

Deutscher Bundestag  
Ausschuss für Inneres und Heimat

Ausschussdrucksache  
19(4)731 I



Deutscher **Anwalt** Verein

# Stellungnahme

des Deutschen Anwaltvereins durch  
den Ausschuss Gefahrenabwehrrecht

zum Regierungsentwurf eines Gesetzes zur  
Änderung des BND-Gesetzes zur Umsetzung der  
Vorgaben des Bundesverfassungsgerichts sowie  
des Bundesverwaltungsgerichts vom 25.01.2021  
(BT-Drs. 19/26103)

Stellungnahme Nr.: 23/2021

Berlin, im März 2021

## Mitglieder des Ausschusses

- Rechtsanwältin Lea Voigt, Bremen (Vorsitzende)
- Rechtsanwalt Wilhelm Achelpöhler, Münster
- Rechtsanwalt Dr. David Albrecht, Berlin
- Rechtsanwalt Dr. Eren Basar, Düsseldorf
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln  
(Berichterstatter)
- Rechtsanwalt Dr. Andreas Grözinger, Köln (Berichterstatter)
- Rechtsanwalt Prof. Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt / Main
- Prof. Dr. Mark A. Zöllner, München (ständiges Gastmitglied im  
Ausschuss, Berichterstatter)
- Prof. Dr. Annika Dießner, Berlin (ständiges Gastmitglied im  
Ausschuss)

## Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Uta Katharina Schmidt
- Rechtsanwalt Max Gröning

**Deutscher Anwaltverein**  
Littenstraße 11, 10179 Berlin  
Tel.: +49 30 726152-0  
Fax: +49 30 726152-190  
E-Mail: [dav@anwaltverein.de](mailto:dav@anwaltverein.de)

**Büro Brüssel**  
Rue Joseph II 40, Boîte 7B  
1000 Brüssel, Belgien  
Tel.: +32 2 28028-12  
Fax: +32 2 28028-13  
E-Mail: [bruessel@eu.anwaltverein.de](mailto:bruessel@eu.anwaltverein.de)  
EU-Transparenz-Registernummer:  
87980341522-66

[www.anwaltverein.de](http://www.anwaltverein.de)

## **Verteiler**

---

Bundesministerium des Innern, für Bau und Heimat  
Bundesministerium der Justiz und für Verbraucherschutz

Deutscher Bundestag – Ausschuss für Recht und Verbraucherschutz  
Deutscher Bundestag – Ausschuss für Inneres und Heimat

Arbeitsgruppe Recht und Verbraucherschutz der im Deutschen Bundestag vertretenen Parteien  
Arbeitsgruppe Inneres der im Deutschen Bundestag vertretenen Parteien

Justizministerien und -senatsverwaltungen der Länder  
Landesministerien und Senatsverwaltungen des Innern  
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit  
Landesdatenschutzbeauftragte  
Innenausschüsse der Landtage  
Rechtsausschüsse der Landtage

Europäische Kommission - Vertretung in Deutschland  
Bundesrechtsanwaltskammer  
Deutscher Richterbund  
Bundesverband der Freien Berufe  
Gewerkschaft der Polizei (Bundesvorstand)  
Deutsche Polizeigewerkschaft im DBB  
Ver.di, Recht und Politik  
stiftung neue verantwortung e.V.  
Institut für Deutsches und Europäisches Strafprozessrecht und Polizeirecht (ISP)  
der Universität Trier  
Deutsches Institut für Menschenrechte  
Gesellschaft für Freiheitsrechte

Vorstand und Landesverbände des DAV  
Vorsitzende der Gesetzgebungs- und Geschäftsführenden Ausschüsse des DAV  
Vorsitzende des FORUM Junge Anwaltschaft des DAV

Frankfurter Allgemeine Zeitung  
Süddeutsche Zeitung  
Berliner Verlag GmbH  
Hamburger Abendblatt  
Der Tagesspiegel  
Der Spiegel  
Juris Newsletter  
JurPC  
Netzpolitik.org  
Heise  
LTO

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt mehr als 62.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 252 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

---

## A. Übersicht

A. Übersicht.....	3
B. Einleitung .....	5
C. Die Ausland-Ausland-Fernmeldeaufklärung in der bisherigen Praxis .....	6
I. Datenerhebung.....	7
II. Datenübermittlung und Kooperation mit ausländischen Nachrichtendiensten	9
III. Kontrolle .....	9
D. Zentrale Feststellungen des BVerfG .....	11
I. Allgemeine Feststellungen.....	11
1. Weltweite Grundrechtsbindung.....	11
2. Vereinbarkeit der anlasslosen Ausland-Ausland-Fernmeldeaufklärung mit der Verfassung .....	13
II. Datenerhebung .....	13
III. Übermittlung von Daten aus der strategischen Telekommunikationsüberwachung.....	16
IV. Kooperation mit ausländischen Nachrichtendiensten .....	17
V. Kontrolle .....	18
E. Zum Regierungsentwurf.....	21
I. Datenerhebung.....	21
1. Strategische Ausland-Ausland-Fernmeldeaufklärung (§ 19 BNDG-E).....	21
2. Besondere Formen der strategischen Ausland-Fernmeldeaufklärung (§ 20 BNDG-E).....	24
3. Online-Durchsuchung (§ 34 BNDG-E).....	24
4. Unzureichender Schutz von Vertraulichkeitsbeziehungen (§§ 21, 35 BNDG-E).....	26
5. Ausufernde Überwachungskapazität (§§ 19 Abs. 8, BNDG-E).....	30
6. Unzulässige Überschreitung der zulässigen Höchstspeicherdauer von Verkehrsdaten (§ 26 Abs. 5 S. 2 BNDG-E).....	31

7.	Unzureichende Dokumentationspflichten .....	32
II.	Übermittlung und Kooperation .....	33
1.	Verfassungswidrigkeit der Übermittlungsvorschriften und Reformbedarf ..	33
2.	Übermittlung personenbezogener Daten an inländische Stellen .....	35
3.	Insbesondere: Übermittlung personenbezogener Daten an Private .....	36
III.	Kontrolle .....	37
2.	Anordnungs- statt Vollzugsvorbehalt .....	39
3.	Parlamentarische Kontrolle als zentrales Kontrollinstrument .....	39

## B. Einleitung

Mit Urteil vom 19.05.2020<sup>1</sup> erklärte der Erste Senat beim BVerfG die Ausland-Ausland-Fernmeldeaufklärung nach dem BND-Gesetz (BNDG) für verfassungswidrig.

Zugleich erteilte das BVerfG der Rechtsauffassung des BND und der Bundesregierung, dass der BND bei der Überwachung der Telekommunikation von Ausländerinnen und Ausländern im Ausland nicht an die Grundrechte des Grundgesetzes gebunden sei, eine klare Absage. Bereits im ersten Leitsatz der Entscheidung heißt es: „Die Bindung der deutschen Staatsgewalt an die Grundrechte nach Art. 1 Abs. 3 GG ist nicht auf das deutsche Staatsgebiet begrenzt“.<sup>2</sup> Jedenfalls der Schutz des Art. 10 Abs. 1 und des Art. 5 Abs. 1 Satz 2 GG als Abwehrrechte gegenüber einer Telekommunikationsüberwachung erstreckte sich auch auf Ausländer im Ausland. Das gelte unabhängig davon, ob die Überwachung vom Inland oder vom Ausland aus erfolge.

Da der Gesetzgeber dagegen von der Unanwendbarkeit der Grundrechte ausgegangen war, folgte die Verfassungswidrigkeit bereits aus der notorischen Verletzung des Zitiergebots aus Art. 19 Abs. 1 S. 2 GG. Dennoch nahm das BVerfG auch ausführlich zu den „zentralen“ materiell-rechtlichen Defiziten der Vorschriften des BNDG Stellung und erklärte neben den Vorschriften zur strategischen Ausland-Ausland-Fernmeldeaufklärung (§§ 6, 7, 19 Abs. 1 BNDG) auch die Vorschriften zur Übermittlung an andere Behörden (§ 24 Abs. 1 S. 2, Abs. 2 S. 1, Abs. 3 BNDG), die Vorschriften zur Kooperation mit ausländischen Diensten (§§ 13 bis 15 BNDG) und die Vorschriften zur Kontrolle der Aufklärungstätigkeit des BND für verfassungswidrig. Zugleich gab das BVerfG dem Gesetzgeber detaillierte Maßstäbe für die Schaffung verfassungskonformer Normen an die Hand.

Schließlich hat das BVerfG dem Gesetzgeber aufgegeben, seine Vorgaben bis spätestens zum 31.12.2021 umzusetzen.<sup>3</sup>

---

<sup>1</sup> BVerfGE 154, 152 = NJW 2020, 2235.

<sup>2</sup> BVerfG NJW 2020, 2235.

<sup>3</sup> BVerfG NJW 2020, 2235 (2269).

