichtendienst (BND-Gesetz) in der Fassung des Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23. Dezember 2016 (Bundesgesetzblatt I Seite 3346)

hat das Bundesverfassungsgericht - Erster Senat -

unter Mitwirkung der Richterinnen und Richter

Vizepräsident Harbarth,

Masing,

Paulus,

Baer,

Britz,

Ott,

Christ,

Radtke

aufgrund der mündlichen Verhandlung vom 14. und 15. Januar 2020 durch

Urteil

für Recht erkannt:

1. **§§ 6, 7, 13 bis 15 des Gesetzes über den Bundesnachrichtendienst in der Fassung des Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23. Dezember 2016 (Bundesgesetzblatt I Seite 3346), auch in der Fassung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 30. Juni 2017 (Bundesgesetzblatt I Seite 2097), sind mit Artikel 10 Absatz 1 des Grundgesetzes sowie mit Artikel 5 Absatz 1 Satz 2 des Grundgesetzes nicht vereinbar.**

2. **§ 19 Absatz 1, § 24 Absatz 1 Satz 1, Absatz 2 Satz 1, Absatz 3 des Gesetzes über den Bundesnachrichtendienst sind mit Artikel 10 Absatz 1 des Grundgesetzes sowie mit Artikel 5 Absatz 1 Satz 2 des Grundgesetzes nicht vereinbar, soweit sie zur Verarbeitung von im Zusammenhang mit der strategischen Fernmelde- aufklärung nach §§ 6, 7, 13 bis 15 des Gesetzes über den Bundesnachrichtendienst erhobenen personen- bezogenen Daten ermächtigen.**

3. **Bis zu einer Neuregelung, längstens jedoch bis zum 31. Dezember 2021 gelten die für mit dem Grundgesetz unvereinbar erklärten Vorschriften fort.**

4. **Die Bundesrepublik Deutschland hat den Beschwerdeführerinnen und Beschwerdeführern ihre notwendigen Auslagen aus dem Verfassungsbeschwerdeverfahren zu erstatten.**

Inhaltsverzeichnis

G r ü n d e :

A.

Die Verfassungsbeschwerde richtet sich gegen die gesetzlichen Ermächtigungen des Bundesnachrichtendienstes zur sogenannten Ausland-Ausland-Fernmeldeaufklärung, zur Übermittlung der dadurch gewonnenen Erkenntnisse an inländische und ausländische Stellen und zu in diesem Zusammenhang ermöglichten Kooperationen mit ausländischen Nachrichtendiensten. Die angegriffenen Vorschriften wurden, soweit sie die Fernmeldeaufklärung und die Kooperationen betreffen, durch das am 31. Dezember 2016 in Kraft getretene Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23. Dezember 2016 (BGBl I S. 3346) in das Gesetz über den Bundesnachrichtendienst (BND-Gesetz – BNDG) vom 20. Dezember 1990 (BGBl I S. 2954, 2979), zuletzt geändert durch Art. 4 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 30. Juni 2017 (BGBl I S. 2097), eingefügt. Die Gesetzesnovelle diente in Reaktion auf Erkenntnisse und Diskussionen im 1. Untersuchungsausschuss des 18. Deutschen Bundestages (NSA-Untersuchungsausschuss, vgl. Abschlussbericht BTDrucks 18/12850) der Klärung der Rechtslage in Hinblick auf eine bereits zuvor bestehende Praxis des Bundesnachrichtendienstes. Die angegriffenen Vorschriften zur Übermittlung sind demgegenüber älteren Datums und wurden durch die Novelle in ihrem Wortlaut nicht verändert; sie erstrecken sich nun aber auch auf die Übermittlung von Erkenntnissen, die auf den neu gestalteten Aufklärungsbefugnissen beruhen. 1

I.

1. Die unmittelbar oder mittelbar angegriffenen Bestimmungen des BND-Gesetzes und die dort in Bezug genommenen Vorschriften des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG) vom 20. Dezember 1990 (BGBl I S. 2954, 2970) in der angegriffenen Fassung des Art. 1 des Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23. Dezember 2016 (BGBl I S. 3346) lauten wie folgt: 2

§ 6 BNDG – 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.

(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.

(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.

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

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

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

(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.

§ 7 BNDG – 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.

(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.

§ 8 BNDG – 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 Telekom-

munikation zu erteilen, Sendungen, die ihm zur Übermittlung auf dem Tele- kommunikationsweg 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.

(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.

(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 abgese-

hen werden.

§ 9 BNDG – Anordnung; Unterrichtung

(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.

(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.

(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.

(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.

(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.

§ 10 BNDG – Kennzeichnung und Löschung

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

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

(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 Such- begriff 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.

(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 personen- bezogenen Daten werden gesperrt; sie dürfen nur zu diesen Zwecken verwendet werden.

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

§ 11 BNDG – 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.

§ 13 BNDG – 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.

(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.

(3) Einzelheiten der Kooperation sind vor ihrem Beginn zwischen dem Bundesnachrichtendienst und der ausländischen öffentlichen Stelle in einer Absichtserklärung schriftlich niederzulegen. In die Absichts- erklärung 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.

(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.

(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.

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

(1) Die Erhebung von Informationen einschließlich personenbezo-

gener 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.

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

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

§ 15 BNDG – 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.

(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.

(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.

(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.

§ 16 BNDG – Unabhängiges Gremium

(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 Bundes- anwalt 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 Bundes- gerichtshof 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.

(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.

(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.

(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.

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

§ 19 BNDG – Speicherung, Veränderung und Nutzung personenbezogener Daten

(1) Der Bundesnachrichtendienst darf personenbezogene Daten nach § 10 des Bundesverfassungsschutzgesetzes speichern, verändern und nutzen, soweit es zur Erfüllung seiner Aufgaben erforderlich ist.

(2) Die Speicherung, Veränderung und Nutzung personenbezogener Daten über Minderjährige ist nur unter den Voraussetzungen des § 11 des Bundesverfassungsschutzgesetzes sowie dann zulässig, wenn nach den Umständen des Einzelfalls nicht ausgeschlossen werden kann, dass von dem Minderjährigen eine Gefahr für Leib oder Leben deutscher Staatsangehöriger im Ausland oder für deutsche Einrichtungen im Ausland ausgeht.

§ 20 BNDG – Berichtigung, Löschung und Sperrung personenbezogener Daten

(1) Der Bundesnachrichtendienst hat die in Dateien gespeicherten personenbezogenen Daten zu berichtigen, zu löschen und zu sperren nach § 12 des Bundesverfassungsschutzgesetzes mit der Maßgabe, dass die Prüffrist nach § 12 Abs. 3 Satz 1 des Bundesverfassungsschutzgesetzes zehn Jahre beträgt.

(2) Der Bundesnachrichtendienst hat personenbezogene Daten in Akten zu berichtigen und zu sperren nach § 13 Absatz 1 und 2 des Bundesverfassungsschutzgesetzes. Für die Verwendung elektronischer Akten findet § 13 Absatz 4 des Bundesverfassungsschutzgesetzes mit der Maßgabe Anwendung, dass die Erforderlichkeit der elektronischen Akten für die Aufgabenerfüllung spätestens nach zehn Jahren zu prüfen ist.

§ 24 BNDG – Übermittlung von Informationen durch den Bundesnachrichtendienst

(1) Der Bundesnachrichtendienst darf Informationen einschließlich personenbezogener Daten an inländische öffentliche Stellen übermitteln, wenn dies zur Erfüllung seiner Aufgaben erforderlich ist oder wenn der Empfänger die Daten für erhebliche Zwecke der öffentlichen Sicherheit benötigt. Informationen einschließlich personenbezogener Daten, die mit den Mitteln nach § 5 erhoben worden sind, darf er an die in § 19 Absatz 1 Satz 1 des Bundesverfassungsschutzgesetzes bezeichneten Stellen nur unter den dort geregelten Voraussetzungen oder nach Absatz 3 übermitteln. Der Empfänger darf die übermittelten Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verwenden, zu dem sie ihm übermittelt wurden.

(2) Für die Übermittlung von Informationen einschließlich personen- bezogener Daten an andere Stellen ist § 19 Abs. 2 bis 5 des Bundesverfassungsschutzgesetzes entsprechend anzuwenden; dabei ist die Übermittlung nach Absatz 4 dieser Vorschrift nur zulässig, wenn sie zur Wahrung außen- und sicherheitspolitischer Belange der Bundesrepublik Deutschland erforderlich ist und das Bundeskanzleramt seine Zustimmung erteilt hat. Für vom Verfassungsschutz übermittelte personenbezogene Daten im Sinne des § 18 Abs. 1a Satz 1 des Bundesverfassungsschutzgesetzes gilt § 18 Abs. 1a Satz 2 bis 4 des Bundesverfassungsschutzgesetzes entsprechend.

(3) Der Bundesnachrichtendienst übermittelt Informationen einschließlich personenbezogener Daten an die Staatsanwaltschaften, die Polizeien und den Militärischen Abschirmdienst entsprechend § 20 des Bundesverfassungsschutzgesetzes.

Die in Bezug genommenen Vorschriften des Bundesverfassungsschutzgesetzes lauten wie folgt: 3

§ 10 BVerfSchG – Speicherung, Veränderung und Nutzung personenbezogener Daten

(1) Das Bundesamt für Verfassungsschutz darf zur Erfüllung seiner Aufgaben personenbezogene Daten in Dateien speichern, verändern und nutzen, wenn

1. tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 vorliegen,

2. dies für die Erforschung und Bewertung von Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 erforderlich ist oder

3. das Bundesamt für Verfassungsschutz nach § 3 Abs. 2 tätig wird.

(2) Unterlagen, die nach Absatz 1 gespeicherte Angaben belegen, dürfen auch gespeichert werden, wenn in ihnen weitere personenbezogene Daten Dritter enthalten sind. Eine Abfrage von Daten Dritter ist unzulässig.

(3) Das Bundesamt für Verfassungsschutz hat die Speicherungsdauer auf das für seine Aufgabenerfüllung erforderliche Maß zu beschränken.

§ 12 BVerfSchG – Berichtigung, Löschung und Sperrung personenbezogener Daten in Dateien

(1) Das Bundesamt für Verfassungsschutz hat die in Dateien gespeicherten personenbezogenen Daten zu berichtigen, wenn sie unrichtig sind.

(2) Das Bundesamt für Verfassungsschutz hat die in Dateien gespeicherten personenbezogenen Daten zu löschen, wenn ihre Speicherung unzulässig war oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. Die Löschung unterbleibt, wenn Grund zu der Annahme besteht, daß durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden. In diesem Falle sind die Daten zu sperren. Sie dürfen nur noch mit Einwilligung des Betroffenen übermittelt werden.

(3) Das Bundesamt für Verfassungsschutz prüft bei der Einzelfallbearbeitung und nach festgesetzten Fristen, spätestens nach fünf Jahren, ob gespeicherte personenbezogene Daten zu berichtigen oder zu löschen sind. Gespeicherte personenbezogene Daten über Bestrebungen nach § 3 Absatz 1 Nummer 1, 3 und 4 sind spätes-

tens zehn Jahre nach dem Zeitpunkt der letzten gespeicherten relevanten Information zu löschen, es sei denn, die zuständige Abteilungsleitung oder deren Vertretung trifft im Einzelfall ausnahmsweise eine andere Entscheidung.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

§ 18 BVerfSchG – Übermittlung von Informationen an die Verfassungsschutzbehörden

(1) […]

(1a) Das Bundesamt für Migration und Flüchtlinge übermittelt von sich aus dem Bundesamt für Verfassungsschutz, die Ausländerbehörden eines Landes übermitteln von sich aus der Verfassungsschutzbehörde des Landes ihnen bekannt gewordene Informationen einschließlich personenbezogener Daten über Bestrebungen oder Tätigkeiten nach § 3 Abs. 1, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung für die Erfüllung der Aufgaben der Verfassungsschutzbehörde erforderlich ist. Die Übermittlung dieser personenbezogenen Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen nach § 19 Abs. 3 unterbleibt auch dann, wenn überwiegende schutzwürdige Belange Dritter entgegenstehen. Vor einer Übermittlung nach § 19 Abs. 3 ist das Bundesamt für Migration und Flüchtlinge zu beteiligen. Für diese Übermittlungen des Bundesamtes für Verfassungsschutz gilt § 8b Absatz 3 entsprechend. […]

(1b) – (6) […]

§ 19 BVerfSchG – Übermittlung personenbezogener Daten durch das Bundesamt für Verfassungsschutz

(1) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten, die mit den Mitteln nach § 8 Absatz 2 erhoben worden sind, an die Staatsanwaltschaften, die Finanzbehörden nach § 386 Absatz 1 der Abgabenordnung, die Polizeien, die mit der Steuerfahndung betrauten Dienststellen der Landesfinanzbehörden, die Behörden des Zollfahndungsdienstes sowie andere Zolldienststellen, soweit diese Aufgaben nach dem Bundespolizeigesetz wahrnehmen, übermitteln, soweit dies erforderlich ist zur

1. Erfüllung eigener Aufgaben der Informationsgewinnung (§ 8 Ab-

satz 1 Satz 2 und 3),

2. Abwehr einer im Einzelfall bestehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben, Gesundheit oder Freiheit einer Person oder für Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist,

3. Verhinderung oder sonstigen Verhütung von Straftaten von erheblicher Bedeutung oder

4. Verfolgung von Straftaten von erheblicher Bedeutung;

§ 20 bleibt unberührt. […]

(2) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an Dienststellen der Stationierungsstreitkräfte übermitteln, soweit die Bundesrepublik Deutschland dazu 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) verpflichtet ist.

(3) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen übermitteln, wenn die Übermittlung zur Erfüllung seiner Aufgaben oder zur Wahrung erheblicher Sicherheitsinteressen des Empfängers erforderlich ist. Die Übermittlung unterbleibt, wenn auswärtige Belange der Bundesrepublik Deutschland oder überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Die Übermittlung ist aktenkundig zu machen. Der Empfänger ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie ihm übermittelt wurden, und das Bundesamt für Verfassungsschutz sich vorbehält, um Auskunft über die vorgenommene Verwendung der Daten zu bitten.

(4) Personenbezogene Daten dürfen an andere Stellen nur übermittelt werden, wenn dies zum Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes oder der Sicherheit des Bundes oder eines Landes oder zur Gewährleistung der Sicherheit von lebens- oder verteidigungswichtigen Einrichtungen nach § 1 Abs. 4 des Sicherheitsüberprüfungsgesetzes erforderlich ist. Übermittlungen nach Satz 1 bedürfen der vorherigen Zustimmung durch das Bundesministerium des Innern. Das Bundesamt für Verfassungsschutz führt einen Nachweis über den Zweck, die Veranlassung, die

Aktenfundstelle und die Empfänger der Übermittlungen nach Satz 1. Die Nachweise sind gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr ihrer Erstellung folgt, zu vernichten. Der Empfänger darf die übermittelten Daten nur zu dem Zweck verwenden, zu dem sie ihm übermittelt worden sind. Der Empfänger ist auf die Verwendungsbeschränkung und darauf hinzuweisen, dass das Bundesamt für Verfassungsschutz sich vorbehält, um Auskunft über die Verwendung der Daten zu bitten. Die Übermittlung der personenbezogenen Daten ist dem Betroffenen durch das Bundesamt für Verfassungsschutz mitzuteilen, sobald eine Gefährdung seiner Aufgabenerfüllung durch die Mitteilung nicht mehr zu besorgen ist.

(5) Absatz 4 findet keine Anwendung, wenn personenbezogene Daten zum Zweck von Datenerhebungen nach § 8 Absatz 1 Satz 2 an Stellen übermittelt werden, von denen die Daten erhoben werden, oder die daran mitwirken. Hiervon abweichend findet Absatz 4 Satz 5 und 6 in Fällen Anwendung, in denen die Datenerhebung nicht mit den in § 8 Absatz 2 bezeichneten Mitteln erfolgt.

§ 20 BVerfSchG – Übermittlung von Informationen durch das Bundesamt für Verfassungsschutz an Strafverfolgungs- und Sicherheitsbehörden in Angelegenheiten des Staats- und Verfassungsschutzes

(1) Das Bundesamt für Verfassungsschutz übermittelt den Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, den Polizeien von sich aus die ihm bekanntgewordenen Informationen einschließlich personenbezogener Daten, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung zur Verhinderung oder Verfolgung von Staatsschutzdelikten erforderlich ist. Delikte nach Satz 1 sind die in §§ 74a und 120 des Gerichtsverfassungsgesetzes genannten Straftaten sowie sonstige Straftaten, bei denen auf Grund ihrer Zielsetzung, des Motivs des Täters oder dessen Verbindung zu einer Organisation tatsächliche Anhaltspunkte dafür vorliegen, daß sie gegen die in Artikel 73 Nr. 10 Buchstabe b oder c des Grundgesetzes genannten Schutzgüter gerichtet sind. Das Bundesamt für Verfassungsschutz übermittelt dem Bundesnachrichtendienst von sich aus die ihm bekanntgewordenen Informationen einschließlich personenbezogener Daten, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für die Erfüllung der gesetzlichen Aufgaben des Empfängers erforderlich ist.

(2) […] [Übermittlungsersuchen der Polizeien und des BND]

2. Die Ausland-Ausland-Fernmeldeaufklärung zielt allein auf die Überwachung des Telekommunikationsverkehrs von im Ausland befindlichen Ausländerinnen und Ausländern. Sie ist eingebunden in die allgemeine Aufklärungsaufgabe des Bundesnachrichtendienstes, die gemäß § 1 Abs. 2 Satz 1 BNDG darin besteht, zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen zu sammeln und auszuwerten. 4

Zur Erfüllung seines Aufklärungsauftrags bedient sich der Bundesnachrichtendienst verschiedener Informationsquellen. Diese lassen sich in vier Säulen gliedern, nämlich die Sammlung und Auswertung allgemeinverfügbarer Quellen, die Auswertung von – überwiegend mittels Satelliten gewonnenem – Bildmaterial, die Sammlung und Auswertung von Informationen, die durch menschliche Quellen gewonnen wurden, und die von der Abteilung Technische Aufklärung durchgeführte Tele- kommunikationsüberwachung („signals intelligence“, SIGINT), zu der die verfahrensgegenständliche strategische Ausland-Ausland-Fernmeldeaufklärung gehört. Nach Angaben der Bundesregierung beruhen etwa 50 Prozent der vom Bundesnachrichtendienst insgesamt generierten Meldungen aus Aufkommen der Abteilung Technische Aufklärung, wobei wiederum 36 Prozent der Meldungen und damit durchschnittlich 260 am Tag aus der streitgegenständlichen Ausland-Ausland- Fernmeldeaufklärung stammen. 5

Die angegriffenen Vorschriften regeln die sogenannte strategische Telekommunikationsüberwachung. Diese ist dadurch gekennzeichnet, dass sie auf Telekommunikationsübertragungswege oder -netze bezogen ist und darauf zielt, aus der Gesamtheit der in den Netzen übermittelten Telekommunikationsdaten diejenigen herauszufiltern, die eine nachrichtendienstliche Relevanz besitzen. Dementsprechend hat sie zwangsläufig eine große Streubreite und ist typischerweise nicht an konkrete Anlässe oder Verdachtsmomente geknüpft. Stattdessen wirkt sie im Vorfeld und bezweckt in erster Linie die Gewinnung von Anhaltspunkten, Verdachtsmomenten, allgemeinen Erkenntnissen und Lagebildern zu Themen, die durch das Auftragsprofil der Bundesregierung (vgl. § 6 Abs. 1 Satz 1 Nr. 3 BNDG, üblicherweise abgekürzt „APB“; näher unten Rn. 9) als für das außen- und sicherheits- politische Handeln der Bundesrepublik bedeutsam ausgewiesen sind. Daneben sind mit dem Mittel der strategischen Telekommunikationsüberwachung jedoch auch auf konkrete Einzelpersonen bezogene Aufklärungsmöglichkeiten eröffnet und bezweckt. 6

Neben der hier angegriffenen Befugnis zur strategischen Überwachung der Telekommunikation von im Ausland befindlichen Ausländern verfügt der Bundesnachrichtendienst – zusätzlich zur Befugnis zu Beschränkungen in Einzelfällen – über eine Befugnis zur strategischen Überwachung des internationalen Telekommunikationsverkehrs, also der Telekommunikation zwischen im Ausland befindlichen Ausländern auf der einen und Inländern oder Deutschen auf der anderen Seite. Diese Befugnisse sind – hier nicht streitgegenständlich – im Artikel 10-Gesetz vom 26. Juni 2001 (BGBl I S. 1254, 2298), zuletzt geändert durch Artikel 12 des Gesetzes vom 17. August 2017 (BGBl I S. 3202), geregelt und dabei rechtlich anders ausgestaltet. Andere 7

Behörden, insbesondere das Bundesamt für Verfassungsschutz als inländischer Nachrichtendienst, verfügen über solche Befugnisse nicht.

3. Die angegriffenen Vorschriften treffen spezifische Regeln sowohl für die Erhebung von Daten vom Inland aus und deren Verarbeitung (§ 6 BNDG) als auch für die weitere Verarbeitung vom Ausland aus erhobener Daten (§ 7 Abs. 1 BNDG). Eine ausdrückliche Befugnisnorm zur Erhebung personenbezogener Daten vom Ausland aus regelt § 7 BNDG bewusst nicht und enthält das BND-Gesetz auch anderweitig nicht. Der Gesetzgeber geht davon aus, dass es hierfür einer Eingriffsgrundlage nicht bedürfe und Datenerhebungen allein auf die Aufgabennorm in § 1 Abs. 2 BNDG gestützt werden könnten, weil hier keine Bindung an die Grundrechte des Grundgesetzes bestehe (vgl. BTDrucks 18/9041, S. 25). 8

Aufklärungsfokus, -tiefe und -prioritäten der durch die angegriffenen Vorschriften begründeten Überwachungsmaßnahmen werden durch das vom Bundeskanzleramt im Einvernehmen mit den anderen im Bereich der Außen- und Sicherheitspolitik tätigen Bundesministerien (vgl. § 6 Abs. 1 Satz 1 Nr. 3 BNDG) festgelegte, der Geheimhaltung unterliegende Auftragsprofil der Bundesregierung konkretisiert. Daneben existieren nach Angaben der Bundesregierung in der Praxis auch kurzfristige Einzelaufträge seitens des Bundeskanzleramts. § 6 Abs. 1 Satz 1 Nr. 1 und 2 BNDG eröffnet dem Dienst auch unabhängig von Aufträgen der Bundesregierung die Durchführung von Überwachungsmaßnahmen. 9

Erhoben werden dürfen dabei alle Informationen und Daten aus Netzen, die durch Anordnung des Bundeskanzleramts festgelegt werden („Netzanordnung“, vgl. § 6 Abs. 1 Satz 2, § 9 Abs. 1, 3 und 4 BNDG). Eine Ausnahme gilt nur für Daten aus Telekommunikationsverkehren unter Beteiligung von Deutschen oder Inländern (§ 6 Abs. 4 BNDG); die Vorschrift wird in der Praxis so verstanden, dass zunächst auch deren Daten erfasst werden dürfen, diese dann aber ohne inhaltliche Auswertung nach Möglichkeit ausgefiltert werden müssen. Umfasst sind sowohl Verkehrs- und Inhaltsdaten aus Telekommunikationsvorgängen zwischen Personen als auch – nach Angaben der Bundesregierung zu der Handhabung der Vorschrift in der Praxis – andere in den Netzen transportierte Daten aus Mensch-zu-Maschine- oder Maschine-zu-Maschine-Kommunikation, wie beispielsweise automatisch abgesetzte Lokalisationsdaten eingeschalteter Mobiltelefone. Inhaltsdaten der Telekommunikation dürfen nur auf Basis von Suchbegriffen erhoben werden, die zur Aufklärung von auf die gesetzlichen Aufklärungszwecke bezogenen Sachverhalten geeignet und erforderlich sind (§ 6 Abs. 2 BNDG). Die gezielte Erfassung der Telekommunikation von Unionsbürgern und öffentlichen Stellen der Europäischen Union oder ihrer Mitgliedstaaten unterliegt besonderen materiellen (§ 6 Abs. 3 BNDG) und teilweise auch verfahrensrechtlichen (§ 9 Abs. 2 und 5 BNDG) Bedingungen. Eine Datenerhebung und -verarbeitung zu Zwecken der Wirtschaftsspionage ist nicht erlaubt (§ 6 Abs. 5 BNDG). Verkehrsdaten, zu denen in der Praxis ersichtlich nicht nur die Daten aus Telekommunikation zwischen Personen, sondern auch sonstige in den Netzen transportierte personenbezogene (Meta-)Daten gezählt werden, dürfen be- 10

vorratend für einen Zeitraum von bis zu sechs Monaten gespeichert werden (§ 6 Abs. 6 Satz 1 BNDG) und unterliegen währenddessen einer nicht näher geregelten Verarbeitung und Auswertung. Im Fall einer konkret festzustellenden nachrichtendienstlichen Erforderlichkeit kann auch eine längere Speicherung gerechtfertigt sein (§ 6 Abs. 6 Satz 2 BNDG). § 7 BNDG regelt die weitere Verarbeitung vom Ausland aus erhobener Telekommunikationsdaten; die Befugnis zu deren Erhebung selbst regelt er nicht, sondern setzt sie voraus.

Soweit technisch erforderlich, sind Anbieter von Telekommunikationsdiensten nach § 8 BNDG auf entsprechende Ausleitungsanordnung zur Ermöglichung und Mitwirkung an der Datenerfassung verpflichtet. § 9 BNDG regelt das Verfahren der Anordnung der zu erfassenden Netze sowie der Festlegung von Suchbegriffen in besonderen Fällen zum Schutz vor einer gezielten Erfassung bestimmter Akteure in der Europäischen Union, einschließlich einer gewissen Kontrolle dieser Vorgaben durch das nach § 16 BNDG einzurichtende Unabhängige Gremium. Nach § 10 Abs. 1 BNDG sind erhobene Daten zu kennzeichnen und unterliegen gemäß § 10 Abs. 2 bis 5 BNDG in Fällen unzulässiger Erhebung der Löschung. Abweichend davon trifft § 10 Abs. 4 Satz 2 bis 6 BNDG besondere Verfahrensvorgaben für den Fall, dass eine unverzügliche Löschung von Kommunikation unter nachträglich erkannter Beteiligung von Deutschen oder Inländern unterbleibt. Rechtliche Vorkehrungen zum Schutz des Kernbereichs der persönlichen Lebensgestaltung sind in § 11 BNDG geregelt. 11

4. §§ 13 bis 15 BNDG regeln die Kooperation des Bundesnachrichtendienstes mit ausländischen Nachrichtendiensten einschließlich der automatisierten Übermittlung von Daten an ausländische öffentliche Stellen. Die Vorschriften erlauben – weithin unter Verweis auf die soeben erläuterten Vorgaben zur Datenerhebung (§ 14 Abs. 2 BNDG) – insoweit zunächst eine Datenerhebung zur strategischen Telekommunikationsüberwachung durch den Bundesnachrichtendienst auch zugunsten kooperierender Nachrichtendienste (§ 14 BNDG). Grundlage sind eine näher geregelte gemeinsame Absichtserklärung (§ 13 BNDG) und die dort niedergelegten Kooperationsziele. Erlaubt ist dabei insbesondere der Abgleich der vom Bundesnachrichtendienst erfassten Telekommunikationsdaten mit von Partnerdiensten benannten Suchbegriffen (§ 14 Abs. 1 Satz 1 BNDG). Darauf aufbauend ermächtigen die Vorschriften den Bundesnachrichtendienst dann – nach besonderen inhaltlichen und verfahrensmäßigen Maßgaben (§ 15 Abs. 1 und 2 BNDG), zu denen die automatische Ausfilterung der inländischen und internationalen Kommunikation gehört – zur automatisierten Übermittlung der anhand fremdbenannter Suchbegriffe selektierten Datenverkehre an Kooperationspartner. Daneben ist auch eine automatisierte Übermittlung unselektiert erhobener Verkehrsdaten zulässig (§ 15 Abs. 1 BNDG). Die Entgegennahme und Verarbeitung von Daten, die ausländische Dienste im Rahmen von Kooperationen erheben und an den Bundesnachrichtendienst übermitteln, sind durch §§ 14 f. BNDG nicht spezifisch geregelt. 12

5. Neben diesen besonderen Erhebungs-, Verarbeitungs-, Speicher-, Löschungs- und Übermittlungsregelungen für den Bereich der Ausland-Ausland-Fernmeldeaufklärung gelten die allgemeinen, durch die Gesetzesnovelle vom 23. Dezember 2016 nicht veränderten Vorschriften des BND-Gesetzes zur Nutzung, Verarbeitung, Speicherung, Berichtigung, Löschung und Übermittlung beim Bundesnachrichtendienst vorhandener personenbezogener Daten (§§ 19, 20, 24 BNDG). Danach darf der Bundesnachrichtendienst die aus der Ausland-Ausland-Aufklärung stammenden personenbezogenen Daten speichern, verändern und nutzen, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist (§ 19 Abs. 1 BNDG). Er muss sie berichtigen und löschen, wenn sie unrichtig oder zur Erfüllung seiner Aufgaben nicht mehr erforderlich sind, wobei die hierbei vorausgesetzten Prüffristen bis zu zehn Jahre betragen können (§ 20 Abs. 1 BNDG, § 12 BVerfSchG). § 24 BNDG und die dort in Bezug genommenen Normen des Bundesverfassungsschutzgesetzes ermächtigen den Bundesnachrichtendienst zur Übermittlung der von ihm gewonnenen Informationen, insbesondere personenbezogener Daten, an näher aufgeführte in- und ausländische Stellen im Einzelfall. 13

6. Die näheren Einzelheiten des Erhebungs- und Verarbeitungsprozesses, der Kontrollzuständigkeiten innerhalb des Dienstes sowie der Datenübermittlung im Rahmen von Kooperationen sind in Dienstvorschriften zu regeln, die der Zustimmung des Bundeskanzleramts bedürfen (§ 6 Abs. 7, § 15 Abs. 3 Satz 5 BNDG). Auch über diese gesetzlichen Vorgaben hinaus sind die technischen und praktischen Einzelheiten des gesamten Erhebungs- und Auswertungsprozesses, der Kooperationen sowie der Datenübermittlung durch nichtöffentliche Dienstvorschriften geregelt. Dem Senat lagen bei der Entscheidung die „Dienstvorschrift nach § 6 Abs. 7 BNDG für die strategische Fernmeldeaufklärung des BND (DV SIGINT)“ – mit vereinzelten Schwärzungen –, die „Dienstvorschrift zur Übermittlung von Informationen durch den Bundesnachrichtendienst (DV Übermittlung)“, die „Dienstvorschrift zum Auftragsprofil der Bundesregierung (DV APB)“ und die „Dienst- vorschrift über den Abschluss internationaler Absprachen mit ausländischen Nachrichtendiensten (DV Internationale Absprachen – AND)“ vor. 14

7. Bereits vor Erlass der angegriffenen Befugnisse sowie seitdem in deren Ausübung hat sich eine Praxis der strategischen Ausland-Ausland-Fernmeldeaufklärung herausgebildet, die in verschiedene Schritte gegliedert ist. 15

a) Zunächst verschafft sich der Bundesnachrichtendienst Zugriff auf Tele- kommunikationsdatenströme, indem er mittels eigener Vorrichtungen Signale aus Telekommunikationsnetzen abfängt oder sich gemäß § 8 BNDG von Tele- kommunikationsdiensteanbietern Datenströme ausleiten lässt. Zugrunde liegen die Netzanordnungen des Bundeskanzleramts (§ 6 Abs. 1 Satz 2; siehe oben Rn. 10). Drei von 17 der derzeit in Geltung befindlichen Netzanordnungen beziehen sich auf in Deutschland gelegene Internetknotenpunkte. Die übrigen Anordnungen beziehen sich im Wesentlichen auf Satellitennetze. 16

Auf die durch das Bundeskanzleramt angeordneten Netze können sich dann insbesondere konkrete Ausleitungsanordnungen des Bundesnachrichtendienstes gegenüber Telekommunikationsdiensteanbietern nach § 8 Abs. 1 Satz 1 BNDG richten. § 8 BNDG ermöglicht die Erfassung leitungsgebundener Telekommunikation im Inland auf Grundlage von an Telekommunikationsdiensteanbieter gerichteten Ausleitungsanordnungen des Bundesnachrichtendienstes. Diese Ausleitungsanordnungen haben besondere praktische Bedeutung. Nach Angaben der Bundesregierung befinden sich von den weltweit hunderten Internetknotenpunkten, an denen die das Internet ausmachenden Teilnetze miteinander verschaltet sind, 27 Knotenpunkte in Deutschland, darunter der zur Zeit weltweit größte und von der Lage her wichtige Knotenpunkt DE-CIX in Frankfurt am Main. 17

Im Rahmen einer Netzanordnung des Bundeskanzleramts (§ 6 Abs. 1 Satz 2 BNDG), aber auch im Rahmen der die Netzanordnungen teilweise umsetzenden Ausleitungsanordnungen (§ 8 Abs. 1 Satz 1 BNDG) können mehrere Netze gleichzeitig zur Erfassung angeordnet werden, was auch der Praxis entspricht. Hierbei werden oftmals deutlich mehr Netze mit einer wesentlich größeren Kapazität zur Erfassung angeordnet als tatsächlich Daten abgerufen werden. Nach Angaben der Bundesregierung in der mündlichen Verhandlung greift der Bundesnachrichtendienst durchschnittlich auf ungefähr zehn Prozent der insgesamt zur Erfassung angeordneten Netzkapazität tatsächlich zu, um die darin enthaltenen Daten zu verarbeiten und auszuwerten. Soweit sich der Bundesnachrichtendienst bei der Erfassung im Inland einer Mitwirkung nach § 8 BNDG verpflichteter Telekommunikationsdiensteanbieter bedient, erfolgt die Auswahl der tatsächlich überwachten Netze in der Weise, dass der Dienst von den in der Ausleitungsanordnung enthaltenen Netzen beim jeweiligen Anbieter einzelne Netze, Teilnetze oder Über- tragungsstrecken über sogenannte Statustabellen zur Ausleitung anfordert (vgl. BVerwG, Urteil vom 30. Mai 2018 - 6 A 3.16 -, Rn. 5). Nach Angaben in der schriftlichen Stellungnahme des Branchenverbands eco – Verband der Internetwirtschaft e.V. haben die am Internetknotenpunkt DE-CIX installierten technischen Systeme des Bundesnachrichtendienstes derzeit die Kapazität, etwa fünf Prozent des hier durchgeleiteten Telekommunikationsverkehrs zu erfassen und zu verarbeiten. 18

b) Mit der Übertragung des durch Ausleitung von Daten oder mittels anderer Abfangmethoden zugänglich gemachten Datenstroms auf die Erfassungssysteme des Bundesnachrichtendienstes beginnt ein mehrstufiger und vollautomatisierter Filterungs- und Auswertungsprozess, der jeweils mit einer Speicherung oder Löschung der zwischengespeicherten Daten endet. Dabei werden die Datenströme zunächst technisch aufbereitet, um sie verschiedenen Datenarten (zum Beispiel Daten aus Streaming, Internetverlaufsdaten, Daten aus Telekommunikationsvorgängen) zuordnen und, soweit schon nach technischen Gesichtspunkten irrelevant, aussondern zu können. Anschließend werden die erfassten Telekommunikationsdaten mit dem Zweck elektronisch gefiltert, den nicht der Ausland-Ausland- Aufklärung unterliegenden Datenverkehr unter Beteiligung von deutschen Staatsangehörigen oder Inlän- 19

dern zu erkennen und auszuscheiden (sogenannte DAFIS-Filterung). Dazu werden die erfassten Telekommunikationsverkehre anhand verschiedener metadatenbezogener Formalkriterien (z.B. Verwendung einer deutschen Toplevel-Domain) auf einen Inlands- oder Deutschenbezug überprüft und zusätzlich mit einer beim Bundesnachrichtendienst geführten Liste („G 10- Positivliste“) von Telekommunikationskennungen abgeglichen, die Inländern oder Deutschen zugeordnet werden können. Der Grad der Verlässlichkeit dieser Filterung ist ebenso wie die derzeitigen technischen Möglichkeiten besserer Filterung zwischen den Beteiligten strittig. Nach Angaben der Bundesregierung lassen sich IP-Adressen mit einer Sicherheit von 98 Prozent ländergenau zuordnen. Um auch solchen Datenverkehr unter Beteiligung von Inländern oder Deutschen zu erkennen, der beispielsweise aufgrund der Zwischenschaltung im Ausland gelegener Server oder der Nutzung von Hotspots ausschließlich ausländischen IP-Adressen zuzuordnen ist, bezieht der Bundesnachrichtendienst in seine Filterung zusätzlich weitere Formalkriterien und Metadaten ein. Welche Fehlerquote für die Einordnung eines Verkehrs als reiner Auslandsverkehr daraus insgesamt folgt, ist nicht bekannt.

Die Bundesregierung macht geltend, dass die Zahl der Telekommunikationsverkehre, bei denen die Beteiligung von deutschen Staatsangehörigen oder Inländern durch die Filterprozesse zunächst nicht erkannt, dann aber später im Rahmen der weiteren Auswertung und Datenverwendung dem Bundesnachrichtendienst offenbar wird, in der Praxis sehr gering sei. Bei der händischen Auswertung der durch Suchbegriffe selektierten Telekommunikationsverkehre, bei der rund 270.000 täglich erhobene Inhaltsverkehre durch ein Bündel vielfältiger Kriterien auf rund 260 relevante Meldungen reduziert würden (unten Rn. 24 f.), werde täglich im Durchschnitt tatsächlich nur ein Telekommunikationsverkehr bekannt, dessen Inländer- oder Deutschenbezug elektronisch nicht erkannt worden sei. Nach Angaben der Bundesregierung wurde bisher nur ein einziger Fall verzeichnet, in dem eine Löschung eines nachträglich erkannten Telekommunikationsverkehrs mit Inlands- oder Deutschenbezug mit Genehmigung der G10-Kommission unterblieb (§ 10 Abs. 4 Satz 2 bis 6 BNDG). 20

c) Die nach der DAFIS-Filterung verbleibenden Verkehrsdaten (§ 6 Abs. 6 Satz 1 BNDG) erhebt und speichert der Bundesnachrichtendienst pauschal, also unabhängig von Selektoren, und wertet sie zu einem späteren Zeitpunkt durch Datenabgleich und weitere Analysemethoden in erster Linie computergestützt aus. 21

d) Telekommunikationsinhalte gelangen hingegen nach § 6 Abs. 2 BNDG nur dann in eine über die technisch notwendige Zwischenspeicherung hinausgehende Speicherung und Auswertung, wenn Elemente einer erfassten Telekommunikation beim computergesteuerten Abgleich mit zuvor festgelegten Suchbegriffen (Selektoren) erkannt und als relevant aus dem Datenstrom ausgesondert wurden. Nach Angaben der Bundesregierung und den Vorgaben der einschlägigen Dienstvorschrift (DV SIGINT) werden die hierzu verwendeten Suchbegriffe vor einer aktiven Verwendung („Steuerung“) dienstintern durch eine Untereinheit („Qualitätssicherung SIGINT“) auf Auftragskonformität, rechtliche Zulässigkeit – insbesondere hinsichtlich ihrer Verhält- 22

nismäßigkeit – und Plausibilität überprüft. Von den Systemen des Bundesnachrichtendienstes erfasste, aber nicht anhand der Suchbegriffe selektierte Telekommunikationsinhaltsdaten werden nach dem Abgleich rückstandslos aus den Erfassungssystemen gelöscht.

Bei den Selektoren werden inhaltliche und formale Begriffe unterschieden, wobei der Bundesnachrichtendienst ganz überwiegend (nach Angaben der Bundesregierung ungefähr zu 90 Prozent) formale Suchbegriffe verwendet. Dies sind Kommunikationsmerkmale, wie beispielsweise Anschlusskennungen oder E-Mail- Adressen, die nachrichtendienstlich für relevant erachteten Personen, Entitäten, Gruppen oder Phänomenen zugeordnet werden können. Mittels solcher Suchbegriffe kann der Bundesnachrichtendienst aus den erfassten Datenströmen alle Telekommunikation identifizieren und zur Speicherung aussondern, die an die als Suchbegriff verwendete Kennung oder Adresse gerichtet ist, von ihr stammt oder sie enthält. Nach Angaben der Bundesregierung dienen circa fünf Prozent der Suchbegriffe dem Zweck, gezielt Erkenntnisse zu einzelnen Personen in Hinblick auf gegenüber ihnen zu ergreifende Maßnahmen zu erlangen; in den übrigen Fällen sind die hinter den gesteuerten Suchbegriffen stehenden Personen nur zum Teil bekannt, ohne dass sie selbst und ihr Verhalten im Fokus des Aufklärungsinteresses stehen. 23

Auf diesem Weg selektiert der Bundesnachrichtendienst aus dem erfassten Datenvolumen mittels einer sechsstelligen Zahl von Suchbegriffen die Inhaltsdaten von täglich circa 270.000 Telekommunikationsvorgängen zwischen Menschen (E-Mail, Telefonat, Chat-Nachrichten) und speichert sie zur weiteren händischen Auswertung. Diese Zahl setzt sich aus vom Inland aus erhobenen Verkehren (circa 60 Prozent) und Auslandserfassungen (circa 40 Prozent) sowie einer niedrigen fünfstelligen Zahl von Telekommunikationsverkehren zusammen, die dem Dienst von kooperierenden ausländischen Nachrichtendiensten zugeleitet werden. Zusätzlich erfasst und speichert der Bundesnachrichtendienst täglich eine um mehrere Größenordnungen höhere Menge von Verkehrsdaten. 24

e) An die Selektion und Speicherung von Inhaltsverkehren mittels Suchbegriffen schließt sich deren weitere Auswertung an. Kernstück dieses Arbeitsschritts ist die händische Bewertung auf nachrichtendienstliche Relevanz. Hierbei werden zur Zeit im täglichen Durchschnitt rund 260 Datenverkehre identifiziert, die an die „abnehmenden Bereiche“ weitergeleitet werden. Nach Angaben der Bundesregierung wird in diesem Rahmen – zusammen mit der Bewertung der Relevanz und der händischen Sichtung auf eine versehentliche Erfassung internationaler oder inländischer Telekommunikation – auch der Kernbereichsschutz nach § 11 BNDG praktisch implementiert. Für die vorherigen Verfahrensschritte entfalten die Vorgaben zum Kernbereichsschutz demgegenüber nach Angaben der Bundesregierung keine praktische Wirkung. Nach der einschlägigen Dienstvorschrift (DV SIGINT) und Angaben der Bundesregierung wird bei der händischen Auswertung auch die geschützte Kommunikation von nach § 53 StPO zeugnisverweigerungsberechtigten Personen berücksichtigt; solche Kommunikation darf danach nur dann verwendet werden, wenn der 25

besondere Informationswert des erfassten Telekommunikationsinhalts bei einer Abwägung mit den entgegenstehenden Geheimhaltungsinteressen überwiegt.

f) In §§ 13 bis 15 BNDG ist erstmals die Praxis der nachrichtendienstlichen Kooperationen gesetzlich geregelt. Darauf lag ein Hauptaugenmerk der Aufklärungsarbeit im NSA-Untersuchungsausschuss (vgl. BTDrucks 18/12850, S. 516 ff.; 706 ff.; 761 bis 1007). Ziele dieser Praxis sind nach den Gesetzesmaterialien (BTDrucks 18/9041, S. 29) und Angaben der Bundesregierung die effektive Nutzung von Aufklärungsressourcen, die Erweiterung der den Diensten insgesamt zugänglichen Datenbasis und der stetige Austausch nachrichtendienstlichen Knowhows, insbesondere technischer Fähigkeiten und geeigneter Suchbegriffe. 26

Dementsprechend benutzt der Bundesnachrichtendienst im Rahmen von Kooperationen, aber auch für die eigene Fernmeldeaufklärung, in erheblichem Umfang von den Partnerdiensten benannte Suchbegriffe. Dies betrifft etwa 50 bis 60 Prozent der Suchbegriffe, die der Bundesnachrichtendienst aktuell zur Erfassung verwendet. Dabei nutzt der Dienst jedoch keine Suchbegriffe, deren Bedeutung, Funktionsweise oder Typus ihm unbekannt sind. Vielmehr verlangt er nach der einschlägigen Dienstvorschrift und Angaben der Bundesregierung zu jedem von einem Partnerdienst benannten Suchbegriff nähere Angaben, die in eine elektronische Prüfung der Suchbegriffe integriert werden. Daneben prüft er die von ausländischen Diensten benannten Suchbegriffe vor ihrer Verwendung elektronisch auf einen Deutschen- oder Inländerbezug, auf einen Verstoß gegen die Grenzen gezielter Erfassungen nach § 6 Abs. 3 BNDG, auf einen Verstoß gegen Interessen der Bundesrepublik Deutschland sowie auf bestimmte, in Hinblick auf die jeweilige Kooperation und ihre Ziele definierte Formalkriterien. Zusätzlich führt der Bundesnachrichtendienst für jede Kooperation monatlich eine in der Dienstvorschrift definierte Mindestanzahl händischer Stichproben durch, wobei die tatsächliche Zahl der Stichproben nach eigenen Angaben über das durch die Dienstvorschrift gebotene Maß hinausgeht und monatlich ungefähr 300 Suchbegriffe betrifft. 27

Die gemäß § 15 Abs. 1 Nr. 1a BNDG vor einer automatischen Übermittlung gebotene elektronische Ausfilterung inländischer und internationaler Telekommunikation geschieht in der Praxis nach dem oben erläuterten Muster. Zudem werden hierbei Filterverfahren zur Aussonderung solcher Erfassungen angewandt, deren Übermittlung einen Verstoß gegen deutsche Interessen befürchten ließe (§ 15 Abs. 1 Nr. 1b BNDG). Zur Überprüfung der Funktionstüchtigkeit dieser automatischen Filterverfahren (§ 15 Abs. 3 BNDG) führt der Bundesnachrichtendienst nach Angaben der Bundesregierung in der mündlichen Verhandlung wiederum händische Stichproben durch, deren monatliche Mindestanzahl je Kooperation ebenfalls in der Dienstvorschrift festgelegt ist und die sich in der Praxis monatlich auf etwa 25 bis 40 übermittelte Erfassungen erstreckt. 28

Die Übermittlung von Daten an Partnerdienste nach § 15 Abs. 1 BNDG ist eingerahmt durch die nach § 13 Abs. 3 Nr. 4 bis 6 BNDG zwingend in der Kooperations- 29

vereinbarung vorzusehenden Verwendungsbeschränkungen und Zusicherungen zur Gewährleistung eines rechtsstaatlichen Datenumgangs und zur Datenlöschung. Der Inhalt der dementsprechend in der Absichtserklärung vorzusehenden Klauseln ist durch die einschlägige Dienstvorschrift vorgegeben. Ebenfalls zur Sicherung eines rechtsstaatlichen Anforderungen genügenden Umgangs mit den Daten versieht der Bundesnachrichtendienst nach der einschlägigen Dienstvorschrift und den Angaben der Bundesregierung jede Einzelübermittlung (§ 24 BNDG) ins Ausland mit einem Zusatz, der Verwendungsbeschränkungen und -verbote enthält.

