Hochschule des Bundes
für öffentliche Verwaltung

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)731 C

POSTANSCHRIFT HS BUND, POSTFACH 40527, 10063 BERLIN

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin

Prof. Dr. Markus Löffelmann
HAUSANSCHRIFT Habersaathstr. 51, 10115 Berlin
POSTANSCHRIFT Postfach 40527, 10063 Berlin
TEL 030 – 22 00 89 – 85513
E-MAIL markus.loeffelmann@hsbund-nd.de

DATUM Berlin, 18.02.2021

BETREFF **Schriftliche Stellungnahme zur öffentlichen Anhörung am 18. Februar 2021 zu BT-Drs. 19/26103, 19/26221, 19/19502 und 19/509**

Stellungnahme zum

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts

Bundestags-Drucksache 19/26103

sowie

zu dem Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN Legitimität und Leistungsfähigkeit der Nachrichtendienste stärken – Kontrolle auf allen Ebenen verbessern und ausbauen, Bundestags-Drucksache 19/26221,

zu dem Gesetzentwurf der Fraktion der FDP Entwurf eines Gesetzes zur Stärkung der parlamentarischen Kontrolle der Nachrichtendienste, Bundestags-Drucksache 19/19502 und

zu dem Antrag der Fraktion der FDP Reform der Nachrichtendienste – Lehren aus dem Urteil des Bundesverfassungsgerichts zum BND-Gesetz, Bundestags-Drucksache 19/19509

A. Vorbemerkung

Der Gesetzentwurf unter BT-Drs. 19/26103 dient in erster Linie der Umsetzung der Vorgaben des BVerfG in seinem Urteil vom 19.5.2020, 1 BvR 2835/17. Darüber hinaus werden mit dem Gesetz eine Befugnis des BND zu Eingriffen in informationstechnische Systeme („Online-Durchsuchung“, „informationstechnische Operation“, „Computer Network Exploitation“) von Ausländern im Ausland sowie Befugnisse zur zweckändernden Weiterverarbeitung von Telekommunikationsverkehrsdaten, die aus Maßnahmen der Fernmeldeaufklärung nach §§ 3, 5 und 8 G 10 gewonnen wurden, geschaffen. Der Antrag unter BT-Drs. 19/26221 versammelt über den durch das Urteil des BVerfG vom 19.5.2020 veranlassten Regelungsbedarf hinausgehend eine Vielzahl von Vorschlägen für eine grundsätzliche Änderung der Kontrollregimes betreffend die Nachrichtendienste des Bundes, namentlich für einen Ausbau der parlamentarischen Kontrolle. Der Gesetzentwurf unter BT-Drs. 19/19502 und der Antrag unter BT-Drs. 19/19509 betreffen den Vorschlag der Errichtung des Amts eines parlamentarischen Nachrichtendienstbeauftragten.

B. Zu BT-Drs. 19/26103

I. Zu Artikel 1 (Änderung des BNDG)

1. Zu Ziff. 2 (Geltungsbereich)

Die Regelung des § 1 Abs. 2 S. 2 BNDG knüpft an den bisherigen Charakter des BNDG als Datenschutzgesetz an (vgl. BGBl. I 1990 S. 2954; dazu näher Kutzschbach, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, Teil VI § 6 Rn. 2 ff.), dessen Geltung auf das Hoheitsgebiet der Bundesrepublik Deutschland beschränkt ist. Dahinter steht der Gedanke, dass die Erhebung von Informationen durch den BND nur dann einen regelungsbedürftigen Grundrechtseingriff darstellt, wenn sie auf deutschem Hoheitsgebiet erfolgt. Mit der Klarstellung der Erstreckung des Grundrechtsschutzes auf Ausländer im Ausland durch das Urteil des BVerfG vom 19.5.2020 wird diese territoriale Unterscheidung hinfällig. § 1 Abs. 2 S. 2 BNDG sollte daher gestrichen werden, zumal die Auslegung der Norm schon bislang erhebliche Schwierigkeiten bereitet hat (vgl. Gusy, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2018, § 1 BNDG Rn. 45 ff.).

2. Zu Ziff. 5 (nachrichtendienstliche Mittel)

Nach der Entwurfsbegründung (S. 51) soll mit der Verschiebung der Verweisung auf § 8 Abs. 2 BVerfSchG keine inhaltliche Änderung des rechtlichen Handlungsrahmens einhergehen. Dem Wortlaut des § 5 S. 1 BNDG-E nach ist jedoch durch das Wegfallen der Verweisung auf § 8 Abs. 2 BVerfSchG – ungeachtet der Tatsache, dass diese Norm wegen ihrer im Gegensatz zu Parallelnormen mehrerer LVerfSchG offenen Fassung und Verweisung auf interne Dienstvorschriften der Kritik ausgesetzt ist – eine erweiternde Auslegung auf andere, dort nicht genannte nachrichtendienstliche Mittel möglich. Im Gegensatz zu den §§ 9, 9a, 9b BVerfSchG stellt § 8 Abs. 2 BVerfSchG, wie erst durch das Änderungsgesetz vom 17.11.2015 (BGBl. I S. 1938) klargestellt wurde, auch keine Befugnisnorm dar (BT-Drs. 18/4654, S. 25; Roth, in: Schenke/Graulich/Ruthig, a. a. O., § 8 BVerfSchG Rn. 20), so dass

die Verlagerung in den Kontext der erstgenannten Normen systematisch nicht stimmig ist. Die bisherige Formulierung des § 5 BNDG sollte vor diesem Hintergrund beibehalten werden.

3. Zu Ziff. 9 (Datenweiterverarbeitung)

Die bisherigen §§ 19 bis 21 BNDG werden vom Entwurf unverändert als §§ 6 bis 8 BNDG-E übernommen. Die bisherige Rechtslage weist allerdings durch mehrere Verweise auf das BVerfSchG Unstimmigkeiten auf. So haben die einschränkenden Voraussetzungen nach § 10 Abs. 1 Nr. 1 bis 3 BVerfSchG im BNDG, welches in § 19 Abs. 1 auf diese Norm verweist, keinen Anwendungsbereich. Unstimmig – und regelungstechnisch unübersichtlich – ist auch die Einhegung der Verarbeitung personenbezogener Daten Minderjähriger durch die Bezugnahme in § 19 Abs. 2 BNDG auf § 11 BVerfSchG, der wiederum auf den Straftatenkatalog des G 10 verweist. Das gegenständliche Regelungskonzept löst sich gerade von einem auf Anlasstaten bezogenen Ordnungskonzept und differenziert zwischen politischer Unterrichtung und Gefahrenfrüherkennung. Auch die Unterscheidung zwischen Dateien und Akten bei den Berichtigungs- und Löschungspflichten nach § 20 BNDG und § 12 BVerfSchG erscheint nicht mehr zeitgemäß. Die gegenständlichen Normen sollten – wenn nicht im gegenständlichen Entwurf, so doch perspektivisch – ebenfalls neu gefasst und dabei im BNDG ein selbständiges Regelungsregime etabliert werden.

4. Zu Ziff. 12 (Datenabfrage)

Die Übermittlungsvorschrift des § 23 BNDG wird vom Entwurf als § 10 BNDG-E übernommen und lediglich redaktionell an den datenschutzrechtlichen Sprachgebrauch angepasst. Soweit § 23 Abs. 3 BNDG eine Abfragebefugnis des BND für bei anderen Sicherheitsbehörden gespeicherte personenbezogene Daten enthält, entspricht diese nicht den Vorgaben des BVerfG zur präzisen und normenklaren Regelung der Abfragebefugnis unter Berücksichtigung qualifizierter Eingriffsschwellen, die der Intensität des durch die Abfrage vermittelten Grundrechtseingriffs entsprechen. Die Monita des BVerfG aus seiner Entscheidung vom 27.5.2020, 1 BvR 1873/13, 1 BvR 2618/13 (Bestandsdatenauskunft II) sind dem Gedanken nach auf den Austausch anderer Arten von personenbezogenen Daten als Bestandsdaten übertragbar. § 23 Abs. 3 BNDG (§ 10 Abs. 3 BNDG-E) unterscheidet weder zwischen verschiedenen Erhebungskontexten, noch zwischen verschiedenen Arten personenbezogener Daten und Kategorien der Schutzbedürftigkeit, noch enthält die Norm qualifizierte Anforderungen an die Abfrage. Alleiniges materielles Anforderungskriterium ist die Erforderlichkeit zur Aufgabenerfüllung. Für die nachrichtendienstliche Praxis entsteht dadurch das Problem, dass handlungsleitende Maßstäbe für die Beurteilung der Rechtmäßigkeit einer Anforderung weitgehend fehlen. Angesichts der generellen Unübersichtlichkeit des sicherheitsbehördlichen Datenübermittlungsregimes, der großen Tragweite der mit einer Datenanforderung - oder deren Unterlassen - verbundenen Konsequenzen und hohen Verantwortlichkeit des einzelnen Sachbearbeiters, welche durch die gesetzliche Dokumentationspflicht (§ 23 Abs. 3 S. 2 BNDG i. V. m. § 18 Abs. 5 BVerfSchG) lückenlos nachvollziehbar ist, erscheint diese Regelung nicht sachgerecht. Eine adäquate Überarbeitung der Norm würde freilich vorgängig die Entwicklung eines in sich konsistenten Systems von Schutzbedürftigkeitsklassen für

personenbezogene Daten und die Zuordnung gewichteter hoheitlicher Zwecke voraussetzen. Ein solches System existiert bislang nicht und wird aus datenschutzrechtlichen Gründen, aber auch zur Herstellung von Handlungssicherheit für die Mitarbeiter der Nachrichtendienste sowie aus verfahrensökonomischen Gründen dringend benötigt (vgl. bereits ausf. zu den Übermittlungsregelungen bei der Bestandsdatenabfrage Löffelmann, Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschussdrucksache 19(4)696 B).

5. Zu Ziff. 13 (Datenübermittlung)

Die vorstehenden Ausführungen gelten sinngemäß für die in § 24 BNDG (§ 11 BNDG-E) geregelte Übermittlung von personenbezogenen Daten durch den BND an andere Behörden (in diese Richtung auch die Kritik des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in seiner Stellungnahme vom 18.12.2020 unter Ziff. 7). Die Schwellen nach § 24 Abs. 1 S. 2, Abs. 2 und 3 BNDG i. V. m. § 19 Abs. 1 BVerfSchG dürften zwar den verfassungsrechtlichen Anforderungen an die Übermittlung von personenbezogenen Daten, welche durch qualifizierte Grundrechtseingriffe erhoben wurden, genügen. Das Regelungsregime ist aber überaus unübersichtlich, impraktikabel und dadurch fehleranfällig, was nicht mit der großen Tragweite von Datenübermittlungen im Sicherheitsbereich korrespondiert. Die Regelungen wurden deshalb vom BVerfG unter Bestimmtheitsgesichtspunkten beanstandet (BVerfG, a. a. O., Rn. 312 - 314)

6. Zu Ziff. 14 (Beteiligung der Bundeswehr an gemeinsamen Dateien)

Die Beteiligung der Bundeswehr an gemeinsamen Dateien nach § 25 BNDG (§ 12 BNDG-E) erscheint aus den in der Begründung genannten Gesichtspunkten (S. 52) grundsätzlich sachgerecht. Das Konzept der gemeinsamen Dateien beruht allerdings darauf, dass bei jedem Einstellen eines Datums durch eine Behörde die Zugriffsberechtigung aller anderen beteiligten Behörden überprüft werden muss (§ 25 Abs. 2 S. 1 BNDG). Danach wäre also eine Befugnis der beteiligten Behörden zur Datenübermittlung an die Bundeswehr im Einzelfall erforderlich, entsprechend auch eine Befugnis der Dienststellen der Bundeswehr zur Abfrage und Nutzung solcher Daten. An solchen Übermittlungs- und Abfragebefugnissen unter Beteiligung der Dienststellen der Bundeswehr fehlt es bislang, weshalb die Änderung ins Leere läuft. § 25 Abs. 3 S. 1 BNDG i. V. m. § 19 Abs. 2 BVerfSchG bezieht sich nur auf die Dienststellen der in Deutschland stationierten NATO-Streitkräfte. § 23 Abs. 1 S. 2 BNDG enthält eine Befugnis nur für den umgekehrten Fall der Datenübermittlung von der Bundeswehr an den BND.

7. Zu Ziff. 21 (Technische Aufklärung)

a) Zu § 19 BNDG-E (strategische Ausland-Fernmeldeaufklärung)

aa) Zu Absatz 1

Die Legaldefinition der strategischen Fernmeldeaufklärung in § 19 Abs. 1 BNDG-E vermengt Begrifflichkeiten mit Bezug zum Recht auf informationelle Selbstbestimmung („personenbezogen“) und zum Fernmeldegeheimnis („Inhaltsdaten“). Weder allgemeinsprachlich noch

technisch macht die Rede von „Inhaltsdaten von Ausländern“ Sinn. Gemeint sind Inhaltsdaten der Telekommunikation von Ausländern. Das Fernmeldegeheimnis unterscheidet auch nicht, wie die Entwurfsbegründung (S. 54) unterlegt, zwischen personenbezogenen Daten einer Telekommunikation und Sachdaten. Vielmehr ist der Telekommunikationsvorgang als solcher durch Art. 10 GG geschützt, einerlei, ob die Telekommunikationsinhalte sich zu Personen verhalten oder sich um „reine Sachdaten“ handelt. Für die nachrichtendienstliche Praxis mag eine solche Differenzierung zu einer prima facie wünschenswerten Absenkung der Schwelle für die Verarbeitung vermeintlich „nicht-personenbezogener“ Telekommunikationsdaten führen. Zugleich bedeutet diese Differenzierung aber auch eine Pflicht zur Unterscheidung von „personenbezogenen“ und lediglich „sachbezogenen“ Telekommunikationsdaten. Eine solche Unterscheidung ist schon theoretisch kaum möglich, da es nach ständiger Rechtsprechung des BVerfG im Kontext der digitalen Datenverarbeitung und Speicherung kein persönlichkeitsrechtlich „belangloses Datum“ mehr gibt (vgl. bereits BVerfGE 65, 1, 45; 120, 378, 398 f. u. ö.), und erscheint daher auch wenig praktikabel. Jedenfalls erschließt sich nicht, welcher Datenbestand unter die „nicht-personenbezogenen“ Inhaltsdaten fällt, und welche Regelungen hierfür gelten. § 19 Abs. 1 BNDG-E kommt insoweit als Ermächtigungsgrundlage wegen der einschränkenden Formulierung „personenbezogene“ nicht in Betracht. Es sollte geprüft werden, ob auf diesen einschränkenden Begriff verzichtet werden kann. Gegebenenfalls sollte klargestellt werden, welche Regelungen für „sachbezogene“ Telekommunikationsdaten gelten, die dem Schutzbereich des Art. 10 GG unterfallen.