Das Bundeskanzleramt hat nunmehr einen Entwurf eines Gesetzes zur Änderung des Gesetzes über den Bundesnachrichtendienst und zur Umsetzung der Vorgaben aus dem Urteil des Bundesverfassungsgerichts vom 19.05.2020 ausgearbeitet. Der Gesetzesentwurf bleibt indes weit hinter den Anforderungen, die das BVerfG an die Ausgestaltung eines verfassungsgemäßen BNDG stellt, zurück.

In dieser Stellungnahme werden die Kritikpunkte nicht abschließend angeführt. Es kann nur auf die aus Sicht des Deutschen Anwaltverein (DAV) besonders gravierenden Punkte hingewiesen werden, die einer Korrektur bedürfen.

### **C. Die Ausland-Ausland-Fernmeldeaufklärung in der bisherigen Praxis**

Die Verfassungsbeschwerden richteten sich in erster Linie gegen die strategische Ausland-Ausland-Fernmeldeaufklärung, die allein auf die Überwachung des Telekommunikationsverkehrs von im Ausland befindlichen Ausländerinnen und Ausländern abzielt.

Mit der strategischen Telekommunikationsüberwachung werden Telekommunikationsübertragungswege oder -netze mit dem Ziel überwacht, aus der Gesamtheit der in den Netzen übermittelten Telekommunikationsdaten diejenigen herauszufiltern, die eine nachrichtendienstliche Relevanz besitzen.

Sie ist typischerweise nicht an bestimmte Eingriffsschwellen, etwa einen Tatverdacht oder eine (konkrete) Gefahr gebunden, sondern soll es als Vorfeldmaßnahme in der Regel erst ermöglichen, Anhaltspunkte, Verdachtsmomente, allgemeine Erkenntnisse und Lagebilder zu Themen zu gewinnen, die durch das Auftragsprofil der Bundesregierung (§ 6 Abs. 1 S. 1 Nr. 3 BNDG) als für das außen- und sicherheitspolitische Handeln der Bundesrepublik bedeutsam ausgewiesen sind. Allerdings wird die strategische Telekommunikationsüberwachung auch zur gezielten Überwachung konkreter Einzelpersonen angewendet.

## I. Datenerhebung

Die einzelnen Schritte der Datenerhebung werden durch das BNDG umfassend geregelt:

Zunächst müssen die Telekommunikationsnetze, aus denen Daten erhoben werden sollen, vom Bundeskanzleramt im Wege einer sog. Netzanordnung gemäß § 6 Abs. 1 S. 2 BNDG bestimmt werden. Unzulässig war dagegen auch bisher die Erhebung von Daten deutscher Staatsbürger oder Inländer, § 6 Abs. 4 BNDG. In der Praxis werde die Vorschrift ausweislich der Feststellungen des BVerfG jedoch – entgegen dem Gesetzeswortlaut – so verstanden, dass auch Daten von Deutschen und Inländern zunächst erhoben, aber in der Folge „nach Möglichkeit“ ausgefiltert werden.<sup>4</sup>

Der eigentliche Zugriff auf Telekommunikationsdatenströme erfolgt, indem der BND mittels eigener Vorrichtungen Signale aus Telekommunikationsnetzen abfängt oder sich gemäß § 8 BNDG von Telekommunikationsdiensteanbietern Datenströme mittels einer Ausleitungsanordnung ausleiten lässt. Die vom BND am weltweit größten Internetknotenpunkt DE-CIX in Frankfurt am Main installierten technischen Systeme können gegenwärtig etwa fünf Prozent des dort durchgeleiteten Telekommunikationsverkehrs erfassen und verarbeiten.<sup>5</sup>

Die einmal erfassten Daten werden sodann an den BND übertragen, was einen mehrstufigen und vollautomatisierten Filterungs- und Auswertungsprozess in Gang setzt. Diese sog. DAFIS-Filterung des Datenstroms erfolgt anhand von Suchbegriffen (sog. Selektoren), § 6 Abs. 2 BNDG. Dadurch sollen etwa deutsche E-Mail-Adressen oder Verbindungen mit der Deutschlandvorwahl „0049“ von vornherein aussortiert werden. Bereits hier zeigen sich die erheblichen praktischen Schwierigkeiten einer automatisierten Datenfilterung. Denn nutzt ein Deutscher etwa ein E-Mail-Konto eines internationalen Anbieters wie „gmail.com“ oder „hotmail.com“, stehen die Chancen schlecht, dass die E-Mail am Ende der DAFIS-Filterung herausgefiltert wurde.

Umgekehrt bedeutet eine automatisierte Ausfilterung von deutschen E-Mail-Adressen, dass sich jeder Anhänger einer ausländischen terroristischen Gruppierung lediglich eine

---

<sup>4</sup> BVerfG – 1 BvR 2835/17, Rn. 10.

<sup>5</sup> BVerfG – 1 BvR 2835/17, Rn. 18.

deutsche E-Mail-Adresse anlegen müsste, um Datenerhebungen durch den BND zu umgehen.

Nach Angaben der Bundesregierung zielen fünf Prozent der Suchbegriffe konkret darauf ab, Erkenntnisse zu einzelnen Personen im Hinblick auf gegenüber ihnen zu ergreifende Maßnahmen zu erlangen.<sup>6</sup> Eine gezielte Datenerhebung in diesem Sinne kann etwa dadurch erfolgen, dass eine bekannt gewordene E-Mail-Adresse als Selektor verwendet wird, die der Zielperson in der Vergangenheit zugeordnet werden konnte. Auf diesem Weg erhält der BND sämtliche unter dieser E-Mail-Adresse gesendeten Nachrichten, die über einen der von ihm überwachten Knotenpunkte versandt worden sind.

In den übrigen Fällen sind die hinter den gesteuerten Suchbegriffen stehenden Personen nur zum Teil bekannt, ohne dass sie selbst und ihr Verhalten im Fokus des Aufklärungsinteresses stehen.

Im Wege der DAFIS-Filterung selektiert der Bundesnachrichtendienst aus dem erfassten Datenvolumen mittels einer sechsstelligen Zahl von Suchbegriffen die Inhaltsdaten von täglich circa 270.000 Telekommunikationsvorgängen zwischen Menschen (E-Mail, Telefonat, Chat-Nachrichten) und speichert sie zur weiteren händischen Auswertung durch die Mitarbeiter des BND.<sup>7</sup>

Erst auf der Ebene der händischen Auswertung wird die nachrichtendienstliche Relevanz durch die Mitarbeiter des BND überprüft. Außerdem sollen kernbereichsrelevante Daten gemäß § 11 BNDG gemäß der internen Dienstvorschrift SIGINT ebenso aussortiert werden wie besonders geschützte Kommunikation i.S. des § 53 StPO.

Von den 270.000 zunächst erhobenen Telekommunikationsvorgängen verbleiben nach Abschluss des Filtervorgangs täglich etwa 260 Datenverkehre, die an die „abnehmenden Bereiche“ weitergeleitet werden.<sup>8</sup>

---

<sup>6</sup> BVerfG – 1 BvR 2835/17, Rn. 23.

<sup>7</sup> BVerfG – 1 BvR 2835/17, Rn. 24.

<sup>8</sup> BVerfG – 1 BvR 2835/17, Rn. 25.

## **II. Datenübermittlung und Kooperation mit ausländischen Nachrichtendiensten**

Die Zusammenarbeit mit ausländischen Partnerdiensten macht einen großen Teil der Fernmeldeaufklärung durch den BND aus. Zwischen 50 und 60 Prozent der im Zuge der Datenerhebung verwendeten Selektoren kommen von sog. Partnerdiensten des BND.<sup>9</sup> Entsprechend groß ist die Bedeutung der in den §§ 13 – 15 BNDG geregelten Praxis der nachrichtendienstlichen Kooperation. Die Datenerhebung mit Suchbegriffen des Partnerdienstes läuft dabei im Wesentlichen in gleicher Weise ab, wie eine Datenerhebung mit eigenen Suchbegriffen. Zusätzlich werden die von ausländischen Diensten genannten Suchbegriffe vor ihrer Verwendung elektronisch auf einen Deutschen- oder Inländerbezug, auf einen Verstoß gegen die Grenzen gezielter Erfassungen nach § 6 Abs. 3 BNDG, auf einen Verstoß gegen Interessen der Bundesrepublik Deutschland sowie auf bestimmte, im Hinblick auf die jeweilige Kooperation und ihre Ziele definierte Formalkriterien geprüft.<sup>10</sup> Zusätzlich überprüft der Bundesnachrichtendienst für jede Kooperation monatlich etwa 300 Suchbegriffe stichprobenartig.<sup>11</sup>

Eine Übermittlung der danach erhobenen Daten erfolgt auf Grundlage und im Rahmen einer Kooperationsvereinbarung, § 13 Abs. 3 Nr. 4 – 6 BNDG, in der neben Verwendungsbeschränkungen auch Zusicherungen zur Gewährleistung eines rechtsstaatlichen Datenumgangs und Grundsätze zur Datenlöschung geregelt sind.<sup>12</sup> Im Falle einer automatisierten Datenübermittlung ist inländische und internationale Telekommunikation auszufiltern, § 15 Abs. 1 Nr. 1a BNDG. Die Filterung der Telekommunikation erfolgt ebenfalls automatisiert, wird jedoch anhand von Stichproben auf ihre Funktionstüchtigkeit kontrolliert.

