Leitsätze

zum Beschluss des Ersten Senats vom 8. Oktober 2024

- 1 BvR 1743/16 -

- 1 BvR 2539/16 -

BND – Cybergefahren

1. Die Befugnis zur strategischen Inland-Ausland-Fernmeldeaufklärung in Bezug auf Cybergefahren hat unter den heutigen Bedingungen der Kommunikationstechnik und ihrer Bedeutung für die Kommunikationsbeziehungen eine außerordentliche Reichweite. Das Eingriffsgewicht dieser Befugnis ist nicht mehr zu vergleichen mit demjenigen der Befugnisse, über die das Bundesverfassungsgericht in seiner Entscheidung zur strategischen Inland-Ausland-Fernmeldeaufklärung im Jahr 1999 zu entscheiden hatte (BVerfGE 100, 313), sondern übersteigt dieses deutlich. Zugleich haben sich die Analysemöglichkeiten der Nachrichtendienste weiterentwickelt.

2. a) Diesem besonders schweren Eingriffsgewicht steht ein überragendes öffentliches Interesse an einer wirksamen Inland-Ausland-Aufklärung gegenüber. Die für die Gewichtung dieses öffentlichen Interesses bedeutsamen Umstände sind sowohl mit Blick auf die grundlegend gewandelte außen- und sicherheitspolitische Lage als auch hinsichtlich der erheblich gesteigerten technologischen Möglichkeiten, auf die bei der Entwicklung von Gefahrenlagen zulasten der staatlichen Interessen der Bundesrepublik Deutschland zurückgegriffen werden kann, ebenfalls nicht mehr mit den damaligen Gegebenheiten (BVerfGE 100, 313) vergleichbar.

   b) In der digital transformierten Gesellschaft kann die Gefahr internationaler Cyberangriffe auf die IT-Infrastruktur elementarer Bereiche ein vergleichbares Ausmaß wie die Gefahr eines bewaffneten Angriffs erreichen.

3. Die Befugnis zur strategischen Inland-Ausland-Aufklärung ist trotz ihres besonders hohen Eingriffsgewichts aufgrund des überragenden öffentlichen Interesses grundsätzlich mit Art. 10 Abs. 1 GG vereinbar, bedarf aber der verhältnismäßigen Ausgestaltung.

   Erforderlich sind danach insbesondere Maßgaben zur Aussonderung der Telekommunikationsdaten aus rein inländischen Telekommunikationsverkehren, die Gewährleistung des Kernbereichsschutzes und Löschungspflichten sowie eine unabhängige objektivrechtliche Kontrolle.

Inhaltsverzeichnis

BUNDESVERFASSUNGSGERICHT

- 1 BvR 1743/16 -
- 1 BvR 2539/16 -

IM NAMEN DES VOLKES

In den Verfahren
über
die Verfassungsbeschwerden

I. des Herrn (...),

- Bevollmächtigte: (...) -

gegen 1. § 5 Absatz 1 Satz 3 Nummer 8, § 5a, § 10 Absatz 4 Sätze 3 und 4, § 15 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) in der Fassung des Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (Bundesgesetzblatt I Seite 1938),

2. § 5b Artikel 10-Gesetz in der Fassung des Gesetzes zur Änderung des BND-Gesetzes vom 22. Dezember 2023 (Bundesgesetzblatt I Nummer 410)

- 1 BvR 1743/16 -,

II. 1. des (...) e.V.,

2. der Frau (...),

3. der Frau (...),

4. des Herrn (...),

5. der Frau (...),

6. des Herrn (...),

- Bevollmächtigter: Prof. Dr. Matthias Bäcker, LL.M.,
Trützschlerstraße 11, 68199 Mannheim -

gegen

1. § 5 Absatz 1 Satz 3 Nummer 8, Absatz 2 Sätze 3 und 6, § 5a Satz 7, § 6 Absatz 1 Satz 5, § 12 Absatz 1 Satz 2 in Verbindung mit Absatz 2 Satz 1, § 15 Absatz 5 Satz 2 des Artikel 10-Gesetzes in der Fassung des Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (Bundesgesetzblatt I Seite 1938),

2. § 26a Absatz 2 Satz 2 des Bundesverfassungsschutzgesetzes (BVerfSchG) 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)

- 1 BvR 2539/16 -

hat das Bundesverfassungsgericht - Erster Senat -

unter Mitwirkung der Richterinnen und Richter

Präsident Harbarth,
Ott,
Christ,
Radtke,
Härtel,
Wolff,
Eifert,
Meßling

am 8. Oktober 2024 beschlossen:

1. § 5 Absatz 1 Satz 3 Nummer 8 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz) in der Fassung des Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (Bundesgesetzblatt I Seite 1938) ist mit Artikel 10 Absatz 1 des Grundgesetzes nicht vereinbar.

2. Im Übrigen werden die Verfassungsbeschwerden zurückgewiesen.

3. Bis zu einer Neuregelung, längstens jedoch bis zum 31. Dezember 2026 gilt die für mit dem Grundgesetz unvereinbar erklärte Vorschrift mit der folgenden Maßgabe fort:

   a) Maßnahmen gemäß § 5 Absatz 1 Satz 3 Nummer 8 Artikel 10-Gesetz dürfen nur getroffen werden, wenn durch den Einsatz automatisierter Filter – soweit technisch möglich – dafür gesorgt wird, dass Daten aus rein inländischen Telekommunikationsverkehren herausgefiltert und unverzüglich automatisiert gelöscht werden, und entsprechende Daten, die trotz dieser automatisierten Filterung erhoben werden, unverzüglich gelöscht werden.

   b) § 5 Absatz 2 Satz 3 Artikel 10-Gesetz findet in Bezug auf § 5 Absatz 2 Satz 2 Nummer 2 Artikel 10-Gesetz keine Anwendung.

   c) Auf die Protokolldaten gemäß § 5 Absatz 2 Satz 5 Artikel 10-Gesetz findet statt § 5 Absatz 2 Satz 6 Artikel 10-Gesetz die Regelung aus § 6 Absatz 1 Sätze 6 und 7 Artikel 10-Gesetz Anwendung.

4. Die Bundesrepublik Deutschland hat dem Beschwerdeführer in dem Verfahren 1 BvR 1743/16 zwei Drittel seiner notwendigen Auslagen zu erstatten. In dem Verfahren 1 BvR 2539/16 hat die Bundesrepublik Deutschland den Beschwerdeführenden zu 1) und 5) zwei Drittel und den Beschwerdeführenden zu 2) bis 4) und 6) ein Viertel ihrer notwendigen Auslagen zu erstatten.

Gründe:

A.

Die beiden Verfassungsbeschwerden richten sich gegen die gesetzliche Ermächtigung des Bundesnachrichtendienstes zur strategischen Inland-Ausland-Fernmeldeaufklärung in Bezug auf internationale Cybergefahren gemäß § 5 Abs. 1 Satz 3 Nr. 8 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10). Diese Überwachungsbefugnis wurde durch das am 21. November 2015 in Kraft getretene Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl I S. 1938) in das Artikel 10-Gesetz eingefügt. Zudem wenden sie sich gegen bereits zuvor eingeführte flankierende Regelungen zur verhältnismäßigen Ausgestaltung und Begrenzung der Befugnis des § 5 Abs. 1 Satz 3 G 10, die auch für die neue Ermächtigung in Nummer 8 gültig sind. 1

I.

Mit der neuen Befugnis zur Aufklärung von internationalen Cybergefahren in § 5 Abs. 1 Satz 3 Nr. 8 G 10 beabsichtigte der Bundesgesetzgeber, die bestehende Ermächtigung zur strategischen Inland-Ausland-Fernmeldeaufklärung an neue Bedrohungsszenarien im virtuellen Raum auch angesichts weltweit vernetzter oder vernetzbarer informationstechnischer Systeme (Cyberraum) anzupassen. Um den neuen Gefahren wirkungsvoll zu begegnen, seien die Befugnisse für die in § 5 Abs. 1 Satz 3 Nummern 1 bis 7 G 10 genannten Gefahrbereiche nicht ausreichend. Vielmehr sei eine gesetzliche Befugnis des Bundesnachrichtendienstes zur Aufklärung von Cyberangriffen insbesondere in Form von Cyberspionage oder Cybersabotage erforderlich. Mit der neuen Befugnis solle der Bundesnachrichtendienst einen Beitrag zum Ausbau und zur Verbesserung der Sicherheit der Informationstechnik (IT) im staatlichen und nichtstaatlichen Bereich sowie insgesamt zu einem sicheren Cyberraum leisten (vgl. BTDrucks 18/4654, S. 40 f.). 2

II.

Die für das Verfahren maßgeblichen Normen – die Befugnisnorm (1) und die sie flankierenden Regelungen (2) – haben folgenden Inhalt und Wortlaut: 3

1. § 5 Abs. 1 G 10 ermächtigt den Bundesnachrichtendienst zur strategischen Inland-Ausland-Fernmeldeaufklärung und hat auszugsweise den folgenden Wortlaut: 4

§ 5 G 10 – Voraussetzungen

(1) [1]Auf Antrag des Bundesnachrichtendienstes dürfen Beschränkungen nach § 1 für internationale Telekommunikationsbeziehungen, soweit eine gebündelte Übertragung erfolgt, angeordnet werden. [2]Die jeweiligen Telekommu-

nikationsbeziehungen werden von dem nach § 10 Abs. 1 zuständigen Bundesministerium mit Zustimmung des Parlamentarischen Kontrollgremiums bestimmt. [3]Beschränkungen nach Satz 1 sind nur zulässig zur Sammlung von Informationen über Sachverhalte, deren Kenntnis notwendig ist, um die Gefahr

1. bis 7. [...]
8. des internationalen kriminellen, terroristischen oder staatlichen Angriffs mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland

rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen. [...]

(2) [...]

Der in Bezug genommene § 1 G 10 lautet auszugsweise wie folgt: 5

§ 1 G 10 – Gegenstand des Gesetzes

(1) Es sind

1. [...]
2. der Bundesnachrichtendienst im Rahmen seiner Aufgaben nach § 1 Abs. 2 des BND-Gesetzes auch zu den in § 5 Abs. 1 Satz 3 Nr. 2 bis 8 [...] bestimmten Zwecken

berechtigt, die Telekommunikation zu überwachen und aufzuzeichnen [...].

(2) [...]

Der wiederum in Bezug genommene § 1 Abs. 2 des Gesetzes über den Bundesnachrichtendienst (BND-Gesetz – BNDG) lautet in Auszügen folgendermaßen: 6

§ 1 BNDG – Organisation und Aufgaben

(1) [...]

(2) [1]Der Bundesnachrichtendienst sammelt zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen und wertet sie aus. [...]

2. a) Die seit dem 29. Juni 2001 (BGBl I S. 1254) geltenden flankierenden Regelungen zur Begrenzung des Überwachungsvolumens in § 10 Abs. 4 Sätze 3 und 4 G 10 haben den folgenden Wortlaut: 7

§ 10 G 10 – Anordnung

(1) bis (3) [...]

(4) [1]In den Fällen der §§ 5 und 8 sind die Suchbegriffe in der Anordnung zu benennen. [2]Ferner sind das Gebiet, über das Informationen gesammelt werden sollen, und die Übertragungswege, die der Beschränkung unterliegen, zu bezeichnen. [3]Weiterhin ist festzulegen, welcher Anteil der auf diesen Übertragungswegen zur Verfügung stehenden Übertragungskapazität überwacht werden darf. [4]In den Fällen des § 5 darf dieser Anteil höchstens 20 vom Hundert betragen.

(5) bis (7) [...]

b) Die in § 5 Abs. 2 Satz 3 G 10 in Bezug auf ausländische Personen im Ausland geregelte Ausnahme von den Verboten nach § 5 Abs. 2 Satz 2 Nummern 1 und 2 G 10 lauten in der seit dem 5. August 2009 (BGBl I S. 2499) geltenden Fassung wie folgt: 8

§ 5 G 10 –Voraussetzungen

(1) [...]

(2) [1]Bei Beschränkungen von Telekommunikationsbeziehungen darf der Bundesnachrichtendienst nur Suchbegriffe verwenden, die zur Aufklärung von Sachverhalten über den in der Anordnung bezeichneten Gefahrenbereich bestimmt und geeignet sind. [2]Es dürfen keine Suchbegriffe verwendet werden, die

1. Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung bestimmter Telekommunikationsanschlüsse führen, oder
2. den Kernbereich der privaten Lebensgestaltung betreffen.

[3]Dies gilt nicht für Telekommunikationsanschlüsse im Ausland, sofern ausgeschlossen werden kann, dass Anschlüsse, deren Inhaber oder regelmäßige Nutzer deutsche Staatsangehörige sind, gezielt erfasst werden. [...]

c) Die ebenfalls seit August 2009 geltenden Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung in § 5a Sätze 1 bis 4 in Verbindung mit § 3a G 10 sind im laufenden Verfahren durch das Gesetz zur Anpassung des Verfassungsschutzrechts vom 5. Juli 2021 (BGBl I S. 2274) geändert worden. In § 3a G 10 ist ein zweiter Absatz angefügt worden; der Verweis in § 5a Satz 4 G 10 ist daraufhin redaktionell angepasst worden. Die Vorschriften lauten nunmehr wie folgt: 9

§ 5a G 10 – Schutz des Kernbereichs privater Lebensgestaltung

[1]Durch Beschränkungen nach § 1 Abs. 1 Nr. 2 dürfen keine Kommunikationsinhalte aus dem Kernbereich privater Lebensgestaltung erfasst werden. [2]Sind durch eine Beschränkung nach § 1 Abs. 1 Nr. 2 Kommunikationsinhalte aus dem Kernbereich privater Lebensgestaltung erfasst worden, dürfen diese nicht verwertet werden. [3]Sie sind unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. [4]§ 3a Absatz 1 Satz 2 bis 7 und Absatz 2 gilt entsprechend. [...]

§ 3a G 10 – Schutz des Kernbereichs privater Lebensgestaltung

(1) [...] [2]Soweit im Rahmen von Beschränkungen nach § 1 Abs. 1 Nr. 1 neben einer automatischen Aufzeichnung eine unmittelbare Kenntnisnahme erfolgt, ist die Maßnahme unverzüglich zu unterbrechen, soweit sich während der Überwachung tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. [3]Bestehen insoweit Zweifel, darf nur eine automatische Aufzeichnung fortgesetzt werden. [4]Automatische Aufzeichnungen nach Satz 3 sind unverzüglich einem bestimmten Mitglied der G 10-Kommission oder seinem Stellvertreter zur Entscheidung über die Verwertbarkeit oder Löschung der Daten vorzulegen. [5]Das Nähere regelt die Geschäftsordnung. [6]Die Entscheidung des

Mitglieds der Kommission, dass eine Verwertung erfolgen darf, ist unverzüglich durch die Kommission zu bestätigen. [7]Ist die Maßnahme nach Satz 2 unterbrochen worden, so darf sie für den Fall, dass sie nicht nach Satz 1 unzulässig ist, fortgeführt werden. [...]

(2) [...]

d) Die Regelung zum Schutz zeugnisverweigerungsberechtigter Personen in § 5b G 10, die durch das Gesetz zur Änderung des BND-Gesetzes vom 22. Dezember 2023 (BGBl I Nr. 410), in Kraft getreten am 1. Januar 2024, in das Artikel 10-Gesetz eingefügt worden ist, hat den folgenden Wortlaut: 10

§ 5b G 10 – Schutz zeugnisverweigerungsberechtigter Personen

Für den Schutz zeugnisverweigerungsberechtigter Personen gilt § 3b entsprechend.

§ 3b G10, auf den § 5b G 10 verweist, lautet wie folgt: 11

§ 3b G 10 – Schutz zeugnisverweigerungsberechtigter Personen

(1) [1]Maßnahmen nach § 1 Abs. 1 Nr. 1, die sich gegen eine in § 53 Absatz 1 Satz 1 Nummer 1, 2, 3 oder Nummer 4 der Strafprozessordnung genannte Person, im Falle von § 53 Absatz 1 Satz 1 Nummer 3 der Strafprozessordnung beschränkt auf Rechtsanwälte und Kammerrechtsbeistände, richten und voraussichtlich Erkenntnisse erbringen würden, über die diese Person das Zeugnis verweigern dürfte, sind unzulässig. [2]Dennoch erlangte Erkenntnisse dürfen nicht verwertet werden. [3]Aufzeichnungen hierüber sind unverzüglich zu löschen. [4]Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. [5]Die Sätze 2 bis 3 gelten entsprechend, wenn durch eine Maßnahme, die sich nicht gegen eine in Satz 1 genannte Person richtet, von einer dort genannten Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte.

(2) [1]Soweit durch eine Beschränkung eine in § 53 Abs. 1 Satz 1 Nr. 3 bis 3b oder Nr. 5 der Strafprozessordnung genannte Person, im Falle von § 53 Absatz 1 Satz 1 Nummer 3 der Strafprozessordnung mit Ausnahme von Rechtsanwälten und Kammerrechtsbeiständen, betroffen wäre und dadurch voraussichtlich Erkenntnisse erlangt würden, über die diese Person das Zeugnis verweigern dürfte, ist dies im Rahmen der Prüfung der Verhältnismäßigkeit unter Würdigung des öffentlichen Interesses an den von dieser Person wahrgenommenen Aufgaben und des Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. [2]Soweit hiernach geboten, ist die Maßnahme zu unterlassen oder, soweit dies nach der Art der Maßnahme möglich ist, zu beschränken.

(3) Die Absätze 1 und 2 gelten entsprechend, soweit die in § 53a der Strafprozessordnung Genannten das Zeugnis verweigern dürften.

(4) Die Absätze 1 bis 3 gelten nicht, sofern die zeugnisverweigerungsberechtigte Person Verdächtiger im Sinne des § 3 Abs. 2 Satz 2 ist oder tatsächliche Anhaltspunkte den Verdacht begründen, dass sie dessen in § 3 Abs. 1 bezeichnete Bestrebungen durch Entgegennahme oder Weitergabe von Mitteilungen bewusst unterstützt.

e) Die Protokollierung der Durchführung der strategischen Inland-Ausland-Fernmeldeaufklärung und die Löschung der Protokolldaten ist seit Juni 2001 in § 5 Abs. 2 Sätze 4 bis 6 G 10 geregelt. § 5 Abs. 2 G 10 lautet auszugsweise: 12

§ 5 G 10 – Voraussetzungen

(1) [...]

(2) [1]Bei Beschränkungen von Telekommunikationsbeziehungen darf der Bundesnachrichtendienst nur Suchbegriffe verwenden, die zur Aufklärung von Sachverhalten über den in der Anordnung bezeichneten Gefahrenbereich bestimmt und geeignet sind.

[...]

[4]Die Durchführung ist zu protokollieren. [5]Die Protokolldaten dürfen ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden. [6]Sie sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen.

Die Regelung in § 5a Sätze 5 bis 7 G 10 zur Protokollierung der Erfassung und Löschung von Kommunikationsinhalten, die den Kernbereich privater Lebensgestaltung betreffen, lautete seit August 2009 wie folgt: 13

§ 5a G 10 2009 – Schutz des Kernbereichs privater Lebensgestaltung

[...] [5]Die Tatsache der Erfassung der Daten und ihrer Löschung ist zu protokollieren. [6]Die Protokolldaten dürfen ausschließlich zum Zwecke der Durchführung der Datenschutzkontrolle verwendet werden. [7]Sie sind zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich sind, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt.

Am 5. Juli 2021 (BGBl I S. 2274) ist § 5a Satz 7 G 10 geändert worden und lautet nunmehr: 14

§ 5a G 10 2021 – Schutz des Kernbereichs privater Lebensgestaltung

[...] [5]Die Tatsache der Erfassung der Daten und ihrer Löschung ist zu protokollieren. [6]Die Protokolldaten dürfen ausschließlich zum Zwecke der Durchführung der Datenschutzkontrolle verwendet werden. [7]Sie sind sechs Monate nach der Mitteilung oder der Feststellung nach § 12 Absatz 2 zu löschen.

Die seit August 2009 geltenden Regelungen zur Protokollierung der Löschung von durch die strategische Inland-Ausland-Fernmeldeaufklärung erhobenen personenbezogenen Daten in § 6 Abs. 1 Sätze 3 bis 7 G 10 sind im laufenden Verfassungsbeschwerdeverfahren mehrfach geändert worden und haben nunmehr folgenden Wortlaut: 15

§ 6 G 10 – Prüf-, Kennzeichnungs- und Löschungspflichten, Zweckbindung

(1) [1]Der Bundesnachrichtendienst prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die erhobenen personenbezogenen Daten im Rahmen seiner Aufgaben allein oder zusammen mit bereits vorliegenden Daten für die in § 5 Abs. 1 Satz 3 bestimmten Zwecke erforderlich sind.

[2]Soweit die Daten für diese Zwecke nicht erforderlich sind und nicht für eine Übermittlung an andere Stellen benötigt werden, sind sie unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen.[3]Die Löschung ist zu protokollieren. [4]Die Protokolldaten dürfen ausschließlich zur Durchführung von Kontrollen der Datenverarbeitung, einschließlich der Datenschutzkontrolle, verwendet werden. [5]Die Protokolldaten sind am Ende des Kalenderjahres zu löschen, das dem Jahr der Protokollierung folgt. [6]Außer in den Fällen der erstmaligen Prüfung nach Satz 1 unterbleibt die Löschung, soweit die Daten für eine Mitteilung nach § 12 Abs. 2 oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Beschränkungsmaßnahme von Bedeutung sein können. [7]In diesem Fall ist die Verarbeitung der Daten einzuschränken; sie dürfen nur zu diesen Zwecken verwendet werden.

(2) bis (6) [...]

f) Die Regelung zu den Benachrichtigungspflichten in § 12 G 10 lautet seit August 2009 folgendermaßen: 16

§ 12 G 10 – Mitteilungen an Betroffene

(1) [1]Beschränkungsmaßnahmen nach § 3 sind dem Betroffenen nach ihrer Einstellung mitzuteilen. [2]Die Mitteilung unterbleibt, solange eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann oder solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist. [3]Erfolgt die nach Satz 2 zurückgestellte Mitteilung nicht binnen zwölf Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der Zustimmung der G 10-Kommission. [4]Die G 10-Kommission bestimmt die Dauer der weiteren Zurückstellung. [5]Einer Mitteilung bedarf es nicht, wenn die G 10-Kommission einstimmig festgestellt hat, dass

1. eine der Voraussetzungen in Satz 2 auch nach fünf Jahren nach Beendigung der Maßnahme noch vorliegt,
2. sie mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft vorliegt und
3. die Voraussetzungen für eine Löschung sowohl bei der erhebenden Stelle als auch beim Empfänger vorliegen.

(2) [1]Absatz 1 gilt entsprechend für Beschränkungsmaßnahmen nach den §§ 5 und 8, sofern die personenbezogenen Daten nicht unverzüglich gelöscht wurden. [2]Die Frist von fünf Jahren beginnt mit der Erhebung der personenbezogenen Daten.

(3) [...]

g) Die seit Juni 2001 geltende Regelung zur unabhängigen objektivrechtlichen Kontrolle in § 15 G 10 ist seit Erhebung der beiden Verfassungsbeschwerden mehrfach geändert worden und hat nunmehr folgende Fassung: 17

§ 15 G 10 – G 10-Kommission

(1) [1]Die G 10-Kommission besteht aus dem Vorsitzenden und vier Beisitzern sowie fünf stellvertretenden Mitgliedern, die an den Sitzungen mit Rede- und Fragerecht teilnehmen können. [2]Mindestens drei Mitglieder und drei stellvertretende Mitglieder müssen die Befähigung zum Richteramt besitzen. [3]Die

Mitglieder der G 10-Kommission sind in ihrer Amtsführung unabhängig und Weisungen nicht unterworfen. [4]Sie nehmen ein öffentliches Ehrenamt wahr und werden von dem Parlamentarischen Kontrollgremium nach Anhörung der Bundesregierung für die Dauer einer Wahlperiode des Deutschen Bundestages mit der Maßgabe bestellt, dass ihre Amtszeit erst mit der Neubestimmung der Mitglieder der Kommission endet. [5]Die oder der Ständige Bevollmächtigte des Parlamentarischen Kontrollgremiums nimmt regelmäßig an den Sitzungen der G 10-Kommission teil.

