Prof. Dr. Matthias Bäcker, LL.M.
…

Mannheim, den 29. Dezember 2022

Bundesverfassungsgericht
Schlossbezirk
76131 Karlsruhe

Verfassungsbeschwerde[1]

1. der Reporters sans frontières,
   ...,
   Französische Republik,
2. der Frau …,
   ...,
3. des Herrn …,
   ...,
4. des Herrn Goran Lefkov,
   ...,
5. der Frau Dragana Pećo,
   ...,
6. der Frau Sara Creta,
   ...,
7. der Frau Meron Estefanos,
   ...,
8. des Herrn Szabolcs Panyi,

[1] Dieses Dokument ist um Adressdaten und persönliche Informationen bereinigt. Es gibt den Verfahrensgegenstand wieder, wie er dem Bundesverfassungsgericht zur Entscheidung vorliegt.

...,

9. des Herrn Peter Verlinden,

...,

10. des Herrn Awil Mohamud Abdi,

...,

11. des Herrn Can Dündar,

...,

12. des Herrn ...,

...,

13. der Gesellschaft für Freiheitsrechte e.V.,
vertreten durch den Vorstand, bestehend aus Dr. Ulf Buermeyer, LL.M., Prof. Dr. Boris Burghardt und Prof. Dr. Nora Markard, MA,
Boyenstr. 41, 10115 Berlin,

14. der Reporter ohne Grenzen e.V.,
vertreten durch den Geschäftsführer Christian Mihr,
Potsdamer Str. 144, 10783 Berlin,

15. des Herrn Dr. Ulf Buermeyer, LL.M.,

...,

16. des Herrn Martin Kaul,

...,

17. der Frau Prof. Dr. Nora Markard, MA,

...,

18. des Herrn Christian Mihr,

...,

19. des Herrn Dr. Kerem Schamberger,

…

20. der Frau Eva Schulz,

…

g e g e n

§ 19 Abs. 4 Nr. 1 lit. e und Nr. 2 lit. d, Abs. 7 Satz 1 Nr. 3, Abs. 8,

§ 20 Abs. 1,

§ 21 Abs. 1 Satz 1,

§ 23 Abs. 5 Satz 2, Abs. 6 Satz 2,

§ 24 Abs. 7 Satz 1 und 2,

§ 26,

§ 29 Abs. 1, Abs. 2, Abs. 3, Abs. 4 Nr. 1, Abs. 5, Abs. 6 Satz 1,

§ 30 Abs. 1, Abs. 2, Abs. 6, Abs. 9,

§ 31 Abs. 1 Satz 2 Nr. 3 und Satz 3, Abs. 3, Abs. 5 Nr. 5, 6, 8, 9 und 11,

§ 34 Abs. 2, Abs. 3, Abs. 5, Abs. 6 Satz 3,

§ 36 Abs. 1, Abs. 3,

§ 38 Abs. 1, Abs. 2, Abs. 3, Abs. 5, Abs. 6,

§ 39 Abs. 1, Abs. 2, Abs. 6,

§ 59 Abs. 2 Satz 1

des Gesetzes über den Bundesnachrichtendienst in der Fassung des Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts vom 19. April 2021 (BGBl I S. 771).

Namens und in Vollmacht der Beschwerdeführerinnen und Beschwerdeführer **(Anlage)** erhebe ich Verfassungsbeschwerde. Ich rüge Verletzungen der Menschenwürdegarantie in ihrer Ausprägung als Schutz des Kernbereichs privater Lebensgestaltung (Art. 1 Abs. 1 GG), des Rechts auf informationelle Selbstbestimmung sowie des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 GG), des allgemeinen Gleichheitssatzes (Art. 3 Abs. 1 GG) und des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG).

Ich rege an, zur Klärung von Fragen der Auslegung der Charta der Grundrechte der Europäischen Union, die durch einige der vorgebrachten Rügen aufgeworfen werden, ein Vorabentscheidungsverfahren vor dem Gerichtshof der Europäischen Union (Art. 267 AEUV) durchzuführen.

....

Gliederung

Überblick

Die Verfassungsbeschwerde richtet sich gegen die gesetzlichen Ermächtigungen des Bundesnachrichtendienstes zur strategischen Überwachung der ausländischen Telekommunikation (sogenannte strategische Ausland-Fernmeldeaufklärung) sowie zu Online-Durchsuchungen im Ausland.

Soweit die Verfassungsbeschwerde die strategische Ausland-Fernmeldeaufklärung zum Gegenstand hat, knüpft sie an das erledigte Verfahren 1 BvR 2835/17 an, das zu dem Urteil des Bundesverfassungsgerichts zur (damals sogenannten) Ausland-Ausland-Fernmeldeaufklärung vom 19. Mai 2020 führte. Die Beschwerdeführerin zu 1 und der Beschwerdeführer zu 4 waren bereits an diesem Verfahren beteiligt. Die mit der vorliegenden Verfassungsbeschwerde erhobenen Rügen lassen sich grob in zwei Kategorien einteilen:

Erstens rügt die Verfassungsbeschwerde, dass der Gesetzgeber bei der Neuregelung der strategischen Ausland-Fernmeldeaufklärung die in dem Urteil des Bundesverfassungsgerichts vom 19. Mai 2020 herausgearbeiteten verfassungsrechtlichen Vorgaben missachtet oder nur defizitär umgesetzt hat. In diese Kategorie fallen die Rügen betreffend das Ausmaß der Überwachung, die zulässigen Ziele einer Überwachung zur Gefahrenfrüherkennung, den Schutz von Inländerinnen und Inländern sowie von Vertraulichkeitsbeziehungen, die Details der bevorratenden Speicherung von Verkehrsdaten, die Kontrolle der Überwachung, die Übermittlung der durch eine Überwachung erlangten Daten an andere Stellen im In- und Ausland sowie die Kooperation des Bundesnachrichtendienstes mit ausländischen Nachrichtendiensten.

Zweitens wirft die Verfassungsbeschwerde Fragen auf, die nicht Gegenstand des Verfahrens 1 BvR 2835/17 waren, in dem Urteil vom 19. Mai 2020 noch offengelassen wurden oder einer Neubewertung bedürfen.

Neue verfassungsrechtliche Fragen betreffen die Benachrichtigung inländischer Betroffener einer Überwachungsmaßnahme, die Weiterverarbeitung von Daten, die der Bundesnachrichtendienst durch eine sogenannte Eignungsprüfung erlangt hat, sowie das Zusammenwirken des Bundesnachrichtendienstes mit der Bundeswehr bei der strategischen Ausland-Fernmeldeaufklärung.

In dem Urteil vom 19. Mai 2020 blieb offen, inwieweit Unionsbürgerinnen und Unionsbürger sowie juristische Personen des EU-ausländischen Rechts von Verfassungs wegen einen besonderen Überwachungsschutz genießen müssen, der dem Schutz von Inländerinnen und Inländern gleichkommt. Diese Frage ist nunmehr zu entscheiden.

Eine Neubewertung erscheint den Beschwerdeführerinnen und Beschwerdeführern hinsichtlich der bevorratenden Speicherung von Verkehrsdaten angezeigt. Die jüngste Rechtsprechung des Gerichtshofs der Europäischen Union zu den Unionsgrundrechten enthält gewichtige Anhaltspunkte dafür, dass insoweit ein strengerer Maßstab anzulegen ist als in dem Urteil vom 19. Mai 2020.

Schließlich betritt die Verfassungsbeschwerde Neuland auch insoweit, als sie Online-Durchsuchungen im Ausland zum Gegenstand hat. Die angegriffenen Regelungen stellen erstmals eine ausdrückliche gesetzliche Ermächtigung hierzu bereit. Diese Regelungen konzipieren die Online-Durchsuchung im Ausland parallel zur strategischen Ausland-Fernmeldeaufklärung als strategische Überwachungsmaßnahme, die ohne konkreten Anlass durchgeführt werden darf und im Wesentlichen nur durch ihr Ziel konturiert wird, bestimmte Erkenntnisse zu beschaffen. Die Verfassungsbeschwerde geht demgegenüber davon aus, dass eine individualisierende Überwachungsmaßnahme wie die Online-Durchsuchung auch im Ausland nur bei einem hinreichend verfestigten konkreten Anlass zugelassen werden darf. Darüber hinaus wendet sich die Verfassungsbeschwerde gegen die Regelungen zu den Betroffenen von Online-Durchsuchungen, zum Schutz des Kernbereichs privater Lebensgestaltung sowie zur Übermittlung der durch eine Online-Durchsuchung erlangten Daten.

A. Sachverhalt

Gegenstand der Verfassungsbeschwerde sind Ermächtigungen des Bundesnachrichtendienstes zu technischen Überwachungsmaßnahmen und zur Weiterverarbeitung der hierdurch erlangten Daten sowie zugehörige Verfahrensregelungen.

I. Angegriffene Vorschriften

Die angegriffenen Regelungen wurden durch das Gesetz zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts vom 19. April 2021 in das Gesetz über den Bundesnachrichtendienst (im Folgenden: BNDG) eingefügt. Die Gesetzesänderung verfolgte im Wesentlichen zwei Ziele:

Erstens sollte die strategische Überwachung der Telekommunikation von Ausländern im Ausland (nunmehr als strategische Ausland-Fernmeldeaufklärung bezeichnet) neu geregelt werden, um diese Überwachungsbefugnis an die verfassungsrechtlichen Maßstäbe anzupassen, die das Bundesverfassungsgericht in seinem Urteil zu der früheren Ausland-Ausland-Fernmeldeaufklärung vom 19. Mai 2020 (Az. 1 BvR 2835/17) herausgearbeitet hatte. Dies erforderte eine grundlegende Neukonzeption der Überwachung. Denn das Bundesverfassungsgericht hatte in diesem Urteil die früheren Regelungen, die maßgeblich auf der unzutreffenden Prämisse beruhten, das Fernmeldegeheimnis des Art. 10 GG erfasse die ausländische Telekommunikation nicht, praktisch umfassend beanstandet.

In diesem Zusammenhang sollte eine gesetzliche Grundlage für die seit längerem bestehende Praxis des Bundesnachrichtendienstes geschaffen werden, die bei strategischen Telekommunikationsüberwachungen miterfassten Verkehrsdaten der inländischen Telekommunikation in unkenntlich gemachter Form für Analysezwecke in einer Datenbank zu speichern. Das Bundesverwaltungsgericht hatte diese Praxis in zwei weitgehend gleichlautenden Entscheidungen vom 13. Dezember 2017 (Az. 6 A 6.16 und 6 A 7.16) mit der Begründung beanstandet, es fehle an der erforderlichen formellgesetzlichen Ermächtigung.

Zweitens sollte erstmals eine gesetzliche Ermächtigung für verdeckte Zugriffe auf informationstechnische Systeme von Ausländern im Ausland durch den Bundesnachrichtendienst (sogenannte Online-Durchsuchung) geschaffen werden. Insoweit handelte der Gesetzgeber, ohne hierzu durch eine Gerichtsentscheidung gezwungen worden zu sein. Nach der Gesetzesbegründung

ging es auch hierbei um die gesetzliche Absicherung einer bereits bestehenden Praxis des Bundesnachrichtendienstes,

BT-Drs. 19/26103, S. 93.

Die Verfassungsbeschwerde richtet sich gegen Normen aus beiden Regelungskomplexen. Die folgende Darstellung der Rechtsgrundlagen für die strategische Ausland-Fernmeldeaufklärung und die Online-Durchsuchung beschränkt sich auf die Vorschriften, die Gegenstand der Verfassungsbeschwerde sind. Andere Regelungen werden nur insoweit einbezogen, als dies zum Verständnis der angegriffenen Vorschriften unerlässlich ist.

1. Strategische Ausland-Fernmeldeaufklärung

Die Regelungen über die strategische Ausland-Fernmeldeaufklärung finden sich in §§ 19 ff. BNDG. Die zentrale Vorschrift in § 19 BNDG enthält die Überwachungsermächtigungen. Sie sieht eine Gliederung der strategischen ausland-Fernmeldeaufklärung in Überwachungsprojekte vor, die durch Angaben zum Aufklärungszweck, zum Aufklärungsthema, zum geografischen Fokus und zur Dauer der Überwachung einzugrenzen sind. Das Gesamtvolumen der Überwachung ist dabei auf nicht mehr als 30 Prozent der bestehenden Telekommunikationsnetze zu begrenzen, um eine unzulässige unbeschränkte Überwachung auszuschließen.

In Anlehnung an das Urteil des Bundesverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung differenziert § 19 BNDG hinsichtlich des Aufklärungszwecks zwischen Überwachungen zur politischen Unterrichtung der Bundesregierung und zur Früherkennung von aus dem Ausland drohenden Gefahren von internationaler Bedeutung. Überwachungen zur politischen Unterrichtung sind generell zulässig, um Informationen über das Ausland von außen- und sicherheitspolitischer Bedeutung zu gewinnen. Überwachungen zur Gefahrenfrüherkennung müssen darüber hinaus dazu dienen, Erkenntnisse mit Bezug zu bestimmten Gefahrenbereichen oder zum Schutz bestimmter Rechtsgüter zu gewinnen, die jeweils in einem Katalog abschließend aufgeführt sind.

Der Bundesnachrichtendienst darf im Rahmen der strategischen Ausland-Fernmeldeaufklärung Inhaltsdaten der Telekommunikation nur anhand von Suchbegriffen erheben. Unzulässig ist zudem eine Erhebung von Inhaltsdaten, die sich auf deutsche Staatsangehörige, inländische juristische Personen und sich im Bundesgebiet aufhaltende Personen beziehen. Soweit der Bundesnachrichtendienst solche Daten gleichwohl erhebt – insbesondere weil sich ihre Miterhebung technisch nicht durchweg ausschließen lässt –, hat er sie

grundsätzlich unverzüglich zu löschen. Der gegen strategische Überwachungen grundsätzlich abgeschirmte Personenkreis wird im Folgenden mit dem Oberbegriff „Inländerinnen und Inländer“ bezeichnet.

In §§ 20 ff. BNDG finden sich Regelungen zum Schutz weiterer Personenkreise und bestimmter Kommunikationsinhalte. Bedeutsam für diese Verfassungsbeschwerde ist zum einen § 20 Abs. 1 BNDG, der Unionsbürgerinnen und Unionsbürgern einen begrenzten Überwachungsschutz vermittelt. Zum anderen richtet sich die Verfassungsbeschwerde gegen § 21 BNDG, der bestimmte Vertraulichkeitsbeziehungen schützt.

§ 24 BNDG befasst sich mit sogenannten Eignungsprüfungen. Hierbei handelt es sich um Datenerhebungen aus Telekommunikationsnetzen, mit deren Hilfe der Bundesnachrichtendienst geeignete Telekommunikationsnetze oder geeignete Suchbegriffe für strategische Telekommunikationsüberwachungen bestimmt. Eine Eignungsprüfung dient also nicht unmittelbar der nachrichtendienstlichen Aufklärung, und der Bundesnachrichtendienst darf die dabei erhobenen Daten grundsätzlich nicht zur Generierung nachrichtendienstlicher Erkenntnisse nutzen. Ausnahmsweise darf der Bundesnachrichtendienst die Daten weiterverarbeiten, wenn eine erhebliche Gefahr für bestimmte Rechtsgüter besteht. Darüber hinaus darf er die Daten in weitem Umfang manuell oder automatisiert an die Bundeswehr weiterleiten.

Die Verarbeitung von Verkehrsdaten, die der Bundesnachrichtendienst im Rahmen einer strategischen Aufklärungsmaßnahme erhebt, ist gesondert in § 26 BNDG geregelt. Anders als für Inhaltsdaten verlangt die Norm nicht, dass der erfasste Datenstrom bei der Erhebung anhand von Suchbegriffen reduziert wird. Der Bundesnachrichtendienst darf die erfassten Verkehrsdaten der ausländischen Telekommunikation vielmehr gesamthaft bevorraten und bis zu sechs Monate lang speichern, wobei er diese Frist überschreiten kann, soweit die Speicherung zur Aufgabenerfüllung weiterhin erforderlich ist. Darüber hinaus genießen Inländerinnen und Inländer zwar auch gegenüber der Weiterverarbeitung von Verkehrsdaten einen grundsätzlichen Überwachungsschutz. Jedoch darf der Bundesnachrichtendienst inländische Verkehrsdaten bevorraten, wenn sie im Rahmen des automatisierten Informationsaustausches zwischen informationstechnischen Systemen ohne unmittelbaren Bezug zu einem konkreten menschlichen Kommunikationsvorgang anfallen. Zudem darf er sämtliche Verkehrsdaten der inländischen Telekommunikation speichern, wenn er sie unverzüglich nach der Erhebung automatisiert unkenntlich macht. § 26 BNDG sieht im Übrigen hinsichtlich der Bevorratung von Verkehrsdaten

keinen besonderen Überwachungsschutz für Unionsbürgerinnen und Unionsbürger oder für Vertraulichkeitsbeziehungen vor.

Gemäß § 29 und § 30 BNDG darf der Bundesnachrichtendienst die bei der strategischen Ausland-Fernmeldeaufklärung erhobenen Daten an zahlreiche Stellen im In- und Ausland übermitteln. Die Übermittlungsvoraussetzungen sind abhängig von dem Überwachungszweck (politische Unterrichtung oder Gefahrenfrüherkennung) und dem Zweck der Übermittlung differenziert geregelt. An die Bundeswehr darf der Bundesnachrichtendienst Daten auch automatisiert übermitteln, sofern die Daten aus Aufklärungsmaßnahmen mit Bezug zu den Aufgaben der Bundeswehr (Landes- oder Bündnisverteidigung, Einsätze im Ausland) oder zum Schutz von Leib, Leben oder Freiheit einer Person stammen. Die materiellen Übermittlungsermächtigungen werden durch prozedurale Schutzregelungen flankiert, die unter anderem die Zweckbindung der übermittelten Daten absichern und im Fall von Auslandsübermittlungen eine menschenrechtswidrige Datenverwendung verhüten sollen.

Nach §§ 31 ff. BNDG darf der Bundesnachrichtendienst bei der strategischen Ausland-Fernmeldeaufklärung mit ausländischen öffentlichen Stellen kooperieren. Die Einzelheiten der Kooperation sind im Voraus zwischen dem Bundesnachrichtendienst und dem Kooperationspartner in einer Absichtserklärung schriftlich niederzulegen. Eine Kooperation ist zulässig, um erhebliche Gefahren für die innere oder äußere Sicherheit der Bundesrepublik, die Verteidigung oder das Gemeinwohl zu erkennen, die außen- und sicherheitspolitische Handlungsfähigkeit der Bundesrepublik zu wahren oder die Aufgabenerfüllung durch den Bundesnachrichtendienst sicherzustellen. Zudem muss der Zweck der Kooperation darauf gerichtet sein, Informationen über bestimmte Gefahrenbereiche zu gewinnen. Wegen des Schutzes von Unionsbürgerinnen und Unionsbürgern sowie von Vertraulichkeitsbeziehungen verweisen die Kooperationsermächtigungen weitgehend auf die für Überwachungen (allein) durch den Bundesnachrichtendienst geltenden Schutzregelungen in §§ 20 ff. BNDG.

Zur Kontrolle der Überwachung errichten §§ 40 ff. BNDG ein zweigliedriges Kontrollregime, das institutionell unter dem Dach des Unabhängigen Kontrollrats zusammengeführt wird. Der Unabhängige Kontrollrat untergliedert sich in ein gerichtsähnliches und ein administratives Kontrollorgan, deren Aufgaben und Befugnisse jeweils differenziert geregelt sind. Die Kontrollzuständigkeiten des gerichtsähnlichen Kontrollorgans sind in § 42 BNDG aufgezählt, wobei teilweise eine obligatorische Vorabkontrolle, teilweise eine begleitende und stichprobenartige Kontrolle vorgesehen ist. Der Bundesnachrichtendienst ist

gemäß § 56 BNDG verpflichtet, den Unabhängigen Kontrollrat zu unterstützen, was Befugnisse des Unabhängigen Kontrollrats zur Einsichtnahme in Akten und Dateien, zum Zugang zu Dienststellen und informationstechnischen Systemen sowie zu Befragungen und Auskunftsersuchen gegenüber Mitarbeiterinnen und Mitarbeitern des Bundesnachrichtendienstes einschließt. Im Übrigen regelt der Unabhängige Kontrollrat sein Vorgehen gemäß § 41 Abs. 5 BNDG in einer Geschäftsordnung und in einer Verfahrensordnung.

2. Online-Durchsuchung

Die Regelungen über Online-Durchsuchungen durch den Bundesnachrichtendienst finden sich in §§ 34 ff. BNDG. Die Eingriffsermächtigungen sind in § 34 BNDG geregelt, der – parallel zu den Regelungen über die strategische Ausland-Fernmeldeaufklärung – zwischen Überwachungsmaßnahmen zur politischen Unterrichtung und zur Gefahrenfrüherkennung differenziert. Die Überwachungsvoraussetzungen lehnen sich gleichfalls an § 19 BNDG an, werden allerdings jeweils qualifiziert. Eine Online-Durchsuchung zur politischen Unterrichtung ist zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass sie der Gewinnung von Informationen von herausgehobener außen- und sicherheitspolitischer Bedeutung dienen, mit deren Aufklärung das Bundeskanzleramt den Bundesnachrichtendienst beauftragt hat. Eine Maßnahme zur Gefahrenfrüherkennung setzt voraus, dass Tatsachen die Annahme rechtfertigen, dass sie der Gewinnung von Informationen dient, mit deren Aufklärung das Bundeskanzleramt den Bundesnachrichtendienst beauftragt hat, und durch sie Erkenntnisse über Gefahren nach dem Katalog des § 19 Abs. 4 BNDG in Fällen von herausgehobener außen- und sicherheitspolitischer Bedeutung gewonnen werden.

Eine Online-Durchsuchung zum Zweck der Gefahrenfrüherkennung darf sich zudem nur gegen Personen richten, hinsichtlich derer tatsächliche Anhaltspunkte dafür vorliegen, dass sie Gefahren verursachen, für einen Gefahrverursacher Kommunikation vermitteln oder ein Gefahrverursacher ihr informationstechnisches System benutzt. Im Übrigen dürfen Online-Durchsuchungen auch durchgeführt werden, wenn andere Personen oder Informationssysteme unvermeidbar mitbetroffen werden. Unzulässig ist allerdings eine Datenerhebung über deutsche Staatsangehörige, inländische juristische Personen und sich im Bundesgebiet aufhaltende Personen. Hingegen gibt es – anders als bei der strategischen Ausland-Fernmeldeaufklärung – keine besondere Regelung zum Schutz von Unionsbürgerinnen und Unionsbürgern.

§ 36 BNDG enthält prozedurale Vorgaben zum Schutz des Kernbereichs privater Lebensgestaltung. Eine Datenerhebung zum Zweck der Erlangung von

Erkenntnissen zum Kernbereich ist unzulässig. Im Übrigen ist der Kernbereichsschutz bei der Weiterverarbeitung der erhobenen Daten sicherzustellen. In Zweifelsfällen darf der Bundesnachrichtendienst die Daten erst nach einer Prüfung durch den Unabhängigen Kontrollrat weiterverarbeiten.

In § 38 und § 39 BNDG finden sich Ermächtigungen zur Übermittlung der Daten aus Online-Durchsuchungen an in- und ausländische Stellen. Diese Regelungen sind weitgehend den Übermittlungsermächtigungen im Zusammenhang mit der strategischen Ausland-Fernmeldeaufklärung nachgebildet. Teils sind die Ermächtigungen wortlautidentisch, teils enthalten die Übermittlungstatbestände für Daten aus Online-Durchsuchungen qualifizierte Voraussetzungen. Die flankierenden prozeduralen Vorgaben für Übermittlungen im Zusammenhang mit der Ausland-Fernmeldeaufklärung sind entsprechend anzuwenden.

II. Beschwerdeführerinnen und Beschwerdeführer

1. Beschwerdeführerin zu 1: Reporters sans frontières

Die 1985 gegründete Beschwerdeführerin zu 1 ist ein rechtsfähiger Verein französischen Rechts (Association Loi de 1901). Sie bildet die Dachorganisation eines internationalen Netzwerks, dessen Ziel darin besteht, Verstöße gegen die Presse- und Informationsfreiheit weltweit zu dokumentieren und mehr Sicherheit und besseren Schutz für Journalistinnen und Journalisten zu erreichen,

> vgl. zum Folgenden die Selbstdarstellung der Beschwerdeführerin unter https://rsf.org/fr/presentation-0 (letzter Abruf am 23. Dezember 2022).

Zu den Tätigkeiten der Beschwerdeführerin zählen die Veröffentlichung allgemeiner Informationen zum Stand der Pressefreiheit, etwa durch die jährliche Herausgabe des sogenannten Classement mondial de la liberté de la presse/World Press Freedom Index,

> vgl. https://rsf.org/fr/ranking (letzter Abruf am 23. Dezember 2022),

die Alarmierung der Öffentlichkeit bei konkreten Bedrohungen der Pressefreiheit sowie die Unterstützung verfolgter Journalistinnen und Journalisten und ihrer Familien. Der Schwerpunkt dieser zuletzt genannten Nothilfetätigkeit liegt auf der Hilfe in den Herkunftsländern der Betroffenen. Sie soll den Betroffenen helfen, damit diese ihre journalistische Tätigkeit weiterführen oder wiederaufnehmen können. Hierzu ersetzt die Beschwerdeführerin etwa zerstörte oder

beschlagnahmte Ausrüstung, vermittelt und finanziert anwaltliche Unterstützung oder hinterlegt Kautionen zur Haftverschonung. Nach Misshandlungen oder Anschlägen ermöglicht die Beschwerdeführerin den betroffenen Journalistinnen und Journalisten eine medizinische Behandlung. Bei Arbeitsverboten oder Entlassungen sorgt sie für eine finanzielle Überbrückung und unterstützt die Angehörigen der betroffenen Journalistinnen und Journalisten.

Die Beschwerdeführerin beschäftigt an ihrem Sitz in Paris 45 Mitarbeiterinnen und Mitarbeiter. Sie unterhält ständige Kontakte zu insgesamt 12 weiteren rechtlich eigenständigen Büros oder Sektionen in anderen Ländern sowie zu mehr als 130 individuellen Korrespondentinnen und Korrespondenten weltweit. Bei diesen Korrespondentinnen und Korrespondenten handelt es sich in der Regel um investigativ tätige Journalistinnen und Journalisten, von denen die Beschwerdeführerin Informationen über die Arbeitsbedingungen für Journalistinnen und Journalisten in dem jeweiligen Land bezieht, die sie für ihre laufende Analysearbeit benötigt.

Die Mitarbeiterinnen und Mitarbeiter der Beschwerdeführerin nutzen in deren Auftrag und Namen zahlreiche elektronische Kommunikationsdienste wie Sprachtelefonie, E-Mail, Instant Messaging (…) und Videokonferenzdienste (…) in großem Umfang. Insbesondere gilt dies für die Kontakte mit den Korrespondentinnen und Korrespondenten sowie im Rahmen der Nothilfetätigkeit der Beschwerdeführerin für verfolgte Journalistinnen und Journalisten. Sowohl für die Kontaktaufnahme zu diesen Journalistinnen und Journalisten selbst und ihren Angehörigen als auch für die Kommunikation mit weiteren Stellen in den Herkunftsstaaten verfolgter Person wie Anwaltskanzleien, Ärztinnen und Ärzten, Kreditinstituten oder staatlichen Einrichtungen des Herkunftsstaates bedient sich die Beschwerdeführerin praktisch ausschließlich elektronischer Kommunikationsdienste. Gerade diese Kommunikation ist angesichts der bedrohten Lage der jeweils verfolgten Journalistin oder des verfolgten Journalisten auf besondere Vertraulichkeit angewiesen, um eine wirksame Nothilfe leisten zu können. Würde vorzeitig bekannt, dass die Beschwerdeführerin eine bestimmte Journalistin oder einen bestimmten Journalisten unterstützt und an wen sich die Beschwerdeführerin hierzu wendet, so könnte dies ihre Hilfsbemühungen vereiteln und schlimmstenfalls die betroffene Person sogar noch schwereren Bedrohungen bis hin zu Gefahren für Leib und Leben aussetzen.

Darüber hinaus nutzen die Beschwerdeführerin und ihre Mitarbeiterinnen und Mitarbeiter zur Außendarstellung verschiedene soziale Medien (Twitter, Facebook, LinkedIn und YouTube). Auch um Büroarbeiten zu erledigen, finanzielle

Transaktionen abzuwickeln und Reisen zu planen und durchzuführen, bedienen sich die Beschwerdeführerin und ihre Mitarbeiterinnen und Mitarbeiter internetbasierter Dienste wie …, diverser Online-Banking-Apps und Google Maps.

2. Beschwerdeführerin zu 2: ...

Die Beschwerdeführerin zu 2 ist … als freiberufliche Journalistin tätig …. Ihre Tätigkeitsschwerpunkte bilden Berichte über Gerichtsverfahren in Äußerungssachen einschließlich Verfahren gegen Journalistinnen und Journalisten, Massenproteste in der Türkei und die Bewältigung genozidaler Gewalt

...

3. Beschwerdeführer zu 3: ...

Der Beschwerdeführer zu 3 ...

war als Menschenrechtsaktivist einer der Anführer der Proteste in Hongkong ...

….

4. Beschwerdeführer zu 4: Goran Lefkov

Der Beschwerdeführer zu 4 ist nordmazedonischer Staatsbürger und lebt im Osten des Landes. Er arbeitet als freiberuflicher Journalist und ist größtenteils für die Nichtregierungsorganisation Scoop tätig, die als Teil eines internationalen Netzwerks investigativen Journalismus und Recherchen unterstützt und fördert. Scoop veröffentlicht eigene Rechercheergebnisse, die auch von allen großen Medien in Nordmazedonien aufgegriffen werden und so eine hohe Reichweite erzielen,

> vgl. http://en.scoop.mk/about-us (letzter Abruf am 23. Dezember 2022).

...

5. Beschwerdeführerin zu 5: Dragana Pećo

Die Beschwerdeführerin zu 5 ist serbische Staatsangehörige und lebt ... in Nordserbien. Sie ist beruflich als investigative Journalistin tätig. Im Jahr 2015 gründete die Beschwerdeführerin zusammen mit Kolleginnen und Kollegen das Berichterstattungsnetzwerk KRIK, das auf die Berichterstattung über organisierte Kriminalität und Korruption spezialisiert ist. ...

6. Beschwerdeführerin zu 6: Sara Creta

Die Beschwerdeführerin zu 6 ist italienische Staatsangehörige und lebt in …. Sie arbeitet international als Fotojournalistin und Dokumentarfilmerin. ...

Einen Arbeitsschwerpunkt der Beschwerdeführerin bilden Fluchtbewegungen nach Mitteleuropa, insbesondere über das Mittelmeer. ...

7. Beschwerdeführerin zu 7: Meron Estefanos

Die Beschwerdeführerin zu 7 ist schwedische Staatsangehörige mit eritreischen Wurzeln und lebt …. Sie ist Journalistin und Menschenrechtsaktivistin. Ihre Beiträge erscheinen zum einen auf dem eritreischen Online-Exilmedium Asmarino, zum anderen auf internationalen Medienkanälen wie This American Life, NDR und Deutschlandfunk. Sie ist zudem als Moderatorin bei dem eritreischen Exilradiosender Radio Erena tätig. Die Beschwerdeführerin ist Mitbegründerin der International Commission on Eritrean Refugees, einer Unterstützungsorganisation für eritreische Flüchtlinge, Opfer von Menschenhandel und Folteropfer. Sie hat sich an zahlreichen Studien, Büchern und wissenschaftlichen Veröffentlichungen zum Menschenhandel beteiligt. In den letzten Jahren hat die Beschwerdeführerin ein Netzwerk von Zeugenberichten und Quellen zum Menschenhandel aufgebaut, das einen Schwerpunkt auf die Lebensbedingungen von Personen legt, die vom Horn von Afrika nach Europa migriert sind,

> vgl. https://asmarino.com/articles/1042-eritrea-20-years-after-independence-the-largest-refugee-producing-country-in-the-world; https://www.ndr.de/nachrichten/info/sendungen/das_feature/diejaegerin,diejaegerin102.html; https://assets.deutschlandfunk.de/dc34255b-327f-4ff1-accd-9833bd29b949/original.pdf; https://www.hertie-school.org/en/events/event-detail/event/europes-deadly-borders-seeking-protection-in-bordered-europe-1 (letzte Abrufe am 23. Dezember 2022).

Die Beschwerdeführerin hat für ihr Werk zahlreiche Preise erhalten und wurde für weitere Auszeichnungen nominiert,

> vgl. https://everydayrebellion.net/everyday-rebellion-videoblog-freedom-friday-movement-in-eritrea; https://asmarino.com/alewana/1246-journalist-meron-estefanos-received-isaak-prize-of-national-press-clubs-western-circuit; https://rsf.org/sites/default/files/update_3_-_rsf_sweden_-_report_-_priso-

ner_of_conscience_since_2001.pdf; https://moviesthatmatter.nl/en/film/sound-of-torture (letzte Abrufe am 23. Dezember 2022).

Seit 2011 ist die Beschwerdeführerin auch praktisch als Menschenrechtsaktivistin für eritreische Flüchtlinge tätig, die auf der Flucht vielfach – etwa auf der Sinai-Halbinsel oder in Libyen – gefangen genommen, misshandelt und als Geiseln genommen werden. Sie reist zu diesem Zweck in die betroffenen Staaten, um sich vor Ort für diese Menschen einzusetzen. Die Beschwerdeführerin hat zudem mit den von ihr zusammengetragenen Informationen unter anderem zu strafrechtlichen Ermittlungen beigetragen, etwa den von niederländischen Behörden und Interpol seit 2017 betriebenen Ermittlungen gegen einen Menschenhändler namens Kidane,

https://africasacountry.com/2013/09/they-beg-to-be-called-refugees-but-israel-calls-them-infiltrators; https://podcasts.apple.com/lv/podcast/episode-14-with-meron-estefanos-the-sound-of-torture-eng/id1534594274?i=1000530376732; https://www.reuters.com/article/ethiopia-trafficking-court-idAFL5N2NY13J (letzte Abrufe am 23. Dezember 2022).

Im Jahr 2015 setzte sich die Beschwerdeführerin für Medhanie Berhe ein, der in Italien wegen einer Verwechslung zu Unrecht wegen Schleusungsdelikten beschuldigt wurde. Sie informierte die Strafverfolgungsbehörden über den tatsächlichen Schleuser, Medhanie Mered, der sie daraufhin kontaktierte und sich von ihr interviewen ließ. In diesem Zusammenhang befragten die Strafverfolgungsbehörden die Beschwerdeführerin und konfrontierten sie mit Inhalten vertraulicher Äußerungen, die sie am Telefon gemacht hatte. Die Beschwerdeführerin geht daher davon aus, dass ihre Telekommunikation in diesem Zeitraum abgehört wurde,

vgl. https://www.wienerzeitung.at/nachrichten/chronik/welt/856961-Verwechslung-bei-Verhaftung-von-Schlepperkoenig-aus-Eritrea.html; https://www.theguardian.com/world/2016/jul/03/eritrean-smuggler-trial-sicily-wrong-man-say-former-victims (letzte Abrufe am 26. Dezember 2022).

Die Beschwerdeführerin nutzt für ihre Arbeit ständig elektronische Kommunikationsmittel wie Sprachtelefonie, E-Mail und Instant Messaging (…). Sie hat darüber hinaus Profile auf den sozialen Medien Twitter und YouTube. Die Beschwerdeführerin bezieht einen erheblichen Teil ihrer Informationen von

menschlichen Quellen, mit denen sie ausschließlich elektronisch kommuniziert, etwa von Regierungsstellen aus europäischen und außereuropäischen Staaten wie Ägypten, Eritrea und Libyen, Angehörigen vulnerabler Gruppen wie Opfern von Menschenhandel und Folter und deren Angehörigen sowie Angehörigen von kriminellen Gruppierungen wie Schleuserbanden oder militanten Gruppen. Die Kontakte der Beschwerdeführerin setzen sich durch ihre Zusammenarbeit mit ihr gewichtigen Risiken bis hin zu Gefahren für Leib und Leben aus. Die Beschwerdeführerin ist daher auf die Vertraulichkeit ihrer Kommunikation zwingend angewiesen.

8. Beschwerdeführer zu 8: Szabolcs Panyi

Der Beschwerdeführer zu 8 ist ungarischer Staatsangehöriger und lebt in …. Er ist als investigativer Journalist für das Journalismuszentrum Direkt36 tätig und befasst sich dort vor allem mit Korruption, nationaler Sicherheit und außenpolitischen Fragen mit einem Fokus auf russische und chinesische Einflussnahmen auf die ungarische Politik.

...

9. Beschwerdeführer zu 9: Peter Verlinden

Der Beschwerdeführer zu 9 ist belgischer Staatsangehöriger und lebt … bei Brüssel. Er war 30 Jahre lang Afrikakorrespondent des belgischen öffentlich-rechtlichen Rundfunksenders VRT. Seit seiner Pensionierung im Jahr 2019 arbeitet er freiberuflich als Journalist für Magazine wie Knack und Humo, Zeitungen wie De Standaard und das Onlinemedium Doorbraak.be.

Der Beschwerdeführer befasst sich in seiner Arbeit vor allem mit der Region um die Afrikanischen Großen Seen und dabei insbesondere mit Ruanda, Burundi und der Demokratischen Republik Kongo. Insbesondere über diese Region hat er 15 Bücher veröffentlicht.

Wegen seiner kritischen Arbeit zu den Regimes dieser Länder ist der Beschwerdeführer bereits mehrfach Ziel von Operationen der dortigen Nachrichtendienste geworden. Im Jahr 2021 entdeckte der belgische militärische Nachrichtendienst ADIV, dass das Mobiltelefon des Beschwerdeführers und das seiner Frau mit der Pegasus-Spionagesoftware infiltriert waren, wahrscheinlich durch den ruandischen Geheimdienst.

Der Beschwerdeführer bezieht häufig Informationen von Quellen innerhalb der Regierung der von ihm fokussierten Staaten. Beispiele bilden zum einen seine Arbeiten über den Schmuggel von Mineralien aus der Demokratischen Republik Kongo nach Ruanda und Uganda und die Korruption im Kongo, die er 2014

in seinem Buch Het Goud van Congo (Das Gold des Kongo) veröffentlichte. Hierfür erhielt er Hinweise aus dem Regierungsapparat eines der betroffenen Länder,

> vgl. https://www.dewereldmorgen.be/community/het-goud-van-congo; https://www.bol.com/be/nl/p/het-goud-van-congo/9200000023054897 (letzte Abrufe am 23. Dezember 2022).

Zum anderen ist seine Arbeit über den ruandischen Hotelier Paul Rusesabagina zu nennen, der vielfach als Held angesehen wird, weil er Gäste seines Hotels, die den Tutsi angehörten, während des ruandischen Völkermordes beschützte. Das ruandische Regime sieht Rusesabagina hingegen als Terroristen, was zu einer Verurteilung zu 25 Jahren Gefängnis führte. Der Beschwerdeführer recherchierte mit Hilfe vertraulicher Quellen für einen Artikel über den Fall. Dieser Artikel bildete wahrscheinlich den Anlass für die Infiltration des Mobiltelefons des Beschwerdeführers. Auch über den mutmaßlich in der Haft getöteten ruandischen Menschenrechtsaktivisten Kizito Mihigo bezog der Beschwerdeführer Informationen von Quellen aus Ruanda,

> https://www.knack.be/nieuws/wereld/is-de-held-van-hotel-rwanda-een-terrorist-een-gesprek-met-zijn-vrouw-en-kinderen; https://www.knack.be/nieuws/wereld/kizito-mihigo-van-ster-tot-paria-ik-kom-je-twee-zaken-zeggen-het-eerste-is-dat-je-moest-sterven (letzte Abrufe am 23. Dezember 2022).

Der Beschwerdeführer nutzt für seine Arbeit ständig elektronische Kommunikationsdienste wie Sprachtelefonie, E-Mail oder Instant Messaging. Als investigativ arbeitender Journalist bezieht er einen großen Teil seiner Informationen von menschlichen Quellen wie Angehörigen von Regierungsstellen oder auch Angehörigen verbotener Organisationen, die sich durch ihre Zusammenarbeit mit dem Beschwerdeführer gewichtigen Risiken bis hin zu Gefährdungen für Leib und Leben aussetzen. Der Beschwerdeführer ist daher auf die Vertraulichkeit seiner Kommunikation zwingend angewiesen.

10. Beschwerdeführer zu 10: Awil Abdi Mohamud

Der Beschwerdeführer zu 10 ist somalischer Staatsangehöriger und lebt in …. Er ist als Radiojournalist tätig. ...

Aufgrund seiner journalistischen Tätigkeit wurde der Beschwerdeführer in Somalia zum Ziel der terroristischen Al-Shabaab-Miliz und des ISIS und erhielt wiederholt Morddrohungen,

vgl. https://www.politico.com/story/2012/11/us-military-behind-africa-news-websites-083772; https://www.nusoj.org/somalilands-guilty-verdict-against-broadcast-journalists-spells-doom-for-the-independent-practice-of-journalism (letzte Abrufe am 23. Dezember 2022).

...

11. Beschwerdeführer zu 11: Can Dündar

Der Beschwerdeführer zu 11 ist türkischer Staatsangehöriger und lebt seit 2016 in …. Er zählt zu den bekanntesten türkischsprachigen Journalisten, war für verschiedene Fernsehsender und Tageszeitungen in der Türkei in leitender Position tätig und ist Autor von mehr als 40 Büchern. ... Gegenwärtige Schwerpunkte seiner journalistischen Arbeit bilden die deutsch-türkischen politischen Beziehungen, Menschenrechtsfragen in der Türkei, das Vorgehen der Türkei zur Stabilisierung der Regierung von Präsident Recep Tayyip Erdoğan und die Behandlung von Minderheiten wie der kurdischen Bevölkerung in der Türkei,

vgl. https://ozguruz.de; https://www.wsj.com/video/can-dundar-exiled-turkish-journalist-on-media-crackdown/999E4AAF-F2FE-4D4E-A86C-6F8C5AC3BD4B.html; https://www.spiegel.de/ausland/can-duendar-erdogan-steht-mit-dem-ruecken-zur-wand-a-63f51c68-fdad-421e-8809-8ca42a846aa9; https://www.zeit.de/2019/51/recep-tayyip-erdogan-denunziation-propaganda-bundesregierung (letzte Abrufe am 23. Dezember 2022).

...

12. Beschwerdeführer zu 12: ...

Der Beschwerdeführer zu 12 ist … investigativer Journalist …. Seine Recherchen haben türkische Politik, Korruption und Kriminalität mit einem Schwerpunkt auf organisierter Betrugskriminalität zum Gegenstand,

...

13. Beschwerdeführerin zu 13: Gesellschaft für Freiheitsrechte

Die 2015 gegründete Beschwerdeführerin zu 13 ist ein eingetragener gemeinnütziger Verein nach deutschem Recht mit Sitz in Berlin. Sie ist im Bereich der strategischen Prozessführung tätig, um gezielt Grund- und Menschenrechte durchzusetzen. Dafür nutzt sie strategische Gerichtsverfahren und juristische Interventionen, um Demokratie und Zivilgesellschaft zu fördern, Überwachung

und digitale Durchleuchtung zu begrenzen und für alle Menschen gleiche Rechte und soziale Teilhabe zu erreichen.

Derzeit beschäftigt die Beschwerdeführerin 31 Mitarbeiterinnen und Mitarbeiter. Diese nutzen im Auftrag der Beschwerdeführerin zahlreiche elektronische Kommunikationsdienste wie Sprachtelefonie, den Videokonferenzdienst Zoom, Twitter, Instagram, Mastodon, E-Mail oder den Instant-Messenger-Dienst Signal in großem Umfang. E-Mails bearbeiten die Mitarbeiterinnen und Mitarbeiter in der Regel mit einem Mail-Programm (Apple Mail und Thunderbird). Die Inhalte der E-Mails werden mit Ende-zu-Ende-Verschlüsselung versendet, sofern die Empfängerinnen und Empfänger ebenfalls Verschlüsselungstechnik verwenden. In großem Umfang tauschen sich die Mitarbeiterinnen und Mitarbeiter untereinander und mit Externen auch per Signal aus, sowohl über eine Smartphone-App als auch über ein Desktop-Programm. Zudem ist die Beschwerdeführerin auf den sozialen Medien Instagram, Twitter, Facebook und YouTube vertreten.

Die für die Arbeit verwendeten Laptops tauschen regelmäßig Daten mit Nextcloud-Servern (vergleichbar mit dem Dienst Dropbox) aus. Auf diesen Servern liegen so gut wie alle arbeitsrelevanten Daten der Beschwerdeführerin. Teilweise bearbeiten die Mitarbeiterinnen und Mitarbeiter die Dokumente kollaborativ in der Cloud. Ein separater Server dient außerdem dem Austausch von Daten mit Externen; auch die hierauf gespeicherten Daten werden regelmäßig auf den Laptops der Mitarbeiterinnen und Mitarbeiter aktualisiert. Zudem werden für die Erstellung von Backups der Daten Cloudserver genutzt. Weiter wird ein internes Buchführungssystem verwendet, das regelmäßig Umsätze mehrerer Vereinskonten automatisiert über das Internet abruft. Ihre berufsbezogenen Passwörter verwalten die Mitarbeiterinnen und Mitarbeiter der Beschwerdeführerin mit einem cloudbasierten Programm. Kontakte, Notizen und Kalendereinträge synchronisieren sich automatisch über das Internet. Die Beschwerdeführerin besitzt außerdem einen DHL-Account, über den Pakete und Päckchen getrackt werden, die sie versendet oder empfängt.

Die Beschwerdeführerin unterhält ständig Kontakte zu nationalen und internationalen Klägerinnen und Klägern, Kooperationsanwältinnen und -anwälten, Journalistinnen und Journalisten sowie zu anderen Organisationen, die im gleichen Themenfeld tätig sind. Mit diesen Kontakten kommunizieren ihre Mitarbeiterinnen und Mitarbeiter ganz überwiegend elektronisch. Darüber hinaus betreibt die Beschwerdeführerin Policy und Advocacy Arbeit, sodass sie auch im regelmäßigen Austausch mit Politikerinnen und Politikern steht. Sämtliche

Kommunikation der Beschwerdeführerin ist auf ein hohes Maß an Vertraulichkeit angewiesen, um wirksam zu arbeiten.

14. Beschwerdeführerin zu 14: Reporter ohne Grenzen

Die Beschwerdeführerin zu 14 ist die unabhängige deutsche Sektion der Beschwerdeführerin zu 1. Sie beschäftigt 46 Mitarbeiterinnen und Mitarbeiter. Die Ziele und die Tätigkeit der Beschwerdeführerin entsprechen denen der Beschwerdeführerin zu 1, sodass insoweit auf die Beschreibung der Beschwerdeführerin zu 1 verwiesen wird. Wie die Beschwerdeführerin zu 1 unterhält die Beschwerdeführerin zahlreiche vertrauliche Kontakte zu Journalistinnen und Journalisten, Unterstützungspersonen wie etwa Rechtsanwältinnen und Rechtsanwälten oder Ärztinnen und Ärzten, Organisationen mit vergleichbarem thematischem Fokus sowie Regierungsstellen weltweit.

Hervorzuheben ist im Zusammenhang der vorliegenden Verfassungsbeschwerde die Nothilfe- und Stipendienarbeit der Beschwerdeführerin, mit der sie bedrohten Journalistinnen und Journalisten einen sicheren Zufluchtsort verschafft. Für bestimmte Länder dient sie hier als Erstanlaufstelle, sodass Kontakte nicht über die Beschwerdeführerin zu 1 vermittelt werden. Soweit die mit der Beschwerdeführerin assoziierten Journalistinnen und Journalisten in ihren Heimatländern mit Gerichtsverfahren überzogen werden, begleitet die Beschwerdeführerin diese Verfahren auch vor Ort und kommuniziert laufend mit dort ansässigen Rechtsanwältinnen und Rechtsanwälten.