## **III. Kontrolle**

Für die Kontrolle der Aktivitäten des BND war bisher kein einheitliches Aufsichtsgremium zuständig. Vielmehr waren die Kontrollaufgaben zwischen dem sog.

---

<sup>9</sup> BVerfG – 1 BvR 2835/17, Rn. 27.

<sup>10</sup> BVerfG – 1 BvR 2835/17, Rn. 27.

<sup>11</sup> BVerfG – 1 BvR 2835/17, Rn. 27.

<sup>12</sup> BVerfG – 1 BvR 2835/17, Rn. 28.

Unabhängigen Gremium, der G-10-Kommission und dem Bundesbeauftragten für Datenschutz aufgeteilt.

Die weitreichendsten Befugnisse hat hierbei das aus zwei Richterinnen und Richtern beim BGH und einem Bundesanwalt bzw. einer Bundesanwältin sowie drei Stellvertreterinnen bzw. Stellvertretern bestehende Unabhängige Gremium, das die nach § 6 Abs. 1 BNDG vom Bundeskanzleramt getroffenen Anordnungen sowie die Bestimmung der Suchbegriffe durch den BND auf Zulässigkeit und Notwendigkeit überprüfen kann, § 9 Abs. 4 und 5 BNDG.

In der Vergangenheit wurde sowohl vom Unabhängigen Gremium als auch vom Bundesdatenschutzbeauftragten gerügt, dass ihre Kontrolltätigkeit unter Berufung auf die mit den Partnerdiensten geschlossenen Vertraulichkeitsvereinbarungen („Third Party Rule“) praktisch eingeschränkt war.<sup>13</sup>

So bemängelte der Bundesdatenschutzbeauftragte in seiner offiziellen Stellungnahme an das BVerfG ausdrücklich, dass die verfassungsrechtlichen Kontrollvorgaben in der Praxis unzureichend umgesetzt werden. Es gebe teilweise ungeklärte und gespaltene Zuständigkeiten, es fehlten Sanktionsmöglichkeiten und es mangle an Austauschmöglichkeiten mit anderen Kontrollorganen. Auch bestünden unzureichende proaktive Informationspflichten und große Wissensasymmetrien gegenüber dem Bundesnachrichtendienst. In Bezug auf im Ausland von anderen Diensten erlangte Daten sei eine Datenschutzkontrolle oftmals unmöglich, da der Bundesnachrichtendienst den Zugriff auf diese Daten unter Berufung auf die „Third Party Rule“ verwehre. Auch sei es in der Praxis dazu gekommen, dass Beanstandungen des Bundesdatenschutzbeauftragten übergangen worden seien, ohne dass Möglichkeiten bestanden hätten, sie zumindest an die Öffentlichkeit zu bringen.<sup>14</sup> Das Regime objektiver und unabhängiger Kontrolle sei insgesamt unzureichend und insbesondere nicht dazu geeignet, den aufgrund der Geheimheit der Maßnahmen und in Ermangelung von Benachrichtigungspflichten faktisch fehlenden gerichtlichen Rechtsschutz zu ersetzen.<sup>15</sup>

---

<sup>13</sup> BVerfG – 1 BvR 2835/17, Rn. 32.

<sup>14</sup> BVerfG – 1 BvR 2835/17, Rn. 51.

<sup>15</sup> BVerfG – 1 BvR 2835/17, Rn. 52.

## D. Zentrale Feststellungen des BVerfG

### I. Allgemeine Feststellungen

#### 1. Weltweite Grundrechtsbindung

Das BVerfG hat klargestellt, dass den Grundrechten des Grundgesetzes extraterritoriale Geltung zukommt. Die Grundrechte entfalten ihren Schutzgehalt somit immer dann, wenn der deutsche Staat Hoheitsgewalt ausübt, unabhängig davon, wo oder gegenüber wem dies geschieht. Danach können sich also auch Ausländerinnen und Ausländer im Ausland auf den Schutz der Grundrechte berufen.

Der DAV begrüßt die Entscheidung des BVerfG. Bereits in seiner Stellungnahme vom Oktober 2016 (Stellungnahme Nr. 65/2016) hatte der DAV darauf hingewiesen, dass Art. 10 GG uneingeschränkt auch auf die Ausland-Auslands-Fernmeldeaufklärung anwendbar ist und die Konsequenzen dieses „Geburtsfehlers“ aufgezeigt.<sup>16</sup>

Diese Auslegung entspricht dem Anspruch eines umfassenden, den Menschen in den Mittelpunkt stellenden Grundrechtsschutzes.

Der BND und mit ihm die Bundesregierung hatten sich zuvor auf den Standpunkt gestellt, dass die gerügten Grundrechte für Ausländerinnen und Ausländer im Ausland und Deutsche, die lediglich in ihrer „Stellung als Funktionsträger ausländischer juristischer Personen“ betroffen seien, bereits keinen Schutz gewährten, weil die Grundrechte nach der Präambel des Grundgesetzes auf das deutsche Staatsgebiet und Staatsvolk beschränkt seien<sup>17</sup> – eine Rechtsauffassung wohlgermerkt, nach der die Verfassung deutschen Hoheitsträgern auch das Foltern von Terrorverdächtigen in sog. Terrorcamps nicht verböte, solange dies nur im Ausland geschähe.

Entsprechend deutlich fiel die Antwort des BVerfG aus. Bereits der erste Leitsatz der Entscheidung enthält eine fundamentale Klarstellung: „*Die Bindung der deutschen Staatsgewalt an die Grundrechte nach Art. 1 Abs. 3 GG ist nicht auf das deutsche Staatsgebiet begrenzt.*“<sup>18</sup> Auch im Ausland und gegenüber Ausländerinnen und Ausländern bewegen sich deutsche Hoheitsträger somit nicht im (grund-)rechtsfreien

---

<sup>16</sup> DAV Stellungnahme Nr. 65/2016, S. 4 f..

<sup>17</sup> BVerfG – 1 BvR 2835/17, Rn. 47 f.

<sup>18</sup> BVerfG NJW 2020, 2235.

Raum. Dieser Satz hat nicht nur unmittelbare Auswirkungen auf die Arbeit des BND, sondern auf sämtliche hoheitliche Aktivitäten im Ausland einschließlich aktueller Bundeswehreinsetze. Daran ändern auch die darauffolgenden Feststellungen des BVerfG nichts, in denen das BVerfG festhält: *„Der Schutz der einzelnen Grundrechte kann sich im Inland und Ausland unterscheiden. Jedenfalls der Schutz des Art. 10 Abs. 1 und des Art. 5 Abs. 1 Satz 2 GG als Abwehrrechte gegenüber einer Telekommunikationsüberwachung erstreckt sich auch auf Ausländer im Ausland.“*

Zwar könnte aus der Formulierung, dass sich „*jedenfalls*“ der Schutz des Art. 10 Abs. 1 und des Art. 5 Abs. 1 Satz 2 GG auch auf Ausländer im Ausland erstrecke, der Schluss gezogen werden, dass das BVerfG dies für andere Grundrechte gerade nicht feststellen wollte. Hierbei handelt es sich allerdings lediglich um eine scheinbare Einschränkung, die deshalb erfolgte, weil andere Grundrechte schlicht nicht Gegenstand der vorliegenden Entscheidung waren. Vor dem Hintergrund der Bezugnahme auf Art. 1 Abs. 3 GG, der sich gerade auf sämtliche Grundrechte bezieht, lässt sich der Entscheidung somit ohne Weiteres die Aussage einer weltweiten Grundrechtsbindung deutscher Hoheitsträger entnehmen. Dies entspricht nicht zuletzt dem der Entscheidung zugrunde liegendem Grundrechtsverständnis, das die Menschen in den Mittelpunkt grundrechtlicher Schutzgarantien stellt.<sup>19</sup>

Die Konsequenz der Feststellung der extraterritorialen Grundrechtsbindung, nämlich dass die derzeitigen Regelungen zur Ausland-Ausland-Fernmeldeaufklärung verfassungswidrig sind, folgte damit bereits aus der Verletzung des Zitiergebots aus Art. 19 Abs. 1 S. 2 GG.