Die Legaldefinition folgt ferner nicht der üblichen (und auch vom BVerfG verwendeten) Unterscheidung von Datenerhebung und Datenverwendung oder Datenverarbeitung. Übersichtlicher wäre es, zunächst die strategische Fernmeldeaufklärung als Mittel der Datenerhebung zu definieren. Nur für das Speichern und die weitere Verwendung der nach der Relevanzprüfung noch vorliegenden Inhaltsdaten sollte der datenschutzrechtliche Begriff des Verarbeitens verwendet werden. Andernfalls besteht Raum für den Fehlschluss, dass auch nach Abschluss der Relevanzprüfung Teile des Rohdatenstroms weiter bevorratet und anderweitig verarbeitet werden können, denn Verarbeitung von Inhaltsdaten „auf der Grundlage zuvor angeordneter strategischer Aufklärungsmaßnahmen“ ist auch die unbegrenzte Speicherung und spätere Auswertung von Rohdaten in anderen Zusammenhängen. Die beabsichtigte Formulierung des Absatzes 1 verschleiert diese Zusammenhänge mehr als sie sie klärt.

bb) Zu Absatz 2

Zumindest missverständlich ist die Formulierung in Absatz 2. Nach dem allgemeinen und sicherheitsbehördlichen Sprachgebrauch handelt es sich bei einer „Maßnahme“ um ein operatives Tätigwerden mit Außenwirkung und (häufig) Grundrechtsrelevanz. Nach der Definition des Absatzes 2 handelt es sich hingegen bei einer „strategischen Aufklärungsmaßnahme“ um eine administrative, zunächst rein interne Festlegung auf ein bestimmtes Aufklärungsziel anhand des Zwecks, Themas, geografischen Fokus und der Dauer der beabsichtigten Aufklärung. Hinter dieser Konstruktion steht offenbar die Überlegung des BVerfG, Ausgangspunkt der strategischen Überwachung müsse einerseits „eine formalisierte Festlegung jeweils begrenzter Überwachungsmaßnahmen sein“ (BVerfG, a. a. O., Rn. 179), andererseits hindere dies nicht, „Netzanordnungen und darauf aufbauende Ausleitungsanordnungen gegenüber einem Telekommunikationsanbieter zur Durchführung einer größeren Zahl verschiedener Überwachungsmaßnahmen zusammenfassend zu treffen“ (BVerfG, a. a. O., Rn.

184). Unter Praktikabilitätsgesichtspunkten macht ein solcher auf die übergeordnete Festlegung der Rahmenbedingungen konkreter Maßnahmen der strategischen Ausland-Fernmeldeaufklärung ausgerichteter Anordnungs- und Kontrollmechanismus viel Sinn. Nach dem Gesetzentwurf bezieht sich die gerichtsähnliche Kontrolle in diesem Sinne auf die „strategische Aufklärungsmaßnahme“ (§ 23 Abs. 4 BNDG-E). Andererseits nimmt die die Zuständigkeit des Kontrollorgans bestimmende Norm (§ 42 Abs. 1 Nr. 1 BNDG-E) durch den Verweis auf § 23 Abs. 1 BNDG-E, welcher wiederum auf § 19 Abs. 1 BNDG-E verweist, aber inkonsequent auf die Legaldefinition der „strategischen Ausland-Fernmeldeaufklärung“ Bezug. Auch ist zu berücksichtigen, dass in anderen Zusammenhängen, insbesondere auch für Maßnahmen der strategischen Fernmeldeaufklärung nach § 5 G 10, unter der anzuordnenden und kontrollierenden Maßnahme die individuelle Überwachung und nicht deren allgemeine Rahmenbedingungen gemeint ist. In diese Richtung deutet auch die Formulierung des BVerfG, „(f)ür die Festlegung der Maßnahme selbst jedoch bedarf es, entsprechend dem Richtervorbehalt bei individualbezogener Telekommunikationsüberwachung durch Einzelfallanordnung, einer gerichtsähnlichen Kontrolle“ (BVerfG, a. a. O., Rn. 181). Der Begriffssynkretismus von „strategischer Auslands-Fernmeldeaufklärung“ und „strategischer Aufklärungsmaßnahme“ erscheint vor diesem Hintergrund ausgesprochen verwirrend und schwer zu durchdringen. Vorzugswürdig wäre die Rede von der „Anordnung einer Maßnahme der strategischen Fernmeldeaufklärung“. Diese Anordnung müsste die in Absatz 2 bestimmten Angaben enthalten und könnte formal mit anderen Anordnungen zusammengefasst werden. Die Rechtmäßigkeit dieser Anordnung wäre Gegenstand der Prüfkompetenz des Unabhängigen Kontrollrats. Was der Gesetzentwurf in Absatz 2 als „strategische Aufklärungsmaßnahme“ definiert, ist hingegen die vom BVerfG erwähnte, einer Anordnung vorgelagerte „interne verfahrensrechtliche Ausgestaltung solcher formalisierter Festlegungen“ (BVerfG, a. a. O., Rn. 180) und sollte daher auch als solche und nicht als „Maßnahme“ bezeichnet werden. Diese interne Ausgestaltung könnte im Übrigen wohl auch Gegenstand einer Dienstvorschrift sein.

cc) Zu Absätzen 3 und 4

Das unklare Verhältnis der Begriffe „strategische Aufklärungsmaßnahme“ und „strategische Ausland-Fernmeldeaufklärung“ zueinander setzt sich fort in den Absätzen 3 und 4, wo für die Zulässigkeit der „strategischen Aufklärungsmaßnahmen“ auf die Differenzierung in Absatz 1 Nummern 1 und 2 Bezug genommen wird, die aber die „strategische Ausland-Fernmeldeaufklärung“ betreffen.

Im Übrigen übernehmen die Regelungen in den Absätzen 3 und 4 im Anschluss an Absatz 1 die vom BVerfG vorgenommene Unterscheidung zwischen den Aufgaben der politischen Unterrichtung und der Früherkennung von Gefahren. Ungeachtet des Umstands, dass diese strenge Kategorisierung künstlich und wenig praktikabel erscheint (vgl. Dietrich, GSZ 2020, 173, 178: „holzschnittartiges Verständnis“; Gärditz, JZ 2020, 825, 830: „erhebliche praktische Probleme“), ist hiergegen regelungstechnisch nichts einzuwenden. Das Erfordernis tatsächlicher Anhaltspunkte für die Aufklärungsrelevanz der Maßnahme zur Gefahrenfrüherkennung hinsichtlich der in Absatz 4 enumerativ aufgelisteten Gefahrbereiche und Rechtsgutsbedrohungen stellt eine hinreichend enge und praktikable Einhegung dar. Der detaillierte Katalog der Aufklärungsanlässe ist regelungstechnisch vorbildlich, indem er einen plastischen Eindruck vom spezifisch nachrichtendienstlichen Zuschnitt und vom Gewicht der verfolgten

Zwecke vermittelt, ohne dabei hoheitliche Geheimhaltungsinteressen zu beeinträchtigen. In seiner inhaltlichen Ausgestaltung ist der Katalog nicht zu beanstanden. Lediglich Buchstabe a) fällt unter Nummer 1 etwas aus dem Rahmen, da die Landes- und Bündnisverteidigung und die Einsätze der Bundeswehr oder verbündeter Streitkräfte im Ausland per se keine Gefahr-, sondern Handlungsbereiche darstellen; eine Einordnung unter Nummer 2 würde hier besser passen. Die ungewöhnlich ausführliche Gesetzbegründung (S. 55 bis 61) unterstreicht den Anspruch, hinsichtlich des Einsatzes der strategischen Ausland-Fernmeldeaufklärung zu Zwecken der Gefahrenfrüherkennung ein hohes Maß an Transparenz herzustellen und die Tätigkeit des BND gegenüber der polizeilichen Gefahrenabwehr abzugrenzen.

Die Formulierung „mit Bezug zu folgenden Gefahrbereichen“ in Zusammenschau mit dem Wortlaut des Absatzes 1 Nummer 2 („Früherkennung von aus dem Ausland drohenden Gefahren“) ist dabei grundsätzlich geeignet, den Aufklärungsauftrag der Nachrichtendienste hinreichend präzise im Gefahrenvorfeld zu beschreiben, sofern der Begriff der Gefahr hier nicht im polizeirechtlichen Sinne ausgelegt wird, sondern im Sinne des Bestehens einer „existenziellen Bedrohungslage“ (so BVerfGE 120, 274, 328; Löffelmann, in: Dietrich/Eiffler, a. a. O., Teil VI § 4 Rn. 33 zu G 10). Alternativ und etwas trennschärfer könnte man in Absatz 1 Nummer 2 formulieren „*2. Der Aufklärung von aus dem Ausland stammenden Bedrohungslagen von internationaler Bedeutung*“ und auch in Absatz 4 Nummer 1 statt von „Gefahrenbereichen“ von „Bedrohungslagen“ sprechen. Das entspräche besser der Wortwahl an zahlreichen Stellen der Entwurfsbegründung und auch dem international üblichen Sprachgebrauch (*threat*).

Kritisch ist in diesem Zusammenhang – auch mit Blick auf die der beabsichtigten Regelung zugrunde liegende Formulierung des BVerfG (a. a. O., Rn. 128: „Früherkennung von aus dem Ausland drohenden Gefahren“) – darauf hinzuweisen, dass der BND bislang weder auf eine Informationsgewinnung *im* Ausland noch auf eine solche zu Bedrohungslagen, die *aus* dem Ausland „drohen“ oder „stammen“ oder dort sonst ihren Ursprung haben, beschränkt ist. Maßgeblich ist vielmehr, dass der BND Informationen *über* das Ausland sammelt und diese Informationen von außen- und sicherheitspolitischer Bedeutung sein müssen (§ 1 Abs. 2 S. 1 BNDG). Der notwendige Auslandsbezug wird durch den Inhalt der zu gewinnenden Erkenntnisse, die sich auf ausländische Vorgänge oder Zustände beziehen, hergestellt (näher Gusy, in: Schenke/Graulich/Ruthig, a. a. O., § 1 BNDG Rn. 24 m. w. N.; Warg, in: Dietrich/Eiffler, a. a. O., Teil V § 1 Rn. 88). So fällt es z. B. in den Aufgabenbereich des BND, Informationen im Ausland über sich dort aufhaltende Mitglieder einer inländischen terroristischen Zelle zu sammeln, von der eine Bedrohung von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik ausgeht. Die Aufgabenbereiche des BND und des Verfassungsschutzes können sich insoweit überschneiden. Die Bindung der strategischen Ausland-Fernmeldeaufklärung auf die Früherkennung von „aus dem Ausland drohenden Gefahren“ stellt demnach eine substanzielle Beschränkung dar, die der Gesetzgeber vornehmen kann, aber nicht muss. § 6 Abs. 1 S. 1 Nr. 1 BNDG in der noch geltenden Fassung ist in Anlehnung an den Zuschnitt des Aufgabenbereichs bewusst weiter gefasst (vgl. BT-Drs. 18/9041, S. 22; Plenarprotokoll 18/184, S. 18274D). Auch die Gesetzbegründung (S. 57) spricht im Zusammenhang mit dem gewaltbereiten Terrorismus und Extremismus allgemein und zutreffend von der Notwendigkeit „der Erkennung von Bedrohungen für die Sicherheit der Bundesrepublik Deutschland“. Vor diesem Hintergrund könnte darüber nachgedacht werden, in Absatz

1 Nummer 2 auf die einschränkende Formulierung „aus dem Ausland drohenden“ zu verzichten.

Am Rande ist darauf hinzuweisen, dass, soweit die Begründung (S. 55) davon spricht, Satz 2 definiere den Gefahrenbegriff im nachrichtendienstlichen Sinn, dies keine Entsprechung im Gesetztext hat.

dd) Zu Absatz 5

Absatz 5 entspricht dem § 6 Abs. 2 BNDG in der geltenden Fassung und ist nicht zu beanstanden.

ee) Zu Absatz 6

Absatz 6 eröffnet dem BND eine Befugnis zum unerlaubten Eindringen in und Nutzen von Datenverarbeitungsanlagen ausländischer Diensteanbieter, die nicht zur Ausleitung von Telekommunikation verpflichtet werden können. Eine solche Befugnis ist erforderlich, wenn man über die unmittelbare Bindungswirkung der Entscheidung des BVerfG vom 19.5.2020 hinausgehend – zurecht – davon ausgeht, dass auch andere Grundrechte als Art. 5 Abs. 1 S. 2 und Art. 10 GG in ihrer abwehrrechtlichen Dimension natürliche und auch (in den Grenzen des Art. 19 Abs. 3 GG) juristische Personen im Ausland schützen. Mit dem unbefugten Eindringen in und Nutzen der Systeme der Anbieter kann für diese ein Eingriff in das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme sowie in Art. 12 und 14 GG verbunden sein (vgl. - allerdings unklar - BVerfGE 120, 274, 308 f.). Da das Eindringen hier nicht nur (wie bei einer Quellen-Telekommunikationsüberwachung, die freilich nicht beim Anbieter, sondern an der „Quelle“ vorgenommen wird) mit dem Ziel erfolgen soll, laufende Telekommunikationsinhalte in Echtzeit zu erheben, sondern auch in einem „Pufferspeicher“ abgelegte Inhalte, und außerdem gespeicherte Bestandsdaten ausgelesen werden sollen, handelt es sich der Sache nach um eine Art „Online-Durchsuchung“ bei den Anbietern. Die „Online-Durchsuchung“ (der Begriff ist im nachrichtendienstlichen Kontext eher unüblich, soll hier aber der leichter nachvollziehbaren verfassungsrechtlichen Einordnung halber beibehalten werden) hat das BVerfG bislang nur zum Schutz „überragend wichtiger Rechtsgüter“ als zulässig erachtet (BVerfGE 120, 274, 328). Fraglich ist, inwieweit der Katalog der Gefahrenanlässe für eine strategische Ausland-Fernmeldeaufklärung damit vergleichbar ist. Hier besteht für den Regelungsentwurf ein gewisses verfassungsrechtliches Risiko. Andererseits erscheint es unter Praktikabilitätsgesichtspunkten auch nicht zielführend, spezifisch für den Fall nicht kooperierender Anbieter ein eigenes Regelungsregime unter erhöhten Anforderungen festzulegen. Da das BVerfG Spielräume angedeutet hat, um besonderen tatsächlichen Rahmenbedingungen im Ausland Rechnung zu tragen (BVerfG, a. a. O., Rn. 104) und auch unter Verhältnismäßigkeitsgesichtspunkten für dort Betroffene die Möglichkeit eines niedrigeren Schutzniveaus anerkannt hat (BVerfG, a. a. O., Rn. 265 ff.), erscheint die hier beabsichtigte Regelung vertretbar. Sie verdeutlicht jedenfalls, dass der Rechtsrahmen für Implementierungsanforderungen bei Aufklärungsmaßnahmen nicht rezeptartig auf Auslandssachverhalte übertragen werden kann und das gesetzgeberische Austarieren von Grundrechtsschutz, hoheitlicher Zweckverfolgung und Praktikabilität dort an Grenzen stößt.