8. Eingebettet sind diese Abläufe in besondere und allgemeine Regelungen zu Transparenz, Aufsicht und Kontrolle. Intern bestehen zunächst eine Kennzeichnungspflicht für erhobene Daten (§ 10 Abs. 1 BNDG) und besondere Protokollierungspflichten bei unzulässigen Datenverarbeitungen (§ 10 Abs. 6, § 11 Satz 4 BNDG) oder bei der automatischen Übermittlung an ausländische Kooperationspartner (§ 15 Abs. 2 BNDG). Seitens der Betroffenen bestehen Auskunftsrechte, die allerdings die Darlegung eines besonderen Interesses voraussetzen und sich nicht auf die Herkunft der Daten erstrecken (§ 22 BNDG). Benachrichtigungspflichten sind nur bei einer unzulässigen Erfassung und anschließenden Speicherung von Daten aus Telekommunikation unter Beteiligung von Inländern oder Deutschen vorgesehen (§ 10 Abs. 4 Satz 2 BNDG); gegenüber betroffenen Ausländern im Ausland sind auch bei Fällen unzulässiger Datenerhebung oder -verarbeitung keine Benachrichtigungen vorgeschrieben. 30

Als besonderes Kontrollorgan errichtet § 16 BNDG das Unabhängige Gremium, dem durch die §§ 6 bis 15 BNDG einzelne Kontrollbefugnisse zugewiesen sind. Eine allgemeine datenschutzrechtliche Kontrolle obliegt dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (§§ 32, 32a BNDG). Für die Kontrolle des Bundesnachrichtendienstes ist dabei ein Referat seiner Behörde zuständig. Zusätzlich greifen die besondere Kontrollzuständigkeit der G10-Kommission bei einer Zurückstellung einer Mitteilung nach § 10 Abs. 4 BNDG, die allgemeine parlamentarische Kontrolle seitens des Parlamentarischen Kontrollgremiums und seines Ständigen Bevollmächtigten sowie einzelne Befugnisse, die diesem Gremium in Bezug auf die Ausland-Ausland-Fernmeldeaufklärung eingeräumt sind (§ 6 Abs. 7 Satz 3, § 13 Abs. 5 Satz 2 BNDG). 31

Nach Angaben der ehemaligen Vorsitzenden des Unabhängigen Gremiums und des Bundesdatenschutzbeauftragten wird die Kontrolltätigkeit beider Organe unter Berufung auf Geheimhaltungsbedürfnisse der kooperierenden Dienste und mit ihnen geschlossene Vertraulichkeitsvereinbarungen („Third Party Rule“) praktisch eingeschränkt. 32

II.

Mit ihrer Verfassungsbeschwerde rügen die Beschwerdeführerinnen und Beschwerdeführer eine Verletzung des Fernmeldegeheimnisses nach Art. 10 GG. Soweit sie journalistisch tätig sind, machen sie darüber hinaus eine Verletzung der Pressefrei- 33

heit gemäß Art. 5 Abs. 1 Satz 2 GG geltend, da das BND-Gesetz für die strategische Überwachung ausländischer Telekommunikation keine besondere Regelung zum Schutz des Vertrauensverhältnisses zwischen der Presse und ihren Informanten enthalte. Schließlich rügen die Beschwerdeführerin zu 1) und die Beschwerdeführer zu 3) bis 5) eine Verletzung des allgemeinen Gleichheitssatzes aus Art. 3 Abs. 1 GG, weil sie als in einem Mitgliedstaat ansässige juristische Person beziehungsweise Unionsbürger nicht denselben Schutz wie Deutsche genössen.

1. Alle Beschwerdeführerinnen und Beschwerdeführer tragen in tatsächlicher Hinsicht vor, von den Ermächtigungen und dem darauf gründenden Handeln des Bundesnachrichtendienstes im Rahmen der Ausland-Ausland-Fernmeldeaufklärung betroffen zu sein. Die Beschwerdeführerin zu 1) ist eine Nichtregierungsorganisation mit Sitz in Frankreich, die sich international für die Pressefreiheit und die Sicherheit von Journalisten vor Repressalien einsetzt und diesen und ihren Angehörigen in diesem Rahmen auch konkrete sachliche und personelle Hilfe in Problemsituationen (z.B. bei Inhaftierung oder Verfolgung) leistet. Die Beschwerdeführerin zu 2) ist in Aserbaidschan und die Beschwerdeführer zu 3) bis 7) sind in Deutschland, im Vereinigten Königreich, in Slowenien, in Mexiko und in Nordmazedonien wohnhafte, dort und andernorts investigativ tätige und berichtende Journalisten mit ausländischer Staatsangehörigkeit, wobei der Beschwerdeführer zu 6) seine Tätigkeit für die journalistische Abteilung einer mexikanischen Nichtregierungsorganisation ausübt. Der Beschwerdeführer zu 8) ist ein in Guatemala wohnhafter deutscher Staatsangehöriger, der als Rechtsanwalt für ein dortiges Menschenrechtsbüro sowie für die Internationale Juristenkommission mit Sitz in Genf tätig ist. 34

Sämtliche Beschwerdeführerinnen und Beschwerdeführer geben an, privat oder im Rahmen ihrer beruflichen Tätigkeit in großem Umfang elektronische Telekommunikationsdienste, insbesondere E-Mails, Telefon und Instant-Messenger, zu nutzen. Sie würden regelmäßig zu Themen arbeiten und mit Personen in Regionen kommunizieren, die naheliegenderweise in den Fokus einer Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes gelangen könnten. Insbesondere bezögen die Beschwerdeführerin zu 2) und die Beschwerdeführer zu 3) bis 7) als investigativ tätige Journalisten einen erheblichen Teil der benötigten Kenntnisse von Informanten, mit denen sie in weitem Umfang mit kommunikationstechnischen Mitteln kommunizierten. Bei diesen Quellen handele es sich oftmals um staatliche oder privatwirtschaftliche Bedienstete, Angehörige illegaler Organisationen oder deren Kontaktpersonen, die sich durch ihre Mitwirkung vielfach erheblichen Risiken aussetzten. Auch die Beschwerdeführerin zu 1) und der Beschwerdeführer zu 8) stünden im Rahmen ihrer satzungsmäßigen oder beruflichen Tätigkeit regelmäßig mit solchen Personen in Kontakt. 35

2. Hinsichtlich der Zulässigkeit tragen die Beschwerdeführerinnen und Beschwerdeführer vor, dass sie mit einiger Wahrscheinlichkeit von Maßnahmen auf Grundlage der angegriffenen Vorschriften betroffen seien. Da bereits in der mit einem Suchbegriffsabgleich oder einer Speicherung der Verkehrsdaten einher- gehenden Erfas- 36

sung ihrer Telekommunikationsdaten ein Grundrechtseingriff liege, müssten sie nur darlegen, mit einiger Wahrscheinlichkeit überhaupt in die Erfassung des Bundesnachrichtendienstes im Rahmen der Ausland-Ausland-Aufklärung zu gelangen. Dies sei, wie eine statistische Beispielsrechnung verdeutliche, angesichts der Streubreite der Maßnahmen und des sehr hohen Telekommunikationsaufkommens sämtlicher Beschwerdeführer der Fall. Selbst wenn man verlange, dass deren Telekommunikation mit einiger Wahrscheinlichkeit beim Suchbegriffsabgleich zur weiteren Auswertung selektiert würde, seien sie tatsächlich betroffen, da sich ihre Tätigkeit durchweg auf Themen und Gebiete beziehe, an denen ein gesteigertes Interesse der deutschen Ausland-Ausland-Aufklärung naheliege. Trotz der beim Bundesnachrichtendienst vorgenommenen Anstrengungen zur automatischen Ausfilterung der Kommunikation unter Beteiligung von Inländern und Deutschen sei auch der Beschwerdeführer zu 8) mit einiger Wahrscheinlichkeit von der Ausland-Ausland-Fernmeldeaufklärung tatsächlich betroffen. Denn es sei davon auszugehen, dass der Bundesnachrichtendienst ihn als Funktionsträger einer ausländischen juristischen Person nicht als grundrechtsberechtigt ansehe.

Eine vorherige Geltendmachung eines Auskunftsanspruchs nach § 22 BNDG sei unter dem Gesichtspunkt der Subsidiarität nicht erforderlich, da dieser Anspruch allein gespeicherte Daten erfasse und somit keinen Aufschluss über eine zurück- liegende Erfassung, Erhebung, vorübergehende Speicherung oder weitere Verarbeitung von Telekommunikationsdaten der Beschwerdeführer auf Grundlage der angegriffenen Vorschriften liefere. Eine vorherige Klärung und Aufbereitung des Streitstoffs vor den Fachgerichten, wie sie in der Entscheidung des Bundesverfassungsgerichts zur Kennzeichenerfassung (BVerfGE 150, 309 <326 ff. Rn. 40 ff.>) aus Subsidiaritätsgesichtspunkten grundsätzlich verlangt werde, sei hier angesichts der faktischen und rechtlichen Grenzen des Rechtsschutzes vor dem Bundes- verwaltungsgericht in Konstellationen der strategischen Telekommunikations- überwachung nicht möglich. 37

3. Die Beschwerdeführer zu 6) und 8) seien als Funktionsträger einer aus- ländischen juristischen Person nicht vom Grundrechtsschutz des Art. 10 GG ausgeschlossen. Auch Funktionsträger einer ausländischen juristischen Person könnten grundrechtsberechtigt sein. Art. 10 Abs. 1 GG schütze die Vertraulichkeit der Kommunikation vor Einbrüchen seitens der Staatsgewalt, unabhängig davon, in welcher Funktion die Beteiligten kommunizierten. Zudem ließen sich berufliche und private Kommunikation nicht ex ante voneinander trennen, da berufliche Anschlüsse und Adressen oftmals auch privat genutzt würden. 38

4. Die Beschwerdeführerinnen und Beschwerdeführer zu 1) bis 7) tragen weiter vor, dass die gerügten Grundrechte – jedenfalls in ihrer abwehrrechtlichen Dimension – auch Ausländer im Ausland gegenüber der deutschen Staatsgewalt berechtigten. Bei diesen Grundrechten handele es sich nicht um solche, die auf Deutsche beschränkt seien. Eine Kollision mit dem Völkerrecht durch Anerkennung einer Grundrechtsberechtigung von Ausländern im Ausland stehe nicht zu befürchten. Wenn überhaupt, 39

verstoße die Ausland-Ausland-Fernmeldeaufklärung gegen Völkerrecht, nicht aber deren grundrechtliche Einhegung. Die Garantie der Grundrechte stehe nicht unter der Bedingung eines besonderen Unterworfenseins unter staatliche Hoheitsgewalt. Selbst wenn man dieser Kompensationsthese folge, bestünden im Fall der Ausland-Ausland-Fernmeldeaufklärung spezifische Risiken gerade für Ausländer im Ausland, die eine Erstreckung des Art. 10 GG auf diese rechtfertigten. Ohnehin sei die Trennung des inländischen und internationalen Telekommunikationsverkehrs von rein ausländischer Telekommunikation derart unsicher, dass die fundamentale Frage des Grundrechtsschutzes davon nicht sinnvoll abhängig gemacht werden könne. Für die Unionsbürger unter den Beschwerde- führern ergebe sich ein zwingender Grund für die Anerkennung der Grundrechts- berechtigung zudem aus dem unionsrechtlichen Diskriminierungsverbot aufgrund der Staatsangehörigkeit.

5. In Anbetracht der Grundrechtsberechtigung auch von Ausländern im Ausland seien die angegriffenen Vorschriften verfassungswidrig. Sie verletzten zunächst schon das Zitiergebot gemäß Art. 19 Abs. 1 Satz 2 GG. Im Übrigen griffen die Regelungen unverhältnismäßig in ihre Grundrechte ein. Angesichts der erheblichen Eingriffsintensität der durch sie ermöglichten strategischen Überwachung seien die möglichen Aufklärungsziele unzureichend begrenzt und gewichtig. Insbesondere seien auch die Grenzen gezielter Erfassungen ungenügend und fehlten solche bei Nicht-Unionsbürgern gänzlich. Angesichts der aus Verkehrsdaten generierbaren, mitunter höchst sensiblen Informationen sei die Befugnis zu ihrer pauschalen Erhebung, Vorhaltung und keinen Schwellen und Anlässen unterliegenden Auswertung ebenfalls – insbesondere mit Blick auf die Vorratsdatenspeicherungsentscheidungen des Europäischen Gerichtshofs und des Bundesverfassungsgerichts – grundrechtlich nicht zu rechtfertigen. Auf Auswertungsebene fehle es an Maßgaben zum Schutz besonderer Vertraulichkeitsbeziehungen, insbesondere von Journalisten und Rechtsanwälten. Erhebliche Defizite bestünden schließlich im Bereich der unabhängigen Kontrolle. Zuständigkeiten und Kontrollrahmen des Unabhängigen Gremiums seien zu restriktiv gefasst. Zudem sei die Kontrolle in dysfunktionaler Weise zwischen verschiedenen Organen aufgespalten und insgesamt nicht ausreichend wirksam, um den faktisch fehlenden Individualrechtsschutz zu ersetzen. Die Befugnisse zur Datenübermittlung in Einzelfällen genügten nicht den aktuellen, insbesondere in der Entscheidung des Bundesverfassungsgerichts zum BKA-Gesetz (BVerfGE 141, 220) entfalteten Anforderungen. Dies gelte vor allem hinsichtlich ihrer Übermittlungsschwellen und verfahrensmäßiger Sicherungen gegenüber einer rechtsstaatswidrigen Datenverwendung auf Empfängerseite. Die gerügten Mängel beträfen sämtlich auch die nachrichtendienstlichen Kooperationen. In gesteigerter Form betreffe dies dort die elektronische Ausleitung von Daten an Partnerdienste, in deren Rahmen Übermittlungsschwellen gänzlich wegfielen. Das Regime der vom Ausland aus praktizierten Fernmeldeaufklärung sei schließlich nur höchst rudimentär, lückenhaft und unbestimmt geregelt. 40

Die Beschwerdeführer haben zur Unterstützung ihres Vortrags zur mangelnden automatischen Trennbarkeit inländischer, internationaler und ausländischer Telekom- 41

munikation ein technisches Gutachten eingereicht, dessen Inhalt sie sich zu eigen machen.

III.

Zur Verfassungsbeschwerde haben Stellung genommen: die Bundesregierung, die Bayerische Staatsregierung, die jeweils amtierenden Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie der 6. Revisionssenat des Bundesverwaltungsgerichts. 42

1. Die Bundesregierung ist dem Verfahren beigetreten. In tatsächlicher Hinsicht betont sie die außerordentliche Bedeutung der Ausland-Ausland-Fernmelde- aufklärung des Bundesnachrichtendienstes für die Versorgung der Bundesregierung mit den von ihr benötigten Informationen und Entscheidungsgrundlagen. In rechtlicher Hinsicht hält sie die Verfassungsbeschwerde für unzulässig, jedenfalls aber unbegründet. 43

a) Die Ausland-Ausland-Fernmeldeaufklärung durch den Bundesnachrichtendienst sei von überragender öffentlicher Bedeutung. Dies gelte umso mehr in einer Welt neuer sicherheitspolitischer Herausforderungen und zunehmender Beanspruchung und Inpflichtnahme der Bundesrepublik als eines souveränen, wirtschaftlich starken sowie international tätigen und eingebundenen Partners. Die mit Mitteln der Ausland-Ausland-Fernmeldeaufklärung zu gewinnenden, authentischen, verlässlichen und von den Interessen ausländischer Kooperationspartner unabhängigen Informationen über das Ausland seien durch andere nachrichtendienstliche Quellen oftmals nicht oder nur unter erheblich gesteigertem Aufwand zu erlangen. Der Aufklärungsprozess werde durch das Auftragsprofil der Bundesregierung umfassend gesteuert. Eine Vollüberwachung der Telekommunikation bestimmter Personen oder Regionen sei vor dem Hintergrund der begrenzten Aufklärungsaufgabe und der technischen Kapazitäten des Bundesnachrichtendienstes weder intendiert noch möglich. Vielmehr greife der Bundesnachrichtendienst nur auf ein verschwindend kleines Fenster der weltweiten Telekommunikation zu und fokussiere seine Kapazitäten auf wesentliche auftragsrelevante Ziele. Eine weitergehende gesetzliche Konkretisierung und abschließende Aufzählung der möglichen Ziele der Ausland-Ausland-Aufklärung, insbesondere im Bereich der Kooperationen, seien nicht sinnvoll, da dann die notwendige Flexibilität und Themenfülle fehle. Ebenfalls sei eine gesonderte Anordnung jedes einzelnen Suchbegriffs in einem formalisierten Verfahren im Bereich der Ausland-Ausland-Fernmeldeaufklärung vor dem Hintergrund ihrer dynamischen Erfordernisse und der Anzahl von Themen und Ländern im Auftragsprofil weder praktisch vorstellbar noch sinnvoll. Unabdingbar sei auch das Vorhalten von unselektiert erhobenen Verkehrsdaten für einen gewissen Zeitraum, da sich nur über die zeitliche Vergleichbarkeit dieser Daten Lageentwicklungen, Netzwerke oder Verhaltensmuster analysieren ließen und die Fähigkeit zur raschen Aufklärung neuer Entwicklungen („Kaltstartfähigkeit“) einen gewissen Bestand vorgehaltener Daten voraussetze. Die technischen Verfahren der automatischen Ausfilterung und Löschung von Telekom- 44

munikationsverkehren unter Beteiligung von Deutschen oder Inländern würden stetig weiterentwickelt und seien bereits jetzt höchst verlässlich. So würden aus dem erfassten Datenaufkommen zunächst im Wege der IP-Typfilterung sämtliche IP-Verkehre, die einer in Deutschland lokalisierbaren IP-Adresse zuzuordnen seien, ausgefiltert und verworfen. Anschließend werde die erfasste Kommunikation anhand weiterer Formalkriterien (beispielsweise Verwendung einer deutschen sogenannten Toplevel-Domain) automatisch auf einen Inlands- oder Deutschenbezug durchsucht (DAFIS Stufe 1). Zusätzlich werde sämtliche erfasste Telekommunikation automatisch mit einer stetig fortgeführten und aktualisierten Positivliste abgeglichen (DAFIS Stufe 2), auf der Teilnehmer- oder Anschlusskennungen vermerkt seien, von denen bekannt sei, dass sie Deutschen oder Inländern zuzuordnen sind („G 10-Positivliste“). Zudem werde auch im Rahmen der händischen Auswertung nachträglich als solche erkannte inländische oder internationale Telekommunikation aussortiert. Im Hinblick auf nachrichtendienstliche Kooperationen führt die Bundesregierung aus, dass der Bundesnachrichtendienst zur Erfüllung seines Auftrags auf die Zusammenarbeit mit ausländischen Nachrichtendiensten zwingend angewiesen sei. Dabei müsse er unbedingt auch die „Third Party Rule“ respektieren, da andernfalls die Aufkündigung nachrichtendienstlicher Kooperationen seitens der Partner drohe.

b) In rechtlicher Hinsicht hält die Bundesregierung die Verfassungsbeschwerde bereits für unzulässig. Die Beschwerdeführer hätten nicht dargelegt, von Maßnahmen auf Grundlage der angegriffenen Vorschriften mit einiger Wahrscheinlichkeit betroffen zu sein. Dies gelte selbst, wenn man bereits die Wahrscheinlichkeit einer Erfassung durch die Systeme des Bundesnachrichtendienstes ausreichen lasse. Denn der Dienst erfasse nur einen verschwindend geringen Teil der weltweiten Telekommunikation, so dass selbst bei hohem Telekommunikationsaufkommen eine Erfassung – erst recht eine weitere Verarbeitung und Auswertung – der Telekommunikation der Beschwerdeführer äußerst unwahrscheinlich sei. Lasse man, wie die Beschwerdeführer vortragen, einen allgemeinen Bezug der jeweiligen Tätigkeit und Kommunikation zu Aufklärungsthemen und -gebieten des Bundesnachrichtendienstes genügen, geriete die Verfassungsbeschwerde im Bereich der Ausland-Ausland-Aufklärung zur nicht vorgesehenen Popularklage gegen Gesetze. Darüber hinaus hätten die Beschwerdeführer den gegenüber einer Verfassungsbeschwerde vorrangigen Auskunftsanspruch nach § 22 BNDG nicht geltend gemacht und auch den fachgerichtlichen Rechtsweg nicht beschritten. Die Verfassungsbeschwerde sei schließlich insgesamt verfristet, da die bereits vorher bestehende Praxis des Bundesnachrichtendienstes durch die angegriffenen Regelungen nur ausdrücklich normiert und beschränkt worden sei. Zumindest gelte die Verfristung für alle Vorschriften, die – wie die Übermittlungsermächtigungen – bereits vor der angegriffenen Gesetzesnovelle bestanden hätten. 45

c) Die Verfassungsbeschwerde sei jedenfalls unbegründet. Dies ergebe sich schon aus der fehlenden Grundrechtsbetroffenheit sämtlicher Beschwerdeführer. 46

Für die Beschwerdeführerinnen und Beschwerdeführer zu 1) bis 7) ergebe sich das aus dem Umstand, dass die gerügten Grundrechte zugunsten von Ausländern im Ausland keinen Schutz gewährten. Das Bundesverfassungsgericht habe die Frage der Geltung des Fernmeldegeheimnisses zugunsten von Ausländern im Ausland in seiner Entscheidung zur strategischen Überwachung nach dem Artikel 10-Gesetz im Jahr 1999 (BVerfGE 100, 313) ausdrücklich offen gelassen. Die Frage sei differenziert und orientiert am jeweiligen Umfang der Verantwortung und Verantwortlichkeit der deutschen Staatsgewalt zu behandeln. Die Grundrechte des Grundgesetzes seien ausweislich der Präambel grundsätzlich auf das deutsche Staatsgebiet und Staatsvolk beschränkt. Eine Einräumung subjektiver Grundrechtspositionen zugunsten von Ausländern im Ausland stelle eine Anmaßung auswärtiger Rechtsetzungsgewalt dar und verletze das völkerrechtliche Territorialprinzip. Jenseits des Hoheitsbereiches der Bundesrepublik träten die für den Bundesnachrichtendienst handelnden Personen ausländischen Staatsangehörigen nicht als Hoheitsgewalt gegenüber. Dann sei es folgerichtig, auch die Grundrechtsberechtigung nicht auf sie zu erstrecken. Eine Grundrechtserstreckung auf Ausländer im Ausland berge zudem die Gefahr von Schutzasymmetrien, da sich dann die Grundrechte, nicht aber die nach dem Territorialprinzip auf das Inland beschränkten Eingriffsbefugnisse auf sie erstreckten. 47

Für die Beschwerdeführer zu 6) und 8) ergebe sich die mangelnde Grundrechtsbetroffenheit aus dem Umstand, dass sie sich in ihrer Stellung als Funktionsträger ausländischer juristischer Personen nicht auf Grundrechte des Grundgesetzes berufen könnten. Art. 19 Abs. 3 GG räume eine Grundrechtsberechtigung unter den dort genannten Voraussetzungen ausdrücklich nur inländischen juristischen Personen ein. Da juristische Personen überhaupt nur über natürliche Personen als deren Organe und Vertreter handeln könnten, laufe diese Festlegung in Hinblick auf das Fernmeldegeheimnis leer, wenn sich die für ausländische juristische Personen in dienstlicher Funktion handelnden und kommunizierenden natürlichen Personen, hier also die Beschwerdeführer zu 6) und zu 8), gegenüber staatlichen Überwachungsmaßnahmen auf dieses Grundrecht berufen könnten. Das gelte auch, wenn der Funktionsträger Deutscher sei. 48

d) Selbst wenn man eine Grundrechtsberechtigung der Beschwerdeführer annehme, seien die angegriffenen Vorschriften verfassungsgemäß. Da durch sie der Eingriff im Vergleich zur bisherigen Rechtspraxis nicht vertieft werde, sei das Zitiergebot nicht anwendbar. Die Vorschriften seien hinreichend bestimmt, klar umgrenzt und in Anbetracht der Unentbehrlichkeit der mit Mitteln der Auslandsfernmeldeaufklärung gewonnenen Informationen verhältnismäßig. Die Eingriffstiefe der Ausland-Ausland-Fernmeldeaufklärung sei angesichts ihrer auf allgemeine Informationen und Lagebilder gerichteten Zielrichtung und ihres nicht personen-, sondern sachbezogenen Charakters nicht übermäßig hoch. Durch das näher geregelte Anordnungsverfahren werde ein prozeduraler Grundrechtsschutz mit besonderen Sicherungen in Fällen gezielter Erfassungen eingerichtet. Auch unterliege der Überwachungszugriff des Bundesnachrichtendienstes bereits aus technischen und kapazitätsmäßigen Gründen er- 49

heblichen Grenzen, die zur Verhältnismäßigkeit der Regelung beitrügen. Der Verweis auf die Entscheidungen des Bundesverfassungsgerichts und des Europäischen Gerichtshofs zur Vorratsdatenspeicherung sei verfehlt, da es sich hier weder um eine Vollerfassung handele, noch die Ziele der Auslandsaufklärung mit den dortigen präventivpolizeilichen Zwecken vergleichbar seien. Die Forderung nach einer über den Kernbereichsschutz hinausgehenden Privilegierung zugunsten bestimmter Berufsgruppen gehe über die Rechtsprechung des Bundesverfassungsgerichts hinweg, wonach solche Ausnahmen selbst im präventivpolizeilichen Bereich regelmäßig nicht grundrechtlich geboten seien. Zusätzliche Einhegungen und Strukturierungen der nachrichtendienstlichen Tätigkeit ergäben sich außerdem aus den einschlägigen Dienstvorschriften. Steuerung und Kontrolle des Bundesnachrichtendienstes seien durch das Auftragsprofil der Bundesregierung und das Zusammenspiel der verschiedenen Kontrollorgane, insbesondere durch die stark ausgebaute Fachaufsicht beim Bundeskanzleramt, gewährleistet.

2. Die Bayerische Staatsregierung hebt die sicherheitspolitische Bedeutung der Ausland-Ausland-Fernmeldeaufklärung hervor und unterstützt mit ergänzendem Rechtsvortrag die Argumentation der Bundesregierung zur mangelnden Grundrechtsberechtigung von Ausländern im Ausland. Das Grundgesetz habe ausweislich seiner Präambel nicht den Anspruch, eine Weltordnung zu errichten, sondern beschränke seine Geltung grundsätzlich auf das deutsche Volk und das Gebiet der Bundesrepublik. Zudem differenziere das Grundgesetz ausdrücklich zwischen den als vorstaatlich zu denkenden universalen Menschenrechten (Art. 1 Abs. 2 GG) und den „nachfolgenden Grundrechten“. Die Menschenwürde sei als unveräußerliche Grundlage beiden Festlegungen vorgezogen, was ein abgestuftes Konzept der Grundrechtswirkungen außerhalb der Bundesrepublik systematisch nahelege. Schließlich sei es Aufgabe der jeweiligen ausländischen Rechtsordnungen, die Personen auf ihrem Staatsgebiet vor einer gegebenenfalls nach den dortigen Maßstäben rechtswidrigen Überwachung durch andere Staaten zu schützen, was vor den dortigen Gerichten mit den jeweils zu Gebot stehenden Rechtsbehelfen geltend zu machen sei. Jedenfalls sei die Verfassungsbeschwerde unbegründet, so dass sie keinen Anlass gebe, die Frage der Grundrechtsberechtigung abschließend zu klären. Aufgrund des automatisierten und gerade nicht individualisierten Charakters der Maßnahmen sei bereits der Eingriffscharakter der strategischen Fernmeldeaufklärung zweifelhaft, jedenfalls aber von relativ geringem Gewicht. Für diese eher geringfügigen Eingriffe bildeten die angegriffenen Regelungen eine hinreichende Rechtsgrundlage. 50

3. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit bemängelt – ebenso wie seine Amtsvorgängerin – insbesondere die unzureichende Umsetzung verfassungsrechtlicher Kontrollvorgaben in der Praxis. Es gebe teilweise ungeklärte und gespaltene Zuständigkeiten, es fehlten Sanktionsmöglichkeiten und es mangele an Austauschmöglichkeiten mit anderen Kontrollorganen. Auch bestünden unzureichende proaktive Informationspflichten und große Wissensasymmetrien ge- 51

genüber dem Bundesnachrichtendienst. In Bezug auf im Ausland von anderen Diensten erlangte Daten sei eine Datenschutzkontrolle oftmals unmöglich, da der Bundesnachrichtendienst den Zugriff auf diese Daten unter Berufung auf die „Third Party Rule“ verwehre. Auch sei es in der Praxis dazu gekommen, dass Beanstandungen des Bundesdatenschutzbeauftragten übergangen worden seien, ohne dass Möglichkeiten bestanden hätten, sie zumindest an die Öffentlichkeit zu bringen.

Auch in der Sache bestünden gegenüber den angegriffenen Regelungen erhebliche Bedenken, insbesondere mit Blick auf deren gesetzliche Bestimmtheit. Konkret fehle es etwa an einer Pflicht zur stetigen Anpassung der Filtersysteme an den jeweiligen Stand der Technik. Ebenfalls sei das Regime objektiver und unabhängiger Kontrolle insgesamt unzureichend und insbesondere nicht dazu geeignet, den aufgrund der Geheimheit der Maßnahmen in Ermangelung von Benachrichtigungspflichten faktisch fehlenden gerichtlichen Rechtsschutz zu ersetzen. 52

4. Der für das Sicherheitsrecht zuständige 6. Revisionssenat des Bundesverwaltungsgerichts erklärt, mit den angegriffenen Vorschriften noch nicht unmittelbar befasst gewesen zu sein. Lediglich im Rahmen des rechtlichen Vorgehens gegen die in der Vergangenheit beim Bundesnachrichtendienst geführte VERAS-Datei habe sich der Senat mittelbar mit den §§ 6 ff. BNDG befasst und insbesondere klargestellt, dass Daten aus der Ausland-Ausland-Fernmeldeaufklärung wegen des Ausschlusses durch § 6 Abs. 4, § 10 Abs. 4 BNDG für die auch Inländer betreffende VERAS-Datei nicht genutzt werden dürften. Eine Entscheidung über die im März 2018 beim Bundesverwaltungsgericht eingegangene Klage der DE-CIX Management GmbH gegen eine Anordnung nach § 8 BNDG sei noch nicht absehbar. 53

IV.

Im Vorfeld der mündlichen Verhandlung haben in Antwort auf einen Fragen-katalog des Bundesverfassungsgerichts zu den technischen Gegebenheiten internationaler Telekommunikationsnetze sowie zu den Möglichkeiten und Dimensionen der Aufklärungsarbeit des Bundesnachrichtendienstes schriftliche Stellungnahmen abgegeben: die Bundesregierung, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, der eco-Verband der Internetwirtschaft e.V., die T-Systems International GmbH und der Chaos Computer Club e.V. 54

In der mündlichen Verhandlung haben sich geäußert: die Beschwerdeführerinnen und Beschwerdeführer, die Bundesregierung, der Bundesnachrichtendienst, das Parlamentarische Kontrollgremium, die G10-Kommission und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Als Sachverständige haben der ehemalige IT-Sicherheitsbeauftragte der Bundesregierung Martin Schallbruch und der Barrister und Queen’s Counsel Dr. Tom Hickman, Standing Counsel beim britischen Investigatory Powers Commissioner’s Office, ausgesagt. Als Sachkundige Dritte wurden die ehemalige Vorsitzende des Unabhängigen Gremiums Richterin am Bundesgerichtshof Gabriele Cirener, der eco – Verband der Internetwirtschaft e.V., die T-Systems International GmbH und der Chaos Computer Club e.V. angehört. 55

B.

Die Verfassungsbeschwerde ist zulässig. 56

I.

Die Beschwerdeführerinnen und Beschwerdeführer wenden sich mit ihrer Rechtssatzverfassungsbeschwerde gegen Überwachungs- und Übermittlungs- befugnisse des Bundesnachrichtendienstes für die Ausland-Ausland-Fernmeldeaufklärung. Unmittelbar richten sich ihre Angriffe gegen die die Behörde jeweils ermächtigenden Befugnisnormen, mittelbar aber auch gegen die weiteren Regelungen, mit denen der Gesetzgeber diese Befugnisse zur Gewährleistung ihrer Verhältnismäßigkeit flankiert und ohne die ihre Verfassungsmäßigkeit nicht beurteilt werden kann. Bei verständiger Auslegung der Verfassungsbeschwerde erstrecken sich ihre Angriffe damit unmittelbar zunächst auf §§ 6, 7 und §§ 13 bis 15 BNDG, wobei zur Beurteilung dieser Normen insbesondere auch die §§ 9 bis 11 und §§ 16, 20, 22, 32, 32a BNDG in die Prüfung einzubeziehen sind; in der Sache wird damit über deren Anwendbarkeit und verfassungsrechtliche Tragfähigkeit als Ausgestaltung der angegriffenen Befugnisse mitentschieden. Darüber hinaus wenden sich die Beschwerdeführer gegen § 19 Abs. 1 und § 24 BNDG einschließlich der insoweit in Bezug genommenen weiteren Vorschriften, soweit sie auf den Umgang mit den aus der strategischen Überwachung nach §§ 6, 7, 13 bis 15 BNDG stammenden Daten Anwendung finden. 57

II.

Die Beschwerdeführerinnen und Beschwerdeführer sind beschwerdebefugt. 58

1. Die Beschwerdeführerinnen und Beschwerdeführer rügen eine Verletzung ihrer Grundrechte aus Art. 10 Abs. 1, Art. 5 Abs. 1 Satz 2 und Art. 3 Abs. 1 GG. Sie machen geltend, dass die angegriffenen Vorschriften ihnen gegenüber Telekommunikationsüberwachungen ermöglichten und damit in ihr Grundrecht auf Wahrung des Telekommunikationsgeheimnisses eingriffen. Dabei legen sie näher dar, dass das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG keine Beachtung gefunden habe und die Vorschriften auch den Anforderungen der Verhältnismäßigkeit in verschiedener Hinsicht nicht genügten. Die Beschwerdeführer zu 1) bis 7) berufen sich weiter auf eine Verletzung ihres Grundrechts der Pressefreiheit aus Art. 5 Abs. 1 Satz 2 GG, da die Überwachungsmaßnahmen auch gegen sie als Journalisten gerichtet werden könnten und insoweit keine Schutzvorkehrungen getroffen seien. Darüber hinaus wenden sich die Beschwerdeführerin zu 1) als in der Europäischen Union ansässige juristische Person des Privatrechts sowie die Beschwerdeführer zu 3) und 5) als Unionsbürger dagegen, von solchen Überwachungsmaßnahmen nicht in gleicher Weise ausgenommen zu sein wie deutsche Staatsangehörige und Inländer. Sie sehen hierin einen Verstoß gegen Art. 3 Abs. 1 GG. 59

Mit diesem Vorbringen sind – bezogen auf den sachlichen Schutzgehalt – mögliche Grundrechtsverletzungen substantiiert geltend gemacht. Das gilt nicht nur in Bezug auf die Datenerhebung, sondern auch in Bezug auf die Datenverwendung und -über- 60

mittlung, die als eigene Grundrechtseingriffe an den Grundrechten zu messen sind, die für die Datenerhebung einschlägig waren (vgl. BVerfGE 100, 313 <359 f.; 391>; 141, 220 <327 Rn. 285>; stRspr).

2. Eine Beschwerdebefugnis ist für die Beschwerdeführerinnen und Beschwerdeführer zu 1) bis 7) auch nicht deshalb zu verneinen, weil sie sich als ausländische juristische Person oder als im Ausland lebende Ausländer auf die Grundrechte des Grundgesetzes berufen. Ob und wieweit sich Staatsangehörige anderer Staaten gegenüber Maßnahmen der deutschen Staatsgewalt auch im Ausland auf die Grundrechte des Grundgesetzes berufen können, ist bisher nicht abschließend geklärt. In seiner Entscheidung vom 14. Juli 1999 hat das Bundesverfassungsgericht dies weder positiv beantwortet noch ausgeschlossen (vgl. BVerfGE 100, 313 <362 ff.>). Damit erscheint eine Grundrechtsverletzung jedenfalls möglich. 61

3. Zu verneinen ist die Beschwerdebefugnis auch nicht für die Beschwerdeführerin zu 1), weil sie eine juristische Person mit Sitz im Ausland ist. Die Beschwerdeführerin legt insoweit hinreichend dar, dass für sie jedenfalls möglicherweise die Anwendungserweiterung des Grundrechtsschutzes auf juristische Personen aus der Europäischen Union zur Geltung kommt (a). Auch liegen die Voraussetzungen der wesensmäßigen Anwendbarkeit nach Art. 19 Abs. 3 GG für die geltend gemachten Grundrechte vor (b). 62

a) Veranlasst durch die Europäischen Verträge erkennt die Rechtsprechung des Bundesverfassungsgerichts die Möglichkeit einer Anwendungserweiterung des Grundrechtsschutzes auf juristische Personen aus der Europäischen Union an. Juristische Personen mit Sitz im EU-Ausland werden grundrechtlich ebenso behandelt wie inländische juristische Personen, wenn die betroffene juristische Person aus der Europäischen Union im Anwendungsbereich des Unionsrechts tätig wird und sie einen hinreichenden Inlandsbezug aufweist, der die Geltung der Grundrechte in gleicher Weise wie für inländische juristische Personen geboten erscheinen lässt (vgl. BVerfGE 129, 78 <94 ff.>). 63

Danach kommt eine Erweiterung des Grundrechtsschutzes auf die Beschwerdeführerin als ausländische juristische Person zumindest in Betracht. Ein schutzbedarfsbegründender Inlandsbezug der Beschwerdeführerin zu 1) kann sich vorliegend daraus ergeben, dass die angegriffenen Vorschriften eine Überwachung vom Inland aus ermöglichen und zudem ein Interesse deutscher Behörden an der Auslandstätigkeit überwachter Personen zur Geltung bringen; damit rückt auch die Beschwerdeführerin spezifisch in deren Aufklärungsfokus. 64

Auch unterfällt die Tätigkeit der Beschwerdeführerin im Sinne der genannten Anwendungserweiterung möglicherweise dem Anwendungsbereich des Unionsrechts. In Betracht kommt dies etwa deshalb, weil die Beschwerdeführerin durch die Entgegennahme grenzüberschreitender Dienstleistungen in Ausübung ihrer durch Art. 56 AEUV gewährleisteten passiven Dienstleistungsfreiheit von ihren primärrechtlich gewährleisteten Grundfreiheiten Gebrauch macht. Allerdings fällt insbesondere die na- 65

tionale Sicherheit nach Art. 4 Abs. 2 Satz 3 EUV weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten, so dass ein Tätigwerden im Anwendungsbereich des Unionsrechts jedenfalls im Hinblick auf Teile des Aufgabenprofils des Bundesnachrichtendienstes ausgeschlossen sein könnte. Ob und wieweit das der Fall ist, ist auch unionsrechtlich noch nicht geklärt (vgl. Vorabentscheidungsersuchen des Investigatory Powers Tribunal London [Vereinigtes Königreich], eingereicht am 31. Oktober 2017, Privacy International, C-623/17, ABl EU 2018/C 022/41; Vorabentscheidungsersuchen des Conseil d'État [Frankreich], eingereicht am 3. August 2018, La Quadrature du Net u.a., C-511/18, ABl EU 2018/C 392/10 und French Data Network u.a., C-512/18, ABl EU 2018/C 392/11 zur Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation – Datenschutzrichtlinie für elektronische Kommunikation –, (ABl EU 2002/L 201/37, im Folgenden: RL 2002/58/EG).