(2) [1]Die Beratungen der G 10-Kommission sind geheim. [2]Die Mitglieder der Kommission sind zur Geheimhaltung der Angelegenheiten verpflichtet, die ihnen bei ihrer Tätigkeit in der Kommission bekannt geworden sind. [3]Dies gilt auch für die Zeit nach ihrem Ausscheiden aus der Kommission.

(3) [1]Der G 10-Kommission ist die für die Erfüllung ihrer Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Deutschen Bundestages gesondert im Kapitel für die parlamentarische Kontrolle der Nachrichtendienste auszuweisen. [2]Der Kommission sind Mitarbeiter mit technischem Sachverstand zur Verfügung zu stellen.

(4) [1]Die G 10-Kommission tritt mindestens einmal im Monat zusammen. [2]Sie gibt sich eine Geschäftsordnung, die der Zustimmung des Parlamentarischen Kontrollgremiums bedarf. [3]Vor der Zustimmung ist die Bundesregierung zu hören.

(5) [1]Die G 10-Kommission entscheidet von Amts wegen oder auf Grund von Beschwerden über die Zulässigkeit und Notwendigkeit von Beschränkungsmaßnahmen. [2]Die Kontrollbefugnis der Kommission erstreckt sich auf die gesamte Verarbeitung der nach diesem Gesetz erlangten personenbezogenen Daten durch Nachrichtendienste des Bundes einschließlich der Entscheidung über die Mitteilung an Betroffene. [3]Der Kommission und ihren Mitarbeitern ist dabei insbesondere

1. Auskunft zu ihren Fragen zu erteilen,
2. Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Beschränkungsmaßnahme stehen, und
3. jederzeit Zutritt in alle Diensträume zu gewähren.

[4]Nummer 2 schließt ein, während einer Kontrolle beim Nachrichtendienst des Bundes dort Daten aus automatisierten Dateien selbst abrufen zu können. [5]Die Kommission kann dem Bundesbeauftragten für den Datenschutz Gelegenheit zur Stellungnahme in Fragen des Datenschutzes geben.

(6) [1]Das zuständige Bundesministerium holt die Zustimmung der G 10-Kommission zu den von ihm angeordneten Beschränkungsmaßnahmen ein. [2]Die Anordnung darf erst vollzogen werden, wenn die G 10-Kommission der angeordneten Beschränkungsmaßnahme nach Prüfung der Zulässigkeit und Notwendigkeit zugestimmt hat. [3]Stimmt die G 10-Kommission der angeordneten Beschränkungsmaßnahme nicht zu, hat das zuständige Bundesministerium die Anordnung unverzüglich aufzuheben.

(7) [1]Das zuständige Bundesministerium unterrichtet monatlich die G 10-Kommission über Mitteilungen von Bundesbehörden nach § 12 Abs. 1 und 2 oder über die Gründe, die einer Mitteilung entgegenstehen. [2]Hält die Kommission eine Mitteilung für geboten, ist diese unverzüglich vorzunehmen. [3]§ 12 Abs. 3 Satz 2 bleibt unberührt, soweit das Benehmen einer Landesbehörde erforderlich ist.

(8) Die G 10-Kommission und das Parlamentarische Kontrollgremium tauschen sich regelmäßig unter Wahrung der jeweils geltenden Geheimhaltungsvorschriften über allgemeine Angelegenheiten ihrer Kontrolltätigkeit aus.

§ 26a Abs. 2 Satz 2 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (BVerfSchG), der die Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit beschränkte, soweit eine Kontrolle durch die G 10-Kommission stattfand, lautete seit dem 25. Mai 2018 (BGBl I 2017 S. 2097) wie folgt: 18

§ 26a BVerfSchG 2018 – Unabhängige Datenschutzkontrolle

(1) [...]

(2) [1][...] [2]Soweit die Einhaltung von Vorschriften der Kontrolle durch die G 10-Kommission unterliegt, unterliegt sie nicht der Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, es sei denn, die G 10-Kommission ersucht die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.

(3) und (4) [...]

III.

1. Die strategische Inland-Ausland-Fernmeldeaufklärung nach dem Artikel 10-Gesetz zielt auf die Überwachung des internationalen Telekommunikationsverkehrs („Inland-Ausland-Kommunikation“), an dem mindestens ein inländischer und ein sich im Ausland befindender ausländischer Kommunikationsteilnehmender beteiligt sind. 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. 19

Abzugrenzen ist die strategische Inland-Ausland-Fernmeldeaufklärung von der strategischen Ausland-Ausland-Fernmeldeaufklärung nach dem BND-Gesetz, bei der es um die Überwachung des Telekommunikationsverkehrs geht, an dem ausschließlich ausländische Kommunikationsteilnehmende im Ausland beteiligt sind („Ausland-Ausland-Kommunikation“, vgl. dazu BVerfGE 154, 152 ff.). 20

Generell nicht strategisch überwachen darf der Bundesnachrichtendienst den Telekommunikationsverkehr, an dem auf beiden Seiten ausschließlich deutsche Staatsangehörige oder inländische Personen beteiligt sind (im Folgenden: rein inländische Telekommunikation – vgl. auch BVerfGE 154, 152 <252 Rn. 171>). 21

2. Maßnahmen der strategischen Inland-Ausland-Fernmeldeaufklärung dürfen gemäß § 9 Absätze 1 und 2 Nr. 4 G 10 nur auf Antrag des Bundesnachrichtendienstes angeordnet werden. Dieser Antrag muss nach § 9 Abs. 3 Satz 2 G 10 alle für die Anordnung erforderlichen Angaben enthalten. Der Bundesnachrichtendienst hat den Grund der Anordnung sowie Art, Umfang und Dauer der beabsichtigten Überwachungsmaßnahme anzugeben (vgl. § 10 Abs. 2 Satz 2 G 10) und die Suchbegriffe (Selektoren) zu benennen, die bei der Maßnahme verwendet werden sollen (vgl. § 10 Abs. 4 Satz 1 G 10). Dabei dürfen gemäß § 5 Abs. 2 Satz 1 G 10 nur solche Suchbegriffe verwendet werden, die zur Aufklärung von Sachverhalten über die in den jeweiligen Anordnungen zu bezeichnenden Gefahrenbereiche (vgl. § 5 Abs. 1 Satz 3 Nummern 1 bis 8 G 10) bestimmt und geeignet sind. Zudem sind das Gebiet zu bezeichnen, über das Informationen gesammelt werden sollen, und die Übertragungswege, die überwacht werden sollen (§ 10 Abs. 4 Satz 2 G 10). 22

Aufgrund des jeweiligen Antrags des Bundesnachrichtendienstes ordnet das Bundesministerium des Innern und für Heimat die Beschränkung des Fernmeldegeheimnisses an (vgl. § 10 Abs. 1 G 10). Diese Beschränkungsanordnung muss die soeben für den Antragsinhalt benannten Angaben enthalten. Ferner ist der Anteil der auf diesen Übertragungswegen zur Verfügung stehenden Übertragungskapazität festzulegen, der überwacht werden darf (§ 10 Abs. 4 Satz 3 G 10). Dieser Anteil darf nicht größer sein als 20 % der Übertragungskapazität (§ 10 Abs. 4 Satz 4 G 10). Die Beschränkungsanordnung ist auf höchstens drei Monate zu befristen (§ 10 Abs. 5 Satz 1 G 10). Alle angeordneten Beschränkungsmaßnahmen unterliegen der objektiven Rechtskontrolle durch die G 10-Kommission und bedürfen nach § 15 Abs. 6 Satz 1 G 10 deren Zustimmung. Eine Maßnahme darf erst vollzogen werden, wenn die G 10-Kommission der angeordneten Beschränkungsmaßnahme nach Prüfung der Zulässigkeit und Notwendigkeit zugestimmt hat (vgl. § 15 Abs. 6 Satz 2 G 10). 23

Bei der Überwachung der nicht kabelgebundenen internationalen Telekommunikation (Übertragung durch Satelliten oder Richtfunk) bedarf es nach dem dargelegten Sachverhalt keiner weiteren Verfahrensschritte. Denn der Bundesnachrichtendienst kann die Rohdatenströme der Telekommunikation bei nicht kabelgebundener Übertragung mit eigenen Abhörvorrichtungen selbst erfassen (vgl. BVerfGE 100, 313 <363>; 154, 152 <229 Rn. 114>; zu Abhörstationen des Bundenachrichtendienstes: BTDrucks 18/12850, S. 761 ff., S. 1000 ff.). 24

Bei der Überwachung der kabelgebundenen internationalen Telekommunikation, die in der Praxis den Regelfall darstellt (vgl. BTDrucks 14/5655, S. 17; 18/12850, S. 708 f.; 25

Roggan, G-10-Gesetz, 2. Aufl. 2018, § 5 Rn. 8), sind hingegen weitere Verfahrensschritte erforderlich. Denn hier kann der Bundesnachrichtendienst die Rohdatenströme aus den zu überwachenden Kabeln nicht mit eigenen Abhörvorrichtungen erfassen (vgl. zum technischen Zugriff auf die Datenströme: BVerwG, Urteil vom 30. Mai 2018 – BVerwG 6 A 3.16 –, Rn. 5). Deshalb ist er auf die Mitwirkung oder Duldung der Betreiber von zu überwachenden Telekommunikationsanlagen angewiesen. Nach § 2 Abs. 1a Sätze 1 und 2 G 10 (bis Juli 2021: § 2 Abs. 1 Sätze 3 und 5 G 10 a.F.) sind die Erbringer von Telekommunikationsdiensten (vgl. § 3 Nr. 61 TKG) und die an der Erbringung Mitwirkenden verpflichtet, auf Anordnung entweder Telekommunikationsverkehre an den Bundesnachrichtendienst auszuleiten oder eine Ausleitung zu dulden. Den Betreibern der betroffenen Telekommunikationsanlagen ist die Beschränkungsanordnung des zuständigen Bundesministeriums gemäß § 10 Abs. 6 Satz 1 G 10 insoweit mitzuteilen, als dies erforderlich ist, um die Erfüllung der Mitwirkungspflicht zu ermöglichen.

3. Im Rahmen der strategischen Inland-Ausland-Fernmeldeaufklärung erfasst der Bundesnachrichtendienst in der Praxis zunächst die Rohdaten der gebündelt übertragenen Telekommunikation aus den Übertragungswegen, für die Beschränkungsanordnungen bestehen. Die Bündelung von Telekommunikationsverkehren, die zuerst bei Satellitenverkehren verwendet wurde und nunmehr auch bei kabelgebundener Übertragung verwendet wird, macht es möglich, auf ein- und demselben physikalischen Übertragungsweg (Kabel oder Satellit) mehrere Zehntausend Verkehre gleichzeitig zu übertragen (vgl. BTDrucks 14/5655, S. 17 f.; Roggan, G-10-Gesetz, 2. Aufl. 2018, § 5 Rn. 8; Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 5 G 10 Rn. 2, 4). 26

Anschließend werden die Rohdaten im alleinigen Verfügungsbereich des Bundesnachrichtendienstes in einem mehrstufigen Prozess automatisiert gefiltert und ausgewertet. Dabei werden die Datenströme zunächst technisch aufbereitet, um die verschiedenen Datenarten (etwa Streamingdaten, Internetverlaufsdaten, Daten aus Telekommunikationsvorgängen) zuordnen zu können. 27

Um rein inländische Telekommunikationsverkehre automatisch auszusondern, werden die Rohdaten im Rahmen des Datenfilterungssystems (DAFIS) anhand verschiedener Formalkriterien – wie Ländervorwahlen von Telefonnummern („+49“), Toplevel-Domains („.de“) oder IP-Adressen – gefiltert. Außerdem werden die Datenverkehre mit einer beim Bundesnachrichtendienst geführten Liste von Telekommunikationskennungen abgeglichen, die Deutschen oder Inländern zugeordnet werden können („G 10-Positivliste“). Die bei dieser Filterung als rein inländisch identifizierte Kommunikation wird automatisch ausgesondert und gelöscht. 28

Bei der paketvermittelten Telekommunikation führt der Bundesnachrichtendienst nach Angaben der Bundesregierung ein weiteres elektronisches Filterverfahren zur Erkennung rein inländischer Kommunikation durch („G 10-Bewertung“). Dieses Verfahren berücksichtigt weitere nicht näher präzisierte metadatenbezogene Indizien und Parameter, die auf einen Deutschlandbezug hinweisen. 29

Nach Angaben der Bundesregierung können anhand des DAFIS und der G 10-Bewertung 96 bis 98 % aller rein inländischen Telekommunikationsverkehre automatisch ausgesondert werden. Die exakte Fehlerquote der gesamten Filterung ist nicht bekannt. 30

Im Anschluss werden die nicht ausgefilterten Rohdaten automatisiert mit den vorher in den jeweiligen Beschränkungsanordnungen festgelegten Suchbegriffen abgeglichen. Telekommunikationsinhalte gelangen damit nur in eine händische Auswertung durch Beschäftigte des Bundesnachrichtendienstes, wenn Elemente einer erfassten Telekommunikation bei diesem computergesteuerten Abgleich mit den Suchbegriffen als relevant aus dem Datenstrom ausgesondert wurden („Treffer“). Rohdaten, bei denen der Abgleich mit den Suchbegriffen keinen Treffer ergibt, werden umgehend aus den Erfassungssystemen gelöscht. 31

Die als Treffer gespeicherten Telekommunikationsvorgänge werden in einem mehrstufigen Bewertungsverfahren manuell auf ihre nachrichtendienstliche Relevanz untersucht und weiter ausgewertet. Dabei wird auch manuell geprüft, ob trotz der automatischen Filterung noch rein inländische Telekommunikationsverkehre oder solche mit Bezug zum Kernbereich der privaten Lebensgestaltung erfasst wurden. Nicht nachrichtendienstlich relevante Daten und im automatisierten Verfahren nicht erkannte rein inländische Telekommunikationsverkehre oder solche mit Kernbereichsbezug werden gelöscht. 32

4. Die durch die strategische Inland-Ausland-Fernmeldeaufklärung erhobenen personenbezogenen Daten („Treffer“) sind gemäß § 6 Abs. 1 Satz 1 G 10 unverzüglich und sodann in Abständen von höchstens sechs Monaten vom Bundesnachrichtendienst daraufhin zu prüfen, ob sie im Rahmen seiner Aufgaben allein oder zusammen mit bereits vorliegenden Daten für die in § 5 Abs. 1 Satz 3 G 10 bestimmten Zwecke erforderlich sind. Nicht erforderliche Daten sind nach § 6 Abs. 1 Satz 2 G 10 unverzüglich unter Aufsicht zu löschen. Die Löschung ist gemäß § 6 Abs. 1 Satz 3 G 10 zu protokollieren. Diese Protokolldaten sind am Ende des Kalenderjahrs zu löschen, das dem Jahr der Protokollierung folgt (§ 6 Abs. 1 Satz 5 G 10). Außerdem sind die erhobenen Daten gemäß § 6 Abs. 2 G 10 zu kennzeichnen und dürfen nur zu den in § 5 Abs. 1 Satz 3 G 10 genannten Aufklärungszwecken und zur Datenübermittlung nach §§ 7 und 7a G 10 genutzt werden. 33

IV.

Mit ihren am 5. August 2016 (1 BvR 1743/16) und am 11. November 2016 (1 BvR 2539/16) erhobenen Verfassungsbeschwerden machen die Beschwerdeführenden geltend, durch die angegriffenen Vorschriften in ihrem Fernmeldegeheimnis aus Art. 10 Abs. 1 GG verletzt zu sein. 34

Im Hinblick auf den Kernbereichsschutz rügen die Beschwerdeführenden in dem Verfahren 1 BvR 2539/16 außerdem eine Verletzung des Art. 1 Abs. 1 GG. Hinsichtlich der Regelungen zu den Dokumentations-, Löschungs- und Benachrichtigungspflichten rügen sie auch eine Verletzung des Art. 19 Abs. 4 GG. Bezüglich des nur für Deutsche und Inländer geltenden Verbots der gezielt personenbezogenen Überwachung in § 5 Abs. 2 Satz 2 Nr. 1 G 10 machen die ausländischen Beschwerdeführenden zu 5) und 6) im Verfahren 1 BvR 2539/16 zudem eine Verletzung von Art. 3 Abs. 1 GG geltend. 35

Mit Schriftsatz vom 23. Februar 2024 hat der Beschwerdeführer im Verfahren 1 BvR 1743/16 seine Verfassungsbeschwerde auf die am 1. Januar 2024 in Kraft getretene Regelung zum Schutz zeugnisverweigerungsberechtigter Personen in § 5b G 10 erweitert. 36

Soweit die Beschwerdeführenden im Verfahren 1 BvR 2539/16 zunächst die unzureichende Kooperation der Kontrollorgane bei der objektivrechtlichen Kontrolle gemäß § 15 Abs. 5 G 10 in Verbindung mit § 24 Abs. 2 Satz 3 des Bundesdatenschutzgesetzes in der Fassung vom 25. Februar 2015 (BGBl I S. 162 – im Folgenden: BDSG 2015) gerügt hatten, haben sie ihre Verfassungsbeschwerde mit Schriftsatz vom 4. Juni 2018 umgestellt. Nunmehr wenden sie sich insoweit gegen § 15 Abs. 5 G 10 in Verbindung mit § 26a Abs. 2 Satz 2 BVerfSchG 2018. 37

Soweit die Beschwerdeführenden im Verfahren 1 BvR 2539/16 zunächst auch die Befugnisse des Bundesnachrichtendienstes, gemäß § 5 Abs. 1 Satz 3 Nr. 8 G 10 erhobene Daten an andere Behörden zu übermitteln (§ 7 Absätze 2, 4, 4a und § 7a Abs. 1 Satz 1, Abs. 2 G 10 in der Fassung des Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015, BGBl I S. 1938 – im Folgenden: G 10 2015), beanstandet hatten, haben sie mit Schriftsatz vom 5. Februar 2024 diesen Teil der Verfassungsbeschwerde für erledigt erklärt. 38

1. Die Beschwerdeführenden sind der Ansicht, die Verfassungsbeschwerden seien zulässig. 39

a) Sie seien von der Befugnis zur strategischen Inland-Ausland-Fernmeldeaufklärung und dem darauf gründenden Handeln des Bundesnachrichtendienstes unmittelbar, selbst und gegenwärtig betroffen. Der Beschwerdeführer im Verfahren 1 BvR 1743/16 arbeite als Rechtsanwalt insbesondere zu Fragen des Datenschutz- und IT-Rechts und kommuniziere viel mit ausländischen Kollegen und Mandanten. Der Beschwerdeführer zu 1) im Verfahren 40

1 BvR 2539/16 setze sich als deutscher Ableger einer internationalen Nichtregierungsorganisation für den Schutz der Menschenrechte – insbesondere gegenüber staatlichen Überwachungsmaßnahmen – ein. Die Beschwerdeführenden zu 2) und 4) im Verfahren 1 BvR 2539/16 engagierten sich als Mitglieder des Beschwerdeführers zu 1) für den Menschenrechtsschutz in Indonesien und in den Vereinigten Staaten von Amerika (USA). Hierzu unterhielten sie telefonischen und E-Mail-Kontakt mit Personen im Ausland. Die Beschwerdeführerin zu 3) sei deutsche und iranische Staatsangehörige und kommuniziere mittels E-Mail, Telefon und Messengerdiensten mit ihrer im Iran lebenden Schwester. Die Beschwerdeführenden zu 5) und 6) seien US-amerikanische Staatsangehörige, die in den USA lebten, und in regelmäßigem auch beruflichem Telekommunikationskontakt mit Personen in Deutschland stünden.

Die Beschwerdeführenden führen weiter dazu aus, dass und inwiefern sie aufgrund dieser Umstände direkt oder mittelbar Ziel staatlicher Überwachung werden könnten. Als potenziell Betroffene könnten sie jedoch grundsätzlich nicht gerichtlich gegen konkrete Umsetzungsakte vorgehen, weil sie von der Umsetzung keine Kenntnis erlangten und wegen weitreichender Ausnahmen in § 12 Abs. 1 Satz 2 in Verbindung mit Abs. 2 Satz 1 G 10 eine nachträgliche Benachrichtigung nicht sichergestellt sei. 41

b) Die Verfassungsbeschwerden genügten den Anforderungen des Grundsatzes der Subsidiarität. Es sei nicht zumutbar, zunächst fachgerichtlichen Rechtsschutz zu suchen. 42

2. Die Verfassungsbeschwerden seien begründet. § 5 Abs. 1 Satz 3 Nr. 8 G 10 greife in ungerechtfertigter Weise in das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG ein, denn diese Überwachungsbefugnis sei zu unbestimmt und unverhältnismäßig. 43

a) Die Beschwerdeführenden im Verfahren 1 BvR 2539/16 machen insoweit geltend, dass die anlasslose strategische Inland-Ausland-Fernmeldeaufklärung gegenwärtig nicht mehr zu rechtfertigen sei, weil ihre Eingriffsintensität seit dem Urteil vom 14. Juli 1999 (BVerfGE 100, 313), in dem das Bundesverfassungsgericht diese Überwachungsbefugnis grundsätzlich gebilligt habe, deutlich zugenommen habe. 44

b) Der Beschwerdeführer in dem Verfahren 1 BvR 1743/16 trägt vor, dass dem Bundesgesetzgeber die Kompetenz für den Erlass dieser Befugnis fehle. 45

c) Darüber hinaus machen alle Beschwerdeführenden geltend, § 5 Abs. 1 Satz 3 Nr. 8 G 10 sei nicht angemessen, weil die dort geregelte Befugnis unzureichend strukturiert und begrenzt werde. 46

aa) Sie rügen insoweit, dass das Überwachungsvolumen durch § 10 Abs. 4 Sätze 3 und 4 G 10 unzureichend begrenzt werde. Die Norm setze einen Anreiz, in die Beschränkungs- 47

anordnung möglichst viele Übertragungswege aufzunehmen, um eine möglichst hohe Gesamtüberwachungskapazität zu erreichen, nach der sich die Obergrenze bemesse. Außerdem fehle im Artikel 10-Gesetz eine Gesamtbetrachtung aller Überwachungsanordnungen, so dass der Bundesnachrichtendienst durch unterschiedliche Anordnungen einen erheblich über der 20 %-Obergrenze liegenden Anteil der internationalen Telekommunikation überwachen könne.

bb) Zudem machen die Beschwerdeführenden geltend, dass die im Gesetz vorgesehene Beschränkung der Überwachung auf internationale Telekommunikationsbeziehungen in der Praxis nicht funktioniere, da es keine Übertragungswege mehr gebe, über die ausschließlich internationale Kommunikation übertragen würde. 48

cc) Außerdem wenden sie sich gegen einen unzureichenden Schutz des Kernbereichs der privaten Lebensgestaltung. Der Beschwerdeführer im Verfahren 1 BvR 1743/16 rügt in diesem Zusammenhang, dass § 5a G10 den Kernbereich der privaten Lebensgestaltung bei der Datenerhebung und der Datenauswertung unzureichend schütze. Die Beschwerdeführenden im Verfahren 1 BvR 2539/16 wenden sich dagegen, dass § 5 Abs. 2 Satz 3 G 10 – als Ausnahme zu § 5 Abs. 2 Satz 2 Nr. 2 G 10 – die Verwendung von kernbereichsrelevanten Suchbegriffen in Bezug auf ausländische Personen im Ausland zulasse. 49

dd) Alle Beschwerdeführenden rügen eine unzureichende unabhängige objektivrechtliche Kontrolle. Der Beschwerdeführer im Verfahren 1 BvR 1743/16 macht dazu geltend, die unabhängige objektivrechtliche Kontrolle sei unzureichend ausgestaltet, um die fehlenden subjektiven Rechtsschutzmöglichkeiten zu kompensieren. Die Beschwerdeführenden im Verfahren 1 BvR 2539/16 tragen vor, dass die Zusammenarbeit der verschiedenen Kontrollinstanzen bei der objektiven Rechtskontrolle auf ungenügende Weise geregelt sei. Gemäß § 26a Abs. 2 Satz 2 BVerfSchG 2018 könne sich kein Kontrollorgan ein umfassendes Bild von sämtlichen Aufklärungsaktivitäten des Bundesnachrichtendienstes machen. 50

ee) Der Beschwerdeführer im Verfahren 1 BvR 1743/16 macht zudem geltend, der Schutz von Vertraulichkeitsbeziehungen sei unzureichend. Der neue § 5b G 10 sei zu unbestimmt und nicht normenklar, denn durch den Verweis auf § 3b G 10 entstehe eine mehrgliedrige Verweisungskette mit unklarem Anwendungsbereich. 51

ff) Die Beschwerdeführenden im Verfahren 1 BvR 2539/16 rügen, dass § 5 Abs. 2 Satz 2 Nr. 1 G 10 die Möglichkeit einer gezielten Überwachung deutscher Staatsangehöriger durch formale Suchbegriffe (etwa E-Mail-Adressen, Anschlusskennungen, wie Telefonnummern oder IP-Adressen) nicht – wie aufgrund von Art. 10 GG geboten – umfassend ausschließe. Die Norm verbiete nur die gezielte Erfassung bestimmter „Telekommunikationsanschlüsse“. Dieses Verbot schütze Telekommunikationsteilnehmende vor der gezielten 52