ff) Zu Absatz 7

Absatz 7 Satz 1 sieht der Sache nach ein Verbot des Erhebens von Inhaltsdaten aus Telekommunikation von deutschen Staatsangehörigen, inländischen juristischen Personen und sich auf dem Bundesgebiet aufhaltenden Personen vor und entspricht damit den Vorgaben des BVerfG (vgl. BVerfG, a. a. O., Rn. 253, 260, 264 u. ö.). Missverständlich ist – wie in Absatz 1 – die Rede von „personenbezogenen Daten aus Telekommunikationsverkehren“. Die Sätze 2 bis 4 enthalten Anforderungen an den Einsatz technischer Filter und Löschungspflichten, die nicht zu beanstanden sind. Zu begrüßen ist, dass das Löschungsgebot nach den Sätzen 5 und 6 durchbrochen werden kann. Die materiellen Voraussetzungen hierfür müssten sich jedoch enger an den Anforderungen für die Individualüberwachung nach G 10 orientieren, um eine Umgehung von deren Voraussetzungen zu verhindern. Auch eine Benachrichtigungspflicht Betroffener nach dem Vorbild des § 12 G 10 müsste hier wohl geregelt werden. Die Entwurfsbegründung (S. 63) korrespondiert hier nicht mit dem Gesetztext.

gg) Zu Absatz 8

Die in Absatz 8 vorgesehene Beschränkung des Volumens von Maßnahmen der strategischen Ausland-Fernmeldeaufklärung auf 30 Prozent der Übertragungskapazität aller global bestehenden Telekommunikationsnetze erscheint als quantitative Begrenzung wenig geeignet. Die weltweit verfügbare Übertragungskapazität aller Telekommunikationsnetze ist einerseits in stetem Zunehmen begriffen und wird andererseits nie vollständig ausgeschöpft. Sie bietet damit keinen Anhalt für das tatsächliche Aufkommen an Telekommunikation. Der Gesetztext ist zudem so unscharf gefasst, dass er die Bezugsgröße der weltweiten Übertragungskapazität nicht erkennen lässt. Vorzugswürdig gegenüber einer – durch den Regelungsansatz faktisch nicht erfolgenden – Limitierung des für den BND verfügbaren Rohdatenstroms wäre eine prozentuale Beschränkung des nach der Relevanzanalyse zur weiteren Verarbeitung zur Verfügung stehenden Datenmaterials im Verhältnis zum durchschnittlichen täglichen Kommunikationsaufkommen (so bereits Löffelmann, in: Dietrich/Gärditz/Graulich/Gusy/Warg, Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 33, 40).

hh) Zu Absatz 9

Absatz 9 entspricht der bisherigen Regelung in § 6 Abs. 5 BNDG und ist nicht zu beanstanden.

ii) Zu Absatz 10

Die in Absatz 10 vorgesehene Kennzeichnungspflicht ist essenziell für die Bestimmung der Schwellen einer weiteren Verwendung, insbesondere Übermittlung erhobener Daten. In der Praxis dürfte sich das Problem stellen, dass eine klare Unterscheidung zwischen den Zwecken der politischen Unterrichtung und der Gefahrenfrüherkennung zumeist nicht möglich ist. Zwecke der Gefahrenfrüherkennung sind in aller Regel von so hoher außen- und sicherheitspolitischer Bedeutung, dass auch eine politische Unterrichtung der Regierung erforderlich ist. Das wird in den meisten Fällen der Datenerhebung zu Zwecken der Gefahrenfrüherkennung zu einer Doppelkennzeichnung führen. Besonders deutlich wird die geringe Praktikabilität dieser Differenzierung im Zusammenhang mit der Erhebung von Telekommunikationsmetadaten, die nicht gezielt zu einem der beiden Zwecke erfolgt und bei der eine Zuord-

nung erst im Nachhinein erfolgen kann (vgl. § 26 Abs. 2 BNDG-E, Begründung S. 74), was die unterschiedliche Ausgestaltung von Erhebungsschwellen insoweit sinnlos macht. Soll die Kennzeichnungspflicht nicht leer laufen, muss in Fällen der Doppelkennzeichnung gewährleistet sein, dass hinsichtlich der mit einer Kennzeichnung verbundenen Rechtsfolgen kein Wahlrecht der Behörde besteht, sondern sich die Rechtsfolgen nach dem engeren Zweck der Gefahrenfrüherkennung richtet. Gegenstand und Zweck der „Angabe des Mittels der Datenerhebung“ (Nr. 2) sind unklar und ergeben sich auch nicht aus der Entwurfsbegründung. Dass die Kennzeichnung – entgegen der üblichen Handhabung – bei Übermittlungen entfällt, erscheint nach der Begründung (S. 64) sachgerecht, relativiert aber zugleich den Sinn und die praktische Bedeutung der systematischen Unterscheidung zwischen politischer Unterrichtung und Gefahrenfrüherkennung.

b) Zu § 20 BNDG-E (besondere Formen der Ausland-Fernmeldeaufklärung)

aa) Zu Absatz 1

Die Rede von „personenbezogenen Telekommunikationsinhaltsdaten“ ist auch hier schief, zumal es (auch) um den Schutz von Institutionen, nicht (nur) um den natürlicher Personen geht. Warum sich der Verweis in Satz 1 nur auf Absatz 5 des § 19 bezieht, erschließt sich nicht; das würde dann Sinn machen, wenn es auch eine andere Form der gezielten Erhebung solcher Daten ohne Verwendung von Suchbegriffen gibt, die nicht eingeschränkt sein soll. Soweit die Entwurfsbegründung ausführt, Datenerhebungen nach Absatz 1 dürften „nur in Ausnahmefällen erfolgen, wenn die engen Voraussetzungen des Satzes 1 erfüllt werden“ (S. 65), trifft das in den Fällen der Gefahrenfrüherkennung nicht zu. Die Voraussetzungen sind hier identisch mit den allgemeinen Schwellen, d. h. es besteht nur eine materielle Begrenzung durch den Katalog der in § 19 Abs. 4 BNDG-E genannten Aufklärungsanlässe und die darauf bezogene erwartete Aufklärungsrelevanz der zu erhebenden Daten. Im Hinblick auf die Fälle der politischen Unterrichtung korrespondiert der Gesetztext unter Absatz 1 Satz 1 Nummer 2 nicht mit der Entwurfsbegründung, welche von weiteren Begrenzungen spricht, die im Normtext nicht auftauchen (S. 65). Eine substanzielle und sachgerechte Beschränkung besteht hier in der Begrenzung auf Daten über Vorgänge in Drittstaaten. In Satz 2 erscheint widersprüchlich, dass eine „gezielte Datenerhebung“ erst „nachträglich erkannt“ werden kann. Gezieltes Handeln ist teleologisch und damit voluntativ. Hinter der Formulierung dürfte der Umstand stehen, dass Suchbegriffe automatisiert gesteuert werden und deshalb nicht in jedem Einzelfall ein Erfassen von Daten der besonders schutzwürdigen Institutionen und Personen überprüft werden kann. Dann handelt es sich aber insoweit nicht um eine gezielte Datenerhebung, weshalb auf den Begriff „gezielt“ verzichtet werden sollte. Generell könnte die Norm deutlicher abbilden, wie die Unterscheidung – sofern ein Unterschied überhaupt besteht – zwischen dem allgemeinen und dem qualifizierten Schutzwürdigkeitsniveau (nur Vorgänge in Drittstaaten) technisch umgesetzt wird.

bb) Zu Absatz 2

Absatz 2 knüpft an die Forderung des BVerfG an, eine möglichst zielgerichtete Strukturierung des Überwachungsprozesses zu gewährleisten und bezeichnet bestimmte Personengruppen („Personen, die als mögliche Verursacher von Gefahren oder in Blick auf gegenüber ihnen zu ergreifende Folgemaßnahmen im unmittelbaren Interesse des Nachrichtendienstes

stehen“) als besonders schutzwürdig, so dass für sie ein eigener Schutzmechanismus vorzusehen sei (BVerfG, a. a. O., Rn. 187 f.). Einem solchen Mechanismus in Gestalt einer besonderen Verhältnismäßigkeitsabwägung unterstellt hiervon abweichend Nummer 1 „Verursacher von Gefahren im Sinne des § 19 Absatz 4“. Das kollidiert mit dem in § 19 Abs. 1 Nr. 2, Abs. 4 BNDG-E umgesetzten Konzept der Früherkennung, denn Voraussetzung für das Eingreifen der Beschränkung nach § 20 Abs. 2 Nr. 1 BNDG-E sind tatsächliche Anhaltspunkte dafür, dass erstens bereits eine Gefahr besteht und zweitens ihr Verursacher identifiziert werden kann. Beides widerspricht dem Gedanken des Aufklärens im Gefahrenvorfeld bzw. einer Bedrohungslage. Das BVerfG spricht daher bewusst von Personen, die als *mögliche* Verursacher von Gefahren im Fokus des Dienstes stehen, woran auch die Entwurfsbegründung anschließt (S. 65). Unter Nummer 2 erscheint die Formulierung „beabsichtigt“ etwas zu eng, die voraussetzt, dass zum Zeitpunkt der Datenerhebung bereits eine Absicht der Weitergabe zu Zwecken der Gefahrenabwehr oder Strafverfolgung und damit eine Kenntnis der Voraussetzungen für das Eingreifen der zuständigen Behörden besteht. Vorzugswürdig wäre hier die weichere Formulierung „in Betracht kommt“.

cc) Zu Absatz 3

Absatz 3 dient der Abgrenzung der strategischen Fernmeldeaufklärung gegenüber einer Individualaufklärung. Auch bei einer Individualüberwachung nach G 10 werden aber selten alle Telekommunikationsmerkmale einer Person und damit der gesamte sie betreffende Telekommunikationsverkehr überwacht, schon weil oft nicht alle Merkmale der Zielperson bekannt sind oder sie Merkmale anderer Personen benutzt. Damit enthält die Regelung in Absatz 3 kein substanzielles Abgrenzungskriterium. Im Umkehrschluss kann daraus sogar eine Befugnis zur gezielten Überwachung des vollständigen ein Telekommunikationsmerkmal betreffenden Telekommunikationsverkehrs einer Person, also eine Befugnis zur Individualaufklärung entnommen werden. Auf diesen Anwendungsfall weist auch die Entwurfsbegründung hin (S. 65). Die engeren Voraussetzungen des G 10 wären dann bedeutungslos. Absatz 3 müsste daher durch Einfügen der Worte „ein Telekommunikationsmerkmal betreffenden“ vor dem Wort „Telekommunikationsverkehrs“ enger gefasst werden.

c) Zu § 21 BNDG-E (Schutz von Vertraulichkeitsbeziehungen)

aa) Zu Absatz 1

Dass § 21 BNDG-E Regelungen zum Schutz von Vertraulichkeitsbeziehungen vorsieht, entspricht den Vorgaben des BVerfG und ist grundsätzlich zu begrüßen. Allerdings begnügt sich der Gesetzentwurf damit, vom BVerfG angedeutete Eckpunkte zu übernehmen und nutzt nicht den zur Verfügung stehenden gesetzgeberischen Gestaltungsspielraum. Die Anbindung des Vertraulichkeitsschutzes an § 53 StPO, der auf strafprozessuale Sachverhalte zugeschnitten ist, im Recht der Nachrichtendienste ist schon aus sich heraus schief, weil es dort keine Zeugnispflicht und keine Zeugnisverweigerungsrechte gibt. Hinzu kommt, dass die Ausgestaltung des § 53 StPO selbst dogmatisch hoch umstritten ist und ein methodisches Konzept nicht erkennen lässt (vgl. zur Kritik bereits Löffelmann, in: Dietrich et al, a. a. O., S. 33, 42 f.; ders., BayVBl. 2017, 253, 255; vgl. auch Gärditz, JZ 2020, 825, 831: „dysfunktional hölzerne Zeugnisverweigerungsrechte“). Im hiesigen Kontext stellt sich z. B. die Frage, warum Ärzte, deren Tätigkeit das BVerfG im Einzelfall dem Kernbereich privater Lebensgestal-

tung des Patienten zuordnet (vgl. BVerfGE 32, 373, 380; 109, 279, 322 f.) nicht erfasst sind. Generell ist ein auf die Besonderheiten des Nachrichtendienstrechts zugeschnittenes Schutzkonzept erforderlich (vgl. auch Löffelmann, GSZ 2019, 190, 193 ff.; zu einem konkreten Regelungsvorschlag die Änderungsanträge der Fraktion der SPD in den beiden jüngsten Gesetzgebungsverfahren zum BayVSG, Bayerischer Landtag, Drs. 17/11610, 2, 20 ff. und 17/21807). Im hier gegebenen auslandsbezogenen Kontext kommt hinzu, dass der Gestaltungsspielraum des Gesetzgebers nochmals weiter ist und „den verschiedenen Umständen, unter denen die Presse oder Anwaltschaft in anderen Ländern tätig ist“ Rechnung tragen kann (BVerfG, a. a. O., Rn. 196). Das BVerfG spricht insoweit als Orientierungshilfen ausdrücklich von den „sich aus den Grundrechten des Grundgesetzes ergebenden Wertentscheidungen, die ihrerseits in die internationalen Verbürgungen der Menschenrechte eingebettet sind“ (a. a. O.). Ein solcher Bezug zum Völkerrecht fehlt hier vollständig. Für die Rechtsanwendung wären ferner Auslegungshilfen erforderlich, unter welchen Umständen eine Person im Ausland als Rechtsanwalt oder Journalist zu qualifizieren ist.