Ob oder wieweit nach alledem der Anwendungsbereich des Unionsrechts tatsächlich eröffnet ist, bedarf für die Frage der Zulässigkeit der Verfassungs- beschwerde keiner Entscheidung. Denn die Beschwerdeführerin zu 1) hat jedenfalls die Möglichkeit einer Verletzung eines für sie verfassungsbeschwerdefähigen Rechts aufgezeigt (vgl. BVerfGE 125, 39 <73>; 129, 78 <91>). Einer Vorlage an den Europäischen Gerichtshof nach Art. 267 Abs. 3 AEUV bedarf es nicht, da die Verfassungsbeschwerde danach jedenfalls zulässig ist; die Frage ist auch für die Begründetheit nicht entscheidungserheblich (unten Rn. 328). 66

b) Die von Art. 19 Abs. 3 GG vorausgesetzte wesensmäßige Anwendbarkeit der geltend gemachten Grundrechte auf juristische Personen ist für Art. 10 Abs. 1 GG, Art. 5 Abs. 1 Satz 2 GG und Art. 3 Abs. 1 GG gegeben (vgl. zu Art. 10 Abs. 1 GG: BVerfGE 100, 313 <356>; 106, 28 <43>; zu Art. 5 Abs. 1 Satz 2 GG: BVerfGE 80, 124 <131>; 95, 28 <34>; 113, 63 <75>; zu Art. 3 Abs. 1 GG: BVerfGE 21, 362 <369>; 42, 374 <383>; 53, 336 <345>). 67

4. Die Beschwerdebefugnis der Beschwerdeführer zu 6) und 8) wird auch nicht dadurch ausgeschlossen, dass sie Funktionsträger ausländischer juristischer Personen sind, die nach Art. 19 Abs. 3 GG selbst nicht grundrechtsberechtigt sind. 68

Personen, die geltend machen, in ihren eigenen Grundrechten verletzt zu sein, sind nicht deshalb vom Grundrechtsschutz des Grundgesetzes ausgeschlossen, weil sie als Funktionsträger einer ausländischen juristischen Person handeln (zutreffend Hölscheidt, Jura 2017, S. 148 <153>; anders dagegen Ziffern 2.4.5, 3.2.6 der Dienstvorschrift nach § 6 Abs. 7 BNDG für die strategische Fernmeldeaufklärung des BND vom 7. März 2019 [DV SIGINT]; Karl/Soiné, NJW 2017, S. 919 <920>; Dietrich, in: Schenke/Graulich/Ruthig [Hrsg.], Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 6 BNDG Rn. 8 für Funktionsträger juristischer Personen mit hoheitlichen Aufgaben). Zwar können Funktionsträger nur eigene Grundrechte geltend machen, nicht aber als Sachwalter Grundrechte der juristischen Personen, für die sie handeln. Soweit sie 69

jedoch in eigenen Grundrechten betroffen sind, entfällt ihr Schutz nicht deswegen, weil sie Funktionsträger einer ausländischen juristischen Person sind, die sich ihrerseits nach Art. 19 Abs. 3 GG nicht auf die Grundrechte des Grundgesetzes berufen kann (vgl. Hölscheidt, Jura 2017, S. 148 <153>). Das gilt auch, wenn hierdurch der von ihnen geltend gemachte Schutz im Einzelfall zugleich reflexhaft der juristischen Person zugutekommt. Eine Zurücknahme des jeder Person als Individuum zugesagten Grundrechtsschutzes ist insbesondere nicht geboten, um eine Aushöhlung des Art. 19 Abs. 3 GG zu vermeiden. Art. 19 Abs. 3 GG hat nicht die Aufgabe sicherzustellen, dass gegenüber ausländischen juristischen Personen unbegrenzt hoheitliche Maßnahmen ergriffen werden können, sondern zielt auf eine Erweiterung des individuellen Grundrechtsschutzes auf juristische Personen. Wenn diese Erweiterung auf juristische Personen des Inlands beschränkt bleibt, nimmt das den umfassenden Grundrechtsschutz natürlicher Personen nicht zurück.

Danach sind auch die Beschwerdeführer zu 6) und 8) beschwerdebefugt. Sie berufen sich wie die anderen Beschwerdeführer auf eine Verletzung ihrer Grundrechte aus Art. 10 Abs. 1 GG durch eine heimliche Überwachung ihrer Telekommunikation auf der Grundlage der angegriffenen Vorschriften. Das Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG wahrt als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts und des Rechts am eigenen Wort die Vertraulichkeit individueller Kommunikation als solche (vgl. BVerfGE 106, 28 <35 ff.>; Hermes, in: Dreier, GG, Bd. 1, 3. Aufl. 2013, Art. 10 Rn. 15, 18). Es dient dabei nicht vorrangig dem materiellen Geheimnisschutz, sondern unabhängig von ihrem Inhalt, ihren Umständen oder ihrer Funktion dem Schutz der individuellen Kommunikationsteilnehmer (vgl. BVerfGE 100, 313 <357>; 106, 28 <35 ff.>; siehe auch BVerfG, Beschluss der 3. Kammer des Ersten Senats vom 19. Dezember 1991 - 1 BvR 382/85 -, NJW 1992, S. 815 <816>). In Frage stehen damit eigene Grundrechte der Beschwerdeführer, deren Anwendbarkeit durch die Funktionen, die sie für juristische Personen wahrnehmen, nicht berührt wird. Entsprechendes gilt auch für den Beschwerdeführer zu 6), soweit dieser eine Verletzung des Art. 5 Abs. 1 Satz 2 GG rügt. Auch er beruft sich auf Grundrechtsschutz, der ihm als Journalisten durch Art. 5 Abs. 1 Satz 2 GG unmittelbar als Person zugesagt ist, unabhängig davon, ob er dabei für ein Presseunternehmen oder eine sonstige Organisation tätig ist (vgl. BVerfGE 117, 244 <258 ff.>). 70

III.

Die Beschwerdeführerinnen und Beschwerdeführer sind durch die angegriffenen Vorschriften unmittelbar, selbst und gegenwärtig betroffen. Ihre Verfassungsbeschwerde erfüllt damit die Anforderungen für Verfassungsbeschwerden unmittelbar gegen ein Gesetz. 71

1. Den Beschwerdeführerinnen und Beschwerdeführern fehlt es nicht an einer unmittelbaren Betroffenheit. Zwar bedürfen die angegriffenen Befugnisse der Umsetzung durch weitere Vollzugsakte. Von einer unmittelbaren Betroffenheit durch ein 72

vollziehungsbedürftiges Gesetz ist jedoch auch dann auszugehen, wenn ein Beschwerdeführer den Rechtsweg nicht beschreiten kann, weil er keine Kenntnis von der Maßnahme erlangt, oder wenn eine nachträgliche Bekanntgabe zwar vorgesehen ist, von ihr aber aufgrund weitreichender Ausnahmetatbestände auch langfristig abgesehen werden kann (BVerfGE 150, 309 <324 Rn. 35> m.w.N.; stRspr). Die durch die angegriffenen Vorschriften ermöglichten Überwachungsmaßnahmen werden grundsätzlich heimlich durchgeführt. Nachträgliche Benachrichtigungspflichten sind gesetzlich nur für den Fall des § 10 Abs. 4 Satz 2 BNDG normiert, der die Beschwerdeführerinnen und Beschwerdeführer zu 1) bis 7) als ausländische Staatsangehörige nicht betrifft und der auch dem Beschwerdeführer zu 8) allenfalls in Ausnahmefällen zugutekommt, nämlich wenn eine Mitteilung nicht sogar endgültig unterbleibt (§ 10 Abs. 4 Satz 5 BNDG). Auch die Möglichkeit, nach § 22 BNDG in Verbindung mit § 15 BVerfSchG auf Antrag Auskunft über die nach § 19 BNDG über ihre Person gespeicherten Daten zu erhalten, lässt die Unmittelbarkeit der Beschwer nicht entfallen, da diese Vorschriften nicht gewährleisten, dass die Betroffenen von der Überwachung Kenntnis erlangen (vgl. BVerfGE 150, 309 <324 f. Rn. 36>). Keine Kenntnis erhalten die Betroffenen in der Regel auch von der weiteren Nutzung oder Übermittlung der Daten, die durch die angegriffenen Vorschriften erlaubt werden. Die Beschwerdeführer sind deswegen nicht darauf zu verweisen, Vollzugsakte abzuwarten und gegen sie vorzugehen.

2. Die Beschwerdeführerinnen und Beschwerdeführer sind durch die angegriffenen Vorschriften auch selbst und gegenwärtig betroffen. 73

a) Sie legen dar, dass sie wegen ihrer Betätigung als Journalisten, als Bürger- und Menschenrechtsaktivisten beziehungsweise als Rechtsanwalt im Ausland mit hinreichender Wahrscheinlichkeit durch Maßnahmen der Ausland-Ausland-Aufklärung betroffen sind. Sie berufen sich darauf, im Rahmen ihrer Tätigkeit wiederholt mit oftmals verdeckt bleibenden Informanten zu kommunizieren, an denen und deren Kenntnissen auch der Bundesnachrichtendienst angesichts seiner Aufgaben naheliegenderweise ein erhebliches Interesse habe. Angesichts der Streubreite der durch die angegriffenen Vorschriften eröffneten Maßnahmen, die nicht von vornherein auf einen begrenzten Personenkreis zugeschnitten sind, ist eine hinreichende Wahrscheinlichkeit ihrer gegenwärtigen Betroffenheit in eigenen Rechten dargetan (vgl. BVerfGE 109, 279 <307 f.>; 113, 348 <363 f.>; 133, 277 <312 f. Rn. 86 f.>; 141, 220 <262 Rn. 84>). In Ansehung der bewusst offen gestalteten Ermächtigung, die eine flexible Anpassung an die außen- und sicherheitspolitischen Informationsbedürfnisse der Bundesregierung ermöglichen soll, ist eine Berührung der Tätigkeitsbereiche der Beschwerdeführer nicht fernliegend. Angesichts der verdachts- losen und geheim gehaltenen Fernmeldeüberwachung und den ebenfalls im Verborgenen stattfindenden Folgemaßnahmen kann ihnen eine weitere Konkretisierung des Vortrags nicht abverlangt werden (vgl. BVerfGE 100, 313 <356>). 74

b) Auch der Beschwerdeführer zu 8) ist als deutscher Staatsangehöriger selbst und gegenwärtig betroffen. Zwar ist eine Erhebung von Daten aus Telekommunikations- 75

verkehren von deutschen Staatsangehörigen, von inländischen juristischen Personen oder von sich im Bundesgebiet aufhaltenden Personen nach § 6 Abs. 4 BNDG unzulässig. Schon der Gesetzgeber geht jedoch ausweislich der in § 10 Abs. 4 BNDG getroffenen Regelung davon aus, dass die Filterung eine Aussonderung der Kommunikation solcher Personen nicht immer gewährleistet und es im Einzelfall zu Datenerhebungen entgegen § 6 Abs. 4 BNDG kommen kann. Auch die Bundesregierung hat ausgeführt, dass erfasste Telekommunikationsverkehre gegebenenfalls erst aufgrund einer individuellen Kenntnisnahme durch Mitarbeiter des Bundesnachrichtendienstes als Kommunikation zwischen Deutschen oder Inländern erkannt werden können. In dieser Kenntnisnahme liegt ein Grundrechtseingriff (vgl. BVerfGE 150, 244 <266 Rn. 45>).

Unabhängig davon ergibt sich eine gegenwärtige Selbstbetroffenheit jedenfalls daraus, dass dem Beschwerdeführer zu 8) nach der in den Dienstvorschriften niedergelegten Rechtsauffassung des Bundesnachrichtendienstes auch als Deutschem gegenüber den durch die angegriffenen Vorschriften ermöglichten Überwachungsmaßnahmen vorliegend kein Grundrechtsschutz – und damit auch nicht der Schutz des § 6 Abs. 4 BNDG – zuzuerkennen sein soll. Da er sich in seiner Funktion als Rechtsanwalt für ein guatemaltekisches Menschenrechtsbüro gegen die Überwachung wendet, sieht ihn der Bundesnachrichtendienst, wie von der Bundesregierung vorgetragen, als Funktionsträger einer ausländischen juristischen Person an, der sich als solcher nicht auf die Grundrechte des Grundgesetzes berufen könne. Der Beschwerdeführer, der sich im Auftrag dieses Büros mit Themen- feldern befasst, die verschiedene Berührungspunkte zu möglichen Erkenntnisinteressen des Bundesnachrichtendienstes aufweisen, ist damit von den angegriffenen Vorschriften in gleicher Weise betroffen wie die Beschwerdeführer zu 1) bis 7). 76

IV.

Die Verfassungsbeschwerde genügt den Anforderungen der Subsidiarität. 77

1. Nach dem Grundsatz der Subsidiarität sind auch vor der Erhebung von Rechtssatzverfassungsbeschwerden grundsätzlich alle Mittel zu ergreifen, die der geltend gemachten Grundrechtsverletzung abhelfen können. Zu den insoweit zumutbaren Rechtsbehelfen kann gegebenenfalls die Erhebung einer Feststellungs- oder Unterlassungsklage gehören, die eine fachgerichtliche Klärung entscheidungserheblicher Tatsachen- oder Rechtsfragen des einfachen Rechts ermöglicht (vgl. grundlegend zuletzt BVerfGE 150, 309 <326 ff. Rn. 41 ff.> m.w.N.). Anders liegt dies jedoch, soweit es allein um die sich unmittelbar aus der Verfassung ergebenden Grenzen für die Auslegung der Normen geht. Soweit die Beurteilung einer Norm allein spezifisch verfassungsrechtliche Fragen aufwirft, die das Bundesverfassungsgericht zu beantworten hat, ohne dass von einer vorausgegangenen fachgericht- lichen Prüfung verbesserte Entscheidungsgrundlagen zu erwarten wären, bedarf es einer vorangehenden fachgerichtlichen Entscheidung nicht (vgl. BVerfGE 123, 148 <172 f.>; 143, 246 <322 Rn. 211>; stRspr). Insoweit bleibt es dabei, dass Verfassungsbeschwerden un- 78

mittelbar gegen ein Gesetz weithin auch ohne vorherige Anrufung der Fachgerichte zulässig sind (vgl. BVerfGE 150, 309 <326 f. Rn. 44>).

2. Danach mussten die Beschwerdeführerinnen und Beschwerdeführer hier nicht zunächst fachgerichtlichen Rechtsschutz suchen. Die unmittelbar gegen Normen des Gesetzes über den Bundesnachrichtendienst gerichtete Verfassungsbeschwerde wirft im Kern allein spezifisch verfassungsrechtliche Fragen auf, die das Bundesverfassungsgericht zu beantworten hat, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung substantiell verbesserte Entscheidungs- grundlagen zu erwarten wären. Dies gilt ohnehin für die im vorliegenden Verfahren zentrale Frage, ob sich die Beschwerdeführer als Ausländer im Ausland hinsichtlich der Überwachungsmaßnahmen überhaupt auf die Grundrechte des Grundgesetzes stützen können. Das gilt aber auch für die Prüfung der angegriffenen Vorschriften im Einzelnen. Ihre verfassungsrechtliche Beurteilung hängt nicht an der näheren fachrechtlichen Auslegung der einzelnen Tatbestandsmerkmale der angegriffenen Eingriffsgrundlagen, sondern an der verfassungsrechtlichen Tragfähigkeit der strategischen Telekommunikationsüberwachung als solcher und ihrer hinreichenden Eingrenzung wie Bestimmtheit. Für die Vorschriften zur Datenerhebung und Datenverarbeitung stellt sich dies nicht anders dar als für die Vorschriften zu den Kooperationen mit anderen Diensten. Auch hinsichtlich der Vorschriften zur Datenübermittlung entscheidet sich die verfassungsrechtliche Beurteilung maßgeblich nicht an Details der Auslegung, sondern danach, ob diese als solche in einer Weise gesetzlich ausgestaltet sind, die den verfassungsrechtlichen Anforderungen genügt. 79

Im Übrigen wäre nach dem derzeitigen Stand der verwaltungsgerichtlichen Rechtsprechung diesbezüglich Rechtsschutz auch praktisch nicht zu erreichen. Das Bundesverwaltungsgericht hat Klagen hinsichtlich der strategischen Fernmelde- aufklärung für unzulässig erklärt, da der Kläger jeweils kein hinreichend konkretes Vorgehen des Bundesnachrichtendienstes habe bezeichnen können (vgl. BVerwGE 157, 8 <12 f. Rn. 16 ff.>; 161, 76 <78 Rn. 14>); es ist nicht ersichtlich, dass die Beschwerdeführer diese Anforderungen hier hätten erfüllen können. 80

V.

Die Verfassungsbeschwerde wahrt schließlich die Beschwerdefrist des § 93 Abs. 3 BVerfGG. 81

1. Die am 19. Dezember 2017 erhobene Verfassungsbeschwerde wahrt die gesetzliche Jahresfrist, soweit sie sich gegen Bestimmungen richtet, mit denen der Bundesgesetzgeber die Befugnisse des Bundesnachrichtendienstes zur Ausland-Ausland-Fernmeldeaufklärung und zur Kooperation im Rahmen der Ausland- Ausland-Fernmeldeaufklärung erstmals gesetzlich geregelt hat. Die diesbezüglichen Bestimmungen der §§ 6 ff. und der §§ 13 ff. BNDG sind nach Art. 5 des Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23. Dezember 2016 am Tag nach der Verkündung des Gesetzes, also am 31. Dezember 2016, in Kraft getreten. Dass der Gesetzgeber bei der Neuregelung an eine be- 82

stehende Aufklärungspraxis des Bundesnachrichtendienstes angeknüpft hat, führt nicht zu einer Vorverlagerung des Fristbeginns. Denn Gegenstand der Verfassungsbeschwerde sind nicht konkrete Vollzugsakte des Bundesnachrichtendienstes, für die die Fristenregelung des § 93 Abs. 1 Satz 1 BVerfGG gilt; sie richtet sich vielmehr gegen die gesetzliche Ermächtigung zur Durchführung der Ausland-Ausland-Fernmeldeaufklärung als solche, für die die Beschwerdefrist des § 93 Abs. 3 BVerfGG nicht vor Inkrafttreten des Gesetzes beginnt.

2. Auch im Hinblick auf § 19 Abs. 1 BNDG und § 24 Abs. 1 bis 3 BNDG, die die Befugnisse des Bundesnachrichtendienstes zur Speicherung, Veränderung und Nutzung beziehungsweise zur Übermittlung personenbezogener Daten regeln, ist die Beschwerdefrist des § 93 Abs. 3 BVerfGG gewahrt. Durch das Inkrafttreten der §§ 6 ff. und der §§ 13 ff. BNDG wurde der Anwendungsbereich dieser allgemeinen Übermittlungs- und Verarbeitungsbefugnisse auf die neu geregelten Maßnahmen erstreckt und so teilweise erweitert. Darin liegt eine neue grundrechtliche Beschwer, für welche die Beschwerdefrist neu in Gang gesetzt wird (vgl. BVerfGE 45, 104 <119>; 100, 313 <356>; 141, 220 <262 f. Rn. 85>; stRspr). 83

VI.

Da es sich bei der Auslandsfernmeldeaufklärung jedenfalls nicht um die Umsetzung zwingenden Unionsrechts handelt, richtet sich die verfassungsrechtliche Beurteilung der Gültigkeit der angegriffenen Vorschriften nach den Grundrechten des Grundgesetzes. Damit ist die Zuständigkeit des Bundesverfassungsgerichts eröffnet und die Verfassungsbeschwerde insoweit zulässig. Das gilt unabhängig davon, ob daneben Unionsgrundrechte Geltung beanspruchen können (vgl. BVerfG, Beschluss des Ersten Senats vom 6. November 2019 - 1 BvR 16/13 -, Rn. 39 – Recht auf Vergessen I). 84

Unberührt bleibt hiervon die Frage, ob sich weitere rechtliche Anforderungen unmittelbar aus dem Sekundärrecht der Europäischen Union ergeben, insbesondere aus Art. 15 Abs. 1 RL 2002/58/EG hinsichtlich der Reichweite der den Telekommunikationsanbietern auferlegten Pflichten. Die Auslegung und Anwendung des Fachrechts der Europäischen Union ist nicht Sache des Bundesverfassungsgerichts, sondern obliegt den Fachgerichten im Verbund mit dem Europäischen Gerichtshof (vgl. BVerfGE 148, 40 <48 f. Rn. 22>). 85

C.

Die Verfassungsbeschwerde ist begründet. Die angegriffenen Vorschriften sind an den Grundrechten des Grundgesetzes zu messen und greifen in Art. 10 Abs. 1 und Art. 5 Abs. 1 Satz 2 GG ein (I bis III). Die Eingriffe sind nicht gerechtfertigt, weil die angegriffenen Vorschriften formell verfassungswidrig sind (unten D). Sie genügen auch nicht zentralen materiellen Anforderungen des Art. 10 Abs. 1 und des Art. 5 Abs. 1 Satz 2 GG (unten E). 86

I.

Die Grundrechte des Grundgesetzes binden den Bundesnachrichtendienst und den seine Befugnisse regelnden Gesetzgeber unabhängig davon, ob der Dienst im Inland oder im Ausland tätig ist. Der Schutz der Art. 10 Abs. 1 und Art. 5 Abs. 1 Satz 2 GG gilt auch gegenüber einer Telekommunikationsüberwachung von Ausländern im Ausland. 87

1. Art. 1 Abs. 3 GG begründet eine umfassende Bindung der deutschen Staatsgewalt an die Grundrechte des Grundgesetzes. Einschränkende Anforderungen, die die Grundrechtsbindung von einem territorialen Bezug zum Bundesgebiet oder der Ausübung spezifischer Hoheitsbefugnisse abhängig machen, lassen sich der Vorschrift nicht entnehmen. Das gilt jedenfalls für die Grundrechte als Abwehrrechte gegenüber Überwachungsmaßnahmen, wie sie hier in Frage stehen. 88

a) Nach Art. 1 Abs. 3 GG binden die Grundrechte Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht. Eine Beschränkung auf das Staatsgebiet enthält die Vorschrift nicht. Für das Handeln deutscher Staatsorgane im Ausland kann eine Ausnahme von der Grundrechtsgeltung auch nicht aus einem dahingehenden unausgesprochen konsentierten Grundverständnis bei Entstehung des Grundgesetzes hergeleitet werden (a.A. Hecker, in: Dietrich/Eiffler [Hrsg.], Handbuch des Rechts der Nachrichtendienste, 2017, III § 2 Rn. 46; Löffelmann, in: Dietrich/Eiffler [Hrsg.], Handbuch des Rechts der Nachrichtendienste, 2017, VI § 3 Rn. 15). Art. 1 Abs. 3 GG zielte insbesondere in Reaktion auf die nationalsozialistische Gewalt- und Willkürherrschaft vielmehr auf eine umfassende, in der Menschenwürde wurzelnde Grundrechtsbindung und war bereits 1949 in die Überzeugung eingebettet, dass die Bundesrepublik in der internationalen Staatengemeinschaft ihren Platz als rechtsstaatlicher Partner finden müsse (vgl. Dreier, in: ders., GG, Bd. 1, 3. Aufl. 2013, Art. 1 Abs. 2 Rn. 3; ders., DVBl 1999, S. 667 <672 ff.>). Dies kommt schon in der Präambel sowie insbesondere in Art. 1 Abs. 2 GG und Art. 24 und 25 GG zum Ausdruck. Auch wenn die Grundrechtsbindung außerhalb des eigenen Staatsgebiets in den Beratungen zum Grundgesetz noch kein eigenes Thema war und insbesondere Überwachungsmaßnahmen gegenüber dem Ausland in den heute möglichen Formen jenseits der damaligen Vorstellungen lagen, lässt sich aus der Entstehungsgeschichte nicht ableiten, dass der Schutz der Grundrechte von vornherein an der Staatsgrenze enden sollte. Der Anspruch eines umfassenden, den Menschen in den Mittelpunkt stellenden Grundrechtsschutzes spricht vielmehr dafür, dass die Grundrechte immer dann schützen sollen, wenn der deutsche Staat handelt und damit potentiell Schutzbedarf auslösen kann – unabhängig davon, an welchem Ort und gegenüber wem. 89

b) Die Bindung an die Grundrechte nach Art. 1 Abs. 3 GG als individuelle Abwehrrechte beschränkt sich auch nicht auf Konstellationen, in denen der Staat den Betroffenen als mit dem Gewaltmonopol versehene Hoheitsmacht gegenübertritt (vgl. Hölscheidt, Jura 2017, S. 148 <150 f.>; a.A. Gärditz, Die Verwaltung 48 <2015>, S. 463 <474>; ders., DVBl 2017, S. 525 <526>; Hecker, in: Dietrich/Eiffler [Hrsg.], Handbuch 90

des Rechts der Nachrichtendienste, 2017, III § 2 Rn. 46; Löffelmann, in: Dietrich/ Eiffler [Hrsg.], Handbuch des Rechts der Nachrichtendienste, 2017, VI § 3 Rn. 15). Eine solche Beschränkung, die eine grundrechtliche Bindung der Auslandsaufklärung weitgehend ausschlösse, lässt sich insbesondere nicht daraus herleiten, dass Art. 1 Abs. 3 GG nicht auf die deutsche Staatsgewalt als solche verweist, sondern die Gesetzgebung, die vollziehende Gewalt und die Rechtsprechung als unterschiedene staatliche Funktionen benennt. Hierdurch wird die Grundrechtsbindung nicht beschränkt, sondern deutlich gemacht, dass der Grundrechtsschutz gegenüber allen der traditionellen Gewaltenteilungslehre bekannten Staatsgewalten gilt – insbesondere auch gegenüber dem Gesetzgeber, was damals nicht selbstverständlich war (vgl. Denninger, in: AK-GG, 2. Aufl. 1989, Art. 1 Abs. 2, 3 Rn. 17). Dieser Wille zur lückenlosen Grundrechtsbindung aller Zweige der staatlichen Gewalt (vgl. Herdegen, in: Maunz/Dürig, GG, Art. 1 Abs. 3 Rn. 12 [Oktober 2019]) lag bereits dem ursprünglichen Normwortlaut zugrunde, der mit „Gesetzgebung, Verwaltung und Rechtsprechung“ die drei klassischen Gewalten auf die Grundrechte als unmittelbar geltendes Recht verpflichtete. Mit der Ersetzung des Begriffs der „Verwaltung“ durch den Begriff der „vollziehenden Gewalt“ durch das Gesetz zur Änderung des Grundgesetzes vom 19. März 1956 (BGBl I S. 111) war keine Einengung der Grundrechtsbindung auf die Ausübung spezifisch hoheitlicher Befugnisse intendiert. Vielmehr wurde der Begriff 1956 im Rahmen der Grundgesetznovelle zur Wehrverfassung als gegenüber dem ursprünglichen Begriff der „Verwaltung“ weiter angesehen und an dessen Stelle gesetzt, um klarzustellen, dass auch die Bundeswehr auf die Grundrechte verpflichtet ist (BTDrucks 2/2150, S. 2). Eine Beschränkung der Grundrechtsbindung auf Entscheidungen, die die Exekutive auch mit Hoheitsbefugnissen durchsetzen könnte, liegt hierin nicht.

Die Grundrechte binden die staatliche Gewalt vielmehr umfassend und ins- gesamt, unabhängig von bestimmten Funktionen, Handlungsformen oder Gegenständen staatlicher Aufgabenwahrnehmung (vgl. Hölscheidt, Jura 2017, S. 148 <150 f.>). Das Verständnis der staatlichen Gewalt ist dabei weit zu fassen und erstreckt sich nicht nur auf imperative Maßnahmen oder solche, die durch Hoheitsbefugnisse unterlegt sind. Alle Entscheidungen, die auf den jeweiligen staatlichen Entscheidungsebenen den Anspruch erheben können, autorisiert im Namen aller Bürgerinnen und Bürger getroffen zu werden, sind von der Grundrechtsbindung erfasst. Eingeschlossen sind hiervon Maßnahmen, Äußerungen und Handlungen hoheitlicher wie nicht hoheitlicher Art. Grundrechtsgebundene staatliche Gewalt im Sinne des Art. 1 Abs. 3 GG ist danach jedes Handeln staatlicher Organe oder Organisationen, weil es in Wahrnehmung ihres dem Gemeinwohl verpflichteten Auftrags erfolgt (BVerfGE 128, 226 <244>). Die Bindung an die Grundrechte und die politische Entscheidungsverantwortung sind unhintergehbar miteinander verknüpft (vgl. BVerfG, Beschluss des Ersten Senats vom 6. November 2019 - 1 BvR 16/13 -, Rn. 42 – Recht auf Vergessen I). 91

c) Die Grundrechtsbindung der deutschen Staatsgewalt beschränkt sich dabei auch im Ausland nicht auf eine bloß objektivrechtliche Verpflichtung (zutreffend Hölscheidt, 92

Jura 2017, S. 148 <150 f.>; a.A. Löffelmann, in: Dietrich/Gärditz/Graulich/Gusy/Warg [Hrsg.], Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 33 <38>). Sie korrespondiert vielmehr mit einer Grundrechtsberechtigung derjenigen, die durch die jeweiligen Grundrechtsgarantien als geschützte Grundrechtsträger ausgewiesen sind. Eine Grundrechtsbindung zugunsten individueller Grundrechtsträger, der dann aber keinerlei subjektivrechtliche Entsprechung gegenübersteht, sieht das Grundgesetz nicht vor. Der Charakter als Individualrecht gehört zum zentralen Gehalt des grundgesetzlichen Grundrechtsschutzes.

2. Die Grundrechtsbindung der deutschen Staatsgewalt auch bei einem Handeln gegenüber Ausländern im Ausland entspricht zugleich der Einbindung der Bundesrepublik in die internationale Staatengemeinschaft. 93

a) In Art. 1 Abs. 2 GG bekennt sich das Grundgesetz zu den unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt. Die Grundrechte des Grundgesetzes werden so in den Zusammenhang internationaler Menschenrechtsgewährleistungen gestellt, die über die Staatsgrenzen hinweg auf einen Schutz abzielen, der dem Menschen als Menschen gilt. Entsprechend schließen Art. 1 Abs. 2 und Art. 1 Abs. 3 GG an die Menschenwürdegarantie des Art. 1 Abs. 1 GG an. In Anknüpfung an diese im Ansatz universalistische Einbindung des Grundrechtsschutzes trifft das Grundgesetz für die positivrechtliche Ausgestaltung der Grundrechte im Einzelnen bewusst eine Unterscheidung zwischen Deutschen- rechten und Menschenrechten. Das legt aber nicht nahe, auch die Menschenrechte auf innerstaatliche Sachverhalte oder auf staatliches Handeln im Inland zu begrenzen. Ein solches Verständnis findet auch im Wortlaut des Grundgesetzes keinen Anhaltspunkt. Insbesondere ergibt sich eine solche Begrenzung nicht aus der Präambel des Grundgesetzes, die mit der Bezugnahme auf das „Deutsche Volk in den Ländern“ nicht gebietsbezogen, sondern aus der Perspektive der verfassungsgebenden Akteure formuliert ist und die Verantwortung des Deutschen Volkes in einem vereinten Europa und der Welt betont (vgl. Jarass, in: Jarass/Pieroth, GG, 15. Aufl. 2018, Präambel Rn. 9, Art. 1 Rn. 44; Kahl, in: Bonner Kommentar, GG, Art. 1 Abs. 3 Rn. 199 f. [2014]; Murswiek, in: Bonner Kommentar, GG, Präambel Rn. 306 [2005]; a.A. Löffelmann, in: Dietrich/Eiffler [Hrsg.], Handbuch des Rechts der Nachrichtendienste, 2017, VI § 3 Rn. 15). 94

Gegen eine Einbindung der Grundrechte in den Zusammenhang universell geltender Menschenrechte spricht auch nicht die terminologische Unterscheidung zwischen „unverletzlichen und unveräußerlichen Menschenrechten“ nach Art. 1 Abs. 2 GG und den „nachfolgenden Grundrechten“ in Art. 1 Abs. 3 GG. Auch insoweit lassen Wortlaut und Systematik des Grundgesetzes keinen Anhaltspunkt für eine gebietsbezogene Deutung der Unterscheidung im Sinne getrennter räumlicher Anwendungsbereiche erkennen. Dass die Grundrechte des Grundgesetzes (Art. 1 Abs. 3 GG) im Gegenteil mit der Gewährleistung der Menschenrechte verknüpft sind, zeigt auch die ständige Rechtsprechung des Bundesverfassungsgerichts, nach der die Grundrechte des Grundgesetzes im Lichte der internationalen Menschenrechtsver- 95

bürgungen auszulegen sind (vgl. BVerfGE 111, 307 <317 f.>; 128, 282 <306 f.>; 128, 326 <367 f.>; 142, 313 <345 Rn. 88>; 148, 296 <351 Rn. 128>; BVerfG, Beschluss des Ersten Senats vom 6. November 2019 - 1 BvR 16/13 -, Rn. 58 – Recht auf Vergessen I). Auch bilden die in Art. 1 Abs. 2 GG niedergelegten Grundsätze im Sinne des Art. 79 Abs. 3 GG eine absolute Grenze für Einschränkungen des Grundrechtsschutzes durch den verfassungsändernden Gesetzgeber (vgl. BVerfGE 84, 90 <120 f.>; 141, 1 <15 Rn. 34>).

Mit dieser Verknüpfung der Grundrechte und der Gewährleistung der Menschenrechte wäre ein Verständnis der Grundrechte des Grundgesetzes, das deren Geltung an der Staatsgrenze enden lässt und deutsche Stellen gegenüber Ausländern im Ausland von ihrer Verpflichtung auf die Grund- und Menschenrechte entbindet, nicht vereinbar. Der Anspruch des Grundgesetzes, auf der Grundlage internationaler Konventionen im Zusammenwirken über die Staatsgrenzen hinweg unveräußerliche Rechte einer jeden Person – einschließlich des Schutzes vor Überwachung (vgl. Art. 12 AEMR; Art. 17 Abs. 1 IPbpR) – sicherzustellen, würde damit konterkariert. Unter den Bedingungen der Internationalisierung politischer Handlungsbedingungen und eines zunehmenden Engagements der Staaten auch jenseits der eigenen Grenzen müsste dies dazu führen, dass der Grundrechtsschutz des Grundgesetzes einem erweiterten Handlungsradius der deutschen Staats- gewalt nicht folgen und – im Gegenteil – im Zusammenwirken der Staaten gegebenenfalls sogar unterlaufen werden könnte. Demgegenüber gewährleistet die Anknüpfung der Grundrechtsbindung an den Staat als politisch legitimiertes und rückgebundenes Handlungssubjekt, dass der Grundrechtsschutz auch einer internationalen Ausweitung staatlicher Aktivitäten folgt. 96

b) Ein solches Verständnis der Reichweite der Grundrechte des Grundgesetzes ist auch durch die Europäische Menschenrechtskonvention nahegelegt, die bei der Auslegung der Grundrechte als Auslegungshilfe heranzuziehen ist (vgl. BVerfG, Beschluss des Ersten Senats vom 6. November 2019 - 1 BvR 16/13 -, Rn. 58 m.w.N. – Recht auf Vergessen I). Wieweit deren Gewährleistungen für das Handeln der Konventionsstaaten außerhalb ihres Territoriums gelten, ist zwar noch nicht umfassend geklärt. Der Europäische Gerichtshof für Menschenrechte orientiert sich hierfür maßgeblich an dem Kriterium der effektiven Kontrolle („effective control“) über das Handeln auf fremdem Territorium und hat auf dieser Grundlage in vielen Fällen eine Auslandsgeltung der Konventionsrechte anerkannt (vgl. zusammenfassend EGMR [GK], Al-Skeini and others v. United Kingdom, Urteil vom 7. Juli 2011, Nr. 55721/07, §§ 132 ff. m.w.N.; vgl. auch Aust, AVR 52 <2014>, S. 375 <394 ff.> m.w.N.). Für die Frage nach dem Schutz vor Überwachungsmaßnahmen durch Konventionsstaaten in anderen Staaten liegt allerdings noch keine letztverbindliche Klärung vor. 97

Die 1. Kammer des Europäischen Gerichtshofs für Menschenrechte hat jedoch die Durchführung von Überwachungsmaßnahmen mit Zielen im Ausland in einer noch nicht rechtskräftigen Entscheidung uneingeschränkt an der Konvention gemessen und für konventionswidrig befunden, wobei zu den Beschwerdeführern auch ausländ- 98

dische Staatsangehörige gehörten, die sich nicht im Konventionsstaat aufhielten oder dort wohnhaft waren (vgl. EGMR, Big Brother Watch and others v. United Kingdom, Urteil vom 13. September 2018, Nr. 58170/13 u.a., § 271). Desgleichen wurden die auslandsbezogenen und die Inlandskommunikation ausschließenden strategischen Überwachungsbefugnisse nach schwedischem Recht, die von einer schwedischen Nichtregierungsorganisation angegriffen worden waren, ohne Infragestellung der Auslandsgeltung anhand der Konvention überprüft (vgl. EGMR, Centrum för Rättvisa v. Sweden, Urteil vom 19. Juni 2018, Nr. 35252/08). Beide Verfahren sind nunmehr vor der Großen Kammer anhängig.

Unabhängig von dem Ausgang dieser Verfahren steht die Europäische Menschenrechtskonvention einer Auslandsgeltung der deutschen Grundrechte jedenfalls nicht entgegen. Denn als völkerrechtlicher Vertrag hat sie einen eigenständig definierten Anwendungsbereich, aus dem sich für die Reichweite des Grundrechtsschutzes nach dem Grundgesetz ohnehin keine unmittelbaren Ableitungen ergeben können. Sie schließt einen weitergehenden Grundrechtsschutz durch die Konventionsstaaten jedenfalls nicht aus (Art. 53 EMRK). 99

c) Der Grundrechtsbindung der deutschen Staatsgewalt im Ausland steht auch nicht entgegen, dass hier eine Abgrenzung zu anderen Staaten und Rechts- ordnungen oder eine Abstimmung mit diesen erforderlich wäre, wie es das Bundesverfassungsgericht als – einzigen – möglichen Grund für einen Ausschluss der Bindung an Art. 10 GG bei Auslandssachverhalten erwogen und offengelassen hatte (vgl. BVerfGE 100, 313 <362 ff.>). 100

Die Bindung an die deutschen Grundrechte begründet nur eine Verantwortlichkeit und Verantwortung deutscher Staatsorgane. Sie flankiert allein autonome politische Entscheidungen der Bundesrepublik Deutschland und begrenzt ausschließlich eigene Handlungsspielräume. Entsprechend wirken die Grundrechte als Abwehrrechte auch im Ausland nur gegenüber der deutschen Staatsgewalt und laufen damit parallel zu den durch das völkerrechtliche Interventionsverbot begründeten Beschränkungen. In der Grundrechtsbindung liegt damit weder ein Verstoß gegen das völkerrechtliche Interventionsverbot, noch beschränkt sie die Handlungs- oder Rechtsetzungsmacht anderer Staaten. Sie bewirkt weder einen Oktroi eigenen Rechts noch eine Verdrängung ausländischer Grundrechte. Insbesondere erweitert die Grundrechtsbindung nicht staatliche Befugnisse im Ausland, sondern beschränkt nur potentiell von der deutschen Staatsgewalt in Anspruch genommene Handlungsmöglichkeiten. 101

Dementsprechend wirkt die Geltung der Grundrechte (hier des Art. 10 Abs. 1 GG) nicht auf die Rechtsordnung anderer Staaten ein und entfalten auch hieran anknüpfende Eingriffsermächtigungen für Überwachungsmaßnahmen für deren interne Rechtsordnung keine normative Wirkung. Aus der Geltung der Grundrechte und dem Gesetzesvorbehalt folgen lediglich, dass für deutsche Stellen entsprechende Rechtsgrundlagen geschaffen werden müssen, sofern Überwachungsmaßnahmen auch auf 102

Ausländer im Ausland bezogen werden sollen. Ob und wieweit solche Befugnisse tatsächlich geschaffen werden und von ihnen Gebrauch gemacht wird, ist damit nicht vorgegeben. Insoweit ist auch über die Rechtfertigung von Einzelmaßnahmen aufgrund solcher Befugnisse hinsichtlich ihrer Außenwirkung gegenüber dem jeweiligen Zielstaat nichts gesagt.

Aus der Grundrechtsbindung als solcher folgt damit nichts für die Frage, ob solche Maßnahmen völkerrechtlich zulässig sind. Erst recht sind andere Staaten nicht gehindert, sich gegen diese Maßnahmen auf ihrem Gebiet zur Wehr zu setzen – so wie das nach deutschem Verfassungsrecht auch gegen Überwachungsmaßnahmen ausländischer Dienste im Inland geboten sein kann (unten Rn. 249). In der Bindung der deutschen Staatsgewalt an die Grundrechte liegt insoweit keine Belastung anderer Staaten, die völkerrechtliche Bedenken begründen könnte (vgl. Bäcker, KuR 2014, S. 556 <561>; Becker, NVwZ 2015, S. 1335 <1339>; Gärditz, Die Verwaltung 48 <2015>, S. 463 <472 f.>). Dementsprechend ist es international nicht unüblich, Rechtsgrundlagen für auch auf Ausländer im Ausland bezogene Überwachungsmaßnahmen zu schaffen. Sie haben allein eine innerstaatliche Ermächtigungsfunktion (vgl. Gusy, in: Schenke/Graulich/Ruthig [Hrsg.], Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 1 BNDG Rn. 56; z.B. für die USA: Section 702 Foreign Intelligence Surveillance Act; vgl. Renan, in: Goldman/Rascoff [Hrsg.], Global Intelligence Oversight, 2016, S. 121 <123 ff.>; für das Vereinigte Königreich bis 2017: Section 8 [4] Regulation of Investigatory Powers Act; für das Vereinigte Königreich seit 2017: Part 6 Chapter 1 Investigatory Powers Act 2016; vgl. Leigh, in: Dietrich/Sule [Hrsg.], Intelligence Law and Policies in Europe, 2019, S. 553 ff.; McKay/Walker, in: Dietrich/Gärditz/Graulich/Gusy/Warg [Hrsg.], Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 119 ff.; für Frankreich: Article L854-1 bis L854-9 Code de la sécurité intérieure [Des mesures de surveillance des communications électroniques internationales]; vgl. Le Divelec, in: Dietrich/Sule [Hrsg.], Intelligence Law and Policies in Europe, 2019, 516 ff.; Warusfel, in: Dietrich/Gärditz/Graulich/Gusy/Warg [Hrsg.], Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 129 ff.). 103

3. Die umfassende Bindung der deutschen Staatsgewalt an die Grundrechte lässt unberührt, dass sich die aus den Grundrechten konkret folgenden Schutz- wirkungen danach unterscheiden können, unter welchen Umständen sie zur Anwendung kommen. Das gilt – wie schon für die verschiedenen Wirkungsdimensionen der Grundrechte im Inland – auch für die Reichweite ihrer Schutzwirkung im Ausland. So mögen schon hinsichtlich des persönlichen und sachlichen Schutz- bereichs einzelne Gewährleistungen im Inland und Ausland in unterschiedlichem Umfang Geltung beanspruchen (unten Rn. 196). Ebenso kann zwischen verschiedenen Grundrechtsdimensionen, etwa der Wirkung der Grundrechte als Abwehrrechte, als Leistungsrechte, als verfassungsrechtliche Wertentscheidungen oder als Grundlage von Schutzpflichten zu unterscheiden sein. Soweit die Grundrechte auf Konkretisierungen des Gesetzgebers angewiesen sind, kann auch insoweit den besonderen Bedin- 104

gungen im Ausland Rechnung zu tragen sein (vgl. BVerfGE 92, 26 <41 ff.>; dazu auch BVerfGE 100, 313 <363>). Erst recht ist der Einbindung staatlichen Handelns in ein ausländisches Umfeld bei der Bestimmung von Anforderungen an die Rechtfertigung von Grundrechtseingriffen – insbesondere im Rahmen der Verhältnismäßigkeit – Rechnung zu tragen.