Erfassung nur dann umfassend, wenn deren Telekommunikationsverkehre stets durch solche Telekommunikationsanschlüsse dem jeweiligen Teilnehmenden zugeordnet werden könnten. Dies sei aber nicht der Fall. Ein Telekommunikationsanschluss sei nach § 2 Nr. 10 der Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (TKÜV) der durch eine Adressierungsangabe bezeichnete Zugang zu einer Telekommunikationsanlage, der es einer Person ermögliche, Telekommunikationsdienste zu nutzen. Eine „Telekommunikationsanlage“ sei nach § 3 Nr. 23 des Telekommunikationsgesetzes (TKG) in der Fassung vom 22. Juni 2004 (BGBl I S. 1190) eine technische Einrichtung, die als Nachrichten identifizierbare Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren könne. Die Begriffe der „Telekommunikationsanlage“ und des damit verbundenen „Telekommunikationsanschlusses“ bezögen sich danach auf die technische Schicht der Übertragung von Telekommunikationssignalen, nicht aber auf die Dienstschicht, die auf der Signalübertragung aufsetze. Damit seien Teilnehmerkennungen auf der Dienstschicht (wie E-Mail-Adressen) vom Begriff des Telekommunikationsanschlusses nicht umfasst. E-Mail-Adressen seien auf E-Mail-Postfächer auf der Dienstschicht bezogen und nicht auf Telekommunikationsanschlüsse auf der Schicht der Signalübertragung wie Internetanschlüsse (etwa DSL- oder Glasfaser-Anschlüsse). E-Mail-Postfächer und Telekommunikationsanschlüsse seien technisch auch nicht miteinander verknüpft. Ein E-Mail-Postfach könne vielmehr grundsätzlich von jedem Telekommunikationsanschluss weltweit angesteuert werden. Vor diesem Hintergrund dürfte der Bundesnachrichtendienst nach dem Wortlaut des § 5 Abs. 2 Satz 2 G 10 E-Mail-Adressen unbeschränkt als formale Suchbegriffe verwenden, wodurch deutsche Staatsangehörige unzureichend gegen eine gezielte Überwachung geschützt würden.

gg) Außerdem wenden sich die Beschwerdeführenden im Verfahren 1 BvR 2539/16 gegen die Ausgestaltung der gezielten Überwachung ausländischer Personen im Ausland. Zum einen sei das Fernmeldegeheimnis verletzt, da § 5 Abs. 2 Satz 3 in Verbindung mit Satz 2 Nr. 1 G 10 nicht sicherstelle, dass diese gezielte Überwachung auf hinreichender Tatsachengrundlage und hinreichendem Näheverhältnis der zu überwachenden Person zu dem aufzuklärenden Gefahrenbereich beruhe. Zum anderen sei Art. 3 Abs. 1 GG verletzt, weil ausländische Kommunikationsteilnehmende im Ausland ohne sachliche Rechtfertigung schlechter gestellt seien als Deutsche und inländische Personen. 53

hh) Darüber hinaus rügen die Beschwerdeführenden im Verfahren 1 BvR 2539/16, dass die Aufbewahrungsfristen für die Dokumentation der Durchführung der strategischen Inland-Ausland-Fernmeldeaufklärung (§ 5 Abs. 2 Satz 6 G 10), der Löschung kernbereichsrelevanter Kommunikationsinhalte (§ 5a Satz 7 G 10) und der Löschung im Rahmen der Überwachung erhobener personenbezogener Daten (§ 6 Abs. 1 Satz 5 G 10) zu kurz seien. Sie ermöglichten keine effektive objektivrechtliche Kontrolle und keinen effektiven subjektiven Rechtsschutz. 54

ii) Schließlich wendet sich die Verfassungsbeschwerde 1 BvR 2539/16 dagegen, dass § 12 Abs. 1 Satz 2 in Verbindung mit Abs. 2 Satz 1 G 10 zu weitgehende Ausnahmen von der Benachrichtigungspflicht enthalte. 55

V.

Zu den beiden Verfassungsbeschwerden haben die Bundesregierung, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und für das Bundesverwaltungsgericht der 6. Revisionssenat Stellung genommen. 56

1. Die Bundesregierung hält beide Verfassungsbeschwerden für unzulässig und unbegründet. 57

a) Die Beschwerdeführenden seien nicht beschwerdebefugt. Als Funktionsträger ausländischer juristischer Person seien die Beschwerdeführenden zu 5) und 6) im Verfahren 1 BvR 2539/16 schon nicht grundrechtsberechtigt. Zudem habe keiner der Beschwerdeführenden ausreichend dargelegt, mit einiger Wahrscheinlichkeit von Maßnahmen gemäß § 5 Abs. 1 Satz 3 Nr. 8 G 10 betroffen zu sein. 58

Die Verfassungsbeschwerden wahrten außerdem nicht die Jahresfrist des § 93 Abs. 3 BVerfGG, soweit sie sich gegen die flankierenden Regelungen zur verhältnismäßigen Ausgestaltung der Überwachungsbefugnis richteten. Diese Vorschriften seien durch die angegriffene Gesetzesänderung im November 2015 nicht verändert worden, und es sei nicht ersichtlich, dass ihnen mit der Gesetzesänderung eine neue, die Beschwerdeführenden stärker als bisher belastende Wirkung verliehen worden sei. 59

b) Die Verfassungsbeschwerden seien auch unbegründet, denn § 5 Abs. 1 Satz 3 Nr. 8 G 10 sei mit dem Grundgesetz vereinbar. 60

Dem Bund stehe die Gesetzgebungskompetenz für den Erlass dieser Überwachungsbefugnis aus Art. 73 Abs. 1 Nr. 1 GG zu. 61

§ 5 Abs. 1 Satz 3 Nr. 8 G 10 sei auch hinreichend bestimmt und normenklar. Aufgrund der Diversität von Angriffen auf informationstechnische Systeme hinsichtlich technischer Durchführung, Urheberschaft und Zielrichtung sei eine genauere Umschreibung der Cybergefahren nicht möglich. 62

Die Überwachungsbefugnis sei zudem verhältnismäßig. Sie verfolge das legitime Ziel, die durch staatliche, terroristische und kriminelle Akteure hervorgerufenen neuen Gefahren des Cyberraums rechtzeitig zu erkennen und ihnen zu begegnen. § 5 Abs. 1 Satz 3 Nr. 8 G 10 sei geeignet und erforderlich, diesen Gesetzeszweck zu erreichen. Die strategische Inland-Ausland-Fernmeldeüberwachung sei eine wesentliche Säule 63

nachrichtendienstlicher Informationsgewinnung. Sie liefere aktuelle, authentische Erkenntnisse in Echtzeit und sei eine sichere Art der Informationsgewinnung, da weder menschliche Quellen noch Mitarbeitende des Bundesnachrichtendienstes im Einsatzland tätig werden müssten.

Außerdem sei die Befugnis des § 5 Abs. 1 Satz 3 Nr. 8 G 10 verhältnismäßig im engeren Sinne, da sie durch flankierende Regelungen hinreichend begrenzt werde. 64

Gemäß § 10 Abs. 4 Sätze 3 und 4 G 10 dürfe nur ein Anteil von 20 % der Übertragungskapazität überwacht werden, die auf den der Beschränkung unterliegenden Übertragungswegen zur Verfügung stehe. Mit dieser Regelung habe der Gesetzgeber der Erweiterung der strategischen Inland-Ausland-Fernmeldeaufklärung im Juni 2001 von der nicht kabelgebundenen auf die kabelgebundene Telekommunikation ausreichend Rechnung getragen. 65

Zudem würden rein inländische Telekommunikationsverkehre, die der Bundesnachrichtendienst miterfasse, in der Praxis ausgesondert und gelöscht. Im Bereich der leitungsvermittelten klassischen Telefonie (einschließlich Fax und herkömmlicher SMS, vgl. BTDrucks 18/12850, S. 712 f.) erlaube die Ländervorwahl („+49“) in der Anschlusskennung regelmäßig die Identifizierung einer rein inländischen Telekommunikation. Bei der paketvermittelten Übertragung im Internet (vgl. BTDrucks 18/12850, S. 713 ff.) könnten IP-Adressen mithilfe von kommerziell verfügbaren Geodatenbanken verortet werden. Diese Verortung sei zu 96 bis 98 % genau. 66

Die gezielte personenbezogene Überwachung ausländischer Personen im Ausland gemäß § 5 Abs. 2 Satz 3 in Verbindung mit Satz 2 Nr. 1 G 10 werde hinreichend begrenzt. Ein ausreichender Bezug zu dem jeweiligen Gefahrenbereich sei gewährleistet. Denn der Bundesnachrichtendienst dürfe auch bei der gezielt personenbezogenen Überwachung nur solche formalen Suchbegriffe verwenden, die zur Aufklärung von Sachverhalten über den in der Beschränkungsanordnung bezeichneten Gefahrenbereich bestimmt und geeignet seien. 67

Darüber hinaus werde der Kernbereich der privaten Lebensgestaltung ausreichend geschützt. Bei der Datenerhebung erfolge dies durch § 5 Abs. 2 Satz 2 Nr. 2 in Verbindung mit § 5a G 10. Danach dürften keine Suchbegriffe angeordnet werden, welche den Kernbereich der privaten Lebensgestaltung beträfen. Werde gleichwohl kernbereichsrelevante Kommunikation erfasst, enthalte das Gesetz in § 5a Sätze 2 bis 7 in Verbindung mit § 3a Abs. 1 Sätze 2 bis 7 G 10 die notwendigen Vorkehrungen zum Schutz des Kernbereichs bei der Datenauswertung. 68

Die Dokumentationspflichten in § 5 Abs. 2 Satz 6, § 5a Satz 7 und § 6 Abs. 1 Satz 5 G 10 gewährleisteten effektive Rechtsschutzmöglichkeiten und eine wirksame Kontrolle. Insbesondere unterbleibe die Löschung der Dokumentation am Ende des Kalenderjahres, das dem Jahr der Protokollierung folge, soweit die Daten für eine Benachrichtigung nach § 12 Abs. 2 G 10 oder für eine gerichtliche Überprüfung von Bedeutung sein könnten. 69

Auch die Beschränkung der Benachrichtigungspflicht in § 12 Abs. 1 Satz 2 in Verbindung mit Abs. 2 Satz 1 G 10 sei verfassungskonform. Nach Ablauf von zwölf Monaten müsse die G 10-Kommission einer weiteren Zurückstellung der Benachrichtigung zustimmen und über die Dauer der weiteren Zurückstellung entscheiden. Dies sichere eine ausgewogene Abwägung zwischen den Interessen der Allgemeinheit und denen der Betroffenen. 70

Schließlich unterliege die gesamte strategische Inland-Ausland-Fernmeldeaufklärung der wirksamen Kontrolle durch die G 10-Kommission. Die Kontrollbefugnis erstrecke sich auf die gesamte Prozesskette der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten. Die G 10-Kommission habe ein umfassendes Prüf- und Kontrollrecht, das sich nach § 15 Abs. 5 G 10 durch Frage-, Einsichts- und Zutrittsrechte verwirkliche. Zudem sei der G 10-Kommission gemäß § 15 Abs. 3 Satz 1 G 10 die für die Aufgabenerfüllung notwendige Sach- und Personalausstattung zur Verfügung zu stellen. 71

2. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat sich zu der gesetzlich vorgesehenen zweigeteilten datenschutzrechtlichen Kontrolle des Bundesnachrichtendienstes durch die G 10-Kommission einerseits und die Bundesbeauftragte andererseits geäußert. Insoweit sei bedenklich gewesen, dass nach § 24 Abs. 2 Satz 3 BDSG 2015 personenbezogene Daten, die der Kontrolle der G 10-Kommission unterlegen hätten, von der Bundesbeauftragten nicht hätten kontrolliert werden dürfen, es sei denn, die G 10-Kommission habe die Bundesbeauftragte darum ersucht. Diese Regelung sei fast wortgleich in § 26a Abs. 2 Satz 2 BVerfSchG 2018 übernommen worden. Allerdings habe der Gesetzgeber in der Gesetzesbegründung zu dieser Norm ausgeführt, dass die Bundesbeauftragte zur Erfüllung der ihr gesetzlich zugewiesenen Kontrollbefugnis auch Daten zur Kenntnis nehmen dürfe, die nach dem Artikel 10-Gesetz erhoben worden seien. 72

3. Für das Bundesverwaltungsgericht hat der für das Sicherheitsrecht zuständige 6. Revisionssenat mitgeteilt, mit den angegriffenen Vorschriften nur am Rande befasst gewesen zu sein. Dabei habe der Senat in einer Entscheidung die Löschungsregelungen der Protokolldaten am Ende des auf die Protokollierung folgenden Kalenderjahres in § 5 Abs. 2 Satz 6 und § 6 Abs. 1 Satz 5 G 10 für mit der Rechtsschutzgarantie des Art. 19 Abs. 4 Satz 1 GG vereinbar gehalten (unter Verweis auf BVerwGE 157, 8). 73

B.

I.

1. Beide Verfassungsbeschwerden richten sich unmittelbar gegen die im November 2015 neu in das Artikel 10-Gesetz eingefügte Befugnis des Bundesnachrichtendienstes zur strategischen Inland-Ausland-Fernmeldeüberwachung nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 im Bereich der Cybergefahren. Solche sind insbesondere Bedrohungen durch mögliche Angriffe mittels Schadprogrammen (etwa Virensoftware) oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von informationstechnischen Systemen und Netzen (also Gefahren von Cyberangriffen etwa in Gestalt von Cyberspionage oder Cybersabotage, vgl. BTDrucks 18/4654, S. 40 f.). 74

2. Darüber hinaus rügen die Verfassungsbeschwerden die Verfassungswidrigkeit verschiedener flankierender Regelungen zur verhältnismäßigen Ausgestaltung der Überwachungsbefugnis des § 5 Abs. 1 Satz 3 Nr. 8 G 10 (§ 5 Abs. 2 Satz 2 Nummern 1 und 2, Satz 3 i. V. m. Satz 2 Nummern 1 und 2, Satz 6, § 5a Satz 1, Sätze 2 bis 4, Satz 7, § 5b i. V. m. § 3b, § 6 Abs. 1 Satz 5, § 10 Abs. 4 Sätze 3 und 4, § 12 Abs. 2 Satz 1 i. V. m. Abs. 1 Satz 2, § 15 G 10 und § 15 Abs. 5 Satz 2 G 10 i. V. m. § 26a Abs. 2 Satz 2 BVerfSchG 2018). Diese können deshalb mittelbar Gegenstand verfassungsgerichtlicher Kontrolle sein (vgl. BVerfGE 155, 119 <157 Rn. 64> – Bestandsdatenauskunft II; 162, 1 <50 Rn. 90 und 64 f. Rn. 132> – Bayerisches Verfassungsschutzgesetz; 165, 1 <44 f. Rn. 75> – Polizeiliche Befugnisse nach SOG MV; stRspr). 75

3. Nicht mehr Gegenstand des Verfassungsbeschwerdeverfahrens 1 BvR 2539/16 sind die Ermächtigungen des Bundesnachrichtendienstes, die durch die strategische Inland-Ausland-Fernmeldeaufklärung gemäß § 5 Abs. 1 Satz 3 Nr. 8 G 10 gewonnenen Daten an andere Behörden zu übermitteln (§ 7 Absätze 2, 4, 4a und § 7a Abs. 1 Satz 1, Abs. 2 G 10 2015). Diese Übermittlungsbefugnisse sind durch Art. 2 des Gesetzes zur Änderung des BND-Gesetzes vom 22. Dezember 2023 (BGBl I Nr. 410) grundlegend geändert worden. Daraufhin haben die Beschwerdeführenden in dem Verfahren 1 BvR 2539/16 ihre Verfassungsbeschwerde insoweit wirksam für erledigt erklärt. Diese Teilerledigungserklärung lässt – im Rahmen ihrer Reichweite – die Grundlage für eine Entscheidung entfallen (vgl. BVerfGE 85, 109 <113>; 162, 1 <49 f. Rn. 88>; stRspr). 76

II.

Die Zuständigkeit des Bundesverfassungsgerichts für die Prüfung, ob die angegriffenen Normen mit den Grundrechten des Grundgesetzes vereinbar sind, ist gegeben, auch wenn die angegriffenen Vorschriften Bezüge zu datenschutzrechtlichen Bestimmungen in Rechtsakten der Europäischen Union aufweisen. Denn die datenschutzbezogenen 77

Rechtsakte der Europäischen Union sind auf die Befugnisse des Bundesnachrichtendienstes zur strategischen Inland-Ausland-Fernmeldeaufklärung gemäß Art. 4 Abs. 2 Satz 3 EUV nicht anwendbar. Danach fällt insbesondere die nationale Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten.

Der Gerichtshof der Europäischen Union hat bereits entschieden, dass das Ziel der Wahrung der nationalen Sicherheit dem zentralen Anliegen entspricht, die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft zu schützen. Umfasst sind die Verhütung und Repression von Tätigkeiten, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, wie insbesondere terroristische Aktivitäten (vgl. EuGH, Urteile vom 6. Oktober 2020, La Quadrature du Net u.a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 135 und Privacy International, C-623/17, EU:C:2020:790, Rn. 74; Urteil vom 5. April 2022, Commissioner of An Garda Síochána, C-140/20, EU:C:2022:258, Rn. 61; Urteil vom 20. September 2022, SpaceNet AG u.a., C-793/19 und C-794/19, EU:C:2022:702, Rn. 92; Urteil vom 23. März 2023, Generalstaatsanwaltschaft Bamberg, C-365/21, EU:C:2023:236, Rn. 55). 78

Die zentral angegriffene Ermächtigung des Bundesnachrichtendienstes zur strategischen Inland-Ausland-Fernmeldeaufklärung nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 dient der nationalen Sicherheit, nämlich der Früherkennung internationaler Cyberangriffe, die geeignet sind, die tragenden Strukturen der Bundesrepublik Deutschland im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen. 79

Vor diesem Hintergrund findet die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (JI-RL) nach ihrem Art. 2 Abs. 3 Buchstabe a im Licht ihres 14. Erwägungsgrunds keine Anwendung (vgl. EuGH, Urteil vom 30. Januar 2024, Direktor na Glavna direktsia „Nationala politsia“ pri MVR-Sofia, C-118/22, EU:C:2024:97, Rn. 38). Nach Art. 2 Abs. 3 Buchstabe a JI-RL ist diese Richtlinie nicht anwendbar auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt. Dies ist gemäß dem 14. Erwägungsgrund bei Tätigkeiten, welche die nationale Sicherheit betreffen, der Fall. 80

Gleiches gilt für die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) gemäß ihrem Art. 2 Abs. 2 Buchstabe a im Licht ihres 16. Erwägungsgrunds. 81

III.

Die Verfassungsbeschwerden sind teilweise zulässig, und zwar soweit der Beschwerdeführer im Verfahren 1 BvR 1743/16 und die Beschwerdeführenden zu 1) bis 4) im Verfahren 1 BvR 2539/16 geltend machen, dass die Ermächtigung zur strategischen Inland-Ausland-Fernmeldeaufklärung im Sachbereich Cybergefahren gemäß § 5 Abs. 1 Satz 3 Nr. 8 G 10 nicht angemessen sei, weil sie die Aussonderung von Daten aus der rein inländischen Telekommunikation unzureichend sicherstelle (Rn. 95 ff.). Zulässig sind die Verfassungsbeschwerden auch, soweit ein unzureichender Kernbereichsschutz bei der Datenerhebung für inländische Personen gemäß § 5 Abs. 2 Satz 2 Nr. 2 und § 5a Satz 1 G 10 vom Beschwerdeführer im Verfahren 1 BvR 1743/16 (Rn. 105) und für ausländische Personen im Ausland nach § 5 Abs. 2 Satz 3 in Verbindung mit Satz 2 Nr. 2 G 10 von der Beschwerdeführerin zu 5) im Verfahren 1 BvR 2539/16 gerügt wird (Rn. 106 f.). Die Verfassungsbeschwerden sind ebenfalls zulässig, soweit alle Beschwerdeführenden im Verfahren 1 BvR 2539/16 die Aufbewahrungsfrist für die Dokumentation der Durchführung der strategischen Inland-Ausland-Fernmeldeaufklärung nach § 5 Abs. 2 Satz 6 G 10 als zu kurz rügen (Rn. 108) und soweit der Beschwerdeführer im Verfahren 1 BvR 1743/16 geltend macht, die unabhängige objektivrechtliche Kontrolle sei unzureichend ausgestaltet (Rn. 109). 82

Hingegen sind beide Verfassungsbeschwerden unzulässig, soweit sich alle Beschwerdeführenden gegen eine unzureichende Begrenzung des Überwachungsvolumens durch § 10 Abs. 4 Sätze 3 und 4 G 10 wenden (Rn. 111 ff.). Die Verfassungsbeschwerde 1 BvR 1743/16 ist zudem unzulässig, soweit der Beschwerdeführer geltend macht, dass der Kernbereichsschutz bei der Datenauswertung gemäß § 5a Sätze 2 bis 4 in Verbindung mit § 3a Abs. 1 Sätze 2 bis 7 G 10 (Rn. 114) und der Schutz von Vertraulichkeitsbeziehungen durch § 5b in Verbindung mit § 3b G 10 unzureichend seien (Rn. 115). Die Verfassungsbeschwerde 1 BvR 2539/16 ist außerdem unzulässig, soweit die Beschwerdeführenden eine unzureichende Ausgestaltung der gezielt personenbezogenen Überwachung von Inländern gemäß § 5 Abs. 2 Satz 2 Nr. 1 G 10 (Rn. 116 f.) sowie von ausländischen Personen im Ausland nach § 5 Abs. 2 Satz 3 in Verbindung mit Satz 2 Nr. 1 G 10 (Rn. 118 f.), eine unzureichende Dokumentation der Löschung einerseits von kernbereichsrelevanten Kommunikationsinhalten nach § 5a Satz 7 G 10 (Rn. 120) und andererseits von erhobenen personenbezogenen Daten nach § 6 Abs. 1 Satz 5 G 10 (Rn. 121 ff.), unzureichende Benachrichtigungspflichten gemäß § 12 Abs. 1 Satz 2 in Verbindung mit Abs. 2 Satz 1 G 10 (Rn. 124) und eine unzureichende Kooperation der verschiedenen Instanzen der objektivrechtlichen Kontrolle nach § 15 Abs. 5 G 10 in Verbindung mit § 26a Abs. 2 Satz 2 BVerfSchG 2018 (Rn. 125) rügen. 83