Von der Möglichkeit eines Absehens des Schutzes von Vertraulichkeitsbeziehungen im Zusammenhang mit dem Zweck der politischen Unterrichtung (vgl. BVerfG, a. a. O., Rn. 198) macht der Entwurf keinen Gebrauch, verwirklicht den Schutz von Vertraulichkeitsbeziehungen insoweit also in überobligatorischer Weise.

bb) Zu Absatz 2

Die in Absatz 2 vorgesehene Ausnahme vom Verbot der Datenerhebung aus Vertraulichkeitsbeziehungen ist grundsätzlich zu begrüßen, die dort verwendeten Schwellen der strafrechtlichen Verstrickung oder Verhinderung einer Gefahr aber insoweit systemfremd als hier wieder nicht das Gefahrenvorfeld oder eine Bedrohungslage, sondern das bereits eröffnete repressive oder präventiv-polizeiliche Handlungsspektrum in Bezug genommen wird. Das BVerfG spricht in diesem Zusammenhang in einem weiteren Sinne davon, dass „Erkenntnisse über schwerwiegende und sich konkret abzeichnende Gefahren gewonnen werden“ können (BVerfG, a. a. O., Rn. 195).

cc) Zu Absatz 3

Die Regelung ist nicht zu beanstanden.

d) Zu § 22 BNDG-E (Kernbereichsschutz)

Die Regelung zum Kernbereichsschutz ist vorbildlich ausgestaltet. Eine gesetzliche Regelung, dass der präventive Kernbereichsschutz bereits informationstechnisch durch die Auswahl der Suchbegriffe zu gewährleisten sei (vgl. BVerfG, a. a. O., Rn. 206), ist entbehrlich, da kernbereichsrelevantes Verhalten in aller Regel keine Informationen von außen- und sicherheitspolitischer Bedeutung vermittelt, auf deren Erhebung die Auswahl der Suchbegriffe zielt.

e) Zu § 23 BNDG-E (Anordnung)

Die Regelung des Anordnungsverfahrens in § 23 BNDG-E ist im Grundsatz nicht zu beanstanden.

Verwerfungen können sich möglicherweise ergeben, soweit nach Absatz 5 Satz 2 eine Anordnung bei Vorliegen einer Beschränkungsanordnung nach dem G 10 entbehrlich ist. Ob das G 10 überhaupt auf das Erfassen der Telekommunikation von Ausländern im Ausland ausgelegt ist und insoweit eine Befugnis vermitteln kann, ist ungeklärt. Bislang gingen der Gesetzgeber und die Rechtsanwendung davon aus, dass damit kein Grundrechtseingriff verbunden sei. § 1 Abs. 1 Nr. 2 G 10 bezieht sich auf § 1 Abs. 2 BNDG, der in Satz 2 die Datenerhebung des BND im Bundesgebiet regelt. Die Individualüberwachung nach § 3 G 10 erlaubt nur die Überwachung der Telekommunikation bestimmter natürlicher Personen (§ 3 Abs. 2 S. 2 G 10), besitzt also keinen Anwendungsbereich hinsichtlich der Überwachung von Institutionen, die § 23 Abs. 5 Nr. 1 BNDG-E bezeichnet. Die strategische Überwachung nach § 5 G 10 wiederum darf nur den grenzüberschreitenden Telekommunikationsverkehr erfassen und unterliegt spezifischen Voraussetzungen, die sich von denen des § 19 BNDG-E unterscheiden. Vor diesem Hintergrund erscheint es vorzugswürdig, keine Substituierung einer Anordnung nach § 23 BNDG-E durch eine solche nach dem G 10 vorzusehen.

Regelungstechnisch könnte die Wiederholung des Absatzes 4 in Absatz 7 durch einen Verweis ersetzt werden. Absatz 7 Satz 3 ist mit Blick auf Satz 5 redundant.

f) Zu § 24 BNDG-E (Eignungsprüfung)

In Absatz 2 erschließt sich nicht, weshalb lediglich die Prüfung der Geeignetheit von Telekommunikationsnetzen nach Absatz 1 Nummer 1 dem Erfordernis tatsächlicher Anhaltspunkte und einer Befristung unterliegt. Für die Eignungsprüfung von Suchbegriffen sind keine über die Erforderlichkeit hinausgehenden Voraussetzungen vorgesehen. Die Kernbereichsregelung in Absatz 5 durch Bezugnahme auf das BSIG ist sachgerecht und schließt eine bislang bestehende Regelungslücke (vgl. Löffelmann, in: Dietrich/Eiffler, a. a. O., Teil VI § 4 Rn. 186). Die Ausnahmen für die Weiterverarbeitung von erhobenen Daten außerhalb der Eignungsprüfung nach Absatz 7 beherbergen die Gefahr, dass im Gewand der Eignungsprüfung außerhalb der sonstigen formellen und materiellen Voraussetzungen für eine strategische Auslands-Fernmeldeaufklärung systematische Datenerhebungen zu anderen Zwecken durchgeführt werden können. Die Darstellung des systemischen Bedarfs an solchen Daten für Auslandseinsätze der Bundeswehr in der Entwurfsbegründung (S. 80) stützt diesen Eindruck. Eine solche systematische Datenerhebung sollte deshalb auf die Fälle des § 19 BNDG-E beschränkt sein, von denen auch Belange der Bundeswehr umfasst sind. Andererseits sind die in der Entwurfsbegründung genannten praktischen Probleme eines solchen regulären Vorgehens nicht von der Hand zu weisen, was letzten Endes die Impraktikabilität der verfassungsgerichtlichen Vorgaben für Zwecke der Auslandsüberwachung illustriert.

g) Zu § 25 BNDG-E (Mitwirkungspflichten)

Die Regelung entspricht im Wesentlichen § 8 BNDG in der geltenden Fassung sowie den Parallelvorschriften für Überwachungsmaßnahmen nach dem G 10 und ist nicht zu beanstanden.

h) Zu § 26 BNDG-E (Verarbeitung von Verkehrsdaten)

Soweit die Vorschrift zwischen Verkehrsdaten (Absatz 1) und personenbezogenen Verkehrsdaten (Absatz 3) differenziert, findet diese Unterscheidung in der Rechtsprechung des BVerfG zu Art. 10 GG keine Stütze (vgl. auch die Ausführungen zu § 19 Abs. 1 BNDG-E). Verkehrsdaten sind durch das Fernmeldegeheimnis geschützt, sofern sie auf einen individuellen Kommunikationsvorgang einer natürlichen Person bezogen sind (vgl. BVerfGK 9, 62, 74 ff.; BVerfG NJW 2016, 3508, 3509 f. m. w. N.). Die Darstellung in der Entwurfsbegründung (S. 73), „personenbezogene Verkehrs- und Metadaten, die nicht im Zusammenhang mit einer Individualkommunikation stehen“ unterfielen nicht dem Schutzbereich des Fernmeldegeheimnisses, ist daher zumindest missverständlich. § 26 Abs. 1 S. 2 BNDG-E erlaubt durch den Verweis auf § 19 Abs. 6 S. 1 und 2 BNDG-E auch die Online-Durchsuchung beim ausländischen Telekommunikationsanbieter und erscheint unter Verhältnismäßigkeitsgesichtspunkten nicht unbedenklich.

Im Übrigen sind die in der Entwurfsbegründung (S. 74 - 76) ausführlich dargestellten praktischen Bedarfe für eine Verarbeitung von Telekommunikationsverkehrsdaten auch deutscher Staatsangehöriger, inländischer juristischer Personen und sich im Bundesgebiet aufhaltender Personen gut nachvollziehbar. Fraglich ist aber, ob diesem Bedarf die komplizierte Regelungstechnik mit Verarbeitungsbefugnis (Absatz 1), Teilausnahme (Absatz 3 Satz 1), differenzierten Gegenausnahmen (Absatz 3 Satz 2) und an diese teilweise anschließende Verfahrensregelungen (Absatz 3 Satz 3 und 4) gerecht wird. Das BVerwG hat in seinen beiden Entscheidungen zur Speicherung und Verarbeitung von Verkehrsdaten moniert, dass hierfür keine gesetzliche Grundlage bestehe (BVerwG, U. v. 13.12.2017, 6 A 6.16 und 6 A 7.16, jew. Rn. 28 ff.). Die Notwendigkeit einer Beschränkung auf Metadaten, die nicht dem Art. 10 GG unterfallen oder eine Anonymisierung der Daten hat es nicht gefordert. Vor diesem Hintergrund wäre auch die Schaffung einer Befugnis zur Verarbeitung nicht anonymisierter Verkehrsdaten deutscher Staatsangehöriger, inländischer juristischer Personen und sich im Bundesgebiet aufhaltender Personen grundsätzlich denkbar. Dabei müsste freilich darauf geachtet werden, dass die Verarbeitungszwecke ausreichend eng gesetzlich (wie in der Entwurfsbegründung dargestellt) definiert werden, damit es sich nicht um eine unzulässige anlasslose und nicht zweckgebundene Speicherung von Verkehrsdaten „auf Vorrat“ handelt (vgl. BVerfGE 125, 260 ff.).

Die in Absatz 5 Satz 1 bezeichnete Höchstspeicherfrist erscheint aufgrund des Auslandsbezugs der Maßnahme unbedenklich. Die in Satz 2 vorgesehene Ausnahme ist jedoch zu weit, da als „erforderlich“ auch eine längere Bevorratung der Rohdaten angesehen werden kann. Das bloße Merkmal der Erforderlichkeit ist angesichts der dezidierten Vorgaben des BVerfG (BVerfG, a. a. O., Rn. 191 m. d. H. a. BVerfGE 125, 260, 322) zu unscharf, um eine weitere Speicherung des Datenvorrats zu legitimieren. Weniger riskant wäre es, wenn sich die Ausnahmeregelung auf das nach der Relevanzprüfung verbleibende Datenmaterial bezieht.

i) Zu § 27 BNDG-E (Auswertung und Prüfpflichten)

Die Vorschrift betrifft die zulässige Speicherdauer der aus dem Rohdatenstrom erhobenen oder ausgefilterten, aber noch keiner ergiebigen Relevanzprüfung unterzogenen Inhaltsdaten. Die Formulierung von Absatz 1 Satz 1 ist insoweit missverständlich, als sie den Schluss

zulassen könnte, dass nach einer erfolglosen Relevanzprüfung der ausgefilterte Rohdatenstrom weiter gespeichert werden darf und lediglich in siebenjährigen Abständen einer erneuten Prüfung zu unterziehen sei. Eine derartige langjährige, gegebenenfalls zeitlich unbegrenzte „Vorratsspeicherung“ von Telekommunikationsinhaltsdaten wäre mit den verfassungsrechtlichen Anforderungen an Löschungspflichten (BVerfGE 100, 313, 364 f.) nicht zu vereinbaren. Es wäre daher vorzugswürdig, die Formulierung „und sodann regelmäßig in Abständen von höchstens sieben Jahren“ in Satz 1 zu streichen. In einem eigenen Absatz 2 könnte dann geregelt werden, dass die nach der Relevanzprüfung verbleibenden Daten regelmäßig in Abständen von höchstens sieben Jahren auf ihre weitere Erforderlichkeit zu prüfen sind und ggf. die Löschungsvorschriften nach Absatz 1 entsprechend gelten.

Nicht unproblematisch erscheint weiter, dass § 27 BNDG-E wie bislang schon § 4 Abs. 1 G 10 nur zur Überprüfung und ggf. Löschung der personenbezogenen Daten verpflichtet. Danach können relevante Daten ohne Personenbezug weiterhin als Sachinformationen vorrätig gehalten werden (so Huber, in: Schenke/Graulich/Ruthig, a. a. O., § 12 G 10 Rn. 8). Ungeachtet des Umstands, dass Art. 10 GG nicht zwischen Telekommunikationsdaten mit und ohne Personenbezug unterscheidet, wurde diese Praxis und einfachrechtliche Einschränkung der Überprüfungs- und Löschungspflicht bislang als zulässig angesehen (so auch Löffelmann, in: Dietrich/Eiffler, a. a. O., Teil VI § 4 Rn. 72). In seiner VERAS-Entscheidung hat das BVerwG aber die Anonymisierung der erhobenen Telekommunikationsdaten gerade nicht als einen Umstand gewertet, der einen Grundrechtseingriff ausschließt (BVerwG, U. v. 13.12.2017, 6 A 6.16, Rn. 23, 27). Vor diesem Hintergrund sollte die Begrenzung der Überprüfungs- und Löschungspflicht auf personenbezogene Daten nochmals eingehend auf ihre Verfassungsmäßigkeit geprüft werden. Auch könnte darüber nachgedacht werden, wenigstens kompensatorisch die gerichtsähnliche Kontrolle durch den Unabhängigen Kontrollrat auf die Prüfung der weiteren Erforderlichkeit der Daten und ggf. ihre Anonymisierung zu erstrecken. Das läge dann auf einer Linie mit der quasi-gerichtlichen Kontrolle der Zurückstellung der Benachrichtigungspflichten durch die G 10-Kommission nach § 12 Abs. 1 S. 2 bis 5, Abs. 2 G 10.

j) Zu § 28 BNDG-E (Datenerhebung ausländischer öffentlicher Stellen)

Die Regelung ist nicht zu beanstanden.

k) Zu §§ 29 und 30 BNDG-E (Datenübermittlung)

§ 29 BNDG-E enthält äußerst detaillierte Vorschriften zur Übermittlung von durch eine strategische Ausland-Fernmeldeaufklärung erhobene Daten an inländische Stellen. Diese Regelungen begegnen in mehrfacher Hinsicht Einwänden:

Der in Absatz 1 Nummer 1 und weiter mehrfach verwendete unbestimmte Rechtsbegriff „besonders gewichtige Rechtsgüter“, welcher Entscheidungen des BVerfG entnommen wurde (vgl. etwa BVerfG, a. a. O., Rn. 174, 313), ist bislang weder durch eine ständige Rechtsprechung konkretisiert noch lässt sich sein Umfang dem Gesetz entnehmen. Der erläuternde Hinweis in der Entwurfsbegründung, es müsse sich bei diesen Rechtsgütern „um solche handeln, die als gewichtig anzuerkennen sind“ (S. 80), illustriert anschaulich diese Unbe-

stimmtheit. In Absatz 2 und entsprechend in Absatz 4, der darauf verweist, bestehen Bedenken, ob die Sammelbezeichnung „andere inländische öffentliche Stellen“ der vom BVerfG geforderten präzisen und normenklaren Regelung der Übermittlungsanlässe und Empfängerbehörden genügt (vgl. BVerfG, a. a. O., Rn. 316 zu ausländischen öffentlichen Stellen; BVerfG, B. v. 27.5.2020, 1 BvR 1873/13 u. a., Rn. 133 f., 145). Außerdem erschließt sich nicht, warum Absatz 1 eine die Nachrichtendienste „privilegierende Vorschrift“ darstellen soll (so S. 78), wenn die Übermittlungsbefugnis zur politischen Unterrichtung an andere Stellen in Absatz 2 identisch ausgestaltet ist. Da ohnehin nicht jeder anderen öffentlichen Stelle die Aufgabe der Unterrichtung der Bundes- oder einer Landesregierung zukommt, wäre es sinnvoll, die Aufgabe der politischen Unterrichtung bei einer Stelle – auf Landesebene etwa den Landesämtern für Verfassungsschutz – zu bündeln. Erst recht gilt dieser Einwand für den Verwendungszweck der Gefahrenabwehr in Absatz 4 und Absatz 7 sowie des Verfassungsschutzes in Absatz 6. Die letztgenannte Befugnis wie auch die Übermittlungsbefugnis zur Gefahrenabwehr in Absatz 7 Satz 2 ist nicht einmal auf öffentliche Stellen beschränkt, sondern bezeichnet pauschal „andere inländische Stellen“ – also auch private – als Übermittlungsempfänger. Die Aufgaben der Gefahrenabwehr und des Verfassungsschutzes werden aber nicht schlechthin von „anderen inländischen Stellen“, sondern von Behörden mit spezifischem Aufgabenzuschnitt wahrgenommen. Für eine Übermittlung an nicht-öffentliche Stellen im Inland ist schon kein Bedarf erkennbar (vgl. S. 81). Die Übermittlungsbefugnisse in den Absätze 2, 4, 6 und 7 sollten daher auf konkrete Empfänger spezifiziert werden. Im Hinblick auf die Datenübermittlung an die Bundeswehr nach Absatz 5 stellt sich die Frage, ob für die empfangende Stelle eine Abfragebefugnis geschaffen werden muss. Die Zweckänderungsbefugnis in Absatz 7, desgleichen die Durchbrechung des Vertraulichkeitsschutzes in Absatz 8 und die Erweiterung der Zweckänderungsbefugnis in Absatz 12 Satz 6 sind sinnvoll und zu begrüßen. In Absatz 9 Satz 2 ist unklar, was unter einer „erheblichen Gefahr“ zur verstehen ist. Die Feststellung in Absatz 11 Satz 1, dass der BND die „Verantwortung“ für die Zulässigkeit der Übermittlung trägt, drückt - ungeachtet der Frage, was damit überhaupt gemeint ist – eine datenschutzrechtliche Selbstverständlichkeit aus. Satz 2 weicht von dieser Selbstverständlichkeit aus nicht nachvollziehbaren Gründen ab, was mitnichten „allgemeinen datenschutzrechtlichen Grundsätzen“ entspricht (so S. 82): Datenschutzrechtlich trägt immer der die Verantwortung für die Übermittlung, dem die Befugnis hierzu eingeräumt wird (vgl. zur – ungeklärten – Parallelproblematik bei der Bestandsdatenauskunft Petri, ZD 2020, 588, 589).