Die Mitarbeiterinnen und Mitarbeiter der Beschwerdeführerin nutzen ständig elektronische Kommunikationsdiensten wie Sprach- und Videotelefonie, E-Mail oder Instant Messaging. Darüber hinaus betreibt die Beschwerdeführerin eine Website, auf der sie sich präsentiert, Spenden sammelt und einen Online-Shop betreibt. Zudem ist sie in vielen sozialen Medien wie Twitter, Facebook, YouTube, LinkedIn oder Instagram vertreten.

Im Rahmen der Nothilfe- und Stipendienarbeit fragt die Beschwerdeführerin von den unterstützten Personen zahlreiche persönliche Informationen ab, darunter etwa … Nachweise über die journalistische Arbeit, … sowie die Darstellung der eigenen, … politischen Verfolgung. ….

15. Beschwerdeführer zu 15: Ulf Buermeyer

Der Beschwerdeführer zu 15 ist deutscher Staatsangehöriger und wohnt in Berlin. Er ist seit 2007 Richter des Landes Berlin, zuletzt als Richter am Landgericht Berlin. Derzeit ist er beurlaubt. Zudem ist er Vorstandsmitglied der Beschwerdeführerin zu 13. Daneben ist er journalistisch tätig und moderiert den

wöchentlichen Politik-Podcast Lage der Nation, der von etwa 750.000 Menschen regelmäßig gehört wird und damit einer der populärsten deutschen Podcasts ist. ...

16. Beschwerdeführer zu 16: Martin Kaul

Der Beschwerdeführer zu 16 ist … als Journalist tätig und gehört dem Vorstand der Beschwerdeführerin zu 14 an. Der Beschwerdeführer arbeitet für das Investigativressort des Westdeutschen Rundfunks in der Recherchekooperation von NDR, WDR und Süddeutscher Zeitung. In dieser Funktion ist er regelmäßig in Recherchen von nationaler und internationaler Bedeutung eingebunden, in bundesweiten und internationalen Recherchegruppen und Recherchezusammenhängen,

> vgl. https://www.martinkaul.de/meine-bio; https://www.reporter-ohne-grenzen.de/ueber-uns/vorstand/martin-kaul (letzte Abrufe am 28. Dezember 2022).

…

17. Beschwerdeführerin zu 17: Nora Markard

Die Beschwerdeführerin zu 17 ist deutsche Staatsangehörige und wohnt in Berlin. Sie hat seit 2020 den Lehrstuhl für Internationales Öffentliches Recht und Internationalen Menschenrechtsschutz an der Westfälischen Wilhelms-Universität Münster inne. Ihre Forschungsschwerpunkte bilden das Verfassungsrecht einschließlich der Rechtsvergleichung, das Völkerrecht, das internationale Flüchtlingsrecht, das Migrationsrecht sowie die Legal Gender Studies. Außerdem ist sie Vorstandsmitglied der Beschwerdeführerin zu 13.

...

18. Beschwerdeführer zu 18: Christian Mihr

Der Beschwerdeführer zu 18 ist deutscher Staatsangehöriger und wohnt in Berlin. Er ist Menschenrechtsaktivist und Experte für internationale Medienpolitik, als solcher arbeitet er seit 2012 als Geschäftsführer der Beschwerdeführerin zu 14.

...

19. Beschwerdeführer zu 19: Kerem Schamberger

Der Beschwerdeführer zu 19 ist deutscher Staatsangehöriger und wohnt in München. Er ist seit 2022 Referent für Migration und Flucht in der Öffentlichkeitsarbeit der Hilfs- und Menschenrechtsorganisation Medico International.

Zuvor war er als wissenschaftlicher Mitarbeiter an der Ludwig-Maximilians-Universität München beschäftigt.

...

20. Beschwerdeführerin zu 20: Eva Schulz

Die Beschwerdeführerin zu 20 ist deutsche Staatsangehörige und wohnt in Berlin. Sie ist als freiberufliche Journalistin vor allem für öffentlich-rechtliche Medien tätig, daneben für weitere Stellen etwa als Moderatorin oder Beraterin. Im Jahr 2017 hat sie Deutschland3000 gegründet, eine öffentlich-rechtliche journalistische Content-Marke, die jungen Menschen helfen soll, sich eine Meinung zu Politik- und Gesellschaftsthemen zu bilden. Inhalte von Deutschland3000 erscheinen auf Facebook, Instagram, Tiktok sowie als Podcast und Radiosendung.

...

B. Zulässigkeit

Die Verfassungsbeschwerde ist zulässig. Die Beschwerdeführerinnen und Beschwerdeführer, die teils identische, teils unterschiedliche verfassungsrechtliche Rügen erheben (unten I), sind hinsichtlich der jeweils erhobenen Rügen beschwerdebefugt (unten II). Die Anforderungen des Subsidiaritätsgrundsatzes (unten III) und die Beschwerdefrist (unten IV) sind gewahrt.

I. Verfassungsrechtliche Rügen

Die Beschwerdeführerinnen und Beschwerdeführer erheben teils gleichläufige, teils unterschiedliche Rügen.

Die Beschwerdeführerin zu 1 als ausländische juristische Person und die Beschwerdeführerinnen und Beschwerdeführer zu 2 bis 9 als Ausländerinnen und Ausländer im Ausland wenden sich umfassend gegen die Ermächtigungen zu strategischen Ausland-Fernmeldeaufklärungen und zu Online-Durchsuchungen im Ausland. Mit Blick auf die strategische Ausland-Fernmeldeaufklärung rügen sie Defizite hinsichtlich des Ausmaßes der Überwachung (unten C. I. 1.), der Ziele der Gefahrenfrüherkennung (unten C I. 2.), der bevorratenden Speicherung von Verkehrsdaten (unten C. I. 5.), der Kontrolle der Überwachung (unten C. I. 7.), der Übermittlung der erlangten Daten (unten C. I. 8.), der Weiterverarbeitung von Daten aus sogenannten Eignungsprüfungen (unten C. I. 9.) und der Kooperation des Bundesnachrichtendienstes mit ausländischen Partnerdiensten (unten C. I. 10.). In Bezug auf Online-Durchsuchungen wenden sie sich gegen die Regelungen zu den Voraussetzungen der Maßnahme (unten C. II. 1.), zu den Betroffenen (unten C. II. 2.), zum Schutz des Kernbereichs privater Lebensgestaltung (unten C. II. 3.) und zur Übermittlung der erlangten Daten (unten C. II. 4.).

Die Beschwerdeführerin zu 1 als juristische Person des französischen Rechts und die Beschwerdeführerinnen und Beschwerdeführer zu 6 bis 9 als Unionsbürgerinnen und Unionsbürger rügen zudem den unzureichenden Schutz von natürlichen und juristischen Personen aus anderen Mitgliedstaaten der Europäischen Union bei der strategischen Ausland-Fernmeldeaufklärung (unten C. I. 3. b) und c)) wie auch bei Online-Durchsuchungen (unten C. II. 2.).

Die Beschwerdeführerinnen und Beschwerdeführer zu 2 bis 9 als im Ausland wohnhafte ausländische Journalistinnen und Journalisten rügen darüber hinaus den unzureichenden Schutz von Vertraulichkeitsbeziehungen bei der suchwortbasierten Erhebung von Inhaltsdaten (unten C. I. 4.) wie auch bei der bevorratenden Speicherung von Verkehrsdaten (unten C. I. 5. b) dd)) im Rahmen der strategischen Ausland-Fernmeldeaufklärung.

Die Beschwerdeführer zu 10 bis 12 als ausländische Staatsangehörige, die ihren aktuellen Lebensmittelpunkt in der Bundesrepublik haben, rügen, dass der ihnen gewährleistete besondere Überwachungsschutz nur greift, solange sie sich im Inland aufhalten (unten C. I. 3. a) und C. II. 2.). Soweit sie daher während ihrer Auslandsaufenthalte von Maßnahmen der strategischen Ausland-Fernmeldeaufklärung und von Online-Durchsuchungen betroffen sein können, wenden sie sich ebenso wie die Beschwerdeführerinnen und Beschwerdeführer zu 1 bis 9 umfassend gegen die Defizite der gesetzlichen Ermächtigungen zu diesen Maßnahmen sowie als Journalisten gegen die unzureichenden Regelungen zum Schutz von Vertraulichkeitsbeziehungen.

Die Beschwerdeführer zu 10 bis 12 rügen zudem zusammen mit den Beschwerdeführerinnen zu 13 und 14 als juristischen Personen des deutschen Rechts und den Beschwerdeführerinnen und Beschwerdeführern zu 15 bis 20 als deutschen Staatsangehörigen zwei Defizite der Regelungen über die strategische Ausland-Fernmeldeaufklärung mit Inlandsbezug: Erstens wenden sich diese Beschwerdeführerinnen und Beschwerdeführer gegen die Ermächtigung, sie betreffende erfasste Verkehrsdaten nach einer Unkenntlichmachung sowie Verkehrsdaten der inländischen intermaschinellen Kommunikation auch unmodifiziert zu bevorraten und weiterzuverarbeiten (unten C. I. 5. b) ee) und ff)). Zweitens sind die Beschwerdeführerinnen und Beschwerdeführer nach den Regelungen über die Erhebung von Inhaltsdaten zwar grundsätzlich von der Überwachung auszunehmen und die gleichwohl erfassten Inhaltsdaten unverzüglich zu löschen. Hiervon besteht allerdings eine Ausnahme, wenn durch eine Datenweiterverarbeitung eine erhebliche Gefahr für bestimmte Rechtsgüter abgewendet werden kann. In diesem Fall sind die betroffenen Personen zu benachrichtigen. Von dieser Benachrichtigungspflicht sieht das Gesetz jedoch zu weitgehende Ausnahmen vor (unten C. I. 6.). Da die auf die Beschwerdeführerinnen und Beschwerdeführer zu 10 bis 20 bezogenen Daten im Rahmen der strategischen Ausland-Fernmeldeaufklärung anfallen, rügen sie zudem die Verfassungswidrigkeit der auch sie betreffenden Vorschriften über das Ausmaß der Überwachung (unten C. I. 1.), die Kontrolle der Überwachung (unten C. I. 7.) und die Übermittlung der bevorrateten Daten (unten C. I. 8.).

II. Beschwerdebefugnis

Die Beschwerdeführerinnen und Beschwerdeführer sind hinsichtlich der von ihnen jeweils vorgebrachten Rügen beschwerdebefugt im Sinne von § 90 Abs. 1 BVerfGG. Eine Grundrechtsverletzung ist gegenüber allen von ihnen möglich (unten 1). Die Beschwerdeführerinnen und Beschwerdeführer sind

durch die von ihnen jeweils angegriffenen Regelungen selbst und gegenwärtig (unten 2) sowie unmittelbar betroffen (unten 3).

1. Möglichkeit einer Grundrechtsverletzung

Es ist zumindest möglich, dass Überwachungsmaßnahmen auf der Grundlage der angegriffenen Regelungen Grundrechte der Beschwerdeführerinnen und Beschwerdeführer verletzen.

Insbesondere hat das Bundesverfassungsgericht in seinem Urteil zur Ausland-Ausland-Fernmeldeaufklärung ausgeführt, dass sich auch Ausländerinnen und Ausländer im Ausland wie die Beschwerdeführerinnen und Beschwerdeführer zu 2 bis 9 gegenüber strategischen Überwachungsmaßnahmen des Bundesnachrichtendienstes auf das Fernmeldegeheimnis in seiner abwehrrechtlichen Dimension berufen können,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 87 ff.

Nichts anderes kann für das aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG herzuleitende Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme mit Blick auf Online-Durchsuchungen im Ausland gelten. Die Ausführungen des Urteils vom 19. Mai 2020 zur Bindung des Bundesnachrichtendienstes an das Fernmeldegeheimnis lassen sich auf dieses Grundrecht vollständig übertragen.

Zudem ist auch die Beschwerdeführerin zu 1 als juristische Person des französischen Rechts Trägerin dieser Grundrechte,

> dies noch offenlassend BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 63 ff.

Das Bundesverfassungsgericht hat bereits entschieden, dass die deutschen Grundrechte über Art. 19 Abs. 3 GG hinausgehend auch juristische Personen aus dem EU-Ausland schützen. Zur Begründung hat es auf die Grundfreiheiten des AEUV sowie auf das allgemeine Diskriminierungsverbot des Art. 18 AEUV verwiesen, die eine grundrechtliche Gleichbehandlung juristischer Personen aus dem Inland und aus dem EU-Ausland erforderlich machten, soweit letztere im Anwendungsbereich des Unionsrechts tätig würden. Hierzu müsse eine EU-ausländische juristische Person einen hinreichenden Inlandsbezug aufweisen, der die Geltung der Grundrechte in gleicher Weise wie für inländische juristische Personen geboten erscheinen lasse,

> BVerfGE 129, 78 (94 ff.).

Die Voraussetzungen dieser Anwendungserweiterung des deutschen Grundrechtsschutzes auf juristische Personen aus der Europäischen Union liegen bei der Beschwerdeführerin zu 1 mit Blick auf die Überwachung ausländischer Telekommunikation und ausländischer informationstechnischer Systeme durch den Bundesnachrichtendienst vor.

Zum einen kann sich die Beschwerdeführerin zu 1 gegenüber Aufklärungsmaßnahmen des Bundesnachrichtendienstes zumindest auf das allgemeine Diskriminierungsverbot des Art. 18 AEUV berufen und verlangen, hinsichtlich solcher Maßnahmen ebenso gestellt zu werden wie eine inländische juristische Person. Wie noch zu zeigen sein wird, fallen Aufklärungsmaßnahmen des Bundesnachrichtendienstes in weitem Umfang in den Anwendungsbereich der Verträge; dies unter anderem, wenn ein Zusammenhang mit der Ausübung der Grundfreiheiten des europäischen Binnenmarkts besteht,

siehe unten C. I. 3. b) aa).

Ein solcher Zusammenhang ist hinsichtlich der Beschwerdeführerin zu 1 anzunehmen. Sie ist grenzüberschreitend tätig, um die Lage der Pressefreiheit weltweit zu dokumentieren, durch Veröffentlichungen und politische Kampagnen zur Verbesserung der Lage beizutragen und bedrohten Journalistinnen und Journalisten sowie deren Familien im Einzelfall beizustehen. Sowohl die allgemeine Informationstätigkeit der Beschwerdeführerin zu 1 als auch ihre Nothilfetätigkeit im Einzelfall schließt Mitgliedstaaten der Europäischen Union ein. Dass auch innerhalb der Europäischen Union ein Bedarf für eine grenzüberschreitende Beobachtung der Freiheit der Presse wie auch für Hilfeleistungen im Einzelfall besteht, zeigt sich etwa daran, dass die Beschwerdeführerin zu 1 in ihrem jüngsten Index von 2022 die Lage der Pressefreiheit in mehreren Mitgliedstaaten (Bulgarien, Griechenland, Italien, Polen, Rumänien, Slowenien, Ungarn) als problematisch eingestuft hat,

siehe https://rsf.org/en/index (letzter Abruf am 23. Dezember 2022).

Im Rahmen ihrer Tätigkeiten nimmt die Beschwerdeführerin zu 1 in großem Umfang grenzüberschreitende Dienstleistungen in Anspruch, etwa indem sie anwaltliche Beratungs- oder medizinische Versorgungsleistungen in den Herkunftsländern bedrohter Journalistinnen und Journalisten beschafft und bezahlt. Gerade dieser grenzüberschreitende Bezug von Dienstleistungen durch die Beschwerdeführerin zu 1, der auch innerhalb der Europäischen Union den Interessen staatlicher Stellen diametral widersprechen kann, ist im besonderen Maße auf Vertraulichkeit angewiesen. Aufklärungsmaßnahmen von Nachrichtendiensten der Mitgliedstaaten können daher die grenzüberschreitende

Tätigkeit der Beschwerdeführerin zu 1 erheblich beeinträchtigen und im schlimmsten Fall dazu führen, dass sie ihre satzungsmäßigen Aufgaben nicht mehr erfüllen kann, da sich eine Vertrauensbasis zu Quellen oder zu bedrohten Journalistinnen und Journalisten nicht mehr herstellen lässt. Dementsprechend können sich solche Aufklärungsmaßnahmen negativ auf den grenzüberschreitenden Bezug von Dienstleistungen durch die Beschwerdeführerin zu 1 auswirken. Die Auslandsaufklärung des Bundesnachrichtendienstes berührt daher die (passive) Dienstleistungsfreiheit der Beschwerdeführerin zu 1 aus Art. 56 AEUV.

Zum anderen weist die Tätigkeit der Beschwerdeführerin zu 1 einen hinreichenden Inlandsbezug auf, um die Grundrechte des Grundgesetzes auf sie anzuwenden, soweit diese Grundrechte einen Schutz gegen nachrichtendienstliche Überwachungen vermitteln. Maßgeblich hierfür ist nicht isoliert der Tätigkeitskreis der Beschwerdeführerin zu 1, sondern sind die potenziellen Auswirkungen der Aufklärungstätigkeit des Bundesnachrichtendienstes auf die Beschwerdeführerin zu 1. Der erforderliche Inlandsbezug ergibt sich daraus, dass die Beschwerdeführerin zu 1 nach dem Zuschnitt ihrer Tätigkeit als Zielorganisation oder Drittbetroffene von Aufklärungsmaßnahmen des Bundesnachrichtendienstes in Betracht kommt und zudem mit zahlreichen Einzelpersonen im europäischen und außereuropäischen Ausland in Kontakt steht, die als potenzielle Zielpersonen solche Aufklärungsmaßnahmen anzusehen sind. Zudem können gerade Aufklärungsmaßnahmen des Bundesnachrichtendienstes die Tätigkeit der Beschwerdeführerin zu 1 erheblich beeinträchtigen. Dies folgt schon aus der – auch im Vergleich zu anderen Nachrichtendiensten – beträchtlichen Größe und technischen Kompetenz des Bundesnachrichtendienstes sowie der außenpolitischen Durchsetzungskraft der Bundesregierung, zu deren Information der Bundesnachrichtendienst in erster Linie tätig wird. Hinzu kommen die zahlreichen und intensiven Kooperationen des Bundesnachrichtendienstes mit ausländischen Nachrichtendiensten, die ebenfalls erhebliche Nachteile für die Tätigkeit der Beschwerdeführerin zu 1 zur Folge haben können. Sollte sich herausstellen, dass die Beschwerdeführerin zu 1 in größerem Ausmaß durch den Bundesnachrichtendienst überwacht wird, so würde aller Voraussicht nach insbesondere ihre einzelfallbezogene Hilfstätigkeit stark leiden, da die dafür erforderliche Vertrauensbasis verloren ginge.

2. Eigene und gegenwärtige Betroffenheit

Die Beschwerdeführerinnen und Beschwerdeführer sind durch die von ihnen jeweils angegriffenen Regelungen gegenwärtig und selbst betroffen.

Ergibt sich eine konkrete Beeinträchtigung erst aus dem Vollzug der angegriffenen Vorschriften, erlangen die Betroffenen jedoch in der Regel keine Kenntnis von den Vollzugsakten, so reicht es für die Möglichkeit der eigenen und gegenwärtigen Betroffenheit aus, darzulegen, mit einiger Wahrscheinlichkeit durch die auf den angegriffenen Rechtsnormen beruhenden Maßnahmen in eigenen Grundrechten berührt zu werden. Ein Vortrag, für sicherheitsgefährdende oder nachrichtendienstlich relevante Aktivitäten verantwortlich zu sein, ist zum Beleg der Selbstbetroffenheit grundsätzlich ebenso wenig erforderlich wie Darlegungen, durch die sich Beschwerdeführende selbst einer Straftat bezichtigen müssten. 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. Hingegen kann nicht ohne Weiteres von der Wahrscheinlichkeit eigener Betroffenheit ausgegangen werden, wenn durch die Begrenzung auf bestimmte Eingriffsschwellen und zu schützende Rechtsgüter ein deutlicher Einzelfallbezug verlangt ist. Dann bedarf es näherer Darlegungen, warum dennoch eine individuelle Betroffenheit hinreichend wahrscheinlich ist,

BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 97 f.

a) Strategische Ausland-Fernmeldeaufklärung

Nach diesem Maßstab besteht für alle Beschwerdeführerinnen und Beschwerdeführer die hinreichende Wahrscheinlichkeit, zukünftig von Maßnahmen der strategischen Ausland-Fernmeldeaufklärung in ihren eigenen Grundrechten berührt zu werden.

aa) Hinreichende Wahrscheinlichkeit einer Erfassung

Als strategisch ausgerichtete, im Wesentlichen nur final angeleitete Überwachungsmaßnahme zeichnet sich die strategische Ausland-Fernmeldeaufklärung durch eine äußerst große Streubreite aus. Die Erfassungsanlagen des Bundesnachrichtendienstes erfassen alle Inhalts- und Verkehrsdaten, die während einer Überwachung über die überwachten Telekommunikationsnetze geleitet werden. Angesichts der großen Bedeutung der Bundesrepublik, in der sich mit dem DE-CIX der größte Internetknoten der Welt befindet, für den internationalen Telekommunikationsverkehr, des sehr großen potenziell überwachbaren Volumens von 30 Prozent der bestehenden Telekommunikationsnetze weltweit (§ 19 Abs. 8 Satz 2 BNDG) und der extensiven Nutzung elektronischer Kommunikationsdienste durch alle Beschwerdeführerinnen und Beschwerdeführer ist mit an Sicherheit grenzender Wahrscheinlichkeit davon

auszugehen, dass der Bundesnachrichtendienst im Rahmen der strategischen Ausland-Fernmeldeaufklärung sie betreffende Kommunikationsdaten erfassen wird.

Diese Prognose lässt sich anhand einer Beispielsrechnung veranschaulichen: Angenommen, pro Tag ist eine Beschwerdeführerin an nur 100 Telekommunikationsvorgängen beteiligt oder werden bei solchen Vorgängen personenbezogene Daten über die Beschwerdeführerin verarbeitet (Beispiele: ein- oder ausgehender Telefonanruf, Empfang oder Versand einer E-Mail oder Kurznachricht, Aufruf eines sozialen Mediums, Bearbeitung einer Textdatei über vernetzte Anwendungssoftware, Synchronisierung eines Cloudspeicherdienstes, Anfrage bei einem Navigationssystem – die tatsächliche Zahl dürfte um ein Vielfaches höher liegen). Hieraus ergeben sich im Jahr 36.500 Telekommunikationsvorgänge. Wenn weiter angenommen wird, dass ein einzelner Telekommunikationsvorgang lediglich mit einer Wahrscheinlichkeit von 1:10.000 durch den Bundesnachrichtendienst im Rahmen der strategischen Ausland-Fernmeldeaufklärung erfasst wird, so ergibt sich in einem Jahr eine Erfassungswahrscheinlichkeit von über 97% ($1 - 0{,}9999^{36500} \approx 0{,}974$). Selbst bei einer Erfassungswahrscheinlichkeit von 1:100.000 pro Telekommunikationsvorgang ergäbe sich über das Jahr noch eine Wahrscheinlichkeit von gut 63% ($1 - 0{,}99999^{36500} \approx 0{,}632$).

Die Erfassung führt hinsichtlich aller Beschwerdeführerinnen und Beschwerdeführer zu einem Grundrechtseingriff. Hinsichtlich der Beschwerdeführerinnen und Beschwerdeführer zu 1 bis 12, die sich als Ausländerinnen und Ausländer dauerhaft oder temporär im Ausland aufhalten, ist die Erfassung als Grundrechtseingriff anzusehen, da sie die erfassten Daten für einen Abgleich mit Suchbegriffen beziehungsweise eine bevorratende Speicherung verfügbar macht,

vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 115.

Hinsichtlich der Beschwerdeführerinnen und Beschwerdeführer zu 10 bis 20, die hinsichtlich von Inhaltsdaten als Ausländer während ihres Aufenthalts in der Bundesrepublik beziehungsweise als juristische Personen des deutschen Rechts oder deutsche Staatsangehörige ortsunabhängig einen weitreichenden Überwachungsschutz genießen, ergibt sich nichts anderes. Soweit sie betreffende Inhaltsdaten erfasst werden, müssen diese zwar grundsätzlich unmittelbar bei der Signalaufbereitung herausgefiltert und gelöscht werden. Jedoch ist dies nach dem derzeitigen technischen Stand nicht vollständig möglich. Die Erfassung macht die nicht herausgefilterten Daten insbesondere für eine spätere Weiterverarbeitung zur Gefahrenabwehr verfügbar,

vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 117.

Soweit der Bundesnachrichtendienst Verkehrsdaten der elektronischen Kommunikation erfasst, die sich auf die Beschwerdeführerinnen und Beschwerdeführer zu 10 bis 20 beziehen lassen, darf er diese Daten in ihrer Gesamtheit ohne weitere Voraussetzungen teils in unkenntlich gemachter Form, teils – soweit es sich um Verkehrsdaten der intermaschinellen Kommunikation handelt – in unmodifizierter Form bevorraten. Da die Unkenntlichmachung den Personenbezug der bevorrateten Daten nicht aufhebt,

näher unten C. I. 5. b) ff),

ist in beiden Fallkonstellationen gleichermaßen von einem Grundrechtseingriff durch die Erfassung auszugehen.

Da also alle Beschwerdeführerinnen und Beschwerdeführer im Rahmen der strategischen Ausland-Fernmeldeaufklärung mit an Sicherheit grenzender Wahrscheinlichkeit Grundrechtseingriffen ausgesetzt sein werden, sind sie durch die von ihnen jeweils angegriffenen Vorschriften auch selbst und gegenwärtig beschwert. Denn diese Grundrechtseingriffe lassen sich nur rechtfertigen, wenn die Rechtsgrundlagen der strategischen Ausland-Fernmeldeaufklärung, soweit sie eine Weiterverarbeitung der erfassten Daten hinsichtlich der jeweiligen Beschwerdeführerinnen und Beschwerdeführer zulassen, insgesamt den verfassungsrechtlichen Anforderungen genügen. Die Beschwerdeführerinnen und Beschwerdeführer zu 1 bis 12 sind daher durch die Regelungen über die Verarbeitung von Inhalts- und Verkehrsdaten von Ausländern im Ausland beschwert; für die Beschwerdeführer zu 10 bis 12 gilt dies mit Blick auf ihre Auslandsaufenthalte, während derer sie nicht als Inländer geschützt sind. Die Beschwerdeführerinnen und Beschwerdeführer zu 10 bis 20 sind beschwert, soweit das Gesetz eine Weiterverarbeitung von Daten, die sich auf Inländerinnen und Inländer beziehen, ausnahmsweise (im Fall von Inhaltsdaten) oder stets (im Fall von unkenntlich gemachten Verkehrsdaten sowie von Verkehrsdaten der intermaschinellen Kommunikation) zulässt. Die eigene und gegenwärtige Beschwer erstreckt sich jeweils auf die zugehörigen Regelungen zum Verfahren der Überwachung sowie zur Gewährleistung von Transparenz, Kontrolle und wirksamem Rechtsschutz.

Diesem Ergebnis kann nicht entgegengehalten werden, dass in gleicher Weise die Betroffenheit aller anderen regelmäßigen Telekommunikationsnutzerinnen und -nutzer begründet werden könnte. Die annähernd universale Beschwerdebefugnis beruht darauf, dass die angegriffenen Regelungen eine hoheitliche

Maßnahme ermöglichen und ermöglichen sollen, die praktisch jedermann betrifft. Die Reichweite der Beschwerdebefugnis in persönlicher Hinsicht folgt also schlicht der Streubreite der Eingriffsermächtigung. Dies ist kein neuartiger Befund, sondern wurde durch das Bundesverfassungsgericht etwa in dem Urteil über die Bevorratung innerstaatlich anfallender Telekommunikations-Verkehrsdaten und dem Beschluss zur automatisierten Erfassung von Kfz-Kennzeichen in Baden-Württemberg und Hessen bereits anerkannt,

vgl. BVerfGE 125, 260 (304 f.); 152, 309 (325 f.).

bb) Hinreichende Wahrscheinlichkeit einer Erhebung von Inhaltsdaten

Strengere Anforderungen an die Darlegung der eigenen und gegenwärtigen Beschwer lassen sich mit Blick auf die strategische Ausland-Fernmeldeaufklärung allenfalls hinsichtlich der Inhaltsdaten begründen, die anders als die erfassten Verkehrsdaten nicht gesamthaft bevorratet, sondern nur anhand von Suchbegriffen erhoben werden dürfen. Selbst wenn insoweit zu fordern wäre, dass neben der an Sicherheit grenzenden Wahrscheinlichkeit einer zukünftigen Datenerfassung auch eine gewisse Wahrscheinlichkeit einer zukünftigen Datenerhebung dargelegt wird, wäre dieses Erfordernis hinsichtlich der Beschwerdeführerinnen und Beschwerdeführer zu 1 bis 12, die sich auch gegen die Regelungen zur Erhebung und Weiterverarbeitung von Inhaltsdaten wenden, gewahrt. Hinsichtlich dieser Beschwerdeführerinnen und Beschwerdeführer besteht zudem das – gleichfalls für die Zulässigkeit der Verfassungsbeschwerde nicht erforderliche – gesteigerte Risiko, dass der Bundesnachrichtendienst die auf sie bezogenen bevorratend gespeicherten Verkehrsdaten später im Rahmen nachrichtendienstlicher Analysen nutzt.

Für die Beschwerdeführerinnen und Beschwerdeführer zu 1 bis 12 ist im Vergleich zum Bevölkerungsdurchschnitt in ihren Ländern das Risiko erheblich erhöht, dass der Bundesnachrichtendienst die Inhalte von Telekommunikationsverkehren, an denen sie beteiligt sind, aufgrund eines Abgleichs mit den Suchbegriffen erhebt. Gesteigert wahrscheinlich ist darüber hinaus sogar, dass der Bundesnachrichtendienst die erhobenen Inhalts- und Verkehrsdaten dieser Beschwerdeführerinnen und Beschwerdeführer als nachrichtendienstlich relevant einstuft und daher weiterverarbeitet. Denn aufgrund ihrer Tätigkeitsfelder befassen sich die Beschwerdeführerinnen und Beschwerdeführer zu 1 bis 12 in ihrer Kommunikation mit Themen, bei denen naheliegt, dass ihnen eine gesteigerte außen- und sicherheitspolitische Relevanz für die Bundesrepublik zukommt und sie eine Nähe zu den für eine Gefahrenfrüherkennung in Betracht kommenden Gefahrenbereichen aufweisen. Darüber hinaus stehen die Beschwerdeführerinnen und Beschwerdeführer zu 1 bis 12 sämtlich

in Kontakt mit Personen und Organisationen, denen gleichfalls naheliegend eine solche Relevanz zugeschrieben werden könnte, sodass ihre Kommunikationskennungen als metadatenbezogene Suchbegriffe genutzt werden könnten. Denkbar erscheint sogar, dass der Bundesnachrichtendienst die eigenen Kommunikationskennungen dieser Beschwerdeführerinnen und Beschwerdeführer als Suchbegriffe verwenden könnte.

Die Beschwerdeführerin zu 1 setzt sich weltweit für die Freiheit der Presse ein und unterstützt im Einzelfall Journalistinnen und Journalisten, die aufgrund ihrer Tätigkeit Repressalien ausgesetzt sind.

Der Schutz der Pressefreiheit in ausländischen Staaten ist bereits für sich genommen ein Anliegen von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik. Die Recherchen der Beschwerdeführerin zu 1 zum Stand der Pressefreiheit weltweit können daher dem Aufklärungsauftrag des Bundesnachrichtendienst insbesondere insoweit unterfallen, als die Beschwerdeführerin ihre Erkenntnisse – etwa zum Schutz vertraulicher Quellen – weder veröffentlicht noch in sonstiger Weise weitergibt. Insoweit kann ein Aufklärungsinteresse des Bundesnachrichtendienstes bestehen, das sich nur durch Überwachungsmaßnahmen befriedigen lässt.

Darüber hinaus kommuniziert die Beschwerdeführerin zu 1 in großem Ausmaß über politisch brisante Themen, an denen ein erhebliches außen- und sicherheitspolitisches Interesse der Bundesrepublik besteht und die darum im Zentrum des Aufklärungsauftrags des Bundesnachrichtendienstes mit Blick sowohl auf die Unterrichtung der Bundesregierung als auch auf die Früherkennung drohender Gefahren stehen. Denn sowohl die Korrespondentinnen und Korrespondenten der Beschwerdeführerin zu 1 als auch die Journalistinnen und Journalisten, denen sie in Notlagen hilft, befassen sich typischerweise mit solchen Themen. Beispielhaft seien Korruption im wirtschaftlichen und staatlichen Bereich, internationale finanzielle Verflechtungen zur Verschleierung von Finanzflüssen, internationaler Terrorismus und internationale organisierte Kriminalität genannt. Im Rahmen ihrer Kommunikation mit gefährdeten Journalistinnen und Journalisten muss die Beschwerdeführerin zu 1 zwangsläufig deren Recherchethemen erörtern, um von ihnen nähere Informationen zum Stand der Pressefreiheit zu erlangen oder um ihnen gezielte Unterstützung anbieten zu können. Zudem kann an den Kommunikationspartnern der Beschwerdeführerin zu 1 selbst oder deren Quellen auch ein unmittelbares nachrichtendienstliches Interesse des Bundesnachrichtendienstes bestehen, zu dessen Befriedigung ihre Kommunikationskontakte ausgewertet werden sollen.

Es liegt daher nahe, dass die Beschwerdeführerin zu 1 und ihre Kommunikationspartner Begriffe nutzen werden, die der Bundesnachrichtendienst als inhaltsbezogene Suchbegriffe nutzt. Zudem ist anzunehmen, dass auch eine metadatenbezogene Suche etwa nach den Kommunikationskennungen journalistischer Quellen oder auch von Journalistinnen und Journalisten selbst Telekommunikationsverkehre der Beschwerdeführerin zu 1 erfassen wird.

Die Beschwerdeführerinnen und Beschwerdeführer zu 2 bis 12 befassen sich als Journalistinnen und Journalisten sowie im Fall des Beschwerdeführers zu 3 und der Beschwerdeführerin zu 7 als Menschenrechtsaktivist und Menschenrechtsaktivistin durchweg mit Vorgängen im Ausland, die dem Aufklärungsauftrag des Bundesnachrichtendienstes mit Blick sowohl auf die Unterrichtung der Bundesregierung als auch auf die Früherkennung drohender Gefahren unterfallen. Die oben unter A. II. 2. bis 12. jeweils näher behandelten Schwerpunkte ihrer Tätigkeit umfassen etwa Korruption in hochrangigen politischen Kreisen ausländischer Staaten von hoher Relevanz für die Bundesrepublik und bei international agierenden, auch in Deutschland tätigen Unternehmen, die Einflussnahme ausländischer Mächte wie Russland und China auf die europäische Politik und Wirtschaft, internationale kriminelle Strukturen des Terrorismus, des Menschenhandels, der Geldwäsche oder der Proliferation sowie Operationen ausländischer Nachrichtendienste. Die durch die Beschwerdeführerinnen und Beschwerdeführer zu 2 bis 12 recherchierten Informationen sind darum ebenso potenziell von nachrichtendienstlichem Interesse wie die von ihnen genutzten Quellen.

Es liegt darum nahe, dass der Bundesnachrichtendienst bei der Erhebung von Inhaltsdaten Suchbegriffe nutzt, die zu einer Erhebung von Kommunikationsvorgängen der Beschwerdeführerinnen und Beschwerdeführer zu 2 bis 12 führen. In Betracht kommen zum einen inhaltsbezogene Suchbegriffe wie beispielsweise die Namen von Protagonisten unterschiedlicher Gefahrenbereiche oder die Bezeichnungen von Unternehmen oder kriminellen Gruppierungen. Zum anderen besteht eine gesteigerte Wahrscheinlichkeit, dass die elektronische Kommunikation der Beschwerdeführerinnen und Beschwerdeführer zu 2 bis 12 bei einer metadatenbasierten Suche erhoben wird, die etwa auf Kommunikationskennungen ihrer Quellen beruht. Derartige Suchbegriffe könnten im Übrigen auch zur Analyse bevorrateter Verkehrsdaten genutzt werden und wiederum dazu führen, dass die auf die Beschwerdeführerinnen und Beschwerdeführer zu 2 bis 12 bezogenen Daten einer näheren Sichtung unterzogen werden.

Gegen die eigene und gegenwärtige Betroffenheit der Beschwerdeführerinnen und Beschwerdeführer zu 1 bis 12 kann nicht der besondere Vertraulichkeitsschutz des § 21 BNDG angeführt werden. Die Beschwerdeführerin zu 1 unterfällt dieser Regelung nicht, da sie nicht selbst journalistisch tätig sind. Für die Beschwerdeführerinnen und Beschwerdeführer zu 2 bis 12 ist der Anwendungsbereich der Norm hingegen zwar eröffnet. Geschützt sind die Beschwerdeführerinnen zu 2 bis 12 jedoch nur gegen die Erhebung von Inhaltsdaten „aus“ einer Vertraulichkeitsbeziehung, was eine Datenerhebung „über“ eine Vertraulichkeitsbeziehung nicht ausschließt,

näher unten C. I. 4.

Zudem gilt der Vertraulichkeitsschutz nicht ausnahmslos, sondern unterliegt Einschränkungen nach § 21 Abs. 2 BNDG, die nicht durchweg an das Verhalten der betroffenen Vertrauensperson anknüpfen und darum durch die Beschwerdeführerinnen und Beschwerdeführer zu 2 bis 12 nicht zu beherrschen sind. Im Übrigen besteht ungeachtet dieser Schutzregelung das gerade bei der Auslandsaufklärung beträchtliche Risiko, dass der Bundesnachrichtendienst bei der Datenerhebung und auch bei der Weiterverarbeitung der erhobenen Daten nicht erkennt und möglicherweise nicht einmal erkennen kann, dass die Voraussetzungen von § 21 Abs. 1 oder Abs. 3 BNDG vorliegen. So ist davon auszugehen, dass der Bundesnachrichtendienst nicht alle im Ausland journalistisch tätigen Personen kennt. Bei dem Beschwerdeführer zu 3 und der Beschwerdeführerin zu 7 könnte der Bundesnachrichtendienst aus deren Doppelrolle als Journalist/in und Menschenrechtsaktivist/in auch darauf schließen, dass der Anwendungsbereich von § 21 BNDG generell oder hinsichtlich bestimmter Kommunikationsvorgänge nicht eröffnet ist. Schließlich erstreckt sich der Vertraulichkeitsschutz von vornherein nicht auf die Speicherung und Weiterverarbeitung von Verkehrsdaten.

Eine gegenwärtige und unmittelbare Beschwer entfällt auch nicht bei den Beschwerdeführerinnen und Beschwerdeführer zu 6 bis 9 aufgrund ihrer Eigenschaft als Unionsbürgerinnen und Unionsbürgern. Zwar gewährleistet § 20 Abs. 1 BNDG ihnen einen spezifischen Überwachungsschutz. Dieser ist aber nur schwach ausgeprägt. Die Norm lässt eine Erhebung von Inhaltsdaten in weitem Umfang zu und bietet überhaupt keinen Schutz gegen die bevorratende Speicherung und Weiterverarbeitung von Verkehrsdaten,

näher unten C. I. 3. b).

cc) Hinreichende Wahrscheinlichkeit einer Weiterverarbeitung von Verkehrsdaten der inländischen Kommunikation

Hinsichtlich der inländischen Beschwerdeführerinnen und Beschwerdeführer zu 10 bis 20 ist, wie oben ausgeführt, eine nähere Darlegung nicht erforderlich, dass an ihnen und ihrer Kommunikation ein nachrichtendienstliches Interesse besteht. § 26 Abs. 3 Satz 2 BNDG erlaubt ihnen gegenüber in jedem Fall eine langfristige bevorratende Speicherung von Verkehrsdaten. Diese stellt schon für sich genommen einen schwerwiegenden Grundrechtseingriff dar, gegen den sich diese Beschwerdeführerinnen und Beschwerdeführer wehren können müssen.

Selbst wenn gleichwohl die Darlegung eines potenziellen nachrichtendienstlichen Interesses zu fordern wäre, läge dieses jedenfalls hinsichtlich der Beschwerdeführerin zu 14 und der Beschwerdeführer zu 10, 11, 12, 16, 18 und 19 vor.

Die Beschwerdeführer zu 10, 11 und 12 unterhalten als Journalisten im Exil nach wie vor häufige vertrauliche Kontakte zu Quellen in ihren Heimatstaaten. Bei diesen Quellen handelt es sich teilweise um Personen, an denen oder an deren Umfeld ein außen- und sicherheitspolitisches Interesse naheliegt. Dies gilt etwa für Oppositionelle aus den Heimatstaaten der Beschwerdeführer, Regierungsstellen oder auch die Angehörigen krimineller Organisationen. Eine Analyse der bevorrateten Verkehrsdaten könnte etwa von den Kommunikationskennungen dieser Personen ausgehen und würde dann mit gewisser Wahrscheinlichkeit auch Kommunikationsvorgänge zutage fördern, an denen die Beschwerdeführer beteiligt waren.

Die Beschwerdeführerin zu 14 unterhält – ebenso wie ihre französische Dachorganisation, die Beschwerdeführerin zu 1 – zahlreiche Kontakte zu Personen im Ausland, an denen aufgrund ihrer Befassung mit außen- und sicherheitspolitisch relevanten Themen ein beträchtliches nachrichtendienstliches Interesse bestehen kann. Eine Analyse der bevorrateten Verkehrsdaten, die etwa von den Kommunikationskennungen solcher Personen ausgeht, wird darum mit beträchtlicher Wahrscheinlichkeit in beträchtlichem Ausmaß Verkehrsdaten umfassen, die sich auf die Beschwerdeführerin zu 14 beziehen. Dies könnte Anlass geben, die weitere Auswertung auch auf die Beschwerdeführerin zu 14 als möglichen Inlandskontakt von nachrichtendienstlichem Interesse zu fokussieren.

Der Beschwerdeführer zu 16 unterhält als investigativer Journalist mit einem Schwerpunkt auf Fragen der nationalen Sicherheit Kontakte zu Personen und

Gruppierungen im Ausland, an denen ein unmittelbares nachrichtendienstliches Interesse besteht. Beispielhaft seien seine Recherchen zur Lage in Afghanistan während des Abzugs der Bundeswehr genannt, in deren Rahmen er unter anderem mit Angehörigen des Taliban-Regimes kommunizierte. Auch die Recherchen des Beschwerdeführers zu 16 zu rechtsextremistischen Gruppierungen können sich wegen der verbreiteten internationalen Verflechtung solcher Gruppierungen auf ausländische Milieus von hoher sicherheitspolitischer Relevanz erstrecken. Bei einer Verkehrsdatenanalyse könnte der Beschwerdeführer zu 16 daher als Inlandskontakt seiner Kommunikationspartner eingestuft werden und darum in den Fokus des Bundesnachrichtendienstes geraten.

Der Beschwerdeführer zu 18 hat im Rahmen seiner Tätigkeit für die Beschwerdeführerin zu 14 gleichfalls häufig Kontakte zu Personen und Stellen im Ausland, die als außen- und sicherheitspolitisch relevant eingestuft werden könnten. Auch er könnte bei einer Verkehrsdatenanalyse daher als Inlandskontakt solcher Stellen eingeordnet und darum näher betrachtet werden.

Der Beschwerdeführer zu 19 unterhält Kontakte zu Angehörigen verschiedener Organisationen im Ausland, die in Deutschland teilweise dem terroristischen Spektrum zugerechnet werden und auch ansonsten teils militant agieren. Es liegt nahe, dass an diesen Organisationen aus Sicht des Bundesnachrichtendienstes ein außen- und sicherheitspolitisches Interesse besteht. Dementsprechend erscheint es wahrscheinlich, dass eine Verkehrsdatenanalyse die Kommunikation des Beschwerdeführers mit ihnen erschließt, was ihn noch stärker als bereits heute in das Aufmerksamkeitsfeld des Bundesnachrichtendienstes und anderer deutscher Sicherheitsbehörden rücken könnte.

b) Online-Durchsuchung

Die Beschwerdeführerinnen und Beschwerdeführer zu 1 bis 12 sind auch durch die Ermächtigung des Bundesnachrichtendienstes zu Online-Durchsuchungen selbst und gegenwärtig betroffen. Es besteht für diese Beschwerdeführerinnen und Beschwerdeführer eine im Vergleich zum ausländischen Bevölkerungsdurchschnitt erheblich erhöhte Wahrscheinlichkeit, durch eine solche Maßnahme erfasst zu werden.

Die Beschwerdeführerinnen und Beschwerdeführer zu 2 bis 12 könnten sogar als Zielpersonen einer Online-Durchsuchung in Betracht gezogen werden. Sie kommunizieren im Rahmen ihrer Recherchetätigkeit vielfach mit Personen, die als Gefahrverursacher im Sinne von § 34 Abs. 5 Nr. 1 BNDG eingestuft werden

könnten. Beispiele bilden Angehörige politischer Gruppierungen oder wirtschaftlicher Einheiten, gegen die ein Korruptionsverdacht besteht, oder Personen, die international agierenden kriminellen Strukturen zugeordnet werden könnten. Aufgrund dieser Kontakte erscheint denkbar, dass die Beschwerdeführerinnen und Beschwerdeführer zu 2 bis 12 gemäß § 34 Abs. 5 Nr. 2 BNDG als Kommunikationsmittler eingestuft und darum gezielt überwacht werden; im Fall der Beschwerdeführer zu 10 bis 12 gilt dies mit der Einschränkung, dass die Überwachung sich auf deren Auslandsaufenthalte beschränken müsste.

Der besondere Vertraulichkeitsschutz des § 35 BNDG steht einer solchen Überwachung nicht zwingend entgegen. Zum einen unterliegt er gemäß § 35 Abs. 2 BNDG Ausnahmen, die teilweise nicht vom Verhalten der betroffenen Vertrauensperson abhängen. Zum anderen setzt der Schutz faktisch voraus, dass der Bundesnachrichtendienst das Bestehen einer geschützten Vertraulichkeitsbeziehung überhaupt erkennt. Gerade im Rahmen der Auslandsaufklärung liegt nahe, dass die Eigenschaft eines Kommunikationsmittlers als Journalistin oder Journalist und das Verhältnis dieser Person zum Gefahrverursacher für den Bundesnachrichtendienst selbst im Nachhinein bei der Auswertung der erhobenen Daten nicht erkennbar ist.

Darüber hinaus besteht eine gesteigerte Wahrscheinlichkeit, dass die Beschwerdeführerinnen und Beschwerdeführer zu 2 bis 12 von einer Online-Durchsuchung als Drittbetroffene im Sinne von § 34 Abs. 6 BNDG erfasst werden. Grund hierfür ist wiederum, dass diese Beschwerdeführerinnen und Beschwerdeführer in erheblichem Umfang mit Personen kommunizieren, die naheliegenderweise als Gefahrverursacher eingestuft und überwacht werden könnten. Hinzu kommt, dass eine Online-Durchsuchung auch durchgeführt werden kann, um Erkenntnisse nicht lediglich über Einzelpersonen, sondern über größere Personenzusammenhänge und Strukturen zu gewinnen. Zu diesem Zweck kann der Bundesnachrichtendienst etwa dienstlich genutzte informationstechnische Systeme oder informationstechnische Infrastruktur infiltrieren,

vgl. die Gesetzesbegründung, BT-Drs. 19/26103, S. 94.

Eine solche Maßnahme bringt aufgrund ihres breiteren Erkenntnisziels auch eine größere Streubreite mit sich. Sie kann sich auf ein größeres soziales Umfeld eines potenziellen Gefahrverursachers erstrecken. Insbesondere eine solche Umfeldüberwachung kann neben den Beschwerdeführerinnen und Beschwerdeführern zu 2 bis 12 auch die Beschwerdeführerin zu 1 erfassen, die

zwar in der Regel keine unmittelbaren Kontakte zu Gefahrverursachern unterhält, wohl aber zu Journalistinnen und Journalisten, die in intensivem Austausch mit solchen Personen stehen können.