Dennoch hält das BVerfG die verfassungsgemäße Ausgestaltung einer anlasslosen Ausland-Ausland-Fernmeldeaufklärung für möglich<sup>20</sup> und betont die hohe Bedeutung nachrichtendienstlicher Tätigkeit, die aufgrund wachsender Gefahren im Zusammenhang mit der Informationstechnik und der allgemeinen Internationalisierung noch zunehme.<sup>21</sup>

---

<sup>19</sup> BVerfG NJW 2020, 2235 (2241).

<sup>20</sup> BVerfG NJW 2020, 2235 (2248).

<sup>21</sup> BVerfG NJW 2020, 2235 (2243 f.).

## **2. Vereinbarkeit der anlasslosen Ausland-Ausland-Fernmeldeaufklärung mit der Verfassung**

Der Erste Senat beim BVerfG gab dem Gesetzgeber nicht nur weitreichende Maßstäbe zur Schaffung eines verfassungsgemäßen BNDG an die Hand, sondern signalisierte ihm darüber hinaus, dass die bisherige Überwachungspraxis der anlasslosen Ausland-Ausland Fernmeldeaufklärung „mit Art. 10 Abs. 1 GG nicht grundsätzlich unvereinbar“ sei.<sup>22</sup> Nicht zuletzt diese Feststellung demonstriert die Ausgewogenheit der Entscheidung.

Zugleich unterstrich das BVerfG, dass die Überwachungspraxis in geregelten und kontrollierbaren Bahnen verlaufen müsse. Eine globale und pauschale Überwachung lasse das Grundgesetz auch zu Zwecken der Auslandsaufklärung nicht zu.<sup>23</sup>

### **II. Datenerhebung**

Obwohl die Verfassungswidrigkeit weiter Teile des BNDG wegen des Verstoßes gegen das Zitiergebot aus Art. 19 Abs. 1 S. 2 GG bereits feststand,<sup>24</sup> ging das BVerfG in der Folge auch auf die (zentralen) materiellen Verstöße ein und gab dem Gesetzgeber außergewöhnlich detaillierte Maßstäbe zur Schaffung eines verfassungsgemäßen Regelungswerks für die Ausland-Ausland-Fernmeldeaufklärung an die Hand.

Zwar sei eine Befugnis zur Datenerhebung und Verarbeitung in Form der strategischen Telekommunikationsüberwachung im Grundsatz mit Art. 10 Abs. 1 GG vereinbar, hierfür bedürfe es aber einer hinreichend begrenzenden Ausgestaltung.<sup>25</sup> Das BVerfG betont, dass die strategische Telekommunikationsüberwachung ein Instrument von besonders schwerem Eingriffsgewicht sei, weil die Maßnahme heimlich durchgeführt werde, oftmals private und höchstvertrauliche Daten erhoben werden, die Maßnahme eine hohe Streubreite aufweist und die Daten an andere Dienste mit operativen Befugnissen weitergegeben werden. Zudem seien die im Zuge der Digitalisierung

---

<sup>22</sup> BVerfG NJW 2020, 2235 – LS 5.

<sup>23</sup> BVerfG NJW 2020, 2235 (2251).

<sup>24</sup> BVerfG NJW 2020, 2235 (2246 f.).

<sup>25</sup> BVerfG NJW 2020, 2235 (2248).

erlangten Analysemöglichkeiten enorm. Die Überwachung erfasse damit tief in den Alltag hineinreichende, auch höchst private und spontane Kommunikationsvorgänge.<sup>26</sup>

Dennoch sei eine anlasslose Überwachung, also eine Überwachung ohne objektivierbare Eingriffsschwelle, grundsätzlich möglich. Dies gelte selbst dann, wenn personenbezogene formale Suchbegriffe eingesetzt werden.<sup>27</sup> Das BVerfG begründet dies zum einen damit, dass dem BND selbst keine operativen Befugnisse zustehen,<sup>28</sup> zum anderen mit dem überragenden öffentlichen Interesse an einer wirksamen Auslandsaufklärung.<sup>29</sup> Das BVerfG bezieht sich insoweit insbesondere auf Aktivitäten, die auf eine Destabilisierung des Gemeinwesens abzielen oder eine Bedrohung der verfassungsmäßigen Ordnung darstellen und demonstriert hierbei seine Fähigkeit, Entscheidungen am Zeitgeist und den aktuellen Herausforderungen auszurichten.<sup>30</sup>

Beispielhaft nennt das BVerfG insoweit die Herausforderungen durch weltweit verflochtene Kreise organisierter Kriminalität und Geldwäsche wie auch Menschenhandel, elektronische Angriffe auf informationstechnische Systeme, den internationalen Terrorismus oder den Handel mit Kriegswaffen.<sup>31</sup>

Allerdings habe der Gesetzgeber die Zwecke für eine anlasslose Überwachung zu präzisieren.<sup>32</sup> Zudem müsse der Gesetzgeber Verfahrensregelungen schaffen, die die Ausrichtung auf die jeweiligen Zwecke rationalisierend strukturieren und damit kontrollierbar machen. Sowohl die Auswahl der Suchbegriffe als auch die Auswahl der Übertragungswege müssen einer unabhängigen Kontrolle zugänglich gemacht werden.<sup>33</sup> Der Gesetzgeber habe weiter dafür Sorge zu tragen, dass die Streubreite der Maßnahme eingeschränkt werde. So habe er dafür Sorge zu tragen, einschränkende Maßgaben zum Volumen der auszuleitenden Daten vorzugeben. Diese Maßgabe entspricht der Forderung des DAV in seiner Stellungnahme vom Oktober 2016 (Nr. 65/2016), in der unter Verweis auf § 10 Abs. 4 S. 4 G-10 dafür plädiert wurde, den

---

<sup>26</sup> BVerfG NJW 2020, 2235 (2248).

<sup>27</sup> BVerfG NJW 2020, 2235 (2250 f., 2253).

<sup>28</sup> BVerfG NJW 2020, 2235 (2251).

<sup>29</sup> BVerfG NJW 2020, 2235 (2250).

<sup>30</sup> BVerfG NJW 2020, 2235 (2250).

<sup>31</sup> BVerfG NJW 2020, 2235 (2250).

<sup>32</sup> BVerfG NJW 2020, 2235 (2251).

<sup>33</sup> BVerfG NJW 2020, 2235 (2252).

Anteil der auf den Übertragungswegen zur Verfügung stehenden Übertragungskapazitäten auf 20 % zu begrenzen.

Der DAV begrüßt ausdrücklich, dass das BVerfG ferner vorgegeben hat, dass besondere Anforderungen an den Schutz von Vertraulichkeitsbeziehungen – wie insbesondere zwischen Journalisten und ihren Informanten oder Rechtsanwälten und ihren Mandanten – zu stellen sind.<sup>34</sup>

Schließlich sei die Höchstspeicherdauer auf sechs Monate zu beschränken.<sup>35</sup>

Von besonderem Eingriffsgewicht sei die strategische Telekommunikationsüberwachung, wenn sie gezielt zur personenbezogenen Überwachung eingesetzt werde.<sup>36</sup> Zwar könne auch in diesen Fällen eine anlasslose Überwachung möglich sein, die Grenze einer möglichen Ermächtigung liege aber dort, wo der Einsatz eines personenbezogenen Suchbegriffs von vornherein mit annähernd vergleichbarer Sicherheit und Wirkung wie eine Einzelanordnung zu einer individualisierenden Überwachung des Telekommunikationsverkehrs führe.<sup>37</sup> Das BVerfG betont, dass der Gesetzgeber sicherstellen müsse, dass dann die diesbezüglichen Anforderungen gewahrt und nicht durch die strategische Überwachung unterlaufen werden.<sup>38</sup> Verwendet der BND somit Suchbegriffe, die auf die Überwachung der Telekommunikation einer bestimmten Person abzielen, hat der BND die entsprechenden Eingriffsschwellen einzuhalten. Das BVerfG verweist insoweit auf seine Entscheidung zur heimlichen Überwachung nach dem BKAG und somit auf die von ihm dort statuierten Eingriffsschwellen.<sup>39</sup> Entsprechend sind Überwachungsmaßnahmen, die sich gezielt gegen bestimmte Personen richten, einer gerichtsähnlichen *ex-ante* Kontrolle zu unterziehen.<sup>40</sup>

---

<sup>34</sup> BVerfG NJW 2020, 2235 (2253).

<sup>35</sup> BVerfG NJW 2020, 2235 (2253).

<sup>36</sup> BVerfG NJW 2020, 2235 (2249).

<sup>37</sup> BVerfG NJW 2020, 2235 (2253).

<sup>38</sup> BVerfG NJW 2020, 2235 (2253).

<sup>39</sup> BVerfGE 141, 220 (268 ff.).

<sup>40</sup> BVerfG NJW 2020, 2235 (2253).