Insgesamt vermögen die unübersichtlichen Regelungen zur Datenübermittlung im Inland nicht zu überzeugen und unterstreichen den Befund, dass ein übergreifendes Ordnungssystem für den Datentransfer im Sicherheitsrecht dringend benötigt wird (vgl. bereits Löffelmann, Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschussdrucksache 19(4)696 B, S. 15 f.).

§ 30 BNDG-E (Datenübermittlung an ausländische Stellen) ist demgegenüber nicht zu beanstanden. Anders als bei § 29 BNDG-E kann bei Übermittlungen ins Ausland ein Bedarf zur Weitergabe von Daten an nicht-öffentliche Stellen erkannt werden (Absatz 4, Absatz 5 Satz 2). Eine nähere Bezeichnung der empfangenden Stellen ist hier nicht möglich. Die Übermittlungsverbote nach Absatz 6 entsprechen den Vorgaben des BVerfG und sind angemessen und praktikabel ausgestaltet. Die Übermittlungsbefugnis bezüglich Daten, die zur politischen Unterrichtung gewonnen wurden, ist in Absatz 8 den Vorgaben des BVerfG folgend (BVerfG,

a. a. O., Rn. 228) auf wenige Ausnahmetatbestände beschränkt, was freilich strukturelle Probleme verursacht (vgl. bereits Dietrich, GSZ 2020, 173, 180).

l) Zu § 31 BNDG-E (Kooperationen mit ausländischen öffentlichen Stellen)

aa) Zu Absatz 1

Soweit Absatz 1 bestimmt, dass im Rahmen von Kooperationen *auch* personenbezogene Daten nach den §§ 32 und 33 BNDG-E verarbeitet werden dürfen, wird der Anwendungsbereich des § 31 BNDG-E und sein Verhältnis zu den beiden anderen Vorschriften nicht deutlich. Dem Wortlaut nach dürfen im Rahmen von Kooperationen nicht nur Daten nach §§ 32, 33 BNDG-E verarbeitet werden, sondern auch andere Daten. Welche das sind und welche Regelungen für sie gelten, ist nicht erkennbar.

bb) Zu Absatz 2

Die Regelung in Absatz 2 setzt die Vorgaben des BVerfG (a. a. O., Rn. 249) zu den Schutzpflichten des deutschen Staates im Inland um. In diesem Zusammenhang ist darauf hinzuweisen, dass aufgrund des Personalprinzips besondere Schutzpflichten auch gegenüber deutschen Staatsangehörigen im Ausland bestehen. Es sollte geprüft werden, ob das eine Erstreckung der Norm auf Überwachungsmaßnahmen im Rahmen einer Kooperation gebietet, die im Ausland erfolgen, insbesondere um sicherzustellen, dass keine Daten deutscher Staatsangehöriger erfasst werden.

cc) Zu Absatz 3

Das BVerfG knüpft die Zulässigkeit von Kooperationen – worauf auch die Entwurfsbegründung zutreffend hinweist (S. 86 f.) – an das Bestehen von „Erkenntnisinteressen ausländischer Dienste und Staaten“, die „mit einem legitimen Aufklärungsinteresse des Bundesnachrichtendienstes vergleichbar“ sein müssen (BVerfG, a. a. O., Rn. 247). Absatz 3 soll nach der Entwurfsbegründung diese Voraussetzung regeln, enthält aber keinerlei Bezüge zu Erkenntnisinteressen ausländischer Dienste und Staaten.

dd) Zu Absatz 4

Absatz 4 trägt der verfassungsgerichtlichen Vorgabe Rechnung, dass „(f)ür jede der gemeinsam durchgeführten Überwachungsmaßnahmen (…) die Vergewisserung jeweils einmal sicherzustellen“ sei (BVerfG, a. a. O., Rn. 253; ähnlich Rn. 261). Die Möglichkeit von Rahmenvereinbarungen, auf die die Entwurfsbegründung (S. 87) hindeutet, erachtet das BVerfG als zulässig (BVerfG, a. a. O., Rn. 253). Missverständlich ist allerdings, dass Absatz 1 hiervon abweichend an den engeren Begriff der „strategischen Ausland-Fernmeldeaufklärung“ anknüpft, nicht an den der „strategischen Aufklärungsmaßnahme“ (§ 19 Abs. 1 und 2 BNDG-E). Das könnte die Notwendigkeit einer maßnahmenspezifischen Zusicherung nahelegen. Soweit Absatz 4 Nummer 3 Buchstaben c) und d) Zusicherungen bei der unbeabsichtigten Verarbeitung von Daten aus einer Vertraulichkeitsbeziehung und aus dem Kernbereich privater Lebensgestaltung vorsehen, enthält dies außerdem keine – vom BVerfG geforderte (BVerfG, a. a. O., Rn. 257) – Einschränkung der *gezielten* Erfassung solcher Daten und eine darauf bezogene Zusicherung.

dd) Zu Absatz 5

Nach der Entwurfsbegründung (S. 88) dient Absatz 5 der Umsetzung der Vorgaben des BVerfG (a. a. O., Rn. 253), dass Kooperationen im Rahmen der strategischen Ausland-Fernmeldeaufklärung nur zum Schutz hochrangiger Rechtsgüter zulässig seien. Die Begründung führt weiter aus, eine Kooperation sei „nur zur Früherkennung der in den Nummern 1 bis 10 genannten sowie vergleichbaren (Nummer 11) Gefahren zulässig“. Der Katalog des Absatzes 5 bezieht sich aber nicht ausschließlich auf Gefahrenbereiche als Kooperationszwecke, etwa unter den Ziffern 6, 7, 9 und 11. Andererseits enthält der Katalog die Anlassgefahren gem. § 19 Abs. 4 Nr. 1 Buchst. g) und h) BNDG-E nicht. Warum der Katalog von dem des § 19 Abs. 4 BNDG-E in Inhalt und Ordnung abweicht, ist ebenfalls nicht nachzuvollziehen und erscheint ausgesprochen impraktikabel. Vorzugswürdig wäre hier eine Bezugnahme auf und ggf. Ergänzung der vorgenannten Vorschrift.

m) Zu §§ 32 und 33 BNDG-E (Verarbeitung von selektierten und unselektierten Daten)

Der Anwendungsbereich der §§ 32 und 33 BNDG-E ist aus dem Gesetz heraus und auch unter Hinzuziehung der Entwurfsbegründung kaum zu erschließen. Das BVerfG differenziert in seiner Entscheidung zwischen sechs Arten des Datenaustausches im Rahmen einer Kooperation und fordert jeweils spezifische Regelungen: 1. die Einräumung der Befugnis an den Partnerdienst, im Inland selbst Überwachungsmaßnahmen vorzunehmen (BVerfG, a. a. O., Rn. 249, geregelt in § 31 Abs. 2 BNDG-E); 2. die Übermittlung von Suchbegriffen durch den BND an den Partnerdienst zum Zwecke der Erlangung und Nutzung der durch diesen zur Verfügung gestellten Datenströme durch den BND (BVerfG, a. a. O., Rn. 250); 3. die Entgegennahme der durch den Partnerdienst zur Verfügung gestellten Datenbestände zur eigenen Auswertung durch den BND ohne vorherige Übermittlung von Suchbegriffen (BVerfG, a. a. O., Rn. 250); 4. die Durchführung von Überwachungsmaßnahmen durch den BND im Interesse und unter Anleitung von Partnerdiensten unter Verwendung von diesen zur Verfügung gestellter Suchbegriffe und automatisierter Übermittlung der Überwachungsergebnisse an die Partnerdienste (BVerfG, a. a. O., Rn. 251, 254 ff.); 5. die Durchführung von Überwachungsmaßnahmen durch den BND im Interesse und unter Anleitung von Partnerdiensten unter Verwendung von diesen zur Verfügung gestellter Suchbegriffe und automatisierter Übermittlung nicht oder nur teilweise ausgewerteter Überwachungsergebnisse an die Partnerdienste (BVerfG, a. a. O., Rn. 259 ff.). 6. die Durchführung von Überwachungsmaßnahmen durch den BND im Interesse und unter Anleitung von Partnerdiensten ohne Verwendung von diesen zur Verfügung gestellter Suchbegriffe und unter automatisierter Übermittlung unselektierter Überwachungsergebnisse in Form von Verkehrsdaten an die Partnerdienste (BVerfG, a. a. O., Rn. 251, 262 ff.).

§ 32 BNDG-E betrifft offenbar Fallgruppe 4, spricht aber missverständlich von der „Verarbeitung selektierter personenbezogener Daten“ und nicht von deren durch den BND zu leistender Selektierung anhand zur Verfügung gestellter Suchbegriffe. Die Vorschriften in Absatz 1 Satz 3 und Absätzen 3 bis 8 zur Gewährleistung der vom BVerfG geforderten „sorgfältigen Kontrolle der für den Partnerdienst eingesetzten Suchbegriffe sowie der hieran anknüpfenden Trefferfälle“ (BVerfG, a. a. O., Rn. 255 ff.) erscheinen trotz ihrer recht detaillierten Ausgestaltung nicht ausreichend. Die Vorgaben des BVerfG, insbesondere zur möglichen Kon-

trolle anhand von Listen gefährdeter Personen (BVerfG, a. a. O., Rn. 256), zeigen, dass die Schutzvorkehrungen materiell und prozessual über das allgemein gebotene Maß hinausgehen müssen. Der Gesetzentwurf setzt zwar die Vorgaben zu einem automatisierten und anschließenden manuellen Prüfverfahren sowohl hinsichtlich der Suchbegriffe als auch der Treffer in den Absätzen 3 bis 8 sachgerecht um. Alle Prüfmechanismen beziehen sich aber lediglich auf Vertraulichkeitsbeziehungen nach § 21 Abs. 1 S. 2 BNDG-E und nicht auf besonders gefährdete Personen (etwa Dissidenten, Regimegegner o. ä.). Unzureichend dürfte ferner die externe prozessuale Kontrolle ausgestaltet sein. Das BVerfG verlangt eine „gerichtsähnliche Vorabkontrolle“, welche „möglichst wirksam ausgestaltet werden“ muss (BVerfG, a. a. O., Rn. 257 a. E., 258). Die Vorabkontrolle durch den Unabhängigen Kontrollrat bezieht sich nach § 42 BNDG-E aber gerade nicht auf Kooperationen nach § 32 BNDG-E. Ferner erschließt sich nicht, warum für diese Konstellation nicht die mengenmäßige Begrenzung nach § 19 Abs. 8 BNDG-E gilt, auf die sich § 32 Abs. 1 S. 3 BNDG-E nicht bezieht. Schließlich ist dem Gesetzentwurf nicht zu entnehmen, ob und mit welchem Ergebnis die Bundesregierung geprüft hat, wieweit Zusicherungen im Rahmen einer Kooperation „auch durch Auskunftsrechte oder Mitteilungspflichten sowie auch durch Kommunikations- und Einwirkungsregelungen – wie etwa ein Löschungsverlangen – flankiert werden können“ (BVerfG, a. a. O., Rn. 261). Diese Prüfung sollte im weiteren Gesetzgebungsverfahren vorgenommen und dokumentiert werden.

§ 33 BNDG-E betrifft demgegenüber offenbar die oben als Fallgruppe 6 bezeichnete Konstellation. Die Vorschrift setzt die Vorgaben des BVerfG zum Bestehen eines qualifizierten Aufklärungsinteresses (BVerfG, a. a. O., Rn. 263) grundsätzlich sachgerecht um; lediglich bei dem Aufklärungsanlass gem. § 33 Abs. 2 S. 2 Nr. 5 BNDG-E (Desinformationskampagnen) ist fraglich, ob ein mit den anderen Anlässen vergleichbares Gewicht vorliegt. § 33 BNDG-E enthält zwar durch den Kettenverweis in Absatz 1 auf § 31 Abs. 1 S. 2 und § 19 Abs. 7 S. 1 bis 4 BNDG-E das vom BVerfG geforderte (BVerfG, a. a. O., Rn. 263) Gebot des Ausfilterns von Daten von deutschen Staatsangehörigen und Inländern, nicht jedoch ein solches zum Ausfiltern von Daten aus Vertraulichkeitsbeziehungen, wie vom BVerfG ebenfalls verlangt (a. a. O.). Außerdem erscheinen auch hier Vorkehrungen zum Schutz besonders gefährdeter Personen sachgerecht.