Gerade im Rahmen einer derartigen Umfeldüberwachung, bei der der Bundesnachrichtendienst über die einzelnen erfassten Personen vielfach keine vertieften Kenntnisse hat, ist hinsichtlich der Beschwerdeführerinnen und Beschwerdeführer zu 2 bis 12 die faktische Wirksamkeit der Schutzregelung in § 35 BNDG erheblich reduziert. Die Beschwerdeführerin zu 1 wird durch diese Norm ohnehin nicht geschützt.

3. Unmittelbare Betroffenheit

Die Beschwerdeführerinnen und Beschwerdeführer sind durch die angegriffenen Regelungen auch unmittelbar betroffen. Zwar bedürfen die angegriffenen Befugnisse der Umsetzung durch weitere Vollzugsakte. Von einer unmittelbaren Betroffenheit durch ein vollziehungsbedürftiges Gesetz ist jedoch auch dann auszugehen, wenn ein Beschwerdeführer den Rechtsweg nicht beschreiten kann, weil er keine Kenntnis von der Maßnahme erlangt, oder wenn eine nachträgliche Bekanntgabe zwar vorgesehen ist, von ihr aber aufgrund weitreichender Ausnahmetatbestände auch langfristig abgesehen werden kann,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 72; Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 99.

Danach ist hier eine unmittelbare Betroffenheit zu bejahen. Die durch die angegriffenen Vorschriften ermöglichten Überwachungsmaßnahmen werden heimlich durchgeführt. Eine Benachrichtigung der Beschwerdeführerinnen und Beschwerdeführer zu 1 bis 9, bei denen es sich um Ausländer im Ausland handelt, ist nach § 59 Abs. 1 BNDG nicht vorgesehen. Die inländischen Beschwerdeführerinnen und Beschwerdeführer zu 10 bis 20 sind nur nach Maßgabe von § 59 Abs. 2 BNDG zu benachrichtigen, der weitreichende Ausnahmen von der grundsätzlichen Benachrichtigungspflicht vorsieht und unter bestimmten Voraussetzungen ein endgültiges Absehen von der Benachrichtigung ermöglicht. Auch die Möglichkeit, nach § 9 BNDG i.V.m. § 15 BVerfSchG auf Antrag Auskunft über die zu ihrer Person gespeicherten Daten zu erhalten, lässt die Unmittelbarkeit der Beschwer für die Beschwerdeführerinnen und Beschwerdeführer nicht entfallen, da diese Vorschriften nicht gewährleisten, dass die Betroffenen von der Überwachung Kenntnis erlangen. Insbesondere wird dann, wenn eine Benachrichtigung nach § 59 Abs. 2 BNDG

ausgeschlossen ist, so gut wie immer auch der Auskunftsanspruch nicht bestehen. Keine Kenntnis erhalten die Betroffenen schließlich in der Regel von der weiteren Nutzung oder Übermittlung der Daten, die durch die angegriffenen Vorschriften erlaubt werden.

III. Subsidiarität

Der Zulässigkeit der Verfassungsbeschwerde steht auch der Subsidiaritätsgrundsatz nicht entgegen.

Nach dem Grundsatz der Subsidiarität sind vor der Erhebung von Rechtssatzverfassungsbeschwerden grundsätzlich alle Mittel zu ergreifen, die der geltend gemachten Grundrechtsverletzung abhelfen können. Zu den insoweit zumutbaren Rechtsbehelfen kann gegebenenfalls die Erhebung einer Feststellungs- oder Unterlassungsklage gehören, die eine fachgerichtliche Klärung entscheidungserheblicher Tatsachen- oder Rechtsfragen des einfachen Rechts ermöglicht. Soweit die Beurteilung einer Norm allein spezifisch verfassungsrechtliche Fragen aufwirft, die das Bundesverfassungsgericht zu beantworten hat, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung verbesserte Entscheidungsgrundlagen zu erwarten wären, bedarf es einer vorangehenden fachgerichtlichen Entscheidung hingegen nicht. Darüber hinaus gelten Ausnahmen von der Pflicht zur vorherigen Anrufung der Fachgerichte, wenn die angegriffene Regelung die Beschwerdeführenden zu gewichtigen Dispositionen zwingt, die später nicht mehr korrigiert werden können, wenn die Anrufung der Fachgerichte offensichtlich sinn- und aussichtslos wäre oder sie sonst nicht zumutbar ist,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 78; Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 100 ff.

Nach diesem Maßstab sind die Beschwerdeführerinnen und Beschwerdeführer nicht gehalten, vor Erhebung der Verfassungsbeschwerde fachgerichtlichen Rechtsschutz zu suchen.

Soweit sich die Verfassungsbeschwerde gegen die Ermächtigungen zu strategischen Telekommunikationsüberwachungen und die damit zusammenhängenden Verfahrensregelungen richtet, ist ein fachgerichtlicher Rechtsschutz von vornherein nicht eröffnet. Das Bundesverwaltungsgericht hat als erst- und letztinstanzlich zuständiges Fachgericht bereits entschieden, dass Klagen gegen solche Überwachungsmaßnahmen eine darzulegende Betroffenheit durch eine konkrete Maßnahme des Bundesnachrichtendienstes voraussetzen,

> BVerwG, Urteil vom 28. Mai 2014 – 6 A 1.13 –, Rn. 19 ff.; Urteil vom 14. Dezember 2016 – 6 A 9.14 –, Rn. 13 ff.

Eine solche Darlegung wird den Beschwerdeführerinnen und Beschwerdeführern praktisch nie möglich sein, selbst wenn mit einiger Wahrscheinlichkeit davon auszugehen ist, dass sie früher oder später durch strategische Telekommunikationsüberwachungen nach den angegriffenen Vorschriften erfasst werden. Den Beschwerdeführerinnen und Beschwerdeführern zu 1 bis 9 als Ausländern im Ausland wird eine Überwachung nicht mitgeteilt, selbst wenn ihre Kommunikation nicht nur erfasst, sondern sogar nach einem Suchbegriffabgleich erhoben und ausgewertet wird. Die inländischen Beschwerdeführerinnen und Beschwerdeführer zu 10 bis 20 haben eine faktische Klagemöglichkeit nur, wenn Inhalte ihrer Kommunikation erhoben und nicht unverzüglich gelöscht werden, sodass sie nach § 59 Abs. 2 BNDG zu benachrichtigen sind. Selbst in einem solchen Fall ist ihre Benachrichtigung wegen der weitreichenden Ausnahmen von der Benachrichtigungspflicht nicht zuverlässig gewährleistet. Überhaupt keine Klagemöglichkeit besteht für alle Beschwerdeführerinnen und Beschwerdeführer hinsichtlich der in § 26 BNDG vorgesehenen gesamthaft bevorratenden Speicherung von Verkehrsdaten, soweit sie nicht ein konkretes Speicherungsprojekt beschreiben können, was ihnen wegen der Geheimhaltung solcher Projekte und des Fehlens einer Benachrichtigungspflicht in aller Regel unmöglich sein wird,

> vgl. zu einem Sonderfall, in dem eine solche Beschreibung hinsichtlich einer konkreten Datei des Bundesnachrichtendienstes ausnahmsweise möglich war, BVerwG, Urteil vom 13. Dezember 2017 – 6 A 7.16. Im Übrigen sah das Bundesverwaltungsgericht die gegen die Bevorratungspraxis des Bundesnachrichtendienstes erhobene Klage wiederum als unzulässig an.

Des Weiteren ist ein vorbeugender Rechtsschutz gegen zukünftige, im Einzelnen noch nicht feststehende Überwachungsprojekte nicht eröffnet. Zusammenfassend zu seiner eigenen Rechtsprechung hat das Bundesverwaltungsgericht festgehalten, dass die im Rahmen strategischer Telekommunikationsüberwachungen nach § 5 G 10 ergehenden „Beschränkungsanordnungen engen, verfahrensmäßig abgesicherten Begrenzungen in inhaltlicher und zeitlicher Hinsicht unterliegen und der dadurch bedingte ständige Wandel das Überwachungsregime als solches einem vorbeugenden Rechtsschutz nicht zugänglich erscheinen lässt“,

> BVerwG, Urteil vom 13. Dezember 2017 – 6 A 7.16 –, Rn. 14.

Diese Einschätzung lässt sich auf die strategische Ausland-Fernmeldeaufklärung ohne weiteres übertragen. Sie ist daher der Subsidiaritätsprüfung im vorliegenden Verfahren zugrunde zu legen.

Darüber hinaus ist hinsichtlich aller vorgebrachten Rügen eine vorherige Anrufung der Fachgerichte auch darum nicht angezeigt, weil die Verfassungsbeschwerde allein spezifisch verfassungsrechtliche Fragen aufwirft, die das Bundesverfassungsgericht zu beantworten hat, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung substantiell verbesserte Entscheidungsgrundlagen zu erwarten wären. Die verfassungsrechtliche Beurteilung der angegriffenen Regelungen hängt nicht an der näheren fachrechtlichen Auslegung der einzelnen Tatbestandsmerkmale der angegriffenen Eingriffsgrundlagen, sondern an der verfassungsrechtlichen Tragfähigkeit dieser Normen mit Blick auf die Gebote der Bestimmtheit, Normenklarheit und Verhältnismäßigkeit. Für die Vorschriften zur Datenerhebung durch Maßnahmen der strategischen Ausland-Fernmeldeaufklärung und durch Online-Durchsuchungen stellt sich dies nicht anders dar als für die hiermit zusammenhängenden Regelungen zu nachrichtendienstlichen Kooperationen, zum Verfahren und zur Kontrolle der Überwachung sowie zur Weiterverarbeitung erlangter Daten.

Der Subsidiaritätsgrundsatz steht der Zulässigkeit der Verfassungsbeschwerde schließlich auch insoweit nicht entgegen, als sich die Beschwerdeführerinnen und Beschwerdeführer zu 10 bis 20 im Zusammenhang mit der strategischen Ausland-Fernmeldeaufklärung gegen die Ausnahmeregelungen zu der grundsätzlichen Benachrichtigungspflicht in § 59 Abs. 2 Satz 1 BNDG wenden. Zwar hat das Bundesverfassungsgericht eine Rüge gegen eine gleichläufige Vorschrift des Bayerischen Verfassungsschutzgesetzes für unzulässig gehalten. Zur Begründung hat das Bundesverfassungsgericht darauf verwiesen, die dortigen Beschwerdeführer hätten zunächst versuchen müssen, die Reichweite der Benachrichtigungspflicht und ihrer Beschränkungen im fachgerichtlichen Verfahren zu klären,

BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 136.

Diese Ausführungen sollten jedoch nicht auf das vorliegende Verfahren übertragen werden, denn sie überspannen den Subsidiaritätsgrundsatz.

Ein fachgerichtliches Rechtsschutzverfahren, das die gesetzlichen Beschränkungen einer grundsätzlichen Pflicht zur Benachrichtigung der betroffenen Person über eine verdeckte Datenerhebungsmaßnahme zum Gegenstand hat, kann zwangsläufig nur von einer Person eingeleitet werden, die 1. von einer solchen Maßnahme betroffen wurde und 2. über diese Maßnahme nicht

benachrichtigt wurde. Hat keine Datenerhebung stattgefunden, so wurde die grundsätzliche Benachrichtigungspflicht von vornherein nicht ausgelöst, sodass deren gesetzliche Beschränkungen nicht streitentscheidend sind. Hat die Datenerhebung stattgefunden und ist eine Benachrichtigung erfolgt, so ist die von der Datenerhebung betroffene Person hinsichtlich der Benachrichtigungspflicht nicht beschwert. Eine einzelfallunabhängige Klärung der Rechtsfrage, wie weit die gesetzliche Benachrichtigungspflicht reichen müsste und welche Beschränkungen verfassungsrechtlich noch hinnehmbar sind, lässt sich im Rahmen des am Schutz subjektiver Rechte im Einzelfall orientierten deutschen Verwaltungsprozessrechts nicht erlangen. Insbesondere setzt eine verwaltungsgerichtliche Feststellungsklage, die in vielen Fallkonstellationen einen weitreichenden mittelbaren Rechtsschutz gegen verfassungswidrige gesetzliche Regelungen eröffnen mag, ein feststellungsfähiges konkretes Rechtsverhältnis voraus. Gefordert wird,

> „dass das Feststellungsbegehren auf einen hinreichend bestimmten, bereits überschaubaren, d.h. nicht nur gedachten und als möglich vorgestellten Sachverhalt bezogen ist“,
>
> Möstl, in: BeckOK VwGO, § 43 Rn. 5, m.w.N.

Ein solcher hinreichend bestimmter Sachverhalt fehlte, wenn eine Feststellungsklage sich allgemein auf die Reichweite der Benachrichtigungspflicht bezöge, ohne von einer konkreten Datenerhebungsmaßnahme auszugehen. Eine solche Feststellungsklage hätte nicht ein konkretes Rechtsverhältnis, sondern eine gerade nicht feststellungsfähige abstrakte Rechtsfrage zum Gegenstand,

> vgl. zur Unzulässigkeit derartiger Feststellungsklagen beispielhaft für die gefestigte ständige Rechtsprechung BVerwG, Urteil vom 23. August 2007 – 7 C 13.06 –, Rn. 31; BVerwG, Urteil vom 28. Januar 2010 – 8 C 38.09 –, Rn. 32; BVerwG, Urteil vom 28. Mai 2014 – 6 A 1.13 –, Rn. 20 f.; BVerwG, Urteil vom 12. September 2019 – 3 C 3.18 –, Rn. 23.

Wer hingegen von einer verdeckten Datenerhebungsmaßnahme betroffen war, aber nicht benachrichtigt wurde, weiß nichts von der Maßnahme. Eine solche Person hat keinen Anlass, gegen eine unterbliebene Benachrichtigung gerichtlich vorzugehen, ebenso wie sie keinen Anlass hat, gegen die Maßnahme selbst vorzugehen. Von ihr unter Subsidiaritätsgesichtspunkten ein derartiges Vorgehen zu erwarten, liefe darauf hinaus, der Person einen anlasslosen Rechtsschutz anzusinnen. Sie müsste „ins Blaue hinein“ vorbringen,

dass sie möglicherweise einmal durch eine verdeckte Datenerhebungsmaßnahme betroffen worden sei, von der sie in verfassungswidriger Weise nicht benachrichtigt worden sei. Ob ein solcher Rechtsbehelf, der die beanstandete hoheitliche Maßnahme nicht näher eingrenzen könnte, überhaupt zulässig wäre, erscheint sehr zweifelhaft. Nahe läge die Bewertung, dass es an einem hinreichend konkreten Streitgegenstand fehlte und die Klage stattdessen auf die gerade nicht statthafte Klärung einer abstrakten Rechtsfrage abzielte. Denkbar wäre auch, dem Klageantrag – gerade in einem Verfahren zum Nachrichtendienstrecht – als „Ausforschungsantrag“ das Rechtsschutzbedürfnis zu versagen. Jedenfalls wäre eine solche Klage für den Kläger oder die Klägerin mit einem extremen, für ihn oder sie kaum einschätzbaren Prozessrisiko verbunden, da sie nur Erfolg haben könnte, wenn es wirklich zu einer Datenerhebung gekommen sein sollte.

Die möglicherweise von einer verdeckten Datenerhebungsmaßnahme nach § 19 BNDG betroffene Person hätte in der Regel auch keine realistische Möglichkeit, durch einen Auskunftsantrag nach § 9 BNDG i.V.m. § 15 BVerfSchG von der Datenerhebungsmaßnahme zu erfahren und dann gegebenenfalls gegen ihre unterbliebene Benachrichtigung vorzugehen. Grund hierfür sind die zahlreichen Einschränkungen des gesetzlichen Auskunftsanspruchs, die gerade in den Fällen, in denen eine Benachrichtigung unterbleibt, zumindest in aller Regel auch die Auskunft sperren werden,

> vgl. zu Art. 23 Abs. 1 Satz 1 BayVSG auch BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 107.

Der Rechtsschutz gegen eine unterbliebene Benachrichtigung wäre insgesamt sogar mit noch höheren prozessualen Hürden verbunden als ein Rechtsschutz gegen eine möglicherweise drohende verdeckte Datenerhebungsmaßnahme, den der Senat den Beschwerdeführerinnen und Beschwerdeführern mit guten Gründen grundsätzlich gerade nicht zumutet,

> vgl. zuletzt BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 106 ff., wo der Subsidiaritätsgrundsatz nicht einmal erwähnt wird.

Personen, die befürchten, durch eine Sicherheitsbehörde zukünftig einmal überwacht zu werden, können gegen die drohende Überwachung immerhin möglicherweise mit einer verwaltungsgerichtlichen (vorbeugenden) Unterlassungsklage vorgehen,

> vgl. für die Zulässigkeit einer solchen Klage – wenngleich es sich möglicherweise wegen des ständigen Betriebs und der großen

> Streubreite der in Rede stehenden Überwachungseinrichtung eher um einen Sonderfall oder auch um eine „Ausreißerentscheidung“ handelte – BVerwG, Urteil vom 22. Oktober 2014 – 6 C 7.13 –, Rn. 15 ff.

Eine solche Klagemöglichkeit scheidet mit Blick auf das drohende Unterlassen einer Benachrichtigung aus. Bei der Benachrichtigung handelt es sich um eine behördliche positive Leistung, die durch eine vorangehende Eingriffsmaßnahme bedingt ist. Eine vorbeugende Klage auf eine rechtlich bedingte Leistung ist dem Verwaltungsprozessrecht unbekannt.

Im Übrigen ist eine Klagemöglichkeit gegen die im vorliegenden Verfahren in Rede stehenden strategischen Telekommunikationsüberwachungen, wie oben ausgeführt, nach mittlerweile gefestigter Rechtsprechung des Bundesverwaltungsgerichts generell nicht eröffnet, wenn der Kläger oder die Klägerin nicht konkret vorbringen kann, von einer solchen Überwachungsmaßnahme betroffen zu sein. Nichts anderes kann – erst recht – für die der Maßnahme nachgelagerte Benachrichtigungspflicht und ihre Grenzen gelten.

Der Unterzeichner möchte daher respektvoll an das Bundesverfassungsgericht appellieren, zu seiner bisherigen Rechtsprechung zurückzukehren, nach der zusammen mit einer Ermächtigung zu verdeckten Datenerhebungsmaßnahmen auch die Regelung über die Benachrichtigung der betroffenen Person und ihre Einschränkungen zulässigerweise unmittelbar mit einer Rechtssatzverfassungsbeschwerde angegriffen werden können,

> vgl. BVerfGE 100, 313 (354 ff., 397 ff.); 109, 279 (305 ff., 363 ff.); 125, 260 (304 ff., 353 f.); 141, 220 (260 ff., 319 f.); 155, 119 (159 ff.; 226 f.), jeweils ohne Thematisierung des Subsidiaritätsgrundsatzes im Zusammenhang mit den Beschränkungen der Benachrichtigungspflicht.

Der im Urteil zum Bayerischen Verfassungsschutzgesetz aufgezeigte Weg über einen fachgerichtlichen Rechtsschutz ist praktisch aussichtslos, zumindest aber für die betroffenen Personen mit einem außerordentlichen prozessualen Risiko verbunden, dem kein auch nur annähernd gleichgewichtiger Ertrag in Form eines wirksamen Grundrechtsschutzes oder einer Aufbereitung der fachrechtlichen Rechtslage gegenübersteht. Es handelt sich um eine unzumutbare und sinnlose Anrufung der Fachgerichte, die der Subsidiaritätsgrundsatz nicht gebietet.

IV. Beschwerdefrist

Die Beschwerdefrist des § 93 Abs. 3 BVerfGG ist gewahrt. Gemäß Art. 13 des Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts sind die angegriffenen Regelungen am 1. Januar 2022 in Kraft getreten.

C. Begründetheit

Die Verfassungsbeschwerde ist begründet. Sowohl die Regelungen über die strategische Ausland-Fernmeldeaufklärung (unten I) als auch die Ermächtigung zu Online-Durchsuchungen im Ausland (unten II) weisen zahlreiche verfassungsrechtliche Mängel auf und verletzen darum die Grundrechte der Beschwerdeführerinnen und Beschwerdeführer.

I. Strategische Ausland-Fernmeldeaufklärung

Die angegriffenen Regelungen über die strategische Ausland-Fernmeldeaufklärung verletzen das durch Art. 10 Abs. 1 GG gewährleistete Fernmeldegeheimnis und teilweise den allgemeinen Gleichheitssatz des Art. 3 Abs. 1 GG.

Das Bundesverfassungsgericht hat in seinem Urteil zur Ausland-Ausland-Fernmeldeaufklärung im Einzelnen herausgearbeitet, dass auslandsbezogene strategische Telekommunikationsüberwachungen am Fernmeldegeheimnis zu messen sind und einen schwerwiegenden Eingriff in dieses Grundrecht darstellen,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 113 ff., 146 ff.

Die gesetzlichen Ermächtigungen zu solchen Überwachungen müssen darum durch ein Bündel materieller und prozeduraler Vorgaben gewährleisten, dass die Überwachung sich in einem angemessenen Rahmen hält,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 167 ff.

Die Regelungen über strategische Ausland-Fernmeldeaufklärungen verfehlen nahezu jede dieser Vorgaben zumindest teilweise. Sie begrenzen das Ausmaß der Überwachung nicht wirksam (unten 1), erlauben Überwachungen zur Früherkennung von Gefahren teils mit Blick auf nicht hinreichend gewichtige Bedrohungen (unten 2), enthalten hinsichtlich der betroffenen Personen sachwidrige Differenzierungen (unten 3), schützen Vertraulichkeitsbeziehungen unzureichend (unten 4), ermöglichen in zu weitgehendem Ausmaß eine gesamthaft bevorratende Speicherung von Metadaten der Kommunikation (unten 5), sehen zu weitreichende Ausnahmen von der grundsätzlichen Pflicht zur Benachrichtigung inländischer betroffener Personen vor (unten 6), gewährleisten nicht in jeder Hinsicht eine hinreichend wirksame Kontrolle der Überwachung (unten 7), lassen die Übermittlung der erlangten Daten in zu großem Ausmaß zu (unten 8), begrenzen die Weiterverarbeitung von Daten aus soge-

nannten Eignungsprüfungen nicht hinreichend (unten 9) und ermöglichen Kooperationen des Bundesnachrichtendienstes mit ausländischen Partnerdiensten in zu weitem Umfang (unten 10).

1. Ausmaß

Auch wenn eine strategische, im Wesentlichen nur final programmierte Überwachung der ausländischen Telekommunikation verfassungsrechtlich gerechtfertigt werden kann, muss sie als hinreichend fokussiertes Instrument ausgestaltet werden und damit begrenzt bleiben. Dementsprechend muss der Gesetzgeber einschränkende Maßgaben zum Volumen der auszuwertenden Daten und zur geografischen Begrenzung des von der Überwachung abgedeckten Gebiets schaffen. Der Verweis auf wandelbare faktische Kapazitätsgrenzen reicht demgegenüber nicht aus,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 168 f.

Diese Anforderung verfehlt § 19 Abs. 8 BNDG. Danach ist eine „unbeschränkte“ Ausland-Fernmeldeaufklärung unzulässig und ist das Volumen der Überwachung auf maximal 30 Prozent der bestehenden Telekommunikationsnetze zu begrenzen.

Soweit die Norm eine „unbeschränkte“ Überwachung ausschließt, benennt sie keine praktisch handhabbare Grenze. Zu einer im Wortsinn unbeschränkten, also allumfassenden Überwachung sämtlicher Telekommunikationsvorgänge im Ausland wird der Bundesnachrichtendienst nie in der Lage sein. Unterhalb dieses hypothetischen Szenarios ist unklar, wann die Schwelle einer „unbeschränkten“ Überwachung überschritten sein soll.

Die konkretisierende Vorgabe, das Volumen der Überwachung dürfe 30 Prozent der bestehenden Telekommunikationsnetze nicht überschreiten, ist gleichfalls so unrealistisch, dass sie die praktische Überwachungstätigkeit des Bundesnachrichtendienstes nicht erkennbar beschränkt. Wie der Wortlaut von § 19 Abs. 8 BNDG nahelegt und die Gesetzesbegründung ausdrücklich bestätigt, bezieht sich die 30-Prozent-Grenze auf „alle bestehenden Telekommunikationsnetze weltweit“,

BT-Drs. 19/26103, S. 66.

Unabhängig von der problematischen Frage, wie genau diese Grenze zu berechnen ist (etwa nach der Zahl der physisch oder logisch zu definierenden Telekommunikationsnetze, nach der Zahl der Netzbetreiber oder nach der Übertragungskapazität der verschiedenen Netze), liegt nach allen denkbaren

Berechnungsweisen fern, dass der Bundesnachrichtendienst gegenwärtig oder in absehbarer Zeit auch nur annähernd auf 30 Prozent aller Telekommunikationsnetze in der Welt zugreifen könnte. Die 30-Prozent-Grenze hat daher bezogen auf die Netze als physische Infrastrukturen faktisch keine begrenzende Wirkung. Wäre hingegen dem Bundesnachrichtendienst eine Erfassung von mehr als 30 Prozent der weltweiten Telekommunikationsnetze faktisch möglich, so würde die gesetzliche Überwachungsbeschränkung hinsichtlich der übertragenen Daten, um deren Schutz es eigentlich geht, kaum etwas bewirken. Denn in der Regel verlaufen Telekommunikationsverkehre netzübergreifend, sodass die zugehörigen Inhalts- und Verkehrsdaten in mehreren Netzen erhoben werden können. Eine hypothetische Überwachung von 30 Prozent aller Telekommunikationsnetze dürfte einer vollständigen Überwachung der Telekommunikation weltweit zumindest nahekommen.

Die in § 19 Abs. 8 BNDG enthaltene Überwachungsgrenze ist daher insgesamt sinnlos und kann die verfassungsrechtlich gebotene quantitative Beschränkung des Überwachungszugriffs nicht leisten.

Schließlich sieht weder § 19 Abs. 8 BNDG noch eine andere Vorschrift des Gesetzes eine geografische Begrenzung der Überwachung in ihrer Gesamtheit vor; lediglich für einzelne Überwachungsprojekte ist nach § 19 Abs. 2 Nr. 3 BNDG ein geografischer Fokus anzugeben. Im Rahmen der 30-Prozent-Grenze und nach Maßgabe der – zulässigerweise teils offen gefassten – gesetzlichen Überwachungsziele könnte der Bundesnachrichtendienst im Rahmen der zu erwartenden Vielzahl an Überwachungsprojekten große Teile der Welt zu Zielgebieten der Überwachung machen. Insbesondere Erkenntnisse von außen- und sicherheitspolitischer Bedeutung, die der Dienst zur politischen Unterrichtung der Bundesregierung beschaffen darf, dürften grundsätzlich weltweit anfallen.

2. Ziele der Gefahrenfrüherkennung

Aufgrund ihrer besonders hohen Eingriffsintensität muss die strategische Ausland-Fernmeldeaufklärung Zwecken von hinreichendem Gewicht dienen. Nur wenn sich das Aufklärungsziel darin erschöpft, Regierungsentscheidungen zu unterstützen, kann der Gesetzgeber Überwachungsmaßnahmen für das gesamte Aufgabenspektrum des Bundesnachrichtendienstes ermöglichen. Soll die Überwachung (auch) der Gefahrenfrüherkennung dienen, so muss sie auf den Schutz hochrangiger Gemeinschaftsgüter gerichtet sein, deren Verletzung schwere Schäden für den äußeren und inneren Frieden oder die Rechtsgüter Einzelner zur Folge hätte,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 175 ff.

Nach diesem Maßstab genügt die Regelung der möglichen Erkenntnisziele für Überwachungen zum Zweck der Gefahrenfrüherkennung in § 19 Abs. 4 BNDG nicht vollständig den verfassungsrechtlichen Anforderungen.

a) Organisierte Kriminalität

§ 19 Abs. 4 Nr. 1 lit. e BNDG, der Überwachungen zur Früherkennung von Gefahren aus dem Gefahrenbereich der Organisierten Kriminalität zulässt, ist zu unbestimmt und zu weit gefasst.

Das BNDG definiert den Begriff der Organisierten Kriminalität nicht. Auch ansonsten enthält das Bundesrecht keine Legaldefinition, die zur Auslegung von § 19 Abs. 4 Nr. 1 lit. e BNDG herangezogen werden könnte. Es liegt allerdings nahe, das anerkannte polizeiliche Begriffsverständnis zu übernehmen, das 1990 von der bundesweiten Gemeinsamen Arbeitsgruppe Justiz/Polizei als Arbeitsdefinition beschlossen wurde. Danach ist Organisierte Kriminalität

> „die von Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig
>
> a) unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen,
>
> b) unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder
>
> c) unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft
>
> zusammenwirken“,
>
> Bundeskriminalamt, Organisierte Kriminalität – Bundeslagebild 2021, S. 10; wie hier die Gesetzesbegründung, BT-Drs. 19/26103, S. 60.

Organisierte Kriminalität in diesem Sinne kann erhebliche Bedrohungen für die Integrität des Gemeinwesens verursachen. Insbesondere gilt dies für Gruppierungen, die – entsprechend der Variante c der Arbeitsdefinition – bedeutsame hoheitliche oder gesellschaftliche Funktionsträger korrumpieren oder legale Wirtschaftskreisläufe unterwandern. Daneben erfasst die Arbeitsdefinition der

Organisierten Kriminalität jedoch auch verstetigte Zusammenschlüsse zur arbeitsteiligen Begehung von Straftaten der mittleren Kriminalität. Diese können für die Opfer beträchtliche wirtschaftliche Schäden verursachen, beeinträchtigen aber auch dann, wenn es sich um international operierende kriminelle Gruppierungen handelt, weder den inneren und äußeren Frieden noch besonders bedeutsame Rechtsgüter. Beispielsweise gehören nach der Arbeitsdefinition zur Organisierten Kriminalität auch Banden von Taschendieben oder Trickbetrügern, wenn sie eine gewerbliche Struktur aufweisen. Diese Einschätzung entspricht der polizeilichen Einstufungspraxis. So nennt das aktuelle Bundeslagebild Organisierte Kriminalität des Bundeskriminalamts als ein praktisch besonders bedeutsames Tätigkeitsfeld der Organisierten Kriminalität „Betrugsdelikte zum Nachteil älterer Menschen“,

> Bundeskriminalamt, Organisierte Kriminalität – Bundeslagebild 2021, S. 2; näher zu den Erscheinungsformen der Organisierten Kriminalität im Zusammenhang mit dem Wirtschaftsleben und im Bereich der Eigentumskriminalität ebd., S. 39 f.

Die zu weitreichende Überwachungsermächtigung lässt sich nicht mit der Erwägung rechtfertigen, dass die aufzuklärende Gefahr schon aus kompetenziellen Gründen eine außen- und sicherheitspolitische Bedeutung haben müsse,

> vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 128,

und der Begriff der Organisierten Kriminalität in § 19 Abs. 4 Nr. 1 lit. e BNDG darum restriktiv auszulegen sei. Es ist Sache des Gesetzgebers, die Ermächtigung auf entsprechend herausgehobene Strukturen der Organisierten Kriminalität zu beschränken. Auf diese Weise erfüllt er seine Aufgabe, die Überwachungstätigkeit des Bundesnachrichtendienstes so anzuleiten, dass die Anforderungen der Kompetenzordnung und des Verhältnismäßigkeitsgrundsatzes gewahrt sind.

Hingegen konterkariert § 19 Abs. 4 Nr. 1 lit. e BNDG durch die nicht weiter konkretisierte Inbezugnahme des für sich genommen sehr weiten Begriffs der Organisierten Kriminalität die Beschränkung der Überwachung auf Vorgänge von außen- und sicherheitspolitischer Bedeutung. Die zu weite Beschreibung des Gefahrenbereichs erzeugt damit erhebliche Interpretationsschwierigkeiten und lässt sich weder mit dem Verhältnismäßigkeitsgrundsatz noch mit den Geboten der Bestimmtheit und Normenklarheit vereinbaren. Die Grenzen einer denkbaren restriktiven Auslegung der Ermächtigung lassen sich nicht trennscharf bestimmen. Im Ergebnis überlässt es § 19 Abs. 4 Nr. 1 lit. e BNDG einer

normativ nicht näher angeleiteten Beurteilung durch die handelnden Mitarbeiterinnen und Mitarbeiter des Bundesnachrichtendienstes, welche Erscheinungsformen der Organisierten Kriminalität hinreichend gewichtig sind, um eine Überwachung zu legitimieren. Es fehlt der Norm damit an den verfassungsrechtlich gebotenen ausdrücklichen Begrenzungen der Erkenntnisziele der Überwachung,

> vgl. im Zusammenhang mit der strategischen Beschränkung der internationalen Telekommunikation zu der zu weiten Fassung eines konkreten Deliktsbereichs (Geldfälschung), die sich gleichfalls nicht im Wege einer einschränkenden Norminterpretation konkretisieren ließ, BVerfGE 100, 313 (384 f.).

Solche Begrenzungen wären unschwer möglich gewesen. So hätte eine differenziertere Ermächtigung zum einen nach dem Vorbild von § 5 Abs. 1 G 10 bestimmte Deliktsbereiche wie etwa die international organisierte Betäubungsmittel-, Schleusungs- oder Geldwäschekriminalität in Bezug nehmen können, bei denen sich eine außen- und sicherheitspolitische Bedeutung bereits aus den bedrohten Rechtsgütern ergibt,

> auf diese Kriminalitätsfelder verweist die Gesetzesbegründung, BT-Drs. 19/26103, S. 60 f.

Zum anderen hätten deliktsunabhängig Handlungsmodalitäten der Organisierten Kriminalität mit besonderem Bedrohungspotenzial benannt werden können, etwa die planmäßige Unterwanderung legaler Wirtschaftskreisläufe oder die großflächige Korruption von Hoheitsträgern. Die pauschale Inbezugnahme der Organisierten Kriminalität als aufzuklärender Gefahrenbereich lässt sich daher auch nicht mit regelungstechnischen Erfordernissen legitimieren. Vielmehr hat der Gesetzgeber seine Aufgabe verfehlt, mit Blick auf den Gefahrenbereich der Organisierten Kriminalität zu konkretisieren, welche kriminellen Organisationen eine außen- und sicherheitspolitische Bedeutung aufweisen und darum für eine Überwachung in Betracht kommen.

b) Außenpolitische Handlungsfähigkeit der Bundesrepublik

Ebenfalls zu unbestimmt und weit gefasst ist § 19 Abs. 4 Nr. 2 lit. d BNDG, der Überwachungen zur Früherkennung von Gefahren für die außenpolitische Handlungsfähigkeit der Bundesrepublik zulässt.

Weitgehend unklar ist bereits, was genau unter der außenpolitischen Handlungsfähigkeit der Bundesrepublik zu verstehen ist. Eine Legaldefinition dieses

Begriffs gibt es nicht. Die einzigen Vorschriften des Bundesrechts, die ihn enthalten, finden sich im BNDG (§ 4 Abs. 3 Nr. 2 lit. e, § 19 Abs. 4 Nr. 2 lit. d und § 31 Abs. 3 Nr. 2 BNDG; in § 33 Abs. 2 Satz 1 BNDG wird allgemeiner die Handlungsfähigkeit der Bundesrepublik genannt). Die Begründungen zu diesen Vorschriften enthalten gleichfalls keine Definition und erhellen dieses Tatbestandsmerkmal auch ansonsten kaum. So heißt es in der Begründung zu § 19 Abs. 4 Nr. 2 lit. d BNDG, die insoweit die ältere Begründung zu § 4 Abs. 3 Nr. 2 lit. e BNDG wörtlich wiederholt, die „Herausforderungen der globalisierten, multipolaren Welt“ schüfen „neue Rahmenbedingungen und Gefährdungspotenziale durch Destabilisierung politischer Systeme“, woraus sich „wichtige strategische Konsequenzen für die deutsche Außen- und Wirtschaftspolitik“ ergäben. Weiter führt die Gesetzesbegründung aus, Handlung sei „ein zielgerichtetes Vorgehen zur Durchsetzung der eigenen Interessen“, das zwingend eine „umfassende und zutreffende Kenntnis des internationalen Sachverhalts“ und der „Interessen der Akteure“ voraussetze. (Lediglich) beispielhaft verweist die Gesetzesbegründung auf Situationen, in denen „die Bundesrepublik Deutschland in internationalen Konflikten als neutrale Stelle eine Vermittlerrolle“ einnehme,

> BT-Drs. 19/26103, S. 63; vgl. zu § 4 Abs. 3 Nr. 2 lit. e BNDG BT-Drs. 19/25294, S. 44 f.; keine weitergehenden Erläuterungen finden sich in den Begründungen zu § 31 und § 33 BNDG, vgl. BT-Drs. 19/26103, S. 89 und 93.

Ein subsumtionsfähiger Begriff der außenpolitischen Handlungsfähigkeit der Bundesrepublik lässt sich diesen Ausführungen nicht entnehmen. Die Gesetzesbegründung legt vielmehr nahe, dass grundsätzlich jede Information von außen- und sicherheitspolitischer Relevanz zugleich die außenpolitische Handlungsfähigkeit der Bundesrepublik berührt, da prinzipiell zur Durchsetzung der Interessen der Bundesrepublik eine zielgerichtete Reaktion auf jede solche Information angezeigt sein kann. Es erscheint daher sehr zweifelhaft, ob der Begriff der außenpolitischen Handlungsfähigkeit der Aufgabenbeschreibung des § 1 Abs. 2 BNDG überhaupt zusätzliche tatbestandliche Erfordernisse hinzufügt,

> vgl. zu dem Überwachungszweck, die Handlungsfähigkeit der Bundesrepublik zu wahren, in § 6 Abs. 1 Satz 1 Nr. 2 BNDG a.F. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 305.

Hinzu kommt, dass § 19 Abs. 4 Nr. 2 lit. d BNDG die außenpolitische Handlungsfähigkeit der Bundesrepublik als Rechtsgut bezeichnet, zu dessen Schutz die Überwachung dienen soll. Die Überwachung soll also dabei helfen,

Gefahren für die außenpolitische Handlungsfähigkeit in einem frühen Stadium zu erkennen. Anders als bei den anderen Schutzgütern des § 19 Abs. 4 Nr. 2 BNDG ist aber nicht nachvollziehbar, wodurch sich eine Situation kennzeichnet, in der die außenpolitische Handlungsfähigkeit der Bundesrepublik gefährdet ist. Wenn mit der Gesetzesbegründung davon ausgegangen wird, dass die außenpolitische Handlungsfähigkeit im Wesentlichen auf umfassenden Informationen über internationale Sachverhalte und Akteure beruht, so ist dieses Rechtsgut immer dann bedroht, wenn solche Informationen fehlen oder Lücken aufweisen. In der Folge dieses Begriffsverständnisses ermöglicht das Schutzgut der außenpolitischen Handlungsfähigkeit damit eine Informationsbeschaffung um der beschafften Informationen willen.

Schließlich ist unklar, inwieweit es einer Ermächtigung zu Überwachungen mit dem Ziel der Früherkennung von Gefahren für die außenpolitische Handlungsfähigkeit der Bundesrepublik neben der in § 19 Abs. 1 Nr. 1, Abs. 3 BNDG enthaltenen Ermächtigung zu Überwachungen zur politischen Unterrichtung der Bundesregierung bedarf. Wie bereits der Begriff der außen*politischen* Handlungsfähigkeit nahelegt und die Gesetzesbegründung erhärtet, geht es diesem Eingriffstatbestand darum, das nach außen gerichtete politische Handeln der Bundesrepublik zu unterstützen. Dieses Handeln ist – ungeachtet der Beteiligung des Bundestags und des Bundespräsidenten an der Ausübung der auswärtigen Gewalt – Sache der Bundesregierung,

> vgl. zu den Organkompetenzen für die auswärtige Gewalt statt vieler Sauer, Staatsrecht III, 7. Aufl. 2022, § 4 Rn. 27 ff.

Eine eigenständige Ermächtigung zur Früherkennung von Gefahren für die außenpolitische Handlungsfähigkeit der Bundesrepublik ist daher überflüssig. Zweck der Norm scheint stattdessen zu sein, Überwachungen unter den Voraussetzungen für die politische Unterrichtung und zugleich eine Übermittlung der Überwachungsergebnisse an andere Stellen als die Bundesregierung unter den Voraussetzungen für die Gefahrenfrüherkennung zu ermöglichen. Der Gefährdungstatbestand in § 19 Abs. 4 Nr. 2 lit. d BNDG unterläuft so die gebotene Differenzierung beider Aufklärungsziele und die verfassungsrechtliche Wertung, dass eine Gefahrenfrüherkennung gerade nicht generell zur Gewinnung außen- und sicherheitspolitisch relevanter Informationen, sondern nur zum Schutz gegen herausgehobene Gefährdungen zugelassen werden darf.

3. Betroffene

Die strategische Telekommunikationsüberwachung kann nur als Instrument der Auslandsaufklärung gerechtfertigt werden. Der Gesetzgeber muss darum

Regelungen zur Aussonderung von Daten aus der Inlandskommunikation schaffen,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 170 ff.

Diese verfassungsrechtliche Vorgabe wird durch § 19 Abs. 7 BNDG umgesetzt. Diese Vorschrift ist jedoch defizitär, da sie nicht alle Inländerinnen und Inländer erfasst.

Darüber hinaus führen § 19 Abs. 7 und § 20 Abs. 1 BNDG zu einer Schlechterstellung von Unionsbürgerinnen und Unionsbürgern sowie von juristischen Personen aus anderen Mitgliedstaaten der Europäischen Union, die sich – auch aufgrund unionsgrundrechtlicher Wertungen – vor dem allgemeinen Gleichheitssatz des Art. 3 Abs. 1 GG nicht rechtfertigen lässt.

a) Inländerinnen und Inländer mit ausländischer Staatsangehörigkeit

Nach § 19 Abs. 7 Satz 1 BNDG erstreckt sich die strategische Ausland-Fernmeldeaufklärung nicht auf personenbezogene Daten von deutschen Staatsangehörigen, inländischen juristischen Personen sowie sich im Bundesgebiet aufhaltenden natürlichen Personen mit ausländischer Staatsangehörigkeit. Diese Vorgabe schützt nicht alle Personen, die von Verfassungs wegen als Inländerinnen und Inländer von der Überwachung ausgenommen werden müssen. Es fehlt eine Schutzregelung für ausländische Staatsangehörige, die sich temporär im Ausland aufhalten, deren Wohnsitz oder gewöhnlicher Aufenthaltsort sich jedoch in der Bundesrepublik befindet.

Der für die verfassungsrechtlichen Grenzen der strategischen Telekommunikationsüberwachung maßgebliche verfassungsrechtliche Inländerbegriff umfasst mehrere Personengruppen, die von der Überwachung auszunehmen sind. Als Inländerinnen und Inländer sind zum einen deutsche Staatsangehörige unabhängig von ihrem Wohnsitz oder ihrem gegenwärtigen Aufenthaltsort anzusehen. Zum anderen können auch Personen mit ausländischer Staatsangehörigkeit einen Schutz gegen strategische Überwachungsmaßnahmen genießen. Das Bundesverfassungsgericht stellt in seinem Urteil zur Ausland-Ausland-Fernmeldeaufklärung dementsprechend an verschiedenen Stellen deutsche Staatsangehörige und (sonstige) Inländer nebeneinander,

vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 147, 171, 174, 253, 264, 268, 278, 288.

Maßgebliches Kriterium für die Reichweite des Inländerschutzes ist, dass Inländerinnen und Inländer in gesteigertem Maße dem Zugriff deutscher Behör-

den unterliegen und darum eher Folgemaßnahmen ausgesetzt sind als Ausländer im Ausland, die allenfalls in Sonderfällen in unmittelbaren Kontakt mit der deutschen Hoheitsgewalt geraten. Ihnen sind darum die mit einer strategischen Telekommunikationsüberwachung verbundenen qualifizierten Risiken nicht zumutbar,

> vgl. zu diesem Schutzzweck mit Blick auf deutsche Staatsangehörige, aber insoweit verallgemeinerbar BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 186.

Neben deutschen Staatsangehörigen und Personen, die sich zum Überwachungszeitpunkt in der Bundesrepublik aufhalten, sind auch Ausländerinnen und Ausländer mit inländischem Wohnsitz oder gewöhnlichem Aufenthaltsort im Inland unabhängig von ihrem Aufenthaltsort zum Zeitpunkt der Überwachung besonders schutzbedürftig. Denn diese Personen weisen eine spezifische Bindung an die Bundesrepublik auf, die sie in besonderem Ausmaß dem Zugriff deutscher hoheitlicher Stellen aussetzt. Im Vergleich zu deutschen Staatsangehörigen, die sich dauerhaft im Ausland aufhalten, erscheint ihre Vulnerabilität sogar eher gesteigert. Die Herausnahme dieser Personengruppe aus dem Überwachungsschutz des § 19 Abs. 7 BNDG ist daher sachwidrig und nicht zu rechtfertigen,

> Gärditz, BT-Ausschussdrs. 19(4)731 A, S. 4.

Diesem Befund lassen sich nicht denkbare praktische Schwierigkeiten entgegenhalten, die Telekommunikation von Ausländerinnen und Ausländern zu identifizieren, die sich zwar zum Kommunikationszeitpunkt im Ausland aufhalten, ihren Wohnsitz oder gewöhnlichen Aufenthaltsort jedoch in der Bundesrepublik haben. Diese Schwierigkeiten gehen nicht über die von § 19 Abs. 7 BNDG ohnehin geforderte Identifikation der Telekommunikation von deutschen Staatsangehörigen im Ausland hinaus. Ihnen begegnet die gesetzliche Vorgabe, dass die Überwachung auch zulässig ist, wenn eine Unterscheidung von Inlands- und Auslandskommunikation nicht trennscharf möglich ist, sofern die erhobenen Daten unverzüglich gelöscht werden, sobald sich zeigt, dass sie Inländerinnen und Inländer betreffen.

b) Unionsbürgerinnen und Unionsbürger

Sowohl gegen das Fernmeldegeheimnis des Art. 10 GG als auch gegen den allgemeinen Gleichheitssatz des Art. 3 Abs. 1 GG verstößt § 20 Abs. 1 BNDG, der hinsichtlich von Unionsbürgerinnen und Unionsbürgern eine gezielte Datenerhebung in weitem Umfang und eine Weiterverarbeitung ungezielt erhobener Daten ohne qualifizierte Voraussetzungen zulässt. Diese Regelung stellt

Unionsbürgerinnen und Unionsbürger wesentlich schlechter als deutsche Staatsangehörige, sofern sich diese Personen jeweils im Ausland aufhalten.

Das Bundesverfassungsgericht hat in seinem Urteil zur Ausland-Ausland-Fernmeldeaufklärung offengelassen, ob die Ungleichbehandlung von Unionsbürgerinnen und Unionsbürgern gegenüber Deutschen gerechtfertigt werden kann,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 112.

Im vorliegenden Verfahren ist diese Frage zu entscheiden. Dabei sind für die verfassungsrechtliche Maßstabsbildung neben den deutschen Grundrechten in ihrer hergebrachten Auslegung auch die Unionsgrundrechte auf Achtung des Privatlebens (Art. 7 GRCh) und auf Schutz personenbezogener Daten (Art. 8 GRCh) sowie das Verbot einer Diskriminierung aus Gründen der Staatsangehörigkeit (Art. 21 Abs. 2 GRCh) heranzuziehen. Denn die Unionsgrundrechte bilden eine Rechtserkenntnisquelle für die Auslegung der Grundrechte des Grundgesetzes und definieren in ihrem Anwendungsbereich ein Mindestniveau des Grundrechtsschutzes, das bei der Auslegung und Anwendung der Grundrechte des Grundgesetzes zu beachten ist,

> BVerfGE 152, 152 (177 ff., 180 ff.).

aa) Anwendungsbereich der Unionsgrundrechte

Der Anwendungsbereich der Unionsgrundrechte ist gemäß Art. 51 Abs. 1 Satz 1 GRCh eröffnet. Für die Bindung eines Mitgliedstaats an die Unionsgrundrechte kommt es nach dieser Norm maßgeblich darauf an, ob dieser Mitgliedstaat Unionsrecht durchführt.