### III. Übermittlung von Daten aus der strategischen Telekommunikation-überwachung

Bedeutsam sind ferner die vom BVerfG aufgestellten Maßstäbe zur Übermittlung von Daten aus der Ausland-Ausland-Fermeldeaufklärung. Das BVerfG stellt dabei erneut klar, dass die Übermittlung von Daten einen im Vergleich zur Erhebung eigenständigen Grundrechtseingriff darstellt. Übermittlungen bedürfen somit einer eigenen normenklaren und hinreichend bestimmten Rechtsgrundlage.<sup>41</sup>

Anders als die noch zu schaffende Rechtsgrundlage für die anlasslose Datenerhebung müsse eine Rechtsgrundlage für die Datenübermittlung jedenfalls dann eine Eingriffsschwelle vorsehen, wenn die Datenübermittlung nicht lediglich der politischen Information der Bundesregierung dient, sondern an operativ tätige Behörden erfolgen würden.<sup>42</sup>

Wörtlich heißt es in der Entscheidung:

*„Wenn schon die Datenerhebung für die Auslandsaufklärung selbst keine nachprüfbaren Eingriffsschwellen voraussetzt und damit ermöglichen soll, bereits weit im Vorfeld von konkreten Gefahren Bedrohungen und Gefährdungen zu ermitteln und nach ihnen proaktiv zu suchen, setzt dies verfassungsrechtlich im Gegenzug voraus, dass entsprechende Eingriffsschwellen wenigstens für die Übermittlung der hieraus gezogenen Erkenntnisse gelten müssen [...]. Danach kommt es für die Verfassungsmäßigkeit der Übermittlung auch hier darauf an, ob die Daten nach verfassungsrechtlichen Maßstäben für den Übermittlungszweck mit vergleichbar eingriffsintensiven Mitteln erhoben werden dürften“<sup>43</sup>*

Das BVerfG bemüht zutreffend den Gedanken der hypothetischen Datenneuerhebung<sup>44</sup> und nimmt Bezug auf die strafprozessualen und gefahrenabwehrrechtlichen Vorschriften zur Wohnraumüberwachung und Online-Durchsuchung und die dort geltenden Eingriffsschwellen.<sup>45</sup>

---

<sup>41</sup> BVerfG NJW 2020, 2235 (2255).

<sup>42</sup> BVerfG NJW 2020, 2235 (2256).

<sup>43</sup> BVerfG NJW 2020, 2235 (2256).

<sup>44</sup> BVerfG NJW 2020, 2235 (2256).

<sup>45</sup> BVerfG NJW 2020, 2235 (2256).

Sollen die Daten aus der strategischen Telekommunikationsüberwachung dagegen an eine ausländische Stelle übermittelt werden, bedarf es darüber hinaus einer Rechtsstaatlichkeitvergewisserung über den Umgang der ausländischen Stelle mit den ihnen übermittelten Daten, weil die Daten ab diesem Zeitpunkt nicht mehr den Anforderungen des Grundgesetzes unterliegen.<sup>46</sup> Eine Rechtsstaatlichkeitvergewisserung in diesem Sinne schließe neben der Wahrung der Menschenrechte bei der Nutzung der Information die Wahrung der datenschutzrechtlichen Garantien ein und müsse durch die Einholung belastbarer Zusagen der Empfänger sichergestellt werden.<sup>47</sup> Der Staat müsse sich zudem durch das jeweilige Empfängerland Auskunftsrechte zusichern lassen,<sup>48</sup> die eine nachvollziehbare Kontrolle der Einhaltung international-menschenrechtlicher Voraussetzungen ermöglichen, und sich selbst davon vergewissern, dass diese Anforderungen auch eingehalten werden.<sup>49</sup>

Aus diesen Maßstäben des BVerfG folgt nach Auffassung des DAV, dass ein Verzeichnis von ausländischen Partnerdiensten geschaffen werden muss, das solche ausländischen Partnerdienste führt, die der vom BVerfG geforderten Rechtsstaatlichkeitsvergewisserung gerecht werden. Zudem müssen Regelungen geschaffen werden, die sicherstellen, dass die Berichte über die Rechtsstaatlichkeit der Partnerdienste fortlaufend aktualisiert und geprüft werden. Zudem muss eine ausreichende Kontrolle dieser Rechtsstaatlichkeitsvergewisserung durch das Parlament, insbesondere durch das PKGr, sichergestellt werden.

#### **IV. Kooperation mit ausländischen Nachrichtendiensten**

Im Hinblick auf die Kooperation mit ausländischen Nachrichtendiensten hat das BVerfG entschieden, dass eine Zusammenarbeit bei der Telekommunikationsüberwachung so gestaltet sein müsse, dass der grundrechtliche Schutz nicht unterlaufen werde. Dies schließe insbesondere aus, dass ausländische Nachrichtendienste dem BND ihrerseits

---

<sup>46</sup> BVerfG NJW 2020, 2235 (2258).

<sup>47</sup> BVerfG NJW 2020, 2235 (2258).

<sup>48</sup> BVerfG NJW 2020, 2235 (2258).

<sup>49</sup> BVerfG NJW 2020, 2235 (2258).

etwaige Erkenntnisse aus auf Deutschland bezogenen Überwachungsmaßnahmen zur Verfügung stellen.<sup>50</sup>

Eine Zusammenarbeit müsse unter striktem Schutz der Inlandskommunikation erfolgen.<sup>51</sup>

Schließlich müssen die von einem ausländischen Nachrichtendienst bestimmten Suchbegriffe anhand der grundrechtlichen Grenzen ebenso kontrolliert werden wie die hieran anknüpfenden Trefferfälle.<sup>52</sup>

Daten von besonders schutzbedürftigen Personen wie Dissidenten, Whistleblowern, Rechtsanwälten und Journalisten seien von vornherein auszufiltern.<sup>53</sup>

## **V. Kontrolle**

Die wohl bedeutsamste Vorgabe des BVerfG an den Gesetzgeber ist die Forderung nach einer effektiven und unabhängigen Kontrolle sämtlicher Ebenen der strategischen Telekommunikationsüberwachung (Erhebung, Auswertung, Übermittlung, Kooperation, Löschung). Das BVerfG verlangt diese unabhängige Kontrolle insbesondere als Ausgleich dafür, dass Transparenz und individueller Rechtsschutz gegen die Maßnahmen des BND aufgrund der Geheimheit der Maßnahmen erheblich zurückgenommen sind.<sup>54</sup>

Zwar sieht das BNDG mit der G10-Kommission, dem Bundesdatenschutzbeauftragten und dem Unabhängigen Gremium Kontrollinstanzen vor. Eine effektive Kontrolle fand in der Vergangenheit indes nicht statt, was auch durch die Vertreter der jeweiligen Kontrollinstanzen gerügt worden war. Als Grund für den Mangel an effektiver Kontrolle wurde neben fehlenden Kontrollinstrumenten insbesondere die fehlende Kooperationsbereitschaft des BND angeführt, der etwa die Herausgabe von (ungeschwärzten) Dokumenten regelmäßig mit dem Hinweis auf die gegenüber

---

<sup>50</sup> BVerfG NJW 2020, 2235 (2260).

<sup>51</sup> BVerfG NJW 2020, 2235 (2260).

<sup>52</sup> BVerfG NJW 2020, 2235 (2261).

<sup>53</sup> BVerfG NJW 2020, 2235 (2261).

<sup>54</sup> BVerfG NJW 2020, 2235 (2262).

ausländischen Nachrichtendiensten abgegebene Vertraulichkeitserklärungen („Third Party Rule“) verweigerte.

Das BVerfG zwingt den Gesetzgeber nunmehr zur Schaffung einer echten Kontrolle des BND, die sämtliche Ebenen der Datenerhebung und -verarbeitung umfasst und in Teilen „gerichtsähnlich“ ausgestaltet sein muss.<sup>55</sup> Wörtlich heißt es in der Entscheidung:

*„Die strategische Telekommunikationsüberwachung ist danach mit den Anforderungen der Verhältnismäßigkeit nur vereinbar, wenn sie durch eine ausgebaute unabhängige objektivrechtliche Kontrolle flankiert ist.“*<sup>56</sup> Diese Kontrolle sei als kontinuierliche Rechtskontrolle auszugestalten, die einen umfassenden Kontrollzugriff ermöglicht.

Ausweislich der Entscheidung des BVerfG muss die Kontrolle des BND auf zwei Säulen gestützt werden. So differenziert das BVerfG in seiner Entscheidung zwischen der Kontrolle durch eine *gerichtsähnlich* ausgestaltete Stelle<sup>57</sup> und einer unabhängigen Rechtskontrolle *administrativen* Charakters<sup>58</sup>.