Zu der oben unter Fallgruppe 5 bezeichneten Konstellation, dass Inhaltsdaten unselektiert oder nur teilselektiert weitergegeben werden, enthält der Gesetzentwurf keine Regelung. Eine derartige Kooperation ist folglich unzulässig, was klargestellt werden sollte.

n) Zu §§ 34 bis 39 BNDG-E (Eingriffe in informationstechnische Systeme)

Die §§ 34 bis 39 BNDG-E betreffen über den Entscheidungsgegenstand des Urteils des BVerfG vom 19.5.2020 hinaus die Einführung eines neuen nachrichtendienstlichen Mittels, das bislang im Bereich der Nachrichtendienste nur vom bayerischen Landesamt für Verfassungsschutz genutzt werden kann (Art. 10 i. V. m. Art. 9 BayVSG; dazu ausf. Löffelmann, in: Dietrich/Eiffler, a. a. O., Teil VI § 5 Rn. 28 ff.): der heimliche Eingriff in informationstechnische Systeme („Online-Durchsuchung“). Aus Sicht der sicherheitsrechtlichen Praxis ist die Schaffung dieser Befugnis gerade im Tätigkeitsbereich des Auslandsnachrichtendienstes nachdrücklich zu begrüßen, da es sich um ein sehr wirksames Instrument der Informations-

beschaffung handelt, den Nachrichtendiensten keine aktionellen Befugnisse zustehen und im Übrigen die Informationsbeschaffung im Ausland erheblichen faktischen Schwierigkeiten unterliegt. Andererseits handelt es sich um ein äußerst eingriffsintensives Instrument. Unter Verhältnismäßigkeitsgesichtspunkten erscheint sein Einsatz im Ausland als deutlich besser legitimierbar als im Inland.

Die einfachrechtliche Ausgestaltung der Befugnis folgt im Wesentlichen den in anderen Bereichen des Sicherheitsrechts bereits bestehenden Regelungsvorbildern (vgl. § 49 BKAG, Art. 45 BayPAG, § 31c POG RP, § 100b StPO). Hinsichtlich der materiellen Anordnungsvoraussetzungen verlangt das BVerfG, dass die Maßnahme der Abwehr von Gefahren für „überragend wichtige Rechtsgüter“ dienen muss (BVerfGE 120, 274, 328). Da im Zusammenhang mit Auslandssachverhalten aber die Anforderungen an Eingriffsschwellen abgesenkt werden können (zutreffend Entwurfsbegründung S. 92), erscheint es vertretbar, dass die besonderen Anlässe nach § 34 Abs. 1 BNDG-E eine ausreichend enge Einhegung darstellen. Hinzu kommt, dass nach der Entwurfsbegründung (S. 92, 93) Zielobjekte in der Regel *hoheitliche* informationstechnische Anlagen sind, welche nicht dem Schutz der Grundrechte unterfallen. Letzten Endes lässt sich diese Verhältnismäßigkeitsfrage anhand des vorliegenden singulären Judikats des BVerfG zur Auslandsgeltung von Grundrechten nicht verlässlich beantworten und obliegt es der Einschätzungsprärogative des Gesetzgebers, welches Gewicht er den mit der Befugnis verfolgten hoheitlichen Zwecken beimisst.

In formeller Hinsicht erscheint der Prüfzeitraum nach § 34 Abs. 7 BNDG-E von drei Jahren deutlich zu lang. Hierdurch wird de facto eine dreijährige „Vorratsdatenspeicherung“ hoch sensibler Daten ermöglicht. Die Prüfdauer sollte sich mit der – ohnehin langen – Anordnungsdauer nach § 37 Abs. 3 BNDG-E decken. Auf diese Weise kann der Bezug der Datenverarbeitung zu der konkreten Anordnung der Maßnahme besser gewahrt werden. Zu § 38 Abs. 2, 4, 6 und 7 BNDG-E (Übermittlung an andere inländische öffentliche Stellen) wird Bezug genommen auf oben k).

Hervorzuheben ist, dass § 34 Abs. 9 BNDG-E eine Sonderregelung für die Auswertung von informationstechnischen Systemen, die in den Besitz des BND gelangt sind, vorsieht. Eine Regelung dieser Art der Informationsbeschaffung ist dringend zu begrüßen, da hier eine Regelungslücke und ein Wertungswiderspruch zur „Online-Durchsuchung“ und Telekommunikationsüberwachung besteht (vgl. näher Löffelmann, in: Dietrich/Eiffler, a. a. O., Teil VI § 5 Rn. 20 ff.; ders., GSZ 2019, 190, 193). Die Regelung in Absatz 9 behebt diesen Wertungswiderspruch nicht. Erforderlich hierfür wäre insbesondere eine Erstreckung der Schutzvorschriften der §§ 35 und 36 BNDG-E auf die Auswertung informationstechnischer Systeme. Dabei müsste im Blick behalten werden, inwiefern es tatsächlich technisch möglich ist, kernbereichsrelevante und vertrauliche Inhalte automatisch auszufiltern. Sinnvoller Weise müssten Schutzvorschriften hier auf der Ebene des nach einer manuellen Relevanzprüfung noch vorhandenen Datenmaterials ansetzen. Ein gutes Beispiel für die gegebene Problematik sind Daten betreffend Minderjährige (etwa Fotos), die bereits de lege lata strengeren datenschutzrechtlichen Anforderungen unterliegen: Ob solche Daten zu Zwecken der Gefahrenfrüherkennung tatsächlich erforderlich sind, lässt sich häufig nicht von vornherein erkennen, sondern erst nach einer Auswertung. Dasselbe gilt für (vermeintlich) kernbereichsrelevante Inhalte und solche aus Vertrauensbeziehungen.

Worauf der Entwurf verzichtet, ist die Schaffung einer Übermittlungsregelung für aus einem informationstechnischen Eingriff gewonnene Daten an ausländische Partner. Der dadurch gebotene Rückgriff auf die allgemeinen Übermittlungsregeln erscheint ausgesprochen impraktikabel.

Aus Transparenzgründen sollte in den Titel des Gesetzes die Thematik der Schaffung einer Befugnis zur Online-Durchsuchung aufgenommen werden. Klargestellt werden sollte ferner aufgrund der entsprechenden öffentlichen Debatte, dass die Befugnis lediglich informationelles und kein aktionelles Handeln, etwa in Gestalt eines „Hack-back“ erlaubt, dessen völkerrechtliche Zulässigkeit hoch umstritten ist (vgl. dazu Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017).

o) Zu §§ 40 bis 58 BNDG-E (unabhängige Rechtskontrolle)

Die Regelungen in den §§ 40 bis 58 BNDG-E etablieren für den Bereich der technischen Aufklärung des BND mit dem Unabhängigen Kontrollrat ein neues Kontrollorgan, das, entsprechend den Vorgaben des BVerfG (BVerfG, a. a. O., Rn. 275 ff.) eine gerichtsähnliche (§ 42 BNDG-E) und eine administrative Kontrolle (§§ 51, 52 BNDG-E) durchführt. Der Unabhängige Kontrollrat verfügt über weitreichende Befugnisse (§§ 42, 52, 56, 58 BNDG-E) und ist personell ausgesprochen hochrangig ausgestattet. Die Vorgaben des BVerfG zur Erforderlichkeit eines gerichtsähnlichen Schutzmechanismus (vgl. BVerfG, a. a. O., Rn. 274 ff.) werden damit weit übererfüllt. Der breite gesetzgeberische Gestaltungsspielraum hätte auch andere Konstruktionen erlaubt, die besser mit dem Kontrollniveau in anderen Bereichen des Sicherheitsrechts harmoniert hätten.

Zu berücksichtigen ist außerdem, dass auf Seiten des BND entsprechende personelle Strukturen geschaffen werden müssen, um eine sachgerechte Vorbereitung und Zuarbeit im Rahmen der Kontrolle zu ermöglichen. Diese strukturellen Veränderungen werden den BND voraussichtlich vor große Herausforderungen stellen und seine Personalressourcen beträchtlich beanspruchen, zumal der gesamte Kontrollmechanismus mit zahlreichen beteiligten Organen mit sich überschneidenden Befugnissen weiterhin hoch komplex und unübersichtlich bleibt. De lege ferenda erscheint es wichtig, die Kontrollbefugnisse möglichst bei einem Organ zu bündeln. Aus einer verwaltungsökonomischen Sicht (die der der nachrichtendienstlichen Praxis im Grundsatz entsprechen dürfte) erscheint nicht die Tiefe einer Kontrolle kritisch, sondern die Effizienz und Effektivität der Strukturen und Verfahren, innerhalb derer sie agiert. Mit der Aufwertung des Unabhängigen Gremiums zu einem Unabhängigen Kontrollrat verbessert sich zwar die Kontrolltiefe, nicht aber die Praktikabilität der Verfahren.

Etwas unschlüssig bei der gewählten Ausgestaltung erscheint weiterhin, dass die richterlichen Mitglieder aus dem Kreis der Richterinnen und Richter am Bundesgerichtshof rekrutiert werden sollen (§ 43 Abs. 1 Nr. 1 BNDG-E), die sich zahlenmäßig weit überwiegend mit zivilrechtlicher Revisionsrechtsprechung befassen. Obwohl zweifellos alle diese Personen geeignet sind, „die Vorgänge in der Behörde zu durchdringen und im gegenseitigen Zusammenwirken eine unabhängige wie professionell fachkundige Kontrolle sicherzustellen“ (BVerfG, a. a. O., Rn. 285), könnte bei einer Ausweitung des Kandidatenkreises (etwa auf Richter des BVerwG oder Richter an Oberlandesgerichten) eine weitere fachliche Stärkung erzielt werden. Wenig einleuchtend erscheint weiter, wieso die richterlichen Mitglieder über

eine langjährige Erfahrung in ihrer vormaligen Tätigkeit als Bundesrichter verfügen müssen. Das BVerfG spricht zur Gewährleistung einer richterlichen Perspektive lediglich vom Erfordernis langjähriger richterlicher Erfahrung einer maßgeblichen Zahl der Mitglieder (BVerfG, a. a. O., Rn. 286). Dazu zählt auch die Erfahrung an den Instanzengerichten. Soweit die Entwurfsbegründung (S. 104) davon spricht, „in der Regel sollten die Mitglieder mindestens zwanzig Jahre richterlicher Erfahrung mitbringen“, dürfte das den Kreis geeigneter Richterinnen und Richter beträchtlich einschränken, da viele Justizangehörige - darunter gerade solche, die später an eines der Bundesgerichte gewählt werden - ganz erhebliche Teile ihrer Dienstzeit in Abordnungen, unter anderem als wissenschaftliche Mitarbeiter an Bundesgerichten oder als Referenten in Bundes- und Landesministerien – also außerhalb einer richterlichen Tätigkeit – ableisten. Hinzu kommen in Wechselsystemen Verwendungen bei der Staatsanwaltschaft sowie Freistellungen, etwa durch Mutterschutz und Elternzeit. Eine *mindestens* zwanzigjährige richterliche Berufserfahrung als Qualifikationsvoraussetzung erscheint vor diesem Hintergrund zu anspruchsvoll. Im Übrigen ist darauf hinzuweisen, dass die Dauer einer richterlichen Tätigkeit kein Merkmal richterlicher Unabhängigkeit ist.

Im Vergleich zur präventiven als auch nachträglichen gerichtlichen oder quasi-gerichtlichen Kontrolle in anderen Bereichen des Sicherheitsrechts, die in der Regel beim Amtsgericht, also bei einem Einzelrichter der Besoldungsgruppe R 1, liegt (so etwa auch für die Anordnung einer Online-Durchsuchung nach BayVSG), verfügt der Unabhängige Kontrollrat mit sechs Mitgliedern der Besoldungsgruppen B 7 und B 9 (Präsident oder Präsidentin) sowie einer Direktorin oder einem Direktor als Leiterin oder Leiter des administrativen Kontrollorgans der Besoldungsstufe B 4 (§§ 46, 50 BNDG-E) über ein beeindruckendes personelles Gewicht, das den hohen Rang des Grundrechtsschutzes im Zusammenhang mit Maßnahmen der technischen Aufklärung widerspiegelt. Um Wertungswidersprüche zu vermeiden und dem hohen Rang des Grundrechtsschutzes auch in anderen Bereichen des Sicherheitsrechts adäquat Rechnung zu tragen, sollte darüber nachgedacht werden, auch dort den gerichtlichen Rechtsschutz entsprechend aufzuwerten.

p) Zu §§ 59 bis 63 BNDG-E (Mitteilungen und Evaluierung)

Der in § 59 Abs. 1 BNDG-E vorgesehene Ausschluss der Benachrichtigung betroffener Ausländer im Ausland ist sachgerecht und entspricht dem vom BVerfG eröffneten Gestaltungsspielraum. Die Benachrichtigungspflicht in Absatz 2 orientiert sich an den entsprechenden Regelungen des G 10 und ist gleichfalls nicht zu beanstanden.

Die Evaluierungspflicht in § 61 BNDG-E ist aus Gründen der Transparenz und als Grundlage der gesetzgeberischen Rechtsfolgenbeobachtungspflicht und Fortentwicklung des Rechts ausdrücklich zu begrüßen. Der fünfjährige Zeitraum erscheint angesichts der hohen Praxisrelevanz der Maßnahme als zu lang.

§ 62 BNDG-E bezieht sich auf eine gängige Regelungspraxis, welche die interne exekutive Selbstkontrolle maßgeblich stärkt.

8. Zu Ziff. 22 (unabhängige Datenschutzkontrolle)

Durch die Beibehaltung des § 32 BNDG i. V. m. § 26a BVerfSchG und die Erstreckung des Anwendungsbereichs der Normen auf die strategische Ausland-Fernmeldeaufklärung wird auch betroffenen Ausländern im Ausland die Möglichkeit einer unabhängigen Datenschutzkontrolle eröffnet. Angesichts der ausgeschlossenen Benachrichtigungspflicht ist das zu begrüßen.

9. Zu Ziff. 24 (Berichtspflicht und Information der Öffentlichkeit)

Die Regelung entspricht im Wesentlichen § 33 BNDG und ist nicht zu beanstanden.

10. Zu Ziff. 27 (Zitiergebot und Übergangsvorschriften)

Inwiefern durch das Gesetz eine Einschränkung des Art. 13 GG erfolgt, ist nicht erkennbar. Maßnahmen der Online-Durchsuchung, die nicht auf eine – hier nicht geregelte – Überwachung von Wohnraum durch Fernsteuerung von Peripheriegeräten zielen, stellen keinen Eingriff in das Wohnungsgrundrecht dar. Artikel 12 des Änderungsgesetzes nennt ebenfalls nicht Art. 13 GG.

Die in den Übergangsvorschriften vorgesehenen Fristen erscheinen zur Ermöglichung einer reibungslosen Implementierung der neuen technischen und administrativen Strukturen durchweg sachgerecht, wenngleich ambitioniert.