Der Gerichtshof der Europäischen Union versteht den Begriff der Durchführung des Unionsrechts in seiner Rechtsprechung seit jeher weit. Unter anderem unterfallen diesem Begriff zum einen mitgliedstaatliche Regelungen und darauf beruhende Handlungen mitgliedstaatlicher Behörden, die unionsrechtlichen Bindungen unterliegen, ohne notwendigerweise durch unionsrechtliche Vorgaben vollständig determiniert zu werden,

> vgl. etwa EuGH, Urteil vom 26. Februar 2013, Rs. C-617/10 – Åkerberg Fransson, Rn. 19 ff.; Urteil vom 29. Juli 2019, Rs. C-476/17 – Pelham u.a., Rn. 79.

Zum anderen handelt es sich auch um eine Durchführung des Unionsrechts im Sinne von Art. 51 Abs. 1 Satz 1 GRCh, wenn mitgliedstaatliche Regelungen und darauf beruhende Handlungen mitgliedstaatlicher Behörden die Wirtschaftsfreiheiten des AEUV beschränken,

vgl. etwa EuGH, Urteil vom 30. April 2014, Rs. C-390/12 – Pfleger, Rn. 35 f.

Nach diesen Maßstäben ist die strategische Ausland-Fernmeldeaufklärung zumindest zu erheblichen Teilen als Durchführung des Unionsrechts einzustufen.

(1) Unmittelbare Bindung des Bundesnachrichtendienstes an das allgemeine europäische Datenschutzrecht

Es spricht viel dafür, dass weite Teile der strategischen Ausland-Fernmeldeaufklärung bereits deshalb als Durchführung des Unionsrechts anzusehen sind, weil der Bundesnachrichtendienst hierbei unmittelbar an Vorschriften des in der Datenschutz-Grundverordnung (im Folgenden: DSGVO) geregelten allgemeinen europäischen Datenschutzrechts gebunden ist.

Der räumliche Anwendungsbereich der DSGVO ist für den Bundesnachrichtendienst als deutsche Behörde unabhängig vom Ort der Datenverarbeitung und von der Staatsangehörigkeit und dem Aufenthaltsort der betroffenen Personen gemäß Art. 3 Abs. 1 DSGVO eröffnet. Der Bundesnachrichtendienst erhebt und verwendet Daten im Rahmen der strategischen Ausland-Fernmeldeaufklärung im Rahmen seines allgemeinen Auftrags zur Auslandsaufklärung, der mit seinem inländischen Behördensitz untrennbar verknüpft ist,

vgl. zum räumlichen Anwendungsbereich mit Blick auf Behörden Reimer, Verwaltungsdatenschutzrecht, 2019, Rn. 89.

Auch der sachliche Anwendungsbereich der DSGVO ist zumindest für erhebliche Teilbereiche der strategischen Ausland-Fernmeldeaufklärung eröffnet. Die allgemeinen Voraussetzungen des Art. 2 Abs. 1 DSGVO liegen vor, da der Bundesnachrichtendienst bei der Aufklärung in großem Ausmaß personenbezogene Daten automatisiert verarbeitet. Die strategische Ausland-Fernmeldeaufklärung fällt auch zumindest nicht generell unter einen der Ausnahmetatbestände des Art. 2 Abs. 2 DSGVO.

Nicht anwendbar auf die strategische Ausland-Fernmeldeaufklärung ist Art. 2 Abs. 2 lit. d DSGVO, nach dem die Verordnung nicht für Datenverarbeitungen durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit gilt. Der Bundesnachrichtendienst ist, selbst soweit er zur Gefahrenfrüherkennung tätig wird, keine zuständige Behörde in diesem Sinne, da er an der Verhütung oder Verfolgung von Straftaten nicht unmittelbar beteiligt ist

und sich mangels operativer Befugnisse auch nicht unmittelbar daran beteiligen kann. Im Übrigen würde die Anwendung des Ausnahmetatbestands in Art. 2 Abs. 2 lit. d DSGVO lediglich dazu führen, dass statt der DSGVO die Richtlinie (EU) 2016/680 über den Datenschutz bei Polizei und Strafjustiz anwendbar wäre. An dem hier maßgeblichen Befund, dass die Aufklärungstätigkeit des Bundesnachrichtendienstes als Durchführung des Unionsrechts anzusehen ist, würde sich hierdurch nichts ändern.

Zudem fällt zumindest nicht die gesamte strategische Ausland-Fernmeldeaufklärung unter den Ausnahmetatbestand des Art. 2 Abs. 2 lit. a DSGVO, nach dem die Verordnung nicht auf Datenverarbeitungen im Rahmen einer Tätigkeit anzuwenden ist, die nicht in den Anwendungsbereich des Unionsrechts fällt.

Für die Aufklärungstätigkeit des Bundesnachrichtendienstes ist bedeutsam, dass aufgrund von Art. 4 Abs. 2 Satz 3 EUV die nationale Sicherheit in die alleinige Verantwortung der einzelnen Mitgliedstaaten und damit nicht in den Anwendungsbereich des Unionsrechts fällt. Die nationale Sicherheit wird auch in Erwägungsgrund 16 der Verordnung, der sich auf Art. 2 Abs. 2 lit. a DSGVO bezieht, ausdrücklich genannt. Wie weit die Bereichsausnahme für die nationale Sicherheit genau reicht, ist allerdings in der Rechtsprechung des Gerichtshofs der Europäischen Union noch nicht abschließend geklärt. Der Gerichtshof geht aber jedenfalls von einer engen Begriffsbildung aus und ordnet dem Schutz der nationalen Sicherheit lediglich „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“ zu,

> so mit Blick auf Art. 15 Abs. 1 RL 2002/58/EG EuGH, Urteil vom 6. Oktober 2020, Rs. C-511/18, C-512/18 und C-520/18 – La Quadrature du Net u.a., Rn. 135.

Weniger existenzielle und herausgehobene Bedrohungen unterfallen hingegen nicht der nationalen Sicherheit, selbst wenn sie schwere Schäden verursachen können,

> vgl. mit Blick auf Art. 15 Abs. 1 RL 2002/58/EG zur Bekämpfung selbst besonders schwerer Kriminalität EuGH, Urteil vom 5. April 2022, Rs. C-140/20 – Commissioner of An Garda Síochána u.a., Rn. 62; Urteil vom 20. September 2022, Rs. C-793/19 und C-794/19 – SpaceNet u.a., Rn. 93.

Angesichts dieser sehr engen Begriffsbildung liegt es fern, die strategische Ausland-Fernmeldeaufklärung generell dem Schutz der nationalen Sicherheit zuzuschlagen und darum dem Anwendungsbereich der DSGVO zu entziehen. Der Bundesnachrichtendienst darf dieses Instrument zu einer Vielzahl von Aufklärungszwecken einsetzen, die nicht durchweg mit existenziellen und herausgehobenen Bedrohungen einhergehen.

So darf der Bundesnachrichtendienst Überwachungen zur politischen Unterrichtung der Bundesregierung grundsätzlich in seinem gesamten Aufgabenbereich zur Gewinnung außen- und sicherheitspolitisch bedeutsamer Informationen durchführen. Die Außen- und Sicherheitspolitik eines international stark verflochtenen Staates wie der Bundesrepublik lässt sich jedoch nicht auf den Schutz der nationalen Sicherheit reduzieren. Sie umfasst etwa wirtschaftliche oder kulturelle Vorgänge von politischer Bedeutung, selbst wenn von ihnen keine unmittelbaren Bedrohungen für inländische Rechtsgüter ausgehen.

Soweit der Bundesnachrichtendienst strategische Telekommunikationsüberwachungen zur Gefahrenfrüherkennung durchführen darf, beschränken sich die gesetzlichen Ermächtigungen gleichfalls nicht durchweg auf den Schutz der nationalen Sicherheit in dem engen Begriffsverständnis des Gerichtshofs der Europäischen Union. So erlaubt § 19 Abs. 4 BNDG Aufklärungsmaßnahmen unter anderem zur Aufklärung des (nicht-terroristischen) gewaltbereiten Extremismus, von Cyberkriminalität und Organisierter Kriminalität oder zum Schutz hochrangiger Individualrechtsgüter unabhängig von Quelle und Art der Bedrohung. Hierbei geht es um einen Schutz gegen gewichtige, aber nicht notwendigerweise existenzielle und herausgehobene Bedrohungen.

Schließlich unterfällt die strategische Ausland-Fernmeldeaufklärung nicht generell dem Ausnahmetatbestand des Art. 2 Abs. 2 lit. b DSGVO für mitgliedstaatliche Tätigkeiten im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik. Das BNDG beschränkt die Aufklärung nicht auf Erkenntnisziele, die im Zusammenhang mit dem außenpolitischen Handeln der Europäischen Union oder mit gemeinsamen Maßnahmen der Mitgliedstaaten und der Union stehen, sondern lässt sie auch zur eigenständigen Wahrung rein nationaler Interessen zu.

Insgesamt fällt daher die strategische Ausland-Fernmeldeaufklärung, wie sie das BNDG anlegt, in beträchtlichem Umfang unmittelbar in den Anwendungsbereich der DSGVO. Ihre gesetzlichen Grundlagen sind aus unionsrechtlicher Sicht primär auf die Öffnungsklauseln in Art. 6 Abs. 2 und Abs. 3 DSGVO zu stützen. Insoweit handelt es sich bei der Regelsetzung ebenso wie bei der

Anwendung dieser Regelungen um eine Durchführung von Unionsrecht im Sinne von Art. 51 Abs. 1 Satz 1 DSGVO.

(2) Mittelbare Bindung durch das Telekommunikations-Datenschutzrecht

Auch soweit der Bundesnachrichtendienst unmittelbar nicht an das europäische Datenschutzrecht gebunden ist, fällt die strategische Ausland-Fernmeldeaufklärung teils mittelbar in den Anwendungsbereich datenschutzrechtlicher Vorgaben. Diese mittelbare Bindung entsteht in den Fällen, in denen der Bundesnachrichtendienst sich Inhalts- und Verkehrsdaten von den Anbietern von Telekommunikationsdiensten ausleiten lässt. Die dazu erforderlichen Mitwirkungshandlungen der Diensteanbieter unterfallen dem Telekommunikations-Datenschutzrecht, das auf der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation beruht. Die Diensteanbieter benötigen zu ihrer Mitwirkung eine datenschutzrechtliche Erlaubnis. Art. 15 Abs. 1 RL 2002/58/EG ermöglicht den Mitgliedstaaten, solche Verarbeitungserlaubnisse (und zugehörige Verarbeitungspflichten) der Diensteanbieter zu schaffen.

Aufgrund von Art. 15 Abs. 1 RL 2002/58/EG führen neben den an die Diensteanbieter gerichteten Erlaubnisnormen auch die korrespondierenden Ermächtigungen der Sicherheitsbehörden zur Erhebung und Weiterverarbeitung der ausgeleiteten Daten im Sinne von Art. 51 Abs. 1 Satz 1 GRCh Unionsrecht durch. Die Erlaubnis zur Ausleitung der Daten steht mit der Öffnungsklausel nur in Einklang, wenn sie einem der in ihr genannten Zwecke – unter anderem dem Schutz der nationalen Sicherheit – dient und in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Dies lässt sich nur mit Blick auf die Weiterverarbeitung der ausgeleiteten Daten beurteilen. Ist die Erhebung und Weiterverarbeitung der Daten durch den Bundesnachrichtendienst nicht hinreichend restriktiv geregelt, so kann auch ihre Ausleitung durch die Diensteanbieter nicht gerechtfertigt werden. Ist wiederum die Ausleitung der Daten unzulässig, so darf auch ihre Weiterverarbeitung nicht zugelassen werden.

Dieser mittelbare Kontrollansatz ist in der Rechtsprechung des Gerichtshofs der Europäischen Union mittlerweile etabliert. Er ist insbesondere auch dann zu beachten, wenn die Weiterverarbeitung der Daten durch die Empfangsbehörde für sich genommen nicht in den Anwendungsbereich des Unionsrechts fällt. Die strategische Ausland-Fernmeldeaufklärung ist daher ungeachtet von Art. 4 Abs. 2 Satz 3 EUV mittelbar auch insoweit an den Unionsgrundrechten zu messen, als sie dem Schutz der nationalen Sicherheit dient,

vgl. zur Ausleitung inländischer Verkehrsdaten EuGH, Urteil vom 6. Oktober 2020, Rs. C-623/17 – Privacy International, Rn. 34 ff.

(3) Einschränkung von Grundfreiheiten

Schließlich kann die strategische Ausland-Fernmeldeaufklärung zu einer Einschränkung der Wirtschaftsfreiheiten des AEUV führen. Diese Freiheiten schützen durchweg neben Diskriminierungen und imperativen Beschränkungen auch vor Maßnahmen der Mitgliedstaaten, die eine grenzüberschreitende wirtschaftliche Tätigkeit lediglich faktisch erschweren,

vgl. im Überblick Herdegen, Europarecht, 24. Aufl. 2023, § 14 Rn. 3 ff.; beispielhaft für die ständige Rechtsprechung EuGH, Urteil vom 10. Mai 1995, Rs. C-384/93 – Alpine Investments, Rn. 35; Urteil vom 30. November 1995, Rs. C-55/94 – Gebhard, Rn. 37; Urteil vom 16. März 2010, Rs. C-325/08 – Olympique Lyonnais, Rn. 34.

Aufklärungsmaßnahmen des Bundesnachrichtendienstes können grenzüberschreitende wirtschaftliche Tätigkeiten erheblich erschweren und sind darum insoweit an den Wirtschaftsfreiheiten zu messen. Beispielhaft lässt sich dies an den Beschwerdeführerinnen zu 6 und 7 und an dem Beschwerdeführer zu 8 aufzeigen, die grenzüberschreitend als investigative Journalisten tätig sind, indem sie auch in Medien aus anderen Mitgliedstaaten der Europäischen Union als ihrem Wohnsitzstaat veröffentlichen. Sie sind für diese Tätigkeit zwingend auf die Vertraulichkeit der Kommunikation mit ihren Quellen angewiesen. Die strategische Überwachung der ausländischen Telekommunikation kann diese Vertraulichkeit in beträchtlichem Maße aufheben. Dies bedroht den Informationszugang der Beschwerdeführerinnen zu 6 und 7 und des Beschwerdeführers zu 8 und stellt mittelbar den Fortbestand ihrer grenzüberschreitenden Dienstleistungstätigkeit in Frage.

Dem Befund, dass derartige Beschränkungen an den Wirtschaftsfreiheiten des AEUV zu messen sind, lässt sich wiederum nicht entgegenhalten, dass gemäß Art. 4 Abs. 2 Satz 3 EUV die nationale Sicherheit in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt. Diese Vorschrift errichtet eine Kompetenzausübungsschranke der Europäischen Union, begrenzt also deren aktives Tätigwerden in einem bestimmten Sachbereich,

vgl. Schill/Krenn, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, Art. 4 EUV Rn. 45; Obwexer, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, Art. 4 EUV Rn. 52.

Hingegen stellt Art. 4 Abs. 2 Satz 3 EUV die Mitgliedstaaten nicht generell davon frei, beim Schutz der nationalen Sicherheit unionsrechtliche Pflichten wie die Grundfreiheiten und das allgemeine Diskriminierungsverbot des AEUV zu beachten, wo der Anwendungsbereich dieser Regelungen eröffnet ist. Der Schutz der nationalen Sicherheit kann lediglich herangezogen werden, um Einschränkungen der Grundfreiheiten und des Diskriminierungsverbots zu rechtfertigen, soweit diese Einschränkungen sich auf das erforderliche und angemessene Maß beschränken,

> vgl. Schill/Krenn, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, Art. 4 EUV Rn. 47; Obwexer, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, Art. 4 EUV Rn. 53.

bb) Ungleichbehandlung von Unionsbürgerinnen und Unionsbürgern und deutschen Staatsangehörigen

Die Regelungen über die strategische Ausland-Fernmeldeaufklärung stellen Unionsbürgerinnen und Unionsbürger, die sich außerhalb der Bundesrepublik aufhalten, weitaus schlechter als deutsche Staatsangehörige, die sich außerhalb der Bundesrepublik aufhalten.

Deutsche Staatsangehörige genießen gemäß § 19 Abs. 7 Satz 1 Nr. 1 BNDG unabhängig von ihrem Wohn- oder Aufenthaltsort einen umfassenden Überwachungsschutz. Der Bundesnachrichtendienst darf Inhalte ihrer Fernkommunikation auch dann, wenn sie sich im Ausland aufhalten, weder gezielt noch ungezielt erheben. Er muss automatisierte Filtertechnik einsetzen, um eine solche Datenerhebung möglichst zu vermeiden. Soweit der Bundesnachrichtendienst gleichwohl Kommunikationsinhalte von deutschen Staatsangehörigen erhebt, muss er sie unverzüglich löschen. Eine Ausnahme von dieser Löschpflicht gilt lediglich, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass durch die Weiterverarbeitung der Daten eine erhebliche Gefahr für Leib, Leben oder Freiheit einer Person, die Sicherheit des Bundes oder eines Landes oder die Sicherheit anderer Mitgliedstaaten der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages abgewendet werden kann. Schließlich ist die gesamthaft bevorratende Verkehrsdatenspeicherung über deutsche Staatsangehörige gemäß § 26 Abs. 3 Satz 1 Nr. 1 BNDG grundsätzlich unzulässig; Ausnahmen bestehen für Metadaten der intermaschinellen Kommunikation sowie für unkenntlich gemachte Verkehrsdaten,

> siehe unten C. I. 5. b) ee) und ff).

Hingegen fallen Unionsbürgerinnen und Unionsbürger, die sich im Ausland aufhalten und darum keinen Überwachungsschutz als Inländerinnen und Inländer nach § 19 Abs. 7 Satz 1 Nr. 3 BNDG genießen, unter die Schutzregelung des § 20 Abs. 1 BNDG. Diese Norm beschränkt lediglich die gezielte Datenerhebung, also den Einsatz von personenbezogenen Suchbegriffen, wie beispielsweise der E-Mail-Adresse eines Unionsbürgers oder einer Unionsbürgerin. Eine ungezielte Datenerhebung über Unionsbürgerinnen oder Unionsbürger – etwa als Kommunikationspartner von Drittstaatsangehörigen oder auf der Grundlage eines inhaltsbezogenen Suchbegriffs wie beispielsweise einer chemischen Formel oder der Signatur einer Schadsoftware – ist unter den allgemein für Ausländerinnen und Ausländer im Ausland geltenden Voraussetzungen zulässig. Selbst die gezielte Erhebung von Daten über Unionsbürgerinnen und Unionsbürger ist zudem in weitem Umfang zulässig: zur politischen Unterrichtung der Bundesregierung, wenn ausschließlich Daten über Vorgänge in Drittstaaten gewonnen werden sollen, die von besonderer außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, und zur Gefahrenfrüherkennung ohne Einschränkungen. Hinsichtlich der gesamthaft bevorratenden Verkehrsdatenspeicherung enthält § 26 BNDG überhaupt keine Schutzregelungen für Unionsbürgerinnen und Unionsbürger.

Insgesamt genießen also Unionsbürgerinnen und Unionsbürger, die sich im Ausland aufhalten, nur gegen die gezielte Erhebung von Inhaltsdaten zum Zweck der politischen Unterrichtung einen partiellen Überwachungsschutz. Ansonsten sind sie der strategischen Ausland-Fernmeldeaufklärung im selben Ausmaß ausgesetzt wie Drittstaatsangehörige im Ausland.

cc) Kontrollmaßstab

Diese Ungleichbehandlung von deutschen Staatsangehörigen und Unionsbürgerinnen und Unionsbürgern im Ausland ist nach einem strengen Kontrollmaßstab zu bewerten.

Hohe Anforderungen ergeben sich bereits auf der Grundlage des vom Bundesverfassungsgericht zu Art. 3 Abs. 1 GG entwickelten gleitenden Kontrollrahmens,

zusammenfassend Britz, NJW 2014, S. 346 ff.

Die Ungleichbehandlung knüpft – bezogen auf Personen, die sich im Ausland aufhalten, als Oberbegriff – allein an die Staatsangehörigkeit und damit ein Merkmal an, das für die Betroffenen weitgehend unverfügbar ist,

vgl. BVerfGE 130, 240 (255); 138, 136 (181).

Zudem haben Unionsbürgerinnen und Unionsbürger, die sich im Ausland aufhalten, in der Regel keine zumutbare Möglichkeit, der strategischen Telekommunikationsüberwachung durch eigenes Verhalten zu entgehen,

vgl. BVerfG, Beschluss vom 21. Juli 2022 – 1 BvR 469/20 u.a. –, Rn. 157.

Insbesondere ist der denkbare Ausweg, sich dauerhaft in die Bundesrepublik zu begeben und dort den für Inländerinnen und Inländer geltenden Überwachungsschutz zu genießen, für Personen mit Lebensmittelpunkt im Ausland auch dann kaum gangbar, wenn sie als Unionsbürgerinnen und Unionsbürger hierzu grundsätzlich berechtigt wären.

Schließlich steht die Ungleichbehandlung in unmittelbarem Zusammenhang mit einem – sehr schwerwiegenden – Eingriff in das Grundrecht aus Art. 10 GG,

vgl. BVerfGE 88, 87 (96); 145, 20 (87).

Der Kontrollmaßstab ist weiter zu verschärfen, um den Anforderungen des unionsrechtlichen Diskriminierungsverbots aus Art. 21 Abs. 2 GRCh Rechnung zu tragen. Diese Norm entspricht inhaltlich Art. 18 Abs. 1 AEUV. Zu ihrer Konkretisierung kann daher auch auf die Rechtsprechung des Gerichtshofs zu dieser Vorschrift zurückgegriffen werden,

EuGH, Urteil vom 10. Oktober 2019, Rs. C-703/17 – Krah, Rn. 18.

Das unionsrechtliche Diskriminierungsverbot aus Art. 21 Abs. 2 GRCh und Art. 18 Abs. 1 AEUV errichtet besonders strenge Anforderungen an unmittelbare Diskriminierungen aufgrund der Staatsangehörigkeit. Eine solche unmittelbare Diskriminierung sehen § 19 Abs. 7 und § 20 Abs. 1 BNDG mit Blick auf Personen vor, die sich im Ausland aufhalten. Die Reichweite des Überwachungsschutzes, den diese Personen genießen, richtet sich unmittelbar und ausschließlich nach ihrer Staatsangehörigkeit.

Nach der jüngeren Rechtsprechung des Gerichtshofs der Europäischen Union sind unmittelbare Diskriminierungen aufgrund der Staatsangehörigkeit im Anwendungsbereich von Art. 21 Abs. 2 GRCh und Art. 18 Abs. 1 AEUV zwar nicht generell unzulässig. Eine Schlechterstellung von Unionsbürgerinnen und Unionsbürgern gegenüber inländischen Staatsangehörigen kann aber nur ausnahmsweise gerechtfertigt werden, wenn sie auf objektiven, von der Staatsangehörigkeit der Betroffenen unabhängigen Erwägungen beruht und in einem angemessenen Verhältnis zu einem legitimerweise verfolgten Zweck steht,

EuGH, Urteil vom 16. Dezember 2008, Rs. C-524/06 – Huber, Rn. 75; ferner EuGH, Urteil vom 6. September 2016, Rs. C-182/15 – Petruhhin, Rn. 34 und 38; Urteil vom 10. April 2018, Rs. C-191/16 – Pisciotti, Rn. 46.

Bei der Prüfung, ob die Ungleichbehandlung gerechtfertigt werden kann, sind auch die besondere rechtliche Verflechtung der Mitgliedstaaten durch unionsrechtliche Vorgaben und das in Art. 4 Abs. 3 EUV verankerte Gebot der loyalen Zusammenarbeit und wechselseitigen Unterstützung zu beachten,

EuGH, Urteil vom 6. September 2016, Rs. C-182/15 – Petruhhin, Rn. 42.

dd) Verfassungswidrigkeit der Ungleichbehandlung

Nach diesem Maßstab kann die in § 19 Abs. 7, § 20 Abs. 1 und § 26 BNDG angelegte Ungleichbehandlung zwischen deutschen Staatsangehörigen und Unionsbürgerinnen und Unionsbürgern im Ausland zumindest nicht in dem gesetzlich vorgesehenen Ausmaß gerechtfertigt werden. Die Gründe, mit denen das Bundesverfassungsgericht die strategische Telekommunikationsüberwachung als Maßnahme (allein) der Auslandsaufklärung legitimiert und insoweit eine Ungleichbehandlung von deutschen und ausländischen Staatsangehörigen akzeptiert hat, kommen hier nicht oder zumindest nur mit geringerem Gewicht zum Tragen.

Soweit das Bundesverfassungsgericht zur Rechtfertigung der strategischen Telekommunikationsüberwachung auf spezifische Aufklärungshürden im Ausland verwiesen hat,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 159,

ergeben sich diese Hürden aus dem Zielort der Überwachung, nicht aber aus der Staatsangehörigkeit der betroffenen Personen. Das Verhalten deutscher Staatsangehöriger im Ausland lässt sich genauso gut oder schlecht beobachten wie das Verhalten von Unionsbürgerinnen und Unionsbürgern im Ausland.

Im Übrigen bestehen gegenüber Unionsbürgerinnen und Unionsbürgerinnen typischerweise weitaus weiterreichende Aufklärungsmöglichkeiten als gegenüber Drittstaatsangehörigen. Es erscheint plausibel, dass sich die meisten Unionsbürgerinnen und Unionsbürger primär in der Europäischen Union aufhalten. Innerhalb der Europäischen Union sind die vom Bundesverfassungsgericht hervorgehobenen Aufklärungsschwierigkeiten durch die Zusammenarbeit der Mitgliedstaaten auf den Feldern der inneren und äußeren Sicherheit abge-

mildert. So ermöglicht die polizeiliche und justizielle Zusammenarbeit in Strafsachen eine im Vergleich zur internationalen Rechtshilfe erheblich beschleunigte und friktionsärmere Beschaffung von Beweismitteln und sonstigen für die Strafverfolgung relevanten Erkenntnissen.

Umgekehrt trägt das Argument, die strategische Telekommunikationsüberwachung berge für Ausländerinnen und Ausländer im Ausland geringere Folgerisiken als für deutsche Staatsangehörige im Ausland,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 165, 186,

mit Blick auf Unionsbürgerinnen und Unionsbürger allenfalls begrenzt. Insbesondere wenn sich diese Personen – wie typischerweise – innerhalb der Europäischen Union aufhalten, bestehen ihnen gegenüber aufgrund der Instrumente der europäischen Sicherheitszusammenarbeit deutlich erweiterte Zugriffsmöglichkeiten der deutschen Staatsgewalt. Beispielsweise können mithilfe Europäischer Haftbefehle Unionsbürgerinnen und Unionsbürger sogar aus ihren Heimatstaaten zuverlässig einer Strafverfolgung in der Bundesrepublik zugeführt werden. Soweit es um Personen geht, die sich innerhalb der Europäischen Union aufhalten, kommen die Eingriffspotenziale der deutschen Hoheitsgewalt gegenüber Unionsbürgerinnen und Unionsbürgern denen gegenüber deutschen Staatsangehörigen zumindest nahe.

Insgesamt unterscheiden sich somit die Situationen von deutschen Staatsangehörigen im Ausland und von Unionsbürgerinnen und Unionsbürgern im Ausland mit Blick auf strategische Telekommunikationsüberwachungen nicht so stark, dass sich die sehr weitgehende Freigabe einer Überwachung durch § 20 Abs. 1 und § 26 BNDG legitimieren ließe. Vielmehr ist auch gegenüber Unionsbürgerinnen und Unionsbürgern im Ausland, mindestens aber innerhalb der Europäischen Union eine strategische Telekommunikationsüberwachung als unverhältnismäßig anzusehen. Selbst wenn dies anders zu sehen wäre, müsste der Überwachungsschutz von Unionsbürgerinnen und Unionsbürgern im Ausland deutlich gestärkt werden. Hierzu müsste zum einen die – gezielte oder ungezielte – Inhaltsüberwachung zur Gefahrenfrüherkennung auf materiell besonders herausgehobene Gefährdungslagen beschränkt werden, die sich in tatsächlicher Hinsicht zumindest ansatzweise konturiert abzeichnen. Zum anderen müsste der Überwachungsschutz auf die bevorratende Verkehrsdatenspeicherung erstreckt werden.

c) EU-ausländische juristische Personen des Privatrechts

Die Regelungen über die strategische Ausland-Fernmeldeaufklärung verletzen Art. 10 und Art. 3 Abs. 1 GG schließlich auch insoweit, als es an gesetzlichen Vorgaben zum Schutz EU-ausländischer juristischer Personen des Privatrechts fehlt. Dies führt zu einer Schlechterstellung solcher Personen gegenüber inländischen juristischen Personen, die gemäß § 19 Abs. 7 Satz 1 Nr. 2 und § 26 Abs. 3 Satz 1 Nr. 2 BNDG denselben Überwachungsschutz wie deutsche Staatsangehörige genießen.

Hinsichtlich dieser Ungleichbehandlung ist ein strenger Rechtfertigungsmaßstab anzulegen, der auch unionsrechtliche Anforderungen einbeziehen muss. Dies folgt zum einen aus den allgemeinen Diskriminierungsverboten aus Art. 21 Abs. 2 GRCh und Art. 18 AEUV, die auf EU-ausländische juristische Personen zu übertragen sind,

vgl. zu Art. 18 AEUV BVerfGE 129, 78 (94 ff.).

Zum anderen sind EU-ausländische juristische Personen durch die Grundfreiheiten des Binnenmarktrechts geschützt, die durch Maßnahmen der strategischen Ausland-Fernmeldeaufklärung berührt werden können, etwa wenn Einschüchterungseffekte dazu führen, dass EU-ausländische Personen wie die Beschwerdeführerin zu 1 grenzüberschreitende Dienstleistungen nicht mehr ungehindert erbringen oder beziehen können.

Die Ungleichbehandlung von inländischen und EU-ausländischen juristischen Personen kann demnach nur gerechtfertigt werden, wenn sie auf objektiven, von der rechtlichen Zugehörigkeit unabhängigen Sachgründen beruht und verhältnismäßig ist. Da es sich um eine unmittelbare Diskriminierung aufgrund des Sitzes der juristischen Person handelt, sind insoweit hohe Anforderungen zu stellen.

Nach diesem Maßstab kann die Schlechterstellung EU-ausländischer juristischer Personen mit Blick auf die Auslandskommunikation jedenfalls nicht in dem gesetzlich vorgesehenen Maß gerechtfertigt werden. Die Ausführungen zur Ungleichbehandlung von deutschen Staatsangehörigen und Unionsbürgerinnen und Unionsbürgern lassen sich insoweit übertragen: Aufklärungsprobleme hängen nicht von der rechtlichen Zugehörigkeit der betroffenen juristischen Person, sondern vom überwachten Ort ab. Gegenüber EU-ausländischen juristischen Personen bestehen weitaus weitergehende Erkenntnis- und Zugriffsmöglichkeiten der deutschen Staatsgewalt als gegenüber juristischen

Personen aus Drittstaaten. Die Stellung inländischer und EU-ausländischer juristischer Personen muss daher zumindest im Vergleich zur gegenwärtigen Rechtslage deutlich angenähert werden.

d) Anregung einer Vorlage an den Gerichtshof der Europäischen Union

Die aus Art. 7 und Art. 8 GRCh folgenden Anforderungen an strategische Telekommunikationsüberwachungen, die Unionsbürgerinnen und Unionsbürger betreffen, sind in der Rechtsprechung des Gerichtshofs der Europäischen Union bislang nicht aufgeworfen worden. Ob und gegebenenfalls inwieweit die Mitgliedstaaten angesichts von Art. 21 Abs. 2 GRCh bei der Durchführung solcher Überwachungen ihren eigenen Staatsangehörigen im Ausland einen weitergehenden Überwachungsschutz gewährleisten dürfen als Unionsbürgerinnen und Unionsbürgern im Ausland, ist ebenfalls bislang ungeklärt. Dasselbe gilt schließlich für die Frage nach der unionsrechtlichen Zulässigkeit einer unterschiedlichen Behandlung von in- und ausländischen juristischen Personen.

Da die unionsgrundrechtlichen Vorgaben für die Konturierung der Schutzgehalte von Art. 3 Abs. 1 und Art. 10 GG bedeutsam sind, rege ich an, vor einer Sachentscheidung im vorliegenden Verfahren eine Vorabentscheidung durch den Gerichtshof der Europäischen Union (Art. 267 AEUV) einzuholen,

> vgl. zur Behandlung dieser Fallkonstellation BVerfGE 152, 152 (183).

4. Schutz von Vertraulichkeitsbeziehungen

Besondere Anforderungen sind an den Schutz von Vertraulichkeitsbeziehungen – wie insbesondere zwischen Journalisten und ihren Informanten oder Rechtsanwälten und ihren Mandanten – zu stellen. Gegenüber Berufs- und Personengruppen, deren Kommunikationsbeziehungen einen besonderen Schutz der Vertraulichkeit verlangen, ist im Rahmen einer Überwachung zur Gefahrenfrüherkennung zunächst deren gezielte Überwachung zu begrenzen. Die Nutzung von Suchbegriffen, die zu einer gezielten Erfassung der Telekommunikationsanschlüsse solcher Personen führen, kann nicht schon allein damit gerechtfertigt werden, dass hierdurch potenziell nachrichtendienstlich relevante Informationen erlangt werden können. Deren gezielte Überwachung als Nachrichtenmittler ist vielmehr auch im Rahmen der strategischen Überwachung an qualifizierte Eingriffsschwellen zu binden. Soweit die Erfassung von besonders schutzwürdigen Vertraulichkeitsbeziehungen erst im Rahmen der Auswertung bemerkt wird, bedarf es auch insoweit einer Prüfung der Voraussetzungen und gegebenenfalls dann einer Abwägung, ob die entsprechende Kommunikation ausgewertet und genutzt werden darf,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 193 ff.

Diesen verfassungsrechtlichen Anforderungen genügen die Schutzregelungen in § 21 BNDG nicht vollständig.

Diese Regelungen gewährleisten zwar, dass Telekommunikationsinhalte, die unmittelbar aus einer Vertraulichkeitsbeziehung stammen, grundsätzlich nicht gezielt erhoben und bei einer unabsichtlichen Datenerhebung grundsätzlich nicht weiterverarbeitet werden dürfen. Auch der eng gefasste Ausnahmetatbestand in § 21 Abs. 2 BNDG ist für sich genommen nicht zu beanstanden.

Jedoch greift § 21 Abs. 1 Satz 1 BNDG insoweit zu kurz, als nur Inhalte geschützt werden, die unmittelbar „aus einer Vertraulichkeitsbeziehung“ stammen. Die Kommunikation „über eine Vertraulichkeitsbeziehung“ wird von der Norm hingegen nicht erfasst. Geschützt wird also etwa die Kommunikation zwischen einer Journalistin und ihrer Quelle oder zwischen einem Rechtsanwalt und seinem Mandanten, nicht aber die Weitergabe der betroffenen Inhalte von der Journalistin an die Redaktion oder von dem Rechtsanwalt an eine Kollegin, die dasselbe Mandat bearbeitet. Im Rahmen einer strategischen Ausland-Fernmeldeaufklärung könnte der Bundesnachrichtendienst dementsprechend die Telekommunikationsmerkmale der Journalistin oder des Rechtsanwalts als Suchbegriffe nutzen, um solche Kommunikationen über Vertraulichkeitsbeziehungen gezielt zu erheben. Entgegen dem Urteil zur Ausland-Ausland-Fernmeldeaufklärung gibt es also keinen prinzipiellen Schutz gegen eine gezielte Erfassung bestimmter Telekommunikationsanschlüsse, sondern nur einen Schutz gegen die gezielte Erfassung bestimmter Kommunikationsvorgänge.

Dieses Schutzdefizit lässt sich nicht mit der Erwägung legitimieren, dass der Vertraulichkeitsschutz nach § 21 BNDG den für innerstaatliche Telekommunikationsüberwachungen geltenden Vorkehrungen entspricht. Es trifft zwar zu, dass die gesetzlichen Regelungen zum Schutz von Vertraulichkeitsbeziehungen bei innerstaatlichen Überwachungen wie § 160a StPO oder § 62 BKAG gleichfalls nur die unmittelbare Kommunikation zwischen Vertrauenspersonen und den jeweils geschützten Personen von der Überwachung ausnehmen. Diese Schutzregelungen stehen jedoch in dem anders gelagerten Kontext individualisierender Überwachungsmaßnahmen.

Soweit nur individualisierende Überwachungsmaßnahmen im Raum stehen, muss eine Vertrauensperson in der Regel nicht damit rechnen, dass ihre Kommunikation mit Dritten über eine Vertraulichkeitsbeziehung gezielt überwacht

wird. Eine solche Überwachung würde voraussetzen, dass die Vertrauensperson selbst Zielperson der Überwachung ist. Eine gezielte Überwachung der Vertrauensperson als Nachrichtenmittlerin oder Anschlussgeberin der geschützten Person (vgl. etwa § 100a Abs. 3 StPO oder § 51 Abs. 1 Satz 1 Nr. 4 und 5 BKAG) wird durch die Schutzregelungen jedoch gerade ausgeschlossen. Eine gezielte Überwachung der Kommunikation der Vertrauensperson zu Dritten setzt in der Folge voraus, dass gegen die Vertrauensperson selbst ein Tat- oder Störerverdacht besteht, was in der Regel nicht der Fall sein wird.

Eine strategische Telekommunikationsüberwachung, die sich gerade nicht gegen bestimmte individualisierte Zielpersonen richtet, kann hingegen grundsätzlich jedermann erfassen. Insbesondere können die Telekommunikationsmerkmale von Vertrauenspersonen und ihren Kontakten grundsätzlich als Suchbegriffe genutzt werden, sofern sich hieraus nachrichtendienstlich relevante Erkenntnisse ergeben können. Auf besondere Verdachtsmomente kommt es nicht an. Damit kann das Verbot der Datenerhebung *aus* Vertraulichkeitsbeziehungen durch die Erhebung von Daten *über* Vertraulichkeitsbeziehungen in einer Weise umgangen werden, die bei innerstaatlichen individualisierenden Überwachungen kein Pendant hat. Dementsprechend ist eine weitergehende Schutzregelung erforderlich als sie § 21 Abs. 1 Satz 1 BNDG enthält.

5. Bevorratende Speicherung von Verkehrsdaten

Nach dem Urteil des Bundesverfassungsgerichts zur strategischen Ausland-Ausland-Fernmeldeaufklärung dürfen im Rahmen einer strategischen Telekommunikationsüberwachung Metadaten der Kommunikation (Verkehrsdaten) anders als Inhaltsdaten grundsätzlich auch gesamthaft bevorratet und ausgewertet werden,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 166.

Die zwischenzeitlich ergangene Rechtsprechung des Gerichtshofs der Europäischen Union gibt Anlass, diese Wertung zu überdenken. Selbst wenn jedoch an der grundsätzlichen Zulässigkeit einer gesamthaft bevorratenden Verkehrsdatenspeicherung und den dazu in dem Urteil vom 19. Mai 2020 herausgearbeiteten verfassungsrechtlichen Maßstäben vollumfänglich festgehalten wird, verfehlt die Ermächtigung zur Verarbeitung von Verkehrsdaten in § 26 BNDG in mehrfacher Hinsicht die verfassungsrechtlichen Anforderungen.

a) Jüngere Rechtsprechung des Gerichtshofs der Europäischen Union

Das Bundesverfassungsgericht hat in seinem Urteil zur strategischen Ausland-Ausland-Fernmeldeaufklärung ausgeführt, aus den Unionsgrundrechten ergäben sich keine weitergehenden Maßgaben für die Überwachung als aus den Grundrechten des Grundgesetzes. Es fehle an konkreten Anhaltspunkten dafür, dass die Grundrechte des Grundgesetzes in ihrer Auslegung durch dieses Urteil das Schutzniveau der Unionsgrundrechte nicht mit gewährleisteten. Solche Anhaltspunkte ergäben sich insbesondere nicht in Hinblick auf die Befugnis zur bevorratenden Speicherung und Auswertung von Verkehrsdaten aus den – seinerzeit vorliegenden – Entscheidungen des Gerichtshofs der Europäischen Union zur sogenannten Vorratsdatenspeicherung aus den Jahren 2014 und 2016. In jenen Entscheidungen sei es um die Anforderungen an eine innerstaatlich vollständige Erfassung sämtlicher Telekommunikationsverbindungsdaten gegangen, die nahezu lückenlose Persönlichkeitsprofile einzelner Kommunikationsteilnehmer ermöglichten. Hiervon unterscheide sich die Erhebung eines begrenzten Volumens an Verkehrsdaten der Auslandskommunikation aus ausgewählten Netzen – die damit in der Regel nicht die vollständigen Kommunikationsbeziehungen betroffener Personen erfassen könnten – grundlegend. Es sei nicht ersichtlich, dass der Grundrechtsschutz des Grundgesetzes hier das Schutzniveau der Grundrechtecharta der Europäischen Union im Rahmen eines auf Vielfalt angelegten Grundrechtsschutzes in Europa nicht gewährleisten würde,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 326.

Die seit dem Urteil zur Ausland-Ausland-Fernmeldeaufklärung ergangene Rechtsprechung des Gerichtshofs der Europäischen Union gibt Anlass, diesen Standpunkt zu überdenken. Der Gerichtshof hatte sich zwar bislang nicht zu einem Überwachungsregime zu verhalten, das der strategischen Ausland-Fernmeldeaufklärung in jeder Hinsicht gleichkäme. Er hat jedoch verschiedentlich erkennen lassen, dass gerade auch für Massendatenerfassungen durch Nachrichtendienste strenge Anforderungen aus den Unionsgrundrechten folgen. Insbesondere die Vereinbarkeit der nicht anlassbezogenen und auch nicht durch einen Abgleich mit Suchbegriffen angeleiteten Metadatenspeicherung unterliegt daher schwerwiegenden unionsgrundrechtlichen Zweifeln.

Zu nennen ist zunächst das im Juli 2020 ergangene *Schrems II*-Urteil, dessen Gegenstand Datentransfers in die Vereinigten Staaten waren. Darin erklärte der Gerichtshof den Durchführungsbeschluss (EU) 2016/1250 der Kommission über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen

Schutzes für nichtig. Ein Grund hierfür war, dass in den Vereinigten Staaten wegen des Risikos sicherheitsbehördlicher Zugriffe kein Datenschutzniveau bestand, das dem innerhalb der Europäischen Union durch die Unionsgrundrechte verbürgten Standard gleichwertig war. Insoweit verwies der Gerichtshof auf die unzureichende Ausgestaltung der Autorisierung von Überwachungsprogrammen durch den United States Foreign Intelligence Surveillance Court (FISC). Der FISC prüfe nach den Feststellungen der Kommission, ob Überwachungsprogramme dem Ziel entsprächen, Auslandsaufklärungsdaten zu erlangen, nicht aber die Frage, ob Personen vorschriftsgemäß als Zielpersonen für die Beschaffung von Auslandsaufklärungsdaten ausgewählt wurden. Daher sei nicht erkennbar, dass für die gesetzliche Ermächtigung zur Durchführung von Überwachungsprogrammen zum Zweck der Auslandsaufklärung Einschränkungen bestünden,

> EuGH, Urteil vom 16. Juli 2020, Rs. C-311/18 – Schrems, Rn. 179 f.; vgl. auch die vom Gerichtshof in Bezug genommenen Schlussanträge von Generalanwalt Saugmandsgaard Øe vom 19. Dezember 2019, Rn. 290 ff.

Des Weiteren weist der Gerichtshof darauf hin, dass das US-amerikanische Recht nach den dem Angemessenheitsbeschluss beigefügten Unterlagen die Sammelerhebung einer relativ großen Menge von signalerfassenden Aufklärungsdaten unter Bedingungen erlaube, in denen die Intelligence Community keinen mit einer bestimmten Zielperson verbundenen Identifikator für eine zielgerichtete Erhebung verwenden könne. Hinsichtlich dieser Überwachungsprogramme sei der Umfang einer solchen Sammelerhebung personenbezogener Daten nicht hinreichend klar und präzise eingegrenzt,

> EuGH, Urteil vom 16. Juli 2020, Rs. C-311/18 – Schrems, Rn. 183.

Diese Ausführungen legen nahe, dass der Gerichtshof bei einer Massendatenerfassung, wie sie die strategische Ausland-Fernmeldeaufklärung kennzeichnet, eine Fokussierung auf bestimmte Zielpersonen oder zumindest eine gesetzlich angeordnete unverzügliche Relevanzprüfung der erfassten Daten für unabdingbar hält. Solche Begrenzungen finden sich bei der bevorratenden Verkehrsdatenspeicherung jedoch gerade nicht. Dabei beschränken sich die vom Gerichtshof gewürdigten Überwachungsprogramme US-amerikanischer Nachrichtendienste ebenso wie die strategische Ausland-Fernmeldeaufklärung auf ausländische Kommunikation und bleiben darum notwendig fragmentarisch. Dieser Umstand hat die Bewertung dieser Programme jedoch anscheinend nicht maßgeblich beeinflusst. Damit ergeben sich aus dem

Schrems II-Urteil zumindest konkrete Anhaltspunkte dafür, dass die gesamthaft bevorratende Verkehrsdatenspeicherung, wie sie § 26 BNDG vorsieht, mit den Unionsgrundrechten nicht zu vereinbaren ist.

Weitere Anhaltspunkte in dieselbe Richtung enthält das im Oktober 2020 ergangene Urteil in Sachen *Privacy International*. Dieses Urteil wird oft in den Kontext der innerstaatlichen Vorratsdatenspeicherung gestellt, hatte allerdings einen hiervon deutlich abweichenden Gegenstand. Es erging auf Vorlage des Investigatory Powers Tribunal des Vereinigten Königreichs, das die Unionsrechtskonformität von Überwachungsprogrammen der dortigen Nachrichtendienste Security Service (MI5), Secret Intelligence Service (MI6) und Government Communications Headquarters (GCHQ) zu beurteilen hatte. Im Rahmen dieser Programme waren Telekommunikationsanbieter verpflichtet, unselektierte Metadaten der Telekommunikation (Bulk Communications Data) an Nachrichtendienste auszuleiten. Die Dienste bevorrateten diese Daten für eine spätere Analyse und Nutzung. An dieser Überwachungsform waren sowohl MI5 als Inlandsnachrichtendienst als auch GCHQ als Auslandsnachrichtendienst beteiligt,

> vgl. die eingehende Darstellung des Überwachungsverfahrens bei Anderson, Report of the Bulk Powers Review, 2016, S. 29 ff., abrufbar unter https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf; vgl. auch die Schilderung in dem Vorabentscheidungsersuchen des Investigatory Powers Tribunal, Urteil vom 8. September 2017, No. IPT/15/110/CH, abrufbar unter https://www.ipt-uk.com/docs/Privacy%20International%20v%20SSFCA%20and%20Ors%20September%202017.pdf (letzte Abrufe vom 29. Dezember 2022).