4. Vorliegend geht es um den Schutz vor Überwachungsmaßnahmen im Rahmen der Auslandsfernmeldeaufklärung durch die von den Beschwerdeführerinnen und Beschwerdeführern als verletzt gerügten Grundrechte der Art. 10 Abs. 1 und Art. 5 Abs. 1 Satz 2 GG in ihrer Abwehrdimension. Aus der grundsätzlich umfassenden Grundrechtsbindung der deutschen Staatsgewalt folgt, wie sich aus den vorstehenden Darlegungen ergibt, jedenfalls insoweit eine Grundrechtsbindung auch des Bundesnachrichtendienstes und des Gesetzgebers bei der Regelung seiner Befugnisse. Eine Freistellung nachrichtendienstlicher Aufklärungsmaßnahmen von der Grundrechtsbindung wegen ihrer Auslandsgerichtetheit kennt das Grundgesetz ebensowenig wie wegen ihres politischen Charakters. Vielmehr schafft die umfassende Grundrechtsbindung nach Art. 1 Abs. 3 GG die Voraussetzungen dafür, auch Grundrechtsgefährdungen durch neue technische Entwicklungen und sich hierdurch ergebende Kräfteverschiebungen Rechnung tragen zu können. Das gilt insbesondere für die sich wandelnde Bedeutung der Nachrichtendienste im Zuge der Fortentwicklung der Informationstechnik und des hiermit möglich gewordenen Ausgriffs auf das Ausland. 105

a) Die nachrichtendienstliche Auslandsaufklärung hat für die Handlungsfähigkeit der Bundesrepublik Deutschland in der Außen- und Sicherheitspolitik seit jeher eine erhebliche, in jüngerer Zeit aber spezifisch gewachsene Bedeutung gewonnen. Im Zuge der Entwicklung der Informationstechnik und der Internationalisierung haben sich Bedeutung und Bedingungen der Auslandsfernmeldeaufklärung als eines zentralen Elements der nachrichtendienstlichen Auslandsaufklärung grund- legend geändert. 106

Früher zielte die Fernmeldeaufklärung allein auf die Gefahrenfrüherkennung zur Abwehr bewaffneter Angriffe auf das Bundesgebiet und beschränkten sich unmittelbar personenbezogene Maßnahmen sowohl von den technischen Möglichkeiten als auch vom Erkenntnisinteresse her auf einen kleinen Kreis von Personen (vgl. BVerfGE 67, 157 <178>). Im Zuge der heutigen Kommunikationsmöglichkeiten und damit verbunden der internationalisierten Handlungszusammenhänge haben sich potentiell aus dem Ausland drohende Gefahren vervielfältigt. Die Informations- technik erlaubt, über Grenzen hinweg unmittelbar und ungehindert durch räumliche Distanzen miteinander zu kommunizieren und sich ohne Zeitverlust zu koordinieren. Hierdurch stellen sich neue Herausforderungen für die Erfassung politisch oder militärisch relevanter Kommunikation, die für die Handlungsfähigkeit der Bundes- regierung von erheblicher Bedeutung sein kann. Auch können internationale Aktivitäten heute für das Gemeinwesen insgesamt destabilisierende Wirkung entfalten, wie exemplarisch in Cyberangriffen, international organisierter Kriminalität wie etwa Men- 107

schenhandel oder Geldwäsche und internationalem Terrorismus sichtbar wird (vgl. Kojm, in: Goldman/Rascoff [Hrsg.], Global Intelligence Oversight, 2016, S. 95 ff.; Goodman/Ischebeck-Baum, in: Dietrich/Sule [Hrsg.], Intelligence Law and Policies in Europe, 2019, S. 1 <Rn. 104 ff.>; Rosand, Journal of Conflict & Security Law 11 <2006>, S. 399 <400 f.>; hinsichtlich des Gefahrenbereichs „Cyber“ siehe auch BT-Drucks 18/4654, S. 40 f.). Der Auslandsaufklärung mittels Telekommunikationsüberwachung kommt damit außen- und sicherheitspolitisch eine zunehmende Bedeutung zu, die politisch etwa auch in den im Vergleich zu vielen anderen Bereichen deutlich gestiegenen Haushaltsansätzen der Nachrichtendienste ihren Ausdruck findet (vgl. die Verdoppelung des veranschlagten Budgets des Bundesnachrichtendienstes von 475,5 Millionen Euro im Jahr 2011 [vgl. Haushaltsrechnung des Bundes für das Jahr 2011, S. 185] auf 966,5 Millionen Euro im Jahr 2019 [vgl. Haushaltsgesetz 2019 vom 17. Dezember 2018, BGBl I S. 2528, Einzelplan 04, S. 22], während im gleichen Zeitraum das Gesamtbudget von 306,8 Milliarden Euro [vgl. Haushaltsrechnung des Bundes für das Jahr 2011, S. 14] auf 356,4 Milliarden Euro [vgl. Haushaltsgesetz 2019 vom 17. Dezember 2018, BGBl I S. 2528, Gesamtplan, S. 16] um 16 Prozent anstieg).

b) Die unter veränderten Bedingungen zunehmende Bedeutung der Auslandsaufklärung geht im Spannungsfeld von Freiheit und Sicherheit mit neuen Herausforderungen nicht nur für die Wahrung der Sicherheit, sondern auch für die Wahrung der Freiheit einher, die rechtsstaatlich auf der Basis der Grundrechte ausbalanciert werden muss. 108

Mit den Entwicklungen der Informationstechnik verbindet sich, dass die Datenströme über Satelliten und durch Kabel volatil nach von Staatsgrenzen unabhängigen technischen Kriterien weltweit geführt werden (vgl. zu dieser Entwicklung bereits BT-Drucks 14/5655, S. 17). Dadurch ist es möglich, auch vom Inland aus in erheblichem Umfang Auslandskommunikation zu erfassen. Gleichzeitig vollzieht sich gesellschaftliche Kommunikation zunehmend in internationalen Zusammenhängen. Auf der Grundlage grenzüberschreitender Dienstleistungsangebote stützt sich der Austausch zwischen Bürgerinnen und Bürgern als Grundrechtsträgern – innerhalb der Staaten wie über die Staatsgrenzen hinaus – weitgehend auf Telekommunikationsdienstleistungen, die nicht nach der Unterscheidung zwischen Inland und Ausland strukturiert sind (vgl. Kojm, in: Goldman/Rascoff [Hrsg.], Global Intelligence Oversight, 2016, S. 95 <100 f.>). Vor dem Hintergrund, dass sich unter den gegenwärtigen Bedingungen der Informationstechnik zunehmend Handlungen und Kommunikationsbeziehungen aller Art in digitaler Form niederschlagen, und angesichts ständig steigender Datenverarbeitungskapazitäten erstrecken sich die Möglichkeiten der Telekommunikationsüberwachung so auf breite Bereiche der gesamten Zivilgesellschaft auch außerhalb des eigenen Hoheitsgebiets – so wie umgekehrt die Inlandskommunikation auch der Überwachung durch andere Staaten ausgesetzt ist (vgl. BTDrucks 18/12850, S. 1283 ff.). 109

Ein Verständnis der Grundrechte, das deren Geltung an den Staatsgrenzen enden ließe, stellte die Grundrechtsträger angesichts solcher Entwicklungen schutzlos und ließe die Reichweite des Grundrechtsschutzes hinter die Bedingungen der Internationalisierung zurückfallen (vgl. Becker, NVwZ 2015, S. 1335 <1339>; Papier, NVwZ 2017, S. 3025 <3029>; Marxsen, DÖV 2018, S. 218 <226>). Es könnte dazu führen, dass der Grundrechtsschutz in einem zunehmend wichtiger werdenden Bereich eingriffsintensiven staatlichen Handelns und – mit dem Sicherheitsrecht – in einem Feld, in dem den Grundrechten zudem typischerweise besondere Bedeutung zukommt, leerliefe. Indem Art. 1 Abs. 3 GG an den Staat als Handlungssubjekt anknüpft, trägt er demgegenüber auch solchen neuen Gefährdungspotentialen Rechnung und hilft, sie in den allgemeinen rechtsstaatlichen Rahmen des Grundgesetzes einzuordnen. 110

II.

1. Die angegriffenen Vorschriften berühren die Beschwerdeführerinnen und Beschwerdeführer in ihren Grundrechten aus Art. 10 Abs. 1 und Art. 5 Abs. 1 Satz 2 GG. Sie ermächtigen zur Erhebung personenbezogener Daten im Wege der heimlichen Telekommunikationsüberwachung und betreffen damit den Gewährleistungsgehalt des durch Art. 10 Abs. 1 GG geschützten Telekommunikationsgeheimnisses. Hieran anknüpfend berührt auch die Übermittlung der aus solchen Maßnahmen erlangten Daten den Schutz des Telekommunikationsgeheimnisses, so dass auch sie an Art. 10 GG zu messen ist. Ebenfalls berühren die angegriffenen Vorschriften die als Journalisten tätigen Beschwerdeführer in ihrem Grundrecht aus Art. 5 Abs. 1 Satz 2 GG. Denn sie ermächtigen den Bundesnachrichtendienst zur Erhebung, Verarbeitung und Übermittlung von Daten aus Telekommunikation im Rahmen ihrer beruflichen Tätigkeit einschließlich der gezielten Überwachung und Auswertung ihrer in diesem Zusammenhang geführten Kommunikation etwa mit Informanten (vgl. EGMR, Weber and Saravia v. Germany, Entscheidung vom 29. Juni 2006, Nr. 54934/00, §§ 143 ff.; Big Brother Watch and others v. United Kingdom, Urteil vom 13. September 2018, Nr. 58170/13 u.a., §§ 476, 490 ff.; siehe auch BVerfGE 100, 313 <365>). 111

2. Nicht zu klären ist in vorliegendem Verfahren, ob die angegriffenen Vorschriften in Blick auf die Unterscheidung von Deutschen und Unionsbürgern mit Gleichheitsanforderungen vereinbar sind. Offenbleiben muss insoweit insbesondere, ob § 6 Abs. 3 BNDG, auch in Verbindung mit § 14 Abs. 2 BNDG, diesbezüglich eine sachlich gerechtfertigte Differenzierung schafft. Denn die Frage der Gleichbehandlung von deutschen Staatsangehörigen und Unionsbürgern findet nicht nur Maßstäbe im Grundgesetz, sondern wirft zugleich ungeklärte Fragen des Unionsrechts auf; hierzu gehören zunächst schon dessen Anwendbarkeit in Anbetracht des Art. 4 Abs. 2 EUV und der Grundfreiheiten sowie dann gegebenenfalls die inhaltliche Reichweite des unionsrechtlichen Diskriminierungsverbots (vgl. Kreuter/Möbius, BWV 2009, S. 146 <148>; Hölscheidt, Jura 2017, S. 148 <156>; Marxsen, DÖV 2018, S. 218 <224>; vgl. auch die anhängigen Verfahren vor dem EuGH, Privacy International, C-623/17, ABl EU 2018/C 022/41 [Vereinigtes Königreich]; La Quadrature du Net u.a., C-511/18, ABl EU 2018/C 392/10 und French Data Network u.a., C-512/18, ABl EU 2018/C 392/11 112

[jeweils Frankreich]). Eine abschließende Klärung der Frage, welchen Gleichheitsanforderungen der Gesetzgeber bei einer Gestaltung der strategischen Überwachung unterliegt, ist dem Bundesverfassungsgericht damit allein nicht möglich. Es kann diese Frage mangels Entscheidungs- erheblichkeit auch nicht dem Europäischen Gerichtshof vorlegen, da die angegriffenen Vorschriften schon aus formellen Gründen verfassungswidrig sind (unten Rn. 134 f.). Unter diesen Umständen bedarf es vorliegend auch keiner weiteren materiellen Klärung dieser Fragen anhand des Grundgesetzes.

III.

Die angegriffenen Vorschriften begründen Grundrechtseingriffe auf verschiedenen Stufen. 113

1. § 6 Abs. 1 BNDG berechtigt den Bundesnachrichtendienst zunächst zur Erfassung individueller Telekommunikationsverkehre aus durch Anordnung näher bestimmten Netzen; eröffnet werden damit insbesondere das Abfangen von Satellitensignalen und die Erfassung leitungsgebundener Datenströme, und zwar sowohl mittels eigener Vorrichtungen als auch einer nach § 8 BNDG angeordneten Ausleitung. Entsprechend ermächtigt § 14 Abs. 1 BNDG den Bundesnachrichtendienst zur Erhebung personenbezogener Daten im Rahmen von Kooperationen mit ausländischen Nachrichtendiensten. 114

a) Gegenüber den Beschwerdeführerinnen und Beschwerdeführern zu 1) bis 7) als im Ausland lebenden ausländischen Staatsangehörigen liegt in einer solchen Erfassung ein Eingriff. Es handelt sich bei einer solchen Erfassung personenbezogener Daten im verfassungsrechtlichen Sinne um eine Datenerhebung. Sie macht die Daten der Betroffenen dem Bundesnachrichtendienst gezielt zugänglich, damit dieser sie nach inhaltlichen Kriterien auswerten kann – sei es auf der Grundlage von Suchbegriffen zur Erfassung von Inhaltsdaten, sei es zur Auswertung von (möglicherweise bevorratend akkumulierten) Verkehrsdaten oder sei es zur Übermittlung an ausländische öffentliche Stellen im Rahmen einer Kooperation. Die später wieder ausgesonderten Daten werden dabei auch nicht nur ungewollt miterfasst, sondern bewusst erhoben, um auf relevante Erkenntnisse hin ausgewertet und gegebenenfalls genutzt zu werden (vgl. hierzu auch BVerfGE 100, 313 <366>). 115

b) Gegenüber dem Beschwerdeführer zu 8), der deutscher Staatsangehöriger ist, gilt das im Ergebnis angesichts des derzeitigen Stands der Technik ebenfalls. Da § 6 Abs. 4 BNDG (gegebenenfalls in Verbindung mit § 14 Abs. 2 BNDG) Überwachungsmaßnahmen gegenüber deutschen Staatsangehörigen und Inländern nicht erlaubt, liegt in der anfänglichen Erfassung auch ihrer Daten zwar grundsätzlich kein Eingriff. Diese Daten werden lediglich ungezielt und allein technisch bedingt miterfasst und sollen unmittelbar nach der Signalaufbereitung mittels verschiedener Filterungsprozesse technisch spurenlos wieder aussortiert werden. Das behördliche Interesse an den erfassten Daten hat sich hier nicht derart verdichtet, dass ein Betroffensein in einer einen Grundrechtseingriff auslösenden Qualität anzunehmen ist (vgl. BVerfGE 116

100, 313 <366>; 115, 320 <343>; 150, 244 <266 Rn. 43>).

Allerdings ist nach dem derzeitigen Stand der Technik eine Herausfilterung der Daten von deutschen Staatsangehörigen und Inländern nicht vollständig möglich, so dass teilweise auch solche Daten in die Auswertung gelangen. Aussortiert werden sie dann erst bei Identifizierung im Rahmen der händischen Sichtung. § 6 Abs. 1, Abs. 4 BNDG erlaubt dies zwar nicht in klar erkennbarer Weise, setzt ein solches Verständnis jedoch, um überhaupt angewendet werden zu können, voraus; so wird die Vorschrift denn seit jeher auch in der Praxis verstanden. In Bezug auf Personen, deren Daten auf diese Weise erfasst werden, ohne nach der Signalaufbereitung technisch wieder spurenlos ausgesondert zu werden, und die damit von Mitarbeitern des Bundesnachrichtendienstes zur Kenntnis genommen werden, begründet dies einen Eingriff. Indem § 6 Abs. 1, Abs. 4 BNDG hierfür die Rechtsgrundlage bietet, liegt in ihm auch gegenüber dem Beschwerdeführer zu 8) die Ermächtigung zu Eingriffen in sein Grundrecht aus Art. 10 Abs. 1 GG. 117

2. Weitere Grundrechtseingriffe gegenüber den Beschwerdeführerinnen und Beschwerdeführern begründet § 6 Abs. 1 bis 3 BNDG durch die Ermächtigung zur weiteren Auswertung der Daten. Zum einen ermächtigen § 6 Abs. 1 BNDG und in dem dort geregelten Umfang auch § 14 Abs. 1 BNDG in Verbindung mit § 19 Abs. 1 BNDG zu einem Eingriff in Form der Auswertung der erhobenen, gegebenenfalls auch bevorratend akkumulierten Telekommunikationsverkehrsdaten. Zum anderen ermächtigt § 6 Abs. 1 bis 3 BNDG zur Auswertung der erfassten Telekommunikation mittels Suchbegriffen zur Sichtung der Inhaltsdaten. Weitere Eingriffe liegen in der von der Vorschrift gleichermaßen gedeckten händischen Auswertung der hierbei herausgefilterten Telekommunikationsverkehre, die die weitere Daten- verarbeitung – von der Sichtung der mittels Suchbegriffen aufgegriffenen Tele- kommunikationsverkehre über ihre Dekodierung und Meldung an die sogenannten „abnehmenden Bereiche“ bis hin zu ihrer dortigen Nutzung – umfasst. 118

3. Eigene Grundrechtseingriffe liegen in einer etwaigen Übermittlung der sich aus der Überwachung ergebenden Erkenntnisse, soweit sie personenbezogene Daten enthalten, wie sie § 24 BNDG in verschiedenen Einzeltatbeständen vorsieht. Hiermit werden die erlangten Daten anderen Behörden zugänglich gemacht, was stets einen eigenen Grundrechtseingriff bedeutet (vgl. BVerfGE 141, 220 <324 f. Rn. 279>). Entsprechend liegt auch in der automatisierten Übermittlung von Informationen an ausländische öffentliche Stellen, wie sie § 15 Abs. 1 BNDG im Rahmen von Kooperationen vorsieht, ein Grundrechtseingriff. 119

4. Eingriffe in Art. 10 Abs. 1 GG sowie gegebenenfalls in Art. 5 Abs. 1 Satz 2 GG begründet auch § 7 BNDG. Zwar regelt dieser nicht unmittelbar die Erhebung von Daten durch Überwachungsmaßnahmen selbst, sondern setzt sie voraus (vgl. Dietrich, in: Schenke/Graulich/Ruthig [Hrsg.], Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 7 BNDG Rn. 2; Marxsen, DÖV 2018, S. 218 <223>; Löffelmann, in: Dietrich/Gärditz/Graulich/Gusy/Warg [Hrsg.], Reform der Nachrichtendienste zwischen Verge- 120

setzlichung und Internationalisierung, 2019, S. 33 <39>). § 7 Abs. 1 BNDG rechtfertigt aber die weitere Verarbeitung der insoweit gewonnenen Daten, worin ein eigener Eingriff liegt (vgl. BVerfGE 100, 313 <366 f.>). Überdies regelt § 7 Abs. 2 BNDG Einschränkungen der Datenerhebung und schafft damit den Rechtsschein, dass eine Datenerhebung vom Ausland aus ohne weitere Rechtsgrundlage zulässig sei. Im Ergebnis will § 7 Abs. 1, 2 BNDG damit auch eine Datenerhebung des Bundesnachrichtendienstes vom Ausland aus legitimieren.

D.

Diese Grundrechtseingriffe sind verfassungsrechtlich nicht gerechtfertigt. Die zu ihnen ermächtigenden Vorschriften genügen bereits in formeller Hinsicht nicht den verfassungsrechtlichen Anforderungen an Ermächtigungen zum Eingriff in die betroffenen Grundrechte. Zwar können sie sich auf eine hinreichende Kompetenzgrundlage stützen. Sie verstoßen jedoch gegen das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG. 121

I.

Keine durchgreifenden verfassungsrechtlichen Bedenken bestehen hinsichtlich der Gesetzgebungskompetenz. Der Bundesgesetzgeber kann die angegriffenen Vorschriften auf Art. 73 Abs. 1 Nr. 1 GG stützen. 122

1. Maßgebliche Kompetenzgrundlage ist Art. 73 Abs. 1 Nr. 1 GG, der eine Gesetzgebungskompetenz des Bundes über die auswärtigen Angelegenheiten sowie die Verteidigung begründet. 123

a) Die Einrichtung einer Stelle zur umfassenden Auslandsaufklärung fällt unstreitig unter die auswärtigen Angelegenheiten im Sinne von Art. 73 Abs. 1 Nr. 1 GG (vgl. BVerfGE 100, 313 <369>). Dazu zählt auch die Ausstattung mit aufgaben- adäquaten Befugnissen. Allerdings sind die Aufgaben, die der Gesetzgeber einer solchen Stelle übertragen kann, begrenzt. 124

aa) Der Begriff der auswärtigen Angelegenheiten in Art. 73 Abs. 1 Nr. 1 GG kann nicht ohne Rücksicht auf die Verteilung der Gesetzgebungskompetenzen im Übrigen bestimmt werden. Zum einen darf er nicht in einer Weise ausgelegt werden, dass die Kompetenzverteilung zwischen Bund und Ländern unterlaufen wird. Zum anderen muss er sich in die verschiedenen Kompetenzzuweisungen an den Bund einfügen. Unter beiden Gesichtspunkten verbietet sich ein Verständnis des Begriffs, nach dem alle Tatbestände mit Auslandsbezug zu den auswärtigen Angelegenheiten zählen. Darunter sind diejenigen Fragen zu verstehen, die für das Verhältnis der Bundesrepublik Deutschland zu anderen Staaten oder zwischenstaatlichen Einrichtungen, insbesondere für die Gestaltung der Außenpolitik, Bedeutung haben (vgl. BVerfGE 100, 313 <368 f.>; vgl. auch BVerfGE 133, 277 <319 Rn. 101>). 125

Abzugrenzen ist die Gesetzgebungskompetenz nach Art. 73 Abs. 1 Nr. 1 GG insbesondere von der Gesetzgebungskompetenz nach Art. 73 Abs. 1 Nr. 9a GG, der dem Bund für die Abwehr von Gefahren des internationalen Terrorismus eine Gesetzge- 126

bungskompetenz allein in Bezug auf das Bundeskriminalpolizeiamt einräumt. Im Grenzbereich zur Verbrechensbekämpfung ist weiter von Belang, dass Art. 73 Abs. 1 Nr. 10 GG dem Bund bestimmte und zugleich begrenzte Gesetz- gebungskompetenzen für die Zusammenarbeit zwischen Bund und Ländern im Bereich der Kriminalpolizei, für die Einrichtung eines Bundeskriminalpolizeiamtes sowie für die internationale Verbrechensbekämpfung zuweist. Darunter ist nicht die Bekämpfung internationaler Verbrechen zu verstehen, sondern die internationale Bekämpfung von Verbrechen, also etwa die Zusammenarbeit deutscher mit ausländischen Stellen in kriminalpolizeilichen Fragen. Im Übrigen fällt das Polizeirecht als Gefahrenabwehrrecht in die Zuständigkeit der Länder (vgl. BVerfGE 100, 313 <369>).

bb) Hieraus ergibt sich, dass der Bund den Bundesnachrichtendienst mit der Auslandsaufklärung nicht allgemein zum Zweck der Gewährleistung der inneren Sicherheit betrauen kann. Art. 73 Abs. 1 Nr. 1 GG berechtigt den Bundesgesetzgeber nicht dazu, Befugnisse einzuräumen, die auf die Verhütung, Verhinderung oder Verfolgung von Straftaten als solche gerichtet sind (vgl. BVerfGE 100, 313 <370>; 133, 277 <319 Rn. 101>). Dem Bundesnachrichtendienst können insoweit nur Aufgaben und Befugnisse übertragen werden, die eine außen- und sicherheitspolitische Bedeutung haben und damit eine internationale Dimension aufweisen. 127

Dies beschränkt den Bundesgesetzgeber umgekehrt allerdings nicht darauf, den Bundesnachrichtendienst allein mit der Aufgabe zu betrauen, die Bundesregierung mit Entscheidungsgrundlagen zur Sicherung ihrer außen- oder verteidigungspolitischen Handlungsfähigkeit zu versorgen (vgl. BVerfGE 100, 313 <368 ff.>). Zwar liegt hierin die primäre Aufgabe der Auslandsaufklärung, von der das Gesamtprofil des auf Art. 73 Abs. 1 Nr. 1 GG gestützten Dienstes auch geprägt bleiben muss. Jedoch kann dem Bundesnachrichtendienst als eigene Aufgabe auch die Früherkennung von aus dem Ausland drohenden Gefahren anvertraut werden, wenn diese eine hinreichend internationale Dimension aufweisen. Maßgeblich ist, dass es sich um Gefahren handelt, die sich ihrer Art und ihrem Gewicht nach auf die Stellung der Bundesrepublik in der Staatengemeinschaft auswirken können und gerade in diesem Sinne von außen- und sicherheitspolitischer Bedeutung sind. Zu denken ist hier etwa an Gefahren durch staatenübergreifend machtvoll agierende Netzwerke der organisierten Kriminalität, durch von außen gesteuerte Cyberangriffe auf wichtige Infrastruktur oder durch Terrorakte, die sich als Ausdruck international verflochtener Konfliktlagen darstellen. Demgegenüber umfasst die Kompetenz nicht die Schaffung von Regelungen zur Aufklärung einzelner, auch bedeutsamer Straftaten im Inland, allein weil sich hierfür Tatbeiträge oder Erkenntnisquellen im Ausland befinden. Auch könnte die Zuständigkeit des Bundesnachrichtendienstes etwa nicht generell auf die Aufklärung von Auslandsstraftaten nach § 6 StGB erstreckt werden. Dass hier die Tatbegehung im Ausland unter Strafe gestellt wird und solche Normen in internationale Vereinbarungen einbezogen sind, begründet für sich noch nicht, dass ihrer Aufklärung in jedem Fall eine außen- und sicherheitspolitische Bedeutung zukommt, die alleine dem Bund eine Gesetzgebungskompetenz nach Art. 73 Abs. 1 Nr. 1 GG eröffnet. 128

b) Die angegriffenen Vorschriften lassen sich danach auf die Gesetzgebungskompetenz des Art. 73 Abs. 1 Nr. 1 GG stützen. Dies gilt zunächst für § 6 BNDG. Zwar eröffnet § 6 Abs. 1 Nr. 1 BNDG den Einsatz der strategischen Überwachung nicht nur, um Gefahren für die äußere, sondern auch um Gefahren für die innere Sicherheit zu erkennen. Eingebunden ist dies jedoch in die alle Tatbestände übergreifende Beschränkung des § 6 BNDG auf die Aufgaben des Bundesnachrichtendienstes. Dies gilt für die Nummer 1 ebenso wie für die Nummer 2 und die Nummer 3 – und damit auch für das Auftragsprofil der Bundesregierung. Zulässig sind Überwachungsmaßnahmen nach § 6 Abs. 1 BNDG demnach nur zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung sind (§ 1 Abs. 2 BNDG). Das ist in Blick auf Art. 73 Abs. 1 Nr. 1 GG kompetenzrechtlich unbedenklich, setzt allerdings eine Auslegung und Hand- habung der Vorschrift voraus, die den dargelegten kompetenzrechtlichen Grenzen Rechnung trägt. Insbesondere können danach die Befugnisse nicht uneingeschränkt als Grundlage für Dienstleistungen für Behörden der inneren Sicherheit genutzt werden – auch nicht mittels Auftragserteilung durch die Bundesregierung. 129

Nichts anderes gilt für § 7 und §§ 13 bis 15 BNDG. Auch diese Vorschriften sind an die Aufgabenbestimmung des § 1 Abs. 2 BNDG gebunden und durch sie begrenzt. Dass §§ 13 bis 15 BNDG im Rahmen von Kooperationen auch eine Überwachung zur Gewinnung von Erkenntnissen im Interesse anderer Staaten eröffnet, ändert kompetenzrechtlich nichts. Die Zuordnung einer solchen Regelung zu den „auswärtigen Angelegenheiten“ steht hier erst recht außer Zweifel. 130

Die Zuständigkeit des Bundes zur Regelung auch der Übermittlung der aus den Überwachungsmaßnahmen gewonnenen Erkenntnisse durch § 24 BNDG ergibt sich kraft Sachzusammenhangs aus Art. 73 Abs. 1 Nr. 1 GG als der für die Datenerhebung geltenden Kompetenzgrundlage (vgl. BVerfGE 125, 260 <314>; 133, 277 <319 f. Rn. 101>). 131

2. Demgegenüber können die angegriffenen Vorschriften nicht auf andere Kompetenztitel gestützt werden. Das gilt insbesondere für Art. 73 Abs. 1 Nr. 10 GG und die dort geregelte Kompetenz des Bundes für die internationale Verbrechens- bekämpfung. 132

In Bezug auf die §§ 6, 7 BNDG scheidet dies schon deshalb aus, weil diese nicht die internationale Zusammenarbeit regeln (vgl. BVerfGE 100, 313 <368 f.>). Nichts anderes gilt aber auch für die §§ 13 bis 15 BNDG. Zwar haben diese Vorschriften Formen der internationalen Zusammenarbeit zum Gegenstand. Sie regeln jedoch nicht im Schwerpunkt die Koordination der Verbrechensbekämpfung, sondern eine Verbreiterung der Befugnisse des Bundesnachrichtendienstes zur Erhebung, Auswertung und Übermittlung von Daten, um damit Aufklärungsinteressen anderer Dienste aufgreifen zu können. Entsprechend hat sich auch der Bundes- gesetzgeber für die Schaffung der §§ 13 bis 15 BNDG allein auf Art. 73 Abs. 1 Nr. 1 GG berufen (vgl. BTDrucks 18/9041, S. 19). Offenbleiben kann damit die grundsätzliche Frage, 133

ob Art. 73 Abs. 1 Nr. 10 GG dem Bund die Befugnis zur Regelung der internationalen Verbrechensbekämpfung allgemein – und damit die Länder generell ausschließend – einräumt, oder ob er dem Bund diese Regelungskompetenz nur in Bezug auf die Ausgestaltung der Befugnisse des Bundeskriminalpolizeiamts verleiht (vgl. Bäcker, DÖV 2011, S. 840 <847>; Zöller, in: Roggan/Kutscha, Handbuch zum Recht der Inneren Sicherheit, 2. Aufl. 2006, S. 447 <459>; vgl. auch Uhle, in: Maunz/Dürig, GG, Art. 73 Rn. 255 [Oktober 2019]; zur Entstehungsgeschichte Schneider, Das Grundgesetz, Dokumentation seiner Entstehung, Bd. 17, 2007, S. 905 ff.).

II.

Die angegriffenen Vorschriften sind jedoch in formeller Hinsicht verfassungswidrig, weil sie gegen das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG verstoßen (vgl. Huber, ZRP 2016, S. 162 <163>; Hölscheidt, Jura 2017, S. 148 <155>; Marxsen, DÖV 2018, S. 218 <225>; Dietrich, in: Schenke/Graulich/Ruthig [Hrsg.], Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 6 BNDG Rn. 11). Das Bundesnachrichtendienstgesetz nennt Art. 10 Abs. 1 GG in Bezug auf Eingriffe nach § 3 BNDG (vgl. dort Abs. 3), nicht aber für die Eingriffe nach den hier in Streit stehenden Vorschriften. Der Verzicht auf die Beachtung des Zitiergebots lässt sich nicht damit begründen, dass die angegriffenen Vorschriften eine lange bestehende Verwaltungspraxis aufgreifen und nunmehr erstmals gesetzlich regeln. Hierfür lässt sich insbesondere nicht darauf verweisen, dass das Zitiergebot dann nicht greift, wenn das Gesetz geltende Grundrechtsbeschränkungen durch das bisherige Recht unverändert oder mit geringen Abweichungen wiederholt (vgl. dazu BVerfGE 35, 185 <188 f.>). Denn eine gesetzlose Verwaltungspraxis ist weder geltendes Recht noch geltende Grundrechtsbeschränkung und beruht – anders als Parlamentsgesetze, die das Zitiergebot beachten – nicht auf bereits getroffenen Wertungen des parlamentarischen Gesetzgebers. Auch die Warnfunktion des Zitiergebots wird durch eine bloße Verwaltungspraxis nicht ersetzt. Dies gilt zumal für die geheime Praxis eines Nachrichtendienstes. 134

Das Zitiergebot ist vielmehr gerade dann verletzt, wenn der Gesetzgeber ausgehend von einer bestimmten Auslegung des Schutzbereichs – wie hier der Annahme fehlender Grundrechtsbindung deutscher Staatsgewalt bei im Ausland auf Ausländer wirkendem Handeln – die Grundrechte als nicht betroffen erachtet. Denn es fehlt dann am Bewusstsein des Gesetzgebers, zu Grundrechtseingriffen zu ermächtigen, und an dessen Willen, sich über deren Auswirkungen Rechenschaft abzulegen, was gerade Sinn des Zitiergebots ist (vgl. BVerfGE 85, 386 <404>; 113, 348 <366>; 129, 208 <236 f.>). Zudem entzieht sich der Gesetzgeber einer öffentlichen Debatte, in der Notwendigkeit und Ausmaß von Grundrechts- eingriffen zu klären sind (vgl. BVerfGE 85, 386 <403 f.>; 129, 208 <236 f.>). 135

E.

Die angegriffenen Vorschriften sind auch materiell mit dem Grundgesetz nicht vereinbar. Zwar steht das Grundgesetz dem Instrument der strategischen Über- wa- 136

chung und diesbezüglichen Kooperationen mit anderen Nachrichtendiensten nicht grundsätzlich entgegen. Die Vorschriften genügen jedoch schon den sich hierfür aus den Grundrechten ergebenden zentralen Anforderungen nicht.

I.

1. Eingriffe in Art. 10 Abs. 1 GG und ebenso in Art. 5 Abs. 1 Satz 2 GG müssen – wie Eingriffe in alle Grundrechte – auf einer gesetzlichen Ermächtigung beruhen, die dem Gebot der Normenklarheit und dem Bestimmtheitsgrundsatz genügt (vgl. BVerfGE 65, 1 <44; 54>; 100, 313 <359 f.>; stRspr). Dabei sind an die Normenklarheit und Bestimmtheit von Ermächtigungen zur heimlichen Erhebung und Verarbeitung personenbezogener Daten in der Regel gesteigerte Anforderungen zu stellen, weil die Datenverarbeitung von den Betroffenen unbemerkt stattfindet und sich die Befugnisse somit nicht im Wechselspiel von behördlicher Einzelanordnung und gerichtlicher Kontrolle schrittweise konkretisieren können (vgl. BVerfGE 141, 220 <265 Rn. 94>; vgl. auch EGMR, Big Brother Watch and others v. United Kingdom, Urteil vom 13. September 2018, Nr. 58170/13 u.a., § 306). 137

Für die Nachrichtendienste gilt hiervon keine Ausnahme. Zwar bedarf ihre Aufgabenwahrnehmung in weitem Umfang der Geheimhaltung. Gerade die Aufklärung im Ausland ist grundsätzlich auf strenge Abschirmung verwiesen, um Informationen erlangen zu können, ohne die eigenen Ressourcen und Quellen zu gefährden (vgl. BVerfGE 30, 1 <18 f.>; 100, 313 <397 f.>). Geheim gehalten werden müssen dabei nicht nur die einzelnen Maßnahmen und Erkenntnisse des hiermit betrauten Bundesnachrichtendienstes, sondern auch Informationen, inwieweit dem Dienst die Aufklärung zu welchen Fragen möglich oder unmöglich ist und welchen Grad der Detailliertheit er hierbei erreicht. Da der Dienst davon ausgehen muss, seinerseits den Ausforschungsversuchen ausländischer Dienste ausgesetzt zu sein, setzen sich die Geheimhaltungserfordernisse bis tief in die Organisation der Dienste fort. Dem darf der Gesetzgeber Rechnung tragen. 138

Aus der Geheimhaltungsbedürftigkeit der Auslandsaufklärung lässt sich jedoch nicht ableiten, dass über den Bundesnachrichtendienst überhaupt möglichst wenig bekannt werden dürfte und auch seine Rechtsgrundlagen möglichst weitgehend im Dunkeln bleiben müssten. Für die Handlungsgrundlagen und Grenzen der nachrichtendienstlichen Befugnisse kann es im demokratischen Rechtsstaat eine prinzipielle Geheimhaltung nicht geben. Ebenso wie der Gesamthaushalt und die Personalstärke der Nachrichtendienste vollständig durch das Parlament festgelegt und öffentlich verantwortet werden müssen (zur Kontrolle der Mittelbewirtschaftung im Einzelnen vgl. demgegenüber § 10a BHO), müssen auch ihre Befugnisse durch Gesetz normenklar und bestimmt vor der Öffentlichkeit geregelt werden und Verantwortlichkeiten klar zugeordnet sein (vgl. Gusy, in: Schenke/Graulich/Ruthig [Hrsg.], Sicherheitsrecht des Bundes, 2. Aufl. 2019, BNDG Vorb. Rn. 10, 13). Mit der Grundrechtsbindung korrespondiert die parlamentarisch-demokratische Verantwortung für die Einschränkung der Grundrechte. Geheimhaltung gilt insoweit nur nach 139

Maßgabe des öffentlichen Gesetzes. Sie ist auch für die Auslandsaufklärung kein Selbstzweck, sondern nur gerechtfertigt, wenn Art und Umfang der geheimhaltungsbedürftigen Tätigkeit des Dienstes in demokratisch-öffentlicher Weise legitimiert sind und die Geheimhaltung in den spezifischen Grenzen funktionaler Notwendigkeit verbleibt.

Das Erfordernis einer normenklaren und hinreichend bestimmten Fassung der gesetzlichen Befugnisse stellt dabei die Möglichkeit, sie in der Sache geheim handzuhaben, nicht in Frage. Da die Befugnisse nur abstrakt rechtliche Möglichkeiten schaffen, sagen sie nichts darüber aus, ob, wie, mit welcher Reichweite und welchem Erfolg von ihnen Gebrauch gemacht wird. 140

2. Als Ermächtigungen zu Eingriffen in das Telekommunikationsgeheimnis und die Pressefreiheit sind die angegriffenen Vorschriften nur zu rechtfertigen, wenn sie dem Verhältnismäßigkeitsgrundsatz genügen. Sie müssen danach einen legitimen Zweck verfolgen, zur Erreichung des Zwecks geeignet, erforderlich und verhältnismäßig im engeren Sinne sein (vgl. BVerfGE 67, 157 <173>; 120, 378 <427>; 141, 220 <265 Rn. 93>; stRspr). Für geheime Überwachungsmaßnahmen durch Sicherheitsbehörden hat das Bundesverfassungsgericht die sich hieraus ergebenden Anforderungen durch eine Vielzahl von Entscheidungen konkretisiert und insbesondere in der Entscheidung zum Bundeskriminalamtgesetz zusammengefasst (vgl. BVerfGE 141, 220 <268 ff. Rn. 103 ff.>). Diese Maßstäbe, die auch für Über- wachungsmaßnahmen der Nachrichtendienste gelten, bilden sowohl für die Anforderungen an die Datenerhebung und -verarbeitung als auch für die Anforderungen an die Übermittlung der Daten den Ausgangspunkt. Allerdings ist mit ihnen das Instrument der strategischen Überwachung als besonderes Mittel der Auslands- aufklärung noch nicht in den Blick genommen. Sie bedürfen daher – in Anknüpfung an die Entscheidung zu den strategischen Überwachungsbefugnissen nach dem Artikel 10-Gesetz (vgl. BVerfGE 100, 313 <368 ff.>) – der Konkretisierung. 141

II.

Die Befugnis zur Datenerhebung und Datenverarbeitung in Form der strategischen Telekommunikationsüberwachung ist als besonderes Instrument der Auslandsaufklärung mit Art. 10 Abs. 1 GG im Grundsatz vereinbar (1.). Es bedarf hierfür jedoch einer hinreichend begrenzenden Ausgestaltung (2.). 142

1. Die Einräumung der Befugnis zur Auslandsaufklärung im Wege der strategischen Fernmeldeüberwachung ist durch Art. 10 Abs. 1 GG nicht von vornherein ausgeschlossen. Obwohl sie nicht auf konkrete und objektiviert bestimmte Anlassfälle begrenzt ist und damit ohne Eingriffsschwelle zu schweren Grundrechtseingriffen berechtigt, kann sie durch das Ziel der Auslandsaufklärung und deren besondere Handlungsbedingungen bei hinreichend begrenzter Ausgestaltung vor Art. 10 Abs. 1 GG und dem Verhältnismäßigkeitsgrundsatz gerechtfertigt werden. 143

a) Die strategische Telekommunikationsüberwachung dient einem legitimen Zweck 144

und ist zu seiner Erreichung nach dem Maßstab des Verhältnismäßigkeitsgrundsatzes geeignet und erforderlich. Nach dem Willen des Gesetzgebers soll die strategische Überwachung Erkenntnisse über das Ausland verschaffen, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik sind. Sie soll damit dazu beitragen, frühzeitig Gefahren zu erkennen, die Handlungsfähigkeit der Bundesrepublik zu wahren und die Bundesregierung in außen- und sicherheits- politischen Fragen mit Informationen zu versorgen. Hierin liegt ein legitimes Ziel. Die strategische Telekommunikationsüberwachung ist hierfür auch ein geeignetes Mittel, denn sie ermöglicht, an solche Informationen zu gelangen. Dass hierbei in großem Umfang zunächst Daten miterfasst werden, die keinen relevanten Informationsgehalt haben, ändert nichts daran, dass die gesamthafte Erfassung und Auswertung von Datenströmen im Ergebnis zu bedeutsamen Erkenntnissen führen kann. Gleichfalls genügt die strategische Überwachung den Anforderungen der Erforderlichkeit. Ohne die breit angelegte anlasslose Erfassung von Datenströmen und deren Auswertung könnten entsprechende Informationen nicht gewonnen werden. Ein weniger eingriffsintensives Mittel, das generell vergleichbare Informationen sicherstellte, ist nicht ersichtlich.

b) Die Ermächtigung des Bundesnachrichtendienstes zur strategischen Überwachung der Telekommunikation von Ausländern im Ausland kann vor Art. 10 Abs. 1 GG vom Grundsatz her auch in Hinblick auf die Verhältnismäßigkeit im engeren Sinne gerechtfertigt werden. 145

aa) Allerdings handelt es sich bei der strategischen Telekommunikations- überwachung um ein Instrument von besonders schwerem Eingriffsgewicht. 146

(1) Schwer wiegen die mit ihr eröffneten Eingriffe zunächst schon deshalb, weil mit ihnen heimlich in persönliche Kommunikationsbeziehungen eingedrungen wird, die oftmals privaten und unter Umständen auch höchstvertraulichen Charakter haben. Eine solche heimliche Überwachung der Telekommunikation bedeutet grundsätzlich einen schweren Eingriff (vgl. BVerfGE 141, 220 <264 f. Rn. 92>), unabhängig davon, ob die Überwachung im Inland oder im Ausland stattfindet oder sich auf Inländer und Deutsche oder Ausländer bezieht. 147

(2) Im Verhältnis zur Überwachung individueller Telekommunikation weist die strategische Überwachung allerdings insoweit ein geringeres Eingriffsgewicht auf, als sie sich auf Datenströme bezieht, deren Ergiebigkeit im Einzelnen nicht vorhersehbar ist. Auch soweit sie mittels formaler Suchbegriffe auf die Überwachung einzelner Personen gerichtet ist, ist sie typischerweise weniger zielgenau und nicht vollständig, da die für eine konkrete Kommunikationsverbindung genutzten Netze und Übertragungsstrecken (sogenanntes Routing) je nach Verfügbarkeit weithin spontan bestimmt werden und nur ein geringer Bruchteil der deutschlandweit und weltweit vorhandenen Netze von Netzanordnungen erfasst wird. Die strategische Überwachung unterscheidet sich in ihrem Eingriffsgewicht damit zumindest prinzipiell von einer Beschränkung im Einzelfall, wie sie etwa durch § 3 G 10 ermöglicht wird. 148

(3) Überdies mindert sich ihr Eingriffsgewicht gegenüber im Ausland befind- lichen 149

Personen dadurch, dass die Überwachung nicht stets in gleicher Weise auf unmittelbar operative Konsequenzen gerichtet ist wie in der Regel Überwachungsmaßnahmen gegenüber Deutschen oder im Inland befindlichen Personen. Die Auslandsaufklärung betrifft Vorgänge in anderen Ländern, in denen der deutsche Staat nicht über Hoheitsbefugnisse verfügt, und ist dabei dem Bundesnachrichtendienst als einer Behörde vorbehalten, die grundsätzlich keine eigenen operativen Befugnisse hat. Die Aufgabe der Auslandsaufklärung liegt primär darin, zunächst eine Informationsbasis zu schaffen, Informationen zu bewerten, auf ihre Relevanz zu prüfen und sie dann aufbereitet der Bundesregierung sowie gegebenenfalls weiteren Adressaten zur Verfügung zu stellen. Allerdings verbindet sich auch hier die Überwachung oftmals mit dem Ziel, gegenüber Betroffenen – unter Umständen auch im Austausch der Erkenntnisse mit anderen Staaten – Maßnahmen zu treffen, und bleibt damit gewichtig. Solche Maßnahmen kann der Bundesnachrichtendienst gegenüber Personen im Ausland jedoch nicht selbst ergreifen. Maßnahmen, die andere Stellen aufgrund dieser Informationen gegen Betroffene ergreifen, sind von Datenübermittlungen abhängig, die rechtlich durch den Grundsatz der hypothetischen Datenneuerhebung begrenzt werden können und müssen (dazu unten Rn. 216 f. und 220 ff.).