Die gerichtsähnliche Kontrolle habe die Schutzaufgabe zu erfüllen, die sonst dem Richtervorbehalt sowie auch nachträglichen Rechtsschutzmöglichkeiten, insbesondere Feststellungsklagen, zukomme. Entsprechend müsse mit ihr eine auf den Einzelfall bezogene Prüfung ermöglicht werden, die materiell und verfahrensmäßig einer gerichtlichen Kontrolle gleichwertig, insbesondere mindestens ebenso wirkungsvoll sei.<sup>59</sup> Für die gerichtsähnliche Kontrolle ist eine Unabhängigkeit der zur Entscheidung berufenen Mitglieder sicherzustellen, die einer richterlichen Unabhängigkeit gleichkommt. Insbesondere müssen sie weisungsfrei und auf hinreichend lange und bestimmte Zeit fest berufen sein. Für die Zusammensetzung der Spruchkörper ist zu gewährleisten, dass der richterlichen Perspektive ein maßgebliches Gewicht zukommt, die für eine maßgebliche Zahl der Mitglieder durch langjährige richterliche Erfahrung belegt sein muss.<sup>60</sup>

---

<sup>55</sup> BVerfG NJW 2020, 2235 (2263).

<sup>56</sup> BVerfG NJW 2020, 2235 (2262 f.).

<sup>57</sup> BVerfG NJW 2020, 2235 (2263).

<sup>58</sup> BVerfG NJW 2020, 2235 (2263).

<sup>59</sup> BVerfG NJW 2020, 2235 (2263).

<sup>60</sup> BVerfG NJW 2020, 2235 (2264).

Die unabhängige Kontrolle administrativen Charakters soll dagegen eine Wächteraufgabe erfüllen. Namentlich soll sie den gesamten Prozess der strategischen Überwachung eigeninitiativ mittels Stichproben auf seine Rechtmäßigkeit überprüfen.

Ferner soll dem administrativen Kontrollorgan die Möglichkeit gegeben werden, das gerichtsähnliche Entscheidungsgremium anzurufen.<sup>61</sup>

Sowohl im Falle der gerichtsähnlichen Kontrolle als auch im Falle der administrativen Kontrolle sei eine kontinuierliche Kontrolle in institutioneller Eigenständigkeit zu garantieren. Hierzu gehören ein den Kontrollinstanzen zugewiesenes eigenes Budget und – abgesehen von der Ernennung der Mitglieder der gerichtsähnlichen Spruchkörper und der Leitungsebene – eine eigene Personalhoheit. Die Kontrollinstanzen müssen in ihrer Arbeit von Einflussnahmen wirksam abgeschirmt und insoweit mit vollständiger Unabhängigkeit ausgestattet sein.<sup>62</sup> Der Gesetzgeber habe die Kontrolle zudem organisatorisch so auszugestalten, dass sie die „Third Party Rule“ nicht behindere.<sup>63</sup>

Schließlich ist beiden Kontrollinstanzen umfassend Zugang zu allen Unterlagen sowie jederzeit Zutritt zu den Diensträumen zu gewähren.<sup>64</sup> Die Kontrolle darf nicht unter Berufung auf die „Third Party Rule“ behindert werden.<sup>65</sup>

Der Gesetzgeber habe insoweit die Bedingungen dafür zu schaffen, dass die mit der Rechtskontrolle betrauten Instanzen nicht mehr als „Dritte“ im Sinne der „Third Party Rule“ angesehen werden.<sup>66</sup>

Der DAV, der bereits in seiner Stellungnahme vom Oktober 2016 (Stellungnahme Nr. 65/2016) die mangelhaften Kontrollmöglichkeiten im Hinblick auf die Arbeit des BND gerügt hatte,<sup>67</sup> begrüßt diese umfangreichen Vorgaben des BVerfG.

Aus den Vorgaben des BVerfG folgt, dass der Gesetzgeber das Unabhängige Gremium als gerichtsähnliche Kontrollinstanz nach den Maßgaben des Urteils ausgestalten und

---

<sup>61</sup> BVerfG NJW 2020, 2235 (2263).

<sup>62</sup> BVerfG NJW 2020, 2235 (2264).

<sup>63</sup> BVerfG NJW 2020, 2235 (2264).

<sup>64</sup> BVerfG NJW 2020, 2235 (2265).

<sup>65</sup> BVerfG NJW 2020, 2235 (2265).

<sup>66</sup> BVerfG NJW 2020, 2235 (2265).

<sup>67</sup> DAV Stellungnahme Nr. 65/2016, S. 7.

ausstatten muss. Neben umfangreichen Zugangsrechten sind insbesondere die personellen Voraussetzungen für eine effektive Kontrolle zu schaffen.

Darüber hinaus hat der Gesetzgeber eine unabhängige Rechtskontrolle administrativen Charakters zu schaffen.

## **E. Zum Regierungsentwurf**

Der nun vorgelegte Regierungsentwurf (im Folgenden: RegE) bleibt weit hinter den Anforderungen zurück, die das BVerfG an eine verfassungskonforme Ausgestaltung des BNDG stellt. Dies ist insbesondere deshalb bemerkenswert, weil das Bundesverfassungsgericht besonders detailreiche Maßstäbe zur Schaffung eines verfassungskonformen BNDG statuiert hat. Dass diese Maßstäbe nunmehr augenscheinlich ignoriert werden, kann nur als Provokation verstanden werden. Auch und insbesondere die avisierte personelle Ausstattung des Unabhängigen Kontrollrats ist ungenügend und führt dazu, dass eine effektive Kontrolle der Überwachungstätigkeit des BND von vornherein vereitelt wird.

### **I. Datenerhebung**

#### **1. Strategische Ausland-Ausland-Fernmeldeaufklärung (§ 19 BNDG-E)**

§ 19 BNDG-E enthält die Rechtsgrundlage zur strategischen Ausland-Ausland-Fernmeldeaufklärung.

##### *a) Unzureichende Konkretisierung der Zwecke*

Zwar legt § 19 BNDG-E erstmals – entsprechend den Vorgaben des BVerfG<sup>68</sup> – konkrete Zwecke fest, nach denen die strategische Ausland-Ausland-Fernmeldeaufklärung zulässig sein soll. Diese soll namentlich zulässig sein für politische Zwecke (Abs. 1 Nr. 1) sowie zur Früherkennung von aus dem Ausland drohenden Gefahren von internationaler Bedeutung (Abs. 1 Nr. 2). Der Begriff der Gefahr wird sodann in Abs. 4 näher konkretisiert. Zu begrüßen ist, dass der Regierungsentwurf im Vergleich zum Referentenentwurf nun nicht mehr den

---

<sup>68</sup> BVerfG NJW 2020, 2235 (2251).

Auffangtatbestand der „vergleichbare(n) Fälle“ vorsieht, der entgegen dem verfassungsrechtlichen Bestimmtheitsgebot zu einer uferlosen Anwendung von § 19 BNDG geführt hätte.

Dennoch soll der BND die Massenüberwachung des § 19 BNDG auch zur Gewinnung von Erkenntnissen über Migrationsbewegungen in Richtung der Bundesrepublik Deutschland einsetzen dürfen.<sup>69</sup> Es liegt auf der Hand, dass der Entwurf u.a. auf die sog. Seenotrettung angewendet werden soll. Die Überwachung humanitärer Rettungsmissionen durch den deutschen Nachrichtendienst ist aus Sicht des DAV nicht akzeptabel.<sup>70</sup>

Dass der Regierungsentwurf in diesem Zusammenhang zudem offenbart, einer überkommenden Tätertypenlehre anzuhängen („Schleuser, Dokumentenfälscher, Menschenhändler“<sup>71</sup>), soll hier nur am Rande angemerkt werden.

#### *b) Unzureichende Kontrolle der verwendeten Selektoren*

Wesentlich schwerer wiegt indes, dass der Entwurf keine Kontrolle der im Rahmen der Ausland-Ausland-Fernmeldeaufklärung verwendeten Suchbegriffe bzw. Selektoren vorsieht. Hierin liegt ein klarer Verstoß gegen die Vorgaben des BVerfG, wonach auch die „Auswahl der Suchbegriffe“ einer unabhängigen Kontrolle zugänglich gemacht werden muss.<sup>72</sup>

Zwar enthalten § 23 Abs. 4 und 6 BNDG-E Regelungen, wonach der unabhängige Kontrollrat die Rechtmäßigkeit der Anordnung von strategischen Aufklärungsmaßnahmen vor deren Vollzug kontrolliert. Die schriftlichen Anordnungen enthalten aber gerade *nicht* die ausgewählten Suchbegriffe, die zur strategischen Ausland-Ausland-Fernmeldeaufklärung verwendet werden sollen, sondern lediglich den Aufklärungszweck, das verfolgte Thema, den geografischen Fokus, die Dauer und eine Begründung (vgl. § 23 Abs. 2 BNDG-E) sowie die Aufklärungsmaßnahme, das Ziel und die Dauer der gezielten Datenerhebung (§ 23 Abs. 6 BNDG-E).

---

<sup>69</sup> RegE S. 65, 67.