Der Gerichtshof hielt in seinem Urteil fest, ein allgemeiner Zugang zu allen auf Vorrat gespeicherten Daten ohne jeden Zusammenhang mit dem verfolgten Ziel könne nicht als auf das absolut Notwendige beschränkt angesehen werden. Erst recht gelte dies für eine Rechtsvorschrift, auf deren Grundlage die zuständige nationale Behörde den Betreibern elektronischer Kommunikationsdienste vorschreiben könne, den Sicherheits- und Nachrichtendiensten Verkehrs- und Standortdaten durch eine allgemeine und unterschiedslose Übermittlung offenzulegen. Da die Daten allgemein und unterschiedslos übermittelt würden, betreffe ihre Übermittlung pauschal sämtliche Personen, die elektronische Kommunikationsdienste nutzten. Sie gelte somit auch für Personen, bei denen keinerlei Anhaltspunkt dafür bestehe, dass ihr Verhalten in einem auch

nur mittelbaren oder entfernten Zusammenhang mit dem Ziel der Wahrung der nationalen Sicherheit stehen könnte, und setze insbesondere keinen Zusammenhang zwischen den Daten, deren Übermittlung vorgesehen ist, und einer Bedrohung der nationalen Sicherheit voraus. Sie könne daher nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden,

> EuGH, Urteil vom 6. Oktober 2020, Rs. C-623/17 – Privacy International u.a., Rn. 78 ff.

Der Gerichtshof differenziert hierbei nicht zwischen Verkehrsdaten der inländischen und der ausländischen Kommunikation, obwohl eine solche Differenzierung gegebenenfalls nahegelegen hätte, da die verfahrensgegenständlichen Überwachungsprogramme beide Datenkategorien umfassten. Maßgeblich scheint vielmehr die fehlende Verknüpfung zwischen den erfassten Personen und Daten und den Zielen der Datenerfassung zu sein, die sich bei Inlands- wie Auslandsüberwachungen gleichermaßen findet. Dies spricht dafür, dass aus dem fragmentarischen Charakter des auslandsbezogenen Datenzugriffs aus Sicht des Gerichtshofs kein maßgeblicher Unterschied für die grundrechtliche Beurteilung einer anlasslosen und massenhaften Erfassung und Bevorratung von Metadaten der Telekommunikation folgt. Zumindest ist diese Frage nach dem *Privacy International*-Urteil als klärungsbedürftig anzusehen, da dieses Urteil hinreichende Anhaltspunkte für Zweifel an der Grundrechtskonformität eines Überwachungsprogramms enthält, das eine anlasslose Bevorratung erfasster Metadaten vorsieht.

Relevant ist schließlich das im September 2022 ergangene *SpaceNet*-Urteil. Gegenstand des Verfahrens war zwar die auf inländische Verkehrsdaten bezogene Vorratsdatenspeicherung in Deutschland, die das Bundesverfassungsgericht für nicht vergleichbar mit der Verkehrsdatenbevorratung im Rahmen einer strategischen Telekommunikationsüberwachung gehalten hat. Jedoch lassen sich dem Urteil gleichwohl Aussagen entnehmen, die das vorliegende Verfahren berühren. Denn die Bundesrepublik hatte vor dem Gerichtshof vorgetragen, auf die deutsche Vorratsdatenspeicherung könnten die bis dahin entwickelten Maßstäbe nicht angewandt werden, weil sich die Datenspeicherung auf einen reduzierten Datensatz und einen kurzen Bevorratungszeitraum von wenigen Wochen beschränke und darum weitaus weniger eingriffsintensiv sei als die anderen durch den Gerichtshof beurteilten Speicherungsregime.

Der Gerichtshof wies dieses Argument zurück. Die Speicherung von Verkehrs- oder Standortdaten, die Informationen über die Kommunikationen des Nutzers eines elektronischen Kommunikationsmittels oder über den Standort der von

ihm verwendeten Endgeräte liefern könnten, sei in jedem Fall schwerwiegend, unabhängig von der Länge des Speicherzeitraums und von der Menge oder Art der gespeicherten Daten, sofern der Datensatz geeignet sei, sehr genaue Schlüsse auf das Privatleben der betroffenen Person bzw. der betroffenen Personen zuzulassen. Insoweit könnten selbst die Speicherung einer begrenzten Menge von Verkehrs- oder Standortdaten oder die Speicherung dieser Daten über einen kurzen Zeitraum geeignet sein, sehr genaue Informationen über das Privatleben des Nutzers eines elektronischen Kommunikationsmittels zu liefern. Außerdem könnten die Menge der verfügbaren Daten und die daraus resultierenden sehr genauen Informationen über das Privatleben des Betroffenen erst nach Konsultation der fraglichen Daten beurteilt werden. Der sich aus der Speicherung der genannten Daten ergebende Eingriff geschehe aber notwendigerweise, bevor die Daten und die daraus resultierenden Informationen konsultiert werden könnten. Somit sei die Schwere des in der Speicherung bestehenden Eingriffs notwendigerweise anhand der mit der Kategorie gespeicherter Daten allgemein verbundenen Gefahr für das Privatleben der Betroffenen zu beurteilen, ohne dass es überdies darauf ankomme, ob die daraus resultierenden Informationen über das Privatleben im konkreten Fall sensiblen Charakter hätten,

> EuGH, Urteil vom 20. September 2022, Rs. C-793/19 und C-794/19 – SpaceNet u.a., Rn. 88 f.

Nach dem *SpaceNet*-Urteil kommt es mithin für die Eingriffsintensität einer Datenbevorratung und für die daraus resultierenden grundrechtlichen Anforderungen auf eine vertypte Ex-ante-Würdigung der bevorrateten Datenkategorien an. Auch wenn nicht alle bei der Telekommunikationsnutzung anfallenden Metadaten gespeichert werden – was ohnehin in keinem innerstaatlichen Bevorratungsregime auch nur annähernd vorgesehen war –, kann die Datenspeicherung so schwer wiegen, dass sie nur unter engen Voraussetzungen und insbesondere nicht anlasslos zulässig ist. Auf eine vollständige Erfassung sämtlicher Telekommunikationsverbindungsdaten, auf die sich das Bundesverfassungsgericht in seinem Urteil zur Ausland-Ausland-Fernmeldeaufklärung bezogen hat, kommt es mithin nicht an.

Ein Vergleich zwischen der gesamthaft bevorratenden Datenspeicherung nach § 26 BNDG und dem im *SpaceNet*-Urteil gegenständlichen Bevorratungsregime ergibt, dass einerseits die Datenspeicherung im Rahmen der strategischen Ausland-Fernmeldeaufklärung – wie das Bundesverfassungsgericht hervorgehoben hat – zumindest in der Regel nicht den gesamten Telekommunikationsverkehr einer Person im Speicherungszeitraum erfassen

wird, während die innerstaatliche Vorratsdatenspeicherung insoweit grundsätzlich auf Vollständigkeit angelegt ist. Gleichwohl kann sich die strategische Überwachung abhängig von den überwachten Telekommunikationsnetzen und den Zielregionen der Überwachung durchaus auf einen beträchtlichen Teil der Telekommunikation bestimmter Personengruppen erstrecken. Immerhin befindet sich mit dem DE-CIX der größte Internetknoten der Welt in der Bundesrepublik.

Andererseits erstreckt sich die Datenbevorratung nach § 26 BNDG potenziell auf sämtliche Metadaten der erfassten Telekommunikation,

> näher zu den damit verbundenen Interpretationsschwierigkeiten unten C. I. 5. b) aa).

Die Bevorratung geht also hinsichtlich des bevorratungsfähigen Datenkranzes über alle innerstaatlichen Bevorratungsregime, die der Gerichtshof bislang zu beurteilen hatte, weit hinaus.

Zudem sieht § 26 Abs. 5 BNDG eine im Vergleich zu der durch den Gerichtshof verworfenen deutschen Vorratsdatenspeicherung weitaus längere Speicherfrist von bis zu sechs Monaten vor. Diese kann sogar noch verlängert werden, ohne dass es eine absolute Obergrenze gäbe,

> näher zu den verfassungsrechtlichen Bedenken gegen diese Regelung unten C. I. 5. b) bb).

Schließlich werden die erfassten Daten von vornherein zentral bei der Überwachungsbehörde zusammengeführt, was ihre Auswertung im Vergleich zu der dezentral durchgeführten innerstaatlichen Vorratsdatenspeicherung erheblich erleichtert und ihren Informationswert erhöht.

Insgesamt liegt darum nahe, dass auch die fragmentarische Datenbevorratung im Rahmen der strategischen Ausland-Fernmeldeaufklärung sehr weitreichende Schlüsse über das Privatleben einer großen Zahl betroffener Personen zulässt. Dies spricht dafür, dass sich entgegen der Annahme des Bundesverfassungsgerichts die Maßstäbe, die der Gerichtshof für innerstaatliche Vorratsdatenspeicherungen entwickelt hat, zumindest ansatzweise und gegebenenfalls mit Modifizierungen auf diese Datenbevorratung übertragen lassen. Jedenfalls ist diese Frage als klärungsbedürftig anzusehen.

Der Befund, dass die Rechtsprechung des Gerichtshofs konkrete Anhaltspunkte für strenge Anforderungen an die Verkehrsdatenspeicherung im Rahmen einer strategischen Ausland-Fernmeldeaufklärung enthält, lässt sich

schließlich nicht mit der Erwägung in Frage stellen, dass der Europäische Gerichtshof für Menschenrechte strategische Überwachungsprogramme konventionsstaatlicher Nachrichtendienste in seiner jüngsten Rechtsprechung grundsätzlich gebilligt hat. Der Gerichtshof der Europäischen Union hat in seinem *SpaceNet*-Urteil ausdrücklich und gerade mit Blick auf Datenspeicherungen zu sicherheitsbehördlichen Zwecken hervorgehoben, dass die Europäische Menschenrechtskonvention für die Auslegung der Unionsgrundrechte nur einen Mindeststandard des Grundrechtsschutzes vorgibt,

> EuGH, Urteil vom 20. September 2022, Rs. C-793/19 und C-794/19 – SpaceNet u.a. –, Rn. 125.

Die Anhaltspunkte aus der jüngsten Rechtsprechung des Gerichtshofs der Europäischen Union machen in einer Zusammenschau deutlich, dass die unionsgrundrechtlichen Anforderungen an strategische Überwachungsprogramme der Mitgliedstaaten und insbesondere an dabei vorgesehene bevorratende Verkehrsdatenspeicherungen dringend klärungsbedürftig sind.

Ich rege daher an, die gebotene Klärung gemäß Art. 267 AEUV durch ein Vorabentscheidungsersuchen an den Gerichtshof herbeizuführen und so der Bedeutung der Unionsgrundrechte als Interpretationsleitlinien und Mindeststandards für die Grundrechte des Grundgesetzes Rechnung zu tragen.

b) Verfassungsrechtliche Mängel auf der Grundlage des Urteils vom 19. Mai 2020

Nach dem Urteil des Bundesverfassungsgerichts über die strategische Ausland-Ausland-Fernmeldeaufklärung kann hingegen eine gesamthaft bevorratende Speicherung von Verkehrsdaten der ausländischen Telekommunikation zwar grundsätzlich gerechtfertigt werden. Als anlasslose, im Wesentlichen allein final angeleitete und begrenzte Befugnis ist eine solche Datenbevorratung jedoch eine Ausnahmebefugnis. Sie muss auf die Auslandsaufklärung durch eine Behörde, welche selbst grundsätzlich keine operativen Befugnisse zur Gefahrenabwehr hat, begrenzt bleiben. Nur durch deren besonderes Aufgabenprofil ist sie gerechtfertigt. Hieran hat sich nach dem Grundsatz der Verhältnismäßigkeit auch die nähere Ausgestaltung auszurichten,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 166.

Selbst nach diesem Maßstab verfehlt die Ermächtigung zur Verarbeitung von Verkehrsdaten in § 26 BNDG in mehrfacher Hinsicht die verfassungsrechtlichen Anforderungen.

aa) Gegenstand der Datenspeicherung

§ 26 Abs. 1 BNDG beschreibt den Gegenstand der Datenspeicherung zu unbestimmt und potenziell zu weitreichend. Da nur Verkehrsdaten, nicht aber Inhaltsdaten gesamthaft bevorratend gespeichert werden dürfen, muss die gesetzliche Grundlage die Speicherung auf solche Daten beschränken, bei denen – ungeachtet ihrer immer noch hohen Sensibilität – eine Speicherung mit dem Übermaßverbot zu vereinbaren ist. § 26 Abs. 1 BNDG leistet dies nicht.

Auf den ersten Blick scheint allerdings der Gegenstand der Datenspeicherung mit dem Begriff der Verkehrsdaten klar bezeichnet zu sein. Scheinbar kann dieser Begriff durch die Legaldefinition in § 3 Nr. 70 TKG ausgefüllt werden, die Verkehrsdaten als Daten definiert, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind. Bei diesem Begriffsverständnis bestünden gegen eine Datenbevorratung nach den Maßstäben des Urteils zur Ausland-Ausland-Fernmeldeaufklärung grundsätzlich keine verfassungsrechtlichen Bedenken.

Aus der Gesetzesbegründung ergibt sich jedoch, dass eine Anknüpfung an § 3 Nr. 70 TKG nicht intendiert ist. Dort heißt es, die Ermächtigung umfasse „neben Verkehrsdaten auch alle weiteren personenbezogenen Metadaten, die in der strategischen Ausland-Fernmeldeaufklärung anfallen“,

BT-Drs. 19/26103, S. 76.

Hierzu erläutert die Begründung zu § 19 Abs. 1 BNDG, die in der Begründung zu § 26 BNDG in Bezug genommen wird, speicherungsfähige Metadaten seien „alle über die Inhaltsdaten hinausgehenden Daten“. Beispielhaft nennt die Gesetzesbegründung Daten, „die den Aufbau und die Benutzung anderer Daten beschreiben, oder Daten über Daten, wie Datentyp, Bedeutung, Beziehungen zwischen Entitätstypen, Integritätsbedingungen, Verdichtungsregeln“,

BT-Drs. 19/26103, S. 56.

Werden Verkehrsdaten somit lediglich negativ von Inhaltsdaten abgegrenzt, so bedarf es einer Definition des Begriffs der Inhaltsdaten. Eine solche Definition enthält das BNDG nicht; sie findet sich auch nicht im Telekommunikationsrecht. Damit ist erheblichen Ausweitungen der Datenspeicherung der Boden bereitet. Grund hierfür ist, dass unter den heutigen technischen Bedingungen Telekommunikationsvorgänge geschichtet ablaufen. Auf der – aus technischer Sicht nach dem ISO/OSI-Referenzmodell ihrerseits in Unterschichten eingeteilten – allgemeinen Transportschicht des Internet als Kommunikations-

Basisinfrastruktur beruhen zahlreiche unterschiedliche Kommunikationsdienste, die zumeist in sich weiter geschichtet sind. Je nachdem, von welcher Schicht die Zuordnung ausgeht, kann sich dasselbe Datum mal als Inhalts- und mal als Metadatum darstellen. Das Fehlen einer Legaldefinition ermöglicht daher – anders als die auf Telekommunikationsdienste i.S.v. § 3 Nr. 61 TKG bezogene Legaldefinition in § 3 Nr. 70 TKG – dem Bundesnachrichtendienst, den Gegenstand der Datenspeicherung durch Auswahl der Bezugsschicht in weitem Umfang nach eigenen Opportunitätserwägungen zu bestimmen.

Dieses Zuordnungsproblem lässt sich beispielhaft anhand des Kaufs eines Grundgesetzkommentars bei einem Online-Buchversandhandel illustrieren, bei dem ein Kunde die Produktseite des Kommentars aufsucht und diesen anschließend bestellt.

Aus Sicht der in § 3 Nr. 70 TKG in Bezug genommenen Transportschicht werden hierbei Datenpakete zwischen zwei Rechnern ausgetauscht, die durch IP-Adressen bezeichnet werden. Die IP-Adresse des Online-Buchversands lässt sich in dessen sogenannte Top- und Second-Level-Domains auflösen (beispielsweise „amazon.de“). Hieraus können etwa Rückschlüsse auf die besuchte Website (im Beispiel „www.amazon.de“) gezogen werden. Die Bezeichnung der von dem Kunden aufgerufenen Produktseite des Grundgesetzkommentars durch einen Pfad (etwa „www.amazon.de/Grundgesetz-f%C3%BCr-Bundesrepublik-Deutschland-Handkommentar/dp/3848779307“) lässt sich der IP-Adresse hingegen nicht entnehmen. Hierbei handelt es sich aus der Perspektive der Transportschicht um ein Inhaltsdatum.

Anders liegt es hingegen, wenn für die Unterscheidung von Inhalts- und Metadaten statt auf die Transportschicht auf das Verkaufsportal des Online-Buchversands abgestellt wird, einen Telemediendienst i.S.v. § 1 Abs. 1 Satz 1 TMG. Auf dieser Ebene ist die Angabe, dass von einer bestimmten IP-Adresse aus und ggfs. unter einem bestimmten Nutzerkonto eine bestimmte Webseite aufgerufen wurde, ein Nutzungsdatum i.S.v. § 2 Abs. 2 Nr. 3 TTDSG. Die Information, dass jemand unter diesen Kennungen die Produktseite des Grundgesetzkommentars aufgerufen hat, ließe sich insoweit als speicherungsfähiges Metadatum einstufen. Inhaltsdaten wären demgegenüber die Daten, die bei der über den Telemediendienst durchgeführten Transaktion übermittelt werden, also die Angabe, dass eine bestimmte Person den Kommentar bestellt hat.

Noch komplexere Zuordnungsprobleme entstehen bei Telemediendiensten, die unterschiedliche und unterschiedlich geschichtete Dienste bündeln. Ein Beispiel bilden soziale Medien, die individual- und massenkommunikative

Funktionen in sich vereinigen und darüber hinaus weitere Leistungen, etwa Identifikationsdienste, anbieten. Werden bei solchen Diensten alle bei der Nutzung anfallenden Metadaten als Verkehrsdaten i.S.v. § 26 Abs. 1 BNDG eingestuft, so lassen sich Daten von hoher Sensibilität in extrem großem Ausmaß speichern. Als Metadaten bevorratungsfähig wären etwa Informationen darüber, von welchen IP-Adressen und ggfs. Nutzerkennungen aus bestimmte Inhalte eingesehen oder (ggfs. mit wem) geteilt wurden. Die Sensibilität dieser Informationen kann über die zugehörigen Inhaltsdaten weit hinausgehen, zumal wenn diese öffentlich verfügbar sind.

Eine so weitreichende Bevorratungspraxis, die selbst bei fragmentarischer Datenerfassung eine weitreichende Ausleuchtung der Person ermöglicht, kann mit der verfassungsgerichtlich zugelassenen „gesamthaft bevorratenden Speicherung von Verkehrsdaten“ aus Sicht des Unterzeichners nicht gemeint sein. Es bedarf daher einer klaren und hinreichend restriktiven Legaldefinition des Begriffs des Verkehrsdatums, um die Speicherermächtigung zu legitimieren.

bb) Dauer der Datenspeicherung

Verfassungswidrig ist zudem die Regelung über die Dauer der Datenspeicherung in § 26 Abs. 5 BNDG. Wie das Bundesverfassungsgericht ausgeführt hat, darf die Datenspeicherung eine Höchstdauer von sechs Monaten nicht überschreiten,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 191.

Hingegen sieht § 26 Abs. 5 Satz 1 BNDG eine sechsmonatige Speicherung lediglich als Regelfall vor. Gemäß § 26 Abs. 5 Satz 2 BNDG ist eine längere Speicherung „im Einzelfall“ möglich, soweit sie „für die Aufgabenerfüllung des Bundesnachrichtendienstes weiterhin erforderlich ist“. Zudem gibt es für die weitere Speicherung keine feste Höchstgrenze. Vielmehr ist gemäß § 26 Abs. 5 Satz 3 BNDG die allgemeine Prüfregelung des § 27 BNDG anzuwenden. Dies kann zu einem bis zu sieben Jahre dauernden Kontrollturnus und dementsprechend einer potenziell über Jahre oder sogar Jahrzehnte andauernden Datenspeicherung führen.

Selbst wenn entgegen der nicht eingeschränkten Aussage des Bundesverfassungsgerichts eine Verlängerung der gesamthaft bevorratenden Datenspeicherung überhaupt verfassungskonform sein könnte, müsste sie zumindest an strenge Anforderungen geknüpft werden. Die Verlängerung müsste von der Feststellung abhängig gemacht werden, dass aus besonderen Gründen eine Relevanzprüfung samt Löschung der nicht benötigten Daten innerhalb des regulären Speicherzeitraums ausnahmsweise nicht möglich ist, etwa weil die

Daten verschlüsselt sind und sich die Verschlüsselung derzeit nicht brechen lässt. Diese Feststellung wäre einer obligatorischen unabhängigen Kontrolle zu unterwerfen. Schließlich müsste die Verlängerung auf einen knappen Zeitraum von allenfalls wenigen Monaten beschränkt bleiben. § 26 Abs. 5 BNDG genügt diesen Mindestanforderungen nicht ansatzweise.

Das Tatbestandsmerkmal der Erforderlichkeit für die Aufgabenerfüllung in § 26 Abs. 5 Satz 2 BNDG ist demgegenüber nahezu konturenlos und setzt der Entscheidung, ob die Daten bevorratet bleiben sollen, keine handhabbaren normativen Grenzen. Es läuft auf eine Anwendung des Verhältnismäßigkeitsgrundsatzes hinaus, ohne diesen durch verbindliche Kriterien zu konkretisieren. Die Beschränkung auf den Einzelfall ergibt im Rahmen der Verkehrsdatenspeicherung, die gerade gesamthaft bevorratend und damit einzelfallunabhängig erfolgt, keinen Sinn und errichtet daher gleichfalls keine handhabbare Grenze für die Bevorratung.

Auch die in § 26 Abs. 5 Satz 3 BNDG vorgesehene Anwendung der Prüfregelung des § 27 BNDG auf die bevorratende Verkehrsdatenspeicherung ist verfehlt. Diese Regelung ist auf die Speicherung von Daten zugeschnitten, deren Relevanz für die Aufgabenerfüllung der Bundesnachrichtendienst bereits aufgrund des Abgleichs der erfassten Daten mit den Suchbegriffen und der anschließenden manuellen Prüfung der Treffer festgestellt hat. Bei solchen ausgefilterten Daten kann grundsätzlich davon ausgegangen werden, dass ihre nachrichtendienstliche Relevanz zumindest mittelfristig bestehen bleibt. Dementsprechend bestehen keine Bedenken dagegen, eine erneute Relevanzprüfung grundsätzlich nur turnusmäßig nach Ablauf einer Prüffrist vorzusehen. Die in § 26 BNDG vorgesehene Verkehrsdatenspeicherung beruht hingegen zunächst nicht auf einer Relevanzprüfung; diese Prüfung erfolgt erst bei der manuellen Auswertung der gespeicherten Daten, für die kein bestimmter Zeitpunkt vorgesehen ist. § 26 Abs. 5 Satz 3 i.V.m. § 27 Abs. 1 Satz 1 BNDG ermöglicht es, diese Relevanzprüfung langfristig hinauszuschieben und so Datenvorräte von enormem Umfang anzulegen. Auf diese Weise wird die verfassungsrechtliche Vorgabe, dass die gesamthaft bevorratende Verkehrsdatenspeicherung zeitlich begrenzt bleiben muss, weitgehend ausgehebelt.

cc) Auswertung der gespeicherten Daten

Darüber hinaus fehlt es in § 26 BNDG an tragfähigen Vorgaben für die Auswertung der bevorrateten Daten. Die Norm erwähnt die Auswertungsphase in § 26 Abs. 2 und Abs. 4 Satz 1 BNDG, ohne hierfür eine spezifische Ermächtigung bereitzustellen. Es liegt daher nahe, als Ermächtigung sowohl für die Datenspeicherung als auch für die Auswertung der gespeicherten Daten auf § 26

Abs. 1 Satz 1 BNDG zurückzugreifen. Diese Norm ist jedoch als Auswertungsermächtigung viel zu weit und unscharf gefasst.

Die in § 26 Abs. 1 Satz 1 BNDG geregelte Datenbevorratung dient nach Wortlaut und Sinn der Ermächtigung nicht allein dem Erkenntnisziel des Überwachungsprojekts, in dessen Rahmen die Verkehrsdaten erhoben werden. Zumeist wird es sich ohnehin um mehrere Projekte handeln, da dasselbe Telekommunikationsnetz in der Regel für mehrere Erkenntnisziele relevant ist. Die Daten müssen zwar „im Rahmen von strategischen Aufklärungsmaßnahmen“ nach § 19 Abs. 1 BNDG verarbeitet werden. Die Verkehrsdatenspeicherung hängt jedoch nicht davon ab, welche Daten für welche Aufklärungsmaßnahme relevant sind, da die Daten ja gerade gesamthaft bevorratet werden sollen. Es handelt sich also um eine Datenspeicherung „bei Gelegenheit“ der Überwachung.

Diese lediglich äußerliche Verknüpfung zwischen den Überwachungsprojekten, die der Datenerhebung zugrunde liegen, und der Verkehrsdatenspeicherung wird schon durch den Wortlaut von § 26 Abs. 1 Satz 1 BNDG nahegelegt. Sie ergibt sich auch aus § 26 Abs. 2 BNDG, der eine Kennzeichnung der Daten nicht schon bei ihrer Speicherung, sondern erst bei ihrer manuellen Auswertung vorsieht. Hierzu führt die Gesetzesbegründung aus, „dass bei der Erhebung der Verkehrs- und sonstigen Metadaten eine Zuordnung der erhobenen Daten zu einem Erhebungszweck nicht möglich ist, da zu diesem Zeitpunkt noch nicht bekannt ist, welchem konkreten Thema die Daten zuzuordnen sind“,

> BT-Drs. 19/26103, S. 76.

Diese Erläuterung ergibt nur Sinn, wenn angenommen wird, dass der Verarbeitungszweck der Daten gerade nicht durch die Überwachungsprojekte festgelegt wird, in deren Rahmen sie erhoben werden, sondern vielmehr der Zweck erst bei der Auswertung bestimmt wird. Auch die Verarbeitungsregelung in § 26 Abs. 3 Satz 4 BNDG, die für gemäß § 26 Abs. 3 Satz 2 Nr. 2 BNDG unkenntlich gemachte Verkehrsdaten gilt, knüpft nicht an den Zweck der Überwachungsprojekte an, in denen die Daten erhoben wurden. Im Übrigen entspricht die Entkoppelung des Auswertungszwecks vom Speicherungszweck der früheren Praxis des Bundesnachrichtendienstes, die durch § 26 BNDG ersichtlich legalisiert werden sollte,

> vgl. dazu BVerwG, Urteil vom 13. Dezember 2017 – BVerwG 6 A 6.16 –, Rn. 28 ff.

Gegen eine projektübergreifende Bevorratung von Verkehrsdaten, die im Rahmen bestimmter Überwachungsprojekte anfallen, bestehen auf der Grundlage des Urteils zur Ausland-Ausland-Fernmeldeaufklärung keine Bedenken. Zu fordern ist dann allerdings, dass die Auswertung der bevorrateten Daten an Voraussetzungen geknüpft wird, die dem hohen Eingriffsgewicht der Datenerhebung und Datenspeicherung Rechnung tragen,

> vgl. zur Weiterverarbeitung von flächendeckend bevorrateten inländischen Verkehrsdaten BVerfGE 125, 260 (327 ff.).

Die Datenauswertung muss darum parallel zur Verarbeitung von Inhaltsdaten an die Konturierung eines Auswertungsprojekts geknüpft werden. Je nach Zielsetzung (politische Unterrichtung der Bundesregierung oder Gefahrenfrüherkennung) sind die Auswertungszwecke auch materiell zu begrenzen. Demgegenüber enthält § 26 Abs. 1 Satz 1 BNDG überhaupt keine Tatbestandsmerkmale und lässt damit die Datenauswertung voraussetzungslos im gesamten Aufgabenbereich des Bundesnachrichtendienstes zu.

dd) Fehlender Schutz von Vertraulichkeitsbeziehungen

Des Weiteren enthält § 26 BNDG keine Vorgaben, um Vertraulichkeitsbeziehungen zu schützen. Solche Vorgaben sind jedoch auch für die Verarbeitung von Verkehrsdaten möglich und geboten. Da das Bundesverfassungsgericht eine gesamthaft bevorratende Verkehrsdatenspeicherung gebilligt hat, müssen Verkehrsdaten mit Bezug zu Vertraulichkeitsbeziehungen zwar nicht schon bei der Datenspeicherung ausgesondert werden. Der besonderen Sensibilität dieser Daten kann und muss aber auf der Ebene der Datenauswertung Rechnung getragen werden,

> vgl. zur Weiterverarbeitung bevorrateter inländischer Verkehrsdaten BVerfGE 125, 260 (334); ferner EuGH, Urteil vom 8. April 2014, Rs. C-293/12 und C-594/12 – Digital Rights Ireland u.a., Rn. 58.

Insoweit könnte parallel zu der Erhebung der Inhaltsdaten zwischen gezielten und ungezielten Auswertungen von Verkehrsdaten mit Bezug zu Vertraulichkeitsbeziehungen unterschieden werden. Auch könnte eine Ausnahmeregelung geschaffen werden, die eine Auswertung solcher Daten in Krisenlagen oder bei einer Verstrickung der betroffenen Vertrauensperson zulässt. Indem § 26 BNDG die Auswertung der bevorrateten Daten hingegen überhaupt nicht gesondert regelt, greift die Norm auch hinsichtlich des Schutzes von Vertraulichkeitsbeziehungen zu kurz.

ee) Verkehrsdaten der inländischen Maschine-Maschine-Kommunikation

Gleichfalls nicht mit den verfassungsrechtlichen Anforderungen an eine gesamthaft bevorratende Verkehrsdatenspeicherung im Rahmen einer strategischen Telekommunikationsüberwachung vereinbar ist § 26 Abs. 3 Satz 2 Nr. 1 BNDG. Diese Regelung erlaubt die Bevorratung von Verkehrsdaten, die im Rahmen des automatisierten Informationsaustausches zwischen informationstechnischen Systemen ohne unmittelbaren Bezug zu einem konkreten menschlichen Kommunikationsvorgang anfallen, unabhängig von der Staatsangehörigkeit und dem Aufenthaltsort der betroffenen Person. Sie wahrt daher nicht die in dem Urteil zur Ausland-Ausland-Fernmeldeaufklärung ausdrücklich geforderte Beschränkung der Verkehrsdatenspeicherung auf die Auslandsaufklärung.

Wie sich aus der Gesetzesbegründung ergibt, beruht § 26 Abs. 3 Satz 2 Nr. 1 BNDG auf der Prämisse, dass das Fernmeldegeheimnis des Art. 10 GG „nur individuelle Kommunikationen von natürlichen Personen und nicht durch deren Endgeräte aus technischen Gründen und ohne unmittelbares Zutun des Nutzers automatisiert ausgelöste Kommunikationen mit anderen Geräten“ schützt,

BT-Drs. 19/26103, S. 76.

Diese Prämisse ist bereits für sich genommen unzutreffend. Zudem ergibt sich aus ihr entgegen der in der Gesetzesbegründung implizit verfochtenen Annahme nicht, dass eine gesamthaft bevorratende Speicherung von Metadaten der intermaschinellen Kommunikation gegenüber Inländerinnen und Inländern verfassungsrechtlich gerechtfertigt werden könnte. Denn selbst wenn die angegriffene Regelung nicht am Fernmeldegeheimnis zu messen sein sollte, würde sie jedenfalls das Recht auf informationelle Selbstbestimmung verletzen.

(1) Schutzbereich des Fernmeldegeheimnisses

Entgegen der Gesetzesbegründung sprechen die besseren Gründe dafür, das Fernmeldegeheimnis auf alle durch Telekommunikation vermittelten Kommunikationsvorgänge zu erstrecken. Auch die intermaschinelle Kommunikation fällt darum in den Schutzbereich dieses Grundrechts. Die Gegenauffassung, nach der Art. 10 GG nur die menschliche Kommunikation schützen soll,

so etwa Pagenkopf, in: Sachs, GG, 9. Aufl. 2021, Art. 10 Rn. 14b; Soiné, MMR 2015, S. 22 (23); wie hier mit Blick auf Cloud Computing hingegen etwa Rückert, in: MüKo StPO, 2. Aufl. 2023, § 100a Rn. 30.

überzeugt aus zwei Gründen nicht:

Erstens führt eine Beschränkung des Fernmeldegeheimnisses auf die menschliche Kommunikation zu kaum überwindbaren Abgrenzungsproblemen. Menschliche Kommunikation und andere durch Telekommunikation vermittelte Kommunikationsvorgänge lassen sich nicht trennscharf voneinander unterscheiden. Jeder Telekommunikationsvorgang ist insoweit rein intermaschinelle Kommunikation, als zwei Endgeräte Daten austauschen und diese weiterverarbeiten. Eine Unterscheidung von menschlicher und rein intermaschineller Kommunikation setzt daher voraus, den menschlichen Beitrag zu einem Kommunikationsvorgang zu gewichten. Handhabbare Kriterien hierfür bieten weder die Gesetzesbegründung noch die Literatur an, soweit sie den Schutzbereich des Fernmeldegeheimnisses auf menschliche Kommunikation beschränken will.

Unklar ist etwa, wie die menschliche Nutzung von internetbasierten Dienstleistungen einzustufen ist, die nach landläufiger Ansicht keine oder zumindest keine ausschließlich individualkommunikative Funktion erfüllen, sich aber faktisch individualkommunikativ nutzen lassen. Beispielsweise können im Rahmen von Onlinespielen häufig Nachrichten an Mitspielende geschickt werden. Beim scheinbar einseitigen Aufruf von Webseiten besteht vielfach die Möglichkeit, Inhalte zu bearbeiten oder zu kommentieren. Dateien auf Cloudspeicherdiensten oder vernetzter Anwendungssoftware können mit Dritten geteilt oder kollaborativ bearbeitet werden,

vgl. zum Problemkreis Bäcker, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, Bd. 1, 2009, S. 99 (104 ff.).

Auch etwa die scheinbar rein intermaschinelle Kommunikation im *Internet of Things* beruht zudem zumindest in vielen Fällen auf menschlichen Entscheidungen wie dem Fahren mit einem vernetzten Kraftfahrzeug oder körperlichen Bewegungen, die durch eine Gesundheitsapp aufgezeichnet werden. Bei manchen Kommunikationsvorgängen lässt sich an den übertragenen Daten nicht erkennen, inwieweit die Kommunikation auf menschliches Verhalten zurückgeht. Beispielsweise kann der Aufruf einer Webseite darauf zurückgehen,

dass ein Mensch die zugehörige Adresse (URL) in die URL-Zeile eines Browsers eingegeben hat, aber auch auf einem automatisierten Suchdurchlauf durch einen sogenannten Webcrawler beruhen

Im Übrigen lassen sich selbst dann, wenn davon ausgegangen wird, dass menschliche und rein intermaschinelle Kommunikationsvorgänge voneinander abgrenzbar sind, die dabei erzeugten Metadaten auf der Transportstrecke nur voneinander unterscheiden, wenn sie näher analysiert werden. Menschliche wie rein intermaschinelle Kommunikation besteht aus dem Versand von Datenpaketen, die nach denselben Strukturvorgaben aufgebaut sind. Erst eine inhaltliche Auswertung ermöglicht es, den Dienst zu identifizieren, der die Daten erzeugt hat. Mit dieser inhaltlichen Auswertung aktualisiert sich ein behördliches Erkenntnisinteresse an den ausgewerteten Daten. Um den Schutzbereich des so verstandenen Fernmeldegeheimnisses praktisch zu handhaben, muss also zunächst in das Fernmeldegeheimnis eingegriffen werden.

Zweitens führt die Engführung des Fernmeldegeheimnisses auf die Individualkommunikation zu einer anachronistischen Versteinerung des Schutzbereichs, die dem Schutzzweck dieses Grundrechts zuwiderläuft. Denn sie trägt der Entwicklung der Telekommunikation von einem funktional klar definierten Kommunikationsmedium zu einer allgegenwärtigen Basisinfrastruktur nicht Rechnung. Das spezifische Schutzbedürfnis, dem Art. 10 GG begegnet, ergibt sich nicht aus einer bestimmten Qualität der fernkommunikativ vermittelten Inhalte. So schützt dieses Grundrecht bei der herkömmlichen Sprachtelefonie die große Mehrzahl banaler Gespräche ebenso wie die wenigen höchstpersönlichen Kontakte. Schutzgrund des Fernmeldegeheimnisses ist vielmehr die besondere Verwundbarkeit der Fernkommunikation. Diese Verwundbarkeit beruht auf der Einschaltung eines Kommunikationsintermediärs, der die Kommunikation wahrnehmen und an Dritte weiterleiten kann,

vgl. BVerfGE 85, 386 (396); 124, 43 (54 f.).

Dieses Schutzbedürfnis besteht für die intermaschinelle Fernkommunikation ebenso wie für die zwischenmenschliche Fernkommunikation. Die Kommunikation weist in beiden Fällen dieselbe Struktur auf und wird durch dieselben technischen Infrastrukturen geleitet. Sie ist darum dem Zugriff der Kommunikationsintermediäre gleichermaßen ausgeliefert.

(2) Unzulässigkeit der Datenbevorratung

Im Ergebnis kommt es für die verfassungsrechtliche Beurteilung der bevorratenden Speicherung von Metadaten der intermaschinellen Fernkommunikation allerdings nicht maßgeblich auf die Zuordnung dieser Kommunikation zum

Fernmeldegeheimnis an. In jedem Fall unterfällt die intermaschinelle Fernkommunikation, wenn sie sich – wie in der Regel – auf bestimmte Personen beziehen lässt, zumindest dem durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gewährleisteten Recht auf informationelle Selbstbestimmung. Die Datenspeicherung greift darum zumindest in dieses Grundrecht ein.

Der Eingriff in das Recht auf informationelle Selbstbestimmung ist, soweit es um die inländische intermaschinelle Kommunikation geht, nicht gerechtfertigt, da er das Übermaßverbot verletzt. Dieser Eingriff weist ein besonders schweres Gewicht auf. Insoweit kann auf die Ausführungen des Bundesverfassungsgerichts zum Eingriffsgewicht der strategischen Telekommunikationsüberwachung verwiesen werden,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 146 ff.

Diese Ausführungen lassen sich auf die intermaschinelle Fernkommunikation ohne weiteres übertragen. Insbesondere sind die Inhalts- und Metadaten der intermaschinellen Fernkommunikation nicht weniger sensibel und schutzbedürftig als die entsprechenden Daten der menschlichen Fernkommunikation. Unter den heutigen technischen und sozialen Bedingungen nutzen Menschen in weitem Umfang vernetzte informationstechnische Systeme, um ihre Lebensgestaltung zu unterstützen und ihre Bedürfnisse zu befriedigen. Die Entwicklung der Telekommunikation zu einer allgegenwärtigen Basisinfrastruktur hat dazu geführt, dass diese Nutzung über die Individualkommunikation weit hinausgeht. Beispielhaft für Gegenstände und Dienstleistungen, die maßgeblich auf nicht-individualkommunikativer intermaschineller Fernkommunikation beruhen und dabei hochgradig sensible Rückschlüsse auf Personen ermöglichen, seien vernetzte Fahrzeuge, Karten- und Navigationsdienste, haustechnische Anlagen, Gesundheitsapplikationen oder Videostreamingdienste genannt. Wer die Metadaten der intermaschinellen Kommunikation solcher Dienste zusammenträgt und auswertet, kann sehr weitreichende Rückschlüsse etwa auf körperliche und psychische Eigenschaften, Neigungen und Interessen oder Bewegungsverhalten der Nutzerinnen und Nutzer der kommunikationsgestützten Produkte und Dienste ziehen. Die Sensibilität dieser Informationen bleibt hinter Informationen mit Bezug zur Individualkommunikation nicht zurück,

> wie hier die Stellungnahme des BfDI, BT-Ausschussdrs. 19(4)682, S. 7.

Dementsprechend ist auch die Folgerung des Bundesverfassungsgerichts, dass sich eine gesamthaft bevorratende Speicherung von Verkehrsdaten, die

anlasslos erfolgt und im Wesentlichen allein final angeleitet wird, auf die Auslandsaufklärung beschränken muss,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 166,

auf Metadaten der intermaschinellen Kommunikation ohne weiteres übertragbar, ohne dass es maßgeblich auf das betroffene Grundrecht ankäme.

Die gesamthafte Erfassung und Auswertung dieser Metadaten über Inländerinnen und Inländer setzt diese Personen einer extrem weitreichenden Ausleuchtung und zugleich hohen Folgerisiken aus. Ein Grund dafür, diesen Eingriff ohne begrenzende tatsächliche Schwelle hinzunehmen, ist nicht ersichtlich, da gegenüber Inländerinnen und Inländern, zumindest soweit sie sich im Inland aufhalten, das gesamte sicherheitsbehördliche Arsenal individualisierender Überwachungsmaßnahmen verfügbar ist. Die besonderen Aufklärungsprobleme, die den strategischen Ansatz bei der Auslandsaufklärung rechtfertigen mögen, bestehen gegenüber diesem Personenkreis nicht.

Hinsichtlich ihres Eingriffsgewichts bleibt die bevorratende Metadatenspeicherung hinter der bevorratenden Speicherung von Telekommunikationsdaten, die das Bundesverfassungsgericht im Jahr 2010 nur unter strengen Auflagen gebilligt und der Gerichtshof der Europäischen Union weitgehend verworfen hat, nicht zurück,

> vgl. BVerfGE 125, 260, sowie zuletzt EuGH, Urteil vom 20. September 2022, Rs. C-793/19 und C-794/19 – SpaceNet u.a.

Soweit sich die Datenspeicherung auf die intermaschinelle Kommunikation im Inland bezieht, ermöglicht aufgrund der üblichen Routingstrecken bereits eine Erfassung eines Bruchteils der inländischen Telekommunikationsnetze eine nahezu vollständige Erfassung der betreffenden Datenkategorien. Anders als die Überwachung der ausländischen Kommunikation bleibt die Überwachung also nicht notwendig fragmentarisch. Darüber hinaus beschränkt sich die Datenspeicherung nach § 26 Abs. 3 Satz 2 Nr. 1 BNDG zwar auf bestimmte Kommunikationsvorgänge. Im Gegenzug erfasst sie jedoch potenziell alle Metadaten und damit weitaus mehr Datenkategorien als die Vorratsdatenspeicherung, die sich gesetzlich auf bestimmte Daten beschränkt. Zudem kann die Speicherdauer nach § 26 Abs. 5 BNDG über den vom Bundesverfassungsgericht noch akzeptierten Höchstzeitraum von sechs Monaten hinaus verlängert werden. Daneben werden die Daten zentral beim Bundesnachrichtendienst statt dezentral bei den Anbietern von Telekommunikationsdiensten gespeichert, sodass sie unmittelbar für – auch verknüpfende – Auswertungen zur Verfügung stehen. Schließlich lässt § 26 Abs. 3 Satz 2 Nr. 1 BNDG die Auswertung

der gespeicherten Metadaten voraussetzungslos zu, während auch das permissivere Urteil des Bundesverfassungsgerichts die Nutzung der Vorratsdaten nur zu herausgehobenen Zwecken und bei einem konkreten Anlass zugelassen hat. Eine so weitreichende Ermächtigung zur anlasslosen Bevorratung und Weiterverarbeitung inländischer Kommunikationsdaten kann unabhängig von dem maßstabsbildenden Grundrecht nicht verfassungskonform sein.

ff) Pseudonymisierte inländische Verkehrsdaten

Verfassungswidrig ist schließlich § 26 Abs. 3 Satz 2 Nr. 2 BNDG, der dem Bundesnachrichtendienst erlaubt, Verkehrsdaten von Inländerinnen und Inländern zu bevorraten, sofern sie unverzüglich nach ihrer Erhebung automatisiert unkenntlich gemacht werden. Mit dieser Vorschrift trägt das Gesetz einer Entscheidung des Bundesverwaltungsgerichts Rechnung, nach der die Bevorratung der bei einer strategischen Telekommunikationsüberwachung anfallenden Verkehrsdaten über das jeweilige Überwachungsprojekt hinaus einer besonderen Rechtsgrundlage bedarf, selbst wenn die Daten vor ihrer Bevorratung unkenntlich gemacht werden,

BVerwG, Urteil vom 13. Dezember 2017 – BVerwG 6 A 6.16.

Die Unkenntlichmachung der Verkehrsdaten ändert jedoch nichts daran, dass diese Daten aus rein inländischer Telekommunikation stammen können. Hinsichtlich solcher Daten können eine strategische Telekommunikationsüberwachung und eine damit verbundene gesamthaft bevorratende Datenspeicherung gerade nicht gerechtfertigt werden. Vielmehr muss die reine Inlandskommunikation – abgesehen vom Ausnahmefall einer Datenverarbeitung zur Abwehr einer unmittelbar bevorstehenden Gefahr für ein besonders hochrangiges Rechtsgut – ausgesondert werden, sobald sie identifiziert werden kann,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 170 ff.

Diese Aussonderungspflicht betrifft Inhalts- und Verkehrsdaten gleichermaßen. Sie steht einer Bevorratung von Verkehrsdaten der Inlandskommunikation daher diametral entgegen.

An der Aussonderungspflicht ändert sich nichts dadurch, dass die Nutzung der bevorrateten Daten nach § 26 Abs. 3 Satz 4 BNDG beschränkt ist und keine inlandsbezogenen Erkenntnisziele verfolgen darf. Auch eine Auswertung zu einem auf das Ausland bezogenen Zweck setzt die betroffenen Inländerinnen und Inländer gewichtigen Risiken aus. So erlaubt § 26 Abs. 3 Satz 4 Nr. 1 BNDG dem Bundesnachrichtendienst eine Datenauswertung zu dem Zweck,

ausländische „Personen […] zu erkennen, die einen Deutschlandbezug aufweisen und über die Informationen erlangt werden können, die für die Aufgabenerfüllung des Bundesnachrichtendienstes relevant sind“. Als aufgabenrelevante Informationen über die ausländische Person könnten etwa Angaben über ihre Kontakte im Inland und deren Verhältnis zueinander angesehen werden, an die dann weitere Überwachungsmaßnahmen anschließen könnten,

> gerade auf eine solche Nutzung der bevorrateten Verkehrsdaten zur Verdachtsgewinnung mit Blick auf (inländische) „auftragsrelevante Teilnehmer und Beziehungsnetze“ verweist auch die Gesetzesbegründung, BT-Drs. 19/26103, S. 77.

In dieser naheliegenden Auslegung ermöglicht § 26 Abs. 3 Satz 4 Nr. 1 BNDG dem Bundesnachrichtendienst also, mittelbar inlandsgerichtete Auswertungsziele zu verfolgen. Eine reine Inlandsaufklärung ist dem Dienst ohnehin wegen seiner Aufgabenstellung verwehrt. Die von dem Bundesverfassungsgericht ausdrücklich errichtete Vorgabe, dass eine strategische Überwachung inländischer Telekommunikation unzulässig ist, ergibt daher nur mit Bezug auf derartige Aufklärung über das Ausland mit Inlandsbezug überhaupt Sinn.

Auch die Unkenntlichmachung der Daten verhindert nicht, dass der Bundesnachrichtendienst solche mittelbar inlandsbezogenen Auswertungsziele verfolgt. Sie kann daher das verfassungsrechtliche Verbot der strategischen Inlandsaufklärung nicht aufheben. Im Übrigen legt das Gesetz die Unkenntlichmachung so an, dass sie eine Identifizierung der betroffenen Inländerinnen und Inländer nicht zuverlässig verhindert. Zwar ordnet § 26 Abs. 3 Satz 3 Hs. 2 BNDG an, die Unkenntlichmachung der bevorrateten Daten müsse dazu führen, dass die „rückwirkende Identifizierung der [betroffenen Inländerinnen und Inländer] unmöglich oder nur mit unvertretbar hohem Aufwand möglich“ sei. Unmittelbar zuvor gibt die Norm jedoch vor, dass die „Eindeutigkeit der Daten“ erhalten bleiben müsse. Auch nach der Unkenntlichmachung soll also feststellbar sein, ob unkenntlich gemachte Datensätze zu derselben oder zu unterschiedlichen Personen gehören. Nahe liegt hierzu die Berechnung eines sogenannten Hashwerts, also einer jeweils einzigartigen Zeichenfolge, die als eindeutiger Identifikator innerhalb des Datenbestands an die Stelle des unkenntlich gemachten Telekommunikationsmerkmals (etwa einer Telefonnummer oder einer E-Mail-Adresse) tritt,

> so BT-Drs. 19/26103, S. 78.