II. Zu Artikel 2 (Änderung des G 10)

1. Zu Ziff. 1 (Weiterverarbeitung von Verkehrsdaten aus § 3 G 10-Maßnahmen)

In dem neuen § 4a G 10 soll offenbar eine Rechtsgrundlage für die vom BVerwG beanstandete Verkehrsdatenanalyse geschaffen werden. Da für im Rahmen einer Individualüberwachung nach § 3 G 10 aufgrund der dortigen qualifizierten Voraussetzungen eine strenge Zweckbindung besteht, geht der Gesetzentwurf zutreffend davon aus, dass für eine zweckändernde Verwendung eine besondere Rechtsgrundlage erforderlich ist. Hier besteht diese Zweckänderung in einer Speicherung der Verkehrsdaten und ihrer Rasterung zu den Zwecken des Erkennens von Personen, die einen Deutschlandbezug aufweisen und für die Tätigkeit des BND relevant sind (Absatz 1 Nummer 1) sowie des Identifizierens der für eine strategische Fernmeldeüberwachung nach § 5 G 10 geeigneten Telekommunikationsnetzen.

Die konkrete Verwendung der Daten (Speicherung, automatisierte oder manuelle Auswertung) kommt im Wortlaut der Norm nicht zum Ausdruck. Auch die in der Entwurfsbegründung (S. 117) genannte Verwendung der Daten als Suchbegriffe im Rahmen einer strategischen Fernmeldeüberwachung stellt eine zweckändernde rechtfertigungsbedürftige Verwendung dar, die im Gesetz normenklar und präzise zu regeln ist. Die geänderte Verwendung unterliegt außerdem – anders als die Erhebung der Daten nach § 3 G 10 – keinerlei qualifizierten Voraussetzungen, was nicht dem verfassungsrechtlichen Grundsatz der hypothetischen Datenneuerhebung entspricht. Soweit die Entwurfsbegründung (S. 117) ausführt, die gespeicherten Anschlusskennungen seien solche des Verdächtigen einer Anlasstat oder eines

Nachrichtenmittlers, ist das unzutreffend. Gespeichert werden auch die Verkehrsdaten der Kommunikationspartner, andernfalls wäre das beabsichtigte Ermitteln der Kontaktpersonen nicht möglich. Aus dieser Erstreckung auf dritte Personen ergibt sich unter anderem die Eingriffsintensität und Rechtfertigungsbedürftigkeit der Verkehrsdatenspeicherung. Letzten Endes erlaubt § 4a G 10-E eine anlasslose „Vorratsdatenspeicherung" von Telekommunikationsverkehrsdaten zu den in Absatz 1 bezeichneten Zwecken. Die Rechtfertigung einer solchen Datenverarbeitung unterliegt verfassungsrechtlich qualifizierten Anforderungen, die hier nicht geregelt sind. Die Ausführungen in der Entwurfsbegründung, insbesondere zu einer in einem Satz 2 geregelten „Nutzungskaskade" (S. 117 f.), finden keine Entsprechung im Gesetztext. Die Speicherfrist gem. Absatz 2 Satz 2 Halbsatz 1 von maximal sechs Monaten entspricht den Vorgaben des BVerfG (vgl. BVerfG, a. a. O., Rn. 191), die – letztlich zeitlich unbegrenzte – Erstreckung der Speicherung unter dem bloßen Vorbehalt der weiteren Erforderlichkeit der Daten im Einzelfall begegnet jedoch Bedenken. Bei einer Beibehaltung der Regelung sollte jedenfalls eine prozessuale Absicherung der Erforderlichkeitsprüfung durch eine gerichtsähnliche Überprüfung erfolgen. Soweit die Entwurfsbegründung (S. 119) die Einbindung der G 10-Kommission erwähnt, findet das im Gesetztext keine Entsprechung.

Soweit die Datenauswertung darauf zielt, geeignete Telekommunikationswege zu bestimmen, erschließt sich ferner nicht, warum sich dieser Zweck nur auf die strategische Aufklärung grenzüberschreitender Telekommunikation nach § 5 G 10 bezieht und nicht auf die strategische Ausland-Fernmeldeaufklärung nach §§ 19 ff. BNDG-E.

2. Zu Ziff. 2 (Weiterverarbeitung von Verkehrsdaten aus § 5 G 10-Maßnahmen)

Die Regelung in § 6 Abs. 4 bis 6 G 10-E stellt das Komplement für die unter Ziff. 1 bezeichnete Maßnahme in Bezug auf Verkehrsdaten dar, die durch Maßnahmen nach § 5 G 10 erlangt wurden. Die Vorschrift unterscheidet dabei zwischen anonymisierten (Absatz 4) und nicht-anonymisierten Verkehrsdaten (Absatz 5). Die Verwendung anonymisierter Verkehrsdaten ist zu denselben Zwecken wie nach § 4a G 10-E zulässig. Auch hier fehlen qualifizierte Anordnungsvoraussetzungen. Da eine mit vertretbarem Aufwand irreversible Anonymisierung erfolgt, erscheint die beabsichtigte Regelung jedoch vertretbar, wenngleich insoweit mangels geklärter Rechtslage ein verfassungsrechtliches Risiko verbleibt.

Die Differenzierung zwischen den Anwendungsbereichen des Absatzes 4 und 5 ist schwer nachzuvollziehen. Laut Entwurfsbegründung (S. 120) betreffe Absatz 4 den Fall, dass „für keinen der beiden Kommunikationsteilnehmer eine Beschränkungsanordnung vorliegt". § 5 G 10 sieht jedoch keine personenbezogenen Beschränkungsanordnungen vor, weshalb dieser Gesichtspunkt sich nicht als Differenzierungskriterium eignet. Gemeint ist vermutlich die Verwendung personenbezogener Suchbegriffe, die nur ausnahmsweise nach § 5 Abs. 2 S. 3 G 10 für Telekommunikationsanschlüsse im Ausland zulässig ist, sofern ausgeschlossen werden kann, dass Anschlüsse deutscher Staatsangehöriger gezielt erfasst werden. Diese Ausnahme ist allerdings immer schon insofern zu eng gefasst, als Inländer in gleichem Maße wie deutsche Staatsangehörige dem Schutz des Art. 10 GG unterfallen. Der Bezug auf § 5 Abs. 2 S. 3 G 10 sollte in § 6 Abs. 5 G 10-E jedenfalls klarer zum Ausdruck kommen. Die Befugnis zur Zweckänderung der hier nicht anonymisierten Verkehrsdaten in Absatz 5 Satz 1 unterliegt ebenfalls keinen qualifizierten Anforderungen. Das widerspricht einerseits schon

dem Ausnahmecharakter des § 5 Abs. 2 S. 3 G 10, denn letztlich sollen auf diesem Wege, wie die Entwurfsbegründung ausführt (S. 120), „relevante Personen auf Seiten der kontaktierten inländischen Anschlüsse erkannt werden." Die Identifizierung und Erfassung bestimmter inländischer Telekommunikationsanschlüsse soll aber gerade durch § 5 Abs. 2 S. 2 G 10 ausgeschlossen werden. Außerdem korrespondiert das Fehlen qualifizierter Anordnungsvoraussetzungen nicht mit dem Grundsatz der hypothetischen Datenneuerhebung, worauf hier mangels Anonymisierung auch nicht verzichtet werden kann. Hinsichtlich einer gerichtsähnlichen Kontrolle der Prüf- und Speicherfristen gelten die Ausführungen zu § 4a G 10-E.

3. Zu Ziff. 4 (Weiterverarbeitung von Verkehrsdaten aus § 8 G 10-Maßnahmen)

Die Überlegungen zu § 6 Abs. 5 G 10-E gelten entsprechend.

Am Rande ist darauf hinzuweisen, dass die beabsichtigten Änderungen keine Schaffung einer Rechtsgrundlage für die entsprechende Auswertung von Verkehrsdaten vorsieht, die dem BND von anderen Stellen, namentlich ausländischen Partnerdiensten, zur Verfügung gestellt werden. Das BVerwG hatte in seinem VERAS-Urteil auch insoweit das Fehlen einer Befugnis moniert (vgl. BVerwG, U. v. 13.12.2017, 6 A 6.16, Rn. 23, 33).

C. Zu BT-Drs. 19/26221

Der Antrag enthält eine große Vielzahl allgemeiner und spezifischer Petita zu einer umfassenderen externen, insbesondere parlamentarischen Kontrolle und engeren Einhegung nachrichtendienstlicher Befugnisse. In dem gegebenen Rahmen können diese Forderungen in ihrer Vielfalt, ihrer staatstheoretischen Einbettung und namentlich in ihrem Zusammenwirken und ihren Konsequenzen vom Verf. nicht detailliert sachverständig bewertet werden. Im Folgenden wird daher lediglich auf einige allgemeine und ausgewählte Gesichtspunkte eingegangen:

I. Stärkung der Befugnisse des PKGr

Der Wunsch nach einer Stärkung der parlamentarischen Kontrolle wurde in der Vergangenheit immer wieder eingehend diskutiert und erscheint nachvollziehbar. Der Antrag enthält insoweit einige sinnvolle Ansätze, um die Wirksamkeit der Kontrolltätigkeit des PKGr zu verbessern (etwa II.2.a.i., ii., iv., II.2.d.ii.). Soweit solche Änderungen Geheimschutzbedürfnisse berühren (etwa II.2.a.iii., v., vi.), kommt es auf die Ausgestaltung im Detail an. Verschriftlichungen und Audiodokumentationen (II.2.b.ii., iii., II.2.c.) sind insoweit mit Vorsicht zu betrachten. Hier zeichnen sich schon in anderen Bereichen des Sicherheitsrechts, die grundsätzlich der öffentlichen Kontrolle zugänglich sind (etwa im Strafverfahren), Problemlagen ab, aus denen zunächst Erfahrungen gewonnen werden sollten. Eine Erstreckung der Tätigkeit des PKGr auf andere Bereiche des Sicherheitsrechts, namentlich den der Gefahrenabwehr (II.2.b.iv.), führt zu weiteren Kompetenzüberschneidungen und Mehrfachzuständigkeiten. Eine erhebliche Gefahr für Geheimschutzinteressen entsteht aus größeren Erweiterungen des Kreises von Personen, die Kenntnis von geheimschutzbedürftigen Sachverhalten haben (II.2.e.). Solche erweiterten Befugnisse, insbesondere länderübergreifend, dürften

auch kompetenzrechtlich nur schwer auf eine tragfähige Grundlage gestellt werden können. Ausgesprochen sinnvoll erscheint de lege ferenda die Bündelung von Kontrollbefugnissen bei einem oder möglichst wenigen Organen (in diese Richtung II.3.a.), wobei hier zahlreiche Gestaltungsvarianten denkbar sind. Die weitere Stärkung der Befugnisse des Bundesbeauftragten für den Datenschutz und die Informationssicherheit (II.4.) dürfte hierzu allerdings eher in Widerspruch stehen. Durchaus sinnvoll erscheint zudem die im Antrag angedeutete Überprüfung der Handhabung der VS-Anordnung (S. 5), wenngleich die Einführung einer zusätzlichen Kontrollinstanz (II.5.a.) eher zu einer weiteren Zersplitterung und Aufblähung der Kontrollmechanismen beitragen dürfte. Bei aller berechtigten Kritik an Defiziten des gegenwärtigen parlamentarischen Kontrollregimes sollte nicht aus dem Blick geraten, dass sich die de lege lata zur Verfügung stehenden Instrumente in der Vergangenheit durchaus als wirksam erwiesen haben. So ist insbesondere die Tätigkeit der Untersuchungsausschüsse des Deutschen Bundestags maßgeblich für die Fortentwicklung von Kontrollinstrumenten der internen und externen Dienst- und Fachaufsicht. Eine ähnliche Funktion erfüllen die parlamentarischen Anfragen, deren Beantwortung eine sorgfältige Dokumentation von Vorgängen voraussetzt.

II. Allgemeine Stärkung der Kontrollmechanismen

Eine wirksame Kontrolle der Nachrichtendienste ist unverzichtbar. In diesem Zusammenhang sollte jedoch nicht übersehen werden, dass die präventive und begleitende parlamentarische und gerichtsähnliche Kontrolle der Nachrichtendienste bereits de lege lata mit zahlreichen Kontrollorganen mit sich überschneidenden Befugnissen (Parlamentarisches Kontrollgremium, Ständiger Bevollmächtigter des Parlamentarischen Kontrollgremiums, Vertrauensgremium, Untersuchungsausschüsse, parlamentarische Fragerechte, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, G 10-Kommission, unabhängiges Gremium, vereinzelt Richtervorbehalt) weit über die Kontrolldichte in allen anderen Bereichen des Sicherheitsrechts hinausreicht. Hinzu kommen im Bereich der Nachrichtendienste komplexe, durch detaillierte Dienstvorschriften geregelte, interne Prüfungsverfahren. Zum Vergleich: Während die Beantragung einer Maßnahme der Telekommunikationsüberwachung nach § 100a StPO einen staatsanwaltlichen Antrag voraussetzt und eine (von der Staatsanwaltschaft in aller Regel vorbereitete) ermittlungsrichterliche Anordnung, also de facto auf einem „Vier-Augen-Prinzip“ beruht, sind an der Vorbereitung eines der Sache nach vergleichbaren Antrags nach § 3 G 10 durch den BND schon vor Befassung der 8-köpfigen G 10-Kommission aufgrund der anspruchsvollen Voraussetzungen zahlreiche Personen im Rahmen der internen und externen Dienst- und Fachaufsicht beteiligt (näher zum Anordnungsverfahren Löffelmann, in: Dietrich/Eiffler, a. a. O., Teil VI § 4 Rn. 62 ff., 92 f.). Das harmoniert nicht mit der viel einfacheren Ausgestaltung des präventiven Kontrollverfahrens im Polizei- und Strafverfolgungsrecht, zumal dort wesentlich höhere Anwendungszahlen in Rede stehen. Die etwas weitere Möglichkeit der dortigen nachträglichen gerichtlichen Kontrolle beseitigt diese Schieflage nicht, denn die nachträgliche Kontrolle ersetzt den präventiven Rechtsschutz nicht und besitzt auch dort nur eine sehr geringe rechtstatsächliche Relevanz. Vor diesem Hintergrund erscheint die Forderung nach einer pauschalen Ausweitung der Kontrollmechanismen im Bereich des Rechts der Nachrichtendienste nicht selbstevident. Zu berücksichtigen ist außerdem, dass die schon gegenwärtig komplizierten Antragsverfahren ein

hohes Maß an personellen Ressourcen binden, die für die Facharbeit nicht mehr zur Verfügung stehen. Dasselbe gilt für den Fall der Einrichtung neuer Kontrollorgane, deren Kompetenzen Zuständigkeiten bei den Diensten entsprechen müssen. Eine weitere Reform der Kontrolle der Nachrichtendienste sollte im Rahmen der breiten gesetzgeberischen Gestaltungsspielräume in erster Linie darauf zielen, klare Zuständigkeiten der Kontrollorgane und einfach zu handhabende Kontrollverfahren zu implementieren. Eine Bündelung von Kompetenzen für die Kontrolle verschiedener Maßnahmen bei einem Organ erscheint insofern durchaus zielführend. Gegenwärtig sind die Kontrollregimes in den verschiedenen Bereichen des Sicherheitsrechts zu heterogen und harmonieren nicht miteinander. Daraus resultieren nicht nur Wertungswidersprüche, sondern auch Verwerfungen beim Datentransfer, der nur an materielle Übermittlungsschwellen gebunden ist. Gerade mit Blick auf die vom Antrag thematisierte „Überwachungsgesamtrechnung“ (S. 2 f., III.1., 3.) erscheint es notwendig, die Gesamtheit der deutschen Sicherheitsarchitektur als eines komplementären Systems zu betrachten. Deshalb sollten das Kontrollniveau und die Prüfdichte in den verschiedenen Bereichen des Sicherheitsrechts sachgerecht aufeinander abgestimmt werden.