<sup>70</sup> Die illegale Migration wird unter „Auswirkungen krisenhafter Entwicklung im Ausland“ bzw. unter „organisierte kriminelle Strukturen“ subsumiert, vgl. RegE S. 65, 67.

<sup>71</sup> RegE S. 67.

<sup>72</sup> BVerfG NJW 2020, 2235 (2252).

Entgegen der Vorgaben des BVerfG wird die Offenlegung der verwendeten Suchbegriffe im BNDG-E ausdrücklich ausgeschlossen. So heißt es in § 23 Abs. 6 S. 3 BNDG-E: *„Die Nennung einzelner Suchbegriffe [...] ist nicht erforderlich“*.

Das Bundeskanzleramt versucht somit augenscheinlich, durch eine sehr eigenwillige Interpretation der Vorgaben des BVerfG diese im Ergebnis zu umgehen. Schließlich hat das BVerfG explizit entschieden, dass die Auswahl der Suchbegriffe einer unabhängigen Kontrolle unterliegen müsse.<sup>73</sup> Damit sind aber nicht (nur) der Prozess der Auswahl der Suchbegriffe gemeint, sondern selbstverständlich auch die Suchbegriffe selbst. Die Regelung, dass die Suchbegriffe gerade nicht offengelegt werden (müssen), verletzt somit evident die Vorgaben des BVerfG, weil eine unabhängige Kontrolle der mittels Suchbegriffe durchgeführten Überwachung ohne Kenntnis von den ausgewählten Suchbegriffen praktisch schlicht unmöglich ist. Diesbezüglich ist aus Sicht des DAV zwingend nachzubessern.

*c) Unzureichende Verfahrensregelungen zur Sicherstellung der Zweckbindung*

Schließlich fehlen auch die vom BVerfG geforderten Verfahrensregelungen, die die Ausrichtung auf die jeweiligen Zwecke rationalisierend strukturieren und damit auch kontrollierbar machen.<sup>74</sup> Mangels Kenntnis der Kontrollinstanzen von der Auswahl der Suchbegriffe können diese auch nicht kontrollieren, ob die Überwachung tatsächlich auf den dargelegten Zweck ausgerichtet ist. Auch insoweit ist zwingend nachzubessern.

---

<sup>73</sup> BVerfG NJW 2020, 2235 (2252).

<sup>74</sup> BVerfG NJW 2020, 2235 (2252).

## **2. Besondere Formen der strategischen Ausland-Fernmeldeaufklärung (§ 20 BNDG-E)**

Mit § 20 BNDG-E soll eine Rechtsgrundlage zur gezielten Datenerhebung geschaffen werden. Zwar sind Datenerhebungen mit dem Ziel der umfassenden Aufklärung von Personen in § 20 Abs. 2 BNDG-E ausdrücklich nicht vorgesehen, und nach § 20 Abs. 3 BNDG-E ist die individualisierte Überwachung des gesamten Telekommunikationsverkehrs einer Person unzulässig. Jedoch soll die gezielte Erhebung von personenbezogenen Daten von Personen bei Vorliegen der Voraussetzungen des Absatzes 3 weiterhin möglich bleiben.<sup>75 76</sup> Zudem wird der Anwendungsbereich der Norm durch § 20 Abs. 2 BNDG-E in unzulässiger Weise auf „mögliche Verursacher“ erweitert.

Der Regierungsentwurf verlangt für die gezielte Erhebung von personenbezogenen Daten, dass „tatsächliche Anhaltspunkte“ dafür vorliegen, dass die hiervon betroffenen Personen Verursacher sind. Auch wenn der nun vorgelegte Entwurf von einer bloßen Möglichkeit einer Verursachereigenschaft Abstand genommen hat, spricht die Entwurfsbegründung dennoch von „Personen, die als mögliche Verursacher von Gefahren“ beeinträchtigt werden.<sup>77</sup> § 20 Abs. 2 BNDG sollte deshalb zur weitergehenden Konkretisierung den gefahrenabwehrrechtlichen Begriff des Störers verwenden.

## **3. Online-Durchsuchung (§ 34 BNDG-E)**

Die §§ 34 ff. BNDG-E sollen dem BND die Befugnis zur sog. Online-Durchsuchung geben. Nach § 34 BNDG-E soll es dem BND möglich sein, zur Erfüllung seiner Aufgaben ohne Wissen der betroffenen Person auf der Grundlage einer zuvor angeordneten individuellen Aufklärungsmaßnahme mit technischen Mitteln in von Ausländern im Ausland genutzte informationstechnische Systeme einzugreifen und aus ihnen gespeicherte personenbezogene Daten zu erheben, soweit dies erforderlich ist für den Zweck der politischen Unterrichtung der Bundesregierung (Nr. 1) oder der

---

<sup>75</sup> § 20 Abs. 3 BNDG-E lautet: „Die individualisierte Überwachung des gesamten Telekommunikationsverkehrs einer Person ist unzulässig.“

<sup>76</sup> Die noch im Ref-E vorgesehene Subjektivierung durch das „Ziel“ der umfassenden Aufklärung von Personen wurde gestrichen.

<sup>77</sup> RegE S. 75

Früherkennung von aus dem Ausland drohenden Gefahren<sup>78</sup> von internationaler Bedeutung (Nr. 2).

Es ist bereits grundsätzlich zweifelhaft, ob einem Auslandsgeheimdienst, der für die Früherkennung von Gefahren zuständig ist, überhaupt eine derart eingriffsintensive Maßnahme zur Verfügung gestellt werden sollte.

Zwar hatte das BVerfG in seinem Urteil zur Verfassungswidrigkeit des BNDG entschieden, dass eine Online-Durchsuchung nicht zwingend ausgeschlossen sein soll. Allerdings bedürfe es hierfür (ebenso wie zur Durchführung anderer Einzelanordnungen) „belastbarer Eingriffsschwellen“.<sup>79</sup> Die „belastbaren Eingriffsschwellen“ hatte das BVerfG bereits in seiner Entscheidung zur Online-Durchsuchung eindeutig formuliert und entschieden, dass

*„[e]in derartiger Eingriff [...] nur vorgesehen werden [darf], wenn die Eingriffsermächtigung ihn davon abhängig macht, dass tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen. Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen.“<sup>80</sup>*

Danach setzt eine Online-Durchsuchung wenigstens „tatsächliche Anhaltspunkte einer konkreten Gefahr“ für die genannten besonders schützenswerten Rechtsgüter voraus. Auch in seiner Entscheidung zur Verfassungswidrigkeit des BNDG verweist das BVerfG in diesem Zusammenhang auf seine Entscheidung zum BKAG, in welcher es die Eingriffsschwellen definiert hat, die nunmehr in § 49 BKAG Niederschlag gefunden haben. Die in den §§ 34 ff. BNDG-E geregelten Eingriffsschwellen bleiben jedoch weit hinter diesen zurück. Diese evidente Missachtung der eindeutigen Vorgaben des BVerfG stellt letztlich eine unnötige Provokation dar, die das verfassungsrechtliche Haltbarkeitsdatum einer solchen Neuregelung erheblich verringern dürfte.

---

<sup>78</sup> RegE S. 46.

<sup>79</sup> BVerfG NJW 2020, 2235 (2249).

<sup>80</sup> BVerfGE 120, 274 Rn. 243.

§ 49 BKAG erlaubt – entsprechend der eindeutigen Vorgaben des BVerfG – eine Online-Durchsuchung grundsätzlich nur zur Abwehr einer tatsächlich bestehenden Gefahr für Leib, Leben oder Freiheit einer Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt. § 34 BNDG-E enthält keine solche Eingriffsschwelle. Vielmehr soll eine Online-Durchsuchung „zur Früherkennung“ von aus dem Ausland „drohenden Gefahren“ sowie zur politischen Unterrichtung der Bundesregierung zulässig sein. Die von § 49 BKAG unter Zugrundelegung der Rechtsprechung des BVerfG statuierte Eingriffsschwelle soll danach gleich in zweifacher Hinsicht abgesenkt werden. Dies erscheint aus Sicht des DAV nicht hinnehmbar.

§ 34 BNDG-E verstößt somit in eklatanter Weise gegen die vom BVerfG aufgestellten Maßstäbe. Der DAV fordert daher, die Maßnahme der Online-Durchsuchung in der vorgesehenen Form nicht umzusetzen und sich die Frage zu stellen, ob eine solche Eingriffsbefugnis, gepaart mit der staatlichen Befugnis zum uneingeschränkten Hacking überhaupt erforderlich ist.

#### **4. Unzureichender Schutz von Vertraulichkeitsbeziehungen (§§ 21, 35 BNDG-E)**

§ 21 BNDG-E und § 35 BNDG-E enthalten zwar Regelungen zum Schutz von Vertraulichkeitsbeziehungen im Zuge der Datenerhebung. Der Schutz von Vertraulichkeitsbeziehungen ist jedoch mangelhaft ausgestaltet und damit faktisch wirkungslos. An dieser Stelle muss dringend nachgebessert werden.