(4) Besonders erschwerend ins Gewicht fällt demgegenüber die außerordent- liche 150
Streubreite der strategischen Telekommunikationsüberwachung. Sie wird anlasslos gegenüber jeder Person erlaubt und ist allein durch bestimmte Zweck- setzungen final angeleitet. Objektive Eingriffsschwellen werden weder in Bezug auf begrenzende Situationen noch auf die von der Überwachung betroffenen Personen vorausgesetzt. Die so ermächtigte Behörde kann im Rahmen nur abstrakt vorgegebener Zwecke frei entscheiden, auf welche Netze, Daten und Personen sie die Maßnahmen richtet.

Eine solche Befugnis hat insbesondere unter den heutigen Bedingungen der Infor- 151
mationstechnik und ihrer Bedeutung für die Kommunikationsbeziehungen eine außerordentliche Reichweite. Sie ist in ihrer Eingriffsintensität nicht mehr zu vergleichen mit den Befugnissen, über die das Bundesverfassungsgericht in seiner Entscheidung zur strategischen Überwachung der Inland-Ausland-Kommunikation im Jahr 1999 zu entscheiden hatte. Während damals die Telekommunikationsüberwachung in tatsächlicher Hinsicht eng begrenzte, allein in spezifischen Situationen benutzte Telekommunikationsmittel betraf (vgl. BVerfGE 100, 313 <379 f.>), werden heute schon quantitativ unvergleichbar größere Datenströme erfasst. Mit ihnen wird eine unübersehbare Zahl von Formen elektronischer Kommunikation transportiert und der Auswertung zugeführt. Angesichts der ubiquitären und vielfältigen Nutzung von Kommunikationsdiensten findet inzwischen zunehmend jede Art individuellen Handelns und zwischenmenschlicher Interaktion in elektronischen Signalen ihren Niederschlag und wird so der Telekommunikationsüberwachung zugänglich. Die Überwachung erfasst damit tief in den Alltag hineinreichende, auch höchst private und spontane Kommunikationsvorgänge einschließlich des Austausches von Bildern und Dokumenten. Technisch möglich ist heute selbst die Überwachung des Nutzerverhaltens im World Wide Web und der hierbei zum Ausdruck kommenden Interessen, Wünsche und Vor-

lieben. Zugleich reichen heutzutage die Analysemöglichkeiten wesentlich weiter. Fehlte es dem Bundesnachrichtendienst 1999 etwa noch an den technischen Möglichkeiten einer automatisierten Spracherkennung, so stehen heute Programme zur Spracherkennung, zur Übersetzung oder zur Bilderkennung schon der allgemeinen Öffentlichkeit zur Verfügung. Insgesamt erstreckt sich die strategische Telekommunikationsüberwachung damit inzwischen potentiell auf annähernd die gesamte Kommunikation auch der Zivilgesellschaft (vgl. zur Aussagekraft von Verkehrsdaten BVerfGE 125, 260 <319>; zu den erweiterten Erkenntnismöglichkeiten der Nachrichtendienste Omand, in: Dietrich/Sule [Hrsg.], Intelligence Law and Policies in Europe, 2019, S. 38 <Rn. 37 ff.>).

(5) Besonderes Eingriffsgewicht kommt der strategischen Telekommunikationsüberwachung insoweit zu, als sie auch gezielt personenbezogene Überwachungen ermöglicht. Gegenüber den Befugnissen, die Gegenstand der Entscheidung des Senats von 1999 waren, eröffnet dies eine eigene Dimension. Während dort die strategische Überwachung allein insoweit in den Blick kam, als sie ohne spezifischen Personenbezug mit inhaltlichen Suchbegriffen arbeitete (vgl. BVerfGE 100, 313 <384>), operiert die strategische Fernmeldeaufklärung, wie sie hier in Frage steht, ganz überwiegend mit formalen Suchbegriffen wie Telekommunikationskennungen, die es auch erlauben, die Überwachung gezielt auf die Telekommunikation einzelner Personen zu richten. Die strategische Fernmeldeaufklärung erhält dadurch eine grundlegend weiterreichende Eingriffstiefe und rückt näher an die individuelle Telekommunikationsüberwachung heran. 152

(6) Im Verhältnis zur früheren Rechtslage kommt belastend hinzu, dass die strategische Überwachung nunmehr in gewissem Umfang auch eine gesamthaft bevorratende Speicherung von Verkehrsdaten eröffnet. Durch deren – wiederum anlasslos und allein final angeleitete – Auswertung können tiefgehende Einblicke in das Kommunikations- und Bewegungsverhalten von Personen gewonnen werden, die über die inhaltliche Auswertung individueller Kommunikationsverkehre unter Umständen weit hinausgehen (vgl. zur Aussagekraft solcher Daten BVerfGE 125, 260 <319>; EuGH, Urteil vom 8. April 2014, Digital Rights Ireland und Seitlinger u.a., C-293/12, C-594/12, EU:C:2014:238, Rn. 48, 56). Auch dies erhöht das Eingriffsgewicht nochmals erheblich. 153

bb) Trotz des damit besonders schweren Eingriffsgewichts der strategischen Überwachung kann diese als spezifische Befugnis der Auslandsaufklärung verfassungsrechtlich gerechtfertigt sein. 154

(1) Allerdings liegt in dem Verzicht auf jede konkretisierende Eingriffsschwelle eine Freistellung von einem Kernelement rechtsstaatlicher Anforderungen, das grundsätzlich und insbesondere in Bezug auf innerstaatlich tätige Sicherheitsbehörden schon für weniger eingriffsintensive, erst recht aber für schwerwiegende Grundrechtseingriffe wie die Überwachung der Telekommunikation unverzichtbar ist (vgl. BVerfGE 141, 220 <269 ff. Rn. 104 ff.>; 150, 244 <280 ff. Rn. 90 ff.>). Das Erfordernis einer an 155

konkrete Umstände anknüpfenden Eingriffsschwelle sichert die Begrenzung von Grundrechtseingriffen, bindet sie an objektivierte Voraussetzungen und ermöglicht eine Kontrolle anhand für sich stehender Kriterien. Eine allein final angeleitete und begrenzte Ermächtigung zu solchen Eingriffen ist mit Art. 10 Abs. 1 GG grundsätzlich unvereinbar.

Das gilt im Grundsatz auch für Nachrichtendienste. Soweit sich Überwachungsmaßnahmen auf die Inlandskommunikation erstrecken, bedarf es entsprechend den allgemeinen Anforderungen belastbarer Eingriffsschwellen. Nicht anders liegt es, wenn gegenüber bestimmten Personen – sei es im Inland, sei es im Ausland – im Wege der Einzelanordnung Überwachungsmaßnahmen etwa in Form einer Telekommunikationsüberwachung oder Onlinedurchsuchung angeordnet werden (vgl. BVerfGE 120, 274 <326 ff.>; 125, 260 <320 ff.>; 141, 220 <270 ff. Rn. 106 ff.>; siehe auch § 3 G 10). 156

(2) Anders verhält es sich demgegenüber für die nachrichtendienstliche Auslandsaufklärung, soweit diese auf die allgemeine Informationssammlung zur Unterrichtung der Bundesregierung oder – noch im Vorfeld von individualgerichteten Beschränkungen im Einzelfall – auf die Gefahrenfrüherkennung zielt. Hier kann der Gesetzgeber dem Bundesnachrichtendienst auch das Instrument der strategischen Telekommunikationsüberwachung an die Hand geben. Dass diese im Wesentlichen nur final angeleitet und begrenzt ist, ist bezogen auf diese spezifische Aufgabe mit den Anforderungen der Verhältnismäßigkeit nicht von vornherein unvereinbar (ebenso zur strategischen Überwachung der internationalen Telekommunikation BVerfGE 100, 313 <373 ff.>). 157

(a) Ausgangspunkt ist hierfür das Aufgabenprofil der Auslandsaufklärung. Bei ihr geht es nicht primär um gezielte Ermittlungen hinsichtlich bereits feststehender Vorgänge und damit nicht um die Aufklärung schon klar umrissener Sachverhalte, sondern vor allem um das Aufspüren und Identifizieren von relevanten Informationen bezüglich nur abstrakt bestimmbarer Erkenntnisinteressen. Die Aufgabe der Auslandsaufklärung liegt insoweit darin, zunächst eine umfangreiche Informationsbasis zu schaffen, um Entwicklungen breitflächig zu beobachten, die Informationen dann zu bewerten, auf ihre Relevanz zu prüfen und sie schließlich in kondensierter Form der Bundesregierung sowie gegebenenfalls weiteren Adressaten zur Verfügung zu stellen. Die potentiellen Erkenntnisinteressen eröffnen dabei mit ihrer Ausrichtung auf die gesamte Außen- und Sicherheitspolitik ein weites Spektrum. 158

(b) Für diese Aufgabe kann auch eine anlasslose, im Wesentlichen allein final gesteuerte Fernmeldeaufklärung in Form der strategischen Überwachung verfassungsrechtlich gerechtfertigt sein. Im Unterschied zu Maßnahmen der frühzeitigen innerstaatlichen Identifizierung von Gefahren hat hierbei zunächst schon Bedeutung, dass die Auslandsaufklärung auf die Erhellung und das Verständnis von Umständen abzielt, hinsichtlich derer es an einer unmittelbaren alltäglichen Wahrnehmung seitens deutscher Stellen und der innerstaatlichen Öffentlichkeit fehlt. Es geht um Erkennt- 159

nisse zu Entwicklungen in Kontexten, die sich allein mit Informa- tionen aus dem Inland nur schwer deuten lassen und zum Teil Länder mit informationell wenig offenen Strukturen betreffen. Maßgeblich sind vor allem aber die besonderen Handlungsbedingungen bei Erfüllung dieser Aufgabe. Die Auslandsaufklärung betrifft Vorgänge in anderen Ländern, in denen der deutsche Staat allenfalls punktuell mit eigenen Erkenntnisquellen präsent ist und sein kann und in denen er nicht über Hoheitsbefugnisse verfügt, die ihm einen unmittelbaren Zugriff auf Informationen ermöglichen (ebenso EGMR, Big Brother Watch and others v. United Kingdom, Urteil vom 13. September 2018, Nr. 58170/13 u.a., § 518). Dabei muss die Aufklärung im Interesse der Handlungsfähigkeit und Sicherheit der Bundesrepublik Deutschland insbesondere auch an Informationen gelangen können, die ihr – möglicherweise in nachteiliger Absicht – gezielt vorenthalten und in der Hoheitssphäre des Drittstaats geheim gehalten werden. Die Maßnahmen der Aufklärung können zudem nach dem Recht des Zielstaats nicht selten illegal, jedenfalls oft unerwünscht sein. Dabei ist der Dienst zugleich mit den Abwehrtätigkeiten der Zielländer konfrontiert, die die Aufklärung ihrerseits mit polizeilichen und nachrichtendienstlichen Mitteln behindern und zu hintertreiben suchen. Die Arbeit ist damit besonders gefährdet und prekär und auf außergewöhnliche Mittel verwiesen.

Zu berücksichtigen ist zugleich, dass die Aufklärung nicht allein im Gegen- einander der verschiedenen Nachrichtendienste, sondern auch im Miteinander zur Aufklärung von die Bundesrepublik Deutschland und andere Länder gleichermaßen betreffenden Fragenkreisen steht. Insbesondere die allein der Information der Bundesregierung dienende Aufklärung politisch oder militärisch relevanter Geschehensabläufe, aber auch die Frühaufklärung von Gefahren der internationalen Kriminalität, zu der auch der internationale Terrorismus gehört, sind für ihre Wirksamkeit heute auf eine Kooperation der Dienste untereinander angewiesen. Kooperationsfähig ist der Bundesnachrichtendienst aber nur, wenn er auch seinerseits Befugnisse hat, mit denen er die Ergebnisse anderer Dienste prüfen, sie aufnehmen und weiter verwerten kann und mit deren Hilfe er auch durch eigene Erkenntnisse als Partner beizutragen vermag. Befugnisse zur anlasslosen Überwachung der Auslandskommunikation dürften dabei, nach allem was bekannt ist, heute zur verbreiteten Ausstattung dieser Dienste gehören (für die USA: Section 702 Foreign Intelligence Surveillance Act; vgl. dazu Renan, in: Goldman/Rascoff [Hrsg.], Global Intelligence Oversight, 2016, S. 121 <insb. 123 ff.>; für das Vereinigte Königreich Part 6 Chapter 1 Investigatory Powers Act 2016; vgl. dazu Leigh, in: Dietrich/Sule [Hrsg.], Intelligence Law and Policies in Europe, 2019, S. 553 ff.; McKay/Walker, in: Dietrich/Gärditz/Graulich/Gusy/Warg [Hrsg.], Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 119 ff.; für Frankreich: Article L854-1 bis L854-9 Code de la sécurité intérieure [Des mesures de surveillance des communications électroniques internationales]; s. dazu auch Le Divelec, in: Dietrich/Sule [Hrsg.], Intelligence Law and Policies in Europe, 2019, S. 516 ff.; Warusfel, in: Dietrich/Gärditz/Graulich/Gusy/Warg [Hrsg.], Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 129 ff.). 160

(c) Zu berücksichtigen ist dabei auch das überragende öffentliche Interesse an einer wirksamen Auslandsaufklärung. 161

Entsprechend der kompetenziellen Rückbindung (oben Rn. 123 ff.) zielt die Auslandsaufklärung immer auf Informationen, die Bedeutung für die Stellung und Handlungsfähigkeit Deutschlands in der Staatengemeinschaft entfalten und damit gerade in diesem Sinne von außen- und sicherheitspolitischer Bedeutung sind. Die Versorgung der Bundesregierung mit Informationen für ihre außen- und sicherheitspolitischen Entscheidungen hilft ihr, sich im machtpolitischen Kräftefeld der internationalen Beziehungen zu behaupten, und kann folgenreiche Fehlentscheidungen verhindern. Insoweit geht es mittelbar zugleich um die Bewahrung demokratischer Selbstbestimmung und den Schutz der verfassungsrechtlichen Ordnung – und damit um Verfassungsgüter von hohem Rang. In Frage steht mithin ein gesamtstaatliches Interesse, das über das Interesse an der Gewährleistung der inneren Sicherheit als solcher deutlich hinausgeht. 162

Von Gewicht ist hierbei, dass im Zuge der Entwicklung der Informationstechnik und der internationalen Kommunikation, ebenso wie damit der engeren grenzüberschreitenden Verflechtung der Lebensbedingungen im Allgemeinen, Bedrohungen vom Ausland aus erheblich zugenommen haben. Die Früherkennung von Gefahrenlagen, die aus dem Ausland drohen, gewinnt hierbei auch für die Sicherheit besondere Bedeutung. Die Erweiterung und Internationalisierung der Kommunikationsmöglichkeiten und die damit gesteigerte Politisierung und Organisationsfähigkeit international agierender krimineller Gruppierungen führen dazu, dass innerstaatliche Gefahrenlagen oftmals durch Netzwerke international zusammenarbeitender Akteure begründet sind und leicht eine außen- und sicherheitspolitische Dimension erhalten können. Die Herausforderungen durch weltweit verflochtene Kreise organisierter Kriminalität und Geldwäsche wie auch Menschenhandel, elek-tronische Angriffe auf informationstechnische Systeme, den internationalen Terrorismus oder den Handel mit Kriegswaffen machen das beispielhaft deutlich (vgl. Kojm, in: Goldman/Rascoff [Hrsg.], Global Intelligence Oversight, 2016, S. 95 ff.; Goodman/Ischebeck-Baum, in: Dietrich/Sule [Hrsg.], Intelligence Law and Policies in Europe, 2019, S. 1 <insb. Rn. 104 ff.>; hinsichtlich des Gefahrenbereichs „Cyber“ siehe auch BTDrucks 18/4654, S. 40 f.; zu den Gefahrenbereichen „internationaler Terrorismus“ und „Kriegswaffenproliferation“ siehe bereits BTDrucks 12/6853, S. 20, 42). Solche Aktivitäten zielen zum Teil auf eine Destabilisierung des Gemeinwesens (vgl. zum internationalen Terrorismus BVerfGE 115, 320 <357>; 133, 277 <333 f. Rn. 133>; 143, 101 <138 f. Rn. 125>) und können zur Bedrohung für die verfassungsmäßige Ordnung, den Bestand und die Sicherheit des Bundes oder der Länder sowie für Leib, Leben und Freiheit werden. Dies sind Rechtsgüter von überragendem verfassungsrechtlichen Gewicht, für deren Schutz der Gesetzgeber eine wirksame und zugleich rechtsstaatlich eingehegte Auslandsaufklärung als unverzichtbar ansehen kann (vgl. BVerfGE 115, 320 <358>; 143, 101 <138 f. Rn. 124 ff.>). 163

Dem ungleich weiteren Datenzugriff der strategischen Überwachung steht heute im Verhältnis zu der Situation, über die das Bundesverfassungsgericht 1999 zu entscheiden hatte, folglich auch ein gesteigertes Gefahrenpotential gegenüber. Aus diesem Grund stehen Art. 10 Abs. 1 GG und die sich aus ihm ergebenden Verhältnismäßigkeitsanforderungen auch der Einbeziehung gezielt personenbezogener Suchbegriffe in die strategische Überwachung nicht prinzipiell entgegen und darf das Gesetz vom Grundsatz her in begrenztem Umfang auch eine bevorratend gesamthafte Speicherung von Verkehrsdaten sowie deren anlasslose Auswertung vorsehen. 164

(d) Ein wichtiger Gesichtspunkt für die Rechtfertigungsfähigkeit der strategischen Telekommunikationsüberwachung liegt schließlich darin, dass die Folgen der anlasslosen Durchführung dadurch etwas abgemildert werden, dass sie durch eine Behörde vorgenommen werden, die selbst grundsätzlich keine operativen Befugnisse hat. Gegenüber Personen im Ausland können Erkenntnisse schon den tatsächlichen Umständen nach in der Regel nicht unmittelbar zu Folgemaßnahmen gegenüber den Betroffenen führen, da insoweit keine Hoheitsbefugnisse deutscher Behörden bestehen. Das stellt allerdings nicht in Frage, dass auch im Ausland durchgeführte Überwachungen zu gravierenden Konsequenzen für die Betroffenen führen können und Folgemaßnahmen gegenüber ihnen – sei es mittels eines Austauschs der Daten, sei es bei späteren Grenzübertritten – auch ermöglichen sollen. Da die Daten jedoch von einer Behörde erhoben werden, die selbst grundsätzlich keine eigenen operativen Befugnisse hat, ist hier eine weitere Datenverwendung zunächst von einer in Distanz zu eigenen Handlungsverantwortlichkeiten vor- genommenen Sichtung der Daten abhängig. Ihre Übermittlung zur operativen Nutzung kann – und muss – daher durch qualifizierte Übermittlungsschwellen sichergestellt werden (unten Rn. 220 ff.). 165

c) Das Instrument der strategischen Überwachung einschließlich des Einsatzes personenbezogener formaler Suchbegriffe und einer zum Teil auch gesamthaft bevorratenden Erfassung und Auswertung von Verkehrsdaten ist danach mit Art. 10 Abs. 1 GG und den hieraus folgenden Verhältnismäßigkeitsanforderungen nicht grundsätzlich unvereinbar. Als anlasslose, im Wesentlichen allein final angeleitete und begrenzte Befugnis ist sie jedoch eine Ausnahmebefugnis, die auf die Auslandsaufklärung durch eine Behörde, welche selbst grundsätzlich keine operativen Befugnisse zur Gefahrenabwehr hat, begrenzt bleiben muss. Nur durch deren besonderes Aufgabenprofil ist sie gerechtfertigt. Hieran hat sich nach dem Grundsatz der Verhältnismäßigkeit auch die nähere Ausgestaltung auszurichten. 166

2. Die Ausgestaltung der Datenerhebung und -verarbeitung in Form der strategischen Überwachung unterliegt danach näheren Anforderungen, die dem besonderen Gewicht der Grundrechtseingriffe und ihrer spezifischen Rechtfertigung durch das besondere Aufgabenprofil der Auslandsaufklärung Rechnung zu tragen haben. 167

a) Ein übergreifendes Ziel der sich aus dem Verhältnismäßigkeitsgrundsatz ergebenden Anforderungen liegt darin, die strategische Telekommunikations- überwa- 168

chung trotz ihrer Streubreite als hinreichend fokussiertes Instrument auszugestalten und damit begrenzt zu halten. Eine globale und pauschale Überwachung lässt das Grundgesetz auch zu Zwecken der Auslandsaufklärung nicht zu (vgl. BVerfGE 100, 313 <376>).

Dafür hat der Gesetzgeber zunächst einschränkende Maßgaben zum Volumen der für die jeweiligen Übertragungswege auszuleitenden Daten vorzugeben (vgl. Löffelmann, in: Dietrich/Gärditz/Graulich/Gusy/Warg [Hrsg.], Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 33 <40>) und sicherzustellen, dass das von der Überwachung abgedeckte geographische Gebiet begrenzt bleibt. Da sich die technischen Möglichkeiten der Datenverarbeitung schnell ändern, reicht es nicht, hierfür allein auf tatsächliche Kapazitätsgrenzen zu verweisen (vgl. Huber, ZRP 2016, S. 162 <164>; Papier, NVwZ 2016, S. 1057 <1058>; Marxsen, DÖV 2018, S. 218 <224>; Dietrich, in: Schenke/Graulich/Ruthig [Hrsg.], Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 6 BNDG Rn. 11; Löffelmann, in: Dietrich/Eiffler [Hrsg.], Handbuch des Rechts der Nachrichtendienste, 2017, IV § 4 Rn. 184). Vor allem aber muss der Gesetzgeber rechtsstaatliche Einhegungen schaffen, die die Datenerhebung und -verarbeitung näher strukturieren und zum Teil auch begrenzen. Hierzu gehören insbesondere Regelungen zum Einsatz von Filtertechniken (b), zu den Überwachungszwecken (c), zur Gestaltung des Über- wachungsverfahrens (d), zu einem fokussierten Umgang mit Suchbegriffen (e), zu Grenzen der bevorratenden Verkehrsdatenspeicherung (f), zu Methoden der Datenauswertung (g), zum Schutz von Vertraulichkeitsbeziehungen (h) und dem des Kernbereichs privater Lebensgestaltung (i) sowie die Vorgabe von Löschungspflichten (j). Hinzu kommen Anforderungen an Transparenz, individuellen Rechtsschutz und vor allem an eine ausgebaute unabhängige objektivrechtliche Kontrolle (dazu übergreifend unten V). 169

b) Da die strategische Überwachung nur als Instrument der Auslandsaufklärung gerechtfertigt werden kann, bedarf es als Grundlage der weiteren Datenverarbeitung einer normenklaren Regelung zur Aussonderung von Daten aus der Inlandskommunikation. 170

aa) Auf jeden Fall bedarf es einer Regelung bezüglich der Aussonderung von Daten aus Telekommunikation, an der auf beiden Seiten Deutsche oder Inländer beteiligt sind, da für diese eine anlasslose Telekommunikationsüberwachung von vornherein nicht in Betracht kommt. 171

Auf der Basis der Aussonderung der Inlandskommunikation kann dann die strategische Überwachung mit zwei Zielrichtungen durchgeführt werden, nämlich einerseits zur Überwachung der in § 5 G 10 sogenannten „internationalen“ Kommunikation (der Inland-Ausland-Kommunikation), und anderseits zur Überwachung der reinen Auslandskommunikation (der Ausland-Ausland-Kommunikation). Zwar sind beide Formen der Überwachung gleichermaßen an Art. 10 Abs. 1 GG zu messen. Doch weist die Ausland-Ausland-Überwachung in bestimmten Hinsichten ein geringeres Eingriffsgewicht auf als die Inland-Ausland-Überwachung, die Kommunikation mit unmit- 172

telbarem Inlandsbezug erfasst und somit tiefer in die innerstaatliche Rechtsordnung hineinreicht. Daher gelten für die Ausland-Ausland-Überwachung zum Teil abgesenkte Anforderungen (vgl. zur Möglichkeit der gefahrunabhängigen Aufklärung zur Information der Bundesregierung unten Rn. 177; zur Möglichkeit der Auswahl der Suchbegriffe erst nach Festlegung der Überwachungsmaßnahme unten Rn. 179 f. und zur automatisierten Übermittlung von Daten an ausländische Nachrichtendienste im Rahmen von Kooperationen unten Rn. 254 ff. und 262 ff.). Will der Gesetzgeber dem unterschiedlichen Gewicht der Eingriffe Rechnung tragen und deshalb verschiedene Regelungen schaffen, muss er weiter vorsehen, dass auch die Inland-Ausland-Kommunikation auszusondern ist.

bb) Die Anforderungen an die Aussonderung der Inlandskommunikation und der Inland-Ausland-Kommunikation müssen klar geregelt sein. Soweit dies technisch möglich ist, muss durch den Einsatz von automatisierten Filterprozessen sichergestellt sein, dass den Mitarbeitern des Bundesnachrichtendienstes solche Telekommunikationsdaten schon gar nicht bekannt werden. Zwar ist es nicht von vornherein unzulässig, wenn, soweit technisch unvermeidbar, zunächst unterschiedslos alle Daten und damit auch die Inlandsdaten von den Systemen des Bundesnachrichtendienstes erfasst werden. Der Gesetzgeber muss dann aber normenklar regeln, dass Daten aus der reinen Inlandskommunikation und gegebenenfalls der Inland-Ausland-Kommunikation mit allen zur Verfügung stehenden Mitteln technisch herausgefiltert und spurenlos gelöscht werden müssen, bevor eine manuelle Auswertung erfolgt. Der Dienst ist darauf zu verpflichten, die Filtermethoden kontinuierlich fortzuentwickeln und auf dem Stand von Wissenschaft und Technik zu halten. 173

Soweit eine solche Filterung technikbedingt eine Trennung der Daten nicht vollständig gewährleisten kann, steht das der weiteren Nutzung und Auswertung der so vorgefilterten Daten nicht entgegen. Insoweit ist jedoch gesetzlich sicherzustellen, dass dann, wenn im Rahmen der weiteren Auswertung Telekommunikationsdaten von Deutschen oder Inländern identifiziert werden, diese nicht genutzt werden dürfen und unverzüglich zu löschen sind. Eine Ausnahme hiervon kann der Gesetzgeber nur vorsehen, soweit die Daten aus sich heraus eine unmittelbar bevor- stehende konkrete Gefahr für Leib, Leben oder Freiheit einer Person, für lebenswichtige Güter der Allgemeinheit oder für den Bestand oder die Sicherheit des Bundes oder eines Landes erkennen lassen. Zur Begründung einer solchen Befugnis reichen dienstinterne Hinweise auf allgemeine strafrechtliche Grundsätze nicht aus (vgl. demgegenüber derzeit 3.9 DV SIGINT), sondern ist eine ausdrückliche gesetzliche Regelung erforderlich. Eine solche Nutzung ist gegebenenfalls zu protokollieren (unten Rn. 291) und bedarf einer gerichtsähnlichen Kontrolle. 174

c) Weiterhin hat der Gesetzgeber die Zwecke hinreichend präzise und normenklar festzulegen, zu denen die Telekommunikation überwacht und die dabei erlangten Erkenntnisse verwendet werden dürfen (vgl. BVerfGE 100, 313 <372>). 175

aa) Als besonders eingriffsintensives Aufklärungsinstrument bedarf es insoweit ei- 176

ner substantiellen Beschränkung auf hinreichend begrenzte und differenzierte Zwecke, die der Gesetzgeber zu verantworten hat. In Betracht kommen Zwecke, die – im Rahmen auch der kompetenzrechtlichen Grenzen – auf den Schutz hochrangiger Gemeinschaftsgüter gerichtet sind, deren Verletzung schwere Schäden für den äußeren und inneren Frieden oder die Rechtsgüter Einzelner zur Folge hätte (vgl. BVerfGE 100, 313 <373>).

cc) Demgegenüber können Überwachungsmaßnahmen der Ausland-Ausland-Aufklärung, die von vornherein allein das Ziel der Information der Bundesregierung und der Vorbereitung von Regierungsentscheidungen haben, auch unabhängig von einer Ausrichtung auf die Gefahrenfrüherkennung erlaubt werden. Der Gesetzgeber kann hierfür Überwachungsmaßnahmen für das gesamte Aufgabenspektrum des Bundesnachrichtendienstes vorsehen und – allerdings auch insoweit schon kompetenziell auf Fragen von außen- und sicherheitspolitischer Bedeutung begrenzt – etwa allein an Aufträge der Bundesregierung binden. Er muss dann aber sicher- stellen, dass eine Zweckänderung insoweit prinzipiell ausgeschlossen ist und die durch solche Überwachungsmaßnahmen gewonnenen Erkenntnisse – von besonderen Ausnahmefällen abgesehen (näher unten Rn. 228) – nicht an andere Stellen weitergeleitet werden dürfen (siehe näher unten Rn. 223 ff.). 177

d) Zur Verfolgung der gesetzlich bestimmten Zwecke darf der Gesetzgeber die strategische Überwachung grundsätzlich anlasslos erlauben und muss sie nicht an objektivierte Eingriffsschwellen knüpfen (oben Rn. 157 ff.). Als nur final angeleitete Befugnis hat er sie dafür aber an Verfahrensregelungen zu binden, die die Ausrichtung auf die jeweiligen Zwecke rationalisierend strukturieren und damit auch kontrollierbar machen (vgl. Dietrich, in: Schenke/Graulich/Ruthig [Hrsg.], Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 6 BNDG Rn. 10). 178

aa) Ausgangspunkt hierfür muss eine formalisierte Festlegung jeweils begrenzter Überwachungsmaßnahmen sein. Im datenschutzrechtlichen Sinne liegt hierin die Zweckbestimmung der Maßnahme. Als Grundlage für deren Rechtfertigung gegenüber den Überwachten muss die Festlegung die Maßnahme hinsichtlich ihrer Erkenntnisziele und Dauer näher konkretisieren. In der Regel werden hierfür die aufzuklärende Art der Gefahr sowie der geographische Fokus der Überwachung zu bestimmen sein. Die Maßnahmen sind zu befristen. Einer – auch wiederholten – Verlängerung steht das nicht entgegen. 179

Die interne verfahrensrechtliche Ausgestaltung solcher formalisierter Fest- legungen ist verfassungsrechtlich nicht vorgegeben. Der Gesetzgeber kann zwischen verschiedenen organisationsrechtlichen Ausgestaltungen wählen und wird dabei – unter Umständen unterschieden nach dem Gegenstand der Über- wachung – auch Behördenleitervorbehalte oder die Mitwirkung des Bundeskanzleramts in Erwägung zu ziehen haben. Soweit der Gesetzgeber die strategische Überwachung auf Daten der reinen Auslandskommunikation beschränkt, ist nicht immer eine Mitwirkung unmittelbar politisch verantwortlicher Organe geboten. Auch müssen die Suchbegriffe bei der 180

Festlegung der Maßnahme nicht in jedem Fall schon vorab bestimmt werden (vgl. zum Artikel 10-Gesetz BVerfGE 100, 313 <373 f.>).

Für die Festlegung der Maßnahme selbst jedoch bedarf es, entsprechend dem Richtervorbehalt bei individualbezogener Telekommunikationsüberwachung durch Einzelfallanordnung (vgl. BVerfGE 125, 260 <337 f.>; 141, 220 <312 Rn. 235>), einer gerichtsähnlichen Kontrolle. Grundsätzlich ist diese Kontrolle im Vorhinein sicherzustellen. Ausnahmen in Eilfällen sind damit nicht ausgeschlossen. 181

bb) An den in dieser Weise näher definierten Zwecken der Überwachungs- maßnahmen ist das weitere Verfahren der Datenerhebung und -auswertung dann auszurichten und damit in der Folge auch einer unabhängigen Kontrolle zugänglich zu machen. Das betrifft sowohl die Auswahl der für die Überwachung erforderlichen Übertragungswege, die der Beschränkung unterworfen und zur Auswertung erfasst werden sollen, als auch die Auswahl der Suchbegriffe. Ebenso liegt hierin der Bezugspunkt der Kennzeichnung und der Nutzung der Daten. Einer Schaffung von Regeln zur Verwertung von Zufallsfunden durch behördeninterne Zweckänderungen steht dies nicht entgegen (vgl. BVerfGE 141, 220 <326 ff. Rn. 284 ff.>). 182

dd) Die danach differenzierend zu bestimmenden Überwachungsmaßnahmen werden sich der Zahl nach nicht auf einige wenige begrenzen lassen. Ausgehend von der derzeitigen Praxis, die freilich noch anders strukturiert ist, wurde die Zahl der aktuell arbeitsteilig unterschiedenen Überwachungsinteressen oder Aufklärungsperspektiven in der mündlichen Verhandlung von Vertretern des Bundesnachrichtendienstes auf etwa 100 bis 200 geschätzt. Bei Zusammenführung dieser Bearbeitungsperspektiven zu im oben genannten Sinne zusammenhängenden, aber zugleich hinreichend differenziert voneinander abgegrenzten Überwachungsmaßnahmen wird sich diese Zahl möglicherweise etwas reduzieren. Allerdings ist es gerade Zweck solcher Strukturierung, dass die jeweiligen Überwachungsmaßnahmen ein klares und hinreichend differenziertes Profil aufweisen, das die Erfassung und Auswertung der Daten näher anleitet. Daher ist es sachgerecht, wenn die Zahl der in dieser Weise festgelegten Überwachungsmaßnahmen jedenfalls deutlich höher liegt als nach derzeitiger Praxis die Zahl der Netzanordnungen, die aktuell 17 beträgt (oben Rn. 16). 183

Dies hindert von Verfassungs wegen nicht, Netzanordnungen und darauf aufbauende Ausleitungsanordnungen gegenüber einem Telekommunikationsanbieter zur Durchführung einer größeren Zahl verschiedener Überwachungsmaßnahmen zusammenfassend zu treffen. Auch kann der Abgleich der erfassten Daten mit den jeweils den verschiedenen Maßnahmen zugeordneten Suchbegriffen technisch in einem Zusammenhang durchgeführt werden und können die Trefferfälle dann in einem anschließenden Schritt wieder den jeweiligen Maßnahmen zugeordnet werden. In welcher Weise der Bundesnachrichtendienst solche technischen Abläufe konkret organisiert, ist von der Verfassung nicht vorgegeben. 184

e) Ein besonderes Eingriffsgewicht kommt der strategischen Überwachung dadurch 185

zu, dass sie heute vorwiegend mittels formaler Suchbegriffe durchgeführt und dabei auch gezielt auf einzelne Personen gerichtet wird. Auch das ist verfassungsrechtlich nicht ausgeschlossen. Es bedarf dafür aber begrenzender Maß- gaben, die dem Schutzbedarf der Betroffenen in einer den Verhältnismäßigkeits- anforderungen genügenden Weise Rechnung tragen.

aa) Entsprechend derzeitiger Praxis ist die gezielte Erfassung der Telekommunikation von deutschen Staatsangehörigen auszuschließen. Wie für die Inland- Ausland-Aufklärung (vgl. § 5 Abs. 2 G 10) gilt das auch für die Ausland-Ausland-Aufklärung. Zwar schützt Art. 10 Abs. 1 GG Ausländer und Deutsche grundsätzlich gleichermaßen und begründet die strategische Telekommunikationsüberwachung beiden gegenüber schwere Grundrechtseingriffe. Das stellt jedoch nicht in Frage, dass solche Überwachung im Einzelnen beiden gegenüber ein unterschiedliches Eingriffsgewicht aufweist, dem bei der Ausgestaltung der gesetzlichen Eingriffs- ermächtigungen Rechnung getragen werden muss. Die Überwachung hat gegenüber deutschen Staatsangehörigen typischerweise ein größeres Eingriffsgewicht als gegenüber sich im Ausland befindenden Ausländern, weil die eigenen Staatsangehörigen in deutlich weitergehendem Umfang dem Zugriff deutscher Behörden unterliegen und damit leichter Folgemaßnahmen ausgesetzt sind. Das gilt zunächst für Deutsche, die sich nur kurzfristig im Ausland aufhalten. Grundsätzlich betrifft das aber alle deutschen Staatsangehörigen, die – selbst wenn sie längerfristig im Ausland leben – weiterhin der Personalhoheit der Bundesrepublik Deutschland unterliegen; auch sie sind – schon zur Erfüllung ausweisrechtlicher Pflichten – auf einen Kontakt mit deutschen Behörden angewiesen, ebenso wie hier eher davon auszugehen ist, dass sie einen engeren Kontakt nach Deutschland haben und auch öfter einreisen. Die gezielte anlasslose Telekommunikationsüberwachung deutscher Staatsangehöriger im Rahmen der strategischen Überwachung hat deshalb ein Gewicht, das die damit verbundenen Eingriffe in Art. 10 Abs. 1 GG als unverhältnismäßig erscheinen ließe. Eine gezielte Überwachung der Telekommunikation deutscher Staatsangehöriger muss sich daher an den Anforderungen orientieren, die für die individuelle Anordnung einer Telekommunikationsüberwachung gelten (vgl. zu deren Anforderungen BVerfGE 141, 220 <268 ff. Rn. 103 ff.; 309 ff. Rn. 228 ff.>). 186

bb) Im Übrigen hat der Gesetzgeber als Grundlage einer zielgerichteten Strukturierung des Überwachungsprozesses die möglichen Gründe und Gesichtspunkte, unter denen strategische Überwachungsmaßnahmen gezielt auf bestimmte Personen gerichtet werden dürfen, festzulegen. So kann er etwa die Überwachung von Personen vorsehen, die als mögliche Verursacher von Gefahren, als Nachrichtenmittler oder als sonst näher qualifizierte Informanten in Betracht kommen und hierbei möglicherweise Präferenzregeln aufstellen, nach denen etwa die zielgerichtete Überwachung von völlig unbeteiligten Personen nur nachrangig in Betracht kommt. Auch insoweit muss er allerdings nicht das Vorliegen objektivierter Eingriffsschwellen verlangen, sondern kann sich mit einer spezifizierenden Benennung der Zwecke, derentwegen Personen gezielt überwacht werden dürfen, und damit wiederum nur finalen Maßga- 187

ben begnügen.