1. Richtet sich eine Verfassungsbeschwerde wie vorliegend gegen ein Gesetz, das Sicherheitsbehörden zu heimlichen Maßnahmen ermächtigt, bestehen besondere Zulässigkeitsanforderungen bezüglich der Beschwerdebefugnis und der Subsidiarität der Verfassungsbeschwerde (vgl. BVerfGE 162, 1 <51 ff. Rn. 93 ff.>; 165, 1 <29 ff. Rn. 37 ff.>). 84

a) Die Zulässigkeit einer Verfassungsbeschwerde setzt nach Art. 93 Abs. 1 Nr. 4a GG, § 90 Abs. 1 BVerfGG die Behauptung voraus, durch einen Akt der öffentlichen Gewalt in Grundrechten oder grundrechtsgleichen Rechten verletzt zu sein (Beschwerdebefugnis; vgl. BVerfGE 140, 42 <54 Rn. 47>; 162, 1 <51 f. Rn. 93>). Dazu müssen sowohl die Möglichkeit der Grundrechtsverletzung (aa) als auch die eigene, unmittelbare und gegenwärtige Betroffenheit (bb) den Begründungsanforderungen nach § 23 Abs. 1 Satz 2, § 92 BVerfGG entsprechend dargelegt sein (vgl. BVerfGE 125, 39 <73>; 159, 355 <375 Rn. 25> – Bundesnotbremse II). 85

aa) Der die behauptete Rechtsverletzung enthaltende Vorgang muss substantiiert und schlüssig vorgetragen sein, und der Vortrag muss die Möglichkeit einer Grundrechtsverletzung hinreichend deutlich erkennen lassen (vgl. BVerfGE 130, 1 <21>; 140, 229 <232 Rn. 9>). Eine genaue Bezeichnung des Grundrechts, dessen Verletzung geltend gemacht wird, ist nicht erforderlich. Dem Vortrag muss sich aber entnehmen lassen, inwiefern sich die Beschwerdeführenden durch den angegriffenen Hoheitsakt in ihren Rechten verletzt sehen (vgl. BVerfGE 115, 166 <180>). Ist die Verfassungsbeschwerde gegen gesetzliche Vorschriften gerichtet, müssen sich die Beschwerdeführenden genau mit der angegriffenen Norm befassen. Sie müssen auch weitere Regelungen des Fachrechts in ihre Darlegungen einbeziehen, wenn diese Bedeutung für die Verfassungsmäßigkeit der angegriffenen Norm haben können. Dabei müssen sich die Beschwerdeführenden nicht nur mit der Auslegung und Anwendung des angegriffenen Gesetzes, sondern auch mit den Erwägungen des Gesetzgebers befassen (vgl. BVerfGE 162, 1 <67 Rn. 139>). Soweit sich eine Verfassungsbeschwerde unmittelbar oder mittelbar gegen ein Gesetz richtet, hat der Beschwerdeführende hinsichtlich jeder angegriffenen Norm konkret darzulegen, aus welchen Gründen die jeweilige Bestimmung gegen die als verletzt gerügten Grundrechte verstoßen soll (vgl. BVerfGE 102, 197 <210>; 122, 342 <359>). Anlass zur verfassungsgerichtlichen Überprüfung einer flankierenden Regelung zur verhältnismäßigen Ausgestaltung einer heimlichen Überwachungsmaßnahme besteht nur dann, wenn die verfassungsrechtliche Unzulänglichkeit dieser flankierenden Regelungen substantiiert dargelegt ist oder wenn sie auf der Hand liegt (vgl. BVerfGE 162, 1 <65 Rn. 132>; 165, 1 <44 f. Rn. 75>). Mit der verfassungsrechtlichen Beurteilung des vorgetragenen Sachverhalts müssen sich die Beschwerdeführenden im Einzelnen auseinandersetzen. Soweit das Bundesverfassungsgericht für bestimmte Fragen bereits verfassungsrechtliche Maßstäbe entwickelt hat, muss anhand dieser Maßstäbe aufgezeigt werden, inwieweit Grundrechte durch die angegriffene Maßnahme verletzt sein sollen 86

(vgl. BVerfGE 101, 331 <345 f.>; 159, 223 <270 Rn. 89> m.w.N. – Bundesnotbremse I; stRspr).

bb) Für die Darlegung der unmittelbaren sowie der eigenen und gegenwärtigen Betroffenheit gelten bei einer Verfassungsbeschwerde gegen eine gesetzliche Ermächtigung zu heimlichen Maßnahmen besondere Anforderungen (vgl. BVerfGE 162, 1 <52 f. Rn. 96>; 165, 1 <31 Rn. 41>). 87

(1) Zwar werden die hier angegriffenen Vorschriften erst auf der Grundlage weiterer Vollzugsakte in Form von Datenerhebung oder -weiterverarbeitung wirksam. Von einer unmittelbaren Betroffenheit durch ein vollziehungsbedürftiges Gesetz ist jedoch auch dann auszugehen, wenn Beschwerdeführende den Rechtsweg nicht beschreiten können, weil sie keine Kenntnis von der Maßnahme erlangen oder wenn eine nachträgliche Bekanntgabe zwar vorgesehen ist, von ihr aber aufgrund weitreichender Ausnahmetatbestände auch langfristig abgesehen werden kann (vgl. BVerfGE 155, 119 <159 Rn. 73>; 162, 1 <53 f. Rn. 99>). 88

(2) (a) Zur Begründung der Möglichkeit eigener und gegenwärtiger Betroffenheit durch eine gesetzliche Ermächtigung zu heimlichen Maßnahmen, bei der die konkrete Beeinträchtigung zwar erst durch eine Vollziehung erfolgt, die Betroffenen in der Regel aber keine Kenntnis von Vollzugsakten erlangen, reicht es aus, wenn die Beschwerdeführenden darlegen, mit einiger Wahrscheinlichkeit durch auf den angegriffenen Rechtsnormen beruhende Maßnahmen in eigenen Grundrechten berührt zu werden (vgl. BVerfGE 155, 119 <160 Rn. 75>). Ein Vortrag, für sicherheitsgefährdende Aktivitäten verantwortlich zu sein, ist zum Beleg der Selbstbetroffenheit grundsätzlich ebenso wenig erforderlich wie Darlegungen, durch die sich Beschwerdeführende selbst einer Straftat bezichtigen müssten (vgl. BVerfGE 130, 151 <176 f.>; stRspr). Für die Wahrscheinlichkeit eigener Betroffenheit spricht eine große Streubreite der Überwachungsmaßnahme, wenn die Maßnahme also nicht auf einen tatbestandlich eng umgrenzten Personenkreis zielt, insbesondere, wenn sie auch Dritte in großer Zahl zufällig erfassen kann (BVerfGE 162, 1 <53 Rn. 98>). In besonderen Fällen müssen die Beschwerdeführenden darüber hinaus nähere Aussagen zu Art und Gegenstand der möglicherweise überwachbaren Techniken und Dienste sowie dem eigenen Nutzungsverhalten treffen. Dies ist erforderlich, wenn sonst nicht ohne weiteres erkennbar ist, ob bei der Nutzung überhaupt Daten anfallen, die in den Fokus sicherheitsrechtlicher Behördenaktivitäten geraten könnten (BVerfGE 162, 1 <53 Rn. 98> m.w.N.). 89

(b) Wenn eine gesetzliche Befugnisnorm zu verschiedenen Maßnahmen ermächtigt, die jeweils eigenständige Grundrechtseingriffe darstellen, ist die Betroffenheit für jede dieser Maßnahmen gesondert zu prüfen. Beschwerdeführende müssen für alle Maßnahmen, gegen die sie sich wenden, gesondert darlegen, mit einiger Wahrscheinlichkeit in eigenen Grundrechten berührt zu werden (vgl. BVerfGE 155, 119 <160 Rn. 75>; 162, 1 <53 Rn. 97>; 90

165, 1 <31 Rn. 43>). Denn die Verfassungsmäßigkeit einer Ermächtigungsgrundlage ist grundsätzlich nur rügebezogen zu überprüfen (vgl. BVerfGE 162, 1 <64 f. Rn. 132>; 165, 1 <44 f. Rn. 75>).

(3) Besonderheiten bei der Betroffenheit bestehen im Hinblick auf die flankierenden Vorschriften zur verhältnismäßigen Ausgestaltung und Begrenzung heimlicher Überwachungsbefugnisse. Diese flankierenden Vorschriften bilden im Verfassungsbeschwerdeverfahren grundsätzlich keinen eigenen Verfahrensgegenstand, sondern sind im Rahmen der Überprüfung der Eingriffsermächtigung mittelbar Gegenstand verfassungsgerichtlicher Kontrolle (vgl. BVerfGE 162, 1 <65 Rn. 132>). Die unzureichende Ausgestaltung und Begrenzung der Überwachungsbefugnis durch diese flankierenden Vorschriften führt zu einer Grundrechtsverletzung in Gestalt der Unangemessenheit dieser Befugnis, stellt aber keinen davon unabhängigen Grundrechtseingriff dar. Vor diesem Hintergrund ist bei der Betroffenheit durch diese flankierenden Vorschriften zu prüfen, ob die Beschwerdeführenden in einer Art und Weise von der Überwachungsbefugnis betroffen sind, die zur Wahrung der Verhältnismäßigkeit eine gesetzliche Ausgestaltung und Begrenzung durch flankierende Vorschriften erforderlich macht. Die Betroffenheit durch die Überwachungsbefugnis indiziert regelmäßig die Betroffenheit durch die flankierenden Vorschriften zur Ausgestaltung und Begrenzung dieser Befugnis. Die Betroffenheit durch die flankierenden Vorschriften ist nur dort gesondert zu prüfen, wo die gesetzliche Ausgestaltung und Begrenzung der Befugnisnorm nur für eine bestimmte Gruppe der von ihr Betroffenen erforderlich ist. 91

b) Besondere Zulässigkeitsanforderungen ergeben sich auch aus der Subsidiarität der Verfassungsbeschwerde. Zwar steht unmittelbar gegen Parlamentsgesetze kein ordentlicher Rechtsweg im Sinne des § 90 Abs. 2 BVerfGG zur Verfügung, der vor Erhebung der Verfassungsbeschwerde erschöpft werden muss. Die Verfassungsbeschwerde muss aber auch den Anforderungen der Subsidiarität im weiteren Sinne genügen. Diese beschränken sich nicht darauf, die zur Erreichung des unmittelbaren Prozessziels förmlich eröffneten Rechtsmittel zu ergreifen, sondern verlangen, alle Mittel zu nutzen, die der geltend gemachten Grundrechtsverletzung abhelfen können. Damit soll auch erreicht werden, dass das Bundesverfassungsgericht nicht auf ungesicherter Tatsachen- und Rechtsgrundlage weitreichende Entscheidungen treffen muss, sondern zunächst die für die Auslegung und Anwendung des einfachen Rechts primär zuständigen Fachgerichte die Sach- und Rechtslage aufgearbeitet haben. Der Grundsatz der Subsidiarität erfordert deshalb grundsätzlich, vor Einlegung einer Verfassungsbeschwerde alle zur Verfügung stehenden prozessualen Möglichkeiten zu ergreifen, um eine Korrektur der geltend gemachten Verfassungsverletzung zu erwirken oder eine Grundrechtsverletzung zu verhindern. Das gilt auch, wenn zweifelhaft ist, ob ein entsprechender Rechtsbehelf statthaft ist und im konkreten Fall in zulässiger Weise eingelegt werden kann (vgl. zum Ganzen BVerfGE 162, 1 <54 Rn. 100>; 165, 1 <32 f. Rn. 45>; BVerfG, Beschluss des Ersten Senats vom 17. Juli 2024 - 1 BvR 2133/22 -, Rn. 40 – Hessisches Verfassungsschutzgesetz; stRspr). 92

c) Die Verfassungsbeschwerde genügt diesen Anforderungen teilweise. Die Beschwerdeführenden haben ihre Beschwerdebefugnis in Teilen hinreichend substantiiert dargelegt (aa), und der Grundsatz der Subsidiarität steht der Zulässigkeit der Verfassungsbeschwerden nicht entgegen (bb). 93

aa) (1) Soweit die Verfassungsbeschwerden geltend machen, dass die Ermächtigung zur strategischen Inland-Ausland-Fernmeldeaufklärung gemäß § 5 Abs. 1 Satz 3 Nr. 8 G 10 nicht angemessen sei, weil sie vom Gesetzgeber unzureichend strukturiert und begrenzt werde, sind beschwerdebefugt im Hinblick auf eine unzureichende Aussonderung von Daten aus der rein inländischen Telekommunikation der Beschwerdeführer im Verfahren 1 BvR 1743/16 und die Beschwerdeführenden zu 1) bis 4) im Verfahren 1 BvR 2539/16 (a). Mit Blick auf die Rüge eines unzureichenden Kernbereichsschutzes für inländische Personen gemäß § 5 Abs. 2 Satz 2 Nr. 2 und § 5a Satz 1 G 10 bei der Datenerhebung ist der Beschwerdeführer im Verfahren 1 BvR 1743/16 (b) und mit Blick auf die Rüge eines solchen für ausländische Personen im Ausland nach § 5 Abs. 2 Satz 3 in Verbindung mit Satz 2 Nr. 2 G 10 ist die Beschwerdeführerin zu 5) im Verfahren 1 BvR 2539/16 beschwerdebefugt (c). In Bezug auf die Rüge einer zu kurzen Aufbewahrungsfrist für die Dokumentation der Durchführung der strategischen Inland-Ausland-Fernmeldeaufklärung nach § 5 Abs. 2 Satz 6 G 10 ist die Beschwerdebefugnis für alle Beschwerdeführenden im Verfahren 1 BvR 2539/16 (d) und in Bezug auf die Rüge einer unzureichenden Ausgestaltung der unabhängigen objektivrechtlichen Kontrolle für den Beschwerdeführer im Verfahren 1 BvR 1743/16 gegeben (e). 94

(a) Der Beschwerdeführer im Verfahren 1 BvR 1743/16 und die Beschwerdeführenden zu 1) bis 4) im Verfahren 1 BvR 2539/16 sind beschwerdebefugt, soweit sie sich gegen die Erfassung von Daten aus der rein inländischen Telekommunikation wenden. 95

Insoweit besteht die Möglichkeit einer Grundrechtsverletzung (aa). Ihre Betroffenheit durch Maßnahmen nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 haben der Beschwerdeführer im Verfahren 1 BvR 1743/16 und im Verfahren 1 BvR 2539/16 die Beschwerdeführenden zu 1) und 5) in vollem Umfang sowie die Beschwerdeführenden zu 2) bis 4) und 6) nur bezogen auf die Erfassung der Rohdatenströme ihrer Telekommunikationsverkehre – nicht aber bezüglich der weiteren nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 zulässigen Eingriffe – hinreichend dargelegt (bb). Nur der Beschwerdeführer im Verfahren 1 BvR 1743/16 und die Beschwerdeführenden zu 1) bis 4) im Verfahren 1 BvR 2539/16 sind als deutsche Staatsangehörige beziehungsweise deutsche juristische Personen von dem Fehlen einer Regelung zur Aussonderung von Daten aus der rein inländischen Kommunikation betroffen (cc). 96

(aa) Die Möglichkeit einer Grundrechtsverletzung dadurch, dass eine gesetzliche Regelung zur Aussonderung von im Rahmen der strategischen Inland-Ausland-Fernmeldeaufklärung zunächst miterfassten Daten aus der rein inländischen Telekommunikation fehlt, ist hinreichend dargelegt. Die strategische Überwachung kann aufgrund ihrer Anlasslosigkeit nur als Instrument der Auslandsaufklärung gerechtfertigt werden (vgl. BVerfGE 100, 313 <389 f.>). Deshalb bedarf es – wie bei der strategischen Ausland-Ausland-Fernmeldeaufklärung – zu ihrer verhältnismäßigen Ausgestaltung und Begrenzung einer normenklaren, strikt am technisch Möglichen ausgerichteten Regelung zur Aussonderung von Daten aus der reinen Inlandskommunikation, einschließlich von Vorgaben zur dabei zu verwendenden Filtertechnik (vgl. dazu auch BVerfGE 154, 152 <251 f. Rn. 170 ff.>). 97

(bb) Alle Beschwerdeführenden sind von Maßnahmen nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 im verfassungsprozessrechtlichen Sinne unmittelbar betroffen. Die Vorschrift ermöglicht heimliche Überwachungsmaßnahmen, und die vorgesehenen Benachrichtigungspflichten wirken dieser Heimlichkeit nur teilweise entgegen. Denn § 12 Abs. 2 Satz 1 in Verbindung mit Abs. 1 Satz 2 G 10 schränkt die Mitteilungspflicht ein oder lässt sie völlig entfallen. 98

Die eigene und gegenwärtige Betroffenheit durch § 5 Abs. 1 Satz 3 Nr. 8 G 10 haben der Beschwerdeführer im Verfahren 1 BvR 1743/16 sowie im Verfahren 1 BvR 2539/16 die Beschwerdeführenden zu 1) und 5) in vollem Umfang und die Beschwerdeführenden zu 2) bis 4) und 6) nur bezogen auf die Erfassung der Rohdatenströme ihrer Telekommunikationsverkehre – nicht aber bezüglich der weiteren nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 zulässigen Eingriffe – hinreichend dargelegt. 99

§ 5 Abs. 1 Satz 3 Nr. 8 G 10 ermächtigt den Bundesnachrichtendienst zu mehreren selbstständigen Grundrechtseingriffen, nämlich zur Erfassung und Speicherung von Telekommunikationsrohdatenströmen aus Übertragungswegen, zur Auswertung dieser Rohdaten durch den automatisierten Abgleich mit Suchbegriffen, zur händischen Auswertung der herausgefilterten Daten sowie zur weiteren eigenen Verwendung der als nachrichtendienstlich relevant eingestuften Daten (ausführlich unten Rn. 139 ff.). Für jeden einzelnen dieser Eingriffe aufgrund des § 5 Abs. 1 Satz 3 Nr. 8 G 10 haben die Beschwerdeführenden ihre eigene und gegenwärtige Betroffenheit darzulegen. 100

Angesichts der großen Streubreite der anlasslosen und heimlichen strategischen Fernmeldeüberwachung und der ebenfalls im Verborgenen stattfindenden Folgemaßnahmen sind an den Vortrag zur eigenen Betroffenheit keine hohen Anforderungen zu stellen. Darzulegen sind lediglich die äußeren Umstände, mögliche Gesprächspartner und Gesprächsthemen, an denen der Bundesnachrichtendienst angesichts seiner Aufgaben naheliegenderweise ein erhebliches Interesse haben könnte (vgl. BVerfGE 100, 313 <355 f.>; 154, 152 <210 f. Rn. 74>). 101

Der Beschwerdeführer im Verfahren 1 BvR 1743/16 und die Beschwerdeführenden zu 1) und 5) im Verfahren 1 BvR 2539/16 machen hinreichend substantiiert geltend, mit einiger Wahrscheinlichkeit von allen Maßnahmen der Datenerhebung und weiteren Datenverarbeitung nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 selbst betroffen zu sein. Sie führen nachvollziehbar aus, regelmäßig von Deutschland ins Ausland (Beschwerdeführer im Verfahren 1 BvR 1743/16 und Beschwerdeführer zu 1) im Verfahren 1 BvR 2539/16) beziehungsweise vom Ausland nach Deutschland (Beschwerdeführerin zu 5) im Verfahren 1 BvR 2539/16) auch mit Bezug zu Cybergefahren zu kommunizieren. Damit legen sie dar, dass ihre Telekommunikation beim Abgleich mit Suchbegriffen als Treffer erfasst werden könnte. 102

Die Beschwerdeführenden zu 2) bis 4) und 6) im Verfahren 1 BvR 2539/16 legen lediglich hinreichend dar, durch die Erfassung und Speicherung von Telekommunikationsrohdatenströmen gemäß § 5 Abs. 1 Satz 3 Nr. 8 G 10 selbst und gegenwärtig betroffen zu sein. Denn sie tragen nur dazu vor, dass sie grenzüberschreitend von beziehungsweise nach Deutschland kommunizieren. Dass ihre Telekommunikation einen Bezug zu dem Aufklärungszweck der Cybergefahren haben und deshalb mit einiger Wahrscheinlichkeit beim Abgleich mit Suchbegriffen aufgrund von § 5 Abs. 1 Satz 3 Nr. 8 G 10 als Treffer erhoben und zur weiteren Verarbeitung gespeichert werden könnte, machen die Beschwerdeführenden zu 2) bis 4) und 6) im Verfahren 1 BvR 2539/16 hingegen nicht geltend. 103

(cc) Von dem Fehlen einer Regelung zur Aussonderung von Daten aus der rein inländischen Kommunikation können nur der Beschwerdeführer im Verfahren 1 BvR 1743/16 und die Beschwerdeführenden zu 1) bis 4) im Verfahren 1 BvR 2539/16 als deutsche Staatsangehörige beziehungsweise deutsche juristische Person betroffen sein, nicht hingegen die Beschwerdeführenden zu 5) und 6) im Verfahren 1 BvR 2539/16 als ausländische Staatsangehörige im Ausland. 104

(b) Der Beschwerdeführer im Verfahren 1 BvR 1743/16 ist darüber hinaus beschwerdebefugt, soweit er rügt, dass der Kernbereichsschutz bei der strategischen Inland-Ausland-Fernmeldeaufklärung gemäß § 5 Abs. 2 Satz 2 Nr. 2 und § 5a Satz 1 G 10 für deutsche Staatsangehörige und inländische Personen auf der Ebene der Datenerfassung nicht ausreichend ausgestaltet sei. Er macht nachvollziehbar geltend, dass weder Filter noch andere Schutzmechanismen gesetzlich vorgesehen seien, um einen effektiven Kernbereichsschutz sicherzustellen. Als deutscher Staatsangehöriger ist er auch von dem als unzureichend gerügten Kernbereichsschutz nach § 5 Abs. 2 Satz 2 Nr. 2 und § 5a Satz 1 G 10 betroffen. 105

(c) Die Beschwerdeführerin zu 5) im Verfahren 1 BvR 2539/16 ist zudem beschwerdebefugt, soweit sie geltend macht, dass § 5 Abs. 2 Satz 3 G 10 – als Ausnahme zu § 5 Abs. 2 Satz 2 Nr. 2 G 10 – in Bezug auf ausländische Personen im Ausland die Verwendung von Suchbegriffen zulassen könnte, die den Kernbereich der privaten Lebensgestaltung betreffen. Insoweit besteht die Möglichkeit einer 106

Grundrechtsverletzung, weil der verfassungsrechtliche Kernbereichsschutz auch gegenüber ausländischen Personen im Ausland gilt.