Aus einem Hashwert kann das unkenntlich gemachte Merkmal nicht unmittelbar zurückgerechnet werden. Die Unkenntlichmachung mittels Hashwert verhindert aber nicht, dass die unkenntlich gemachten Daten mit Zusatzwissen verknüpft werden, um das unkenntlich gemachte Merkmal zu erschließen. Eine solche Verknüpfung liegt gerade für die in § 26 Abs. 3 Satz 2 BNDG genannten Datenbestände ausgesprochen nahe. So wird es in vielen Fällen möglich sein, die unkenntlich gemachten Verkehrsdaten menschlicher Kommunikation mit den nicht unkenntlich gemachten Verkehrsdaten intermaschineller Kommunikation zu verknüpfen und so bestimmte Inländerinnen und Inländer als betroffene Personen zu identifizieren. Wenn beispielsweise einerseits bekannt ist, dass von demselben Mobiltelefon zu unterschiedlichen Zeiten und in unterschiedlichen Funkzellen mehrere Telefongespräche geführt wurden (unkenntlich gemachte menschliche Kommunikation), und andererseits ein Mobiltelefon mit einer bestimmten (personenbeziehbaren) Kennung zu allen Gesprächszeiten jeweils in denselben Funkzellen angemeldet war oder im Wirkungsbereich dieser Funkzellen Navigationsdienste aufgerufen hat (intermaschinelle Kommunikation), so lässt sich je nach Zahl der Telefonate mit hoher bis an Sicherheit grenzender Wahrscheinlichkeit darauf schließen, dass die Telefongespräche von diesem Telefon ausgingen,

> ähnlich die Stellungnahme des BfDI, BT-Ausschussdrs. 19(4)682, S. 7.

Auch andere Datenbestände lassen sich mit den unkenntlich gemachten Verkehrsdaten verknüpfen, um diese zu repersonalisieren. Ist beispielsweise das Bewegungsverhalten einer Person über einen hinreichend langen Zeitraum bekannt, so kann diese Information genutzt werden, um unkenntlich gemachte Standortdaten zuzuordnen. Die Unkenntlichmachung ist daher insgesamt als bloße Pseudonymisierung anzusehen, die eine wichtige Schutzvorkehrung sein kann, an der prinzipiellen Schutzbedürftigkeit der betroffenen Daten jedoch nichts ändert.

6. Benachrichtigung inländischer Betroffener

Erhebt der Bundesnachrichtendienst trotz der in § 19 Abs. 7 Satz 1 BNDG vorgesehenen Filterung personenbezogene Daten von Inländerinnen und Inländern, so hat er diese grundsätzlich unverzüglich zu löschen. Eine Ausnahme gilt nach § 19 Abs. 7 Satz 5 BNDG, wenn durch die Weiterverarbeitung eine erhebliche Gefahr für bestimmte hochrangige Rechtsgüter abgewendet werden kann. Diese nicht zu beanstandende Ausnahmeregelung muss durch eine Pflicht zur Benachrichtigung der betroffenen Inländerinnen und Inländer

flankiert werden, um eine weitestmögliche Transparenz der Überwachung zu gewährleisten,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 268.

Die danach gebotene Regelung über die Benachrichtigung betroffener Personen findet sich in § 59 Abs. 2 Satz 1 BNDG. Jedoch enthält diese Regelungen zu weitreichende Ausnahmen von der grundsätzlichen Benachrichtigungspflicht.

Nach § 59 Abs. 2 Satz 1 Nr. 1 BNDG unterbleibt die Benachrichtigung, solange eine Gefährdung des Zwecks der Maßnahme nicht ausgeschlossen werden kann. Zwar ist die Sicherung des Überwachungszwecks grundsätzlich ein verfassungsrechtlich tragfähiger Grund, die Benachrichtigung zurückzustellen,

> vgl. etwa BVerfGE 129, 208 (254); 141, 220 (283).

Indem jedoch § 59 Abs. 2 Satz 1 Nr. 1 BNDG die Benachrichtigung generell sperrt, solange eine Gefährdung des Überwachungszwecks lediglich *nicht auszuschließen* ist, lässt die Norm nach ihrem Wortlaut schon entfernte Risiken ausreichen, damit der Ausnahmetatbestand greift. Angesichts des großflächigen Überwachungsansatzes der strategischen Ausland-Fernmeldeaufklärung wird sich praktisch nie mit Sicherheit ausschließen lassen, dass eine Benachrichtigung solche Risiken birgt. § 59 Abs. 2 Satz 1 Nr. 1 BNDG beschränkt die Benachrichtigungspflicht daher unverhältnismäßig weit. Zu fordern ist vielmehr eine Regelung, nach der die Benachrichtigung nur unterbleibt, wenn konkrete Tatsachen für eine Gefährdung des Überwachungszwecks sprechen,

> implizit verlangt solche positiven Anhaltspunkte auch BVerfGE 100, 313 (397 f.); vgl. ferner die nochmals einschränkende Auslegung des ohnehin deutlich restriktiver gefassten Ausnahmetatbestands in § 20w Abs. 2 Satz 1 Hs. 2 BKAG a.F. durch BVerfGE 141, 220 (320).

Gleichfalls unverhältnismäßig weit gefasst ist § 59 Abs. 2 Satz 1 Nr. 2 BNDG, der die Benachrichtigung ausschließt, solange ein überwiegender Nachteil für das Wohl des Bundes oder eines Landes absehbar ist.

Sowohl der Begriff des Bundes- oder Landeswohls als auch der Begriff des überwiegenden Nachteils sind weitgehend unbestimmt und grenzen den Grund für eine Zurückstellung der Benachrichtigung praktisch nicht ein. Unter das Wohl des Bundes oder eines Landes lässt sich – anders als unter den etwa in § 74 Abs. 2 Satz 1 BKAG in Bezug genommenen Bestand des Staates

– der gesamte Aufgabenkreis des Bundesnachrichtendienstes oder auch jeder anderen Behörde subsumieren,

> vgl. zur Interpretation dieses Begriffs im Rahmen von § 96 StPO Gerhold, in: BeckOK StPO, § 96 Rn. 5: „Der Begriff des Nachteils für das Staatswohl wird weit gefasst und ist bereits gegeben, wenn die Erfüllung öffentlicher Aufgaben ernstlich gefährdet oder erheblich erschwert würde."

Zudem muss der absehbare Nachteil nach dem Wortlaut der Norm in keinem Zusammenhang mit dem Überwachungszweck stehen, so dass der Ausnahmetatbestand auch hierdurch nicht konkretisiert wird. Für die Zurückstellung und – auf der Grundlage von § 59 Abs. 2 Satz 4 BNDG – den endgültigen Ausschluss der Benachrichtigung reichen damit annähernd beliebige behördliche Opportunitätserwägungen aus, solange diese aufgrund einer normativ nicht angeleiteten Abwägung wichtiger erscheinen als die Benachrichtigung.

Für die Verfassungsmäßigkeit von § 59 Abs. 2 Satz 1 Nr. 2 BNDG lässt sich nicht anführen, dass dieser Ausnahmetatbestand weitgehend wörtlich dem Urteil des Bundesverfassungsgerichts zu strategischen Beschränkungen nach dem G 10 vom 14. Juli 1999 entnommen ist,

> vgl. BVerfGE 100, 313 (398).

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

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

soweit diese eine Ausnahme von der Benachrichtigungspflicht rechtfertigen können,

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

7. Kontrolle

Die strategische Ausland-Fernmeldeaufklärung muss durch eine unabhängige objektivrechtliche Kontrolle flankiert werden. Die Kontrolle muss als kontinuierliche Rechtskontrolle einen umfassenden Kontrollzugriff ermöglichen. Sie ist auf die Wahrung der Grundrechte der Betroffenen auszurichten und gilt der Sicherung und praktischen Effektivierung der rechtlichen Grenzen der staatlichen Überwachungstätigkeit. Die Kontrolle muss zweigliedrig ausgestaltet und auf eine gerichtsähnliche Stelle sowie eine unabhängige administrative Stelle verteilt werden,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 272 ff.

Das BNDG schafft mit dem Unabhängigen Kontrollrat ein Kontrollorgan, das den verfassungsrechtlichen Anforderungen an die institutionelle Ausgestaltung der Kontrolle in der Grundanlage genügt. Im Einzelnen finden sich jedoch erhebliche verfassungsrechtliche Defizite.

a) Anordnung gezielter Datenerhebungen

Ein gesteigertes Kontrollbedürfnis besteht, soweit sich eine strategische Telekommunikationsüberwachung gezielt auf Personen erstreckt, die als mögliche Verursacher von Gefahren oder in Blick auf gegenüber ihnen zu ergreifende Folgemaßnahmen im unmittelbaren Interesse des Nachrichtendienstes stehen. Die Festlegung einer solchen Überwachungsmaßnahme bedarf einer gerichtsähnlichen Ex-ante-Kontrolle. Diese hat zu prüfen, ob die gezielt personenbezogene Überwachung zur Verfolgung des Überwachungszwecks den Verhältnismäßigkeitsanforderungen genügt,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 188.

Dementsprechend sieht § 23 Abs. 7 Satz 1 i.V.m. Abs. 5 Satz 1 Nr. 2 BNDG hinsichtlich gezielt personenbezogener Überwachungen grundsätzlich eine Vorabprüfung durch den Unabhängigen Kontrollrat vor. Hiervon ergibt sich allerdings eine Ausnahme aus § 23 Abs. 5 Satz 2 BNDG, wenn zu dem Überwachungsziel bereits eine Beschränkungsanordnung nach § 3, § 5 oder § 8 G 10 vorliegt. In einem solchen Fall ist gemäß § 23 Abs. 5 Satz 3 BNDG der Unabhängige Kontrollrat lediglich über die Beschränkungsanordnung zu informieren.

Diese Ausnahme steht mit dem Erfordernis einer gerichtsähnlichen Ex-ante-Kontrolle nicht in Einklang. Sie lässt sich insbesondere nicht mit der Erwägung rechtfertigen, dass für Beschränkungsanordnungen nach dem G 10 gemäß § 15 Abs. 6 G 10 eine Vorabkontrolle durch die G 10-Kommission des Bundestages vorgesehen ist. Diese Kontrolle könnte die Vorabkontrolle nach § 23 Abs. 7 Satz 1 BNDG nur ersetzen, wenn beide Kontrollen gleichwertig wären. Hierzu müssten die Regelungen über die G 10-Kommission den Anforderungen an Ausgestaltung und Verfahren des gerichtsähnlichen Kontrollorgans genügen. Dies ist jedoch nicht der Fall.

So verlangt § 15 Abs. 1 G 10 für die Mitglieder der G 10-Kommission weder eine besondere fachliche Expertise noch eine langjährige richterliche Erfahrung zumindest für einen maßgeblichen Teil von ihnen. Auch werden die Mitglieder der G 10-Kommission lediglich ehrenamtlich tätig,

> vgl. demgegenüber BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 284 ff.

Darüber hinaus ist wegen der institutionellen Anbindung der G 10-Kommission an den Bundestag und mangels einer Sicherheitsüberprüfung, wie sie § 43 Abs. 2 BNDG für die Mitglieder des gerichtsähnlichen Kontrollorgans vorsieht, nicht gewährleistet, dass die Kontrolle durch die G 10-Kommission nicht unter Berufung auf die *Third Party Rule* behindert wird,

> vgl. demgegenüber BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 292 ff.

Schließlich ermöglicht § 15a Abs. 1 G 10, dass eine Überwachungsanordnung bei Gefahr im Verzug auch ohne vorherige Zustimmung der G 10-Kommission vollzogen werden kann. Im Unterschied hierzu sieht § 23 Abs. 7 Satz 3 BNDG auch bei Gefahr im Verzug zumindest eine vorläufige Ex-ante-Prüfung durch ein Mitglied des gerichtsähnlichen Kontrollorgans vor. Nur diese Regelung trägt dem verfassungsrechtlichen Erfordernis einer Ex-ante-Kontrolle vollständig Rechnung.

b) Kontrolle des Einsatzes von Suchbegriffen

Die gerichtsähnliche Kontrolle muss sich teilweise auf den Einsatz der Suchbegriffe erstrecken, die der Bundesnachrichtendienst bei der Erhebung von Inhaltsdaten nutzt. Eine gerichtsähnliche Kontrolle des Einsatzes von Suchbegriffen ist zwar nicht generell geboten. Sie ist jedoch angezeigt, wenn und soweit sich die Suchbegriffe gezielt auf Personen richten, die entweder als mög-

liche Gefahrenquelle im unmittelbaren Interesse des Bundesnachrichtendienstes stehen oder deren Kommunikation einen besonderen Vertraulichkeitsschutz genießt,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 188, 194, 278; tendenziell strenger fordert eine Einbeziehung zumindest der Typen oder Kategorien der zu verwendenden Suchbegriffe, EGMR, Urteil vom 25. Mai 2021, No. 58170/13, 62322/14 und 24960/15 – Big Brother Watch u.a. gegen Vereinigtes Königreich, Rn. 354.

Eine gerichtsähnliche Kontrolle der Suchbegriffe ist in diesen Fallkonstellationen auch darum unabdingbar, weil sich ansonsten kaum nachvollziehen lässt, ob die besonderen Schutzregelungen aus § 20 Abs. 2 und § 21 Abs. 2 BNDG gewahrt sind. Die inhaltlichen Vorgaben für die Anordnung der Überwachung aus § 23 Abs. 6 Satz 2 BNDG ermöglichen eine solche nachvollziehende Kontrolle für sich genommen nicht, weil sie die konkrete Verstrickung der Person, gegen die sich die Überwachung richtet, und die daraus resultierenden spezifischen Überwachungsbedürfnisse nicht transparent machen. Insbesondere das Erfordernis, das Ziel der gezielten Datenerhebung anzugeben, ist zu allgemein gehalten, um eine gehaltvolle nachvollziehende Kontrolle zu ermöglichen.

Hinsichtlich der Frage, inwieweit die gebotene Kontrolle der Suchbegriffe ex ante oder ex post und im letzteren Fall – gegebenenfalls im Zusammenwirken mit der administrativen Kontrollinstanz – nur stichprobenmäßig stattfindet, steht dem Gesetzgeber ein Spielraum zu. Auch dieser ist allerdings durch den Verhältnismäßigkeitsgrundsatz gebunden, der jedenfalls im Hinblick auf grundlegende Entscheidungen eine vorherige Kontrolle gebietet,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 278.

Nach dem gesetzlichen Kontrollkonzept unterliegen Anordnungen von gezielten Datenerhebungen gegenüber mutmaßlichen Gefahrverursachern und zur Erlangung von Daten aus einer Vertraulichkeitsbeziehung gemäß § 23 Abs. 5 Satz 1 Nr. 2 und 3, Abs. 7 Satz 1 BNDG grundsätzlich einer Ex-ante-Kontrolle durch das gerichtsähnliche Kontrollorgan. Da allerdings die Anordnung einer solchen Datenerhebung gemäß § 23 Abs. 6 Satz 2 BNDG einzelne Suchbegriffe, die zur gezielten Datenerhebung verwendet werden, nicht nennen muss, erstreckt sich die Ex-ante-Kontrolle nicht auf die Suchbegriffe. Die Überprüfung der Rechtmäßigkeit der Suchbegriffe obliegt stattdessen gemäß § 51 Abs. 1 Satz 2 Hs. 2 BNDG grundsätzlich dem administrativen Kontrollorgan. Das gerichtsähnliche Kontrollorgan gibt dieser Prüftätigkeit gemäß § 51 Abs. 2

BNDG einen Rahmen vor und kann darüber hinaus konkrete und einzelfallbezogene Prüfaufträge erteilen.

Dieses Kontrollkonzept hebelt die verfassungsrechtliche Vorgabe einer gerichtsähnlichen Kontrolle des Einsatzes von Suchbegriffen in den genannten besonders sensiblen Fallkonstellationen weitgehend aus. An ihre Stelle tritt die für sich genommen gerade nicht ausreichende Kontrolle durch das administrative Kontrollorgan. Die Einwirkungsmöglichkeiten des gerichtsähnlichen Kontrollorgans auf das administrative Kontrollorgan können den Ausfall einer verbindlich geregelten gerichtsähnlichen Kontrolle nicht kompensieren, da sie nicht spezifisch auf den gezielten Einsatz von Suchbegriffen in besonders sensiblen Fällen ausgerichtet sind. Wie das gerichtsähnliche Kontrollorgan von § 51 Abs. 2 BNDG im Einzelnen Gebrauch macht, überlässt das Gesetz stattdessen seinem nicht näher angeleiteten Ermessen. Das gerichtsähnliche Kontrollorgan könnte beispielsweise ohne Verstoß gegen § 51 Abs. 2 BNDG dem administrativen Kontrollorgan lediglich allgemein eine stichprobenartige Kontrolle aller Suchbegriffe aufgeben und auf einzelfallbezogene Prüfaufträge hinsichtlich von Suchbegriffen ganz verzichten. Eine auch nur halbwegs systematische Kontrolle des Einsatzes von Suchbegriffen in den hier relevanten Fallkonstellationen wäre dann nicht gewährleistet.

Um dem verfassungsrechtlichen Erfordernis einer gerichtsähnlichen Kontrolle des Einsatzes von Suchbegriffen zu genügen, müsste das Gesetz daher eine ausdrückliche Kontrollregelung enthalten, die eine wenigstens stichprobenartige Kontrolle ausdrücklich festschreibt.

Selbst wenn jedoch der im Gesetz angelegte Kontrollmechanismus für ausreichend gehalten wird, ist er defizitär ausgestaltet, weil eine wirksame Kontrolle der eingesetzten Suchbegriffe auch mit Blick auf das administrative Kontrollorgan nicht gewährleistet ist. Grund hierfür ist, dass es keine Regelung im BNDG gibt, die eine Protokollierung der eingesetzten Suchbegriffe vorsieht. Insbesondere wenn Suchbegriffe nur über kurze Zeit genutzt werden, ist daher davon auszugehen, dass sie selbst für eine regelmäßige stichprobenartige Kontrolle nicht zuverlässig zur Verfügung stehen. Die dadurch bewirkte zufallsabhängige Ausdünnung des Kontrollmaterials ist verfassungsrechtlich angesichts der hohen Sensibilität der Überwachung in den hier relevanten Fallkonstellationen nicht hinnehmbar,

> eine umfassende Protokollierung aller kontrollbedürftigen Umstände einschließlich der Suchbegriffe fordert auch EGMR, Urteil vom 25. Mai 2021, No. 58170/13, 62322/14 und 24960/15 – Big Brother Watch u.a. gegen Vereinigtes Königreich, Rn. 356.

c) Kein Beschwerderecht potenziell betroffener Personen

Die gerichtsähnliche Kontrolle ist zudem insoweit lückenhaft ausgestaltet, als es an einem Recht potenziell betroffener Personen fehlt, ein Kontrollverfahren durch den Unabhängigen Kontrollrat einzuleiten.

Das BNDG sieht für die strategische Ausland-Fernmeldeaufklärung – anders als § 15 Abs. 5 Satz 1 G 10 für strategische Beschränkungen der internationalen Telekommunikation – kein ausdrückliches Beschwerderecht potenziell betroffener Personen gegen Überwachungsmaßnahmen vor. Erst recht enthält das Gesetz keine Verfahrensregelungen für den Umgang mit solchen Beschwerden.

Das Bundesverfassungsgericht hat demgegenüber in seinem Urteil zur Ausland-Ausland-Fernmeldeaufklärung dem Gesetzgeber zur Prüfung aufgegeben, ob Personen, die plausibel machen können, von Überwachungsmaßnahmen möglicherweise betroffen gewesen zu sein, das Recht eingeräumt werden kann, diesbezüglich mit eigenen Verfahrensrechten eine objektivrechtliche Kontrolle anzustoßen,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 280.

Das vorliegende Verfahren gibt Anlass, diesen Auftrag aufzugreifen und zu verschärfen. Die Einrichtung eines solchen Kontrollverfahrens ist unabdingbar, um die betroffenen Personen nicht zu bloßen Objekten der Überwachung zu degradieren. Denn ohne ein derartiges Verfahren haben sie faktisch keine Möglichkeiten, sich gegen möglicherweise rechtswidrige Datenerhebungen und Datenweiterverarbeitungen zu wehren. Ein gerichtlicher Ex-post-Rechtsschutz ist für sie praktisch nicht verfügbar. Insbesondere Ausländerinnen und Ausländer im Ausland, die von der Überwachung nicht benachrichtigt werden, werden so gut wie nie die Möglichkeit haben, zulässigerweise das Bundesverwaltungsgericht anzurufen. Grund hierfür sind die hohen, jedenfalls für diesen Personenkreis kaum überwindbaren Anforderungen an die Konkretisierung des Streitgegenstands,

vgl. oben B. III.

Dementsprechend hat der Europäische Gerichtshof für Menschenrechte in seinem nach dem Urteil des Bundesverfassungsgerichts ergangenen *Big Brother Watch*-Urteil eine Ex-post-Kontrolle auf Antrag potenziell Betroffener als Teil der „Ende-zu-Ende-Garantien“ („end-to-end safeguards“) bezeichnet, die zur Rechtfertigung eines Massenüberwachungsprogramms erforderlich sind,

EGMR, Urteil vom 25. Mai 2021, No. 58170/13, 62322/14 und 24960/15 – Big Brother Watch u.a. gegen Vereinigtes Königreich, Rn. 350 und 357 f.

Diese Wertung ist zur Konkretisierung des Fernmeldegeheimnisses heranzuziehen, da anderenfalls der Grundrechtsschutz nach dem Grundgesetz hinter dem konventionsrechtlichen Mindeststandard zurückbliebe.

d) Verfahren des gerichtsähnlichen Kontrollorgans

Schließlich genügen die Regelungen zum Verfahren des Unabhängigen Kontrollrats in seiner Funktion als gerichtsähnliches Kontrollorgan nicht in jeder Hinsicht den verfassungsrechtlichen Anforderungen. Die gerichtsähnliche Kontrolle hat die Schutzaufgabe zu erfüllen, die sonst dem Richtervorbehalt sowie auch nachträglichen Rechtsschutzmöglichkeiten, insbesondere Feststellungsklagen, zukommt. Entsprechend muss mit ihr eine auf den Einzelfall bezogene Prüfung ermöglicht werden, die materiell und verfahrensmäßig einer gerichtlichen Kontrolle gleichwertig, insbesondere mindestens ebenso wirkungsvoll ist,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 275.

Nach diesem Maßstab sind die Möglichkeiten des gerichtsähnlichen Kontrollorgans zur Informationsbeschaffung teils unzureichend ausgestaltet,

Gärditz, BT-Ausschussdrs. 19(4)731 A, S. 12.

Die für gerichtliche Verfahren geltenden Prozessordnungen sind auf den Unabhängigen Kontrollrat auch in seiner gerichtsähnlichen Funktion nicht anwendbar. Dies gilt insbesondere für die prozessrechtlichen Vorschriften über die Beschaffung von Informationen beziehungsweise Beweismitteln. Stattdessen verpflichtet § 56 BNDG den Bundesnachrichtendienst zur informationellen Unterstützung des Unabhängigen Kontrollrats. Diese Unterstützungspflicht bleibt jedoch in wesentlichen Punkten hinter den gerichtlichen Beweiserhebungsbefugnissen zurück, sodass die Kontrolle einer gerichtlichen Kontrolle nicht gleichwertig ist.

Insbesondere kann der Unabhängige Kontrollrat die Mitwirkungspflicht aus § 56 BNDG nicht durchsetzen. Er kann auskunftspflichtige Personen anders als ein Gericht (vgl. etwa § 96 Abs. 1, § 98 VwGO i.V.m. § 380, § 390, § 409 ZPO) oder auch ein parlamentarischer Untersuchungsausschuss (vgl. § 27, § 29 Abs. 3 PUAG) nicht zur Aussage zwingen. Zwar kann sich das gerichtsähnliche Kontrollorgan gegebenenfalls an den Präsidenten des Bundesnach-

richtendienstes wenden, damit dieser einen Beschäftigten des Bundesnachrichtendienstes anweist, die gesetzliche Mitwirkungspflicht zu erfüllen. Gegenüber dem Präsidenten selbst verfügt das Kontrollorgan jedoch wiederum nicht über eigene Durchsetzungsinstrumente.

Darüber hinaus sind Verstöße gegen die Mitwirkungspflicht aus § 56 BNDG nicht in hinreichendem Ausmaß sanktioniert. Sagt ein Beschäftigter des Bundesnachrichtendienstes vor dem gerichtsähnlichen Kontrollorgan falsch aus, so kann dies zwar dienstrechtliche Konsequenzen haben. Die für Falschaussagen vor Gerichten und parlamentarischen Untersuchungsausschüsse geltenden Straftatbestände (§§ 153 ff. StGB) sind jedoch nicht anwendbar. Insbesondere weil das gerichtsähnliche Kontrollorgan in besonderem Maße auf die Zulieferung von Informationen angewiesen ist, die es für seine Kontrolltätigkeit benötigt, ist diese Sanktionslücke nicht hinnehmbar.

Überhaupt keine auch nur mittelbar nutzbaren Mittel zur Erzwingung einer informationellen Unterstützung hat das gerichtsähnliche Kontrollorgan gegenüber behördenexternen Personen, auf deren Kenntnisse es für seine Tätigkeit ankommt. Hierzu können etwa frühere Beschäftigte des Bundesnachrichtendienstes, behördenexterne menschliche Quellen oder Mitarbeiter von Telekommunikationsunternehmen zählen. Die in § 41 Abs. 5 Satz 1 Nr. 2 BNDG vorgesehene Verfahrensordnung kann die erforderlichen Durchsetzungsmechanismen nicht bereitstellen, da sie mangels außenrechtlicher Qualität keine Grundrechtseingriffe legitimieren kann.

8. Übermittlung der erlangten Daten

Die Ermächtigungen zur Übermittlung der durch die strategische Ausland-Fernmeldeaufklärung gewonnenen Daten müssen dem Verhältnismäßigkeitsgrundsatz in seiner Konkretisierung durch das Kriterium der hypothetischen Datenneuerhebung genügen. Dieses Kriterium ist an den besonderen Kontext der strategischen Telekommunikationsüberwachung anzupassen. Im Einzelnen hängen die verfassungsrechtlichen Anforderungen davon ab, zu welchem Zweck der Bundesnachrichtendienst die Überwachung durchgeführt hat und zu welchem Zweck er die erlangten Daten übermittelt. So dürfen einerseits die Erkenntnisse aus Überwachungen, die zur politischen Unterrichtung der Bundesregierung durchgeführt wurden, nur im Ausnahmefall einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person, für lebenswichtige Güter der Allgemeinheit oder für den Bestand oder die Sicherheit des Bundes oder eines Landes an andere Stellen als die Bundesregierung übermittelt werden. Andererseits darf der Bundesnachrichtendienst Informationen

an die Bundesregierung zur Wahrnehmung ihrer außen- und sicherheitspolitischen Verantwortung ohne Bindung an einen qualifizierten Rechtsgüterschutz oder an besondere Übermittlungsschwellen übermitteln,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 211 ff.

Nach diesen Maßgaben verfehlen die Übermittlungsermächtigungen in § 29 und § 30 BNDG in weiten Teilen die verfassungsrechtlichen Anforderungen.

a) Übermittlung an Inlandsnachrichtendienste

Die Ermächtigung zu Übermittlungen an die Inlandsnachrichtendienste des Bundes und der Länder in § 29 Abs. 1 Nr. 1 BNDG ist hinsichtlich der tatsächlichen Übermittlungsschwelle zu weit gefasst.

Grundsätzlich bestehen an eine Datenübermittlung von einem Nachrichtendienst an einen anderen Nachrichtendienst weniger strenge Anforderungen als für Übermittlungen an operativ tätige Behörden, da das Risiko von Folgeeingriffen reduziert ist. Dieser Umstand rechtfertigt prinzipiell eine Absenkung der Übermittlungsschwelle,

BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 257 ff.

Bei der Übermittlung von Daten, die aus der strategischen Ausland-Fernmeldeaufklärung stammen, sind allerdings die spezifischen verfassungsrechtlichen Grenzen dieser Maßnahme zu berücksichtigen. Die strategische und damit weitgehend verdachtslose großflächige Informationsgewinnung kann selbst als nachrichtendienstliches Mittel nur für die Auslandsaufklärung legitimiert werden,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 154 ff.

Für die Auslandsaufklärung ist ausschließlich der Bundesnachrichtendienst zuständig. Eine Datenübermittlung durch den Bundesnachrichtendienst an einen der Inlandsnachrichtendienste des Bundes und der Länder ergibt daher nur Sinn, wenn sich den durch die Ausland-Fernmeldeaufklärung gewonnenen Daten Informationen mit Relevanz für das Inland entnehmen lassen. Beispiele für danach übermittlungsfähige Daten bilden ausländische Telekommunikationsvorgänge, die sich inhaltlich auf das Inland beziehen, oder bevorratete Verkehrsdaten der inländischen intermaschinellen Kommunikation. In einem solchen Fall werden die Ergebnisse der strategischen Auslandsaufklärung also für die Inlandsaufklärung fruchtbar gemacht, in deren Rahmen eine strategische Telekommunikationsüberwachung jedoch gerade nicht zulässig wäre. Damit stellt sich hier ein ähnliches Umgehungsrisiko, wie es die Übermittlung

nachrichtendienstlicher Informationen an operativ tätige Behörden kennzeichnet,

> vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 246 ff.; Beschluss vom 28. September 2022 – 1 BvR 2354/13 –, Rn. 120.

Dementsprechend ist eine Absenkung der tatsächlichen Übermittlungsschwelle hinsichtlich dieser Datenübermittlung nicht angezeigt. Das Kriterium der hypothetischen Datenneuerhebung ist vielmehr in dem Sinne strikt zu beachten, dass eine Datenübermittlung nur zugelassen werden darf, wenn zumindest hinreichende tatsächliche Anhaltspunkte dafür vorliegen, dass die Daten zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall benötigt werden,

> vgl. allgemein zur Übermittlung nachrichtendienstlicher Daten an nicht operativ tätige Stellen BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 258.

Angesichts des hohen Eingriffsgewichts der strategischen Ausland-Fernmeldeaufklärung liegt darüber hinaus nahe, dass gesteigerte Anforderungen an die Beobachtungsbedürftigkeit der betreffenden Aktion oder Gruppierung zu stellen sind, wie sie für eingriffsintensive Überwachungsmaßnahmen der Verfassungsschutzbehörden bestehen,

> vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 190 ff.

Diesem Erfordernis genügt § 29 Abs. 1 Nr. 1 BNDG nicht. Diese Vorschrift erlaubt eine Datenübermittlung an Inlandsnachrichtendienste, wenn tatsächliche Anhaltspunkte dafür bestehen, dass sie zum Schutz besonders gewichtiger Rechtsgüter erforderlich ist. Dabei mag die für sich genommen wenig klare Bezugnahme auf besonders gewichtige Rechtsgüter angesichts des Umstands, dass das Bundesverfassungsgericht diesen Begriff in seiner Rechtsprechung konturiert hat, hinzunehmen sein. Die Ermächtigung setzt jedoch in tatsächlicher Hinsicht weder ausdrücklich noch implizit voraus, dass sich eine bestimmte Aktion oder Gruppierung benennen lässt, von der eine Bedrohung für solche Rechtsgüter ausgeht. Zum Schutz bestimmter Rechtsgüter kann eine Datenübermittlung bereits weit im Vorfeld einer derart konturierten Bedrohungslage erforderlich sein, etwa um allgemeine Lagebilder zu erstellen oder die Verwendung behördlicher Ressourcen zu planen,

> vgl. zu dem semantisch verwandten Kriterium des „Benötigens“ bestimmter Informationen „für Zwecke der öffentlichen Sicherheit“

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 311; Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 368.

Noch weniger errichtet § 29 Abs. 1 Nr. 1 BNDG qualifizierende Anforderungen an den nachrichtendienstlichen Beobachtungsbedarf, dem die Übermittlung dient.

Eine so weitreichende Absenkung der Übermittlungsschwelle ist angesichts der Eingriffsintensität der strategischen Ausland-Fernmeldeaufklärung, die nur als Instrument der Auslandsaufklärung überhaupt rechtfertigungsfähig ist, selbst bei einer Übermittlung an nicht operativ tätige Behörden nicht mehr hinnehmbar.

b) Übermittlung an inländische Behörden zur Unterrichtung der Bundesregierung oder einer Landesregierung

Die in § 29 Abs. 1 Nr. 2 und Abs. 2 BNDG enthaltenen Ermächtigungen, Daten aus der strategischen Ausland-Fernmeldeaufklärung zum Zweck der Unterrichtung der Bundesregierung oder einer Landesregierung zu übermitteln, verfehlen gleichfalls die verfassungsrechtlichen Anforderungen.

Zwar darf der Gesetzgeber Datenübermittlungen zum Zweck der politischen Information der Bundesregierung ohne besondere Anforderungen an Rechtsgüterschutz und Übermittlungsschwelle zulassen,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 223 ff.

Hingegen lässt sich eine unmittelbare Datenübermittlung an eine Landesregierung ohne besondere Voraussetzungen, wie sie § 29 Abs. 2 BNDG ermöglicht, nicht in derselben Weise legitimieren. Die Landesregierungen können zwar ein erhebliches Interesse an außen- und sicherheitspolitisch relevanten Informationen haben, da sich außenpolitische Spannungslagen im Inland und damit auf dem Hoheitsgebiet eines oder mehrerer Länder auswirken können. Gleichwohl tragen sie anders als die Bundesregierung keine unmittelbare außenpolitische Verantwortung. Die auswärtigen Beziehungen sind vielmehr gemäß Art. 32 Abs. 1 GG Sache des Bundes.

Zudem können die außenpolitischen Interessen der Bundesregierung und einer Landesregierung divergieren. Als Organ des Bundes ist der Bundesnachrichtendienst dazu verpflichtet und darauf beschränkt, den außenpolitischen Interessen der Bundesregierung zu dienen. Wird dem Dienst erlaubt, nach eigenem Ermessen Informationen auch unmittelbar an die Landesregierungen zu übermitteln, so können nicht nur bundespolitische Belange, sondern auch Individualrechte beeinträchtigt werden. Denn eine solche Übermittlung könnte

schlimmstenfalls dem Interesse der Bundesregierung zuwiderlaufen. Sie wäre dann nicht nur im Innenverhältnis des Bundesnachrichtendienstes zur Bundesregierung deplatziert, sondern würde auch den Verhältnismäßigkeitsgrundsatz verletzen. Eine interessenwidrige Datenübermittlung dient keinem verfassungsrechtlich legitimen Ziel, sodass der darin liegende Grundrechtseingriff nicht gerechtfertigt werden kann.

Eine Datenübermittlung durch den Bundesnachrichtendienst unmittelbar zum Zweck der politischen Unterrichtung einer Landesregierung ist darum als Sonderfall anzusehen, der insbesondere einer prozeduralen Einhegung durch den Vorbehalt einer Zustimmung des Bundeskanzleramts bedarf. Eine solche Vorgabe dient nicht nur dem Interesse der Bundesregierung, sondern schützt auch die betroffene Person vor einem nicht zielführenden und darum unverhältnismäßigen Grundrechtseingriff. Im Übrigen ist es Sache der Bundesregierung, die vom Bundesnachrichtendienst erlangten Informationen auf der Grundlage eigener politischer Entscheidungen mit den Landesregierungen zu teilen,

vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 226.

Nicht hinnehmbar ist zudem, dass § 29 Abs. 1 Nr. 2 und § 29 Abs. 2 BNDG Datenübermittlungen zum Zweck der politischen Unterrichtung nicht nur an die Regierung selbst, sondern auch an nachgeordnete Behörden erlaubt. Ein derartiger vermittelter Datenfluss begründet für die Betroffenen erhebliche zusätzliche Risiken. Durch ihn kann sich der Kreis der Stellen und die Zahl der Personen, die sensible personenbezogene Informationen erhalten, erheblich erweitern. Nachgeordnete Behörden können an den übermittelten Daten zudem nach ihrem Aufgabenkreis ein erhebliches Eigeninteresse haben, das über die rein politische Unterrichtung hinausgeht. Auch wenn eine operative Verwendung der gemäß § 29 Abs. 1 Nr. 2 und § 29 Abs. 2 BNDG übermittelten Informationen gemäß § 29 Abs. 12 Satz 2 BNDG unzulässig ist, begründet der gesetzlich vorgesehene Datenfluss faktisch das beträchtliche Risiko einer irrtümlichen oder sogar missbräuchlichen Verwendung der übermittelten Daten zu Zwecken, die über die politische Unterrichtung hinausgehen. Darüber hinaus vergrößert sich mit dem Kreis der Informationsträger auch das Risiko, dass es aufgrund von Sicherheitslücken zu einem Datenabfluss an Unbefugte kommt.

Ein rechtfertigender Grund dafür, diese Risiken hinzunehmen, ist nicht ersichtlich. Datenübermittlungen zum Zweck der Unterrichtung dienen allein der politischen Information auf Regierungsebene. Sollte die Bundesregierung zur

Einordnung bestimmter übermittelter Informationen auf die Expertise nachgeordneter Behörden zurückgreifen wollen,

> vgl. andeutungsweise BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 226,

kann und muss sie sich selbst an diese Stellen wenden. Es ist hingegen nicht Aufgabe des Bundesnachrichtendienstes, eigenständig einen Informationsverbund mit anderen Behörden zum Zweck einer gebündelten Unterrichtung der Bundesregierung herzustellen. Allenfalls dann, wenn eine Übermittlung an nachgeordnete Behörden von einer ausdrücklichen, auf den Einzelfall bezogenen Weisung der Bundesregierung abhängig gemacht würde, könnten die damit verbundenen zusätzlichen Risiken hingenommen werden.

Soweit schließlich die Gesetzesbegründung darauf verweist, die regierungsexternen Empfangsbehörden könnten die übermittelten Daten „für die Erstellung von eigenen Lagebildern nutzen“ und aus den Daten könne sich „für den Empfänger die abstrakte Erforderlichkeit ergeben, die Schwerpunkte der eigenen Arbeit aufgrund der z.B. erkennbaren politischen Veränderungen in relevanten ausländischen Staaten anzupassen“,

> BT-Drs. 19/26103, S. 81,

beschreibt sie Auswertungsinteressen, die über die politische Unterrichtung der Regierung hinausgehen und darum Datenübermittlungen nur nach Maßgabe strengerer Anforderungen rechtfertigen können.

c) Übermittlung zum Zweck der Strafverfolgung

Die Ermächtigung zu Datenübermittlungen zu Strafverfolgungszwecken in § 29 Abs. 3 BNDG ist gleichfalls teils zu weit gefasst. Solche Übermittlungen dürfen aufgrund der hohen Eingriffsintensität der strategischen Ausland-Fernmeldeaufklärung und wegen der mit ihnen beabsichtigten operativen Weiterverwendung der übermittelten Daten nur zur Verfolgung besonders schwerer Straftaten zugelassen werden, wenn bestimmte Tatsachen auf eine solche Tat hindeuten,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 222; vgl. ferner allgemein zur Übermittlung nachrichtendienstlicher Daten zu Strafverfolgungszwecken BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 249 ff.; Beschluss vom 28. September 2022 – 1 BvR 2354/13 –, Rn. 121.

Die Übermittlungsermächtigung in § 29 Abs. 3 BNDG verfehlt diese Anforderungen in zweifacher Hinsicht.

Erstens beschränkt sie sich nicht auf die Verfolgung besonders schwerer Straftaten, sondern lässt die Datenübermittlung auch zur Verfolgung weniger schwerwiegender Kriminalität zu. Zu beanstanden ist insoweit § 29 Abs. 3 Nr. 2 BNDG, der pauschal auf vorsätzliche Straftaten nach § 17 und § 18 AWG verweist. Während die Verbrechenstatbestände des § 17 AWG hinreichend schwer wiegen, gilt dies für die Straftatbestände nach § 18 AWG zumindest nicht durchweg. Dies ergibt sich aus den gesetzlichen Strafrahmen, die einen maßgeblichen Anhaltspunkt für die Schwere der Tat darstellen. Als besonders schwere Straftat können zumindest grundsätzlich nur Taten angesehen werden, die mit einer höheren Höchststrafe als fünf Jahren Freiheitsstrafe bewehrt sind,

> BVerfGE 109, 279 (347 f.)

Zumindest Straftatbestände, die eine niedrigere Höchststrafe als fünf Jahre Freiheitsstrafe vorsehen, beschreiben keine besonders schweren Straftaten,

> vgl. BVerfG, Beschluss vom 28. September 2022 – 1 BvR 2354/13 –, Rn. 155.

Demgegenüber sehen die in § 18 Abs. 1 bis 5 AWG enthaltenen Straftatbestände durchweg keine über fünf Jahre Freiheitsstrafe hinausgehende Höchststrafe vor. Der Strafrahmen von § 18 Abs. 5a und 5b AWG reicht sogar nur bis Freiheitsstrafe von einem Jahr.

Zweitens errichtet § 29 Abs. 3 BNDG insgesamt keine hinreichende Übermittlungsschwelle. Nach dieser Vorschrift reichen für eine Übermittlung tatsächliche Anhaltspunkte für eine Straftat aus. Diese Schwelle entspricht im strafprozessualen Sprachgebrauch dem Anfangsverdacht und bleibt hinter dem Erfordernis bestimmter Tatsachen beträchtlich zurück, das eine konkretisierte Verdachtslage beschreibt,

> vgl. BVerfGE 109, 279 (350 f.).

d) Übermittlung für Folgemaßnahmen mit unmittelbarer Außenwirkung

Die in § 29 Abs. 4 BNDG enthaltene Regelung zu Datenübermittlungen an öffentliche Stellen zum Zweck der Weiterverarbeitung mit unmittelbarer Außenwirkung für den Betroffenen genügt nicht vollständig den verfassungsrechtlichen Anforderungen. Keine Bedenken bestehen zwar gegen die in § 29

Abs. 4 Nr. 2 BNDG geregelte Datenübermittlung zur Gefahrenabwehr. Verfassungswidrig ist hingegen § 29 Abs. 4 Nr. 1 BNDG, der eine Datenübermittlung zulässt, soweit sie „in anderen Rechtsvorschriften vorgesehen ist“.

Diese Regelung verfehlt das Gebot der Normenklarheit. Nach der jüngeren Rechtsprechung des Bundesverfassungsgerichts steht bei diesem Gebot die inhaltliche Verständlichkeit einer Regelung im Vordergrund, insbesondere damit Bürgerinnen und Bürger sich auf mögliche belastende Maßnahmen einstellen können. Hierin unterscheidet es sich von dem Bestimmtheitsgrundsatz, der sich auf die Perspektive von Regierung, Verwaltung und Gerichten bezieht. Bei der heimlichen Datenerhebung und -verarbeitung, die tief in die Privatsphäre einwirken können, ergeben sich aus dem Gebot der Normenklarheit besonders strenge Anforderungen. Da die Handhabung hierauf bezogener Ermächtigungen von den Betroffenen weitgehend nicht wahrgenommen und angegriffen werden kann, kann ihr Gehalt nur sehr eingeschränkt im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden. Zwar nicht generell unzulässig, aber in besonderem Maße kontrollbedürftig sind nach diesem Maßstab Verweisungen aus einer Eingriffsermächtigung auf andere gesetzliche Regelungen,

> eingehend zuletzt BVerfG, Beschluss vom 28. September 2022 – 1 BvR 2354/13 –, Rn. 110 ff.

§ 29 Abs. 4 Nr. 1 BNDG verletzt das Gebot der Normenklarheit, indem er pauschal auf „Rechtsvorschriften“ verweist, die eine Datenübermittlung vorsehen. Als solche „Rechtsvorschriften“ kommen potenziell Regelungen im gesamten Bundesrecht, möglicherweise sogar in Landesgesetzen in Betracht. Zwar mag aus Sicht des Bundesnachrichtendienstes und der potenziellen Empfangsstelle bei der Entscheidung über eine konkrete Datenübermittlung erkennbar sein, nach welcher Regelung sich die Übermittlung richtet, ob diese Regelung die vorgesehene Übermittlung überhaupt tragen kann und wie ihre tatbestandlichen Voraussetzungen mit Blick auf diese Übermittlung auszulegen sind. Für Bürgerinnen und Bürger, die sich über das Spektrum möglicher Datenübermittlungen informieren und gegebenenfalls darüber in eine öffentliche Diskussion eintreten wollen, lässt der Verweis auf „Rechtsvorschriften“ hingegen nicht ansatzweise erkennen, um welche Normen und zugehörigen öffentlichen Interessen es sich handeln könnte.

Insbesondere beschränkt der Wortlaut von § 29 Abs. 4 Nr. 1 BNDG die Übermittlungsermächtigung nicht auf Regelungen, die ausdrücklich gerade Übermittlungen durch den Bundesnachrichtendienst zum Gegenstand haben und

sich darum auch aus Sicht interessierter behördenexterner Personen vergleichsweise leicht auffinden lassen. Vielmehr können unter den Normwortlaut gleichermaßen allgemeine Übermittlungsermächtigungen subsumiert werden, die sich an eine Vielzahl oder alle Behörden des Bundes und der Länder wenden. Von diesem Normverständnis geht auch die Gesetzesbegründung aus, die ausdrücklich die nicht behördenspezifische Regelung des § 99 VwGO als Beispiel für eine Rechtsvorschrift im Sinne von § 29 Abs. 4 Nr. 1 BNDG nennt,

> BT-Drs. 19/26103, S. 82.

Angesichts der durch das Bundesverfassungsgericht herausgearbeiteten strengen Anforderungen an die Übermittlung von Daten aus der strategischen Ausland-Fernmeldeaufklärung zur Vorbereitung außenwirksamer Maßnahmen,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 216 ff.

ist dieses hohe Maß an Unklarheit in dieser Ermächtigung nicht hinnehmbar.

Darüber hinaus verletzt § 29 Abs. 4 Nr. 1 BNDG auch den Verhältnismäßigkeitsgrundsatz, da er übermäßige Datenübermittlungen nicht durch hinreichend restriktive Übermittlungsvoraussetzungen ausschließt. Durch den Verweis auf irgendwelche „Rechtsvorschriften“ überlässt es diese Norm anderen Regelungen, die Voraussetzungen der Datenübermittlung so zu bestimmen, dass sie im Einklang mit den verfassungsrechtlichen Vorgaben stehen. Zumindest soweit dieser Verweis auch landesrechtliche Rechtsvorschriften erfassen sollte,

> so implizit BT-Drs. 19/26103, S. 82, der als Anwendungsfall „Behördenerklärungen zum Zwecke der Gefahrenabwehr an Polizeibehörden“ nennt,

hat der Bundesgesetzgeber damit seine grundrechtliche Regelungsverantwortung verfehlt, die Weiterverarbeitung der im Rahmen der strategischen Ausland-Fernmeldeaufklärung erhobenen Daten in einem angemessenen Rahmen zu halten,

> vgl. – tendenziell noch strenger – BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 –, Rn. 134.