Gegenüber Personen, die als mögliche Verursacher von Gefahren oder in Blick auf gegenüber ihnen zu ergreifende Folgemaßnahmen im unmittelbaren Interesse des Nachrichtendienstes stehen, hat der Gesetzgeber insoweit einen eigenen Schutzmechanismus vorzusehen. Gegenüber ihnen hat die Überwachung eine besondere Intensität und besteht eine gesteigerte Wahrscheinlichkeit von belastenden Folgen. In der mündlichen Verhandlung hat der Bundesnachrichtendienst insoweit angegeben, dass zur Zeit etwa fünf Prozent der Suchbegriffe auf solche Personen gerichtet seien. Soweit Überwachungsmaßnahmen in dieser Weise gegen bestimmte Personen gerichtet sind, bedarf es für deren Festlegung einer gerichtsähnlichen ex ante-Kontrolle. Diese hat zu prüfen, ob die gezielt personenbezogene Überwachung zur Verfolgung des Überwachungszwecks den Verhältnismäßigkeitsanforderungen genügt. 188

cc) Im Übrigen liegt die Grenze der möglichen Ermächtigung zu einer anlass-losen Überwachung dort, wo der Einsatz eines personenbezogenen Suchbegriffs von vornherein mit annähernd vergleichbarer Sicherheit und Wirkung wie eine Einzelanordnung zu einer individualisierenden Überwachung des Telekommunikationsverkehrs führt. Der Gesetzgeber muss sicherstellen, dass dann die diesbezüglichen Anforderungen (vgl. BVerfGE 141, 220 <268 ff. Rn. 103 ff.; 309 ff. Rn. 228 ff.>) gewahrt und durch die strategische Überwachung nicht unterlaufen werden. 189

dd) Auf die genannten Maßgaben und Beschränkungen (soeben Rn. 187 ff.) kann der Gesetzgeber nur verzichten, sofern Überwachungsmaßnahmen ausschließlich zur politischen Information der Bundesregierung bestimmt und auf diese ausgerichtet sind und eine Übermittlung der Erkenntnisse an andere Stellen prinzipiell ausgeschlossen ist (oben Rn. 177). 190

f) Gesetzlicher Beschränkungen bedarf die Ermächtigung zur strategischen Überwachung auch, soweit mit ihr eine gesamthaft bevorratende Speicherung von Verkehrsdaten eröffnet wird. Der Gesetzgeber hat sicherzustellen, dass die hierfür erfassten Datenströme substantiell begrenzt bleiben und eine Höchstspeicherungsdauer von sechs Monaten (vgl. auch BVerfGE 125, 260 <322>) nicht überschritten werden darf. 191

g) Für die einzelnen Schritte der Auswertung der erfassten Daten reicht es, wenn der Gesetzgeber die wesentlichen Grundlagen vorgibt und die nähere Strukturierung im Übrigen dem Bundesnachrichtendienst zur Regelung durch Binnenrecht aufgibt, das freilich einer unabhängigen objektivrechtlichen Kontrolle unterliegen muss (dazu unten Rn. 272 ff.). Zu den gesetzlich vorzugebenden Rahmenbestimmungen gehören dabei das Gebot einer unverzüglichen Auswertung der erfassten Daten (vgl. BVerfGE 100, 313 <385 f.>; 125, 260 <332>; siehe auch die entsprechende Regelung in § 6 Abs. 1 Satz 1 G 10 und die zugehörigen Gesetzgebungsmaterialien BT-Drucks 14/5655, S. 13), die Geltung des Verhältnismäßigkeitsgrundsatzes bei der Auswahl der Suchbegriffe – wie derzeit bereits untergesetzlich in den Dienstvorschriften vorgesehen –, Regelungen zum Einsatz von eingriffsintensiven Methoden 192

der Datenauswertung, insbesondere komplexe Formen des Datenabgleichs (vgl. zur besonderen Erforderlichkeit von Auswertungsregelungen bei der strategischen Überwachung auch EGMR, Big Brother Watch and others v. United Kingdom, Urteil vom 13. September 2018, Nr. 58170/13 u.a., §§ 346 f.) sowie die Beachtung der grundgesetzlichen Diskriminierungsverbote (vgl. zu dieser Anforderung BVerfGE 115, 320 <348>; 133, 277 <359 f. Rn. 189>; zur schwedischen Rechtslage insoweit EGMR, Centrum för Rättvisa v. Sweden, Urteil vom 19. Juni 2018, Nr. 35252/08, § 29). Zu regeln ist gegebenenfalls auch der Einsatz von Algorithmen, insbesondere die Sicherstellung ihrer grundsätzlichen Nachvollziehbarkeit in Blick auf eine unabhängige Kontrolle.

h) Besondere Anforderungen sind an den Schutz von Vertraulichkeitsbeziehungen – wie insbesondere zwischen Journalisten und ihren Informanten oder Rechtsanwälten und ihren Mandanten – zu stellen. Dieser Schutz folgt schon aus Art. 10 Abs. 1 GG und den sich hieraus ableitenden Verhältnismäßigkeitsanforderungen. Er entspricht einem in solchen Beziehungen gesteigerten Schutzbedarf, der auf beiden Seiten der Kommunikation bestehen kann. Für die betroffenen Berufsgruppen wird der Schutz zugleich durch Art. 5 Abs. 1 Satz 2 GG oder die jeweils sonst ihren Schutz gewährleistenden Grundrechte – sofern dem personellen Schutzbereich nach gegenüber der Auslandsaufklärung anwendbar – abgesichert. 193

aa) Gegenüber Berufs- und Personengruppen, deren Kommunikationsbeziehungen einen besonderen Schutz der Vertraulichkeit verlangen, ist zunächst deren gezielte Überwachung zu begrenzen. Die Nutzung von Suchbegriffen, die zu einer gezielten Erfassung der Telekommunikationsanschlüsse solcher Personen führen, kann nicht schon allein damit gerechtfertigt werden, dass hierdurch potentiell nachrichtendienstlich relevante Informationen erlangt werden können. Die journalistische Tätigkeit rechtfertigt nicht, Personen einem höheren Risiko der Überwachung auszusetzen als andere Grundrechtsträger und sie wegen ihrer Kontakte und Recherchen zum Objekt der Informationsabschöpfung zur Verfolgung von Sicherheitsinteressen zu machen (vgl. BVerfGE 107, 299 <336>). Entsprechendes gilt für Rechtsanwältinnen und Rechtsanwälte. Deren gezielte Überwachung als Nachrichtenmittler ist hier vielmehr auch im Rahmen der strategischen Überwachung an qualifizierte Eingriffsschwellen zu binden. Danach ist sicherzustellen, dass das Eindringen in Vertraulichkeitsbeziehungen nur zur Aufklärung von im Einzelfall schwerwiegenden Gefahren und besonders schweren Straftaten beziehungsweise zur Ergreifung bestimmter gefährlicher Straftäter zulässig ist. Es bedarf hierfür belastbarer Erkenntnisse. Im Übrigen ist eine Überwachung und Auswertung nur nach Maßgabe einer Abwägung zulässig, wonach das öffentliche Interesse an der Information das Interesse der Betroffenen an dem Schutz der Vertraulichkeit im Einzelfall überwiegt (vgl. BVerfGE 129, 208 <258 ff.>; 141, 220 <318 f. Rn. 255 ff.>). Der Gesetzgeber wird zu prüfen haben, ob und wieweit hier zwischen verschiedenen Vertraulichkeitsbeziehungen weiter zu differenzieren ist (vgl. § 160a StPO; dazu BVerfGE 129, 208 <259 f.>). Abzusichern ist ihr Schutz jedenfalls grundsätzlich durch eine gerichtsähnliche ex ante-Kontrolle. 194

Soweit die Erfassung von besonders schutzwürdigen Vertraulichkeitsbeziehungen erst im Rahmen der Auswertung bemerkt wird, bedarf es auch insoweit einer Prüfung der Voraussetzungen und gegebenenfalls dann einer Abwägung, ob die entsprechende Kommunikation ausgewertet und genutzt werden darf (zutreffend Löffelmann, in: Dietrich/Gärditz/Graulich/Gusy/Warg [Hrsg.], Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 33 <43 mit Fn. 41>; entgegen Gärditz, DVBl 2017, S. 525 <528>). Auch hier kommt es darauf an, ob zu erwarten ist, dass hierdurch Erkenntnisse über schwerwiegende und sich konkret abzeichnende Gefahren gewonnen werden und dem öffentlichen Interesse hieran gegenüber dem Schutz der Vertraulichkeit nach Maßgabe einer Abwägung im Einzelfall der Vorrang zukommt. Auch diese Entscheidung bedarf einer gerichtsähnlichen Kontrolle. 195

bb) Der Gesetzgeber kann für den Schutz von Berufsgruppen und deren Tätigkeit im Rahmen der Auslandsaufklärung den verschiedenen Umständen, unter denen die Presse oder Anwaltschaft in anderen Ländern tätig ist, Rechnung tragen. Er kann danach den Schutz auf Personen und Situationen beschränken, die tatsächlich schutzwürdig sind, deren Tätigkeit also durch die Freiheit und Unab- hängigkeit gekennzeichnet ist, die den besonderen grundrechtlichen Schutz dieser Institutionen rechtfertigen (vgl. Dietrich, in: Schenke/Graulich/Ruthig [Hrsg.], Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 6 BNDG Rn. 10 a.E.). Maßgeblich sind insoweit die sich aus den Grundrechten des Grundgesetzes ergebenden Wertentscheidungen, die ihrerseits in die internationalen Verbürgungen der Menschenrechte eingebettet sind (vgl. Art. 1 Abs. 2 GG). Unsicherheiten ist auf der Grundlage informierter Einschätzungen zu begegnen. 196

cc) Zu prüfen, ob und wieweit anderen Vertraulichkeitsbeziehungen durch Schutzmaßnahmen zu entsprechen ist, ist zunächst Sache des Gesetzgebers. 197

dd) Sofern Überwachungsmaßnahmen unabhängig von einem sie rechtfertigenden Zweck der Gefahrenfrüherkennung ausschließlich dazu bestimmt und darauf ausgerichtet sind, der politischen Information der Bundesregierung zu dienen und eine Übermittlung der Erkenntnisse an andere Stellen prinzipiell ausgeschlossen ist (oben Rn. 177), kann auf den Schutz von Vertraulichkeitsbeziehungen verzichtet werden, soweit dies erforderlich ist. 198

i) Weitere Anforderungen ergeben sich aus Art. 10 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG zum Schutz des Kernbereichs privater Lebensgestaltung. 199

aa) Der Schutz des Kernbereichs privater Lebensgestaltung gewährleistet dem Individuum einen Bereich höchstpersönlicher Privatheit und sichert einen dem Staat nicht verfügbaren Menschenwürdekern grundrechtlichen Schutzes gegenüber Überwachung. Selbst überragende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Bereich privater Lebensgestaltung nicht rechtfertigen (vgl. BVerfGE 109, 279 <313>; 141, 220 <276 Rn. 120>; stRspr). Dies gilt auch gegenüber Nachrichtendiensten (vgl. BVerfGE 120, 274 <335 ff.>) und auch für Über- 200

wachungsmaßnahmen im Ausland.

Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge, Überlegungen und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen. Geschützt ist insbesondere die nichtöffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens, die in der berechtigten Annahme geführt wird, nicht überwacht zu werden. Solche Gespräche verlieren dabei nicht schon dadurch ihren Charakter als insgesamt höchstpersönlich, dass sich in ihnen Höchstpersönliches und Alltägliches vermischen (vgl. BVerfGE 141, 220 <276 f. Rn. 121; 279 Rn. 128; 314 f. Rn. 243>; stRspr). 201

Demgegenüber gehören die Besprechung und Planung von Straftaten nicht zum Kernbereich privater Lebensgestaltung, selbst wenn sie auch Höchstpersönliches zum Gegenstand haben. Dies bedeutet nicht, dass der Kernbereich unter einem allgemeinen Abwägungsvorbehalt in Bezug auf öffentliche Sicherheits- interessen steht. Ein höchstpersönliches Gespräch fällt nicht dadurch aus dem Kernbereich privater Lebensgestaltung heraus, dass die Kenntnis seiner Inhalte für die Aufklärung von Straftaten oder die Abwehr von Gefahren hilfreiche Aufschlüsse geben kann. Geben Äußerungen hierbei ausschließlich innere Eindrücke und Gefühle wieder, ohne Hinweise auf konkrete Straftaten zu enthalten, gewinnen sie nicht schon dadurch einen Gemeinschaftsbezug, dass sie Ursachen oder Beweggründe eines strafbaren Verhaltens freizulegen vermögen. Auch können trotz Straftatenbezugs Situationen, in denen Einzelnen gerade ermöglicht werden soll, ein Fehlverhalten einzugestehen oder sich auf dessen Folgen einzurichten, wie Beichtgespräche oder vertrauliche Gespräche mit einem Psychotherapeuten oder einem Strafverteidiger, der höchstpersönlichen Privatsphäre unterfallen (vgl. hierzu näher BVerfGE 141, 220 <276 f. Rn. 121 f.>; stRspr). 202

bb) Der Gesetzgeber hat den Schutz des Kernbereichs privater Lebensgestaltung durch eigene Regelungen abzusichern. 203

Absolut auszuschließen ist insoweit zunächst, den Kernbereich zum Ziel staatlicher Ermittlungen zu machen und diesbezügliche Informationen in irgendeiner Weise zu verwerten oder sonst zur Grundlage der weiteren Ermittlungen zu nehmen. Das gilt auch für die strategische Überwachung. Dabei darf das Verständnis des Kernbereichs entsprechend dem dargelegten Verständnis nicht auf Situationen begrenzt werden, in denen „allein“ höchstpersönliche Fragen Gegenstand sind. 204

Des Weiteren muss dem Kernbereichsschutz grundsätzlich auf zwei Ebenen Rechnung getragen werden: auf der Ebene der Datenerhebung und auf der Ebene der Datenauswertung. Die Anforderungen an die gesetzliche Sicherstellung dieses Schutzes unterscheiden sich insoweit jedoch nach der Art der in Frage stehenden Überwachungsmaßnahme (vgl. BVerfGE 141, 220 <279 Rn. 127>). 205

Für die Datenerhebung und den Einsatz von Suchbegriffen sind danach für die strategische Überwachung weitere, über das Verbot der gezielten Kernbereichs- erfas- 206

sung hinausgehende gesetzliche Vorkehrungen nicht geboten. Da sich aus den Suchbegriffen als solchen in der Regel nicht erkennen lässt, dass mit signifikanter Wahrscheinlichkeit kernbereichsrelevante Kommunikation erfasst wird, bedarf es keiner spezifischen Regelungen, die darauf gerichtet sind, kernbereichsrelevante Selektoren im Vorfeld auszusondern. Dies lässt unberührt, dass, soweit der Einsatz von Suchbegriffen erkennbar eine erhebliche Wahrscheinlichkeit der Erfassung kernbereichsrelevanter Kommunikation birgt, diese nach Möglichkeit informationstechnisch schon im Vorfeld von der Erhebung ausgeschlossen werden muss (vgl. BVerfGE 141, 220 <306 f. Rn. 218 ff.>).

Demgegenüber ist dann aber auf der Ebene der händischen Datenauswertung gesetzlich sicherzustellen, dass die weitere Auswertung unverzüglich unterbrochen werden muss, wenn erkennbar wird, dass eine Überwachung in den Kernbereich persönlicher Lebensgestaltung eindringt; schon bei Zweifeln darf ihre Fortsetzung – vorbehaltlich von Regelungen für Eilfälle (vgl. BVerfGE 141, 220 <280 Rn. 129>) – nur in Form von Aufzeichnungen erlaubt werden, die vor ihrer Auswertung von einer unabhängigen Stelle zu sichten sind (vgl. BVerfGE 141, 220 <279 f. Rn. 129>; siehe auch § 3a Satz 2 bis 11 G 10). Dabei ist klarzustellen, dass Erkenntnisse aus dem höchstpersönlichen Lebensbereich nicht verwertet werden dürfen und unverzüglich zu löschen sind; dies ist zu protokollieren und die Löschungsprotokolle müssen zur Gewährleistung einer datenschutzrechtlichen Kontrolle hinreichend lang aufbewahrt werden (vgl. BVerfGE 141, 220 <280 Rn. 129>; siehe auch unten Rn. 289 ff.). 207

j) Zu den Verhältnismäßigkeitsanforderungen an Überwachungsmaßnahmen gehört auch die Vorgabe von Löschungspflichten. Mit ihnen ist sicherzustellen, dass eine Verwendung personenbezogener Daten auf die die Datenverarbeitung rechtfertigenden Zwecke begrenzt bleibt und nach deren Erledigung nicht mehr möglich ist (vgl. BVerfGE 65, 1 <46>; 133, 277 <366 Rn. 206>; 141, 220 <285 f. Rn. 144>; stRspr). 208

Für Überwachungsmaßnahmen, die – wie vorliegend – mittels der Erfassung großer Datenströme arbeiten, auf die sie aber nur teilweise auswertend zugreifen dürfen, haben Löschungsregelungen normenklar sicherzustellen, dass die zunächst miterfassten Daten, die verfassungsrechtlich der inhaltlichen Sichtung entzogen sind, sofort ausgesondert sowie spurenlos und endgültig gelöscht werden. Soweit die Auswertung der Daten sich dann in mehreren Schritten vollzieht, in denen die Datenmenge immer weiter eingegrenzt wird, bedarf es normenklarer Regelungen, die eine zügige Auswertung sowie anschließend auf jeder Stufe eine unverzügliche Löschung der ausgesonderten Daten vorsehen (vgl. BVerfGE 100, 313 <385; 400>). Soweit Informationen als relevant eingestuft werden und in Blick auf eine weitere Verwendung länger gespeichert werden sollen, sind hierfür entsprechende Regelungen zu schaffen. Dabei sind in hinreichend engen Abständen Prüfpflichten vorzusehen (vgl. etwa § 6 Abs. 1 G 10; dazu BVerfGE 100, 313 <400>), die verhindern, dass Daten ohne Rechtfertigung gespeichert bleiben. 209

Die zentralen Schritte der Datenlöschung müssen, soweit dies für eine unabhängige Kontrolle sinnvoll und erforderlich ist, protokolliert werden; die Löschungsprotokolle müssen hinreichend lange aufbewahrt werden, um eine effektive Kontrolle zu ermöglichen (vgl. BVerfGE 141, 220 <302 f. Rn. 205>; siehe auch unten Rn. 291). 210

III.

Personenbezogene Daten aus der strategischen Überwachung dürfen nur dann an andere Stellen übermittelt werden, wenn die Übermittlung durch eine normenklare und hinreichend bestimmte Rechtsgrundlage an den Schutz von Rechtsgütern und an Eingriffsschwellen gebunden wird, die dem Eingriffsgewicht der strategischen Überwachung Rechnung tragen. Übermittlungen sind danach nur zum Schutz besonders gewichtiger Rechtsgüter gerechtfertigt und setzen als Übermittlungsschwelle eine konkretisierte Gefahrenlage oder einen hinreichend konkretisierten Tatverdacht voraus. Anderes gilt für Berichte an die Bundesregierung, soweit diese ausschließlich der politischen Information und Vorbereitung von Regierungsentscheidungen dienen. 211

1. Die Übermittlung personenbezogener Daten, mit der eine Behörde die von ihr erhobenen Daten einer anderen Stelle zugänglich macht, begründet einen eigenen Grundrechtseingriff (vgl. BVerfGE 100, 313 <367>; 141, 220 <334 Rn. 305>; stRspr). Dieser ist an dem Grundrecht zu messen, in das bei der ursprünglichen Datenerhebung eingegriffen wurde (vgl. BVerfGE 100, 313 <367>; 141, 220 <334 Rn. 305>; stRspr). 212

2. Als neuerliche Grundrechtseingriffe bedürfen Übermittlungen einer eigenen normenklaren und hinreichend bestimmten Rechtsgrundlage (vgl. BVerfGE 65, 1 <46>; 100, 313 <389>; stRspr). 213

Der eigene Eingriffscharakter der Datenübermittlung schließt – bezogen auf die hier in Frage stehenden Daten aus besonders eingriffsintensiven Überwachungsmaßnahmen – eine Übermittlung oder einen Austausch von Daten ohne spezifische Rechtsgrundlagen aus, denen insoweit auch eine Warn- und Verdeutlichungsfunktion zukommt. 214

Die Normenklarheit setzt der Verwendung gesetzlicher Verweisungsketten Grenzen. An einer normenklaren Rechtsgrundlage fehlt es zwar nicht schon deshalb, weil in einer Norm auf eine andere Norm verwiesen wird. Doch müssen Verweisungen begrenzt bleiben, dürfen nicht durch die Inbezugnahme von Normen, die andersartige Spannungslagen bewältigen, ihre Klarheit verlieren und in der Praxis nicht zu übermäßigen Schwierigkeiten bei der Anwendung führen. Unübersichtliche Verweisungskaskaden sind mit den grundrechtlichen Anforderungen daher nicht vereinbar (vgl. BVerfGE 110, 33 <57 f.; 61 ff.>). 215

3. Materiell müssen sowohl die gesetzlichen Ermächtigungen zur Datenübermittlung als auch die Übermittlungsmaßnahmen im Einzelfall den Anforderungen der Verhältnismäßigkeit genügen (vgl. BVerfGE 65, 1 <45 f.>; 100, 313 <390 ff.>; 141, 220 <327 Rn. 286>). Die Übermittlung muss zur Erreichung eines legitimen Zwecks 216

geeignet und erforderlich sein. Ausgangspunkt für die Bestimmung der Verhältnismäßigkeit im engeren Sinne ist nach ständiger Rechtsprechung das Gewicht der in der Übermittlung liegenden Zweckänderung gegenüber dem Zweck der Datenerhebung und, hieran anknüpfend, das Kriterium der hypothetischen Datenneuerhebung. Danach kommt es darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln neu erhoben werden dürften (vgl. BVerfGE 141, 220 <327 ff. Rn. 287 ff.>).

Für die vorliegende Konstellation sind insoweit allerdings Besonderheiten zu beachten. Während Behörden normalerweise Daten für spezifische eigene operative Zwecke erheben und die Übermittlung an eine andere Behörde diese dann einem neuen Zweck zuführt, erhebt der Bundesnachrichtendienst seine Daten nicht zu eigenen operativen Zwecken, sondern von vornherein allein mit dem Ziel, diese – nach Herausfilterung und Aufbereitung der relevanten Informationen – an die Bundesregierung und gegebenenfalls weitere Stellen weiterzuleiten (vgl. § 1 Abs. 2 BNDG). Auch zeichnen sich die Befugnisse zur Datenerhebung vorliegend dadurch aus, dass sie nicht an objektivierte Eingriffsschwellen gebunden, sondern im Wesentlichen nur final angeleitet sind. 217

Gerade für diese Konstellation ist die Beachtung gehaltvoller Übermittlungs- anforderungen damit aber von besonderer Bedeutung. Wenn schon die Daten- erhebung für die Auslandsaufklärung selbst keine nachprüfbaren Eingriffsschwellen voraussetzt und damit ermöglichen soll, bereits weit im Vorfeld von konkreten Gefahren Bedrohungen und Gefährdungen zu ermitteln und nach ihnen proaktiv zu suchen, setzt dies verfassungsrechtlich im Gegenzug voraus, dass entsprechende Eingriffsschwellen wenigstens für die Übermittlung der hieraus gezogenen Erkenntnisse gelten müssen (vgl. Gärditz, DVBl 2017, S. 525 <526>). Der Zweck der Datenerhebung und der Zweck der Datenübermittlung rücken insofern zusammen: Dem Nachrichtendienst sind weitreichende Aufklärungsbefugnisse übertragen, damit er auf der Grundlage einer großen Menge weithin auch unstrukturierter Daten wichtige Informationen im Vorfeld operativer Tätigkeit herausfiltern kann. In der Unterscheidung zwischen relevanten und irrelevanten Daten, die darüber bestimmt, welche Informationen der Regierung und gegebenenfalls mit Handlungsbefugnissen ausgestatteten weiteren Stellen zur Kenntnis gebracht werden, liegt ein wesentlicher Zweck der Datenerhebung. Insoweit ist dann aber auf Ebene der Übermittlungsnormen sicherzustellen, dass die aufgrund im Wesentlichen anlassloser Befugnisse gewonnenen Erkenntnisse nur der weiteren Verarbeitung zugänglich werden, wenn eine Erhebung der Daten nach allgemeinen rechtsstaatlichen Anforderungen für die Übermittlungszwecke gerechtfertigt wäre. 218

Danach kommt es für die Verfassungsmäßigkeit der Übermittlung auch hier darauf an, ob die Daten nach verfassungsrechtlichen Maßstäben für den Übermittlungszweck mit vergleichbar eingriffsintensiven Mitteln erhoben werden dürften (vgl. BVerfGE 141, 220 <328 Rn. 288>). Weil den Sicherheitsbehörden ein so weit- reichendes Instrument wie die anlasslose Telekommunikationsüberwachung inner- 219

staatlich von vornherein nicht zur Verfügung gestellt werden darf, gelten – sofern nicht Berichte allein an die Bundesregierung in Frage stehen (unten Rn. 223 ff.) – die verfassungsrechtlichen Anforderungen, die sonst für andere besonders schwere Eingriffsmaßnahmen wie die Wohnraumüberwachung oder die Online-Durch- suchung gelten (vgl. BVerfGE 141, 220 <271 Rn. 110; 273 f. Rn. 115 f.; 327 ff. Rn. 287 ff.>). Das entspricht dem Erfordernis eines herausragenden öffentlichen Interesses und hinreichend konkreter und qualifizierter Übermittlungsschwellen, wie vom Bundesverfassungsgericht für Übermittlungen nachrichtendienstlicher Informationen an operativ tätige Behörden auch in der Entscheidung zum Antiterrordateigesetz verlangt wurde (vgl. BVerfGE 133, 277 <329 Rn. 123>), und konkretisiert dieses.

4. Danach sind Anforderungen sowohl an den Rechtsgüterschutz als auch an die Eingriffsschwellen, hier in Form von Übermittlungsschwellen, zu stellen. Dabei ist jeweils zwischen Übermittlungen zur Gefahrenabwehr und zur Strafverfolgung zu unterscheiden (vgl. BVerfGE 100, 313 <394>; 141, 220 <270 f. Rn. 107 f.>). 220

Was den Rechtsgüterschutz betrifft, ist nach diesen Kriterien eine Übermittlung zur Gefahrenabwehr nur zum Schutz von Rechtsgütern zulässig, die besonders gewichtig sind (vgl. BVerfGE 125, 260 <329 f.>; 133, 277 <365 Rn. 203>; 141, 220 <270 Rn. 108>). Die Übermittlung muss, soweit es das Gesetz als Zweckänderung so vorsieht, nicht auf den Schutz desselben Rechtsguts gerichtet sein wie die nachrichtendienstliche Überwachungsanordnung. Abzustellen ist dabei grundsätzlich unmittelbar auf Rechtsgüter selbst, nicht auf Kataloge von Straftaten; jedenfalls darf ein Verweis auf Straftaten nicht Situationen erfassen, in denen die Strafbarkeitsschwelle durch die Pönalisierung von Vorbereitungshandlungen oder bloßen Rechtsgutgefährdungen ins Vorfeld von Gefahren verlagert wird (vgl. BVerfGE 125, 260 <329 f.>). Eine Übermittlung zu Zwecken der Strafverfolgung ist demgegenüber durch das Erfordernis eines gesteigerten Gewichts der in Frage stehenden Straf- taten zu begrenzen. Gerechtfertigt ist sie nach diesen Kriterien nur zur Verfolgung besonders schwerer Straftaten. Diese werden in der Regel durch Straftatenkataloge näher zu konkretisieren sein. 221

Was die Übermittlungsschwellen betrifft, bedarf es für die Gefahrenabwehr insoweit einer hinreichend konkret absehbaren Gefahrenlage. Zwar muss der Gesetzgeber Übermittlungen nicht nach dem tradierten sicherheitsrechtlichen Modell von der Abwehr einer konkreten, unmittelbar bevorstehenden oder gegenwärtigen Gefahr abhängig machen. Zu verlangen ist jedoch eine hinreichend konkretisierte Gefahr in dem Sinne, dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen (vgl. hierzu näher BVerfGE 141, 220 <271 ff. Rn. 111 ff.>). Soweit Daten zur Strafverfolgung übermittelt werden, bedarf es genügend konkretisierter Tatsachen, die den Verdacht einer besonders schweren Straftat begründen. Hierfür genügen nicht bloße Anhaltspunkte, wie sie ausreichen, um erste allgemeine Ermittlungen einzuleiten (vgl. § 152 Abs. 2 StPO), sondern bedarf es bestimmter Tatsachen für den Verdacht solcher Straftaten (vgl. BVerfGE 125, 260 <328 f.>), wie sie etwa auch eine Wohnraumüberwachung nach § 100c StPO 222

rechtfertigen könnten. Es müssen insoweit konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht vorliegen (vgl. Bruns, in: Karlsruher Kommentar zur StPO, 8. Aufl. 2019, § 100c Rn. 10 m.w.N.).

5. Anders liegt es, soweit die Übermittlung von Erkenntnissen aus der strategischen Überwachung an die Bundesregierung allein in ihrer Regierungsfunktion in Frage steht. Wenn es um die Information der Bundesregierung zur Wahrnehmung ihrer außen- und sicherheitspolitischen Verantwortung geht und eine Weiterleitung an andere Stellen ausgeschlossen ist, sind Anforderungen an einen qualifizierten Rechtsgüterschutz oder an Übermittlungsschwellen verfassungsrechtlich nicht geboten. 223

a) Solche weiteren Anforderungen sind hier entbehrlich, weil es sich bei der Information der Bundesregierung über Sachverhalte von außen- und sicherheitspolitischer Bedeutung um die Erfüllung des primären Zwecks der Auslandsaufklärung handelt, an dem ein überragendes öffentliches Interesse auch unabhängig von konkretisierten Gefahrenlagen anzuerkennen ist. 224

Vor allem hat der Grundrechtseingriff gegenüber den überwachten Personen bei der bloßen politischen Information der Bundesregierung in der Regel ein deutlich geringeres Gewicht. Soweit nicht Informationen zu Personen in unmittelbar staatspolitischen Funktionen des Auslands in Frage stehen, gegenüber denen das öffentliche Interesse eine Überwachung grundsätzlich rechtfertigen kann, wird es im Rahmen solcher Berichte auf personenbezogene Daten oft schon nicht ankommen, so dass diese ausgesondert werden können und gegebenenfalls müssen. Aber auch soweit es erforderlich ist, personenbezogene Informationen in die Berichte aufzunehmen, unterscheiden sich solche Berichte grundlegend von der Übermittlung von Erkenntnissen über Einzelpersonen an innerstaatliche Behörden, die ihrerseits – mittelbar oder unmittelbar – mit eigenen Handlungsbefugnissen ausgestattet sind und diese unter Umständen auch gegenüber den Betroffenen einsetzen können. Das gilt erst recht im Vergleich mit der Übermittlung an ausländische Stellen. Bei der Nutzung als Hintergrundinformation der Bundesregierung oder als Grundlage zur Vorbereitung ihrer Regierungsentscheidungen verblasst typischerweise das Interesse an den konkret betroffenen Privatpersonen, so dass die Übermittlung auch unabhängig von der Einhaltung konkreter Übermittlungsschwellen gerechtfertigt werden kann. 225

Solche Berichte an die Bundesregierung dienen allerdings allein der politischen Information auf Regierungsebene. Soweit die Informationen unabhängig von einer Übermittlungsschwelle zur Verfügung gestellt werden, ist ihre Nutzung daher auf Entscheidungen der Bundesregierung selbst in Fragen der Außen- und Sicherheitspolitik beschränkt. Auf diese kann sie – auch in der Kommunikation mit ausländischen Regierungen und internationalen Organisationen – zu ihrer Aufgabenwahrnehmung zurückgreifen, soweit nicht eine Weitergabe an nachgeordnete Behörden im In- und Ausland zu anderen, insbesondere auch operativen Zwecken erfolgt. Gleiches gilt für die Kommunikation der Bundesregierung mit den Regierungen der Länder. 226

b) Soweit die Informationen aus Überwachungsmaßnahmen stammen, die auf Zwe- 227

cke der Gefahrenfrüherkennung gestützt wurden und damit – wie in der Praxis bisher wohl in der Regel – sowohl der allgemeinen Information der Bundesregierung als auch der Frühaufklärung von Gefahren zu dienen bestimmt sind, können entsprechende Erkenntnisse zwar über die Zwecke der Regierungsarbeit hinaus verwertet werden. Sollen Informationen in diesem Sinne über die Bundesregierung oder über Landesregierungen an andere operativ tätige Stellen – wie insbesondere Sicherheitsbehörden oder die innerstaatliche Verwaltung – weitergeleitet werden, setzt dies aber, wie die unmittelbare Übermittlung der Daten an andere Stellen, gesetzliche Übermittlungsermächtigungen voraus, die den genannten Anforderungen an einen qualifizierten Rechtsgüterschutz und das Vorliegen von Eingriffsschwellen genügen.

c) Selbst auf der Grundlage eigener Übermittlungsvorschriften scheidet eine Weiterleitung an andere Stellen allerdings prinzipiell aus, wenn Daten aus Über- wachungsmaßnahmen stammen, die von vornherein nicht auch durch Ziele der Gefahrenfrüherkennung gerechtfertigt wurden und unabhängig von gefahren- bezogenen Aufklärungsinteressen allein zur politischen Information der Bundes- regierung durchgeführt wurden (oben Rn. 177 und Rn. 226). In diesen Fällen ist eine Übermittlung der Erkenntnisse an andere Stellen auch im Wege der regulären Zweckänderung nicht möglich. Eine Ausnahme hiervon kann der Gesetzgeber nur dann vorsehen, soweit die Daten aus sich heraus eine unmittelbar bevorstehende Gefahr für Leib, Leben oder Freiheit einer Person, für lebenswichtige Güter der Allgemeinheit oder für den Bestand oder die Sicherheit des Bundes oder eines Landes erkennen lassen (entsprechend oben Rn. 174). 228

6. Da die Übermittlung von Daten an andere Stellen einen eigenen Grundrechtseingriff begründet, setzt sie – ebenso wie umgekehrt die Übermittlung personen- bezogener Daten seitens anderer Behörden an den Bundesnachrichtendienst – eine förmliche Entscheidung voraus, bei der die jeweiligen gesetzlichen Übermittlungsvoraussetzungen geprüft werden müssen. Dafür trägt der Bundesnachrichtendienst angesichts seiner weiten Befugnisse eine besondere Verantwortung. So wie ihm einerseits besonders weite Befugnisse zukommen, die zum frühzeitigen Aufspüren von Gefahrenquellen die anlasslose Erfassung personenbezogener Daten erlauben, muss er anderseits die gewonnenen Informationen vor ihrer Übermittlung sorgfältig sichten und diese in Anwendung der jeweils einschlägigen Übermittlungsvorschriften auf das notwendige Maß beschränken. Die Übermittlung ist – sofern es nicht unmittelbar um Berichte allein an das Bundeskanzleramt oder einzelne Bundesminister und deren regierungspolitische Nutzung geht – zu protokollieren, um die Beachtung der Übermittlungsvoraussetzungen einer unabhängigen Kontrolle zugänglich zu machen (vgl. BVerfGE 141, 220 <340 f. Rn. 322>; siehe auch unten Rn. 291). Dabei ist auch die der Übermittlung zugrundegelegte Rechtsvorschrift zu nennen. 229

Die Möglichkeit, für die Verknüpfung von an verschiedenen Stellen vorhandenen Informationen und die Anbahnung ihres Austauschs auf Verbunddateien wie nach dem 230

Antiterrordateigesetz zurückzugreifen, bleibt hiervon unberührt (zu den diesbezüglichen verfassungsrechtlichen Anforderungen BVerfGE 133, 277 <320 ff. Rn. 105 ff.>).

7. Besondere Anforderungen gelten für die Übermittlung von Daten an ausländische Stellen. In Frage stehen hier zunächst – unabhängig von einer möglichen Einbindung in Kooperationen – Übermittlungen von Erkenntnissen im Einzelfall (zur automatisierten Datenübermittlung im Rahmen von Kooperationen siehe unten Rn. 254 ff. und 262 ff.). 231

a) Zum einen gelten die genannten Anforderungen an Rechtsgüterschutz und Eingriffsschwellen wie für die Übermittlung von Daten an inländische Stellen (oben Rn. 216 ff. und 220 ff.). Der Gesetzgeber ist insoweit nicht gehindert, bei der begrifflichen Ausgestaltung der Ermächtigungen der Eigenständigkeit ausländischer Rechtsordnungen Rechnung zu tragen; dies stellt das materielle Schutzniveau jedoch nicht in Frage (vgl. BVerfGE 141, 220 <343 Rn. 331>). 232

b) Zum anderen bedarf die Übermittlung von Daten ins Ausland aber als eigene Voraussetzung einer Rechtsstaatlichkeitsvergewisserung über den Umgang der ausländischen Stellen mit den ihnen übermittelten Daten. Das trägt dem Umstand Rechnung, dass der Umgang mit den von deutschen Behörden erhobenen Daten nach Übermittlung in das Ausland einerseits nicht mehr den Anforderungen des Grundgesetzes unterliegt, da die ausländische Staatsgewalt nur ihren eigenen rechtlichen Bindungen verpflichtet ist, anderseits die deutsche Staatsgewalt aber bei der Übermittlung an die Grundrechte gebunden ist und für die Übermittlung die Verantwortung trägt (vgl. BVerfGE 141, 220 <342 Rn. 326 f.>). 233

Nach der Rechtsprechung betreffen die diesbezüglichen Anforderungen zum einen die Wahrung datenschutzrechtlicher Garantien (aa) und zum anderen die Wahrung der Menschenrechte bei der Nutzung der Informationen (bb) seitens des Empfängerstaats. Für beides bedarf es normenklarer Regelungen, die eine hinreichende Vergewisserung des Bundesnachrichtendienstes sicherstellen (cc). Im Übrigen ist die Wahrung von Übermittlungsgrenzen für die Übermittlung von Daten aus der strategischen Überwachung durch Einholung belastbarer Zusagen der Empfänger zu sichern (dd). 234

aa) Die erste Voraussetzung zielt auf die Wahrung der aus dem Persönlichkeitsrecht folgenden datenschutzrechtlichen Gewährleistungen ab. Allerdings ist nicht erforderlich, dass im Empfängerstaat vergleichbare Regelungen zur Verarbeitung personenbezogener Daten wie nach der deutschen Rechtsordnung gelten oder ein gleichartiger Schutz gewährleistet ist wie nach dem Grundgesetz. Das Grundgesetz anerkennt vielmehr die Eigenständigkeit und Verschiedenartigkeit der Rechts- ordnungen und respektiert sie grundsätzlich auch im Rahmen des Austauschs von Daten. Abgrenzungen und Wertungen müssen nicht mit denen der deutschen Rechtsordnung und auch des deutschen Grundgesetzes übereinstimmen. 235

Erlaubt ist eine Übermittlung der Daten ins Ausland jedoch nur, wenn auch durch den dortigen Umgang mit den übermittelten Daten nicht die Garantien des men- 236

schenrechtlichen Schutzes personenbezogener Daten unterlaufen werden. Dies bedeutet nicht, dass in der ausländischen Rechtsordnung institutionelle und verfahrensrechtliche Vorkehrungen nach deutschem Vorbild gewährleistet sein müssen; insbesondere müssen nicht die formellen und institutionellen Sicherungen vorhanden sein, die datenschutzrechtlich für deutsche Stellen gefordert werden. Geboten ist in diesem Sinne die Gewährleistung eines angemessenen materiellen datenschutzrechtlichen Niveaus für den Umgang mit den übermittelten Daten im Empfängerstaat. In Betracht zu nehmen ist insoweit insbesondere, ob für die Verwendung der Daten die – bei der Übermittlung mitgeteilten – Grenzen durch Zweckbindung und Löschungspflichten sowie grundlegende Anforderungen an Kontrolle und Datensicherheit wenigstens grundsätzlich Beachtung finden. Maßgeblich für diese Beurteilung sind die innerstaatlichen Rechtsvorschriften und die internationalen Verpflichtungen des Empfängerstaats sowie ihre Umsetzung in der täglichen Anwendungspraxis (BVerfGE 141, 220 <344 f. Rn. 334 f.> m.w.N.).

bb) Des Weiteren scheidet eine Datenübermittlung an andere Staaten aus, wenn zu befürchten ist, dass durch die Nutzung der Informationen elementare rechtsstaatliche Grundsätze verletzt werden. Der Staat darf seine Hand nicht zu Verletzungen der Menschenwürde reichen (vgl. BVerfGE 140, 317 <347 Rn. 62>; 141, 220 <342 Rn. 328>). Für die Nutzung im Empfängerstaat muss insbesondere gewährleistet erscheinen, dass die Informationen dort weder zu politischer Verfolgung noch zu unmenschlicher oder erniedrigender Bestrafung oder Behandlung (vgl. Art. 16a Abs. 3 GG) eingesetzt werden. Der Gesetzgeber hat Sorge zu tragen, dass der Schutz der Europäischen Menschenrechtskonvention und der anderen internationalen Menschenrechtsverträge (vgl. Art. 1 Abs. 2 GG) durch eine Übermittlung der von deutschen Behörden erhobenen Daten ins Ausland und an internationale Organisationen nicht ausgehöhlt wird (vgl. BVerfGE 141, 220 <345 Rn. 336>). Angesichts der Spezifika nachrichtendienstlicher Aufklärungs- und Übermittlungstätigkeit, die unter Umständen auch Kontakte mit rechtsstaatlich nicht gefestigten Staaten einschließen kann, ist insbesondere sicherzustellen, dass Informationen nicht dazu genutzt werden, um bestimmte Bevölkerungsgruppen zu verfolgen, Oppositionelle zu unterdrücken, Menschen menschenrechtswidrig oder unter Verstoß gegen humanitäres Völkerrecht zu töten, zu foltern oder sie ohne rechtsstaatliche Verfahren in Haft zu nehmen. Über die Frage, was insoweit die zu beachtenden Völkerrechtsregeln sind, hat sich der Dienst selbst ein Bild zu machen und zu entscheiden. Auch insoweit sind grundsätzlich Auskunftsrechte mit den Empfängerländern zu vereinbaren, die eine nachvollziehende Kontrolle der Einhaltung international-menschenrechtlicher Standards ermöglichen. 237

cc) Zur Wahrung dieser Schutzstandards bedarf es normenklarer gesetzlicher Regelungen, die dem Bundesnachrichtendienst eine Vergewisserung über das Schutzniveau im Ausland aufgeben. Der Dienst hat sich vor der Übermittlung sowohl hinsichtlich der Beachtung der datenschutzrechtlichen als auch der menschenrechtlichen Voraussetzungen zu vergewissern. 238

(1) Die Vergewisserung verlangt nicht in jeder Hinsicht eine umfassende Einzelprüfung oder verbindliche Einzelzusagen, sondern kann sich zunächst auf eine generalisierende tatsächliche Einschätzung der Sach- und Rechtslage in den Empfängerstaaten stützen. Die Prüfung muss aber so gestaltet sein, dass entgegenstehende Tatsachen zur Kenntnis genommen werden und die Einschätzung erschüttert werden kann (vgl. BVerfGE 140, 317 <349 Rn. 69>). Tragen generalisierende Einschätzungen nicht, bedarf es einer mit Tatsachen unterlegten Einzelfallprüfung, aus der sich ergibt, dass die Beachtung jedenfalls der grundlegenden Anforderungen an den Umgang mit Daten hinreichend gewährleistet ist. Erforder-lichenfalls können und müssen verbindliche Einzelgarantien abgegeben werden. Grundsätzlich ist eine verbindliche Zusicherung geeignet, etwaige Bedenken hinsichtlich der Zulässigkeit der Datenübermittlung auszuräumen, sofern nicht im Einzelfall zu erwarten ist, dass die Zusicherung nicht eingehalten wird (vgl. BVerfGE 63, 215 <224>; 109, 38 <62>; 140, 317 <350 Rn. 70>). Welche Anforderungen im Einzelnen gelten, kann der Gesetzgeber auch von einer Einzelfallabwägung abhängig machen (BVerfGE 141, 220 <345 f. Rn. 337 f.>). 239

Da Daten im Rahmen der strategischen Überwachung weithin unabhängig davon erhoben werden, ob die Betroffenen bei objektivierter Sicht in einer Gefahrenlage verfangen sind, sie sich dabei auch auf Umstände in Ländern beziehen, in denen rechtsstaatliche Verhältnisse nicht gesichert sind, und zugleich ihrem Gegenstand nach oft hochpolitische Spannungslagen betreffen, ist dem Bundesnachrichtendienst hierbei besondere Vorsicht abzuverlangen. Auch soweit Einschätzungen zu bestimmten Ländern grundsätzlich generalisiert vorgenommen werden können, bedarf es deshalb stets einer auf die betroffene Person bezogenen Prüfung, wenn es Anhaltspunkte gibt, dass diese durch die Datenübermittlung spezifisch gefährdet werden kann. Soweit sich die Übermittlung auf Daten von schutzwürdigen Journalisten, Rechtsanwälten oder anderen Berufsgruppen bezieht, denen – auch zur Vermeidung ihrer Gefährdung – Vertraulichkeitsschutz zuzu- erkennen ist, bedarf es einer eigenständigen Abwägung, die sich von der allein auf die Inlandsnutzung solcher Daten bezogenen Abwägung (oben Rn. 193 ff.) unterscheidet; sie muss grundsätzlich einer gerichtsähnlichen Vorabkontrolle unterliegen (vgl. United Nations Office of the High Commissioner for Human Rights, Brief der Sonderberichterstatter vom 29. August 2016, OL DEU 2/2016, S. 7). 240

(2) Die Vergewisserung über die Einhaltung des geforderten Schutzniveaus ist eine nicht der freien politischen Disposition unterliegende Entscheidung. Sie hat sich auf gehaltvolle, realitätsbezogene und aktuelle Informationen zu stützen. Sie muss dokumentiert werden und einer unabhängigen Kontrolle zugänglich sein (vgl. BVerfGE 141, 220 <346 Rn. 339>). Für besonders gewichtige oder hinsichtlich der rechtlichen Voraussetzungen schwer zu beurteilende Übermittlungsvorgänge können weitere verfahrensrechtliche Vorkehrungen wie zum Beispiel Behördenleiter- oder Kanzleramtsvorbehalte oder – etwa für die Übermittlung von Informationen über schutzwürdige Journalisten oder Anwälte – eine gerichtsähnliche Vorab- kontrolle erforderlich 241

sein.

dd) Da sich die durch den Bundesnachrichtendienst im Rahmen der strategischen Telekommunikationsüberwachung erhobenen Daten auf anlasslose Über- wachungsmaßnahmen stützen, kommt der Wahrung wirksamer Grenzen für die Übermittlung solcher Erkenntnisse an operative Behörden wie insbesondere an Strafverfolgungs- und Polizeibehörden oder an die innerstaatliche Verwaltung eine besondere Bedeutung zu. Soweit der Bundesnachrichtendienst Erkenntnisse an ausländische Nachrichtendienste übermittelt, ist er deshalb – anknüpfend an die derzeitige Praxis – weiterhin dazu zu verpflichten, diese Übermittlung grundsätzlich von der Zusage abhängig zu machen, dass der ausländische Dienst die Informationen nur mit Zustimmung des Bundesnachrichtendienstes weiterleitet. Unter Umständen kann auch die bloße Zusage des ausländischen Dienstes reichen, dass dieser personenbezogene Erkenntnisse nur dann an andere Stellen weiterleiten wird, wenn ihm belastbare Tatsachen vorliegen, dass die von den Informationen Betroffenen für eine konkrete und besonders schwerwiegende Gefahr verantwortlich oder darin den objektiven Umständen nach verfangen sind oder – soweit es sich um die Weiterleitung an Nachrichtendienste dritter Länder handelt – die Weiter- leitung unter den Vorbehalt einer entsprechenden Zusage gestellt wird (zu Zusagen im Rahmen von Kooperationen siehe unten Rn. 259 ff. und 264). Wie für alle Zusagen setzt dies voraus, dass von der Beachtung solcher Zusagen ausgegangen werden kann und sie durch entsprechende Auskunftsrechte des Bundesnachrichtendienstes gegenüber dem ausländischen Dienst flankiert werden. 242

IV.