Von § 5 Abs. 2 Satz 3 in Verbindung mit Satz 2 Nr. 2 G 10 betroffen ist aber nur die Beschwerdeführerin zu 5) im Verfahren 1 BvR 2539/16. Die Beschwerdeführenden zu 1) bis 4) können als deutsche Staatsangehörige beziehungsweise inländische juristische Person von dieser Regelung nicht betroffen sein. Auch der Beschwerdeführer zu 6) hat seine Betroffenheit nicht hinreichend dargelegt. Denn § 5 Abs. 2 Satz 3 in Verbindung mit Satz 2 Nr. 2 G 10 bezieht sich als flankierende Regelung zur verhältnismäßigen Ausgestaltung und Begrenzung der Ermächtigung des § 5 Abs. 1 Satz 3 Nr. 8 G 10 nur auf den Einsatz von Suchbegriffen, nicht auf die Erfassung der Telekommunikationsrohdaten. Dass ihre grenzüberschreitende Telekommunikation nach Deutschland einen sachlichen Bezug zum Aufklärungszweck der Cybergefahren hat und dass ihre Telekommunikationsverkehre bei dem Abgleich mit Suchbegriffen als Treffer erhoben werden könnten, macht lediglich die Beschwerdeführerin zu 5) nachvollziehbar geltend, nicht aber der Beschwerdeführer zu 6) (vgl. oben Rn. 103). 107

(d) Die Beschwerdeführenden im Verfahren 1 BvR 2539/16 legen des Weiteren hinreichend dar, dass die Frist zur Löschung der Dokumentation der Durchführung der strategischen Inland-Ausland-Fernmeldeaufklärung in § 5 Abs. 2 Satz 6 G 10 zu kurz bemessen sein könnte. Denn eine Aufbewahrungsfrist nur bis zum Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, könnte zu kurz sein, um auf der Grundlage der Dokumentation effektiven subjektiven Rechtsschutz zu ermöglichen und könnte deshalb Art. 10 Abs. 1 und Art. 19 Abs. 4 GG verletzen (vgl. dazu BVerfGE 141, 220 <302 f. Rn. 205, 309 Rn. 226, 315 f. Rn. 246 und 323 Rn. 272>). 108

(e) Schließlich legt der Beschwerdeführer im Verfahren 1 BvR 1743/16 hinreichend dar, dass die unabhängige objektive Rechtskontrolle in Bezug auf die strategische Inland-Ausland-Fernmeldeaufklärung durch die G 10-Kommission gemäß § 15 G 10 insgesamt nicht ausreichend effektiv sein könnte, um zu kompensieren, dass der subjektive Rechtsschutz gegen die strategische Fernmeldeüberwachung nur in erheblichem Maße eingeschränkt zur Verfügung steht. 109

(2) Die Beschwerdeführenden in beiden Verfassungsbeschwerden sind hingegen nicht beschwerdebefugt, soweit sie sich gegen eine unzureichende Begrenzung des Überwachungsvolumens durch § 10 Abs. 4 Sätze 3 und 4 G 10 wenden (a). Der Beschwerdeführer im Verfahren 1 BvR 1743/16 ist zudem nicht beschwerdebefugt, soweit er geltend macht, dass der Kernbereichsschutz bei der Datenauswertung gemäß § 5a Sätze 2 bis 4 in Verbindung mit § 3a Abs. 1 Sätze 2 bis 7 G 10 (b) und der Schutz von Vertraulichkeitsbeziehungen durch § 5b in Verbindung mit § 3b G 10 (c) unzureichend seien. Die Beschwerdeführenden im Verfahren 1 BvR 2539/16 sind außerdem nicht beschwerdebefugt, soweit sie rügen, die 110

gezielt personenbezogene Überwachung von inländischen Personen gemäß § 5 Abs. 2 Satz 2 Nr. 1 G 10 (d) sowie von ausländischen Personen im Ausland nach § 5 Abs. 2 Satz 3 in Verbindung mit Satz 2 Nr. 1 G 10 (e) seien unzureichend ausgestaltet, die Aufbewahrungsfristen bei der Dokumentation nach § 5a Satz 7 G 10 (f) und gemäß § 6 Abs. 1 Satz 5 G 10 (g) seien zu kurz, die Ausnahmen von der Benachrichtigungspflicht gemäß § 12 Abs. 1 Satz 2 in Verbindung mit Abs. 2 Satz 1 G 10 seien zu weitgehend (h) und die Kooperation der Kontrollorgane bei der objektiven Rechtskontrolle gemäß § 15 Abs. 5 G 10 und § 26a Abs. 2 Satz 2 BVerfSchG 2018 sei unzureichend (i).

(a) Alle Beschwerdeführenden haben nicht hinreichend dargelegt, dass die Begrenzung des Überwachungsvolumens in § 10 Abs. 4 Sätze 3 und 4 G 10 verfassungsrechtlich ungenügend sein könnte. 111

Der Beschwerdeführer im Verfahren 1 BvR 1743/16 setzt sich nicht damit auseinander, dass das Bundesverwaltungsgericht die Begrenzung des Überwachungsvolumens in § 10 Abs. 4 Sätze 3 und 4 G 10 für ausreichend gehalten hat, weil der Bundesnachrichtendienst nicht alle Übertragungswege überwachen dürfe, deren Überwachung angeordnet wurde, sondern insoweit eine Auswahl treffen müsse (vgl. BVerwGE 149, 359 <367 Rn. 29>). 112

Auch die Rüge der Beschwerdeführenden im Verfahren 1 BvR 2539/16 genügt nicht den Darlegungsanforderungen. Soweit sie beanstanden, durch § 10 Abs. 4 Sätze 3 und 4 G 10 werde ein Anreiz gesetzt, in die Beschränkungsanordnung möglichst viele Übertragungswege aufzunehmen, um eine möglichst hohe Übertragungsgesamtkapazität zu erreichen, nach der sich dann die Obergrenze der Überwachung bemesse, setzen sie sich nicht damit auseinander, dass und weshalb eine solche Anwendungspraxis in Bezug auf § 10 Abs. 4 Sätze 3 und 4 G 10 trotz der verfassungsrechtlich gebotenen umfassenden, effektiven und unabhängigen objektivrechtlichen Kontrolle (ausführlich dazu unten Rn. 170 ff.) möglich sein könnte. Soweit die Beschwerdeführenden geltend machen, im Artikel 10-Gesetz fehle eine Gesamtbetrachtung aller Überwachungsanordnungen, so dass der Bundesnachrichtendienst durch unterschiedliche Anordnungen in den verschiedenen Gefahrenbereichen des § 5 Abs. 1 Satz 3 Nummern 1 bis 8 G 10 einen erheblich über der Obergrenze von 20 % liegenden Anteil der internationalen Telekommunikation überwachen könne, legen die Beschwerdeführenden nicht hinreichend substantiiert dar, dass und weshalb eine solche Gesamtbetrachtung verfassungsrechtlich geboten sein sollte. 113

(b) Nicht hinreichend dargelegt ist zudem die Rüge des Beschwerdeführers im Verfahren 1 BvR 1743/16, der Kernbereichsschutz gemäß § 5a in Verbindung mit § 3a G 10 für deutsche Staatsangehörige und inländische Personen bei der Datenauswertung sei unzureichend, weil die erfassten Daten nicht durch eine unabhängige Stelle auf ihre Kernbereichsrelevanz hin gesichtet würden. Der Beschwerdeführer setzt sich nicht damit auseinander, dass nach § 5a Satz 4 in Verbindung mit § 3a Abs. 1 Sätze 2 bis 7 G 10 (bis Juli 114

2021: § 3a Sätze 2 bis 7 G 10 2015) dem Kernbereichsschutz bei der Auswertung der erfassten Daten Rechnung getragen wird. Danach sind die automatisch aufgezeichneten Daten in Fällen, in denen möglicherweise eine Kernbereichsrelevanz besteht, von einer vom Bundesnachrichtendienst unabhängigen Stelle, nämlich von einem Mitglied der G 10-Kommission, das verbindlich über die Löschung oder Verwertung der Daten entscheidet, zu sichten.

(c) Der Beschwerdeführer im Verfahren 1 BvR 1743/16 legt nicht hinreichend substantiiert dar, dass der Schutz von Vertraulichkeitsbeziehungen durch den im Dezember 2023 neu geschaffenen § 5b G 10 unzureichend sein könnte. Soweit der Beschwerdeführer rügt, § 5b G 10 sei zu unbestimmt und nicht normenklar, denn durch den Verweis auf § 3b G 10 entstehe eine mehrgliedrige unübersichtliche Verweisungskette, setzt er sich nicht damit auseinander, dass die Normenklarheit nach der Rechtsprechung des Bundesverfassungsgerichts der Verwendung von Verweisungsketten nicht grundsätzlich entgegensteht. Denn Verweisungen entlasten den Normtext, beugen unterschiedlichen Regelungen inhaltlich vergleichbarer Fragen vor und können verhindern, dass Gesetze zu lang und wiederum unverständlich würden (vgl. BVerfGE 163, 43 <84 f. Rn. 113>). 115

(d) Nicht hinreichend substantiiert dargelegt ist die Rüge der Beschwerdeführenden im Verfahren 1 BvR 2539/16, § 5 Abs. 2 Satz 2 Nr. 1 G 10 schließe die Möglichkeit einer gezielten Überwachung deutscher Staatsangehöriger und Inländer durch formale Suchbegriffe nicht – wie aufgrund von Art. 10 Abs. 1 GG geboten – umfassend aus. Die Beschwerdeführenden machen dazu im Wesentlichen geltend, § 5 Abs. 2 Satz 2 Nr. 1 G 10 verbiete nur die gezielte Erfassung bestimmter „Telekommunikationsanschlüsse“, und dieser Begriff beziehe sich nach § 2 Nr. 10 TKÜV in Verbindung mit dem Begriff der „Telekommunikationsanlagen“ in § 3 Nr. 23 TKG 2004 nur auf die technische Schicht der Signalübertragung (wie die Kennung eines Internetanschlusses), nicht aber auf die Dienstschicht, die auf der Signalübertragung aufsetze (wie E-Mail-Adressen). Teilnehmerkennungen auf der Dienstschicht dürften deshalb gemäß § 5 Abs. 2 Satz 2 G 10 unbeschränkt als formale Suchbegriffe genutzt werden (vgl. oben Rn. 52). Dabei bezieht sich der Begriff der „Schicht“ auf die verschiedenen Ebenen von Kommunikationsabläufen in Computernetzen wie dem Internet. Um den Austausch von Daten in einem solchen Netz zu ermöglichen, müssen auf jeder der verschiedenen Schichten der Kommunikation auf der Seite sowohl des Senders als auch des Empfängers festgelegte Regeln (Protokolle) eingehalten werden. 116

Diese Rüge ist nicht hinreichend substantiiert begründet. Es ist keineswegs zwingend, den Begriff des Telekommunikationsanschlusses in § 5 Abs. 2 Satz 2 Nr. 1 G 10 über Bezugnahmen auf § 2 Nr. 10 TKÜV und § 3 Nr. 23 TKG 2004 zu bestimmen. Denn das Artikel 10-Gesetz hat andere und breitere Schutzzwecke als diese Regelungen, bei denen es vor allem um Abgrenzungen in technischer Hinsicht geht. Warum die von § 5 Abs. 2 G 10 bezweckte, im Ausgangspunkt auf Suchbegriffe abstellende Beschränkung der 117

Überwachungsmöglichkeiten mit den Telekommunikationsanschlüssen nur technische Einrichtungen auf der Ebene der Signalübertragung in Bezug nehmen soll, nicht aber etwa auch andere Kommunikationsendpunkte wie E-Mail-Dienste erfasst, wäre angesichts der unterschiedlichen Regelungszwecke näher darzulegen gewesen.

(e) Die Beschwerdeführenden im Verfahren 1 BvR 2539/16 rügen ebenfalls nicht hinreichend substantiiert, dass die Befugnis zur gezielt personenbezogenen Überwachung ausländischer Personen im Ausland durch § 5 Abs. 2 Satz 3 in Verbindung mit Satz 2 Nr. 1 G 10 unzureichend strukturiert und begrenzt werde. Die Beschwerdeführenden setzen sich insoweit nicht hinreichend damit auseinander, dass auch die gezielt personenbezogene Überwachung ausländischer Personen im Ausland nach § 5 Abs. 1 Satz 3 G 10 nicht voraussetzungslos zulässig ist, sondern nur, wenn der Bundesnachrichtendienst in seinem Antrag nach § 9 G 10 schlüssig dargelegt hat, dass diese gezielte Überwachung rechtzeitig Aufschluss über eine der relevanten Gefahren (vgl. § 5 Abs. 1 Satz 3 Nummern 1 bis 8 G 10) geben könnte (vgl. BVerfGE 100, 313 <384>). Die Beschwerdeführenden gehen außerdem nicht darauf ein, dass auch die Anordnung der gezielt personenbezogenen Überwachung – wie die gesamte strategische Inland-Ausland-Fernmeldeaufklärung – einer umfassenden, effektiven und unabhängigen objektivrechtlichen Kontrolle unterliegt, in der auch der bestehende Gefahrenbezug überprüft wird. 118

Soweit die Beschwerdeführenden geltend machen, § 5 Abs. 2 Satz 3 in Verbindung mit Satz 2 Nr. 1 G 10 verletze den Gleichheitsgrundsatz (Art. 3 Abs. 1 GG), setzen sie sich nicht damit auseinander, dass der Umfang und die Reichweite des grundrechtlichen Schutzes von ausländischen Staatsangehörigen im Ausland einerseits und deutschen Staatsangehörigen und Inländern andererseits nicht identisch sein müssen (vgl. BVerfGE 154, 152 <224 Rn. 104>). 119

(f) Nicht hinreichend begründet ist auch die Rüge der Beschwerdeführenden im Verfahren 1 BvR 2539/16, die Frist gemäß § 5a Satz 7 G 10 in der Fassung vom 31. Juli 2009 (BGBl I S. 2499), nach der die Protokolldaten zur Löschung kernbereichsrelevanter Daten spätestens am Ende des dem Jahr der Protokollierung folgenden Kalenderjahres zu löschen waren, ermögliche keinen ausreichend effektiven Rechtsschutz. Die Beschwerdeführenden setzen sich nicht mit der Änderung des § 5a Satz 7 G 10 durch das Gesetz zur Anpassung des Verfassungsschutzrechts vom 5. Juli 2021 (BGBl I S. 2274) auseinander. Seit dieser Änderung sind die Protokolldaten sechs Monate nach der Benachrichtigung oder der Feststellung des endgültigen Unterbleibens der Benachrichtigung nach § 12 Abs. 2 G 10 zu löschen. Dass und weshalb die Löschungsfrist dennoch unzureichend sein könnte, legen die Beschwerdeführenden nicht dar. 120

(g) Nicht hinreichend substantiiert dargetan ist auch die Rüge der Beschwerdeführenden im Verfahren 1 BvR 2539/16, die Aufbewahrungsfrist in § 6 Abs. 1 Satz 5 G 10 für die Protokollierung der Löschung von personenbezogenen Daten verletze Art. 10 Abs. 1 und Art. 19 Abs. 4 GG. 121

Soweit die Beschwerdeführenden hierzu geltend machen, die Aufbewahrungsfrist des § 6 Abs. 1 Satz 5 G 10 – Löschung der Protokolldaten am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt – sei zu kurz bemessen, um eine effektive objektive Rechtskontrolle zu gewährleisten, setzen sie sich nicht damit auseinander, dass die G 10-Kommission zur Durchführung der objektiven Rechtskontrolle mindestens einmal im Monat zusammentritt (vgl. § 15 Abs. 4 Satz 1 G 10). Dass und weshalb die objektive Rechtskontrolle durch die Frist zur Löschung der Protokolldaten trotz dieser sehr regelmäßig stattfindenden Kontrolle beeinträchtigt werden könnte, legen die Beschwerdeführenden nicht dar. 122

Soweit die Beschwerdeführenden rügen, diese Löschungsfrist sei zu kurz, um effektiven subjektiven Rechtsschutz zu ermöglichen, setzen sie sich nicht mit § 6 Abs. 1 Satz 6 G 10 auseinander. Insbesondere setzen sie sich nicht mit dem möglichen Normverständnis auseinander, dass die Löschung auch von Protokolldaten unterbleibt, soweit die Daten für eine Benachrichtigung nach § 12 Abs. 2 G 10 oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Beschränkungsmaßnahme von Bedeutung sein können. 123

(h) Die Beschwerdeführenden im Verfahren 1 BvR 2539/16 rügen nicht hinreichend substantiiert, dass § 12 Abs. 2 Satz 1 in Verbindung mit Abs. 1 Satz 2 G 10 zu weitgehende Ausnahmen von der Benachrichtigungspflicht enthalte. Die Beschwerdeführenden setzen sich insoweit nicht hinreichend damit auseinander, dass über Ausnahmen von der Benachrichtigungspflicht gemäß § 12 Abs. 2 Satz 1 in Verbindung mit Abs. 1 Satz 5 G 10 abschließend nicht der Bundesnachrichtendienst, sondern die unabhängige G 10-Kommission entscheidet. Dass und weshalb es der G 10-Kommission bei dieser Entscheidung nicht möglich sein sollte, eine gegebenenfalls erforderliche enge Auslegung der Beschränkung der Benachrichtigungspflicht (vgl. BVerfGE 162, 1 <66 Rn. 136>) vorzunehmen, legen die Beschwerdeführenden nicht dar. 124

(i) Nicht hinreichend dargetan ist schließlich die Rüge der Beschwerdeführenden im Verfahren 1 BvR 2539/16, die Kontrolle der strategischen Inland-Ausland-Fernmeldeaufklärung nach § 15 Abs. 5 G 10 und § 26a Abs. 2 Satz 2 BVerfSchG 2018 (zuvor § 24 Abs. 2 Satz 3 BDSG 2015) sei nicht ausreichend effektiv. Die Beschwerdeführenden rügen insoweit, dass die Kooperation der beiden Kontrollorgane unzureichend sei, weil nach § 24 Abs. 2 Satz 3 BDSG 2015 und § 26a Abs. 2 Satz 2 BVerfSchG 2018 die Einhaltung von Vorschriften, die der Kontrolle durch die G 10-Kommission unterliege, nicht der Kontrolle durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit unterstehe. Diese Rüge ist nicht hinreichend substantiiert, denn die Beschwerdeführenden setzen sich 125

nicht damit auseinander, dass die Bundesbeauftragte jedenfalls seit Inkrafttreten von § 26a Abs. 2 Satz 2 BVerfSchG 2018 im Rahmen ihrer Kontrolltätigkeit trotz ihrer beschränkten Kontrollkompetenzen auf den gesamten Datenbestand des Bundesnachrichtendienstes zugreifen darf (vgl. BTDrucks 18/11325, S. 122). Zudem gehen die Beschwerdeführenden nicht darauf ein, dass in § 58 Abs. 3 BNDG in der Fassung vom 19. April 2021 (BGBl I S. 771) nunmehr geregelt ist, dass sich die verschiedenen Kontrollorgane – auch die G 10-Kommission und die Bundesbeauftragte – im Rahmen ihrer jeweiligen Kontrollzuständigkeit über allgemeine Angelegenheiten ihrer Kontrolltätigkeit regelmäßig austauschen können.

bb) Der Grundsatz der Subsidiarität steht der Zulässigkeit der Verfassungsbeschwerden nicht entgegen, da kein anderes geeignetes prozessuales Mittel im fachgerichtlichen Verfahren gegeben ist, das den geltend gemachten Grundrechtsverletzungen abhelfen könnte. 126

Die Beschwerdeführenden sind nicht auf die Möglichkeit der Beschwerde bei der G 10-Kommission im Sinne des § 15 Abs. 5 Satz 1 G 10 zu verweisen (vgl. BVerfGE 100, 313 <354 ff.>). Diese Beschwerde ist nicht Teil des fachgerichtlichen Rechtsschutzes. Die G 10-Kommission ist vielmehr ein Kontrollorgan eigener Art außerhalb der rechtsprechenden Gewalt (vgl. BVerfGE 30, 1 <23>; 67, 157 <171>). 127

Auch auf verwaltungsgerichtliche Rechtsschutzmöglichkeiten sind die Beschwerdeführenden nicht zu verweisen (so im Ergebnis auch BVerfGE 100, 313 <354 ff.>; 154, 152 <212 f. Rn. 79 f.>). Insbesondere ist nicht ersichtlich, dass die Beschwerdeführenden die strengen Zulässigkeitsanforderungen des Bundesverwaltungsgerichts für gerichtlichen Rechtsschutz gegen Maßnahmen der strategischen Inland-Ausland-Fernmeldeaufklärung (vgl. BVerwGE 149, 359 <364 Rn. 19 ff.>; 157, 8 <12 ff. Rn. 14 ff.>; 161, 76 <77 f. Rn. 12 ff.>) erfüllen könnten. 128

2. Die Verfassungsbeschwerden sind fristgerecht erhoben worden. Soweit sie sich jeweils gegen den am 21. November 2015 in Kraft getretenen § 5 Abs. 1 Satz 3 Nr. 8 G 10 richten, wahren die am 5. August 2016 (1 BvR 1743/16) und am 11. November 2016 (1 BvR 2539/16) erhobenen Verfassungsbeschwerden die gesetzliche Jahresfrist des § 93 Abs. 3 BVerfGG. 129

Darauf, ob die flankierenden Regelungen zur verhältnismäßigen Ausgestaltung der Überwachungsbefugnis innerhalb der Jahresfrist angegriffen worden sind, kommt es vorliegend nicht an. Diese flankierenden Vorschriften sind – unabhängig von einer Änderung ihres Wortlauts oder Inhalts – bei der Prüfung der Angemessenheit der neuen Befugnis des § 5 Abs. 1 Satz 3 Nr. 8 G 10 mittelbar zu berücksichtigen, wenn die verfassungsrechtliche Unzulänglichkeit dieser flankierenden Regelungen substantiiert dargelegt ist oder wenn sie auf der Hand liegt (vgl. BVerfGE 162, 1 <65 Rn. 132>; 165, 1 <44 f. Rn. 75>). Vor diesem 130

Hintergrund können alle flankierenden Regelungen – unabhängig von ihrer Änderung – innerhalb der mit Blick auf die geänderte Befugnisnorm laufenden Frist und bezogen auf diese Befugnis angegriffen werden. Dies ist hier der Fall.

C.

Die Verfassungsbeschwerden sind, soweit sie zulässig sind, überwiegend begründet. Die Beschwerdeführenden können sich auf das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG berufen (I), und die angegriffenen Regelungen greifen in das Fernmeldegeheimnis ein (II). Diese Grundrechtseingriffe sind verfassungsrechtlich nicht gerechtfertigt (III). 131

I.

1. Die Beschwerdeführenden in beiden Verfassungsbeschwerden können sich auf den Schutz des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG) berufen. Dies gilt auch für den Beschwerdeführer zu 1) im Verfahren 1 BvR 2539/16 als inländische juristische Person, weil Art. 10 Abs. 1 GG auf juristische Personen wesensmäßig anwendbar ist (vgl. BVerfGE 154, 152 <207 Rn. 67>). 132

Die Beschwerdeführenden zu 5) und 6) im Verfahren 1 BvR 2539/16 können sich als ausländische Personen im Ausland auf Art. 10 Abs. 1 GG in seiner abwehrrechtlichen Funktion berufen. Der Schutz des Art. 10 Abs. 1 GG gilt auch gegenüber einer Telekommunikationsüberwachung von ausländischen Personen im Ausland (vgl. BVerfGE 154, 152 <215 Rn. 87>). Dem steht nicht entgegen, dass die Beschwerdeführenden zu 5) und 6) Funktionsträger einer ausländischen juristischen Person sind. Denn Funktionsträger können eigene Grundrechte geltend machen, auch dann, wenn der von den Funktionsträgern geltend gemachte Schutz im Einzelfall zugleich reflexhaft der juristischen Person zugutekommt (vgl. BVerfGE 154, 152 <207 f. Rn. 69>). 133

2. Die angegriffene Ermächtigung in § 5 Abs. 1 Satz 3 Nr. 8 G 10 betrifft den sachlichen Schutzbereich von Art. 10 Abs. 1 GG (Fernmeldegeheimnis/Telekommunikationsgeheimnis). 134

Mit der grundrechtlichen Verbürgung aus Art. 10 Abs. 1 GG soll historisch vermieden werden, dass der vermittelte Meinungs- und Informationsaustausch über Entfernungen deswegen unterbleibt oder nach Form und Inhalt verändert wird, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen (vgl. BVerfGE 100, 313 <359>; 113, 348 <365>). Das Telekommunikationsgeheimnis begegnet nach wie vor alten sowie neuen Persönlichkeitsgefährdungen, die sich aus der gestiegenen Bedeutung der Informationstechnik für die Entfaltung des Einzelnen ergeben (vgl. dazu bereits BVerfGE 120, 274 <307> m.w.N.). 135

Der sachliche Schutzbereich des Telekommunikationsgeheimnisses aus Art. 10 Abs. 1 GG umfasst zuvörderst den Kommunikationsinhalt. Die öffentliche Gewalt soll grundsätzlich nicht die Möglichkeit haben, sich Kenntnis vom Inhalt der über Telekommunikationsanlagen abgewickelten Kommunikationen zu verschaffen. Einen Unterschied zwischen Kommunikationen privaten und anderen, etwa geschäftlichen oder politischen, Inhalts macht Art. 10 GG genauso wenig wie zwischen Übermittlungsarten oder Ausdrucksformen. Der Grundrechtsschutz bezieht sich vielmehr auf alle mittels der Telekommunikationstechnik ausgetauschten Kommunikationen. Ebenso umfasst der Grundrechtsschutz die Kommunikationsumstände. Dazu gehört insbesondere, ob, wann und wie oft zwischen welchen Personen oder Anschlüssen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist. Die Nutzung des Kommunikationsmediums soll in allem vertraulich sein. Indem das Grundrecht die einzelnen Kommunikationsvorgänge grundsätzlich dem staatlichen Zugriff entzieht, will es zugleich die Bedingungen einer freien Telekommunikation überhaupt aufrechterhalten (vgl. BVerfGE 100, 313 <358 f.>). 136

Der Schutz durch Art. 10 Abs. 1 GG gilt nicht nur dem ersten Zugriff, mit dem die öffentliche Gewalt von Telekommunikationsvorgängen und -inhalten Kenntnis nimmt. Seine Schutzwirkung erstreckt sich auch auf die Informations- und Datenverarbeitungsprozesse, die sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließen, und auf den Gebrauch, der von den erlangten Kenntnissen gemacht wird (vgl. BVerfGE 100, 313 <359>; 125, 260 <309>). 137

§ 5 Abs. 1 Satz 3 Nr. 8 G 10 ermächtigt zur Erhebung und weiteren Verarbeitung personenbezogener Daten im Wege der heimlichen strategischen Telekommunikationsüberwachung und betrifft damit diesen Gewährleistungsgehalt des durch Art. 10 Abs. 1 GG geschützten Telekommunikationsgeheimnisses. 138

II.