III. Schaffung integrierter Nachrichtendienstgesetze

Neben den bereits erwähnten parlamentarischen Kontrollmöglichkeiten ist das wichtigste Steuerungsinstrument des Parlaments sein „erster Zugriff“ auf eine Regelungsmaterie. Durch die Schaffung anwendungsfreundlicher Regelungen hat es der Gesetzgeber in der Hand, sowohl den dadurch vermittelten präventiven Grundrechtsschutz als auch die verfolgten hoheitlichen Zwecke zu fördern. Anwendungsfreundliche Normen vermögen den Konflikt von „Freiheit und Sicherheit“ transparent zu machen und sogar aufzulösen. Die größte Gefahr für den Grundrechtsschutz besteht nicht in einem real nicht existierenden „Aufklärungseifer“, der sich mutwillig oder leichtfertig über gesetzliche Grenzen hinwegsetzt, sondern in deren schwerer Erkennbarkeit oder gänzlichem Fehlen. Wer viel Verantwortung trägt und immer alles richtig machen muss, weil schon kleine Fehler weitreichende Konsequenzen haben können, kann auch viel falsch machen. Regeln sollten in dieser Anforderungssituation Hilfe und nicht Hindernis sein. Dass die deutschen Nachrichtendienstegesetze eine überaus sperrige, zerfaserte, unübersichtliche Regelungsmaterie mit zahlreichen Wertungswidersprüchen bilden und für die Rechtsanwendung mehr Hemmnis als Hilfe darstellen, ist kein Geheimnis. Durch die Schaffung integrierter Dienstegesetze sollte dem entgegengewirkt werden. In diesem Zusammenhang ist darauf hinzuweisen, dass zwischen den Aufgaben, Methoden und Befugnissen der Inlandsnachrichtendienste und des Auslandsnachrichtendienstes nicht unerhebliche Unterschiede bestehen, welche bereichsspezifische Regelungen nahelegen. Dem Eigeninteresse der Dienste des Bundes an einem normenklaren Handlungsrahmen würde ein Befugnisgesetz nach dem Vorbild mancher Landesverfassungsschutzgesetze entgegenkommen. Das betrifft insbesondere auch die mit der Auslandsgeltung der Grundrechte erforderliche Regelung der Eingriffsbefugnisse bei einem Tätigwerden im Ausland (II.3.b., III.5.). Leitidee sollte dabei die Anwendungsfreundlichkeit der gesetzlichen Regelungen sein. Auch eine die Rechtsanwendung erleichternde Überarbeitung der Übermittlungsregeln (in diese Richtung III.2.d.) und die Schaffung eines in sich schlüssigen Schutzsystems für Vertraulichkeitsbeziehungen (in diese Richtung III.2.h.) ist ausdrücklich zu begrüßen. Dass übergreifend in allen Bereichen des Rechts der Nachrichtendienste ein erheblicher Reformbedarf und die

Notwendigkeit der Entwicklung neuer Ordnungssysteme besteht, dürfte rechtswissenschaftlicher Konsens sein. Ebenso unstreitig ist aber, dass eine praxisgerechte Reform nicht unter dem Vorzeichen „viel hilft viel“ gelingen kann.

D. Zu BT-Drs. 19/19509

Der Antrag enthält Vorschläge für eine Neustrukturierung des Rechts der Nachrichtendienste, insbesondere im Bereich der Kontrollmechanismen. Einige Regelungsansätze, wie die Vereinheitlichung von Eingriffsschwellen (Ziff. I.2.) und Überarbeitung von Übermittlungsschwellen (Ziff. I.7.), sind im Grundsatz zu begrüßen und spiegeln den Stand der entsprechenden rechtswissenschaftlichen Kritik. Andere Petita werden auch von dem Gesetzentwurf unter BT-Drs. 19/26103 aufgegriffen (vgl. Ziff. II.1.b. Spiegelstrich 5 zur Third Party Rule) oder entsprechen bereits geltender Rechtslage (vgl. Ziff. II.3. Spiegelstrich 1 zur Klagebefugnis Betroffener). Der Vorschlag eines aus drei Säulen bestehenden Kontrollregimes (Ziff. II.) stellt eine von zahlreichen denkbaren Gestaltungsmöglichkeiten dar. Die vorgängige Einbindung eines „Bürgeranwalts“ oder eines Sachverständigen vor einer Entscheidung der G 10-Kommission (Ziff. II.1.a. Spiegelstriche 3, 7) erscheint allerdings eher weniger geeignet, um Geheimschutzbedürfnissen Rechnung zu tragen und eine Straffung der Kontrollverfahren zu erreichen. In keinem anderen Bereich des Sicherheitsrechts ist eine solche Konstruktion im Rahmen des präventiven Rechtsschutzes vorgesehen. Dasselbe gilt für ein Tätigwerden der G 10-Kommission von Amts wegen (Ziff. II.1.a. Spiegelstrich 4) und die Strafbarkeit falscher Angaben ihr gegenüber (Ziff. II.1.a. Spiegelstrich 5). Hier erscheinen disziplinarrechtliche Sanktionen, wie in anderen Bereichen auch, angesichts des ultima ratio-Charakters des Strafrechts als angemesseneres Mittel. Die vorgeschlagene Erstreckung der Prüfpflicht der G 10-Kommission auf jede Zweckänderung (Ziff. II.1.a. Spiegelstrich 6) erscheint - ungeachtet der fehlenden Praktikabilität einer solchen Regelung - unter dem Gesichtspunkt der oft gebotenen Schnelligkeit der Datenübermittlung im Sicherheitsbereich ausgesprochen riskant. Dasselbe gilt unter dem Blickwinkel von - auch gegenüber befreundeten Staaten bestehender - Geheimschutzbedürfnisse für den geforderten internationalen Informationsaustausch der Kontrollorgane (Ziff. II.1.d. Spiegelstrich 2).

E. Zu BT-Drs. 19/19502

Der Gesetzentwurf zielt auf die Einrichtung eines administrativen Kontrollorgans in Gestalt eines parlamentarischen Beauftragten für die Nachrichtendienste. Diese Konstruktion liegt im Gestaltungsspielraum des Gesetzgebers und erscheint grundsätzlich geeignet, um das Ziel einer besseren parlamentarischen Kontrolle zu erreichen. Aufgrund des großen Umfangs der Kontrolltätigkeit setzt eine effektive Aufgabenwahrnehmung allerdings eine erhebliche personelle Ausstattung voraus, die der Entwurf mit 100 Mitarbeitern (S. 3) beziffert. Hierdurch entstehen zwangsläufig gravierende Gefahren für Geheimhaltungsbedürfnisse, zumal die Zugangsberechtigungen dieser Mitarbeiter umfassend ausgestaltet sind und damit sogar über diejenigen der meisten eigenen Mitarbeiter der Dienste hinausgehen. Nicht zuletzt können dadurch auch Gefährdungslagen für die Mitarbeiter des Beauftragten entstehen, weshalb die Einrichtung von Sicherheitssystemen erforderlich wäre, die denen der Dienste kor-

respondieren. Diese mit der Schaffung des Amts eines Beauftragten einhergehenden notwendigen aufwändigen Folgemaßnahmen zum Geheimnis- und Personenschutz lassen diese Alternative nicht als überzeugend erscheinen. Soweit mit dem Vorschlag das Ziel verfolgt wird, „die Nachrichtendienstkontrolle in Deutschland zu vervollständigen“ (S. 12), ist darauf hinzuweisen, dass sich das Kontrollregime aufgrund der Vielzahl von Organen mit sich überschneidenden Kompetenzen schon heute als sehr unübersichtlich und ineffizient darstellt. Mit dem Beauftragten soll ein weiteres Organ hinzutreten, so dass zusätzliche Kompetenzkonflikte absehbar sind. Vorzugswürdig wäre die Konzentrierung einer umfassenden Kontrollzuständigkeit bei einem Organ.

F. Zusammenfassende Würdigung

Der Gesetzentwurf unter BT-Drs. 19/26103 setzt die Vorgaben des BVerfG in seinem Urteil vom 19.5.2020 im Wesentlichen sachgerecht, in einigen Details sogar vorbildlich um. Mit der beabsichtigten Einrichtung des Unabhängigen Kontrollrats wird weit über das Maß des verfassungsrechtlich Gebotenen hinaus ein starkes Kontrollorgan geschaffen, das eine detaillierte Kontrolle der Rechtsanwendung gewährleisten kann. Die bereichsspezifische Weite der Anordnungsschwellen wird auf diese Weise durch einen wirkmächtigen prozessualen Mechanismus kompensiert. Die rechtsstaatliche Verfasstheit der technischen Aufklärung wird so institutionell abgesichert und auch nach außen dokumentiert.

Methodischen bzw. teilweise verfassungsrechtlichen Bedenken begegnet der Gesetzentwurf an acht Stellen:

1. Die Beibehaltung der bisherigen Rechtslage in § 10 Abs. 3 BNDG-E hinsichtlich der Abfragebefugnis des BND für bei anderen Sicherheitsbehörden gespeicherte personenbezogene Daten dürfte nicht den Vorgaben des BVerfG zur präzisen Regelung solcher Befugnisse unter Berücksichtigung qualifizierter Eingriffsschwellen genügen.
2. Der Gesetzentwurf schafft in § 19 Abs. 1 BNDG-E zwar eine Ermächtigungsgrundlage für die strategische Ausland-Fernmeldeaufklärung hinsichtlich „personenbezogener“ Telekommunikationsdaten. Unklar ist aber, was für „sachbezogene“ Telekommunikationsdaten gilt.
3. Die unscharfe begriffliche Differenzierung zwischen „Maßnahmen der strategischen Ausland-Fernmeldeaufklärung“ (§ 19 Abs. 1 BNDG-E) und „strategischen Aufklärungsmaßnahmen“ (§ 19 Abs. 2 BNDG-E) erschwert das Verständnis des Regelungsansatzes und wird nicht immer konsequent durchgehalten.
4. Die mengenmäßige Begrenzung der zur Auswertung zur Verfügung stehenden Telekommunikationsverkehre auf 30 Prozent der weltweiten Übertragungskapazitäten in § 19 Abs. 8 BNDG-E stellt keine substanzielle Einschränkung dar.
5. Die in § 26 Abs. 5 S. 2 BNDG-E vorgesehene Ausnahme von der Begrenzung der Speicherfrist für Verkehrsdaten auf sechs Monate erscheint zu unscharf, um eine längere Bevorratung des Rohdatenbestands zu legitimieren.

6. Soweit § 29 BNDG-E die Datenübermittlung an „inländische öffentliche Stellen“ oder „andere inländische Stellen“ zulässt, bestehen Bedenken, ob die Fassung der Norm hinsichtlich der Bezeichnung der Übermittlungsempfänger ausreichend präzise ist.
7. Der Gesetzentwurf enthält im Rahmen der Weitergabe selektierter und unselektierter Daten nach §§ 32, 33 BNDG-E an ausländische Partner keine besonderen Vorkehrungen zum Schutz besonders gefährdeter Personen.
8. Die Neuregelung der zweckändernden Verwendung von Verkehrsdaten, die durch Maßnahmen nach §§ 3 und 5 G 10 erhoben wurden, nach § 4a Abs. 1 und § 6 Abs. 5 G 10-E dürfte nicht dem Grundsatz der hypothetischen Datenneuerhebung genügen.

Kritisch ist im Übrigen zu sehen, dass der Gesetzentwurf weiter eine Kultur der starken Ausdifferenzierung von Normbefehlen bei einem gleichzeitigen weitgehenden Fehlen übergreifender Ordnungsstrukturen fortschreibt. Das Gesetz ist dadurch für die Rechtsanwendung nur schwer verständlich und umzusetzen. Seine Abbildung in Dienstvorschriften wird voraussichtlich nicht unerhebliche Schwierigkeiten bereiten. Die personellen Ressourcen des BND werden durch die hochkomplexe Rechtslage in noch höherem Maße beansprucht werden, nicht nur in den Justiziariaten, sondern auch auf Ebene der einzelnen Sachbearbeiter in den Fachbereichen. Eine dortige verlässliche Rechtsanwendung wird umfängliche juristische Aus- und Fortbildungen erfordern.

Über die Novellierung der Vorschriften zur strategischen Auslands-Fernmeldeaufklärung hinaus ergeben sich aus der Entscheidung des BVerfG vom 19.5.2020 Konsequenzen für andere in Grundrechte eingreifende Aufklärungsmaßnahmen deutscher Nachrichtendienste im Ausland. Insofern sind weitere Reformen im BNDG und ggf. in anderen Nachrichtendienstgesetzen unausweichlich. Hinsichtlich des BNDG erscheint de lege ferenda gut vorstellbar, den mit dem gegenständlichen Entwurf verfolgten gelungenen Ansatz einer detaillierten einfachrechtlichen Ausgestaltung der Anlassbedrohungen auf andere Maßnahmen zu erstrecken, indem die Unterscheidung von politischer Unterrichtung und Gefahrenfrüherkennung „vor die Klammer“ gezogen wird. Auch die an diese Differenzierung anschließenden weiteren Normen (Übermittlungsregelungen, Kooperationsregelungen) könnten dann vereinheitlicht werden. Insgesamt ist die Schaffung eines integrierten BNDG, welches Befugnisse für die Tätigkeit im In- und Ausland möglichst unter einheitlichen Eingriffsschwellen versammelt und Differenzierungen nur als Ausnahme vorsieht, gut vorstellbar. Sonderregelungen betreffend Grundrechtseingriffe bei Ausländern im Ausland, wie die Handhabung von Benachrichtigungspflichten, Fragen des individuellen Rechtsschutzes oder auch des Personenschutzes, könnten in einem eigenen Abschnitt zusammengefasst werden. Hinsichtlich der sicherheitsbehördlichen Datenübermittlungen sollte ein System von Schutzwürdigkeitsklassen angestrebt werden, das die Zuordnung zu den jeweils zulässigen Übermittlungszwecken leichter erkennen lässt. Mit derartigen Weichenstellungen könnte das Gesetz für die Rechtsanwendung leichter zugänglich und anwendungsfreundlicher ausgestaltet werden.

gez. Prof. Dr. Markus Löffelmann