Vor besondere verfassungsrechtliche Herausforderungen stellt die Ausgestaltung von Regelungen, die die strategische Telekommunikationsüberwachung für eine Kooperation mit ausländischen Nachrichtendiensten öffnen. Der Gesetzgeber will dem Bundesnachrichtendienst im Rahmen solcher Kooperationen ermöglichen, die von ihm erfassten Datenverkehre auch anhand von Suchbegriffen auszuwerten, die von anderen Nachrichtendiensten bestimmt werden, und die diesbezüglichen Treffer an diese automatisiert weiterzuleiten; überdies sollen Verkehrsdaten auch ohne vorherige Auswertung an die Kooperationspartner weitergeleitet werden. Entsprechend soll umgekehrt der Bundesnachrichtendienst auch Daten und Kapazitäten anderer Dienste nutzen dürfen. Insgesamt sollen so im gegenseitigen Austausch die Datengrundlage für den Einsatz der Suchbegriffe verbreitert und die Kapazitäten effektiver genutzt werden (vgl. BTDrucks 18/9041, S. 29). 243

Grundrechtlichen Anforderungen können solche Regelungen nur dann genügen, wenn die rechtsstaatlichen Grenzen der strategischen Überwachung durch den gegenseitigen Austausch nicht überspielt werden und die Verantwortung des Bundesnachrichtendienstes für die von ihm erhobenen und ausgewerteten Daten im Kern gewahrt bleibt (vgl. Gusy, in: Schenke/Graulich/Ruthig [Hrsg.], Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 1 BNDG Rn. 64). 244

1. Als völkerrechtsfreundliche Ordnung ist das Grundgesetz für solche Kooperationen zwischen Nachrichtendiensten offen. Es verlangt aber eigene gesetzliche Regelungen, die den Schutz der Grundrechte auch im Rahmen der internationalen Zusammenarbeit der Nachrichtendienste gewährleisten. 245

a) Mit der Präambel, Art. 1 Abs. 2, Art. 9 Abs. 2, Art. 16 Abs. 2, Art. 23 bis 26 und Art. 59 Abs. 2 GG bindet das Grundgesetz die Bundesrepublik umfassend in die internationale Gemeinschaft ein und hat es die deutsche öffentliche Gewalt programmatisch auf internationale Zusammenarbeit ausgerichtet (vgl. BVerfGE 141, 220 <341 f. Rn. 325> m.w.N.). Dies gilt auch für die Gewährleistung der Sicherheit. Das Bundesverfassungsgericht hat hervorgehoben, dass eine möglichst effektive Zusammenarbeit mit den Sicherheitsbehörden anderer Staaten hierfür von besonderer Bedeutung sein kann. Ein funktionierender Informationsaustausch kann im Interesse des verfassungsrechtlich gebotenen Schutzes der Menschen eine Übermittlung von im Inland erhobenen Erkenntnissen voraussetzen und im Gegenzug auf Unterrichtungen durch ausländische Stellen angewiesen sein (vgl. BVerfGE 141, 220 <268 Rn. 102>). 246

Entsprechend ist das Grundgesetz für eine Zusammenarbeit des Bundesnachrichtendienstes auch mit anderen Nachrichtendiensten offen. Für die Wahrung der außen- und sicherheitspolitischen Interessen der Bundesrepublik und in diesem Rahmen die Abwehr von Gefahren kann eine solche internationale Zusammen- arbeit von großer Bedeutung sein und an die internationale Offenheit des Grund- gesetzes anknüpfen (vgl. auch BVerfGE 143, 101 <152 ff. Rn. 168 ff.>). Dementsprechend darf der Bundesnachrichtendienst auch dazu ermächtigt werden, seine Befugnisse für Erkenntnisinteressen ausländischer Dienste und Staaten zu nutzen. Maßgeblich ist, dass diese mit einem legitimen Aufklärungsinteresse des Bundesnachrichtendienstes vergleichbar sowie mit den außen- und sicherheitspolitischen Interessen der Bundesrepublik vereinbar sind. Zudem muss die Datenverwendung in einen rechtsstaatlichen Rahmen eingebunden sein. 247

b) Eine Zusammenarbeit bei der Telekommunikationsüberwachung muss allerdings so gestaltet sein, dass der grundrechtliche Schutz gegenüber heimlichen Überwachungsmaßnahmen und die diesbezüglichen Anforderungen an die Datenerhebung, -verarbeitung und -übermittlung nicht unterlaufen werden. Das gilt insbesondere für den Schutz vor Inlandsüberwachung, der nicht durch einen freien Austausch mit Erkenntnissen aus auf Deutschland bezogenen Überwachungsmaßnahmen ausländischer Dienste um seine Wirkung gebracht werden darf. Ein solcher „Ringtausch“ ist insoweit verfassungsrechtlich nicht zulässig. Entsprechendes gilt aber auch für die grundrechtlichen Anforderungen an den Bundesnachrichtendienst hinsichtlich der Fernmeldeaufklärung im Ausland. 248

Danach darf ausländischen Diensten selbst die Befugnis zu Überwachungsmaßnahmen vom Inland aus allenfalls dann eingeräumt oder diesbezüglich eine Duldungszusage erteilt werden, wenn hierzu ein bestimmter Anlass besteht und durch 249

detaillierte Rechtsgrundlagen die uneingeschränkte Geltung des Grundrechtsschutzes materiell-rechtlich und prozedural gesichert ist. Aus der Schutz- dimension der Grundrechte folgt, dass der deutsche Staat Personen, die im Inland dem Schutz seiner Rechtsordnung unterstehen, vor grundrechtswidrigen Über- wachungsmaßnahmen anderer Staaten schützen muss (vgl. Gusy, in: Schenke/Graulich/Ruthig [Hrsg.], Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 1 BNDG Rn. 62). Hiervon können auch Kooperationen nicht freistellen.

c) Im Übrigen bedarf es für die Zusammenarbeit mit ausländischen Nachrichtendiensten eigener Rechtsgrundlagen. Erforderlich sind Regelungen zum einen, soweit dem Bundesnachrichtendienst der Zugriff auf Überwachungsmöglichkeiten anderer Dienste und die Erlangung und Nutzung der von diesen erhobenen Daten eröffnet werden sollen. Zu regeln sind insoweit sowohl die Übermittlung von Suchbegriffen durch den Bundesnachrichtendienst an einen ausländischen Dienst zur Nutzung und Auswertung als auch der Abruf oder die Entgegennahme seitens der Partner zugänglich gemachter Datenbestände oder Datenströme zur eigenen Auswertung durch den Bundesnachrichtendienst mittels Selektoren oder anderer Analysetechniken (vgl. zum Erfordernis solcher Regelungen auch EGMR, Big Brother Watch and others v. United Kingdom, Urteil vom 13. September 2018, Nr. 58170/13 u.a., § 424). Hierbei ist dem solchen Praktiken inhärenten Potential einer Umgehung innerstaatlicher Bindungen (vgl. dazu auch EGMR, a.a.O.) und den spezifischen Grundrechtsgefährdungen, die durch die Zusammenarbeit eintreten können, Rechnung zu tragen. Zu regeln ist insoweit insbesondere, wieweit der Bundesnachrichtendienst im Rahmen von Kooperationen personenbezogene Informationen von ausländischen Diensten entgegennehmen und verwerten kann, für die Anhaltspunkte bestehen, dass sie durch eine Überwachung der deutschen Inlandskommunikation gewonnen wurden. Da der Gesetzgeber solche Regelungen bisher nicht geschaffen hat, sind die diesbezüglichen Anforderungen nicht Gegenstand des vorliegenden Verfahrens. 250

Geboten sind Regelungen zum anderen, soweit dem Bundesnachrichtendienst Überwachungs- und Übermittlungsbefugnisse eingeräumt werden sollen, die er auch im Interesse und unter Anleitung anderer Dienste einsetzen kann. Will der Gesetzgeber dem Bundesnachrichtendienst die Auswertung der von ihm erhobenen Daten anhand von Suchbegriffen der Kooperationspartner oder die automatisierte Übermittlung von insoweit vorselektierten Inhaltsdaten oder gegebenenfalls auch von unselektierten Verkehrsdaten an ausländische Dienste ermöglichen, muss er hierfür eigene Rechtsgrundlagen schaffen, so wie er dies mit den §§ 14, 15 BNDG vom Grundsatz her ins Werk gesetzt hat. 251

2. Die an solche Rechtsgrundlagen zu stellenden verfassungsrechtlichen Anforderungen sind darauf ausgerichtet sicherzustellen, dass die für die strategische Überwachung allgemein entwickelten grundrechtlichen Grenzen auch im Rahmen der Zusammenarbeit möglichst wirksam gewahrt bleiben. 252

Da eine solche Zusammenarbeit nur unter striktem Schutz der Inlandskommunika- 253

tion in Betracht kommt, ist sie auf Daten aus der Ausland-Ausland-Aufklärung (oben Rn. 170 ff.) zu beschränken. Zur Wahrung des durch Art. 10 Abs. 1 GG verbürgten Grundrechtsschutzes ist demnach im Rahmen von Kooperationen für die Datenerhebung und -verwertung des Bundesnachrichtendienstes zunächst sicherzustellen, dass Telekommunikationsdaten von Inländern und deutschen Staatsangehörigen nach Möglichkeit ausgefiltert und sonst bei einer erst späteren Identifizierung unverzüglich ausgesondert werden. Dies schließt eine entsprechende Filterung der von den Partnerdiensten übernommenen Suchbegriffe ebenso ein wie die Filterung der für die automatisierte Übermittlung an ausländische Partner vorgesehenen Daten (dazu näher unten Rn. 255 ff. und 264). Die dazu entwickelten Anforderungen (oben Rn. 170 ff.) gelten auch hier. Weiterhin muss der Gesetzgeber auch für Kooperationen die Zwecke, für die die Überwachung im Zusammenwirken der Dienste erlaubt wird, hinreichend präzise und normenklar festlegen und auf den Schutz hochrangiger Gemeinschaftsgüter beschränken (oben Rn. 175 f.). Gleichermaßen sind die Kooperationen auf der Grundlage einer formalisierten Festlegung differenzierter Überwachungsmaßnahmen nach Erkenntnisziel, Gegenstand und Dauer aufzugliedern und verfahrensrechtlich zu strukturieren (oben Rn. 178 ff.). Das schließt die Einbindung solcher gemeinsam durchgeführter, je abgegrenzter Überwachungsmaßnahmen in eine längerfristig und breiter angelegte Zusammenarbeit – gegebenenfalls auf der Grundlage möglicher Rahmenvereinbarungen – nicht aus. Wie die Übermittlung von Einzelerkenntnissen setzt auch die automatisierte Übermittlung von Daten eine dokumentierte Vergewisserung über einen rechtsstaat- lichen Umgang mit den übermittelten Daten voraus (oben Rn. 233 ff.). Für jede der gemeinsam durchgeführten Überwachungsmaßnahmen ist die Vergewisserung jeweils einmal sicherzustellen; soweit es im Laufe der Zusammenarbeit hierfür Anlass gibt, ist sie zu aktualisieren (zur Notwendigkeit von Zusagen, die im Rahmen von Kooperationen eine eigene Bedeutung haben, unten Rn. 259 ff. und 264).

3. Spezifische Anforderungen gelten, soweit der Bundesnachrichtendienst im Rahmen von Kooperationen Suchbegriffe benutzen will, die von einem ausländischen Nachrichtendienst bestimmt wurden, und die Treffer dann ohne nähere inhaltliche Auswertung automatisiert an den Partnerdienst übermittelt. Der Gesetzgeber muss diesbezüglich Regeln schaffen, die die grundrechtliche Verantwortung des Bundesnachrichtendienstes für die von ihm erhobenen Daten und deren Verarbeitung sicherstellen. 254

a) Erforderlich ist hierfür zunächst eine sorgfältige Kontrolle der für den Partnerdienst eingesetzten Suchbegriffe sowie der hieran anknüpfenden Trefferfälle. Der Bundesnachrichtendienst hat sowohl die Suchbegriffe selbst als auch die mit ihnen herausgefilterten Daten daraufhin zu prüfen, ob ihre Verwendung grundrechtlichen Grenzen unterliegt. 255

aa) Hinsichtlich der von den Partnerdiensten bestimmten Suchbegriffe bedarf es dafür – anknüpfend an die bisherige Praxis – zunächst einer Kontrolle, ob diese auf die Zwecke der jeweils festgelegten Überwachungsmaßnahme ausgerichtet sind. 256

Dies setzt eine hinreichende Plausibilisierung der Suchbegriffe durch die Partnerdienste voraus. Darüber hinaus ist sowohl hinsichtlich der Suchbegriffe als auch hinsichtlich der Trefferfälle eine Kontrolle – etwa anhand von Listen gefährdeter Personen – vorzusehen, die darauf ausgerichtet ist, Daten von Personen oder aus Situationen, bei denen Anhaltspunkte für eine besondere Schutzbedürftigkeit bestehen, wie das etwa bei unter Verfolgungsdruck stehenden Dissidenten oder sogenannten Whistleblowern der Fall sein kann, nach Möglichkeit auszufiltern. Ebenso wie schon derzeit im Hinblick auf nationale Interessen oder auf Ziele in der Europäischen Union bedarf es auch in Blick auf die Grundrechte besonderer Schutzvorkehrungen.

Entsprechendes gilt für Personen, deren Tätigkeit von Verfassungs wegen eine besondere Vertraulichkeit voraussetzt, wie insbesondere für schutzwürdige Rechtsanwälte und Journalisten. Diesen gegenüber sind Überwachungsmaßnahmen allerdings auch im Rahmen von Kooperationen nicht insgesamt ausgeschlossen. Sie können aber auch hier nur bezogen auf einen qualifizierten Rechtsgüterschutz und nach Maßgabe von Eingriffsschwellen sowie einer Abwägung zulässig sein (oben Rn. 194 ff.). Um diese Voraussetzungen zu kontrollieren, müssen Suchbegriffe, die auf die Erfassung der Telekommunikation solcher Personen gerichtet sind, nach Möglichkeit im Rahmen von Filterverfahren zunächst identifiziert werden, um dann einer händischen Prüfung einschließlich der gebotenen Abwägung zugeführt zu werden. Für die Frage, ob die Voraussetzungen für die Verwendung solcher Selektoren vorliegen, bedarf es erforderlichenfalls einer näheren Plausibilisierung durch den Partnerdienst. Entsprechend sind die durch die Suchbegriffe erfassten Datenverkehre vor ihrer automatisierten Übermittlung an den ausländischen Dienst darauf zu kontrollieren, ob sie – ausgehend von den dem Bundesnachrichtendienst vorliegenden Kenntnissen – Personen zuzuordnen sind, deren Kommunikation auch zur Vermeidung staatlicher Repressionen besondere Vertraulichkeit verlangt, und gegebenenfalls händisch zu prüfen. Soweit diesbezüglich Einzelfallentscheidungen zu treffen sind, sind sie einer gerichtsähnlichen Vorabkontrolle zu unterwerfen. 257

bb) Diese Kontrolle muss möglichst wirksam ausgestaltet werden. Hierfür kommt – in Anknüpfung an die bisherige Praxis – zunächst eine automatisierte Kontrolle in Betracht. Dem Bundesnachrichtendienst ist gesetzlich aufzugeben, unter Nutzung der Ergebnisse und Erfahrungen seiner Arbeit etwaige Hinweise auf eine besondere Schutzwürdigkeit und Schutzbedürftigkeit bestimmter Personen zu sammeln und auf sie bezogene Telekommunikationskennungen in einer Weise zusammenzuführen, die die Filterung der Suchbegriffe und der für die Übermittlung vorgesehenen Daten ermöglicht. Entsprechendes gilt für die Kennungen von Journalisten, Rechtsanwälten oder ähnlichen Personen, Gruppen oder Einrichtungen, deren Kommunikation besondere Vertraulichkeit zukommt. Die diesbezüglichen Datenbanken und Filterverfahren sind kontinuierlich zu aktualisieren und fortzuentwickeln. Soweit erforderlich, sind die automatisierten Verfahren auf der Grundlage von hinreichend umfangreichen Stichproben durch eine manuelle Kontrolle zu ergänzen. Jedenfalls nach der 258

gegenwärtigen Leistungsfähigkeit der automatisierten Verfahren dürfte dies – ausgehend von den Erkenntnissen der mündlichen Verhandlung – zur Zeit unverzichtbar sein.

b) Für die automatisierte Übermittlung nicht vollständig ausgewerteter Daten an ausländische Dienste kommt der Sicherstellung gehaltvoller Zusagen eine besondere Bedeutung zu. Da hier die Auswertung der vom deutschen Dienst erhobenen Daten in die Hand eines ausländischen Dienstes gelegt wird, der seinerseits an das Grundgesetz nicht gebunden ist, sind spezifische Zusagen der Partnerdienste für den weiteren Umgang mit den Daten einzuholen. Dabei sind die Zusagen nunmehr angesichts der Grundrechtsgeltung auch im Ausland an dem Schutz der Grundrechte der überwachten Personen auszurichten. 259

Danach ist Partnerdiensten zum einen die Zusage abzuverlangen, Daten- verkehre unter Beteiligung von deutschen Staatsangehörigen oder Inländern prinzipiell unverzüglich zu löschen, soweit sie als solche im Rahmen der Auswertung identifiziert werden. Zum anderen bedarf es gehaltvoller Zusagen für den Umgang mit schutzbedürftigen Vertraulichkeitsbeziehungen. Schließlich müssen auch hier Zusagen eingeholt werden, die sicherstellen, dass die für den Bundesnachrichtendienst geltenden Übermittlungsgrenzen durch die Partnerdienste nicht unterlaufen werden (oben Rn. 242). 260

Diese Zusagen sind – entsprechend der allgemeinen Rechtsstaatlichkeits- vergewisserung – auf die jeweils einzeln festgelegten Überwachungsmaßnahmen zu beziehen und bei Verlängerung gegebenenfalls zu erneuern. Sie müssen nicht in völkerrechtlich verbindlicher Form getroffen werden, jedoch tatsächlich wirksam sein. Die Bundesregierung hat hierbei zu prüfen, wieweit solche Vereinbarungen durch Auskunftsrechte oder Mitteilungspflichten sowie auch durch Kommunikations- und Einwirkungsregelungen – wie etwa ein Löschungsverlangen – flankiert werden können, die der Dienst gegebenenfalls nutzen kann und muss. 261

4. Eine eigene Regelung ist schließlich geboten, soweit im Rahmen von Kooperationen ohne vorangehende Selektion anhand bestimmter Suchbegriffe gesamthaft Verkehrsdaten an ausländische Nachrichtendienste übermittelt werden sollen, damit diese sie bevorratend speichern und mit ihren Mitteln auswerten können. 262

a) Da hier der Bundesnachrichtendienst die von ihm erhobenen Daten ohne weitere inhaltliche Kontrollmöglichkeit aus der Hand gibt, bedarf es für eine solche Form der Kooperation spezifisch einschränkender Voraussetzungen. Eine gesamthafte Übermittlung von Verkehrsdaten kann nicht kontinuierlich und allein final angeleitet erlaubt werden, sondern setzt einen qualifizierten Aufklärungsbedarf im Hinblick auf eine spezifisch konkretisierte Gefahrenlage voraus. Insoweit muss über das Bestehen allgemeiner Gefährdungslagen hinaus aufgrund bestimmter Ereignisse Anlass bestehen, durch Aufklärungsmaßnahmen konkreten Bedrohungen entgegenzuwirken und die Handlungsfähigkeit der Bundesrepublik sicherzustellen. Das kann etwa der Fall sein, wenn tatsächliche Anhaltspunkte für die Vorbereitung terroristischer Anschläge vorliegen, für Verschiebungen von Kriegswaffen auf einer bestimmten Route 263

oder für koordinierte Cyberangriffe gegenüber bestimmten Staaten oder Einrichtungen. Im Rahmen der formalisierten Festlegung der Maßnahme (oben Rn. 179 ff.) ist das festzuhalten und die Auswertung durch den ausländischen Dienst auf dieses Ziel zu begrenzen. Die Festlegung einer solchen Maßnahme muss einer gerichtsähnlichen Kontrolle zugänglich sein.

b) Im Übrigen sind – den allgemeinen Maßgaben entsprechend (oben Rn. 170 ff.) – aus den Verkehrsdaten zunächst die Daten von deutschen Staats- angehörigen und Inländern auszufiltern. Auszusondern sind weiterhin auch hier die Telekommunikationsdaten von Personen, die dem Bundesnachrichtendienst als besonders schutzwürdig und schutzbedürftig bekannt sind (oben Rn. 257 f.). Unberührt bleiben ohnehin die Anforderungen an die Rechtsstaatlichkeitsvergewisserung (oben Rn. 233 ff.). Zu den von den ausländischen Diensten einzuholenden Zusagen gehört hier überdies, dass die gesamthaft übermittelten Daten nicht für einen längeren Zeitraum als sechs Monate bevorratend gespeichert werden. Im Übrigen hat die Bundesregierung zu prüfen, ob die grundrechtlichen Grenzen der Überwachung und Datennutzung durch das Verlangen zusätzlicher Zusagen auch für die Form der Kooperation noch weiter abgesichert werden können. 264

V.

Der Verhältnismäßigkeitsgrundsatz stellt für Überwachungsmaßnahmen auch Anforderungen an Transparenz, individuellen Rechtsschutz und Kontrolle (vgl. BVerfGE 141, 220 <282 ff. Rn. 134 ff.> m.w.N.; stRspr). In Bezug auf Transparenz und individuellen Rechtsschutz sind diese für die Auslandsfernmeldeaufklärung allerdings erheblich zurückgenommen. Im Ausgleich hierfür sind dem Verhältnis- mäßigkeitsgrundsatz besondere Anforderungen an eine unabhängige objektivrechtliche Kontrolle zu entnehmen (vgl. BVerfGE 133, 277 <369 Rn. 214>; 141, 220 <284 f. Rn. 140 f.>). 265

1. Zu den Anforderungen an die Gewährleistung von Transparenz der Datenverarbeitung gehören Auskunftsansprüche. Dies gilt grundsätzlich auch gegenüber Nachrichtendiensten (vgl. BVerfGE 125, 260 <331 f.>). Allerdings können diese Ansprüche so weit beschränkt werden, wie das für eine wirksame Aufgabenwahrnehmung unverzichtbar ist (vgl. BVerfGE 133, 277 <367 f. Rn. 209 ff.>; 141, 220 <283 Rn. 137>). Da die Auslandsaufklärung weithin auf Geheimhaltung verwiesen ist, können Auskunftsansprüche betroffener Personen danach in erheblichem Umfang beschränkt werden. Insbesondere kann eine Auskunft darüber, wie die Daten im Einzelnen erlangt wurden, ausgeschlossen werden. Wenn Auskunftsansprüche damit nur in geringem Umfang Transparenz ermöglichen und eine Grundlage für individuellen Rechtsschutz bieten können, ist dem kompensierend aber durch eine ausgebaute unabhängige objektivrechtliche Kontrolle Rechnung zu tragen (vgl. BVerfGE 133, 277 <369 Rn. 214>; näher unten Rn. 272 ff.). 266

2. Zu den Anforderungen an die verhältnismäßige Ausgestaltung heimlicher Überwachungsmaßnahmen – seitens der Nachrichtendienste wie seitens anderer Sicher- 267

heitsbehörden – gehören weiterhin grundsätzlich Benachrichtigungspflichten. Auch hier kann der Gesetzgeber in Abwägung mit verfassungsrechtlich geschützten Rechtsgütern Dritter und zur Gewährleistung einer wirksamen Aufgabenwahrnehmung Ausnahmen vorsehen. Obwohl diese Ausnahmen auf das unbedingt Erforderliche zu beschränken sind (vgl. BVerfGE 109, 279 <364>; 125, 260 <336>; 141, 220 <283 Rn. 136>), reichen die Benachrichtigungspflichten bezüglich der strategischen Überwachung danach nicht weit.

a) Gegenüber Personen im Inland bedarf es allerdings auch bezüglich der strategischen Überwachung differenzierter Regelungen, die eine Benachrichtigung weitestmöglich sicherstellen. Von Bedeutung ist dies insbesondere, wenn trotz der vorhandenen Filtermechanismen Kommunikation unter Beteiligung von Inländern oder Deutschen nicht technisch ausgesondert, sondern erst im Rahmen der manuellen Auswertung erkannt und nicht sogleich gelöscht wird. 268

Demgegenüber darf der Gesetzgeber in Bezug auf Personen im Ausland für Maßnahmen der strategischen Überwachung grundsätzlich von Benachrichtigungspflichten absehen (vgl. Marxsen, DÖV 2018, S. 218 <227>; Dietrich, in: Schenke/Graulich/Ruthig [Hrsg.], Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 6 BNDG Rn. 10). Für Aktivitäten des Bundesnachrichtendienstes, die unmittelbar in das Ausland hineinwirken oder dort vorgenommen werden, besteht ein elementares Interesse daran, dass diese insgesamt unbemerkt bleiben, damit der Dienst seine Aufgaben dauerhaft wahrnehmen kann. Jede förmlich konkretisierende Offen- legung der Präsenz oder der Aufklärungsmöglichkeiten des Dienstes in einem anderen Staat kann insbesondere seine Quellen gefährden (vgl. Gusy, in: Schenke/ Graulich/Ruthig [Hrsg.], Sicherheitsrecht des Bundes, 2. Aufl. 2019, BNDG Vorb. Rn. 10). Umgekehrt kann eine Benachrichtigung von Personen, die im Ausland leben, ihre Funktion auch nur sehr begrenzt erfüllen. Weder die Ermöglichung praktisch erreichbaren Rechtsschutzes (vgl. BVerfGE 65, 1 <70>; 109, 279 <363 f.; 367>; 120, 351 <361>; stRspr), noch das Ziel, Vertrauen in der Öffentlichkeit zu schaffen, noch die Funktion, über solche Maßnahmen einen demokratischen Diskurs zu ermöglichen (vgl. BVerfGE 125, 260 <335 f.>; 133, 277 <366 Rn. 206>; 141, 220 <282 f. Rn. 135 f.>; stRspr), können durch Benachrichtigungen im Ausland in annähernd vergleichbarer Weise erreicht werden wie durch Benachrichtigungen im Inland. Vielmehr kann eine Benachrichtigung für die Betroffenen in der anderen Rechtsordnung unter Umständen sogar gefährlich sein, weil sie diese der Aufmerksamkeit und dem Misstrauen der eigenen Behörden oder gegebenenfalls auch Dritter aussetzt. 269

Damit sind die Anforderungen an die Transparenz staatlichen Handelns und die praktische Möglichkeit, individuellen Rechtsschutz zu erlangen, weit zurückgenommen. Zwar bleibt die Eröffnung des Rechtswegs nach §§ 40, 50 Abs. 1 Nr. 4 VwGO förmlich unberührt, jedoch wird – mangels Kenntnis der Überwachungsmaßnahmen – auf diesem Wege Rechtsschutz für die Betroffenen nur in seltenen Aus- nahmefällen zu erlangen sein. Auch insoweit bedarf es zur Wahrung der Verhältnismäßigkeit im Ausgleich einer ausgebauten unabhängigen objektivrechtlichen Kontrolle 270

(unten Rn. 272 ff.).

b) Sieht das Gesetz Benachrichtigungspflichten nicht vor, kann Art. 10 Abs. 2 Satz 2 GG zu beachten sein. Dieser führt indes nicht zu engen verfassungsrecht- lichen Vorgaben für die organisationsrechtliche Ausgestaltung einer stattdessen zu schaffenden objektivrechtlichen Kontrolle. Sein Anwendungsbereich ist schon hinsichtlich seiner Merkmale „Schutz der freiheitlichen demokratischen Grundordnung“ und „Bestand oder Sicherung des Bundes oder eines Landes“ eng begrenzt (vgl. BVerfGE 100, 313 <397 f.>). Selbst soweit die Voraussetzungen des Art. 10 Abs. 2 Satz 2 GG vorliegen, folgt aus dessen Verweis auf von der Volksvertretung bestellte Organe oder Hilfsorgane keine detaillierte Organisationsanleitung. Vorgegeben ist allein, dass das mit der Nachprüfung betraute Kontrollorgan vom Parlament geschaffen sein muss und seine Mitglieder parlamentarisch – und damit unter Berücksichtigung der verschiedenen im Parlament vertretenen politischen Richtungen – bestimmt werden müssen. Doch kann das Kontrollorgan innerhalb oder außerhalb des Parlaments gebildet werden (vgl. BVerfGE 30, 1 <23>; 143, 1 <12 Rn. 39>). Eine Besetzung mit Bundestagsabgeordneten ist damit folglich nicht notwendig verbunden. Ebensowenig ist hierdurch eine organisatorische Verselbständigung mit strengen Geheimhaltungsregeln auch gegenüber dem Parlament ausgeschlossen (zu der insoweit eigenen Grundsätzen folgenden parlamentarischen Verantwortlichkeit des Bundesnachrichtendienstes, die nicht Gegenstand des vorliegenden Verfahrens ist, vgl. BVerfGE 143, 101 <133 ff. Rn. 106 ff.>). Das Organ kann als unabhängige Institution auch innerhalb des Funktionsbereichs der Exekutive ausgestaltet werden (vgl. BVerfGE 30, 1 <28>; 143, 1 <12 Rn. 39>; näher zu den Gestaltungsanforderungen und -möglichkeiten unten Rn. 274 ff.). 271

3. Die strategische Telekommunikationsüberwachung ist danach mit den Anforderungen der Verhältnismäßigkeit nur vereinbar, wenn sie durch eine ausgebaute unabhängige objektivrechtliche Kontrolle flankiert ist. Dies betrifft sowohl die strategische Überwachung und die damit verbundene Datennutzung selbst als auch die Übermittlung der mit ihr gewonnenen Erkenntnisse und die diesbezügliche Zusammenarbeit mit ausländischen Diensten. Die Kontrolle ist als kontinuierliche Rechtskontrolle auszugestalten, die einen umfassenden Kontrollzugriff ermöglicht. Sie ist auf die Wahrung der Grundrechte der Betroffenen auszurichten und gilt der Sicherung und praktischen Effektivierung der rechtlichen Grenzen der staatlichen Überwachungstätigkeit. 272

a) Die verfassungsrechtlichen Anforderungen an die Ausgestaltung der objektivrechtlichen Kontrolle sind in Bezug auf die strategische Überwachung besonders hoch und detailliert. Denn mit der Kontrolle ist ein Ausgleich dafür zu schaffen, dass übliche rechtsstaatliche Sicherungen in weitem Umfang ausfallen. Sie hat insoweit zwei Funktionen zu erfüllen: Zum einen muss sie das Rechtsschutzdefizit aus- gleichen, das durch die faktische Schwäche der individuellen Rechtsschutzmöglichkeiten besteht. Da die Auslandsfernmeldeaufklärung wegen ihrer Geheimhaltungsbedürftigkeit nur sehr begrenzte Auskunfts- und Benachrichtigungspflichten gebietet 273

und deshalb individueller Rechtsschutz kaum wirksam zu erlangen ist, muss dies mit der objektivrechtlichen Kontrolle durch eine unabhängige Stelle kompensiert werden. Zum anderen hat sie als Ausgleich für die im Wesentlichen nur finale Anleitung der Überwachungsbefugnisse die gebotene verfahrensmäßige Strukturierung der Handhabung dieser Befugnisse abzusichern. Sie bildet damit ein Gegengewicht zu den weiten Handlungsmöglichkeiten des Bundesnachrichtendienstes und gewährleistet, dass diese verfahrensmäßig rationalisierend auf die gesetzlichen Ziele hin ausgerichtet werden.

b) Sicherzustellen sind dabei zwei verschiedene Arten von Kontrolle, die sich auch organisationsrechtlich abbilden müssen. 274

aa) Zum einen ist eine Kontrolle durch eine gerichtsähnlich ausgestaltete Stelle sicherzustellen. Hierfür sind Spruchkörper vorzusehen, die mit Personen in gleichsam richterlicher Unabhängigkeit besetzt sind und in formalisierten Verfahren schriftlich und abschließend mit Wirkung für Bundesregierung und Nachrichtendienst entscheiden. Diese Kontrolle hat die Schutzaufgabe zu erfüllen, die sonst dem Richtervorbehalt sowie auch nachträglichen Rechtsschutzmöglichkeiten, insbesondere Feststellungsklagen, zukommt. Entsprechend muss mit ihr eine auf den Einzelfall bezogene Prüfung ermöglicht werden, die materiell und verfahrensmäßig einer gerichtlichen Kontrolle gleichwertig, insbesondere mindestens ebenso wirkungsvoll ist (vgl. BVerfGE 30, 1 <23>, dort zu Art. 10 Abs. 2 Satz 2 GG). 275

bb) Zum anderen ist eine unabhängige Rechtskontrolle administrativen Charakters einzurichten. Insoweit muss eine Kontrollinstanz geschaffen werden, der es möglich ist, eigeninitiativ stichprobenmäßig den gesamten Prozess der strategischen Überwachung auf seine Rechtmäßigkeit zu prüfen – sowohl Einzelent- scheidungen und Verfahrensabläufe als auch die Gestaltung der Datenverarbeitung und der Filterprozesse sowie der hierfür verwendeten technischen Hilfsmittel. Dieser Kontrollinstanz muss keine abschließende Entscheidungsbefugnis zukommen, vielmehr reicht insoweit ein Beanstandungsrecht. Zur Klärung grundlegender Rechtsfragen muss sie jedoch die Möglichkeit haben, das gerichtsähnliche Entscheidungsgremium anzurufen (zur Notwendigkeit, sich unter bestimmten Voraussetzungen auch an Parlament und Öffentlichkeit wenden zu können, unten Rn. 298). 276

c) Die nähere Ausgestaltung des Ineinandergreifens der Kontrollkompetenzen mit Blick auf die unterschiedlichen Arten der Kontrolle obliegt dem Gesetzgeber. Er hat hierbei einen erheblichen Spielraum, unterliegt aber Maßgaben aus dem Verhältnismäßigkeitsgrundsatz. 277

aa) Sicherzustellen hat er, dass die wesentlichen Verfahrensschritte der strategischen Überwachung und der hiermit verbundenen Datenverarbeitung grundsätzlich einer gerichtsähnlichen Kontrolle mit abschließenden Entscheidungsbefugnissen unterliegen. Hierzu gehören insbesondere, wie sich aus den oben dargelegten materiellen Anforderungen ergibt, die formalisierte Festlegung der verschiedenen Überwachungsmaßnahmen, auch im Bereich der Kooperationen, die konkreten 278

Netzanordnungen, der Einsatz von Suchbegriffen, soweit diese gezielt auf Personen gerichtet sind, welche als mögliche Gefahrenquelle im unmittelbaren Interesse des Nachrichtendienstes stehen, der Einsatz von Suchbegriffen, die gezielt auf Personen gerichtet sind, deren Kommunikation einen besonderen Vertraulichkeitsschutz genießt, die zum Schutz solcher Vertraulichkeitsbeziehungen erforderlichen Abwägungsentscheidungen, der Umgang mit Daten, die möglicherweise dem Kernbereich privater Lebensgestaltung unterfallen, besonders kontrollbedürftige Übermittlungen, vor allem an ausländische Stellen, sowie die Voraussetzungen für die Festlegung einer Zusammenarbeit zur automatisierten Übermittlung von Verkehrsdaten zur bevorratenden Speicherung und Auswertung an ausländische Dienste. Einer gerichtsähnlichen Kontrolle bedarf weiter die ausnahmsweise Nutzung von Daten unter Berufung auf besondere Gefahrensituationen, obwohl es sich um – erst in der manuellen Auswertung erkannte – Daten aus Telekommunikation unter Beteiligung von Deutschen oder Inländern handelt oder die Daten aus Überwachungsmaßnahmen stammen, die sich nicht auf Zwecke der Gefahrenfrüherkennung stützten, sondern unabhängig davon allein zur politischen Information der Bundesregierung angeordnet waren. Hinsichtlich der Frage, inwieweit solche Kontrolle ex ante oder ex post und im letzteren Fall – gegebenenfalls im Zusammenwirken mit der administrativen Kontrollinstanz – nur stichprobenmäßig stattfindet, steht dem Gesetzgeber ein Spielraum zu. Auch dieser ist freilich – wie zum Teil aus den oben entwickelten weiteren Maßgaben ersichtlich – durch den Verhältnismäßigkeitsgrundsatz gebunden, der jedenfalls im Hinblick auf grundlegende Entscheidungen eine vorherige Kontrolle gebietet.

bb) Im Zusammenwirken der Kontrollinstanzen muss gewährleistet sein, dass der gesamte Prozess der strategischen Überwachung einschließlich der hieran anknüpfenden Datenverarbeitung und -übermittlung wie auch der Zusammenarbeit mit ausländischen Nachrichtendiensten potentiell umfassend der Kontrolle unterliegt. Soweit keine gerichtsähnliche Kontrolle vorgesehen ist, muss die Möglichkeit der administrativen Kontrolle eröffnet sein. Geboten ist insoweit freilich allein eine Kontrolle der objektiven Rechtmäßigkeit der Maßnahmen. Die Entscheidung über die fachlich zweckmäßige Ausübung der Befugnisse im Rahmen der rechtlichen Regelungen bleibt hiervon unberührt. 279

cc) Bezogen auf die gerichtsähnliche Kontrolle wird der Gesetzgeber auch zu prüfen haben, ob Personen, die plausibel machen können, von Überwachungsmaßnahmen möglicherweise betroffen gewesen zu sein, das Recht eingeräumt werden kann, diesbezüglich mit eigenen Verfahrensrechten eine objektivrechtliche Kontrolle anzustoßen. Im Rahmen der hier in Frage stehenden objektivrechtlichen Kontrolle, die nicht als Verwirklichung der verfassungsrechtlichen Rechtsschutzgarantie zu verstehen ist und die förmliche Eröffnung des Rechtswegs nach §§ 40, 50 Abs. 1 Nr. 4 VwGO unberührt lässt, steht die Verfassung einer Ausgestaltung als Verfahren unter zumindest partiellem Ausschluss des Betroffenen und der Öffentlichkeit (in camera) nicht von vornherein entgegen. Dies gilt jedenfalls dann, wenn der Ausschluss erforderlich ist, um auf diesem Weg eine Kontrolle zu eröffnen, die andernfalls gar nicht 280

möglich und verfassungsrechtlich deshalb auch nicht geboten wäre (vgl. zu solchen Beschwerdeverfahren nach der Rechtslage im Vereinigten Königreich Leigh, in: Dietrich/Sule [Hrsg.], Intelligence Law and Policies in Europe, 2019, S. 553 <575 ff.>; siehe auch die Ausführungen zur Opfereigenschaft der dortigen Beschwerdeführer beziehungsweise zur Verfügbarkeit interner Rechtsbehelfe in EGMR, Big Brother Watch and others v. United Kingdom, Urteil vom 13. September 2018, Nr. 58170/13 u.a., §§ 249 ff.).

d) Zu gewährleisten ist eine kontinuierliche Kontrolle in institutioneller Eigenständigkeit. Hierzu gehören ein den Kontrollinstanzen zugewiesenes eigenes Budget und – abgesehen von der Ernennung der Mitglieder der gerichtsähnlichen Spruchkörper und der Leitungsebene – eine eigene Personalhoheit. Die Kontrollinstanzen müssen in ihrer Arbeit von Einflussnahmen wirksam abgeschirmt und insoweit mit vollständiger Unabhängigkeit ausgestattet sein. 281

Im Übrigen hat der Gesetzgeber in der Frage der institutionellen Ausformung der Kontrollinstanzen einen großen Gestaltungsspielraum. Dies betrifft etwa die Frage, ob die administrative Rechtskontrolle durch den Bundesdatenschutzbeauftragten oder durch eine verselbständigte Kontrollinstanz gewährleistet werden soll. Der Gesetzgeber wird die Kontrolle hierbei allerdings organisatorisch so ausgestalten müssen, dass sie nicht durch die „Third Party Rule“ behindert wird (unten Rn. 292 ff.). Verfassungsrechtlich nicht vorgegeben ist auch, ob die gerichtsähnliche Kontrolle und die administrative Rechtskontrolle institutionell unter einem Dach zusammengefasst werden, so dass die gerichtsähnlich entscheidenden Spruch- körper – bei Wahrung der richtergleichen Unabhängigkeit ihrer Mitglieder – in eine umfassende Kontrollinstanz integriert sind, oder ob diese jeweils selbständig ausgestaltet werden sollen. Erforderlich ist allerdings die Schaffung institutionell klarer Strukturen. 282

e) Insgesamt muss die Ausstattung der Kontrollinstanzen auf eine wirksame und unabhängige Erfüllung ihrer Aufgaben hin ausgerichtet sein. 283

aa) Die Kontrollinstanzen müssen personell kompetent und professionell ausgestattet sowie ausgewogen zusammengesetzt sein. Der Gesetzgeber hat auch diesbezüglich einen weiten Gestaltungsspielraum. Er ist aber verpflichtet, seine Gestaltung auf die Gewährleistung einer effektiven und rechtlich wie tatsächlich unabhängigen Kontrolle auszurichten. 284

(1) Geboten sind insoweit Regelungen, die eine Bestellung von Personen verlangen, die fachlich besonders ausgewiesen und geeignet sind, die Vorgänge in der Behörde zu durchdringen und im gegenseitigen Zusammenwirken eine unabhängige wie professionell fachkundige Kontrolle sicherzustellen. Hierbei dürfte jedenfalls für die administrative Kontrolle nicht nur die Berücksichtigung von Personen mit rechtlichen, sondern auch weiteren, insbesondere informationstechnischen Kenntnissen erforderlich sein. 285

(2) Für die gerichtsähnliche Kontrolle ist eine Unabhängigkeit der zur Entscheidung 286

berufenen Mitglieder sicherzustellen, die einer richterlichen Unabhängigkeit gleichkommt. Insbesondere müssen sie weisungsfrei und auf hinreichend lange und bestimmte Zeit fest berufen sein. Für die Zusammensetzung der Spruchkörper ist zu gewährleisten, dass der richterlichen Perspektive ein maßgebliches Gewicht zukommt, die für eine maßgebliche Zahl der Mitglieder durch langjährige richterliche Erfahrung belegt sein muss. Das schließt nicht aus, Erfahrung in anderen juristischen Berufen zu berücksichtigen. In Betracht zu ziehen ist auch hier, dass zusätzlich möglicherweise anderweitiger, insbesondere technischer Sachverstand förderlich sein kann. Es liegt in den Händen des Gesetzgebers zu entscheiden, ob er hierfür als Mitglieder des gerichtsähnlichen Entscheidungsgremiums – unter Umständen abhängig von der Art der Entscheidung – ergänzend auch Nichtjuristen vorsieht, oder ob er dem Gremium anderweitige Möglichkeiten an die Hand gibt, technischen Sachverstand heranzuziehen.