Die angegriffene Befugnis zur strategischen Inland-Ausland-Fernmeldeaufklärung nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 ermöglicht verschiedene Grundrechtseingriffe. 139

1. Da Art. 10 Abs. 1 GG die Vertraulichkeit der Kommunikation schützen will, bildet jede Kenntnisnahme, Aufzeichnung und Verwertung von Kommunikationsdaten durch den Staat einen Grundrechtseingriff (vgl. BVerfGE 100, 313 <366>; 125, 260 <310> m.w.N.). 140

2. a) Die Erfassung der Rohdatenströme von Telekommunikationsverkehren aus Übertragungswegen, die durch die Beschränkungsanordnungen näher bestimmt sind – also das Abfangen von Satelliten- und Richtfunksignalen und die Erfassung kabelgebundener Datenströme –, stellen sowohl gegenüber ausländischen Personen als auch gegenüber deutschen Staatsangehörigen einen Eingriff in Art. 10 Abs. 1 GG dar und 141

zwar unabhängig davon, ob sie sich im Inland oder Ausland aufhalten (vgl. BVerfGE 154, 152 <229 f. Rn. 114 ff., 252 Rn. 172>). 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 auf der Grundlage von Suchbegriffen auswerten kann. Die später wieder ausgesonderten Daten werden dabei nicht nur ungewollt miterfasst, sondern bewusst erhoben, um auf relevante Erkenntnisse hin ausgewertet und gegebenenfalls genutzt zu werden (vgl. BVerfGE 154, 152 <229 Rn. 115>; vgl. auch BVerfGE 100, 313 <366>).

Auch die Erfassung der Rohdatenströme von rein inländischen Telekommunikationsverkehren greift in Art. 10 Abs. 1 GG ein. An einem Eingriff fehlte es nur, wenn rein inländische Telekommunikationsverkehre ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Signalaufbereitung technisch wieder spurenlos ausgesondert würden (vgl. BVerfGE 100, 313 <366>). Das behördliche Interesse an solchen ungezielt erfassten Daten hätte sich dann nicht derart verdichtet, dass ein Betroffensein in einer einen Grundrechtseingriff auslösenden Qualität anzunehmen wäre (vgl. BVerfGE 100, 313 <366>; 115, 320 <343>; 150, 244 <266 Rn. 43>). Allerdings ist nach dem derzeitigen Stand der Technik eine Herausfilterung der Daten von rein inländischen Telekommunikationsverkehren nicht vollständig möglich, so dass teilweise auch solche Daten in die Auswertung gelangen. Aussortiert werden sie dann erst bei ihrer Identifizierung im Rahmen der händischen Sichtung. § 5 Abs. 1 Satz 3 Nr. 8 G 10 erlaubt dies zwar nicht in klar erkennbarer Weise, setzt ein solches Verständnis jedoch, um überhaupt angewendet werden zu können, voraus; so wird die Vorschrift auch in der Praxis verstanden (vgl. BVerfGE 154, 152 <230 Rn. 117> zu dem insoweit vergleichbaren Verständnis des § 6 Absätze 1 und 4 BNDG 2016 bei der strategischen Ausland-Ausland-Fernmeldeaufklärung; so auch die Stellungnahme der Bundesregierung im vorliegenden Verfahren). 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 Mitarbeitenden des Bundesnachrichtendienstes zur Kenntnis genommen werden, begründet dies einen Eingriff (vgl. BVerfGE 154, 152 <230 Rn. 117>). 142

b) Weitere Grundrechtseingriffe begründet § 5 Abs. 1 Satz 3 Nr. 8 G 10, in dem diese Norm zur Auswertung der erfassten Daten ermächtigt. Die Befugnisse zur automatisierten Sichtung der erfassten Telekommunikation mittels Suchbegriffen, zur händischen Auswertung der hierbei herausgefilterten Telekommunikationsverkehre und zur weiteren Nutzung der erhobenen Daten durch den Bundesnachrichtendienst stellen jeweils eigenständige Grundrechtseingriffe dar (vgl. auch BVerfGE 154, 152 <230 f. Rn. 118>). 143

III.

Diese Eingriffe in Art. 10 Abs. 1 GG sind verfassungsrechtlich nur teilweise gerechtfertigt. 144
Zwar sind die angegriffenen Normen formell verfassungsgemäß (1), sie genügen aber den Anforderungen des Grundsatzes der Verhältnismäßigkeit nicht (2).

1. Die Ermächtigung zur strategischen Inland-Ausland-Fernmeldeaufklärung im Bereich 145
der Cybergefahren nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 ist in formeller Hinsicht mit der Verfassung vereinbar. Insbesondere steht dem Bund insoweit die Gesetzgebungskompetenz zu.

a) Nach Art. 73 Abs. 1 Nr. 1 GG hat der Bund die ausschließliche Befugnis zur 146
Gesetzgebung über die auswärtigen Angelegenheiten sowie die Verteidigung einschließlich des Schutzes der Zivilbevölkerung. Auswärtige Angelegenheiten im Sinne von Art. 73 Abs. 1 Nr. 1 GG sind diejenigen Fragen, 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.>; 154, 152 <232 f. Rn. 125>). Hierzu gehört auch die Einrichtung einer Stelle zur umfassenden Auslandsaufklärung und ihre Ausstattung mit aufgabenadäquaten Befugnissen, wobei aber die Aufgaben, die der Gesetzgeber einer solchen Stelle übertragen kann, begrenzt sind (vgl. BVerfGE 100, 313 <369 f.>; 154, 152 <232 Rn. 124>). Der Bund kann den Bundesnachrichtendienst mit der Auslandsaufklärung nicht allgemein zum Zweck der Gewährleistung der inneren Sicherheit betrauen, sondern kann ihm nur Aufgaben und Befugnisse übertragen, die eine außen- und sicherheitspolitische Bedeutung haben und damit eine internationale Dimension aufweisen. Dies ist bei der Früherkennung von aus dem Ausland drohenden Gefahren der Fall, wenn 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 (vgl. BVerfGE 154, 152 <233 f. Rn. 126 ff.>).

b) Hiernach lässt sich § 5 Abs. 1 Satz 3 Nr. 8 G 10 kompetenzrechtlich auf Art. 73 Abs. 1 147
Nr. 1 GG stützen.

aa) Bei dieser Befugnis des Bundesnachrichtendienstes handelt es sich um eine Regelung 148
von auswärtigen Angelegenheiten im Sinne des Art. 73 Abs. 1 Nr. 1 GG. Sie trägt den dargelegten kompetenzrechtlichen Grenzen Rechnung (vgl. BVerfGE 100, 313 <370 f.>; 154, 152 <235 Rn. 129>). Überwachungsmaßnahmen des Bundesnachrichtendienstes sind nach ihr nur im Rahmen der allgemeinen Aufgabenzuweisung gemäß § 1 Abs. 1 Nr. 2 G 10 in Verbindung mit § 1 Abs. 2 BNDG zulässig, also nur zur Gewinnung von Erkenntnissen, die von außen- und sicherheitspolitischer Bedeutung sind und damit eine internationale Dimension aufweisen (vgl. BTDrucks 18/4654, S. 41).

bb) Soweit § 5 Abs. 1 Satz 3 Nr. 8 G 10 zugleich Regelungen über den Datenschutz trifft und von Sicherungen der Verhältnismäßigkeit flankiert wird, sind diese als Bestandteile einer verfassungskonformen Ausgestaltung kraft Sachzusammenhang miterfasst (vgl. BVerfGE 125, 260 <314>). 149

cc) Die Gesetzgebungskompetenz nach Art. 73 Abs. 1 Nr. 1 GG besteht entgegen der Auffassung des Beschwerdeführers im Verfahren 1 BvR 1743/16 auch, soweit § 5 Abs. 1 Satz 3 Nr. 8 G 10 die strategische Inland-Ausland-Fernmeldeaufklärung im Hinblick auf die Gefahr internationaler krimineller Angriffe erlaubt. Denn auch der Gefahr internationaler krimineller Angriffe kann außen- und sicherheitspolitische Bedeutung zukommen, etwa bei Cyberangriffen durch staatenübergreifend machtvoll agierende Netzwerke der organisierten Kriminalität oder bei von außen gesteuerten kriminellen Cyberangriffen auf wichtige Infrastrukturen sowie auf informationstechnische Systeme von Verfassungsorganen oder anderen notwendigen Einrichtungen des Verfassungslebens wie Parteien und Fraktionen (vgl. BVerfGE 154, 152 <234 f. Rn. 128>). 150

2. Die durch § 5 Abs. 1 Satz 3 Nr. 8 G 10 ermöglichten Grundrechtseingriffe sind aber nicht gerechtfertigt, weil diese Überwachungsbefugnis dem Grundsatz der Verhältnismäßigkeit nicht gerecht wird. 151

a) Ermächtigungen zu heimlichen Überwachungsbefugnissen sind nur dann materiell verfassungskonform, wenn sie den Anforderungen der Bestimmtheit und Normenklarheit (aa) und der Verhältnismäßigkeit (bb) genügen. 152

aa) Eingriffe in Art. 10 Abs. 1 GG müssen nach Art. 10 Abs. 2 Satz 1 GG auf einer gesetzlichen Ermächtigung beruhen. Diese muss dem Grundsatz der Bestimmtheit und Normenklarheit genügen (vgl. BVerfGE 154, 152 <237 Rn. 137>; stRspr). Für die Bestimmtheit reicht es aus, dass sich im Wege der Auslegung der einschlägigen Bestimmung mit Hilfe der anerkannten Auslegungsregeln feststellen lässt, ob die tatsächlichen Voraussetzungen für die in der Rechtsnorm ausgesprochene Rechtsfolge vorliegen (vgl. BVerfGE 156, 11 <45 Rn. 86>; 163, 43 <83 Rn. 109>; stRspr). Aus der Normenklarheit, bei der die inhaltliche Verständlichkeit der Regelung für Bürgerinnen und Bürger im Vordergrund steht, folgt, dass der Inhalt der einzelnen Norm verständlich und ohne größere Schwierigkeiten durch Auslegung zu konkretisieren sein muss (vgl. BVerfGE 163, 43 <83 Rn. 111>; 165, 1 <54 Rn. 97>; stRspr). 153

Bei der heimlichen Datenerhebung und -verarbeitung sind an die Bestimmtheit und Normenklarheit besonders strenge Anforderungen zu stellen. Heimliche Überwachungsmaßnahmen gelangen den Betroffenen kaum zur Kenntnis und können daher von ihnen nur selten im Rechtsweg angegriffen werden. Der Gehalt der gesetzlichen Regelung kann so nur eingeschränkt im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden, was der Gesetzgeber durch die hinreichende Bestimmtheit der jeweiligen Normen auffangen muss (vgl. BVerfGE 154, 152 <237 f. 154

Rn. 137; 162, 1 <95 Rn. 200, 125 f. Rn. 273> m.w.N.). Für die Nachrichtendienste einschließlich der Auslandsaufklärung gilt keine Ausnahme; ihre Befugnisse müssen im Gesetz bestimmt und normenklar geregelt werden (vgl. BVerfGE 154, 152 <238 f. Rn. 138 ff.>; 162, 1 <126 Rn. 274>).

bb) Als Ermächtigung zu Eingriffen in das Telekommunikationsgeheimnis ist die angegriffene Vorschrift nur zu rechtfertigen, wenn sie dem Verhältnismäßigkeitsgrundsatz genügt. Sie muss danach einen legitimen Zweck verfolgen, zur Erreichung des Zwecks geeignet, erforderlich und verhältnismäßig im engeren Sinne sein. Besondere Anforderungen ergeben sich dabei bei heimlichen Überwachungsbefugnissen aus dem Grundsatz der Verhältnismäßigkeit im engeren Sinne (vgl. BVerfGE 154, 152 <239 Rn. 141>; 162, 1 <72 f. Rn. 149> m.w.N.; stRspr). 155

b) Aus dem Verhältnismäßigkeitsgrundsatz folgen besondere Anforderungen an die Ausgestaltung und Begrenzung der Befugnis zur strategischen Inland-Ausland-Fernmeldeaufklärung. Diese Überwachungsbefugnis kann trotz ihres besonders schweren Eingriffsgewichts (aa) wegen des überragenden öffentlichen Interesses an einer wirksamen Auslandsaufklärung (bb) als besonderes Instrument der Auslandsaufklärung (cc) mit Art. 10 Abs. 1 GG vereinbar sein, wenn sie gesetzlich hinreichend strukturiert und begrenzt wird (dd). 156

aa) Die strategische Telekommunikationsüberwachung ist ein Instrument von besonders schwerem Eingriffsgewicht (vgl. auch BVerfGE 154, 152 <241 Rn. 146>). Ausgangspunkt ist insoweit, dass jede heimliche Überwachung der Telekommunikation grundsätzlich ein schwerer Eingriff in das Telekommunikationsgeheimnis ist, weil im Rahmen dieser Überwachung heimlich in Kommunikationen eingedrungen wird, die oftmals privaten und unter Umständen auch höchstvertraulichen Charakter haben (vgl. BVerfGE 113, 348 <382 ff.>; 141, 220 <264 f. Rn. 92>; 154, 152 <241 Rn. 147>). 157

Allerdings mindert sich das Eingriffsgewicht der strategischen Inland-Ausland-Fernmeldeaufklärung dadurch, dass sie typischerweise weniger zielgenau als die Überwachung individueller Telekommunikation und nicht vollständig ist. Auch ist die Überwachung auf die Gewinnung von Erkenntnissen über das Ausland gerichtet und sie ist dem Bundesnachrichtendienst als einer Behörde vorbehalten, die jedenfalls selbst grundsätzlich nicht über eigene operative Befugnisse verfügt (vgl. insoweit auch BVerfGE 154, 152 <241 f. Rn. 148 f.>). Zu berücksichtigen ist aber auf der anderen Seite, dass die strategische Inland-Ausland-Fernmeldeaufklärung auch deutsche Staatsangehörige und Inländer erfasst und somit tiefer in die innerstaatliche Rechtsordnung hineinreicht. Insoweit verfügt der deutsche Staat nicht nur über Hoheitsbefugnisse; die Überwachungsmaßnahme kann auch – anders als bei der strategischen Ausland-Ausland-Fernmeldeaufklärung (vgl. insoweit BVerfGE 154, 152 158

<242 Rn. 149>) – operative Konsequenzen für deutsche und inländische Betroffene nach sich ziehen. Das Eingriffsgewicht der Inland-Ausland-Fernmeldeaufklärung ist daher in dieser Hinsicht gegenüber dem der strategischen Ausland-Ausland-Fernmeldeaufklärung erhöht (vgl. BVerfGE 154, 152 <252 Rn. 172>).

Besonders erschwerend fällt die außerordentliche Streubreite der strategischen Telekommunikationsüberwachung ins Gewicht, die anlasslos gegenüber jeder Person erlaubt und allein durch bestimmte Zwecksetzungen final angeleitet wird (vgl. BVerfGE 100, 313 <380>; 154, 152 <242 Rn. 150>). 159

Eine solche Befugnis hat insbesondere unter den heutigen Bedingungen der Kommunikationstechnik und ihrer Bedeutung für die Kommunikationsbeziehungen eine außerordentliche Reichweite. Das Eingriffsgewicht dieser Befugnis ist nicht mehr zu vergleichen mit demjenigen der Befugnisse, über die das Bundesverfassungsgericht in seiner Entscheidung zur strategischen Inland-Ausland-Fernmeldeaufklärung im Jahr 1999 zu entscheiden hatte (BVerfGE 100, 313), sondern übersteigt dieses deutlich. Zugleich haben sich die Analysemöglichkeiten der Nachrichtendienste weiterentwickelt. Auch ermöglicht die strategische Telekommunikationsüberwachung mittlerweile durch die Verwendung formaler Suchbegriffe wie Telekommunikationskennungen auch gezielt personenbezogene Überwachungen und rückt dadurch näher an die individuelle Telekommunikationsüberwachung heran (vgl. BVerfGE 154, 152 <242 ff. Rn. 150 ff.>). 160

bb) Diesem besonders schweren Eingriffsgewicht steht mit einer wirksamen darauf gerichteten Inland-Ausland-Aufklärung durch den Bundesnachrichtendienst, die in § 5 Abs. 1 G 10 genannten Gefahren rechtzeitig erkennen und ihnen begegnen zu können, ein überragendes öffentliches Interesse gegenüber. Die für die Gewichtung dieses öffentlichen Interesses bedeutsamen Umstände sind mit Blick auf die grundlegend gewandelte außen- und sicherheitspolitische Lage als auch hinsichtlich der erheblich gesteigerten technologischen Möglichkeiten, auf die bei der Entwicklung von Gefahrenlagen zulasten der staatlichen Interessen der Bundesrepublik Deutschland zurückgegriffen werden kann, ebenfalls nicht mehr mit den damaligen Gegebenheiten (BVerfGE 100, 313) vergleichbar. Das Aufklärungsinteresse ist gerade im Bereich der Inland-Ausland-Aufklärung mit Blick auf ihre Inlandsdimension von besonderer Bedeutung. Von Gewicht ist dabei, dass im Zuge der Entwicklung der Informationstechnik und der internationalen Kommunikation sowie der engeren grenzüberschreitenden Verflechtung der Lebensbedingungen im Allgemeinen Bedrohungen vom Ausland aus erheblich zugenommen haben. Diese betreffen auch die gesteigerte informationstechnische Verletzlichkeit der vielfältig vernetzten modernen Gesellschaft. Die Früherkennung von aus dem Ausland drohenden Gefahrenlagen gewinnt deshalb für die Sicherheit besondere Bedeutung. Die Erweiterung und Internationalisierung der Kommunikationsmöglichkeiten und die damit gesteigerte Politisierung und 161

Organisationsfähigkeit international agierender staatlicher und nichtstaatlicher Gruppierungen führen dazu, dass innerstaatliche Gefahrenlagen oftmals durch Netzwerke international zusammenarbeitender Akteure begründet sind. Solche Aktivitäten zielen zum Teil auf eine Destabilisierung des Gemeinwesens 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 verfassungsrechtlichem Gewicht, für deren Schutz der Gesetzgeber eine wirksame und zugleich rechtsstaatlich eingehegte Auslandsaufklärung als unverzichtbar ansehen kann (vgl. entsprechend zur strategischen Ausland-Ausland-Fernmeldeüberwachung BVerfGE 154, 152 <248 f. Rn. 161 ff.> m.w.N.).

cc) Aufgrund dieses überragenden öffentlichen Interesses an einer wirksamen Auslandsaufklärung lässt sich auch die gegenüber der strategischen Ausland-Ausland-Fernmeldeüberwachung teilweise eingriffsintensivere Befugnis zur strategischen Inland-Ausland-Fernmeldeaufklärung als besonderes Instrument der Auslandsaufklärung im Grundsatz mit Art. 10 Abs. 1 GG vereinbaren, obwohl eine solche grundsätzlich allein final angeleitete Eingriffsbefugnis für innerstaatlich tätige Sicherheitsbehörden und Nachrichtendienste unverhältnismäßig wäre (vgl. BVerfGE 100, 313 <383>; 154, 152 <244 f. Rn. 155 f.>). Auch als Instrument der Auslandsaufklärung ist die anlasslose strategische Auslandsfernmeldeaufklärung aber eine Ausnahmebefugnis, die auf eine Behörde begrenzt bleiben muss, welche selbst grundsätzlich keine operativen Befugnisse zur Gefahrenabwehr hat. Nur durch deren besonderes Aufgabenprofil ist sie gerechtfertigt. Hieran hat sich nach dem Grundsatz der Verhältnismäßigkeit auch die nähere gesetzliche Ausgestaltung auszurichten (vgl. BVerfGE 154, 152 <250 Rn. 166>). 162

dd) Als besonderes Instrument der Auslandsaufklärung ist die gesetzliche Ermächtigung zur strategischen Auslandsfernmeldeaufklärung nur angemessen, wenn sie trotz ihrer Streubreite als hinreichend fokussiertes Instrument normenklar ausgestaltet und damit begrenzt wird. Eine globale und pauschale Überwachung lässt das Grundgesetz auch zu Zwecken der Auslandsaufklärung nicht zu (vgl. BVerfGE 100, 313 <376>; 154, 152 <250 f. Rn. 167 f.>). Dies gilt auch für die strategische Inland-Ausland-Überwachung. 163

(1) Zunächst hat der Gesetzgeber die Befugnis zur strategischen Inland-Ausland-Fernmeldeaufklärung hinreichend präzise und normenklar auf Aufklärungszwecke zu beschränken, die dem Schutz solcher hochrangiger Gemeinschaftsgüter dienen, deren Verletzung schwere Schäden für den äußeren und inneren Frieden oder die Rechtsgüter Einzelner zur Folge hätte (vgl. BVerfGE 100, 313 <373>; 154, 152 <253 f. Rn. 176>). 164

(2) Darüber hinaus bedarf es einer normenklaren, die Nutzung verfügbarer technischer Möglichkeiten fordernden Regelung zur Aussonderung von Daten aus rein inländischen Telekommunikationsverkehren, also aus solchen, an denen nur deutsche Staatsangehörige 165

oder inländische Personen beteiligt sind. Soweit dies technisch möglich ist, muss durch den Einsatz von automatisierten Filterprozessen sichergestellt sein, dass den Mitarbeitenden des Bundesnachrichtendienstes solche Telekommunikationsdaten nicht bekannt werden. Zwar ist es nicht von vornherein unzulässig, wenn, soweit technisch unvermeidbar, zunächst unterschiedslos alle Daten und damit auch die Daten aus rein inländischen Telekommunikationen von den Systemen des Bundesnachrichtendienstes erfasst werden. Der Gesetzgeber muss dann aber normenklar regeln, dass Daten aus der reinen Inlandskommunikation mit allen zur Verfügung stehenden Mitteln technisch herauszufiltern und spurenlos zu löschen sind, bevor eine manuelle Auswertung erfolgt. Der Bundesnachrichtendienst ist zudem darauf zu verpflichten, die Filtermethoden kontinuierlich fortzuentwickeln. Außerdem sind technikbedingt nicht ausgesonderte Daten aus rein inländischen Telekommunikationsverkehren grundsätzlich unverzüglich zu löschen (vgl. zum Ganzen BVerfGE 154, 152 <252 f. Rn. 173 f.>).