Dasselbe gilt, soweit § 29 Abs. 4 Nr. 1 BNDG auch auf Rechtsvorschriften des Bundes verweist, die ohne spezifische Bezugnahme auf den Bundesnachrichtendienst Datenübermittlungen durch eine Vielzahl von Behörden regeln. Neben dem in der Gesetzesbegründung genannten § 99 VwGO könnten so etwa

die strafprozessualen Vorschriften über die Beweisaufnahme in der gerichtlichen Hauptverhandlung genutzt werden, um ohne Rücksicht auf das Gewicht der Straftat Erklärungen des Bundesnachrichtendienstes in strafgerichtliche Verfahren einzuführen, selbst wenn sie auf Informationen beruhen, die der Dienst durch eine strategische Ausland-Fernmeldeaufklärung gewonnen hat. § 29 Abs. 3 BNDG als spezielle Regelung stünde dem nicht zwingend entgegen, da diese Norm sich ausdrücklich lediglich auf Übermittlungen an „Strafverfolgungsbehörden“, also nicht an Gerichte bezieht. Vom Normwortlaut des § 29 Abs. 4 Nr. 1 BNDG gedeckt und nicht durch § 64 BNDG ausgeschlossen wäre sogar eine Anwendung der allgemeinen Verarbeitungsermächtigung des § 3 BDSG, die eine Datenübermittlung in äußerst weitem Ausmaß erlauben würde.

e) Übermittlung an die Bundeswehr

Zu weit gehen auch die Ermächtigungen zu Datenübermittlungen an die Bundeswehr in § 29 Abs. 5 BNDG.

Die in § 29 Abs. 5 Satz 1 BNDG genannten Rechtsgüter wiegen zwar hinreichend schwer, um eine Datenübermittlung zu rechtfertigen. Mit der Formulierung, es müssten tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung zum Schutz dieser Rechtsgüter erforderlich sei, errichtet die Norm jedoch keine hinreichende tatsächliche Übermittlungsschwelle,

> vgl. zu der gleichlautenden Formulierung in § 29 Abs. 1 Nr. 1 BNDG oben C. I. 8. a).

Angesichts der potenziell äußerst weitreichenden Folgen, die gerade eine Weiterverarbeitung übermittelter Daten durch die Bundeswehr für die Betroffenen haben kann, ist eine solche Übermittlungsschwelle verfassungsrechtlich hier im Ausgangspunkt ebenso geboten wie bei Übermittlungen an operativ tätige Polizei- oder Strafverfolgungsbehörden.

Entgegen der in der Gesetzesbegründung implizit vorausgesetzten Rechtsauffassung kann auf eine gesetzliche Umgrenzung der Übermittlungsschwelle nicht deshalb verzichtet werden, weil die Zusammenarbeit zwischen dem Bundesnachrichtendienst und der Bundeswehr verfassungsrechtlich privilegiert wäre. Auch die Begründung, die Bundeswehr selbst handle aufgrund verfassungsunmittelbarer Befugnisnormen sowie von Bundestagsmandaten und/oder völkerrechtlichen Rechtsgrundlagen, was ihre Aufgabenwahrnehmung von Strafverfolgungs- oder Gefahrenabwehrbehörden fundamental unterscheide,

vgl. BT-Drs. 19/26103, S. 82,

kann den Verzicht auf eine tatsächliche Übermittlungsschwelle nicht legitimieren.

Ob diese Rechtsauffassung mit Blick auf die Bundeswehr selbst zutrifft oder ob und inwieweit die Rechtsgrundlagen von deren Tätigkeit, soweit sie mit Grundrechtseingriffen verbunden ist, einer gesetzlichen Nachverdichtung bedürfen, ist im vorliegenden Verfahren nicht zu entscheiden. Jedenfalls lässt sie sich nicht auf Datenübermittlungen durch den Bundesnachrichtendienst übertragen, die gehaltvoll reguliert werden müssen, weil ansonsten die verfassungsrechtliche Legitimation für die strategische Telekommunikationsüberwachung durch den Dienst selbst entfiele,

vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 149, 218.

Auch die Spezifika der unterschiedlichen Tätigkeitsbereiche der Bundeswehr im In- und Ausland rechtfertigen jedenfalls nicht generell, auf gesetzliche Übermittlungsschwellen zu verzichten. Es mag Handlungsfelder der Bundeswehr – wie insbesondere Auslandseinsätze, die potenziell Kampfhandlungen einschließen – geben, die sich sowohl durch besonders weitreichenden Informationsbedarf als auch durch besondere Eilbedürftigkeit auszeichnen. Soweit eine Datenübermittlung unmittelbar dazu dient, die Bundeswehr auf diesen Handlungsfeldern zu unterstützen, erscheint eine Absenkung der Übermittlungsschwelle im Vergleich zu Übermittlungen an innerstaatlich operativ tätigen Sicherheitsbehörden tragbar. Der Schutzgutkatalog in § 29 Abs. 5 Satz 1 BNDG beschränkt sich jedoch nicht hierauf, sondern erfasst mit der Funktionsfähigkeit der Bundeswehr für die Landes- oder Bündnisverteidigung und bei Auslandseinsätzen den Großteil des Auftrags der Bundeswehr. So beinhaltet die Landes- und Bündnisverteidigung nach der Gesetzesbegründung generell „einerseits nationale Verteidigungsinteressen der Bundesrepublik Deutschland und andererseits Bündnisverpflichtungen in internationalen Bündnissen, an denen die Bundesrepublik Deutschland beteiligt ist“, ohne dass diese Interessen spezifiziert oder qualifiziert würden,

so zu § 19 Abs. 4 Nr. 1 lit. b BNDG BT-Drs. 19/26103, S. 57.

Zudem liegt es nahe, auch den Begriff der Funktionsfähigkeit weit im Sinne einer umfassenden Fähigkeit zur Aufgabenerledigung zu verstehen.

Damit erfasst die abgesenkte Übermittlungsschwelle die Hauptaufgaben der Bundeswehr praktisch in vollem Umfang. Dies ist verfassungsrechtlich nicht

haltbar. Es ist vielmehr Aufgabe des Gesetzgebers, für Datenübermittlungen an die Bundeswehr gegebenenfalls durch möglichst trennscharfe differenzierende Regelungen zu gewährleisten, dass sich die Absenkung der Übermittlungsschwelle auf die tatsächlich besonders informations- und zeitkritischen Handlungsfelder beschränkt. Die pauschale Inbezugnahme von Individualrechtsgütern sowie der – definitorisch nicht näher eingegrenzten – Funktionsfähigkeit der Bundeswehr hinsichtlich von sehr unterschiedlichen Aufgaben in § 29 Abs. 5 Satz 1 BNDG leistet dies nicht.

Zudem müsste im Gegenzug zu der grundrechtlich hochsensiblen Lockerung der Übermittlungsschwelle zumindest eine nachlaufende gerichtsähnliche Kontrolle eingerichtet werden, wie sie auch für die besonders kontrollbedürftigen Übermittlungen an ausländische Stellen geboten ist,

> vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 278.

Einen derartigen Kontrollmechanismus sieht § 29 Abs. 5 Satz 1 BNDG nicht vor.

Die Ermächtigung zu automatisierten Datenübermittlungen an die Bundeswehr in § 29 Abs. 5 Satz 2 BNDG ist gleichfalls unverhältnismäßig weit gefasst. Die Übermittlung setzt danach voraus, dass die übermittelten Daten im Rahmen strategischer Aufklärungsmaßnahmen mit Bezug zur Landes- oder Bündnisverteidigung sowie zu Einsätzen der Bundeswehr oder verbündeter Streitkräfte im Ausland (§ 19 Abs. 4 Nr. 1 lit. a BNDG) oder zum Schutz von Leib, Leben oder Freiheit einer Person (§ 19 Abs. 4 Nr. 2 lit. a BNDG) auf der Grundlage von Suchbegriffen erhoben wurden. Da insbesondere der in § 19 Abs. 4 Nr. 1 lit. a BNDG genannte Gefahrenbereich den Aufgabenkreis der Bundeswehr praktisch vollständig erfasst, hat diese Voraussetzung kaum eine begrenzende Wirkung. Eine Relevanzprüfung durch den Bundesnachrichtendienst nach § 27 BNDG ist hingegen nicht vorgesehen. Erst recht hat der Bundesnachrichtendienst nicht zu prüfen, ob in Bezug auf die weitergeleiteten Daten die Übermittlungsvoraussetzungen aus § 29 Abs. 5 Satz 1 BNDG vorliegen, was praktisch nie für *alle* Daten der Fall wäre.

§ 29 Abs. 5 Satz 2 BNDG schafft somit einen Überwachungsverbund zwischen Bundesnachrichtendienst und Bundeswehr. Der Bundesnachrichtendienst definiert das Ziel eines Überwachungsprojekts und bestimmt die maßgeblichen Suchbegriffe, wobei das Gesetz nicht ausschließt, dass Ziele und Suchbegriffe von anderen Stellen (wie der Bundeswehr) angeregt oder zugeliefert werden,

> auf diese Möglichkeit verweist ausdrücklich BT-Drs. 19/26103, S. 83.

Die Prüfung der erhobenen Daten auf ihre Relevanz für die Erkenntnisziele des Projekts wird hingegen an die Bundeswehr delegiert, ebenso alle nachgelagerten Auswertungsschritte. Die Bundeswehr wird auf diese Weise mit Tätigkeiten betraut, die nach der – verfassungsrechtlich angelegten – gesetzlichen Konzeption der strategischen Ausland-Fernmeldeaufklärung Teil der Überwachung selbst sind. In diesem Sinne enthält § 29 Abs. 5 Satz 2 BNDG keine bloße Übermittlungs-, sondern eine Kooperationsermächtigung, die hinsichtlich des arbeitsteiligen Zusammenwirkens der beteiligten Stellen mit den in §§ 31 ff. BNDG geregelten nachrichtendienstlichen Kooperationen vergleichbar ist.

Eine derartige innerstaatliche Überwachungskooperation zwischen Bundesnachrichtendienst und Bundeswehr konterkariert das vom Bundesverfassungsgericht für die Rechtfertigung der strategischen Telekommunikationsüberwachung angeführte Argument, dass die Überwachung mangels operativer Befugnisse des Bundesnachrichtendienstes nicht unmittelbar zu schwerwiegenden Folgen für die Betroffenen führen kann,

> vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 165.

Die Bundeswehr ist im Gegenteil aufgrund ihres Auftrags und ihrer Ausrüstung wie keine andere staatliche Stelle in der Lage und gegebenenfalls dazu berufen, in äußerst schwerwiegendem Ausmaß operativ in Grundrechte einzugreifen, und zwar gerade in die Grundrechte von Ausländerinnen und Ausländern im Ausland.

Wenn § 29 Abs. 5 Satz 2 BNDG gleichwohl – etwa aufgrund des nach außen gerichteten Verteidigungsauftrags der Bundeswehr und der (gesetzlich allerdings nirgends ausdrücklich geregelten) Aufgabe des Bundesnachrichtendienstes als auch militärischem Nachrichtendienst – überhaupt für rechtfertigungsfähig gehalten wird,

> auf das Erfordernis einer „validen und schnellen Datenübermittlung“ verweist BT-Drs. 19/26103, S. 82,

so muss die automatisierte Datenübermittlung zumindest mit strengen Vorgaben für die Auswertung und Weiterverarbeitung der übermittelten Daten verknüpft werden,

> vgl. für Kooperationen mit ausländischen Nachrichtendiensten, wenn dabei nicht vollständig ausgewertete Daten automatisiert übermittelt werden, BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 260 mit Verweis auf Rn. 242.

Hierzu ist gesetzlich sicherzustellen, dass die Daten nur dann für Folgemaßnahmen genutzt werden, die unmittelbar auf die Betroffenen einwirken, wenn sich aus ihnen hinreichend belastbare Anknüpfungspunkte für solche Maßnahmen ergeben. Zudem bedarf es, da mit der Datenauswertung ein erheblicher Teil der Überwachung auf die Bundeswehr verlagert wird, einer wirksamen Kontrolle der Datenauswertung bei der Bundeswehr durch hierfür geschaffene Kontrollstellen. § 29 Abs. 5 Satz 2 BNDG und die damit verknüpften, auf gewöhnliche Datenübermittlungen zugeschnittenen und insoweit nicht zu beanstandenden Schutzregelungen in § 29 Abs. 8 bis 16 BNDG gewährleisten dies nicht.

f) Übermittlung an sonstige inländische Stellen

Ebenfalls zu weit gefasst ist die in § 29 Abs. 6 Satz 1 BNDG enthaltene Ermächtigung zu Datenübermittlungen an sonstige inländische Stellen. Diese Regelung bezieht sich im Wesentlichen auf Datenübermittlungen an Private,

> vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 313.

Die gesetzliche Voraussetzung tatsächlicher Anhaltspunkte dafür, dass die Übermittlung zum Schutz bestimmter Rechtsgüter erforderlich ist, stimmt weitgehend mit der Vorgängerregelung in § 24 Abs. 2 Satz 1 BNDG a.F. i.V.m. § 19 Abs. 4 Satz 1 BVerfSchG überein. Lediglich das Erfordernis tatsächlicher Anhaltspunkte wurde in die Regelung neu aufgenommen. Allerdings ist nicht erkennbar, inwieweit sich hieraus sachliche Unterschiede ergeben sollen, da auch die Vorgängerregelung (selbstverständlich) keine Datenübermittlung aufgrund bloßer Spekulationen zuließ, sondern gleichfalls tatsächliche Anhaltspunkte als Mindestmaß voraussetzte. In der Folge fehlt es in § 29 Abs. 6 Satz 1 BNDG ebenso wie in der Vorgängervorschrift an einer hinreichenden tatsächlichen Eingriffsschwelle,

> vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 313, sowie zu der gleichläufigen Formulierung in § 29 Abs. 1 Nr. 1 BNDG oben C. I. 8. a).

g) Übermittlung ins Ausland

Auch § 30 BNDG, der Datenübermittlungen an ausländische Stellen vorsieht, steht nicht in jeder Hinsicht mit den verfassungsrechtlichen Anforderungen in Einklang.

Ermächtigungen zu Auslandsübermittlungen müssen die allgemeinen Anforderungen an Rechtsgüterschutz und Eingriffsschwellen wahren, wie sie auch für Datenübermittlungen an inländische Stellen gelten. Der Gesetzgeber ist

insoweit nicht gehindert, bei der begrifflichen Ausgestaltung der Ermächtigungen der Eigenständigkeit ausländischer Rechtsordnungen Rechnung zu tragen. Dies stellt das materielle Schutzniveau jedoch nicht in Frage,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 232.

Nach diesem Maßstab verfehlt zunächst § 30 Abs. 1 BNDG die verfassungsrechtlichen Anforderungen. Diese Regelung erlaubt Datenübermittlungen an ausländische öffentliche Stellen sowie über- und zwischenstaatliche Stellen zum Zweck der Unterrichtung im Rahmen der internationalen politischen Zusammenarbeit. Sie erfasst Daten sowohl aus Überwachungsprojekten zum Zweck der politischen Unterrichtung als auch zum Zweck der Gefahrenfrüherkennung. Die Ermächtigung setzt die Unterrichtung im Rahmen der internationalen politischen Zusammenarbeit somit mit der politischen Unterrichtung der Bundesregierung gleich. Diese Gleichsetzung ist jedoch nicht tragfähig. Als Organ der deutschen Staatsgewalt hat der Bundesnachrichtendienst eine spezifische Bindung an die Bundesregierung, die sich von dem Verhältnis des Dienstes zu ausländischen Staaten und zwischen- oder überstaatlichen Einrichtungen fundamental unterscheidet. Das vom Bundesverfassungsgericht begründete Privileg für Datenübermittlungen zum Zweck der politischen Unterrichtung lässt sich darum nicht auf Übermittlungen an ausländische Stellen übertragen. Zwar steht es der Bundesregierung selbst frei, die ihr durch den Bundesnachrichtendienst gelieferten Informationen im Rahmen internationaler politischer Kooperationen an ausländische Stellen weiterzugeben,

vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 226.

Hierbei handelt es sich jedoch um eine spezifische Befugnis der Regierung, die unmittelbar außenpolitisch agiert. Diese Befugnis erstreckt sich nicht auf den Bundesnachrichtendienst als Organ der Bundesverwaltung, das selbst nicht zur genuin politischen Kommunikation mit dem Ausland berufen ist. Eine Datenübermittlung durch den Bundesnachrichtendienst zum Zweck der politischen Unterrichtung einer ausländischen Stelle lässt sich daher nur dann rechtfertigen, wenn die Bundesregierung den Dienst zu der Übermittlung konkret anweist. Einen solchen Mechanismus, der den Bundesnachrichtendienst unmittelbar in die politische Kommunikation der Bundesregierung einbinden würde, sieht § 30 Abs. 1 BNDG nicht vor. Ansonsten ist der Dienst auf Datenübermittlungen im Rahmen der internationalen Verwaltungszusammenarbeit verwiesen. Hierfür sind die allgemeinen Anforderungen an Rechtsgüterschutz und Eingriffsschwellen einzuhalten, denen § 30 Abs. 1 BNDG nicht genügt.

Darüber hinaus ist § 30 Abs. 1 BNDG in sich unschlüssig formuliert, indem die Vorschrift einerseits Datenübermittlungen zum Zweck der Unterrichtung im Rahmen der internationalen politischen Zusammenarbeit vorsieht, andererseits tatsächliche Anhaltspunkte dafür fordert, dass die Übermittlung zur Erfüllung der Aufgaben des Bundesnachrichtendienstes erforderlich ist. Die politische Unterrichtung ausländischer beziehungsweise zwischen- oder überstaatlicher Stellen gehört nicht zu den Aufgaben des Bundesnachrichtendienstes, sodass Übermittlungszweck und Übermittlungsvoraussetzungen nicht zusammenpassen. Dies begründet Zweifel an der Bestimmtheit der Vorschrift, die dadurch zusätzlich genährt werden, dass es in der Gesetzesbegründung im Widerspruch zum Normwortlaut heißt, es müssten „tatsächliche Anhaltspunkte bestehen, dass [die Übermittlung] zur Unterrichtung im Rahmen der internationalen politischen Zusammenarbeit erforderlich ist“,

BT-Drs. 19/26103, S. 85.

Verfassungsrechtlich nicht tragfähig ist auch § 30 Abs. 2 BNDG, der Auslandsübermittlungen zu Strafverfolgungszwecken regelt. Zum einen verweist die Vorschrift zur Beschreibung der Straftaten auf einen wertenden Vergleich mit den in § 29 Abs. 3 BNDG genannten Straftaten. Jedoch wiegen die in § 29 Abs. 3 BNDG genannten Straftaten, wie oben ausgeführt, nicht durchweg schwer genug, um eine Datenübermittlung zu rechtfertigen. Dieses Defizit setzt sich in § 30 Abs. 2 BNDG fort. Zum anderen beschreibt die Norm die tatsächliche Übermittlungsschwelle unzureichend, indem sie – ebenfalls wie § 29 Abs. 3 BNDG – tatsächliche Anhaltspunkte ausreichen lässt,

vgl. oben C. I. 8. c).

Darüber hinaus genügen die Verfahrensregelungen für Auslandsübermittlungen nicht vollständig den verfassungsrechtlichen Anforderungen.

Unzureichend ist die Schutzregelung in § 30 Abs. 6 BNDG, mit der die besonderen Risiken von Auslandsübermittlungen abgeschirmt werden sollen. Eine Datenübermittlung ins Ausland bedarf als eigene Voraussetzung einer Rechtsstaatlichkeitsvergewisserung über den Umgang der ausländischen Stellen mit den ihnen übermittelten Daten. Diese Vergewisserung umfasst die Wahrung datenschutzrechtlicher Garantien und die Wahrung der Menschenrechte bei der Nutzung der Informationen. Sie ist in normenklaren Regelungen vorzusehen,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 233 ff.

Diese Anforderungen verfehlt § 30 Abs. 6 BNDG in zweifacher Hinsicht.

Erstens gibt die Norm nicht vor, dass sich der Bundesnachrichtendienst vor einer Datenübermittlung ins Ausland positiv – zumindest in generalisierender Weise – über das Schutzniveau im Ausland vergewissert. Eine Datenübermittlung ist vielmehr erst ausgeschlossen, wenn für den Bundesnachrichtendienst erkennbar wird, dass dieses Schutzniveau Defizite aufweist. Der Dienst darf also Daten grundsätzlich ins Ausland übermitteln, ohne sich über den rechtsstaatlichen Umgang mit den Daten überhaupt Gedanken zu machen. Er darf sich lediglich nicht blind für gegenläufige Anhaltspunkte stellen. Dies reicht nicht aus.

Zweitens bezieht sich § 30 Abs. 6 Satz 2 BNDG, der den Gegenstand der Rechtsstaatlichkeitsprüfung durch den Bundesnachrichtendienst beschreibt, allein auf Verletzungen von Menschenrechten oder elementaren rechtsstaatlichen Grundsätzen durch die Nutzung der übermittelten Daten. Eine Vergewisserung über das Datenschutzniveau im Ausland, also über die Vorgaben für die der Datennutzung vorgelagerten Verarbeitungsschritte sowie die Anforderungen an Datenschutzkontrolle und Datensicherheit,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 236,

sieht § 30 Abs. 6 BNDG nicht ausdrücklich vor. Lediglich in „Zweifelsfällen“, also wenn schon verdichtete Hinweise für Mängel bestehen, muss der Bundesnachrichtendienst nach § 30 Abs. 6 Satz 3 BNDG eine verbindliche Zusicherung zum Datenschutz „maßgeblich berücksichtigen“. Selbst in solchen Fällen ist mithin anscheinend ein hinreichendes Datenschutzniveau nicht zwingend erforderlich, da eine Übermittlung im Einzelfall trotz der bestehenden Zweifel auch ohne solche Zusicherung zulässig sein kann – die Zusicherung ist nur zu berücksichtigen, aber nicht zwingend zu fordern. Dem verfassungsrechtlichen Gebot, dass eine Auslandsübermittlung zwingend die Wahrung elementarer datenschutzrechtlicher Grundsätze voraussetzen muss, genügt diese Vorgabe nicht.

Mit dem Gebot der Normenklarheit nicht vollständig zu vereinbaren und inhaltlich defizitär ist schließlich § 30 Abs. 9 BNDG, der weitere Schutzvorkehrungen durch einen Verweis auf § 29 Abs. 8 und 13 bis 16 BNDG errichtet. Dieser Verweis ergibt jedoch teilweise keinen Sinn. Insbesondere enthalten § 29 Abs. 13 und Abs. 14 Satz 2 BNDG Pflichten des Übermittlungsempfängers. Diese Pflichten gehen mit Blick auf ausländische (öffentliche) Stellen, die der deutsche Gesetzgeber nicht verpflichten kann, ins Leere. In der Folge ist unklar, wie diese Verweise zu verstehen sind und ob sie überhaupt einen Gehalt haben. Stattdessen hätten besondere Regelungen für Auslandsübermittlungen geschaffen werden können und müssen, die etwa anstelle von Pflichten

des Übermittlungsempfängers Pflichten des Bundesnachrichtendienstes hätten vorsehen können, inhaltsgleiche Garantien von dem Übermittlungsempfänger zu verlangen.

9. Weiterverarbeitung von Daten aus einer Eignungsprüfung

Nach § 24 Abs. 1 BNDG darf der Bundesnachrichtendienst personenbezogene Daten aus Telekommunikationsnetzen erheben und auswerten, soweit dies zur Bestimmung geeigneter Telekommunikationsnetze oder geeigneter Suchbegriffe für strategische Aufklärungsmaßnahmen erforderlich ist. Eine solche Eignungsprüfung setzt, soweit sie geeignete Telekommunikationsnetze bestimmen soll, gemäß § 24 Abs. 2 BNDG tatsächliche Anhaltspunkte dafür voraus, dass in dem zu prüfenden Telekommunikationsnetz geeignete Daten für strategische Aufklärungsmaßnahmen übertragen werden. In diesem Fall ist die Eignungsprüfung auf sechs Monate zu befristen, wobei die Frist jedoch mehrfach um jeweils weitere sechs Monate verlängert werden kann.

Die Eignungsprüfung besteht in einer Vollerhebung der über ein bestimmtes Telekommunikationsnetz übermittelten Inhalts- und Metadaten. Insbesondere werden die erfassten Inhaltsdaten anders als bei der eigentlichen strategischen Fernmeldeaufklärung nicht sogleich durch einen Abgleich mit Suchbegriffen auf potenziell relevante Inhalte reduziert,

BT-Drs. 19/26103, S. 72.

Vor allem die Eignungsprüfung zur Generierung von Suchbegriffen geht potenziell außerordentlich weit. Mangels gesetzlicher Beschränkungen kann der Bundesnachrichtendienst zu diesem Zweck die aus dem betreffenden Telekommunikationsnetz gewonnenen Inhalts- und Metadaten unter Nutzung komplexer Analysetechnik auswerten und mit weiteren Datenbeständen verknüpfen. Hierzu können neben Daten aus der strategischen Ausland-Fernmeldeaufklärung auch etwa Ergebnisse der Analyse öffentlich zugänglicher Inhalte (Open Source Intelligence) oder Datenbestände gehören, die von Partnerdiensten oder Privaten zugeliefert wurden. Eine Bindung an ein bestimmtes Überwachungsprojekt oder ein in sonstiger Weise vorab zu konturierendes Erkenntnisziel besteht nicht.

Als Überwachungsmaßnahme wäre die Eignungsprüfung schon deshalb verfassungswidrig, weil die strategische Überwachung von Telekommunikationsinhalten zwingend suchbegriffsbasiert durchgeführt werden muss, um den Verhältnismäßigkeitsgrundsatz zu wahren,

vgl. zur verfassungsrechtlichen Bedeutung der suchbegriffsbasierten Datenerhebung BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 185 ff.; zur Verletzung des Wesensgehalts des Unionsgrundrechts auf Achtung des Privat- und Familienlebens (Art. 7 i.V.m. Art. 52 Abs. 1 Satz 1 GRCh) durch eine Ermächtigung zur generellen Erfassung von Telekommunikationsinhalten EuGH, Urteil vom 8. April 2014, Rs. C-293/12 und C-594/12 – Digital Rights Ireland u.a., Rn. 39; Urteil vom 6. Oktober 2015, Rs. C-362/14 – Schrems I, Rn. 94.

Auch die praktisch vollständige Freigabe der eingesetzten Analysemethoden und die Freistellung der Analyse von vorab zu definierenden Erkenntniszielen wäre im Rahmen einer Überwachungsmaßnahme nicht zu legitimieren.

Die Eignungsprüfung lässt sich daher nur wegen ihrer vorbereitenden Funktion rechtfertigen. Es handelt sich um ein Instrument nicht der Überwachung, sondern der Überwachungsplanung. Um eine Umgehung der verfassungsrechtlichen Überwachungsgrenzen zu verhindern, muss der Gesetzgeber im Gegenzug gewährleisten, dass der Bundesnachrichtendienst die im Rahmen der Eignungsprüfung gewonnenen Informationen nur für diesen Zweck nutzt. Zur eigentlichen Informationsbeschaffung darf die Eignungsprüfung nicht dienen und dürfen die dabei gewonnenen Daten auch im Wege der Zweckänderung nicht weiterverarbeitet werden. Ausnahmen hiervon können nur unter engen Voraussetzungen in besonderen Krisenlagen zugelassen werden.

Nach diesem Maßstab sind die Ermächtigungen zur Weiterverarbeitung von Daten aus einer Eignungsprüfung in § 24 Abs. 7 Satz 1 und 2 BNDG zu weit gefasst.

Gemäß § 24 Abs. 7 Satz 1 Nr. 1 BNDG darf der Bundesnachrichtendienst die im Rahmen einer Eignungsprüfung erhobenen personenbezogenen Daten weiterverarbeiten, wenn tatsächliche Anhaltspunkte auf eine erhebliche Gefahr für ein besonders wichtiges Rechtsgut aus einem abschließenden Katalog hindeuten. Das Gesetz definiert damit Schutzgüter und eine Weiterverarbeitungsschwelle, mit denen die Weiterverarbeitung auf eng umrissene Ausnahmefälle beschränkt wird. Insoweit lässt sich die Weiterverarbeitung auch nach einem strengen Maßstab legitimieren. Jedoch fehlt es an der erforderlichen Verknüpfung von Anlass und Ziel der Weiterverarbeitung, da § 24 Abs. 7 Satz 1 Nr. 1 BNDG die Weiterverarbeitung nicht daran bindet, dass sie gerade zur Abwehr der bestehenden Gefahr erforderlich sein muss. Die Norm ermöglicht damit Weiterverarbeitungen bei Gelegenheit einer Gefahr, um weiterge-

hende Erkenntnisziele aus dem Aufgabenbereich des Bundesnachrichtendienstes zu verfolgen. Die allgemeine Aufgabe zur Gewinnung von Erkenntnissen von außen- und sicherheitspolitischer Bedeutung kann jedoch die Weiterverarbeitung nicht rechtfertigen,

> vgl. zur Bedeutung der Verknüpfung von Eingriffsanlass und Eingriffsziel mit Blick auf Datenerhebungen BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 301, 311.

Darüber hinaus deckt der in § 24 Abs. 7 Satz 1 Nr. 1 BNDG enthaltene Begriff der Weiterverarbeitung neben Datenverarbeitungen durch den Bundesnachrichtendienst selbst auch eine Übermittlung der Daten an andere Stellen ab. Die Übermittlung von Daten, die durch eine Eignungsprüfung gewonnen wurden, bedarf jedoch angesichts ihrer besonderen Sensibilität einer gerichtsähnlichen Ex-ante-Kontrolle. Hingegen sieht das BNDG für Datenübermittlungen nach § 24 Abs. 7 Satz 1 Nr. 1 BNDG überhaupt keine obligatorische Kontrolle durch das gerichtsähnliche Kontrollorgan vor.

Noch grundlegenderen verfassungsrechtlichen Bedenken begegnet die Weiterverarbeitungsermächtigung in § 24 Abs. 7 Satz 1 Nr. 2 und Satz 2 BNDG. Danach darf der Bundesnachrichtendienst die im Rahmen einer Eignungsprüfung erhobenen personenbezogenen Daten an die Bundeswehr übermitteln, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies zum Schutz bestimmter Rechtsgüter erforderlich ist. Zulässig ist auch eine automatisierte Übermittlung.

Bereits der in § 24 Abs. 7 Satz 1 Nr. 2 BNDG enthaltene Übermittlungstatbestand ist zu weit gefasst, da er keine klare Übermittlungsschwelle benennt. Der weitgehend gleichlautende § 29 Abs. 5 Satz 1 Nr. 2 BNDG kann schon die reguläre Übermittlung von Daten, die der Bundesnachrichtendienst im Rahmen der strategischen Ausland-Fernmeldeaufklärung auf der Grundlage von Suchbegriffen erhoben hat, nicht rechtfertigen,

> siehe oben C. I. 8. e).

Erst recht ist die Übermittlungsermächtigung in § 24 Abs. 7 Satz 1 Nr. 2 BNDG defizitär, die sich auf exzeptionelle Fälle beschränken müsste.

Eine ausufernde Übermittlungspraxis ermöglicht darüber hinaus § 24 Abs. 7 Satz 2 BNDG, der automatisierte Übermittlungen zulässt. Wie die Gesetzesbegründung ausführt, soll diese Regelung als „Baustein der privilegierten Zusammenarbeit zwischen dem Bundesnachrichtendienst und der Bundeswehr“

dem Bundesnachrichtendienst eine en-bloc-Übermittlung von Inhalts- und Metadaten zu bestimmten geografischen Gebieten bzw. Regionen ermöglichen, ohne dass der Datenbestand zuvor durch Suchbegriffe reduziert wird. Hierzu verweist die Gesetzesbegründung vor allem auf den bei Bundeswehreinsätzen bestehenden Zeitdruck. Seinetwegen bestehe nicht immer die Möglichkeit, hinreichend bestimmte Suchbegriffe für die Aufklärung eines Sachverhaltes bzw. relevanter Personen zu benennen,

BT-Drs. 19/26103, S. 73 f.

Die automatisierte en-bloc-Übermittlung ändert die Rollenverteilung zwischen Bundesnachrichtendienst und Bundeswehr fundamental. Der Bundesnachrichtendienst ist im Rahmen von § 24 Abs. 7 Satz 2 BNDG in der Sache nicht mehr Überwachungsbehörde, sondern Datenlieferant der Bundeswehr, in deren Hand die gesamte Auswertung und Weiterverarbeitung der zugelieferten Daten liegt. Die Umgestaltung des institutionellen Rahmens der strategischen Telekommunikationsüberwachung reicht noch weiter als bei automatisierten Datenübermittlungen nach § 29 Abs. 5 Satz 2 BNDG, die eine Arbeitsteilung zwischen Bundesnachrichtendienst und Bundeswehr anlegen,

vgl. oben C. I. 8. e).

Hieran ändert es nichts, dass die automatisierte Übermittlung nur in den Fällen des § 24 Abs. 7 Satz 1 Nr. 2 BNDG, also zum Schutz bestimmter Rechtsgüter zulässig ist.

Zum einen umfasst der in dieser Norm enthaltene Katalog mit der Funktionsfähigkeit der Bundeswehr für die Landes- oder Bündnisverteidigung und bei Auslandseinsätze den Großteil des Auftrags der Bundeswehr,

siehe oben C. I. 8. e).

Zum anderen ist, wie sich gleichfalls aus der Gesetzesbegründung ergibt, die in § 24 Abs. 7 Satz 2 BNDG geregelte automatisierte Übermittlung darauf ausgerichtet, der Bundeswehr die Entscheidung darüber zu überlassen, welche der übermittelten Daten für die in § 24 Abs. 7 Satz 1 Nr. 2 BNDG genannten Schutzaufträge relevant sind. Der Bundesnachrichtendienst soll gerade keine Vorprüfung dieser Daten durchführen, sondern sie – jedenfalls soweit sie sich auf die von der Bundeswehr zu benennenden Zielgebiete beziehen – vollständig übermitteln.

Die Überwachung kann zudem über einen beträchtlichen Zeitraum andauern, da § 24 Abs. 2 Satz 2 BNDG für die Eignungsprüfung zur Bestimmung geeigneter Telekommunikationsnetze einen starren Zeitrahmen von sechs Monaten

vorsieht, der gemäß § 24 Abs. 2 Satz 3 BNDG mehrfach um jeweils weitere sechs Monate verlängert werden kann. Für die Eignungsprüfung zur Bestimmung geeigneter Suchbegriffe findet sich überhaupt keine zeitliche Beschränkung.

Insgesamt legt § 24 Abs. 7 Satz 2 BNDG damit eine äußerst weitreichende strategische Telekommunikationsüberwachung durch die Bundeswehr bei Gelegenheit einer Eignungsprüfung an. Zugleich wiegt der Überwachungseingriff durch die Bundeswehr angesichts ihrer besonders weitreichenden Befugnisse zur unmittelbaren Einwirkung auf die betroffenen Personen noch weitaus schwerer als bei Überwachungen durch den Bundesnachrichtendienst.

Nach den bisher vom Bundesverfassungsgericht entwickelten Maßstäben lässt sich eine Ermächtigung der Bundeswehr zu strategischen Telekommunikationsüberwachungen von vornherein nicht rechtfertigen, da wesentliches Element der Eingriffsrechtfertigung ist, dass der ansonsten zuständige Bundesnachrichtendienst nicht über operative Befugnisse verfügt. Bei der Bundeswehr ist das Gegenteil der Fall. Sie verfügt über die eingriffsintensivsten operativen Befugnisse aller deutschen hoheitlichen Stellen.

Selbst wenn man gleichwohl davon ausginge, dass die Bundeswehr auf Handlungsfeldern, die durch jederzeit drohende schwerwiegende Krisenlagen, hohen Zeitdruck und weitreichenden Informationsbedarf gekennzeichnet sind, gleichwohl zur strategischen Telekommunikationsüberwachung ermächtigt werden kann, müsste ihre Überwachungstätigkeit zumindest durch gehaltvolle gesetzliche Regelungen angeleitet und begrenzt werden. Solche Regelungen gibt es nicht. Die Übermittlungsermächtigung in § 24 Abs. 7 Satz 1 Nr. 2 und Satz 2 BNDG beruht vielmehr auf der von der Bundesregierung auch noch nach dem Urteil des Bundesverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung verfochtenen Prämisse, dass das sogenannte Militärische Nachrichtenwesen der Bundeswehr keiner gesetzlichen Regelung bedarf, sondern unmittelbar auf das Grundgesetz gestützt werden kann,

vgl. BT-Drs. 19/26114, S. 2 f.

Jedoch ist die militärische Aufklärung prinzipiell wie alle anderen hoheitlichen Informationsbeschaffungsvorgänge einer gesetzlichen Regulierung zugänglich, die inhaltlich auf die Spezifika dieses Tätigkeitsfeldes zugeschnitten werden kann. Die Begründung verfassungsunmittelbarer Eingriffsermächtigungen ist dem Grundgesetz hingegen fremd. Jedenfalls wenn sich andere, dem Gesetzesvorbehalt unterliegende Behörden wie der Bundesnachrichtendienst an der Aufklärungstätigkeit der Bundeswehr beteiligen sollen, müssen für diese

kooperative Aufklärung hinreichend gehaltvolle gesetzliche Grundlagen geschaffen werden. § 24 Abs. 7 Satz 2 BNDG legt insoweit hingegen eine nicht zu legitimierende Leerstelle an, indem der Bundesnachrichtendienst als Gehilfe in eine ansonsten vollständig ungeregelte Überwachungstätigkeit eingebunden wird, für die keine der Vorgaben – sei es auch in aufgabenadäquat modifizierter Form – zu beachten ist, die das Bundesverfassungsgericht für die strategische Überwachung der ausländischen Telekommunikation herausgearbeitet hat. Die Vorschrift läuft daher auf eine nicht hinnehmbare umfassende Umgehung der verfassungsrechtlichen Anforderungen an Ziele, Strukturierung, Durchführung und Kontrolle der Überwachung, an die Weiterverarbeitung der erhobenen Daten einschließlich ihrer Übermittlung an in- und ausländische Stellen sowie an Kooperationen mit ausländischen Stellen hinaus.

10. Kooperationen mit ausländischen Nachrichtendiensten

Der Gesetzgeber darf die strategische Telekommunikationsüberwachung für Kooperationen mit ausländischen Nachrichtendiensten öffnen. Grundrechtlichen Anforderungen können solche Regelungen jedoch nur dann genügen, wenn die rechtsstaatlichen Grenzen der strategischen Überwachung durch den gegenseitigen Austausch nicht überspielt werden und die Verantwortung des Bundesnachrichtendienstes für die von ihm erhobenen und ausgewerteten Daten im Kern gewahrt bleibt. Die Erkenntnisinteressen der ausländischen Kooperationspartner müssen mit einem legitimen Aufklärungsinteresse des Bundesnachrichtendienstes vergleichbar sowie mit den außen- und sicherheitspolitischen Interessen der Bundesrepublik vereinbar sein. Zudem muss die Datenverwendung in einen rechtsstaatlichen Rahmen eingebunden sein. Der grundrechtliche Schutz gegenüber heimlichen Überwachungsmaßnahmen und die diesbezüglichen Anforderungen an die Datenerhebung, -verarbeitung und -übermittlung dürfen nicht durch eine Kooperation unterlaufen werden,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 243 ff.

Nach diesem Maßstab genügen die in §§ 31 ff. BNDG enthaltenen Ermächtigungen zu Überwachungen und Datenübermittlungen im Rahmen nachrichtendienstlicher Kooperationen nicht vollständig den verfassungsrechtlichen Anforderungen.

a) Kooperationsziele

Der Gesetzgeber muss für nachrichtendienstliche Kooperationen die Zwecke, denen die Überwachung dienen darf, hinreichend präzise und normenklar fest-

legen und auf den Schutz hochrangiger Gemeinschaftsgüter beschränken. Insoweit gelten die Maßstäbe, die innerstaatlich für Überwachungen zur Gefahrenfrüherkennung zu beachten sind,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 253 mit Verweis auf Rn. 175 f.

Die in § 31 Abs. 3 und Abs. 5 BNDG enthaltenen Zweckvorgaben genügen dem nicht. Bereits das Verhältnis beider Absätze zueinander geht aus dem Normwortlaut nicht eindeutig hervor und wird auch durch die Gesetzesbegründung nicht geklärt. Im Sinne eines effektiven Grundrechtsschutzes liegt nahe, dass für jede Kooperation die Voraussetzungen beider Absätze kumulativ vorliegen müssen. Selbst unter dieser Prämisse verfehlen die gesetzlichen Zweckvorgaben jedoch die verfassungsrechtlichen Anforderungen.

Die in § 31 Abs. 3 BNDG genannten, allgemein gehaltenen Kooperationsziele grenzen die Kooperationsbefugnis des Bundesnachrichtendienstes kaum ein. Allein das in § 31 Abs. 3 Nr. 1 BNDG genannte Ziel der Früherkennung erheblicher Gefahren für die innere und äußere Sicherheit der Bundesrepublik Deutschland, die Verteidigung oder das Gemeinwohl hebt sich zumindest ansatzweise von dem allgemeinen Aufklärungsauftrag des Bundesnachrichtendienstes ab. Allerdings werden die zu erkennenden Gefahren nicht näher spezifiziert. Das in § 31 Abs. 3 Nr. 2 BNDG aufgeführte alternative Ziel der Wahrung der außen- und sicherheitspolitischen Handlungsfähigkeit der Bundesrepublik ist wenig konturiert und wird in der Gesetzesbegründung zu § 19 BNDG sehr weit gefasst, sodass es die Überwachungsziele kaum begrenzt,

> siehe oben C. I. 2. b).

Schließlich erlaubt § 31 Abs. 3 Nr. 3 BNDG Kooperationen, um die Aufgabenerfüllung durch den Bundesnachrichtendienst sicherzustellen, die ohne eine solche Kooperation wesentlich erschwert oder unmöglich wäre. Damit ist der gesamte Aufgabenbereich des Bundesnachrichtendienstes zulässiges Kooperationsziel, sodass § 31 Abs. 3 BNDG insgesamt das Spektrum der zulässigen Kooperationszwecke nicht begrenzt.

Auch die in § 31 Abs. 5 BNDG katalogartig aufgeführten Kooperationszwecke begrenzen den Anwendungsbereich der Kooperationsregelungen im Ergebnis nicht auf den Schutz hochrangiger Gemeinschaftsgüter. Zwar benennt diese Regelung einige bedeutsame Rechtsgüter, die für sich genommen den verfassungsrechtlichen Anforderungen entsprechen. Daneben enthält der Katalog jedoch auch Aufklärungsziele, die potenziell sehr weit reichen und die Kooperationsermächtigung entgrenzen lassen. Bemerkenswert ist dabei, dass § 31

Abs. 5 BNDG deutlich weiter gefasst ist als der für nicht-kooperative Überwachungen maßgebliche Katalog in § 19 Abs. 4 BNDG. Die Vorschrift verfehlt daher die verfassungsrechtlichen Anforderungen in noch erheblich größerem Ausmaß.

Zu offen ist die in § 31 Abs. 5 Nr. 5 BNDG geregelte Kooperationsbefugnis zur Gewinnung von Informationen über die Gefährdungs- und Sicherheitslage von deutschen und ausländischen Staatsangehörigen. Zwar kann auch der Schutz reiner Individualrechtsgüter in herausgehobenen Fällen ein solches Gewicht erlangen, dass er eine kooperative strategische Telekommunikationsüberwachung legitimieren kann. Die Kooperationsermächtigung beschränkt sich jedoch dem Wortlaut nach nicht auf solche Fälle, sondern umfasst Gefährdungen für beliebige Rechtsgüter. Ohne weitere Konkretisierungen ist dieses Schutzanliegen deutlich zu weit gefasst.

Ebenfalls zu weit reicht der Tatbestand in § 31 Abs. 5 Nr. 6 BNDG, der Kooperationen zur Gewinnung von Informationen über politische, wirtschaftliche oder militärische Vorgänge im Ausland von erheblicher außen- und sicherheitspolitischer Bedeutung erlaubt. Dieser Tatbestand hebt die Kooperationsbefugnis kaum aus dem Aufgabenspektrum des Bundesnachrichtendienstes heraus,

> vgl. zu dem Überwachungszweck, allgemein Erkenntnisse von außen- und sicherheitspolitischer Bedeutung zu gewinnen, in § 6 Abs. 1 Satz 1 Nr. 3 BNDG a.F. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 305.

Die Begrenzung auf „politische, wirtschaftliche oder militärische“ Vorgänge ist wenig bedeutsam, da sich nahezu alle aufklärungsbedürftigen Vorgänge unter eines dieser Attribute fassen lassen. Vorgänge aus dem Privatleben einzelner Ausländerinnen und Ausländer im Ausland unterfallen kaum je dem Aufklärungsauftrag des Bundesnachrichtendienstes. Von der allgemeinen Aufgabenbeschreibung des § 1 Abs. 2 BNDG unterscheidet sich § 31 Abs. 5 Nr. 6 BNDG daher im Wesentlichen nur durch das Erfordernis, dass es bei der Kooperation um Informationen von „erheblicher“ außen- und sicherheitspolitischer Bedeutung gehen muss. Diese Erheblichkeitsschwelle ist jedoch zu unspezifisch, um die Kooperationsbefugnis zuverlässig auf den Schutz hochrangiger Gemeinschaftsgüter zu beschränken.

Spezifischer, aber trotzdem zu weit gefasst ist § 31 Abs. 5 Nr. 8 BNDG, der Kooperationen zur Gewinnung von Informationen über die internationale Organisierte Kriminalität zulässt. Von Strukturen der Organisierten Kriminalität

können zwar Bedrohungen hochrangiger Gemeinschaftsgüter ausgehen. Angesichts der Weite dieses Begriffs ist dies aber nicht immer anzunehmen,

siehe oben C. I. 2. a).

Hieran ändert die Beschränkung der Kooperationsbefugnis auf die „internationale“ Organisierte Kriminalität nichts, da auch kleinere kriminelle Strukturen mit begrenztem Gefahrenpotenzial nicht nur vereinzelt grenzüberschreitend operieren.

Zu unscharf und zu offen ist auch § 31 Abs. 5 Nr. 9 BNDG formuliert, der Kooperationen zur Herstellung oder zum Erhalt wesentlicher Fähigkeiten des Bundesnachrichtendienstes oder des Kooperationspartners erlaubt. Aus dem Normwortlaut erschließt sich nicht, um welche Fähigkeiten es hierbei gehen und inwieweit eine kooperative Überwachung sie fördern soll. Soweit die Gesetzesbegründung auf einen Datenaustausch mit dem Ziel verweist, „technische Fähigkeiten des Bundesnachrichtendienstes und des Kooperationspartners im Zusammenhang mit der Fernmeldeaufklärung fortzuentwickeln und an die sich ständig ändernden technischen Rahmenbedingungen der Fernmeldeaufklärung in Zeiten der modernen Digitalisierung anzupassen“,

BT-Drs. 19/26103, S. 90,

benennt sie einen Zweck, der nicht unmittelbar auf den Schutz von Gemeinschaftsgütern bezogen ist, sondern die Instandhaltung des nachrichtendienstlichen Überwachungsinstrumentariums betrifft. Dieses Anliegen kann zwar prinzipiell Datenerhebungen rechtfertigen, erfordert aber im Gegenzug, dass die Weiterverarbeitung der erhobenen Daten streng auf den überwachungstechnischen Erhebungszweck begrenzt wird, damit das grundsätzliche Erfordernis eines qualifizierten Schutzguts für strategische Telekommunikationsüberwachungen zur Gefahrenfrüherkennung nicht umgangen werden kann. Eine derartige Zweckbindung sieht – mit allerdings zu weitreichenden Ausnahmen – der für Eignungsprüfungen maßgebliche § 24 Abs. 5 Satz 1 BNDG vor. Zu § 31 Abs. 5 Nr. 9 BNDG bedarf es einer vergleichbaren Vorgabe, die das Gesetz nicht enthält.

Viel zu weit gefasst ist schließlich § 31 Abs. 5 Nr. 11 BNDG, der eine kooperative Überwachung zur Informationsgewinnung in „vergleichbaren Fällen“ ermöglicht. Ein derartiger Auffangtatbestand verfehlt schon allgemein die Aufgabe des Gesetzgebers, die zulässigen Überwachungszwecke präzise und normenklar festzulegen,

vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 253.