(3) Insgesamt ist eine fachlich kompetente, professionalisierte Kontrolle durch grundsätzlich hauptamtlich tätige Personen sicherzustellen; es reicht nicht, die Durchführung der Kontrolle im Wesentlichen auf eine ehrenamtliche Amtsausübung zu stützen. Zugleich ist auf eine ausgewogene Zusammensetzung der Kontrollinstanzen zu achten. Personell wie strukturell ist zur Sicherstellung der gebotenen Unabhängigkeit auf die Wahrung einer hinreichenden Distanz zum Bundesnachrichtendienst Bedacht zu nehmen. 287

bb) Für beide Arten der Kontrolle sind hinreichendes Personal und hinreichende Mittel bereitzustellen. Für die gerichtsähnliche Kontrolle bedarf es einer genügenden Anzahl von Stellen und Spruchkörpern, die es ermöglicht, den ihnen zu übertragenden Kontrollaufgaben mit Sorgfalt nachzukommen; die Stellen sind finanziell so auszustatten, dass hierfür hervorgehoben qualifizierte Personen zu gewinnen sind. Ebenso bedarf es für die administrative Rechtskontrolle einer hinreichenden Zahl an Stellen für qualifizierte Mitarbeiterinnen und Mitarbeiter. Die Sachmittel müssen einen Umfang haben, der es etwa auch erlaubt, die Filterprozesse zur Aussonderung der Kommunikation von Deutschen und Inländern sowie zum Schutz von Vertraulichkeitsbeziehungen wirksam zu kontrollieren und dafür gegebenenfalls auch eigene Dateien und Kontrollprogramme zu entwickeln. Der Umfang der insoweit zu schaffenden Stellen und Mittel dürfte dabei jedenfalls kaum unterhalb dessen liegen, was derzeit dem Ständigen Bevollmächtigten des Parlamentarischen Kontrollgremiums zugewiesen ist. 288

f) Die Kontrollinstanzen müssen gegenüber dem Bundesnachrichtendienst alle für eine wirksame Kontrolle erforderlichen Befugnisse haben. 289

aa) Beiden Kontrollinstanzen ist umfassend Zugang zu allen Unterlagen einzuräumen. Dabei ist der Bundesnachrichtendienst dazu zu verpflichten, die Kontrollinstanzen bei ihrer Aufgabenerfüllung zu unterstützen, ihnen Auskünfte zu erteilen und Einsicht in Unterlagen und Daten, Aufschluss über verwendete Programme sowie jederzeitigen Zutritt zu Diensträumen zu gewähren (vgl. BVerfGE 133, 277 <370 f. 290

Rn. 215 ff.>; 141, 220 <284 f. Rn. 141>; siehe auch BTDrucks 14/5655, S. 26 unter Bezugnahme auf BVerfGE 100, 313 <401>). Dabei sind den Kontrollinstanzen die Festlegung ihres Verfahrens und die Wahl ihrer Methoden selbst zu überantworten, soweit diese nicht gesetzlich festgelegt sind.

bb) Zu den verfassungsrechtlichen Anforderungen in Blick auf die Kontrolle gehört eine Protokollierung der Datenverarbeitung (vgl. BVerfGE 133, 277 <370 Rn. 215>; 141, 220 <284 f. Rn. 141>; stRspr). Danach müssen die verschiedenen Schritte der Überwachung in einer Weise protokolliert werden, die eine wirksame Kontrolle ermöglicht. Erforderlichenfalls sind die diesbezüglichen Grundsätze im Benehmen zwischen Bundesnachrichtendienst und den Kontrollinstanzen näher zu konkretisieren. 291

cc) Die Kontrolle darf nicht unter Berufung auf die „Third Party Rule“ behindert werden. Der Gesetzgeber hat durch die Ausgestaltung der Kontrollinstanzen sowie durch Maßgaben zu entsprechenden Absprachen des Bundesnachrichtendienstes mit den anderen Diensten die Bedingungen dafür zu schaffen, dass die „Third Party Rule“ den Kontrollinstanzen nicht entgegenhalten werden kann. 292

Allerdings bildet die „Third Party Rule“ eine auf Vereinbarungen mit Partnerdiensten beruhende allgemein anerkannte Verhaltensregel unter den Nachrichtendiensten, nach der Informationen von ausländischen Diensten nach Maßgabe informeller Absprachen nicht ohne deren Zustimmung an Dritte weitergegeben werden dürfen (vgl. BVerfGE 143, 101 <150 Rn. 162; 151 Rn. 164>). Auf diese Regel kann sich auch die Bundesregierung berufen, sofern sie entsprechende Zusagen gegeben hat, auf deren Grundlage Informationen von dem ausländischen Dienst bereits übermittelt wurden und hieran anschließend eine Übermittlung an „Dritte“ in Frage steht; in diesem Sinne konnte sich die Bundesregierung auf diesbezüglich gegebene Zusagen an die Vereinigten Staaten von Amerika berufen und gegenüber einem Untersuchungsausschuss des Deutschen Bundestags als Dritten bestimmte Informationen zurückhalten (vgl. BVerfGE 143, 101 <152 Rn. 167; 155 ff. Rn. 176 ff.>). 293

Dies kann jedoch der Ausgestaltung der verfassungsrechtlich gebotenen umfassenden Rechtskontrolle gegenüber dem Bundesnachrichtendienst in Form strikt auf Geheimhaltung ausgerichteter und verpflichteter unabhängiger Instanzen, die nicht in das Parlament und dessen politische Kommunikationszusammenhänge eingebunden sind, nicht entgegengehalten werden. Ob eine Kontrollinstanz als „Dritter“ im Sinne der „Third Party Rule“ anzusehen ist, ist nicht allgemein definiert, sondern richtet sich nach der organisatorischen Ausgestaltung und entsprechenden Vereinbarungen (vgl. BTDrucks 18/12850, S. 98 f.). Die „Third Party Rule“ ist insoweit eine auf eine rechtlich nicht verbindliche, aber auf Vereinbarung mit anderen Diensten beruhende und damit flexible Verwaltungspraktik, auf deren praktische Bedeutung die Bundesregierung Einfluss hat (vgl. Gärditz, DVBl 2015, S. 903 <904 f.>; Möllers, JZ 2017, S. 271 <277>). Zwar bleiben die Bundesregierung und der Bundesnachrichtendienst an gegebene Zusagen gebunden. Für die Zukunft sind jedoch durch die Art der Ausgestaltung der Kontrollinstanzen sowie durch veränderte Absprachen mit den aus- 294

ländischen Diensten die Bedingungen dafür zu schaffen, dass die mit der Rechtskontrolle betrauten Instanzen nicht mehr als „Dritte“ angesehen werden (vgl. auch European Commission for Democracy through Law [Venice Commission], Report on the Democratic Oversight of Signals Intelligence Agencies, CDL-AD[2015]011, S. 5 [Nr. 13]; Council of Europe, Parliamentary Assembly, Resolution 1838 [2011], S. 2 [Punkt 7]; Council of Europe, Commissioner for Human Rights, Democratic and effective oversight of national security services, 2015, S. 13 [Empfehlung Nr. 16]).

Es ist so zu gewährleisten, dass sich sowohl die verfassungsrechtlich gebotene Kontrolltätigkeit ungehindert von der „Third Party Rule“ auch auf den Umgang des Bundesnachrichtendienstes mit von ausländischen Diensten stammenden Informationen erstreckt, als auch die für die Wahrung der außen- und sicherheitspolitischen Interessen der Bundesrepublik besonders bedeutsame Zusammenarbeit des Bundesnachrichtendienstes mit anderen Nachrichtendiensten (oben Rn. 246 f.) weitergeführt werden kann. Dass dies möglich ist, erweist sich auch mit Blick auf andere Nachrichtendienste, bei denen die Kontrollinstanzen vollen Zugriff auf sämtliche zur Kontrolle erforderlichen Unterlagen der von ihnen überwachten Dienste haben (vgl. für die Auskunftsrechte des Investigatory Powers Tribunal im Vereinigten Königreich EGMR, Big Brother Watch and others v. United Kingdom, Urteil vom 13. September 2018, Nr. 58170/13 u.a., §§ 250, 379; für die unbeschränkten Auskunftsrechte des Investigatory Powers Commissioner siehe Annual Report of the Investigatory Powers Commissioner 2017 vom 31. Januar 2019, S. 41). 295

dd) Die Kontrolle kann grundsätzlich durch strenge Regeln zur Geheimhaltung flankiert werden. Neben der räumlichen wie technischen Ausstattung kann hierauf auch bei der Auswahl der Personen maßgebliches Gewicht gelegt werden. Insbesondere kann die Geheimhaltung durch strikte, mit wirksamen Sanktionen bewehrte Verschwiegenheitspflichten abgesichert werden. 296

(1) Demgegenüber muss zwischen den mit der objektivrechtlichen Kontrolle betrauten Kontrollinstanzen untereinander ein offener und unmittelbarer Austausch gewährleistet sein (vgl. BVerfGE 133, 277 <370 Rn. 216>). Da diese – jeweils gleichermaßen zur Vertraulichkeit verpflichtet – im Zusammenwirken gegenüber den gleichen Maßnahmen zur Kontrolle berufen sind, fordert dies das Gebot einer wirksamen und kohärenten Kontrolle. Soweit im Rahmen der Kontrolle strukturelle Probleme erkennbar werden oder anders nicht auszuräumenden Differenzen mit dem Bundesnachrichtendienst auftreten, ist eine Möglichkeit vorzusehen, Beanstandungen gegenüber der Behördenleitung und erforderlichenfalls der Leitung des aufsichtführenden Bundeskanzleramts vorzutragen, die sich gegebenenfalls hierzu zu verhalten haben. 297

(2) Der Informationsfluss in den parlamentarischen Raum und damit auch zum Parlamentarischen Kontrollgremium kann indes aus Geheimhaltungsgründen grundsätzlich begrenzt werden. Der Gesetzgeber darf insoweit berücksichtigen, dass die parlamentarische Kontrolle einen anderen Charakter aufweist (unten Rn. 300) als eine Kontrolle, die allein auf die Beachtung des objektiven Rechts ausgerichtet ist, und 298

dass Geheimhaltung im parlamentarisch-politischen Umfeld faktischen Grenzen unterliegt. Allerdings ist das Parlamentarische Kontrollgremium nach Art. 45d GG in einer Form, die den Belangen des Geheimschutzes Rechnung trägt, regelmäßig über die Kontrolltätigkeit zu unterrichten. Darüber hinaus muss es den Kontrollinstanzen möglich sein, in abstrakter, die Geheimhaltung gewährleistender Weise ihre Beanstandungen und Kritik letztlich auch an das Parlament und damit an die Öffentlichkeit heranzutragen.

(3) Da die Kontrollprozesse Parlament und Öffentlichkeit weithin verschlossen bleiben, dabei aber zugleich in einem potentiellen Spannungsverhältnis zu der auf dem Prinzip der Geheimhaltung beruhenden Arbeit des Bundesnachrichtendienstes stehen und sich überdies die Bedingungen der Überwachungsmaßnahmen wie deren Kontrolle angesichts der Fortentwicklung der Technik schnell wandeln können, bedarf die Wirksamkeit der Kontrolle ständiger Beobachtung. Dabei ist die Effektivität sowohl der Kontrolle in der Praxis als auch der gesetzlichen Regelungen in regelmäßigen Abständen zu evaluieren (zu Evaluierungspflichten vgl. auch BVerfGE 150, 1 <90 Rn. 176>). 299

g) Die daneben bestehende Kontrolle durch das Parlamentarische Kontrollgremium und dessen Ständigen Bevollmächtigten, die gleichfalls der Ausgestaltung des Gesetzgebers unterliegt und in die Kontrolle der Überwachungsmaßnahmen einbezogen werden kann (vgl. etwa § 14 G 10), ist nicht Gegenstand des vorliegenden Verfahrens. Sie hat eine eigene, nicht speziell auf die Rechts- und Grundrechtskontrolle begrenzte Funktion und ist Ausdruck der allgemeinen parlamentarischen Verantwortung für die sachgerechte und politisch angemessene Aufgabenwahrnehmung der Exekutive (vgl. Waldhoff, in: Dietrich/Gärditz/Graulich/Gusy/Warg [Hrsg.], Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 73 <75>). Anforderungen zu ihrer Ausgestaltung lassen sich aus den in vorliegendem Verfahren geltend gemachten Grundrechten nicht ableiten; umgekehrt bleiben diesbezüglich aus der Verfassung herzuleitende Befugnisse des Parlaments gegenüber der Exekutive von den vorstehenden Maßgaben unberührt (vgl. hierzu BVerfGE 143, 101). 300

VI.

Nach den vorstehenden Maßgaben genügen die angegriffenen Vorschriften den verfassungsrechtlichen Anforderungen auch materiell nicht. Sie beruhen – wie schon die Verletzung des Zitiergebots des Art. 19 Abs. 1 Satz 2 GG (oben Rn. 134 f.) – auf der verfassungsrechtlich unzutreffenden Annahme, die Grundrechte seien für die in Frage stehenden Überwachungsbefugnisse nicht anwendbar. Da die Vorschriften bereits aus formellen Gründen verfassungswidrig sind, werden bei ihrer materiellen Beurteilung nur die zentralen Defizite aufgegriffen. Eine Neuregelung der Befugnisse des Bundesnachrichtendienstes wird die Vorschriften insgesamt auch an den Grundrechten der hinsichtlich ihrer Telekommunikation überwachten Personen und damit an den oben entwickelten Maßgaben auszurichten haben. 301

1. Mit Art. 10 Abs. 1 GG und den sich hieraus ergebenden Verhältnismäßigkeitsanforderungen unvereinbar sind zunächst die Vorschriften zur Datenerhebung und -verarbeitung in §§ 6, 7 BNDG. 302

a) Dies gilt zum einen für die Regelung der strategischen Überwachung vom Inland aus nach § 6 BNDG. 303

aa) § 6 BNDG regelt schon die mit der Auslandsaufklärung aus technischen Gründen derzeit unvermeidbar verbundenen Grundrechtseingriffe gegenüber Deutschen und Inländern nicht in der verfassungsrechtlich gebotenen Weise. Insbesondere regelt er nicht hinreichend die diesbezüglich gebotene Filterung und die an diese Filterung zu stellenden Anforderungen (oben Rn. 170 ff.). Allein das materielle Verbot in § 6 Abs. 4 BNDG, das den Anschein hervorruft, als müsste und könnte die Erhebung von Daten deutscher Staatsangehöriger und von Inländern insgesamt vermieden werden, genügt dem nicht. Auch die gebotene unverzügliche Löschung der unbeabsichtigt miterfassten Inlandskommunikation ist nicht normenklar geregelt. Zwar sieht § 10 Abs. 4 Satz 1 BNDG eine solche Löschung grundsätzlich vor. Ob und wieweit nach Satz 2 bis 6 der Vorschrift aber von einer solchen Löschung abgesehen werden kann, ist der Norm nicht zu entnehmen (vgl. Hölscheidt, Jura 2017, S. 148 <156>). 304

bb) Weiter ist die Überwachung nach § 6 BNDG nicht auf differenziert gefasste, gewichtige Zwecke begrenzt (oben Rn. 175 f.). Die in § 6 Abs. 1 Satz 1 BNDG genannten weit und offen formulierten Zwecke, die auch nach der Begründung des Gesetzesentwurfs das Aufgabenspektrum in keiner Weise einengen sollen (vgl. BTDrucks 18/9041, S. 22), verfehlen diese Anforderung deutlich. Insbesondere kann eine solche gesetzliche Begrenzung nicht durch das allein politisch definierte Auftragsprofil der Bundesregierung ersetzt werden (vgl. insoweit auch schon United Nations Office of the High Commissioner for Human Rights, Brief der Sonder- berichterstatter vom 29. August 2016, OL DEU 2/2016, S. 5). 305

Entsprechend ist die Überwachung nicht auf der Grundlage formalisierter Festlegungen differenzierend begrenzter Überwachungsmaßnahmen strukturiert, an denen sich die Auswahl der zu erfassenden Übertragungswege sowie der Suchbegriffe ebenso wie die weitere Verarbeitung und Nutzung unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes nachprüfbar auszurichten haben (oben Rn. 178 ff.; vgl. allgemein auch schon Marxsen, DÖV 2018, S. 218 <224>). Auch fehlt es an gesetzlichen Maßgaben zum Einsatz gezielt personenbezogener Suchbegriffe (oben Rn. 185 ff.) und zum Schutz von Vertraulichkeitsbeziehungen (oben Rn. 193 ff. sowie Löffelmann, in: Dietrich/Gärditz/Graulich/Gusy/Warg [Hrsg.], Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 33 <43>). Der Kernbereichsschutz in § 11 BNDG ist unzureichend geregelt (oben Rn. 203 ff.). 306

Ebenso enthält das Gesetz keine hinreichenden Regelungen zur Auswertung der durch das Mittel der strategischen Auslandsaufklärung gewonnenen Daten (oben Rn. 192). § 19 BNDG genügt als lediglich allgemein gehaltene Regelung für die Datenverarbeitung des Bundesnachrichtendienstes diesen Anforderungen nicht und ist 307

in seiner unspezifischen Weite und der undifferenzierten Verweisung auf §§ 10, 11 BVerfSchG als Grundlage für die Verarbeitung, Veränderung und Nutzung von Daten, die auf der Grundlage der §§ 6, 7 BNDG erhoben wurden, unverhältnismäßig.

cc) Soweit § 6 BNDG darüber hinaus als Grundlage für die Erhebung sonstiger personenbezogener Daten deutscher Staatsangehöriger, inländischer juristischer Personen oder sich im Bundesgebiet aufhaltender Personen dienen soll, die nicht Art. 10 GG unterfallen (vgl. BTDrucks 18/9041, S. 24), fehlt es der Regelung schon an der gebotenen Normenklarheit (oben Rn. 137 ff.). Der Vorschrift ist bereits nicht zu entnehmen, dass eine Nutzung solcher Daten, die nicht durch das Fernmeldegeheimnis geschützt sind, überhaupt durch sie eröffnet werden soll; erst recht regelt sie nicht, welche Daten zu welcher Nutzung insoweit erhoben werden sollen und auf welcher Grundlage dies mit Blick auf welche Grundrechte vom Gesetzgeber als gerechtfertigt angesehen wird. 308

b) Mit Art. 10 Abs. 1 GG nicht vereinbar ist zum anderen § 7 BNDG, der die weitere Verarbeitung von vom Ausland aus mit Mitteln der Fernmeldeaufklärung gewonnenen Daten sowie gewisse Grenzen solcher Datenerhebung regelt. Der Regelung liegt die unzutreffende Annahme zugrunde, dass eine solche Datenerhebung keiner Ermächtigungsgrundlage bedarf und allein auf der Grundlage der Aufgabennorm des § 1 Abs. 2 BNDG möglich ist. Ohne hinreichende gesetzliche Ermächtigung ist jedoch auch eine solche Datenerhebung unzulässig (oben Rn. 87 ff. und 120). Indem § 7 BNDG die Zulässigkeit dieser Datenerhebung impliziert, sie nur punktuell beschränkt und im Übrigen die weitere Verarbeitung ohne weiteres erlaubt, ist er selbst verfassungswidrig. Als eigene (implizite) Ermächtigung zur Datenerhebung genügte er den oben näher ausgeführten verfassungsrechtlichen Anforderungen an eine solche Rechtsgrundlage nicht. Der Gesetzgeber will § 7 BNDG aber, wie gesehen, überhaupt nicht als Ermächtigungsgrundlage zur Datenerhebung verstanden wissen. Dann verstößt § 7 BNDG schon insofern gegen Art. 10 Abs. 1 GG, als er die Verarbeitung von Daten regelt, die mangels verfassungsgemäßer Rechtsgrundlage erst gar nicht hätten erhoben und deshalb auch nicht weiter hätten verarbeitet werden dürfen. Im Übrigen setzt er so den Anschein, dass solche Daten erhoben werden dürften und legitimiert damit eine Datenerhebung, für die es an einer verfassungsmäßigen Rechtsgrundlage fehlt. 309

2. Auch die Vorschriften zur Datenübermittlung sind mit den verfassungsrechtlichen Anforderungen nicht vereinbar. Zum Teil genügen sie dem Grundsatz der Normenklarheit nicht. Im Übrigen begrenzen sie die Übermittlung nicht hinreichend bestimmt auf den Schutz besonders gewichtiger Rechtsgüter oder die Verfolgung besonders schwerer Straftaten beziehungsweise binden sie nicht an eine hinreichend konkretisierte Gefahrenlage oder an einen durch bestimmte Tatsachen erhärteten Verdacht solcher Straftaten. 310

a) § 24 Abs. 1 Satz 1 BNDG, der die Übermittlung an inländische öffentliche Stellen regelt, genügt schon nicht dem Gebot der Normenklarheit und Bestimmtheit (oben 311

Rn. 137 ff. und 212 ff.). Dies gilt zunächst insoweit, als er dem Bundesnachrichtendienst die Übermittlung allgemein „zur Erfüllung seiner Aufgaben“ erlaubt. Zwar ist ein Verweis auf anderweitig definierte Aufgaben nicht grundsätzlich mit den Anforderungen an die Normenklarheit unvereinbar. Eine allgemeine Bezugnahme auf die gesamten Aufgaben des Bundesnachrichtendienstes, die kein operatives Tätigwerden umfassen, sondern allein auf die Gewinnung von Erkenntnissen und deren Auswertung begrenzt sind (vgl. § 1 Abs. 2 BNDG), lässt jedoch nicht erkennen, zu welchen Zwecken hier eine Datenübermittlung erlaubt werden soll (oben Rn. 215). Die Unsicherheiten hierüber in der mündlichen Verhandlung haben dies bestätigt. Unbestimmt ist die Vorschrift aber auch insoweit, als sie eine Übermittlung erlaubt, wenn der Empfänger die Daten für erhebliche Zwecke der öffentlichen Sicherheit benötigt. Da nicht ersichtlich ist, ob damit sämtliche mit dem Vollzug des – allgemeinen oder möglicherweise auch besonderen – Ordnungsrechts befassten Behörden oder nur spezifische Sicherheitsbehörden gemeint sind, lässt sie schon den Kreis der Empfängerbehörden nicht klar erkennen. Im Übrigen fehlt es für beide Übermittlungstatbestände an Anforderungen sowohl hinsichtlich der erforderlichen Eingriffsschwellen als auch hinsichtlich eines qualifizierten Rechtsgüterschutzes (siehe jeweils oben Rn. 220 ff.). Der unbestimmte Verweis auf „erhebliche“ Zwecke der öffentlichen Sicherheit, der nur bagatellarische Sachverhalte ausschließen soll (vgl. zur gleichlautenden Formulierung in § 19 Abs. 1 Satz 2 BVerfSchG BTDrucks 18/4654, S. 34), reicht hierfür nicht.

b) Nicht mit den verfassungsrechtlichen Anforderungen vereinbar ist auch § 24 Abs. 3 BNDG in Verbindung mit § 20 Abs. 1 Satz 1 und 2 BVerfSchG, der zu einer Übermittlung von Informationen im Kontext von Staatsschutzdelikten an Polizeien und Staatsanwaltschaften ermächtigt. Zwar sind hier die Empfangsbehörden hinreichend bestimmt. Fraglich ist jedoch, ob die mehrgliedrige Verweisungskette noch den Anforderungen an die Normenklarheit genügt (oben Rn. 215). Unabhängig davon sind insoweit jedenfalls die Anforderungen an den Rechtsgüterschutz nicht durchgehend gewahrt (oben Rn. 221). Denn nicht alle in den §§ 74a, 120 GVG genannten und durch die Vorschrift pauschal in Bezug genommenen Straftaten können als besonders schwere Straftaten qualifiziert werden. Gleiches gilt für den offenen Übermittlungstatbestand, der beliebige sonstige Straftaten alleine aufgrund ihrer Zielsetzung oder des Motivs des Täters mit einbezieht. Auch legt die Vorschrift die erforderliche Übermittlungsschwelle nicht hinreichend bestimmt fest (oben Rn. 213 ff., 220 ff. und 227 f.). Der Gesetzgeber hat insoweit Voraussetzungen zu formulieren, die den Anforderungen an eine konkretisierte Gefahrenlage (vgl. BVerfGE 141, 220 <271 ff. Rn. 111 ff.>) oder hinreichend verdachtsbegründende Tatsachen entsprechen müssen. 312

c) Auch § 24 Abs. 2 Satz 1 BNDG in Verbindung mit § 19 Abs. 4 BVerfSchG, der eine Übermittlung an „sonstige“ – und damit im Wesentlichen private – Stellen regelt, genügt den Anforderungen des Art. 10 Abs. 1 GG nicht in jeder Hinsicht. Allerdings ist die Vorschrift weder unter Bestimmtheitsgesichtspunkten noch in Blick auf den mit ihr erstrebten Rechtsgüterschutz zu beanstanden. Der Verweis auf den „Schutz der 313

freiheitlichen demokratischen Grundordnung, des Bestandes oder der Sicherheit des Bundes oder eines Landes“ sowie auf die „Gewährleistung der Sicherheit von lebens- oder verteidigungswichtigen Einrichtungen nach § 1 Abs. 4 des Sicherheitsüberprüfungsgesetzes“ ist im Kontext des auch sonst eingeführten Begriffsverständnisses eindeutig und benennt Rechtsgüter von besonders schwerem Gewicht. Zweifelhaft ist jedoch wiederum, ob die mehrgliedrige Verweisung der Normenklarheit genügt (oben Rn. 213 ff.). Jedenfalls aber fehlt es an einer Übermittlungsschwelle (oben Rn. 216 ff. und 222).

d) Verfassungswidrig ist ebenfalls § 24 Abs. 2 Satz 1 BNDG in Verbindung mit § 19 Abs. 2 BVerfSchG, der – unter Verweis auf Art. 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 (NATO-Truppenstatut-Zusatzabkommen) vom 3. August 1959 (BGBl 1961 II S. 1218) – eine Übermittlung von Informationen an die NATO-Stationierungsstreitkräfte erlaubt. Der Vorschrift fehlt es zunächst schon an der gebotenen Normenklarheit und Bestimmtheit (oben Rn. 137 ff. und 213 ff.). Die dreigliedrige Verweisung auf eine völkervertragsrechtliche Norm, die ihrerseits weit ausladend und offen einen allgemeinen Rahmen der Zusammenarbeit regelt, lässt nicht mehr hinreichend normenklar und bestimmt erkennen, zu welchem Zweck hier Informationen übermittelt werden dürfen. Im Übrigen beschränkt die Vorschrift die Übermittlung nicht auf einen hinreichend gewichtigen Rechtsgüterschutz und setzt auch keine Übermittlungsschwellen voraus (jeweils oben Rn. 220 ff.). Die Bindung an die „Erforderlichkeit“ der Übermittlung reicht hierfür nicht. 314

e) Schließlich erfüllt auch § 24 Abs. 2 Satz 1 BNDG in Verbindung mit § 19 Abs. 3 BVerfSchG, der die Übermittlung an ausländische öffentliche Stellen regelt, die verfassungsrechtlichen Anforderungen in verschiedener Hinsicht nicht. 315

Es fehlt zunächst an einer hinreichend genauen Bestimmung der Empfängerbehörden, die sich vorliegend auch nicht aus den offenen Übermittlungszwecken bestimmen lassen (oben Rn. 137 ff. und 213 ff.; vgl. hierzu BVerfGE 130, 151 <203>; 133, 277 <337 f. Rn. 143>; 141, 220 <334 Rn. 306>). Zudem ist die Übermittlung wiederum nicht auf hinreichend qualifizierte Rechtsgüter beschränkt und ist eine Übermittlungsschwelle nicht vorgegeben (jeweils oben Rn. 220 ff.). 316

Gleichfalls verpflichtet die Vorschrift den Bundesnachrichtendienst nicht in normenklarer Weise zu einer Vergewisserung über den rechtsstaatlichen Umgang mit den übermittelten Daten. Zwar finden sich hierfür Ansätze in § 19 Abs. 3 Satz 2 BVerfSchG. Dieser genügt den maßstäblich dargelegten Anforderungen jedoch nicht (oben Rn. 233 ff.). So fehlt schon ein ausdrücklicher Verweis auf die Vergewisserung über datenschutzrechtliche Mindestgewährleistungen (oben Rn. 235 ff.) sowie eine Protokollierungspflicht (oben Rn. 229). Ferner wird etwa dem Schutz von Vertraulichkeitsbeziehungen nicht spezifisch Rechnung getragen (oben Rn. 240 mit Rn. 193 ff.). 317

Die gebotene Vergewisserung wird auch durch § 31 BNDG in Verbindung mit § 23 318

Nr. 1 BVerfSchG nicht hinreichend sichergestellt: Aus ihr ist nicht erkennbar, dass sich die übermittelnde Behörde aktiv hinsichtlich der Gegebenheiten im Zielland – sowohl hinsichtlich der besonderen datenschutzrechtlichen als auch der menschenrechtlichen Gewährleistungen – vergewissern, dies dokumentieren und gegebenenfalls aufkommenden Zweifeln nachgehen muss (oben Rn. 233 ff.). Auch ist durch die Vorschrift nicht ausgeschlossen, dass elementare rechtsstaatliche Belange im Wege der Abwägung verdrängt werden (oben Rn. 237).

f) Insgesamt genügen die Übermittlungsvorschriften, die überwiegend auf den in ihrer Fassung schon älteren und an die Entwicklung der Rechtsprechung nicht hinreichend angepassten Strukturen des Bundesverfassungsschutzgesetzes und anderer Sicherheitsgesetze beruhen, den verfassungsrechtlichen Anforderungen nicht. In formeller Hinsicht fehlt es überdies für alle Übermittlungstatbestände an einer Pflicht zur Protokollierung der Übermittlung (oben Rn. 229) sowie zur Nennung der für die Übermittlung in Anspruch genommenen Rechtsgrundlage (oben Rn. 229). 319

3. Auch die Regelung der Kooperationen in §§ 13 bis 15 BNDG steht mit den Verhältnismäßigkeitsanforderungen des Art. 10 Abs. 1 GG nicht in Einklang und ist damit nicht nur formell, sondern auch materiell verfassungswidrig. 320

a) Zunächst setzen sich hier verfassungsrechtliche Defizite fort, die schon für § 6 BNDG gelten. So fehlt es auch für die Datenerhebung und -verarbeitung im Rahmen von Kooperationen an hinreichend normenklaren Regelungen zur Aussonderung der Telekommunikationsdaten von Deutschen und Inländern (oben Rn. 176 ff. und 253). Ebenso werden auch hier kooperative Überwachungsmaßnahmen nicht auf gesetzlich hinreichend bestimmte und gewichtige Zwecke begrenzt (oben Rn. 175 f. und 253); § 13 Abs. 4 BNDG leistet eine solche Begrenzungsfunktion nicht hinreichend. Entsprechend wird die Kooperation nicht auf jeweils maßnahmebezogen zu konkretisierende Erkenntnisziele hin verpflichtet und durch sie strukturiert (oben Rn. 178 ff. und 253). 321

b) Soweit § 14 Abs. 1 BNDG die Auswertung der vom Bundesnachrichtendienst erhobenen Daten anhand von seitens der ausländischen Dienste benannten Suchbegriffen erlaubt, ist dies nicht durch hinreichende Kontrollpflichten flankiert. Insbesondere fehlt es an Schutzvorkehrungen für besonders schutzbedürftige Personen und Vertraulichkeitsbeziehungen (oben Rn. 194 ff. und 257). Im Übrigen ist es materiell zwar ausreichend, dass sich Suchbegriffe innerhalb der Kooperationsziele halten, einen Schutz gegenüber einer gezielten Erfassung von Zielen in der Europäischen Union bieten und mit Interessen der Bundesrepublik Deutschland vereinbar sein müssen (vgl. § 14 Abs. 1 Satz 1 und 2, Abs. 2 BNDG). Verfahrensmäßig nicht hinreichend abgesichert ist jedoch auch insoweit eine gesetzliche Pflicht, fremdbenannte Suchbegriffe auf der Grundlage von seitens der ausländischen Dienste zu plausibilisierenden Mindestangaben wirksam – und soweit erforderlich auch stichprobenartig händisch – auf ihre materielle Zulässigkeit zu prüfen (oben Rn. 254 ff.). 322

c) Auch für die automatisierte Datenübermittlung nach § 15 Abs. 1 BNDG fehlt es 323

zunächst an einer hinreichend anspruchsvollen Regelung zur Aussonderung von Daten besonders schutzwürdiger Personen oder von solchen, die aus besonderen Vertraulichkeitsbeziehungen stammen (oben Rn. 194 ff. und 257). Ebenfalls verlangt das Gesetz nicht in geboten normenklarer Form Zusagen der Empfänger zur Achtung von Vertraulichkeitsbeziehungen und Diskriminierungsverboten oder zur Wahrung grundlegender Übermittlungsschwellen (oben Rn. 260). Die abstrakt- allgemeine Zusage einer Datenverwendung nach rechtsstaatlichen Prinzipien gemäß § 13 Abs. 3 Nr. 4 BNDG reicht hierfür nicht. Eine Rechtsstaatlichkeits- vergewisserung ist gleichfalls nicht in der gebotenen Form vorgesehen (oben Rn. 233 ff. und 261). Schließlich enthält die Vorschrift keine Beschränkungen zur Übermittlung unselektierter Verkehrsdaten (oben Rn. 262 ff.).

4. Ohne weiteres ersichtlich ist im Übrigen, dass das Bundesnachrichtendienstgesetz keine ausreichenden Regelungen zur Kontrolle der genannten Befugnisse geschaffen hat. Zwar sind die Regelung der eng begrenzten Auskunftspflichten in § 22 BNDG und das Fehlen von Benachrichtigungspflichten in Bezug auf Über- wachungsmaßnahmen im Ausland gegenüber Ausländern für sich betrachtet nicht zu beanstanden. Jedoch bedarf es als Ausgleich für die Offenheit der Vorschriften und den faktisch erheblich eingeschränkten Rechtsschutz – wie maßstäblich dargelegt (oben Rn. 267 ff.) – einer ausgebauten unabhängigen objektivrechtlichen Kontrolle. Diese kann nach den geltenden Regeln von vornherein durch das Unabhängige Gremium und die Kontrolle des Bundesdatenschutzbeauftragen von den Befugnissen und von der organisatorischen wie institutionellen Ausgestaltung her nicht in der verfassungsrechtlich gebotenen Weise sichergestellt werden. 324

VII.

Die Vorschriften sind auch insoweit, als sie zu Überwachungsmaßnahmen gegenüber Journalisten ermächtigen und damit Eingriffe in Art. 5 Abs. 1 Satz 2 GG begründen, mit der Verfassung unvereinbar, da sie den spezifischen Schutzbedürfnissen unabhängiger ausländischer Journalisten nicht angemessen Rechnung tragen (vgl. dazu auch United Nations Office of the High Commissioner for Human Rights, Brief der Sonderberichterstatter vom 29. August 2016, OL DEU 2/2016, S. 5 f.). 325

F.

Unabhängig davon, wieweit in der vorliegenden Konstellation das Bundes- verfassungsgericht für die Prüfung zuständig wäre, ergeben sich entgegen der Auffassung der Beschwerdeführer aus den Grundrechten der Europäischen Union keine weiteren Maßgaben. Auch wenn die angegriffenen Vorschriften teilweise angesichts des Art. 15 RL 2002/58/EG als Durchführung des Unionsrechts im Sinne des Art. 51 Abs. 1 Satz 1 GRCh anzusehen sein sollten, gibt es schon keine konkreten und hinreichenden Anhaltspunkte dafür, dass die Grundrechte des Grundgesetzes in der vorliegenden Auslegung das Schutzniveau der Grundrechtecharta der Europäischen Union in der Rechtsprechung des Europäischen Gerichtshofs im hier zu entscheiden- 326

den Fall nicht mit gewährleisten (vgl. BVerfG, Beschluss des Ersten Senats vom 6. November 2019 - 1 BvR 16/13 -, Rn. 67 ff. – Recht auf Vergessen I). Insbesondere ergeben sich solche Anhaltspunkte nicht in Hinblick auf die Befugnis zur bevorratenden Speicherung und Auswertung von Verkehrsdaten aus den Entscheidungen des Europäischen Gerichtshofs zur Vorratsdatenspeicherungsrichtlinie (Urteil vom 8. April 2014, Digital Rights Ireland und Seitlinger u.a., C-293/12, C-594/12, EU:C:2014:238) und zu Vorratsdaten- speicherungsbefugnissen der Mitgliedstaaten (Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u.a., C-203/15 und C-698/15, EU:C:2016:970). In jenen Entscheidungen ging es um die Anforderungen an eine innerstaatlich vollständige Erfassung sämtlicher Telekommunikationsverbindungsdaten, die nahezu lückenlose Persönlichkeitsprofile einzelner Kommunikationsteilnehmer ermöglichten. Hiervon unterscheidet sich die Erhebung eines begrenzten Volumens an Verkehrsdaten der Auslandskommunikation aus ausgewählten Netzen – die damit in der Regel nicht die vollständigen Kommunikationsbeziehungen betroffener Personen erfassen können – grundlegend. Es ist also nicht ersichtlich, dass der Grundrechtsschutz des Grundgesetzes hier das Schutzniveau der Grundrechtecharta der Europäischen Union im Rahmen eines auf Vielfalt angelegten Grundrechtsschutzes in Europa nicht gewährleisten würde.

G.

I.

Die §§ 6, 7, 13 bis 15 BNDG sind danach verfassungswidrig. Verfassungswidrig sind auch §§ 19, 24 Abs. 1 Satz 1, Abs. 2 Satz 1, Abs. 3 BNDG, soweit sie Daten betreffen, die nach den vorstehenden Regelungen erhoben wurden. Sie verletzen die Beschwerdeführer zu 2) bis 8) in ihren Grundrechten aus Art. 10 Abs. 1 GG sowie die Beschwerdeführer zu 2) bis 7) in ihren Grundrechten aus Art. 5 Abs. 1 Satz 2 GG. Die §§ 9 bis 11, 16, 19, 20, 22, 32, 32a BNDG, die den Anforderungen an eine verhältnismäßige rechtsstaatliche Flankierung der für verfassungswidrig erklärten Befugnisse nicht hinreichend genügen, verlieren insoweit ihren Anwendungsbereich. 327

Offenbleiben kann, ob durch die angegriffenen Regelungen auch die Beschwerdeführerin zu 1) als juristische Person mit Sitz in einem Mitgliedstaat der Europäischen Union in ihren Grundrechten verletzt wird. Denn mit der Entscheidung über die Unvereinbarkeit der Vorschriften mit dem Grundgesetz, die nach § 31 Abs. 2 Satz 2 BVerfGG in Gesetzeskraft erwächst, hat sie ihr Rechtsschutzbegehren jedenfalls der Sache nach in dem Umfang erreicht, wie es auf der Grundlage einer etwaigen Grundrechtsberechtigung möglich wäre. 328

II.

Die Feststellung der Verfassungswidrigkeit gesetzlicher Vorschriften führt grundsätzlich zu ihrer Nichtigkeit. Allerdings kann sich das Bundesverfassungs- gericht, wie sich aus § 31 Abs. 2 Satz 2 und 3 BVerfGG ergibt, auch darauf beschränken, eine verfassungswidrige Norm nur für mit dem Grundgesetz unvereinbar zu erklären 329

(vgl. BVerfGE 109, 190 <235>). Es verbleibt dann bei einer bloßen Beanstandung der Verfassungswidrigkeit ohne den Ausspruch der Nichtigkeit. Die Unvereinbarkeitserklärung kann das Bundesverfassungsgericht zugleich mit der Anordnung einer befristeten Fortgeltung der verfassungswidrigen Regelung verbinden. Dies kommt in Betracht, wenn die sofortige Ungültigkeit der zu beanstandenden Norm dem Schutz überragender Güter des Gemeinwohls die Grundlage entziehen würde und eine Abwägung mit den betroffenen Grundrechten ergibt, dass der Eingriff für eine Übergangszeit hinzunehmen ist (vgl. BVerfGE 33, 1 <13>; 33, 303 <347 f.>; 40, 276 <283>; 41, 251 <266 ff.>; 51, 268 <290 ff.>; 109, 190 <235 f.>).

Dies ist vorliegend der Fall. Die beanstandeten Befugnisse können für die Sicherheit der Bundesrepublik Deutschland und als Handlungsgrundlage der Bundesregierung je nach politischer Situation, insbesondere bei Berücksichtigung der potentiellen Dynamik bedrohlicher Entwicklungen unter den Bedingungen der Informationstechnik, auch kurzfristig große Bedeutung gewinnen. Durch eine Nichtigerklärung oder eine vorläufige Außerkraftsetzung würden damit erhebliche Risiken eingegangen. Auch würde eine unvermittelte Aussetzung der Möglichkeit der Zusammenarbeit mit anderen Diensten das Vertrauen in eine verlässliche Zusammenarbeit möglicherweise langfristig beschädigen. Zu berücksichtigen ist umgekehrt, dass die beanstandeten Befugnisse ihrer Grundstruktur nach in verfassungsrechtlich tragfähiger Weise ausgestaltet werden können und damit nachbesserungsfähig sind. Es handelt sich zwar um grundlegende Nachbesserungen, da eine Neufassung solche Maßnahmen erstmals im Lichte des Art. 10 Abs. 1 GG regeln und damit in neuartiger Weise rechtsstaatliche Grenzen und Kontrollen schaffen muss. Angesichts der großen Bedeutung, die der Gesetzgeber der Auslandsaufklärung beimessen darf, ist eine vorübergehende Fortgeltung der verfassungswidrigen Vorschriften dennoch eher hinzunehmen als deren Beseitigung bis zu einer Neuregelung, mit der absehbar zu rechnen ist. 330

Der Gesetzgeber hat eine Neuregelung bis spätestens zum 31. Dezember 2021 zu schaffen. Die Fortgeltungsanordnung ist auf diesen Zeitpunkt befristet. 331

III.

Die Auslagenentscheidung beruht auf § 34a Abs. 2 BVerfGG. 332

Harbarth Masing Paulus

Baer Britz Ott

Christ Radtke

Bundesverfassungsgericht, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17

Zitiervorschlag BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 - Rn. (1 - 332), http://www.bverfg.de/e/rs20200519_1bvr283517.html

ECLI ECLI:DE:BVerfG:2020:rs20200519.1bvr283517