(3) Weitere Anforderungen ergeben sich aus Art. 10 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG zum Schutz des Kernbereichs privater Lebensgestaltung (vgl. BVerfGE 154, 152 <262 ff. Rn. 200 ff.>). 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 nicht schon dadurch ihren Charakter als insgesamt höchstpersönlich, dass sich in ihnen Höchstpersönliches und Alltägliches vermischen. Demgegenüber ist die Kommunikation unmittelbar über Straftaten nicht geschützt, selbst wenn sie auch Höchstpersönliches zum Gegenstand hat (vgl. BVerfGE 141, 220 <276 f. Rn. 121 f.>; 154, 152 <262 f. Rn. 201 f.>; 162, 1 <126 f. Rn. 276>; stRspr). 166

Auf der Ebene der Datenerhebung darf der Kernbereich nicht zum Ziel staatlicher Ermittlungen gemacht werden. Über dieses Verbot der gezielten Kernbereichserfassung hinausgehende gesetzliche Vorkehrungen sind auf dieser Ebene 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 (vgl. BVerfGE 154, 152 <263 f. Rn. 204 ff.>). 167

Demgegenüber ist auf der Ebene der händischen Datenauswertung gesetzlich sicherzustellen, dass die weitere Auswertung unverzüglich zu unterbrechen ist, wenn erkennbar wird, dass eine Überwachung in den Kernbereich persönlicher Lebensgestaltung eingedrungen ist. In Zweifelsfällen hat eine unabhängige Stelle die aufgezeichneten Telekommunikationsverkehre zu sichten und darüber zu entscheiden, ob die Auswertung fortgesetzt werden darf (vgl. BVerfGE 141, 220 <279 f. Rn. 129>; 154, 152 <264 Rn. 207>). 168

(4) Zudem ist die Befugnis zur strategischen Auslandsfernmeldeaufklärung durch die Verpflichtungen sowohl zur unverzüglichen Löschung von erhobenen personenbezogenen Daten, deren Speicherung nicht (mehr) erforderlich ist, als auch zur Protokollierung der Löschung zu flankieren und damit verhältnismäßig auszugestalten. 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 100, 313 <364 f.>; 141, 220 <302 f. Rn. 205>; 154, 152 <265 Rn. 210>). Die Länge der Frist zur Aufbewahrung der Löschungsprotokolle muss demnach so bemessen sein, dass die Protokolle bei typisierender Betrachtung nach der Benachrichtigung der Betroffenen und im Rahmen der nächsten periodisch anstehenden datenschutzrechtlichen Kontrolle noch vorliegen (vgl. BVerfGE 100, 313 <400>; 141, 220 <323 Rn. 272>). 169

(5) Schließlich ist die strategische Telekommunikationsüberwachung nur mit den Anforderungen der Verhältnismäßigkeit vereinbar, wenn sie durch eine effektive unabhängige objektivrechtliche Kontrolle flankiert ist. Diese objektivrechtliche Kontrolle muss kontinuierlich und umfassend ausgestaltet sowie auf die Wahrung der Grundrechte der Betroffenen ausgerichtet sein (vgl. BVerfGE 100, 313 <361 f.>; 154, 152 <290 Rn. 272>). Die Kontrolle hat sich grundsätzlich auf alle wesentlichen Verfahrensschritte der strategischen Telekommunikationsüberwachung und der hiermit verbundenen Datenverarbeitung zu erstrecken (vgl. BVerfGE 100, 313 <361 f.>; 154, 152 <291 f. Rn. 278>). 170

Die verfassungsrechtlichen Anforderungen an die Ausgestaltung der objektivrechtlichen Kontrolle der strategischen Überwachung sind besonders hoch. Denn mit der Kontrolle ist ein Ausgleich dafür zu schaffen, dass übliche rechtsstaatliche Sicherungen in weitem Umfang ausfallen. Zum einen muss die Kontrolle die faktische Schwäche der individuellen Rechtsschutzmöglichkeiten ausgleichen, die aus den nur begrenzten Auskunfts- und Benachrichtigungspflichten folgt. Zum anderen hat sie die im Wesentlichen nur finale Anleitung der Überwachungsbefugnisse zu kompensieren. Dazu hat sie abzusichern, dass das Anordnungs- und Anwendungsverfahren ausreichend strukturiert und durchgehend auf die gesetzlichen Ziele hin ausgerichtet wird. Sie bildet damit ein notwendiges Gegengewicht zu den weiten Handlungsmöglichkeiten des Bundesnachrichtendienstes (vgl. BVerfGE 154, 152 <290 Rn. 273>; vgl. auch BVerfGE 100, 313 <361 f.>). 171

Sicherzustellen sind dabei zwei verschiedene Arten von Kontrolle, die sich auch organisationsrechtlich abbilden müssen (BVerfGE 154, 152 <291 Rn. 274). Zum einen ist eine Kontrolle durch eine gerichtsähnlich ausgestaltete Stelle sicherzustellen, die mit Personen in gleichsam richterlicher Unabhängigkeit besetzt ist und abschließend entscheidet. Diese gerichtsähnliche Kontrolle muss materiell und verfahrensmäßig einer gerichtlichen Kontrolle gleichwertig, insbesondere mindestens ebenso wirkungsvoll sein (vgl. BVerfGE 154, 152 <291 Rn. 275>; zu Art. 10 Abs. 2 Satz 2 GG: BVerfGE 30, 1 <23>; vgl. 172

zur hinreichenden Wirksamkeit auch BVerfGE 100, 313 <361 f.>). Zum anderen ist eine unabhängige Rechtskontrolle administrativen Charakters einzurichten (näher dazu BVerfGE 154, 152 <291 Rn. 276>).

Damit die unabhängige objektivrechtliche Kontrolle effektiv erfolgen kann, ist außerdem erforderlich, dass Beschränkungsanordnungen auch insoweit begründet werden, als es im Verwaltungsverfahren zu einer Änderung des ursprünglich beantragten Inhalts kommt. Denn nur anhand einer Begründung auch des geänderten Inhalts kann die objektivrechtliche Kontrollinstanz überprüfen, ob die Voraussetzungen des Artikel 10-Gesetzes bei Anordnung der Beschränkung – auch bezüglich der Änderungen – eingehalten werden. Eine solche Begründung von Änderungen am Inhalt der Beschränkungsanordnungen ist ebenfalls zur Wahrung der subjektiven Rechtsschutzmöglichkeiten der Betroffenen notwendig. 173

c) Die Ermächtigung zur Datenerhebung und weiteren Datenverarbeitung im Wege der strategischen Inland-Ausland-Fernmeldeaufklärung nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 verletzt Art. 10 Abs. 1 GG, weil sie nicht in vollem Umfang dem Verhältnismäßigkeitsgrundsatz genügt. Zwar dient diese Ermächtigung einem legitimen Zweck (aa) und ist geeignet (bb) sowie erforderlich (cc), um diesen Zweck zu erreichen. Jedoch genügt diese Norm den Anforderungen der Verhältnismäßigkeit im engeren Sinn an die Begrenzung und Strukturierung der strategischen Inland-Ausland-Fernmeldeaufklärung nicht vollumfänglich (dd). 174

aa) § 5 Abs. 1 Satz 3 Nr. 8 G 10 dient einem legitimen Regelungszweck. Nach dem Willen des Gesetzgebers soll die strategische Überwachung gemäß § 5 Abs. 1 Satz 3 Nr. 8 G 10 Erkenntnisse über Cybergefahren aus dem Ausland verschaffen, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind. Um Cybergefahren aus dem Ausland wirkungsvoll zu begegnen, wird dem Bundesnachrichtendienst eine gesetzliche Befugnis zur Aufklärung von internationalen Cyberangriffen (etwa in Gestalt von Cyberspionage oder Cybersabotage) eingeräumt. Dabei dient die Früherkennung dieser internationalen Cybergefahren dem Schutz der kritischen digitalen Infrastrukturen oder vergleichbar wichtiger informationstechnischer Systeme (vgl. BTDrucks 18/4654, S. 41). 175

Zur kritischen Infrastruktur gehören nach den maßgeblichen rechtlichen Regelungen Einrichtungen, Anlagen und Systeme, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen auf den Staat hätten (vgl. Art. 2 Buchstabe a der Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, ABl EU Nr. L 345 S. 75; vgl. auch § 2 Abs. 10 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik – BSIG; vgl. für die 176

Rechtslage ab dem 18. Oktober 2024: Art. 2 Nummern 1, 4 und 5 der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates, ABl EU Nr. L 333 S. 164). Danach zählen zu den kritischen Einrichtungen etwa Krankenhäuser, die Wasser- und Energieversorgung sowie wichtige Transportinfrastrukturen wie Flughäfen.

Mindestens ebenso wichtig sind die informationstechnischen Systeme von Verfassungsorganen oder anderen notwendigen Faktoren des Verfassungslebens (etwa Parteien nach Art. 21 GG: vgl. BVerfGE 144, 20 <194 Rn. 512>; 162, 207 <228 f. Rn. 71> m.w.N. – Äußerungsbefugnisse der Bundeskanzlerin; Parlamentsfraktionen gemäß Art. 38 Abs. 1 Satz 2 GG: vgl. BVerfGE 84, 304 <324> m.w.N. oder Gerichte nach Art. 92 GG: vgl. BVerfGE 54, 277 <292>; 153, 74 <155 Rn. 143> – Einheitliches Patentgericht). 177

bb) Die Befugnis zur strategischen Inland-Ausland-Fernmeldeaufklärung gemäß § 5 Abs. 1 Satz 3 Nr. 8 G 10 ist auch geeignet, diesen legitimen Zweck zu erreichen. Für die Eignung genügt bereits die Möglichkeit, durch die gesetzliche Regelung den Gesetzeszweck zu fördern. Dabei steht dem Gesetzgeber ein Spielraum zu, der sich auf die Einschätzung und Bewertung der tatsächlichen Verhältnisse, auf die etwa erforderliche Prognose und auf die Wahl der Mittel bezieht, um die Ziele des Gesetzes zu erreichen (vgl. BVerfGE 159, 223 <305 Rn. 185> m.w.N.; stRspr). Diesen Anforderungen genügt § 5 Abs. 1 Satz 3 Nr. 8 G 10, denn es erscheint jedenfalls möglich, dass aufgrund dieser Befugnis Erkenntnisse über Cybergefahren aus dem Ausland gesammelt werden können, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind. 178

cc) Die Überwachungsermächtigung in § 5 Abs. 1 Satz 3 Nr. 8 G 10 ist zudem erforderlich zur Zweckerreichung. Ohne die breit angelegte anlasslose Erfassung von Datenströmen und deren Auswertung könnten entsprechende Informationen von außen- und sicherheitspolitischer Bedeutung nicht gewonnen werden. Ein weniger eingriffsintensives Mittel, das generell vergleichbare Informationen sicherstellte, ist nicht ersichtlich (vgl. BVerfGE 100, 313 <375>; 154, 152 <241 Rn. 144>). 179

dd) § 5 Abs. 1 Satz 3 Nr. 8 G 10 genügt aber nicht in vollem Umfang den Anforderungen der Verhältnismäßigkeit im engeren Sinne. Zwar kann die Befugnis zur strategischen Inland-Ausland-Fernmeldeaufklärung trotz ihres besonders hohen Eingriffsgewichts grundsätzlich aufgrund des überragenden öffentlichen Interesses gerade auch an der Aufklärung von internationalen Cybergefahren gerechtfertigt werden (1). Auch begrenzt § 5 Abs. 1 Satz 3 Nr. 8 G 10 den Aufklärungszweck hinreichend bestimmt und normenklar auf den Schutz hochrangiger Gemeinschaftsgüter (2). Jedoch fehlt eine hinreichend bestimmte und normenklare Regelung zur Aussonderung von Daten aus der reinen Inlandskommunikation (3). Darüber hinaus wird § 5 Abs. 2 Satz 3 in Verbindung mit Satz 2 180

Nr. 2 G 10 den verfassungsrechtlichen Anforderungen an die Gewährung eines bestimmten und normenklaren Schutzes des Kernbereichs der privaten Lebensgestaltung bezüglich ausländischer Personen im Ausland nicht gerecht (4). Zudem sieht § 5 Abs. 2 Satz 6 G 10 eine zu kurze Aufbewahrungsfrist bei der Dokumentation der Durchführung der strategischen Inland-Ausland-Fernmeldeaufklärung vor (5). Schließlich genügt die Ausgestaltung der unabhängigen objektivrechtlichen Kontrolle durch die G 10-Kommission nicht durchgehend den insoweit bestehenden besonders hohen Anforderungen (6).

(1) Die Befugnis des § 5 Abs. 1 Satz 3 Nr. 8 G 10 kann trotz des besonders hohen Eingriffsgewichts der strategischen Inland-Ausland-Fernmeldeaufklärung das seit der letzten Entscheidung des Bundesverfassungsgerichts zu dieser Überwachungsbefugnis (BVerfGE 100, 313) erheblich zugenommen hat (vgl. Rn. 160), grundsätzlich gerechtfertigt werden. Denn an der mit § 5 Abs. 1 Satz 3 Nr. 8 G 10 bezweckten Früherkennung von Cybergefahren aus dem Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, zum Schutz von kritischen digitalen Infrastrukturen oder vergleichbar wichtigen informationstechnischen Systemen besteht ein überragendes öffentliches Interesse. 181

Das Interesse an einer wirksamen Früherkennung der Gefahr von internationalen Cyberangriffen auf die kritische digitale Infrastruktur oder vergleichbar wichtige informationstechnische Systeme ist besonders groß. Die Zahl der internationalen Cyberangriffe auf informationstechnische Systeme in der Bundesrepublik Deutschland ist hoch und nimmt weiterhin zu (vgl. Bundesamt für Sicherheit in der Informationstechnik – BSI, Lageberichte zur IT-Sicherheit in Deutschland 2019, S. 47; 2020, S. 54; 2022, S. 11, 69 und 2023, S. 9, 62; vgl. zur Bedrohungslage in der Europäischen Union: Agentur der Europäischen Union für Cybersicherheit – ENISA, Threat Landscape 2021, S. 7; 2022, S. 7; 2023, S. 4; Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung – Europol, Spotlight Report Cyber Attacks, 2023, S. 20). In der Bundesrepublik überstiegen in den Jahren 2022 und 2023 die festgestellten Cyber-Auslandstaten, bei denen die Schäden in Deutschland verursacht werden, aber der Aufenthaltsort des Täters im Ausland liegt, die jeweils registrierten Cyber-Inlandstaten (vgl. BKA, Bundeslagebilder Cybercrime 2022, S. 6; 2023, S. 8; die gesamtwirtschaftlichen Schäden, die unmittelbar aus Cyberangriffen resultieren, werden in der Bundesrepublik im Jahr 2023 mit 148 Milliarden Euro beziffert, vgl. BKA, Bundeslagebild Cybercrime 2023, S. 1, 23). Dabei zielen Cyberangriffe gerade auch auf kritische Infrastrukturen ab und beeinträchtigen deren Funktionieren erheblich (vgl. ENISA, Threat Landscape 2021, S. 29; BSI, Lageberichte zur IT-Sicherheit in Deutschland 2019, S. 47; 2020, S. 54; 2022, S. 11, 69 und 2023, S. 9, 62). 182

Das Gefährdungspotential internationaler Cyberangriffe ist außerordentlich hoch. Im Zuge der digitalen Transformation der Gesellschaft, Wirtschaft, Verwaltung und Politik hän- 183

gen nahezu alle Lebensbereiche immer stärker von einer funktionierenden digitalen Infrastruktur und deren Sicherheit ab. Die zentrale Bedeutung sicherer und funktionsfähiger informationstechnischer Systeme für die grundrechtliche Freiheitsverwirklichung (vgl. BVerfGE 120, 274 <303 ff.>; 158, 170 <185 Rn. 33> – IT-Sicherheitslücken) nimmt stetig zu. Auch die Verfassungsorgane und die anderen notwendigen Einrichtungen des Verfassungslebens sind zur Wahrnehmung ihrer Aufgaben in zunehmendem Maße von der Nutzung informationstechnischer Systeme abhängig. Denn die Umstellung ehemals analoger Vorgänge auf digitale Prozesse und nicht zuletzt die immer breitere mobile Nutzung informationstechnischer Systeme erhöhen die Abhängigkeit von Informationstechnologie auch staatlicher Akteure (vgl. BVerfGE 158, 170 <185 Rn. 33>). Zudem haben Bedrohungen aus dem Ausland durch die Weiterentwicklung der internationalen Kommunikation und durch eine generelle engere grenzüberschreitende Verflechtung der Lebensbedingungen im Allgemeinen, erheblich zugenommen (vgl. BVerfGE 154, 152 <248 f. Rn. 163>). Die Fähigkeiten der Akteure, von denen die Cyberbedrohungen ausgehen, sind inzwischen beachtlich und entwickeln sich kontinuierlich weiter (vgl. EGMR <GK>, Big Brother Watch et al. v. the United Kingdom, Urteil vom 25. Mai 2021, Nr. 58170/13 u.a., Rn. 323; ENISA, Threat Landscape 2020, S. 8).

Vor diesem Hintergrund betreffen die in das Gesetz aufgenommenen internationalen Cybergefahren in § 5 Abs. 1 Satz 3 Nr. 8 G 10 hochrangige Gemeinschaftsgüter, deren Verletzung schwere Schäden für den äußeren und inneren Frieden und die Rechtsgüter Einzelner zur Folge hätte (vgl. BVerfGE 100, 313 <373>; 154, 152 <248 f. Rn. 163>). Internationale Cyberangriffe auf kritische digitale Infrastrukturen oder vergleichbar wichtige informationstechnische Systeme zielen auf eine Destabilisierung des Gemeinwesens 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 (vgl. BVerfGE 154, 152 <248 f. Rn. 163>). Durch internationale Cyberangriffe sind feindlich gesinnte staatliche und nichtstaatliche Akteure in der Lage, die digitale Infrastruktur und das einwandfreie Funktionieren demokratischer Verfahren zu stören und damit die nationale Sicherheit zu bedrohen (vgl. EGMR <GK>, Big Brother Watch et al. v. the United Kingdom, Urteil vom 25. Mai 2021, Nr. 58170/13 u.a., Rn. 323). Die Gefahr von internationalen Cyberangriffen kann letztlich sogar ein vergleichbares Ausmaß erreichen wie die Gefahr eines bewaffneten Angriffs auf die Bundesrepublik Deutschland, die in § 5 Abs. 1 Satz 3 Nr. 1 G 10 von Anfang an als legitimer Grund für die strategische Fernmeldeüberwachung anerkannt worden ist (vgl. insoweit BVerfGE 67, 157 <178>; 100, 313 <373>). In der digital transformierten Gesellschaft können gezielte und umfassende Cyberangriffe auf die IT-Infrastruktur elementarer und überlebenswichtiger Bereiche (etwa die Versorgung mit Wasser und Energie sowie das Transport- und Gesundheitswesen) wie ein bewaffneter Angriff wirken. Sowohl internationale Cyberangriffe als auch bewaffnete Angriffe können das Wohlergehen der Bevölkerung, die freiheitlich-demokratische Ordnung und sogar die Existenz des Staates in Frage stellen. 184

(2) Die Überwachungsbefugnis in § 5 Abs. 1 Satz 3 Nr. 8 G 10 wird entgegen der Ansicht der Beschwerdeführenden in beiden Verfassungsbeschwerden auch hinreichend bestimmt und normenklar auf den Schutz hochrangiger Gemeinschaftsgüter, deren Verletzung schwere Schäden für den äußeren und inneren Frieden und die Rechtsgüter Einzelner zur Folge hätte, begrenzt (a). Auch die Art der Cyberbedrohungen, die von dieser Norm erfasst werden, ist hinreichend bestimmt und normenklar geregelt (b). 185

(a) Der Anwendungsbereich des § 5 Abs. 1 Satz 3 Nr. 8 G 10 lässt sich ohne größere Schwierigkeiten mit Hilfe der anerkannten Auslegungsmöglichkeiten dahin konkretisieren, dass diese Befugnis lediglich dem Schutz von hochrangigen Gemeinschaftsgütern dient. 186

Überwachungsmaßnahmen des Bundesnachrichtendienstes nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 sind nur im Rahmen der allgemeinen Aufgabenzuweisung gemäß § 1 Abs. 1 Nr. 2 G 10 in Verbindung mit § 1 Abs. 2 BNDG zulässig, also nur zur Gewinnung von Erkenntnissen über solche Cybergefahren, die von außen- und sicherheitspolitischer Bedeutung sind und damit eine internationale Dimension aufweisen (vgl. BTDrucks 18/4654, S. 41, vgl. auch oben Rn. 148). 187

§ 5 Abs. 1 Satz 3 Nr. 8 G 10 dient allein dem Schutz der kritischen digitalen Infrastrukturen oder vergleichbar wichtiger informationstechnischer Systeme (vgl. BTDrucks 18/4654, S. 41). Damit verbunden ist der Schutz hochrangiger Gemeinschaftsgüter, deren Verletzung schwere Schäden für den äußeren und inneren Frieden oder die Rechtsgüter Einzelner zur Folge hätte (vgl. ausführlich oben Rn. 175 ff.). 188

Darüber hinaus lässt sich die Beschränkung des Anwendungsbereichs von § 5 Abs. 1 Satz 3 Nr. 8 G 10 auf Fälle von erheblicher Bedeutung anhand eines Vergleichs mit den anderen Gefahrenbereichen des § 5 Abs. 1 Satz 3 G 10 (Nummern 1 bis 7) bestimmen. Je näher die Auswirkungen einer Cyberbedrohung den Gefahren für die dort genannten Schutzgüter kommen, desto eher ist von einer „erheblichen Bedeutung“ auszugehen. Vor diesem Hintergrund ergibt sich entgegen der Ansicht der Beschwerdeführenden beider Verfassungsbeschwerden hinreichend bestimmt, dass der Begriff des „internationalen kriminellen Cyberangriffs“ anhand des Merkmals „in Fällen von erheblicher Bedeutung“ so auszulegen ist, dass lediglich Angriffe auf hochrangige Gemeinschaftsgüter und nicht alle Fälle der internationalen Cyberkriminalität erfasst werden. 189

(b) Hinreichend bestimmt und normenklar ist schließlich die Variante der „vergleichbaren schädlich wirkenden informationstechnischen Mittel“, die neben dem Angriff „mittels Schadprogrammen“ in § 5 Abs. 1 Satz 3 Nr. 8 G 10 aufgeführt ist. Aus der Gesetzentwurfsbegründung folgt, dass damit vor allem Überlastungsangriffe mit dem Ziel der Sabotage, Vortäuschen einer Identität, um beispielsweise an Zugangsinformationen zu gelangen, Angriffe auf informationstechnische Systeme unter Umgehung von physikalischen Grenzen 190

und Hardwaremanipulation von Netzwerkgeräten erfasst werden sollen (vgl. BTDrucks 18/4654, S. 41). Die Bundesregierung hat zutreffend darauf hingewiesen, dass aufgrund der Diversität von Angriffen auf informationstechnische Systeme hinsichtlich der technischen Durchführung eine genauere Umschreibung der Cyberangriffe nicht möglich sein dürfte.