Zudem ist der von dieser Norm angeordnete Vergleich gerade für die disparaten Katalogtatbestände des § 31 Abs. 5 BNDG, die unterschiedlich deutlich konturierte Gefahrenbereiche unterschiedlichen Gewichts umfassen, kaum zu leisten. In diesem Regelungskontext läuft § 31 Abs. 5 Nr. 11 BNDG auf eine normativ nicht näher angeleitete Angemessenheitsprüfung hinaus, die dem Bundesnachrichtendienst eine weitreichende Dispositionsbefugnis über mögliche Kooperationszwecke vermittelt.

b) Betroffene Personen

Soweit die Kooperationsregelungen Vorgaben zu den betroffenen Personen enthalten, stimmen sie mit den Ermächtigungen zur strategischen Ausland-Fernmeldeaufklärung überein. Sie teilen darum die Defizite dieser Ermächtigungen: Der Schutz von Inländerinnen und Inländern gemäß § 31 Abs. 1 Satz 2 BNDG erstreckt sich nicht auf Inländerinnen und Inländer mit ausländischer Staatsangehörigkeit, soweit sich diese temporär im Ausland aufhalten. Unionsbürgerinnen und Unionsbürger werden durch § 32 Abs. 1 Satz 3 i.V.m. § 20 Abs. 1 BNDG nur begrenzt vor einer Verarbeitung selektierter personenbezogener Daten geschützt. Hinsichtlich der gesamthaften Übermittlung unselektierter Verkehrsdaten nach § 33 BNDG sind sie – gleichläufig zu der gesamthaft bevorratenden Verkehrsdatenspeicherung durch den Bundesnachrichtendienst nach § 26 BNDG – den Staatsangehörigen von Drittstaaten gleichgestellt. Juristische Personen aus anderen Mitgliedstaaten der Europäischen Union genießen insgesamt keinen besonderen Überwachungsschutz,

> vgl. oben C. I. 3.

Ein spezifisches Defizit der Kooperationsregelungen besteht schließlich darin, dass sie keine Vorkehrungen zum Schutz besonders gefährdeter Personen enthalten. Solche Vorkehrungen sind verfassungsrechtlich geboten, um der besonderen Schutzbedürftigkeit etwa von Dissidenten oder sogenannten Whistleblowern Rechnung zu tragen,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 256, 258, 264.

Dieser verfassungsrechtliche Schutzauftrag hat bei strategischen Telekommunikationsüberwachungen, die der Bundesnachrichtendienst allein durchführt, kein unmittelbares Gegenstück, da der Schutz der betroffenen Personengruppen im Inland durch die allgemeinen rechtsstaatlichen Grundsätze gewährleistet wird, denen alle hoheitlichen Stellen der Bundesrepublik unterliegen. Der Schutz besonders gefährdeter Personen trägt dem Umstand Rechnung, dass der Bundesnachrichtendienst Kooperationen auch mit Nachrichtendiensten

aus Staaten eingehen kann, in denen – ungeachtet der stets erforderlichen Rechtsstaatlichkeitsvergewisserung – eine Nutzung der erlangten Daten zur Verfolgung solcher Personen nicht so zuverlässig ausgeschlossen werden kann wie im Inland.

Die Regelungen über Kooperationen setzen diesen Schutzauftrag nicht um. Sie erhalten lediglich in § 32 Abs. 1 Satz 3, Abs. 3 Nr. 2 lit. b, Abs. 4 Nr. 3, Abs. 5 Satz 1 i.V.m. § 21 BNDG und in § 33 Abs. 1 Satz 2 i.V.m. § 32 Abs. 4 Nr. 3 und Abs. 5 Satz 1 sowie § 21 BNDG Vorkehrungen zum Schutz von Vertraulichkeitsbeziehungen. Der auch im Inland gebotene Schutz von Vertraulichkeitsbeziehungen ist jedoch mit dem Schutz besonders gefährdeter Personen nicht identisch und kann ihn nicht ersetzen.

II. Online-Durchsuchung

Die neu geschaffenen Regelungen zu Online-Durchsuchungen im Ausland verletzen das aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG herzuleitende Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Dieses Grundrecht schützt auch Ausländerinnen und Ausländer im Ausland. Die Ausführungen des Bundesverfassungsgerichts zur territorialen Reichweite des Fernmeldegeheimnisses in seiner abwehrrechtlichen Dimension,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 87 ff.

lassen sich auf andere Grundrechte, die Einzelne gegen staatliche Überwachungsmaßnahmen schützen, ohne weiteres übertragen.

Online-Durchsuchungen sind am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu messen. Dies gilt auch insoweit, als § 34 Abs. 1 Satz 1 BNDG als erhebungsfähige Daten Inhalte und Umstände einer laufenden Kommunikation benennt. Die gesetzlich geregelte Maßnahme beschränkt sich nicht auf eine an Art. 10 GG zu messende Quellen-Telekommunikationsüberwachung, sondern kann sich auf alle verarbeiteten Daten erstrecken. Der Eingriff wiegt schwer und muss darum von strengen materiellen und prozeduralen Vorgaben abhängig gemacht werden,

> vgl. BVerfGE 120, 274 (326 ff.); BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 176, 289 f.

Die Regelungen in §§ 34 ff. BNDG leisten dies nicht. Sie binden Online-Durchsuchungen nicht an hinreichende tatbestandliche Voraussetzungen (unten 1), begrenzen den Kreis der betroffenen Personen nicht restriktiv genug (unten 2),

enthalten teils unzureichende Vorgaben zum Schutz des Kernbereichs privater Lebensgestaltung (unten 3) und erlauben die Übermittlung der durch Online-Durchsuchungen erlangten Daten an andere in- und ausländische Stellen in zu weitem Umfang (unten 4).

1. Voraussetzungen

Das Bundesverfassungsgericht hatte bisher nicht zu entscheiden, welchen verfassungsrechtlichen Anforderungen gesetzliche Ermächtigungen zu Online-Durchsuchungen gegenüber Ausländerinnen und Ausländern im Ausland zum Zweck der Auslandsaufklärung genügen müssen. Der jüngeren Rechtsprechung lassen sich aber wesentliche Leitlinien entnehmen, um diese Anforderungen zu konkretisieren.

Aus dem Urteil zur Ausland-Ausland-Fernmeldeaufklärung geht hervor, dass die spezifischen verfassungsrechtlichen Maßstäbe für strategische Telekommunikationsüberwachungen sich nicht auf Maßnahmen der Auslandsaufklärung übertragen lassen, die gezielt gegen bestimmte Personen durchgeführt werden. Insbesondere kann hinsichtlich solcher Maßnahmen auch dann, wenn sie sich gegen Personen im Ausland richten, nicht auf eine konkretisierende Eingriffsschwelle als Kernelement rechtsstaatlicher Anforderungen verzichtet werden, die gerade für schwerwiegende Grundrechtseingriffe wie eine Online-Durchsuchung unverzichtbar ist,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 155 f.

Denn die verfassungsrechtliche Legitimation der strategischen Telekommunikationsüberwachung als im Wesentlichen nur final angeleiteter Maßnahme ergibt sich gerade auch daraus, dass sie typischerweise weniger zielgenau operiert als eine gegen bestimmte Personen gerichtete Überwachungsmaßnahme,

vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 148.

Dementsprechend darf eine anlasslose Telekommunikationsüberwachung nicht mit annähernd vergleichbarer Sicherheit und Wirkung wie eine Einzelanordnung zu einer individualisierenden Überwachung des Telekommunikationsverkehrs führen. Eine individualisierende Überwachung muss vielmehr den allgemeinen Anforderungen genügen, zu denen eine hinreichende tatsächliche Eingriffsschwelle gehört,

BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 189.

Eine Online-Durchsuchung erschließt gezielt Datenbestand und Nutzung eines konkreten informationstechnischen Systems, das einer bestimmten Person zugeordnet sein kann. In einem solchen Fall handelt es sich um eine Maßnahme, die tiefgreifende Aussagen über Eigenschaften, Verhalten und soziale Einbindungen der betroffenen Person ermöglicht. Die Online-Durchsuchung weist darum eine besonders hohe Eingriffsintensität auf, die über eine individualisierende Telekommunikationsüberwachung – die ohnehin vielfach Teil der Online-Durchsuchung sein wird – sogar noch hinausgeht,

> BVerfGE 120, 274 (322 ff.); BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 166.

Dementsprechend hat das Bundesverfassungsgericht in seinem Urteil zum Bayerischen Verfassungsschutzgesetz (erneut) festgehalten, dass eine Ermächtigung zu Online-Durchsuchungen im Verfassungsschutzrecht denselben Anforderungen genügen muss wie eine präventivpolizeiliche Ermächtigung. Der Umstand, dass die Verfassungsschutzbehörden nicht über operative Befugnisse verfügen, wirkt sich angesichts der besonderen Eingriffsschwere der Maßnahme nicht auf die verfassungsrechtlichen Maßstäbe für die Eingriffsvoraussetzungen aus. Online-Durchsuchungen müssen darum auch im Verfassungsschutzrecht von einer mindestens konkretisierten Gefahr abhängig gemacht werden. Zudem dürfen Verfassungsschutzbehörden zu Online-Durchsuchungen nur subsidiär für den Fall ermächtigt werden, dass geeignete polizeiliche Hilfe für das bedrohte Rechtsgut nicht rechtzeitig erlangt werden kann,

> BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 168, 176, 178.

Es liegt nahe, dass sich diese Anforderungen auf Online-Durchsuchungen zur Auslandsaufklärung nur mit Modifikationen übertragen lassen. Insbesondere das Subsidiaritätserfordernis ergibt für Online-Durchsuchungen, die sich gegen Personen im Ausland richten, wenig Sinn, da deutsche Polizeibehörden im Ausland grundsätzlich nicht hoheitlich tätig werden können. Ob daneben auch die Anforderungen an die tatsächliche Eingriffsschwelle an die besonderen Bedürfnisse der Auslandsaufklärung anzupassen sind, erscheint dagegen fragwürdig. Grundsätzlich kann der Bundesnachrichtendienst auch mit Blick auf Sachverhalte im Ausland beurteilen, ob eine hinreichend konkretisierte Gefahr für ein besonders bedeutsames Rechtsgut als Anlass einer Online-Durchsuchung erkennbar ist. Darüber hinaus unterscheiden sich die unmittelbaren Wirkungen einer Online-Durchsuchung im Ausland nicht von inlandsbezoge-

nen Maßnahmen. Die Online-Durchsuchung erschließt in jedem Fall die gesamte Nutzung des Zielsystems und alle darauf gespeicherten Daten, ohne dass es auf den Standort des Systems ankäme. Das Argument, dass Maßnahmen der Auslandsaufklärung notwendig fragmentarisch bleiben und darum unter niedrigeren Voraussetzungen zugelassen werden können, lässt sich auf Online-Durchsuchungen daher nicht übertragen.

Zumindest müsste eine alternative Überwachungsschwelle für die Auslandsaufklärung eine auf bestimmten Tatsachen beruhende Bedrohungslage beschreiben, die sich wenigstens insoweit konkretisieren lässt, als dies zur Bestimmung von Zielperson(en) und Zielsystem der Überwachung erforderlich ist. Eine nur final auf die Frühaufklärung bestimmter Bedrohungen programmierte Eingriffsermächtigung kann Online-Durchsuchungen auch als Maßnahmen der Auslandsaufklärung hingegen nicht legitimieren.

Hieran ändert es nichts, dass Online-Durchsuchungen des Bundesnachrichtendienstes vielfach nicht darauf ausgerichtet sein mögen, vertiefte Erkenntnisse über einzelne Personen zu gewinnen. Es mag zutreffen, dass der Bundesnachrichtendienst typischerweise dienstlich genutzte informationstechnische Systeme oder informationstechnische Infrastruktur infiltriert,

> so die Gesetzesbegründung, BT-Drs. 19/26103, S. 94.

Die gesetzliche Ermächtigung beschränkt den Bundesnachrichtendienst jedoch nicht auf Erkenntnisziele, die im Vergleich mit anderen sicherheitsbehördlichen Online-Durchsuchungen ein geringeres Eingriffsgewicht aufweisen mögen. Ein Infrastrukturzugriff mit dem Ziel, eine strategische Telekommunikationsüberwachung zu ermöglichen, wird bereits durch § 19 Abs. 6 BNDG ermöglicht, sodass es einer besonderen Ermächtigung zu Online-Durchsuchungen insoweit nicht bedarf. Auch dienstlich genutzte Systeme können zudem eine Vielzahl persönlicher Daten enthalten, die weitreichende Rückschlüsse auf die Person zulassen. Schließlich räumt die Gesetzesbegründung selbst ein, dass in bestimmten Fällen sehr wohl auch eine gezielte Erkenntnisgewinnung über Einzelpersonen Ziel der Maßnahme sein kann,

> vgl. BT-Drs. 19/26103, S. 95.

Nach dem mithin anzulegenden Maßstab für individualisierende Überwachungsmaßnahmen von höchster Eingriffsintensität verfehlen die Überwachungsermächtigungen in § 34 BNDG die verfassungsrechtlichen Anforderungen weit.

§ 34 Abs. 1 Satz 1 BNDG unterscheidet gleichläufig zur strategischen Ausland-Fernmeldeaufklärung zwischen Aufklärungsmaßnahmen zur politischen Unterrichtung der Bundesregierung und zur Früherkennung von aus dem Ausland drohenden Gefahren. Auch wenn davon ausgegangen wird, dass sich diese für strategische Überwachungen begründete Differenzierung auf individualisierende Überwachungsmaßnahmen wie die Online-Durchsuchung übertragen lässt, errichtet das Gesetz für beide Überwachungskategorien keine hinreichenden Eingriffsvoraussetzungen.

Nach § 34 Abs. 2 BNDG ist eine Aufklärungsmaßnahme zur politischen Unterrichtung der Bundesregierung zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass sie der Gewinnung von Informationen dient, mit deren Aufklärung das Bundeskanzleramt den Bundesnachrichtendienst beauftragt hat und die von herausgehobener außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind. Diese Norm ist weitgehend wortlautidentisch mit § 19 Abs. 2 BNDG. Das in § 19 Abs. 2 BNDG nicht enthaltene Erfordernis „tatsächlicher Anhaltspunkte“ ändert hieran schon deshalb nichts, weil sein Bezugspunkt unklar ist. Nach dem Normwortlaut müssen die tatsächlichen Anhaltspunkte auf das Ziel der Maßnahme („…dass sie der Gewinnung von Informationen dient…“) hindeuten, obwohl der Bundesnachrichtendienst dieses Ziel sicher kennt. Selbst wenn die tatsächlichen Anhaltspunkte – im Sinne einer verständigen, wenngleich sprachlich fragwürdigen Interpretation – auf die zu gewinnenden Informationen bezogen werden, lässt sich § 34 Abs. 2 BNDG nicht entnehmen, dass eine auch nur ansatzweise konturierte konkrete Bedrohungslage vorliegen muss, an die der Überwachungseingriff anknüpft und durch die er sachlich und zeitlich begrenzt wird. Als inhaltlicher Unterschied zwischen § 34 Abs. 2 BNDG und § 19 Abs. 3 BNDG verbleibt, dass die individuelle Aufklärungsmaßnahme nach § 34 Abs. 2 BNDG auf Informationen von „herausgehobener“ außen- und sicherheitspolitischer Bedeutung gerichtet sein muss. Abgesehen davon, dass das Gesetz die Kriterien, nach denen sich die gesteigerte Bedeutung bemisst, nicht konkretisiert, ändert dieses Erfordernis nichts daran, dass eine tatsächliche Eingriffsschwelle nicht gefordert wird.

Nach § 34 Abs. 3 BNDG ist eine Aufklärungsmaßnahme zur Gefahrenfrüherkennung zulässig, wenn Tatsachen die Annahme rechtfertigen, dass sie der Gewinnung von Informationen dient, mit deren Aufklärung das Bundeskanzleramt den Bundesnachrichtendienst beauftragt hat, und durch sie Erkenntnisse über Gefahren nach § 19 Abs. 4 BNDG in Fällen von herausgehobener außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland gewonnen werden.

Die durch § 34 Abs. 3 BNDG in Bezug genommenen Gefahrenbereiche des § 19 Abs. 4 BNDG wiegen nicht durchweg schwer genug, um eine Überwachungsmaßnahme höchster Eingriffsintensität wie die Online-Durchsuchung zu legitimieren. Insbesondere gilt dies für den sehr weiten Begriff der Organisierten Kriminalität, der ohne präzisierende Tatbestandsmerkmale neben schwerwiegenden Bedrohungen auch Erscheinungsformen der Alltagskriminalität erfasst, sowie für das kaum handhabbare Schutzgut der außenpolitischen Handlungsfähigkeit der Bundesregierung,

näher oben C. I. 2.

Die Beschränkung der Überwachungsbefugnis auf Fälle von herausgehobener Bedeutung ist zu unscharf formuliert, um dieses Defizit auszugleichen. Sie setzt nicht ausdrücklich voraus und gewährleistet nicht zuverlässig, dass die Überwachung auf den Schutz besonders gewichtiger Rechtsgüter beschränkt bleibt.

Hinsichtlich der Eingriffsschwelle stimmt § 34 Abs. 3 BNDG im Ergebnis mit dem in Bezug genommenen § 19 Abs. 4 BNDG überein. Das gegenüber § 19 Abs. 4 BNDG hinzugetretene Erfordernis von „Tatsachen“ hat wie in § 34 Abs. 2 BNDG einen unklaren Bezugspunkt und stellt jedenfalls nicht klar, dass eine Bedrohungslage im Einzelfall vorliegen muss. Das weitere Erfordernis eines Falls von herausgehobener Bedeutung bezieht sich wiederum nicht auf die tatsächliche Eingriffsschwelle.

Aufgrund der weitgehenden Übereinstimmung von § 34 Abs. 2 und 3 BNDG mit § 19 Abs. 3 und Abs. 4 BNDG, die hinsichtlich der Eingriffsschwelle nicht durch handhabbare zusätzliche Erfordernisse relativiert wird, liegt insgesamt nahe, dass der tatsächliche Eingriffsanlass bei beiden Normen identisch ist. Auch die Online-Durchsuchung im Ausland wird damit im Gesetz wie die strategische Ausland-Fernmeldeaufklärung als im Wesentlichen nur final programmierte Überwachungsmaßnahme konzipiert, die keinen konturierten tatsächlichen Anlass im Einzelfall voraussetzt. Die Gesetzesbegründung bestätigt diesen Eindruck, indem sie – abweichend vom Normwortlaut – darauf abhebt, dass die tatsächlichen Anhaltspunkte beziehungsweise Tatsachen auf die zu gewinnenden Erkenntnisse hindeuten müssen,

BT-Drs. 19/26103, S. 96.

Die tatsachengestützte Erwartung, dass eine Überwachungsmaßnahme bestimmte aufgabenrelevante Erkenntnisse erbringen kann, ist nicht identisch mit der tatsachengestützten Feststellung einer zumindest ansatzweise kontu-

rierten Bedrohungslage. Eine derartige Erkenntnisprognose lässt sich vielmehr schon dann abgeben, wenn überhaupt damit zu rechnen ist, dass von bestimmten Personen oder Gruppierungen irgendwann einmal Bedrohungen ausgehen könnten und dass bestimmte Informationen einmal nützlich sein könnten, um diese Bedrohungen aufzuklären.

An dem Befund, dass die Tatbestände von § 34 Abs. 2 und Abs. 3 BNDG keine zureichende tatsächliche Eingriffsschwelle beschreiben, ändert es nichts, dass § 34 Abs. 5 BNDG für Aufklärungsmaßnahmen zur Gefahrenfrüherkennung bestimmte Anforderungen an die Zielpersonen der Maßnahme errichtet. Diese Vorschrift ist teils wortlautidentisch mit der Regelung über gezielte personenbezogene Überwachungen in § 20 Abs. 2 Nr. 1 BNDG. § 20 Abs. 2 Nr. 1 BNDG steht wiederum im Kontext der strategischen Ausland-Fernmeldeaufklärung, setzt also gerade keinen besonderen tatsächlichen Eingriffsanlass voraus. Diese Norm setzt lediglich die Forderung des Bundesverfassungsgerichts um, Sonderregelungen für zielgerichtete Überwachungen gegen mögliche Verursacher von Gefahren, Nachrichtenmittler oder sonst näher qualifizierte Informanten zu schaffen, ohne dass es einer objektivierten Eingriffsschwelle bedürfte,

vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 187.

Zudem gelten die Anforderungen des § 34 Abs. 5 BNDG nicht für Aufklärungsmaßnahmen zur politischen Unterrichtung der Bundesregierung. Eine solche Maßnahme darf sich gegen jede Person richten, bei der Erkenntnisse erhofft werden, ohne dass es einer Qualifikation als Informantin bedarf,

so auch die Gesetzesbegründung, BT-Drs. 19/26103, S. 96.

Schließlich ändert die Subsidiaritätsregelung in § 34 Abs. 1 Satz 2 BNDG nichts an dem Fehlen einer tragfähigen tatsächlichen Eingriffsschwelle. Diese Regelung setzt die Online-Durchsuchung in Bezug zu anderen möglichen und potenziell erfolgversprechenden Überwachungsmaßnahmen und verlangt eine besondere Dringlichkeit. Über die tatbestandlichen Voraussetzungen der Maßnahme sagt sie hingegen nichts aus.

2. Betroffene

Die in § 34 Abs. 5 und 6 BNDG enthaltenen Vorgaben zu den Betroffenen einer Online-Durchsuchung verfehlen ebenfalls in erheblichem Ausmaß die verfassungsrechtlichen Anforderungen.

Dies gilt zum einen für die Regelung über die zulässigen Zielpersonen einer Überwachung in § 34 Abs. 5 BNDG.

Diese Regelung gilt nur für Aufklärungsmaßnahmen zur Gefahrenfrüherkennung. Für Maßnahmen zur politischen Unterrichtung der Bundesregierung fehlt es hingegen vollständig an einer Betroffenenregelung. Solche Maßnahmen können daher gegen beliebige Personen gerichtet werden, soweit es Anhaltspunkte dafür gibt, dass sich aus deren informationstechnischem System aufgabenrelevante Erkenntnisse gewinnen lassen. Für eine individualisierende Überwachungsmaßnahme von höchster Eingriffsintensität wie die Online-Durchsuchung greift dies zu kurz. Dies gilt selbst dann, wenn in Fortschreibung des Urteils zur Ausland-Ausland-Fernmeldeaufklärung angenommen wird, dass auch eine individualisierende Überwachungsmaßnahme zum Zweck der politischen Unterrichtung für die betroffene Person grundsätzlich weniger schwer wiegt und darum unter abgesenkten Anforderungen zugelassen werden kann. Denn die spezifische Eingriffsintensität der Online-Durchsuchung ergibt sich, wie oben ausgeführt, in erster Linie nicht aus den möglichen Folgen der Maßnahme, sondern aus dem besonders weitreichenden Eindringen in den persönlichen Bereich. Darum bedarf es in jedem Fall einer einschränkenden Betroffenenregelung, die diese Maßnahme für die betroffene Person zumutbar macht.

Nach § 34 Abs. 5 Nr. 1 BNDG darf sich eine Online-Durchsuchung zur Gefahrenfrüherkennung gegen Personen richten, hinsichtlich derer tatsächliche Anhaltspunkte dafür vorliegen, dass sie Verursacher von Gefahren im Sinne des § 19 Abs. 4 BNDG sind. Diese Voraussetzung wäre dann nicht zu beanstanden, wenn sie so zu verstehen wäre, dass von der betroffenen Person eine hinreichend konkretisierte Gefahr im präventivpolizeilichen Sinne ausgehen muss. Diese Interpretation widerspräche aber dem erkennbaren Anliegen des Gesetzes, die Online-Durchsuchung unabhängig von einer konturierten Bedrohungslage zur Gefahrenfrüherkennung zu ermöglichen. Indem das Gesetz gerade keine besondere tatsächliche Eingriffsschwelle voraussetzt, verliert auch das Erfordernis der Gefahrverursachung gegenüber der polizeirechtlichen Begriffsbildung an Konturen. § 34 Abs. 5 Nr. 1 BNDG teilt insoweit das verfassungsrechtliche Defizit von § 34 Abs. 3 BNDG.

Einen eigenständigen Mangel weist demgegenüber § 34 Abs. 5 Nr. 2 BNDG auf. Diese Norm ermöglicht Online-Durchsuchungen gegen Informationsmittler und Systeminhaber, hinsichtlich derer keine Anhaltspunkte für eine Gefahrverursachung bestehen müssen. Selbst wenn die Gefahrverursachung im präventivpolizeilichen Sinne zu verstehen wäre, ginge diese Ermächtigung zu weit. Wegen der besonderen Eingriffsintensität von Online-Durchsuchungen

darf diese Maßnahme nur gegenüber Zielpersonen zugelassen werden, die für die drohende Gefahr verantwortlich sind,

BVerfGE 141, 220 (273 f.).

Selbst wenn für die Auslandsaufklärung Online-Durchsuchungen, die sich gezielt gegen Informationsmittler und Systeminhaber richten, verfassungsrechtlich überhaupt akzeptabel wären, dürften sie zumindest nur subsidiär zu einer Maßnahme gegen den Gefahrverursacher zugelassen werden. Eine derartige Subsidiaritätsregelung fehlt in § 34 Abs. 5 BNDG.

Für sich genommen nicht zu beanstanden ist hingegen, dass nach § 34 Abs. 6 Satz 1 und 2 BNDG eine Online-Durchsuchung auch durchgeführt werden darf, wenn andere Personen oder Informationssysteme unvermeidbar mitbetroffen werden. Würde die Online-Durchsuchung lediglich unter den strengen Voraussetzungen zugelassen, die für präventivpolizeiliche Maßnahmen gelten, so dürfte es sich hierbei um beliebige Dritte handeln, da dann dieselben Maßstäbe wie für innerstaatliche Überwachungen gälten. Soll hingegen an der Regelungsentscheidung des Gesetzgebers festgehalten werden, die Eingriffsvoraussetzungen für Online-Durchsuchungen zur Auslandsaufklärung abzusenken, so liegt nahe, parallel zu den Anforderungen an strategische Telekommunikationsüberwachungen zwischen unterschiedlichen Kategorien von Drittbetroffenen zu differenzieren: Eine derartige Online-Durchsuchung müsste als Instrument der reinen Auslandsaufklärung ausgestaltet werden. Datenerhebungen über Inländerinnen und Inländer sowie richtigerweise auch über Unionsbürgerinnen und Unionsbürger und juristische Personen aus anderen Mitgliedstaaten der Europäischen Union müssten nach Möglichkeit vermieden werden. Gleichwohl erhobene Daten über diese Personenkreise dürften grundsätzlich nicht weiterverarbeitet werden.

Dementsprechend verweist § 34 Abs. 6 Satz 3 BNDG auf die Schutzregelung für Inländerinnen und Inländer in § 19 Abs. 7 BNDG. Diese Schutzregelung greift jedoch zu kurz und erfasst nicht alle zu schützenden Personen, wie bereits zur strategischen Ausland-Fernmeldeaufklärung ausgeführt wurde,

siehe oben C. I. 3. a).

Darüber hinaus fehlt es vollständig an einer Schutzregelung für Unionsbürgerinnen und Unionsbürger sowie für juristische Personen aus anderen Mitgliedstaaten der Europäischen Union. Eine solche Schutzregelung ist jedoch nach dem Gleichheitssatz des Art. 3 Abs. 1 GG, der durch Art. 21 GRCh verstärkt wird, geboten. Auch die gesetzliche Ermächtigung zu Online-Durchsuchungen

durch den Bundesnachrichtendienst ist an den Unionsgrundrechten zu messen,

vgl. oben C. I. 3. b) aa) (1) und (3).

Die Aufklärungstätigkeit des Bundesnachrichtendienstes unterfällt zum einen partiell – soweit sie nicht dem Schutz der nationalen Sicherheit nach dem engen unionsrechtlichen Begriffsverständnis dient – dem europäischen Datenschutzrecht. Zum anderen können Online-Durchsuchungen durch den Bundesnachrichtendienst und die damit verbundenen Risiken für die Vertraulichkeit und Integrität informationstechnischer Systeme die Ausübung der unionsrechtlichen Grundfreiheiten beeinträchtigen. Dies gilt umso mehr, als eine denkbare Bevorratung von Sicherheitslücken durch den Bundesnachrichtendienst zur Ermöglichung von Online-Durchsuchungen neben den potenziell betroffenen Personen auch das kollektive Interesse an einem möglichst hohen Standard der Informationssicherheit bedroht,

vgl. zu dem damit verbundenen Zielkonflikt BVerfG, Beschluss vom 8. Juni 2021 – 1 BvR 2771/18 –, Rn. 34 ff.

Diese Bedrohungslage ist nicht auf die Bundesrepublik beschränkt, sondern gefährdet angesichts der Bedeutung einer sicheren Informationstechnik für nahezu alle wirtschaftlichen Transaktionen auch den grenzüberschreitenden Verkehr von Personen, Waren, Dienstleistungen und Kapital in der Europäischen Union.

Es wird angeregt, gegebenenfalls die unionsgrundrechtlichen Anforderungen an den Schutz von Unionsbürgerinnen und Unionsbürgern sowie von juristischen Personen des EU-ausländischen Rechts gegen Online-Durchsuchungen zur Auslandsaufklärung durch ein Vorabentscheidungsverfahren vor dem Gerichtshof der Europäischen Union zu klären.

3. Kernbereichsschutz

Die verfassungsrechtlichen Anforderungen an den Schutz des Kernbereichs privater Lebensgestaltung im Zusammenhang mit Online-Durchsuchungen sind in der Rechtsprechung des Bundesverfassungsgerichts geklärt. Sie wurden zuletzt im Urteil zum Bayerischen Verfassungsschutzgesetz konsolidiert. Es gibt – anders als möglicherweise bei den Eingriffsvoraussetzungen – keinen Grund, diese Anforderungen für Online-Durchsuchungen des Bundesnachrichtendienstes zurückzunehmen. Der aus der Menschenwürdegarantie folgende Kernbereichsschutz ist einer Differenzierung des Schutzniveaus zwi-

schen Inländerinnen und Inländern einerseits, Ausländerinnen und Ausländern im Ausland andererseits nicht zugänglich, weil eine solche Differenzierung mit der für diese Garantie fundamentalen Anerkennung der gleichen Würde aller Menschen nicht zu vereinbaren wäre,

> vgl. zu dem Zusammenhang zwischen Menschenwürde und elementarer Rechtsgleichheit BVerfGE 144, 20 (207 f.).

Zudem stellen sich Praktikabilitätsfragen, die für die Konkretisierung der Anforderungen an den prozeduralen Kernbereichsschutz bedeutsam sind, zumindest für alle Nachrichtendienste gleichermaßen.

Online-Durchsuchungen bringen typischerweise die Gefahr einer Erfassung auch höchstvertraulicher Daten mit sich. Daher bedarf es besonderer Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung. Hierzu ist vorzusehen, dass die Erhebung von Informationen, die dem Kernbereich zuzuordnen sind, soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt. Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen. Können mit deren Hilfe höchstvertrauliche Informationen aufgespürt und isoliert werden, ist der Zugriff auf diese untersagt. Ansonsten hat der Gesetzgeber dem Schutzbedarf der Betroffenen durch Sicherungen auf der Aus- und Verwertungsebene Rechnung zu tragen und die Auswirkungen eines solchen Zugriffs zu minimieren. Entscheidende Bedeutung hierfür kommt einer Sichtung durch eine unabhängige Stelle zu, die kernbereichsrelevante Informationen vor ihrer Kenntnisnahme und Nutzung durch die Behörde herausfiltert,

> BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 284 ff.

Nach diesen Maßstäben genügt § 36 Abs. 1 BNDG, der den Kernbereichsschutz auf der Ebene der Datenerhebung regelt, nicht vollständig den verfassungsrechtlichen Anforderungen. Diese Vorschrift verbietet allein Datenerhebungen zum Zweck der Erlangung von Kenntnissen zum Kernbereich privater Lebensgestaltung.

Eine derart restriktive Schutzregelung ist zwar bei der strategischen Telekommunikationsüberwachung hinnehmbar, weil der Kernbereichsschutz hier allein an die Auswahl der Suchbegriffe anknüpfen kann und sich aus diesen in der Regel nicht erkennen lässt, dass mit signifikanter Wahrscheinlichkeit kernbereichsrelevante Kommunikation erfasst wird,

> BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 206.

Diese Begründung lässt sich jedoch auf die Online-Durchsuchung nicht übertragen. Hier kann und muss gegebenenfalls bei der Auswahl der erhobenen Daten versucht werden, auch eine unabsichtliche Erhebung kernbereichsrelevanter Daten – etwa mit technischen Filtern – zu vermeiden. Insoweit greift das bloße Verbot eines gezielten Zugriffs auf den Kernbereich zu kurz.

Defizitär ist der Kernbereichsschutz auch auf der nachgelagerten Ebene der Datenauswertung ausgestaltet. Insoweit fehlt es an der gebotenen unabhängigen Kontrolle *aller* erhobenen Daten vor deren Verwertung. Sofern dabei die externe Sichtung an technische und fachliche Grenzen stößt, ist eine – durch gesonderte Verschwiegenheitspflichten abgesicherte – Hinzuziehung auch von Bediensteten des Bundesnachrichtendienstes zur Gewährleistung von ermittlungsspezifischem Fachverstand nicht ausgeschlossen. Darüber hinaus kann für die Sichtung auf technische Unterstützung durch den Dienst zurückgegriffen werden. Die tatsächliche Durchführung muss jedoch maßgeblich bei einer Stelle liegen, die gegenüber dem Bundesnachrichtendienst unabhängig ist,

> vgl. zu Verfassungsschutzbehörden BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 315.

Demgegenüber sieht § 36 Abs. 3 BNDG eine Vorabprüfung der erhobenen Daten durch den Unabhängigen Kontrollrat lediglich in Zweifelsfällen vor.

4. Übermittlung der erlangten Daten

Ermächtigungen zu Datenübermittlungen sind auch hinsichtlich von Daten, die durch Online-Durchsuchungen gewonnen wurden, grundsätzlich an dem Kriterium der hypothetischen Datenneuerhebung zu messen. Dieses Kriterium ist hier wegen der besonders hohen Eingriffsintensität von Online-Durchsuchungen streng zu handhaben. Zum einen muss die Übermittlung dem Schutz eines besonders gewichtigen Rechtsguts oder der Verfolgung einer besonders schweren Straftat dienen,

> BVerfGE 141, 220 (328); BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 236 ff., 250 f., 255 f.

Zum anderen darf der Gesetzgeber anders als bei Daten, die aus weniger eingriffsintensiven Überwachungsmaßnahmen stammen, die tatsächliche Übermittlungsschwelle nicht unter den Standard absenken, der für die Datenerhebung gilt,

> BVerfGE 141, 220 (329).

Für Datenübermittlungen durch Nachrichtendienste an Behörden mit operativen Befugnissen (also Befugnissen zur unmittelbaren Beschränkung grundrechtlich geschützter Freiheiten) gilt generell, dass Übermittlungsschwelle und Erhebungsschwelle einander entsprechen müssen,

> BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 245 ff., 252 f.

Nach diesem Maßstab verfehlen die in § 38 und § 39 BNDG enthaltenen Übermittlungsermächtigungen in erheblichem Ausmaß die verfassungsrechtlichen Anforderungen.

a) Übermittlung an Inlandsnachrichtendienste

Nach § 38 Abs. 1 Nr. 1 BNDG darf der Bundesnachrichtendienst Daten, die er durch eine Online-Durchsuchung im Ausland zur Gefahrenfrüherkennung erhoben hat, an Inlandsnachrichtendienste übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass dies zum Schutz besonders gewichtiger Rechtsgüter erforderlich ist. Diese Regelung stimmt wörtlich mit der Ermächtigung zur Übermittlung von Daten aus einer strategischen Ausland-Fernmeldeaufklärung in § 29 Abs. 1 Nr. 1 BNDG überein,

> vgl. zur Verfassungswidrigkeit von § 29 Abs. 1 Nr. 1 BNDG oben C. I. 8. a).

Der in § 38 Abs. 1 Nr. 1 BNDG enthaltene Übermittlungstatbestand genügt für die Übermittlung von Daten, die der Bundesnachrichtendienst durch eine Online-Durchsuchung erlangt hat, nicht den verfassungsrechtlichen Anforderungen. Er verfehlt das Kriterium einer hypothetischen Datenneuerhebung.

Inlandsnachrichtendiensten dürfen Online-Durchsuchungen nur zur Abwehr einer hinreichend konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut und zudem nur subsidiär zu polizeilichen Maßnahmen der Gefahrenabwehr erlaubt werden,

> BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 168, 176, 178.

Wird dieser strenge Maßstab nach dem Kriterium der hypothetischen Datenneuerhebung auf die Übermittlung von Daten übertragen, die aus einer Online-Durchsuchung stammen, so müsste auch die Übermittlung eine hinreichend konkretisierte Gefahr voraussetzen.

Für den Sonderfall von Daten aus einer Online-Durchsuchung im Ausland durch den Bundesnachrichtendienst erscheint allerdings denkbar, das Kriterium der hypothetischen Datenneuerhebung für diese Übermittlungskonstellation behutsam zu modifizieren. Hierfür lässt sich anführen, dass sich aus solchen Online-Durchsuchungen Erkenntnisse ergeben können, die inländische Behörden mangels eines Aufklärungsauftrags im Ausland nicht beschaffen können. Angesichts dessen mag ein genuin nachrichtendienstlicher Bedarf für solche Erkenntnisse anzuerkennen sein, der nicht durch die präventivpolizeiliche Eingriffsschwelle einer konkretisierten Gefahr konterkariert werden sollte.

Selbst wenn ein derart abgesenkter Maßstab angelegt wird, muss jedoch die Übermittlungsermächtigung dem sehr hohen Eingriffsgewicht der Online-Durchsuchung Rechnung tragen. Erforderlich ist auch für Datenübermittlungen an Nachrichtendienste eine gesetzliche Übermittlungsschwelle, die hinsichtlich des tatsächlichen Übermittlungsanlasses zumindest den Anforderungen an nachrichtendienstliche Überwachungsmaßnahmen von hoher Eingriffsintensität genügt. Die Übermittlung muss danach zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall benötigt werden,

> vgl. allgemein zur Übermittlung nachrichtendienstlicher Daten an nicht operativ tätige Stellen BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 258.

Zudem sind gesteigerte Anforderungen an die Beobachtungsbedürftigkeit der betreffenden Bestrebung zu stellen,

> vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 190 ff.

Diesen Anforderungen an die Übermittlungsschwelle genügt § 38 Abs. 1 Nr. 1 BNDG mit dem bloßen Erfordernis tatsächlicher Anhaltspunkte nicht,

> näher zu dem wortlautgleichen § 29 Abs. 1 Nr. 1 BNDG oben C. I. 8. a).

b) Übermittlung an inländische Behörden zur Unterrichtung der Bundesregierung oder einer Landesregierung

In § 38 Abs. 1 Nr. 2 und Abs. 2 finden sich Ermächtigungen zu Datenübermittlungen an inländische Behörden mit dem Ziel der politischen Unterrichtung der Bundesregierung oder einer Landesregierung. Diese Ermächtigungen sind wortlautidentisch mit den für Daten aus strategischen Ausland-Fernmeldeaufklärungen geltenden Regelungen in § 29 Abs. 1 Nr. 2 und Abs. 2 BNDG.

Ob sich die für Daten aus strategischen Telekommunikationsüberwachungen geltende Prämisse, dass die politische Unterrichtung einen privilegierten Übermittlungszweck darstellt und eine Datenübermittlung deshalb ohne besondere Anforderungen an Rechtsgüterschutz und Eingriffsschwelle zugelassen werden darf, auf Daten aus individualisierenden Überwachungsmaßnahmen ohne weiteres übertragen lässt, mag hier dahinstehen. Selbst unter dieser Prämisse genügen die in § 38 Abs. 1 Nr. 2 und Abs. 2 BNDG enthaltenen Übermittlungstatbestände nicht den verfassungsrechtlichen Anforderungen. Zum einen kann jedenfalls eine weitgehend voraussetzungslose Datenübermittlung auch an Landesregierungen nicht gerechtfertigt werden. Zum anderen gehen diese Ermächtigungen zu weit, soweit sie Datenübermittlungen an nachgeordnete Behörden zulassen. Insoweit lassen sich die zu § 29 Abs. 1 Nr. 2 und Abs. 2 BNDG ausgeführten Argumente vollständig auf § 38 Abs. 1 Nr. 2 und Abs. 2 BNDG übertragen,

siehe oben C. I. 8. b).

c) Übermittlung zum Zweck der Strafverfolgung

Die in § 38 Abs. 3 BNDG enthaltene Ermächtigung zu Datenübermittlungen zu Strafverfolgungszwecken stimmt weitgehend mit § 29 Abs. 3 BNDG überein, auf den die Norm hinsichtlich der zu verfolgenden Straftaten verweist.

Wegen dieses Verweises beschränkt § 38 Abs. 3 BNDG zum einen die Datenübermittlung nicht durchweg auf die Verfolgung besonders schwerer Straftaten. Insbesondere lässt § 38 Abs. 3 i.V.m. § 29 Abs. 3 Nr. 2 BNDG Datenübermittlungen auch zur Verfolgung weniger gewichtiger Delikte zu,

siehe oben C. I. 8. c).

Zum anderen enthält § 38 Abs. 3 BNDG zwar eine restriktivere Eingriffsschwelle als § 29 Abs. 3 BNDG, indem die Übermittlung nur erlaubt wird, wenn Tatsachen die Annahme rechtfertigen, dass sie zur Verfolgung einer Katalogtat erforderlich ist. Auch diese Übermittlungsschwelle unterschreitet jedoch noch das verfassungsrechtliche Erfordernis eines auf *bestimmten* Tatsachen beruhenden Tatverdachts,

vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 252.

Dass das BNDG entsprechend dem strafprozessualen Sprachgebrauch zwischen bloßen „Tatsachen“ und „bestimmten Tatsachen“ unterscheidet, zeigt sich etwa an § 39 Abs. 3 BNDG, der bestimmte Auslandsübermittlungen an das Erfordernis bestimmter Tatsachen bindet. § 29 Abs. 3 BNDG bindet die

Datenübermittlung somit auch nach der Binnensystematik des Gesetzes an eine lediglich mittlere tatsächliche Schwelle, was nicht ausreicht.

d) Übermittlung an die Bundeswehr

Gemäß § 38 Abs. 5 BNDG darf der Bundesnachrichtendienst Daten, die er durch eine Online-Durchsuchung zur Gefahrenfrüherkennung gewonnen hat, an die Bundeswehr übermitteln. Diese Regelung ist weitgehend wortlautidentisch mit § 29 Abs. 5 BNDG und teilt dessen Mängel: § 38 Abs. 5 Satz 1 BNDG, der manuelle Übermittlungen regelt, enthält keine hinreichende tatsächliche Übermittlungsschwelle, auf die auch bei Übermittlungen an die Bundeswehr nicht generell verzichtet werden kann. § 38 Abs. 5 Satz 2 BNDG erlaubt eine automatisierte Übermittlung von Daten aus Online-Durchsuchungen, die einen Bezug zu den Gefahrenbereichen nach § 19 Abs. 4 Nr. 1 lit. a (Landes- und Bündnisverteidigung, Auslandseinsätze) und Nr. 2 lit. a (Leib, Leben oder Freiheit einer Person) BNDG aufweisen. Diese Ermächtigung schafft in der Sache einen Überwachungsverbund zwischen Bundesnachrichtendienst und Bundeswehr, da die Prüfung und Auswertung der en bloc automatisiert übermittelten Daten der Bundeswehr obliegt. Die Datenübermittlung ist dabei, abgesehen von dem nicht näher spezifizierten Gefahrenbezug, praktisch voraussetzungslos zulässig. Insbesondere ist sie nicht an eine besondere tatsächliche Übermittlungsschwelle gebunden. Für die nachgelagerten Weiterverarbeitungsschritte fehlt es an jeglichen materiellen und prozeduralen Vorgaben. Eine so weitreichende Freigabe und so rudimentäre gesetzliche Steuerung ist für eine Überwachungsmaßnahme höchster Eingriffsintensität wie die Online-Durchsuchung auch unter Berücksichtigung der Spezifika militärischer Auswertungsbedarfe rechtsstaatlich nicht tragbar,

vgl. zu § 29 Abs. 5 BNDG oben C. I. 8. e).

e) Übermittlung an sonstige inländische Stellen

Für die Übermittlung von Daten aus Online-Durchsuchungen an andere inländische Stellen, also im Wesentlichen an Private, verweist § 38 Abs. 6 BNDG auf § 29 Abs. 6 BNDG. Die in Bezug genommene Übermittlungsermächtigung in § 29 Abs. 6 Satz 1 BNDG errichtet jedoch keine tragfähige tatsächliche Eingriffsschwelle,

siehe oben C. I. 8. f).

Sie kann auch die Übermittlung von Daten aus Online-Durchsuchungen nicht legitimieren.

f) Übermittlung ins Ausland

Die in § 39 BNDG enthaltenen Ermächtigungen zu Datenübermittlungen ins Ausland entsprechen weitgehend den Regelungen zur Auslandsübermittlung von Daten aus der strategischen Ausland-Fernmeldeaufklärung in § 30 BNDG. Sie teilen damit auch die verfassungsrechtlichen Mängel dieser Vorschrift,

siehe oben C. I. 8. g).

§ 39 Abs. 1 BNDG erlaubt Datenübermittlungen an ausländische öffentliche Stellen zum Zweck der Unterrichtung im Rahmen der internationalen politischen Zusammenarbeit. Die Regelung stimmt nahezu wörtlich mit § 30 Abs. 1 BNDG überein. Es wurde lediglich das Wort „wenn“ durch „soweit“ ersetzt, ohne dass sich daraus ein erkennbarer sachlicher Unterschied ergäbe. Wie § 30 Abs. 1 BNDG ist die Ermächtigung verfassungswidrig, weil sie auf einer nicht tragfähigen Gleichsetzung der politischen Unterrichtung im Rahmen der internationalen politischen Zusammenarbeit mit der politischen Unterrichtung der Bundesregierung beruht und zudem unter Verstoß gegen den Bestimmtheitsgrundsatz in sich unschlüssig formuliert ist.

Die in § 39 Abs. 2 BNDG enthaltene Ermächtigung zu Datenübermittlungen zu Strafverfolgungszwecken stimmt wörtlich mit § 30 Abs. 2 BNDG überein und verfehlt ebenso wie diese Vorschrift die verfassungsrechtlichen Anforderungen. Dies liegt zum einen an dem Verweis auf den seinerseits nicht vollständig tragfähigen Straftatenkatalog in § 29 Abs. 3 BNDG, zum anderen an der unzureichenden tatsächlichen Übermittlungsschwelle (bloß) tatsächlicher Anhaltspunkte.

Wegen des Verfahrens der Übermittlung verweist § 39 Abs. 6 BNDG auf § 30 Abs. 6 bis 9 BNDG. Dieser Verweis erstreckt sich auf die unzureichende Schutzregelung in § 30 Abs. 6 BNDG, die keine positive Vergewisserung über das Schutzniveau im Ausland vorsieht und den Gegenstand der Rechtsstaatlichkeitsprüfung auf die Verletzung von Menschenrechten oder elementaren rechtsstaatlichen Grundsätzen durch die Nutzung der übermittelten Daten verengt. Des Weiteren legt § 39 Abs. 6 BNDG einen Kettenverweis über § 30 Abs. 9 BNDG auf § 29 Abs. 13 und Abs. 14 Satz 2 BNDG an, der sinnwidrig ist, weil dadurch Pflichten des Übermittlungsempfängers begründet werden, ohne dass der deutsche Gesetzgeber diese hinsichtlich von ausländischen öffentlichen Stellen überhaupt regeln könnte.

(Prof. Dr. Bäcker, LL.M.)

Anlage:

Verfahrensvollmachten.

Soweit die Vollmachten nur in Kopie beigefügt sind, werden die Originale zeitnah nachgereicht.