(3) Demgegenüber ist die Befugnis zur strategischen Inland-Ausland-Fernmeldeaufklärung nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 nicht – wie verfassungsrechtlich geboten (vgl. BVerfGE 154, 152 <251 ff. Rn. 170 ff.>) – durch eine hinreichend bestimmte und normenklare Regelung zur Aussonderung von Daten aus rein inländischen Telekommunikationsverkehren begrenzt und ausgestaltet. 191

Bei der Durchführung der strategischen Inland-Ausland-Fernmeldeaufklärung werden zwingend auch Daten aus rein inländischen Telekommunikationsverkehren miterfasst. Zwar sieht § 5 Abs. 1 Satz 3 Nr. 8 G 10 vor, dass nur internationale Telekommunikationsbeziehungen überwacht werden dürfen. Jedoch kann der Bundesnachrichtendienst die Erfassung der Telekommunikationsrohdatenströme – jedenfalls bei der digitalen, paketvermittelten Telekommunikation (vgl. BTDrucks 18/12850, S. 713 ff.), die in der Praxis den weit überwiegenden Anteil der internationalen Telekommunikation ausmacht (unter anderem die gesamte Kommunikation über das Internet) – nicht auf Daten aus Telekommunikationsverkehren mit Auslandsbezug beschränken (vgl. BVerfGE 154, 152 <301 Rn. 304>; Lachenmann, DÖV 2016, S. 501 <504>; Löffelmann, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, 6. Teil, § 4 Rn. 142; Bergemann, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, H. Rn. 82 m.w.N.). 192

Das Artikel 10-Gesetz enthält keine Vorgaben dazu, wie mit diesen notwendig miterfassten Daten aus rein inländischen Telekommunikationsverkehren umzugehen ist. Zwar findet in der Praxis nach Angaben der Bundesregierung eine automatische Filterung und Aussonderung der rein inländischen Telekommunikationsdaten statt. Dies entbindet aber nicht den Gesetzgeber von seiner verfassungsrechtlichen Verpflichtung, bestimmt und normenklar zu regeln, dass Daten aus der rein inländischen Telekommunikation mit allen zur Verfügung stehenden Mitteln technisch herausgefiltert und spurenlos gelöscht werden müssen, bevor eine manuelle Auswertung erfolgt. Außerdem ist zu regeln, dass die Filtermethoden kontinuierlich fortzuentwickeln sind (vgl. oben Rn. 165). 193

(4) Ebenfalls nicht in vollem Umfang ausreichend sind die Vorkehrungen zum Schutz des Kernbereichs der privaten Lebensgestaltung. 194

(a) Bezüglich ausländischer Personen im Ausland wird § 5 Abs. 2 Satz 3 in Verbindung mit Satz 2 Nr. 2 G 10 den verfassungsrechtlichen Anforderungen an die Gewährleistung eines hinreichend bestimmten und normenklaren Schutzes des Kernbereichs der privaten Lebensgestaltung nicht gerecht. § 5 Abs. 2 Satz 3 G 10 macht nach seinem Wortlaut und seiner Systematik für ausländische Personen im Ausland eine Ausnahme von dem Verbot nach § 5 Abs. 2 Satz 2 Nr. 2 G 10, Suchbegriffe betreffend den Kernbereich der privaten Lebensgestaltung zu verwenden. Nach seiner Formulierung („Dies gilt nicht für Telekommunikationsanschlüsse im Ausland“) und seiner systematischen Stellung bezieht sich die Ausnahme des § 5 Abs. 2 Satz 3 G 10 auf den gesamten vorherigen § 5 Abs. 2 Satz 2 G 10, ohne zwischen § 5 Abs. 2 Satz 2 Nr. 1 (Verbot der gezielten Erfassung bestimmter Telekommunikationsanschlüsse) und Nr. 2 G 10 (Verbot der Verwendung von Suchbegriffen, die den Kernbereich betreffen) zu differenzieren. 195

Dies ist nicht mit Art. 10 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG vereinbar. Die gezielte Kernbereichserfassung ist auch gegenüber ausländischen Personen im Ausland unzulässig (vgl. BVerfGE 154, 152 <263 Rn. 204>), so dass Suchbegriffe, die den Kernbereich der Lebensgestaltung betreffen, gegenüber diesen Personen nicht eingesetzt werden dürfen. 196

Zwar steht § 5 Abs. 2 Satz 3 in Verbindung mit Satz 2 Nr. 2 G 10 in einem Spannungsverhältnis zu dem ebenfalls im Jahre 2009 eingeführten § 5a G 10, der ein unbedingtes und allgemeines Erfassungsverbot für Kommunikationsinhalte aus dem Kernbereich privater Lebensgestaltung vorsieht. Aus der Gesetzentwurfsbegründung zur Einführung des § 5a G 10 ergibt sich zudem, dass der Gesetzgeber § 5 Abs. 2 Satz 3 G 10 lediglich als Ausnahme zu § 5 Abs. 2 Satz 2 Nr. 1 G 10 ansieht, durch die zugelassen werden sollte, ausländische Telekommunikationsanschlüsse (etwa Telefonnummern oder E-Mail-Adressen) als sogenannte formale Suchbegriffe zu verwenden, nicht aber als Ausnahme zu dem Verbot des § 5 Abs. 2 Satz 2 Nr. 2 G 10, Suchbegriffe zu verwenden, die den Kernbereich betreffen (vgl. BTDrucks 16/12448, S. 11). 197

Jedoch schließt § 5 Abs. 2 Satz 3 G 10 auch nach der Gesetzentwurfsbegründung jedenfalls nicht hinreichend bestimmt und normenklar die Verwendung von Suchbegriffen aus, die den Kernbereich der privaten Lebensgestaltung betreffen. Denn die Auslegung nach Wortlaut und Systematik einerseits und die historische Auslegung andererseits stehen sich gegenüber und widersprechen sich, ohne dass der historischen Auslegung eindeutig der Vorrang zukommen würde. Damit wird § 5 Abs. 2 Satz 3 G 10 den besonders strengen Anforderungen an die Bestimmtheit und Normenklarheit bei der heimlichen Erhebung und weiteren Verarbeitung von Daten (ausführlich dazu oben Rn. 154) nicht gerecht. 198

(b) Nicht zu beanstanden ist demgegenüber der Kernbereichsschutz für deutsche Staatsangehörige und inländische Personen auf der Datenerhebungsebene gemäß § 5 Abs. 2 Satz 2 Nr. 2 und § 5a Satz 1 G 10. Bei der strategischen Inland-Ausland-Fernmeldeaufklärung sind auf der Ebene der Datenerhebung über das Verbot der gezielten Kernbereichserfassung hinausgehende gesetzliche Vorkehrungen nicht geboten (vgl. BVerfGE 154, 152 <264 Rn. 206>; ausführlich oben Rn. 167). Dieses Verbot der gezielten Kernbereichserfassung ist in § 5 Abs. 2 Satz 2 Nr. 2 und § 5a Satz 1 G 10 im Hinblick auf deutsche Staatsangehörige und inländische Personen hinreichend bestimmt und normenklar gesetzlich geregelt. Gegenüber diesen Personen dürfen nach § 5 Abs. 2 Satz 2 Nr. 2 G 10 keine Suchbegriffe verwendet werden, die den Kernbereich der privaten Lebensgestaltung betreffen. Zudem dürfen gemäß § 5a Satz 1 G 10 durch Beschränkungen nach § 1 Abs. 1 Nr. 2 G 10, also auch durch Maßnahmen der strategischen Inland-Ausland-Fernmeldeaufklärung, keine Kommunikationsinhalte aus dem Kernbereich privater Lebensgestaltung erfasst werden. 199

(5) Auch die Regelung in § 5 Abs. 2 Satz 6 G 10 über die Frist für die Löschung der Dokumentation der Durchführung der strategischen Inland-Ausland-Fernmeldeaufklärung wird den verfassungsrechtlichen Anforderungen nicht gerecht, denn sie ist zu kurz bemessen. 200

Nach § 5 Abs. 2 Satz 4 G 10 ist die Durchführung der strategischen Inland-Ausland-Fernmeldeaufklärung zu protokollieren. Auf diese Weise soll eine korrekte Handhabung der Überwachungsmaßnahmen durch eine lückenlose Dokumentation gewährleistet werden (vgl. BTDrucks 12/6853, S. 43 zum inhaltsgleichen § 3 Abs. 2 Satz 5 G 10 1994). Gemäß § 5 Abs. 2 Satz 6 G 10 ist diese Dokumentation am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen. 201

(a) Allerdings ist die Löschungsfrist des § 5 Abs. 2 Satz 6 G 10 ausreichend lang bemessen, um eine effektive objektivrechtliche Kontrolle durch die G 10-Kommission zu ermöglichen. Denn die G 10-Kommission, deren Kontrollbefugnis sich auf die gesamte Verarbeitung der nach dem Artikel 10-Gesetz erlangten personenbezogenen Daten erstreckt (vgl. § 15 Abs. 5 Satz 2 G 10), tritt mindestens einmal im Monat zusammen (vgl. § 15 Abs. 4 Satz 1 G 10). Angesichts dieser monatlichen Kontrollfrequenz liegen die Protokolldaten bei typisierender Betrachtung im Rahmen der nächsten periodisch anstehenden objektivrechtlichen Kontrolle durch die G 10-Kommission jeweils noch vor, bevor sie gemäß § 5 Abs. 2 Satz 6 G 10 zu löschen sind. 202

Zwar hat das Bundesverfassungsgericht eine gleichlautende Aufbewahrungsfrist, also die Löschung am Ende des Kalenderjahres, das dem Jahr der Protokollierung der Daten folgt, für zu kurz zur Durchführung auch der objektivrechtlichen Kontrolle angesehen (vgl. BVerfGE 141, 220 <302 f. Rn. 205, 323 Rn. 272>). Jedoch unterscheidet sich die Frequenz der objektivrechtlichen Kontrolle der strategischen Inland-Ausland-Fernmeldeaufklärung 203

durch die G 10-Kommission erheblich von der Häufigkeit der Kontrolle der Datenverarbeitung durch den Datenschutzbeauftragten nach dem Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten a.F. (BKAG a.F.), auf die sich das Urteil (BVerfGE 141, 220) bezog. Diesem Urteil lag nämlich die Annahme zugrunde, dass die Kontrolle durch den Datenschutzbeauftragten lediglich in Abständen von bis zu zwei Jahren durchzuführen waren (vgl. BVerfGE 141, 220 <285 Rn. 141>), also deutlich seltener als die monatlichen Kontrollen durch die G 10-Kommission.

(b) Demgegenüber ist die Löschungsfrist des § 5 Abs. 2 Satz 6 G 10 zu kurz, um den von der Überwachung Betroffenen effektiven subjektiven Rechtsschutz zu ermöglichen (vgl. BVerfGE 141, 220 <302 f. Rn. 205, 323 Rn. 272>). Bei typisierender Betrachtung ist nämlich nicht sichergestellt, dass die Daten der Protokollierung nach § 5 Abs. 2 Satz 4 G 10 noch vorhanden sind, wenn ein Betroffener von einer Überwachungsmaßnahme benachrichtigt wird. Denn die starre Löschungsfrist des § 5 Abs. 2 Satz 6 G 10, die im Zeitpunkt der Protokollierung zu laufen beginnt, nimmt keinen Bezug auf die Regelungen zur Benachrichtigung nach § 12 G 10. Dies wäre aber erforderlich, denn die Benachrichtigung erfolgt gemäß § 12 Abs. 2 Satz 1 in Verbindung mit Abs. 1 Satz 1 G 10 erst nach der endgültigen Einstellung der jeweiligen Maßnahme. Dass die Protokolldaten zu diesem Zeitpunkt der endgültigen Einstellung noch vorhanden sind, ist nicht sichergestellt. Denn zum einen kann die Beschränkungsanordnung – auch mehrfach – verlängert werden. Zum anderen kann die Benachrichtigung gemäß § 12 Abs. 2 in Verbindung mit Abs. 1 Satz 2 G 10 auch für einen längeren Zeitraum zurückgestellt werden, weil eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann oder weil der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist. In beiden Fallgruppen kann der Zeitpunkt der endgültigen Einstellung der Beschränkungsmaßnahme und damit der Benachrichtigung nach dem Ende des Kalenderjahres liegen, das dem Jahr der Protokollierung folgt. 204

Nichts anderes folgt daraus, dass das Bundesverwaltungsgericht in einer Entscheidung die Rechtsprechung des Bundesverfassungsgerichts zur Beeinträchtigung des subjektiven Rechtsschutzes durch starre Löschungsfristen (vgl. BVerfGE 141, 220 <302 f. Rn. 205, 323 Rn. 272>) als nicht auf die Löschungsfrist in § 5 Abs. 2 Satz 6 G 10 übertragbar angesehen hat (vgl. BVerwGE 157, 8 <17 Rn. 26>). Das Bundesverwaltungsgericht bezog sich auf Daten, die im Rahmen der strategischen Inland-Ausland-Fernmeldeaufklärung erfasst und unmittelbar nach Erfassung oder Relevanzprüfung wieder gelöscht wurden. Dabei stützte sich das Bundesverwaltungsgericht maßgeblich darauf, dass für diese unverzüglich gelöschten Daten gemäß § 12 Abs. 2 Satz 1 in Verbindung mit Abs. 1 G 10 keine Benachrichtigungspflicht bestehe, so dass der subjektive Rechtsschutz durch die starre Frist für die Löschung der Daten nicht beeinträchtigt werden könne (vgl. BVerwGE 157, 8 <13 ff. 205

Rn. 20 ff.>). Diese Entscheidung des Bundesverwaltungsgerichts ist auf solche Fälle, in denen die erhobenen Daten nicht unverzüglich gelöscht werden und deshalb eine Benachrichtigungspflicht nach § 12 Abs. 2 Satz 1 in Verbindung mit Abs. 1 G 10 besteht, nicht anwendbar. Vielmehr ist aufgrund der Fälle, in denen eine Benachrichtigungspflicht besteht, die Frist zur Löschung der Protokolldaten in § 5 Abs. 2 Satz 6 G 10 so zu bemessen, dass die Protokolle bei typisierender Betrachtung nach der Benachrichtigung der Betroffenen noch vorliegen, wie etwa in § 5a Satz 7 G 10.

Entgegen der Ansicht der Bundesregierung ist auch nicht hinreichend bestimmt und normenklar sichergestellt, dass die Löschung der Protokolldaten am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, unterbleibt, soweit die Daten für eine Mitteilung nach § 12 Abs. 2 G 10 oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Beschränkungsmaßnahme von Bedeutung sein könnten. Es fehlt insoweit an jeglichem normativen Anknüpfungspunkt für eine solche Ausnahme von der Löschungspflicht in § 5 Abs. 2 Satz 6 G 10. Insbesondere ist nicht ersichtlich, dass sich eine solche Ausnahme aus § 6 Abs. 1 Satz 6 G 10 ergeben könnte, denn diese Norm steht in einem anderen Regelungszusammenhang und bezieht sich nach seiner systematischen Stellung auf die Löschungspflichten in § 6 Abs. 1 G 10. Aufgrund der gegen eine Anwendbarkeit auf die Löschungspflicht in § 5 Abs. 2 Satz 6 G 10 sprechenden systematischen Auslegung wäre eine solche Ausnahme von der Löschungspflicht jedenfalls nicht hinreichend bestimmt und normenklar geregelt. 206

(6) Zudem wird die Ausgestaltung der unabhängigen objektivrechtlichen Kontrolle der strategischen Inland-Ausland-Fernmeldeüberwachung nach dem Artikel 10-Gesetz den besonders hohen verfassungsrechtlichen Anforderungen nicht in vollem Umfang gerecht. 207

(a) Zum einen sind die Mitglieder der G 10-Kommission nicht wie verfassungsrechtlich geboten hauptamtlich tätig. Als Ersatz für den in erheblichem Umfang eingeschränkten subjektiven Rechtsschutz gegen Maßnahmen der strategischen Auslandsfernmeldeaufklärung ist eine fachlich kompetente, professionalisierte gerichtsähnliche Kontrolle sicherzustellen, die materiell und verfahrensmäßig einer gerichtlichen Kontrolle gleichwertig, insbesondere mindestens ebenso wirkungsvoll ist (vgl. ausführlich oben Rn. 172). Dafür reicht es nicht aus, die Durchführung der Kontrolle im Wesentlichen auf eine ehrenamtliche Amtsausübung zu stützen (vgl. BVerfGE 154, 152 <295 Rn. 287>). Dem wird die gesetzliche Ausgestaltung in § 15 Abs. 1 Satz 4 G 10 nicht gerecht, denn danach haben die Mitglieder der G 10-Kommission lediglich ein öffentliches Ehrenamt inne. 208

(b) Zudem stellt das Artikel 10-Gesetz nicht sicher, dass eine richterliche Perspektive in der G 10-Kommission vertreten ist. Um die Gerichtsähnlichkeit der Kontrolle sicherzustellen, ist bei der Zusammensetzung des gerichtsähnlichen Kontrollorgans zu gewährleisten, dass die richterliche Perspektive in diesem Kontrollorgan vertreten ist. 209

Dies setzt voraus, dass dem gerichtsähnlichen Kontrollorgan auch Mitglieder mit richterlicher Erfahrung angehören (vgl. BVerfGE 154, 152 <295 Rn. 286>). Auch wenn das Parlamentarische Kontrollgremium in der Vergangenheit in der Praxis regelmäßig auch Richter zu Mitgliedern der G 10-Kommission bestellt hat, ist dies doch gesetzlich nicht vorausgesetzt. Nach § 15 Abs. 1 Satz 2 G 10 genügt insoweit, dass eine Mehrzahl der Mitglieder sowie deren Stellvertreter zwar die Befähigung zum Richteramt haben muss, aber nicht notwendig richterliche Erfahrung.

(c) Schließlich wird eine umfassende objektivrechtliche Kontrolle – und (soweit eröffnet) effektiver subjektiver Rechtsschutz Betroffener – deshalb nicht hinreichend ermöglicht, weil gesetzlich nicht sichergestellt ist, dass Beschränkungsanordnungen auch insoweit begründet werden, als es im Verwaltungsverfahren zu einer Änderung ihres Inhalts kommt. Zwar ist der Bundesnachrichtendienst gemäß § 9 Abs. 3 Satz 1 G 10 verpflichtet, seinen Antrag auf Anordnung einer Beschränkung zu begründen. Jedoch sieht das Artikel 10-Gesetz keine Pflicht zur Begründung vor, soweit das Bundesministerium des Innern und für Heimat bei Anordnung der Beschränkung gemäß § 10 G 10 Änderungen an dem Antrag des Bundesnachrichtendienstes vornimmt. Das zuständige Bundesministerium ist nach § 10 Abs. 2 Satz 1 G 10 lediglich verpflichtet, die beantragte Beschränkung schriftlich anzuordnen, Begründungserfordernisse sind hingegen gesetzlich nicht geregelt. 210

D.

I.

Im Ergebnis genügen die zulässig angegriffenen Normen den verfassungsrechtlichen Anforderungen nur teilweise. Die Verfassungsbeschwerde ist insoweit begründet. 211

Die Ermächtigung zur Datenerhebung und weiteren Datenverarbeitung im Wege der strategischen Inland-Ausland-Fernmeldeaufklärung nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 ist nicht mit Art. 10 Abs. 1 GG vereinbar, denn es fehlt eine hinreichende Regelung zur Aussonderung von Daten aus rein inländischen Telekommunikationsverkehren, der Kernbereichsschutz für ausländische Personen im Ausland in § 5 Abs. 2 Satz 3 in Verbindung mit Satz 2 Nr. 2 G 10 ist unzureichend, die Aufbewahrungsfrist für die Dokumentation der durchgeführten strategischen Inland-Ausland-Fernmeldeaufklärung in § 5 Abs. 2 Satz 6 G 10 ist zu kurz und die Ausgestaltung der objektivrechtlichen Kontrolle in § 15 G 10 unzureichend. 212

II.

1. Die Feststellung der Verfassungswidrigkeit gesetzlicher Vorschriften führt grundsätzlich zu deren Nichtigkeit. Allerdings kann sich das Bundesverfassungsgericht, wie sich aus 213

§ 31 Abs. 2 Sätze 2 und 3 BVerfGG ergibt, auch darauf beschränken, eine verfassungswidrige Norm nur für mit der Verfassung unvereinbar zu erklären. Es verbleibt dann bei einer bloßen Beanstandung der Verfassungswidrigkeit ohne den Ausspruch der Nichtigkeit. Die Unvereinbarkeitserklärung kann das Bundesverfassungsgericht dabei 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. Für die Übergangszeit kann das Bundesverfassungsgericht vorläufige Anordnungen treffen, um die Befugnisse der Behörden bis zur Herstellung eines verfassungsmäßigen Zustands durch den Gesetzgeber auf das zu reduzieren, was nach Maßgabe dieser Abwägung geboten ist (BVerfGE 141, 220 <351 Rn. 355> m.w.N.; stRspr).

2. a) Danach ist § 5 Abs. 1 Satz 3 Nr. 8 G 10 für mit der Verfassung unvereinbar zu erklären. 214
Die Gründe für die Verfassungswidrigkeit dieser Überwachungsermächtigung, soweit sie gerügt worden sind, betreffen nicht den Kern der mit ihr eingeräumten Befugnisse, sondern einzelne Aspekte ihrer rechtsstaatlichen Ausgestaltung. Der Gesetzgeber kann in diesen Fällen die verfassungsrechtlichen Beanstandungen nachbessern und damit den Kern der mit der Ermächtigung verfolgten Ziele auf verfassungsmäßige Weise verwirklichen.

Die Unvereinbarkeitserklärung ist mit der Anordnung ihrer vorübergehenden Fortgeltung 215
bis zum Ablauf des 31. Dezember 2026 zu verbinden. Die beanstandete Befugnis kann für die Sicherheit der Bundesrepublik Deutschland, insbesondere bei Berücksichtigung der potentiellen Dynamik bedrohlicher Entwicklungen unter den Bedingungen der Informationstechnik, auch kurzfristig große Bedeutung gewinnen (vgl. BVerfGE 154, 152 <311 Rn. 330>). Dies gilt insbesondere vor dem Hintergrund, dass sowohl die Anzahl der internationalen Cyberangriffe als auch deren Gefährdungspotential stetig zugenommen haben und aller Voraussicht nach weiter ansteigen werden (ausführlich dazu oben Rn. 182 f.). Deshalb ist eine befristete Fortgeltung zu bestimmen.

b) Die befristete Anordnung der Fortgeltung der Befugnis des § 5 Abs. 1 Satz 3 Nr. 8 G 10 216
bedarf jedoch mit Blick auf das Telekommunikationsgeheimnis einer einschränkenden Maßgabe. Sie ist an die Pflicht zur Aussonderung der Daten aus rein inländischen Telekommunikationsverkehren (bei denen alle Kommunikationsteilnehmenden deutsche Staatsangehörige oder Inländer sind) zu knüpfen. Daten aus rein inländischen Telekommunikationsverkehren sind – soweit technisch möglich – automatisiert herauszufiltern und unverzüglich automatisiert zu löschen, und entsprechende Daten, die trotz dieser automatisierten Filterung erhoben werden, sind unverzüglich zu löschen (vgl. Rn. 165). Außerdem dürfen auch gegenüber ausländischen Personen im Ausland keine Suchbegriffe, die den Kernbereich der privaten Lebensgestaltung betreffen, eingesetzt werden (vgl. Rn. 196 ff.). § 5 Abs. 2 Satz 3 G 10 findet deshalb in Bezug auf § 5 Abs. 2 Satz 2 Nr. 2 G 10 keine Anwendung.

Auf die Protokolldaten gemäß § 5 Abs. 2 Satz 5 G 10 findet statt § 5 Abs. 2 Satz 6 G 10 die Regelung aus § 6 Abs. 1 Sätze 6 und 7 G 10 Anwendung.

III.

Die Auslagenentscheidung im Verfahren 1 BvR 1743/16 beruht auf § 34a Abs. 2 BVerfGG. Im Verfahren 1 BvR 2539/16 folgt die Auslagenentscheidung aus § 34a Abs. 2 BVerfGG bezüglich der Teile der Verfassungsbeschwerde, über die zu entscheiden war und aus § 34 Abs. 3 BVerfGG, soweit die Beschwerdeführenden ihre Verfassungsbeschwerde für erledigt erklärt haben. Der Beschwerdeführer im Verfahren 1 BvR 1743/16 und die Beschwerdeführenden zu 1) und 5) im Verfahren 1 BvR 2539/16 haben jeweils überwiegend obsiegt. Hingegen haben die Beschwerdeführenden zu 2) bis 4) und 6) im Verfahren 1 BvR 2539/16 nur teilweise obsiegt. Insbesondere haben sie ihre Betroffenheit lediglich bezogen auf die Erfassung der Rohdatenströme ihrer Telekommunikationsverkehre – nicht aber bezüglich der weiteren nach § 5 Abs. 1 Satz 3 Nr. 8 G 10 zulässigen Eingriffe – hinreichend dargelegt. 217

Harbarth Ott Christ

Radtke Härtel Wolff

Eifert Meßling