##### *a) Fehlende Definition von Journalisten*

In dem Gesetz selbst wird die Berufsgruppe der Journalisten (ebenso wie alle anderen Berufsgruppen) nicht definiert. Die Regelung dieser zentralen Frage, wer Journalist ist, soll dem BND in einer (geheimen) Dienstvorschrift überlassen werden. Gerade bei Journalisten kann dies zu einer Umgehung des verfassungsrechtlich gebotenen Schutzes führen. Es ist daran zu erinnern, dass nicht selten in autoritären Regimes

kritischen Journalisten der Status als solcher aberkannt wird. Es dürfte den verfassungsrechtlichen Anforderungen nicht gerecht werden, diese wesentliche Frage nicht im Gesetz selbst zu regeln. Der im Entwurf gewählte Weg konterkariert zudem die Möglichkeiten effektiver Kontrolle.

*b) Unzureichender Schutz von Vertraulichkeitsbeziehungen im Falle der Massenüberwachung nach § 19 BNDG-E*

Der durch §§ 21 und 35 BNDG-E gewährte besondere Schutz von Vertraulichkeitsbeziehungen beschränkt sich auf die Fälle der „gezielten“ Datenerhebung. Werden Datenerhebungen dagegen lediglich nach § 19 BNDG-E und nicht gezielt i.S.d. § 20 Abs. 2 BNDG-E zur Überwachung von Vertraulichkeitsbeziehungen verwendet, werden diese auch nicht besonders geschützt. Der DAV fordert, einen effektiven Schutz von Vertraulichkeitsbeziehungen für Überwachungsmaßnahmen gemäß § 19 BNDG-E zu schaffen. Die Beschränkung besonderer Schutzmaßnahmen auf die Maßnahmen der gezielten Überwachung ist ungenügend.

*c) Unzulässige Beschränkung des besonderen Schutzes auf Kommunikation innerhalb einer Vertraulichkeitsbeziehung*

§ 21 BNDG-E soll Vertraulichkeitsbeziehungen unter einen besonderen Schutz stellen. Der Anwendungsbereich ist allerdings deutlich zu eng ausgestaltet.

Zwar erklärt § 21 BNDG-E die gezielte Verwendung von Suchbegriffen nach § 19 Absatz 5 BNDG-E zum Zweck der ausschließlichen Erhebung von personenbezogenen Daten, die aus einer Kommunikation innerhalb einer Vertraulichkeitsbeziehung stammen, für *grundsätzlich* unzulässig. Vertraulichkeitsbeziehungen sollen aber nur solche Beziehungen von Geistlichen, Rechtsanwälten und Journalisten *zu Dritten* sein, die dem Schutz des § 53 Absatz 1 Satz 1 Nr. 1, 2, 3 und 5 sowie S. 2 StPO unterfallen. Dritte, die dem Schutz des § 53 Absatz 1 Satz 1 Nr. 1, 2, 3 und 5 sowie S. 2 StPO unterfallen, sind ihrerseits solche Personen, die die Hilfe und Sachkunde der Berufsangehörigen i.S. des § 53 StPO in Anspruch nehmen.<sup>81</sup>

---

<sup>81</sup> Meyer-Goßner/Schmitt, StPO, 63. Aufl. 2020, § 53 Rn. 1.

Das hätte zur Folge, dass etwa die Kommunikationsbeziehung des betroffenen Rechtsanwalts zu seinen Rechtsanwaltskollegen und Anwaltsgehilfen ebenso vom Schutz des § 21 BNDG-E ausgeschlossen sein soll, wie die Kommunikation zwischen Journalisten und ihrer Redaktion. Diese Auslegung wird auch durch die Entwurfsbegründung bestätigt. Hier heißt es: „*Die Bestimmung bezweckt somit im Hinblick auf Rechtsanwältinnen und Rechtsanwälte den Schutz der Vertraulichkeitsbeziehung zum Mandanten und der ihnen in dieser Eigenschaft anvertrauten Informationen.*“<sup>82</sup>

Dadurch wird der durch § 21 BNDG-E vermeintlich erzeugte besondere Schutz von vornherein ausgehöhlt, weil damit die *Weitergabe* von Informationen aus der geschützten Kommunikation überwacht werden kann. Ein Journalist, der Informationen eines Informanten an seine Redaktion weiterleitet, müsste also befürchten, dass diese vom BND abgefangen werden. Ebenso dürfte ein Rechtsanwalt Informationen, die ihm sein Mandant mitgeteilt hat, nicht an sein Sekretariat zwecks Speicherung übermitteln oder in sonstiger Weise darüber kommunizieren, weil es sich nicht um Kommunikation mit der Person handelt, die ihre Hilfe und Sachkunde in Anspruch genommen hat.

Zwar schützen auch die Vorschriften zum Schutz von Vertraulichkeitsbeziehungen in der StPO nur die Kommunikation zwischen der Vertrauensperson und dem Betroffenen. In diesem Fall muss die Vertrauensperson aber nicht befürchten, ihrerseits überwacht zu werden, weil es hierfür einen gegen sie gerichteten qualifizierten Anfangsverdacht und eine entsprechende Überwachungs(einzel-)anordnung geben muss. Im Falle der Massenüberwachung nach § 19 BNDG-E wird die Kommunikation von Vertrauenspersonen mit ihren Kolleginnen und Kollegen oder anderen Berufshelfern, z.B. die Kommunikation zwischen einem Journalisten und seiner Redaktion oder einer Anwältin und ihrem Sekretariat, automatisch miterfasst, sofern sie über einen vom BND überwachten Internetknotenpunkt abläuft.

Die Beschränkung des besonderen Schutzes von Vertraulichkeitsbeziehungen ist somit im Falle einer Massenüberwachung wie der strategischen Ausland-Ausland-Fernmeldeaufklärung von vornherein wirkungslos.

---

<sup>82</sup> RegE S. 76.

Der DAV fordert daher, nicht nur die Vertraulichkeitsbeziehung und somit die Kommunikationsbeziehung zu Dritten besonders zu schützen, die dem Schutz des § 53 StPO unterfallen, sondern *sämtliche* Kommunikationsbeziehungen der in § 53 StPO genannten Berufsgruppen, sofern sie in ihrer beruflichen Funktion tätig werden. Nur eine solche gesetzliche Ausgestaltung entspricht den Vorgaben des BVerfG und berücksichtigt die tatsächliche Praxis der Arbeitsweise von Angehörigen besonders geschützter Berufsgruppen. Auch das BVerfG hat nicht (nur) die Kommunikationsbeziehung eines Angehörigen dieser Berufs- oder Personengruppe als besonders schutzwürdig angesehen. Vielmehr erklärt das BVerfG Angehörige der in § 53 StPO genannten Berufsgruppen als solche für besonders schutzwürdig.

Wörtlich führt das BVerfG aus:

*„Die Nutzung von Suchbegriffen, die zu einer gezielten **Erfassung der Telekommunikationsanschlüsse solcher Personen** führen, kann nicht schon allein damit gerechtfertigt werden, dass hierdurch potentiell nachrichtendienstlich relevante Informationen erlangt werden können. Die journalistische Tätigkeit rechtfertigt nicht, Personen einem höheren Risiko der Überwachung auszusetzen als andere Grundrechtsträger und sie wegen ihrer Kontakte und Recherchen zum Objekt der Informationsabschöpfung zur Verfolgung von Sicherheitsinteressen zu machen (vgl. BVerfGE 107, 299 <336>). Entsprechendes gilt für Rechtsanwältinnen und Rechtsanwälte.“<sup>83</sup>*

Besonders schützenswert ist also nicht (nur) die Kommunikation innerhalb einer Vertraulichkeitsbeziehung, sondern die Kommunikation eines Berufsangehörigen i.S. des § 53 StPO als solche, sofern der oder die Berufsangehörige in dieser Eigenschaft kommuniziert.

d) *Streichung des Zwecks der „ausschließlichen“ Erhebung von personenbezogenen Daten*

---

<sup>83</sup> BVerfG NJW 2020, 2235 (2254).

Der DAV begrüßt im Übrigen, dass der Regierungsentwurf nun in § 21 Abs. 1 BNDG-E den Anwendungsbereich nicht mehr – wie noch im Referentenentwurf vorgesehen – auf die gezielte Verwendung von Suchbegriffen nach § 19 Abs. 5 BNDG-E zum Zweck der „ausschließlichen Erhebung von personenbezogenen Daten, die aus einer Kommunikation innerhalb einer Vertraulichkeitsbeziehung stammen“, beschränkt. Diese Streichung war aufgrund der besonderen Schutzbedürftigkeit der Vertrauensbeziehung sachlich zwingend geboten. Andernfalls würde der besondere Schutz des § 21 BNDG-E schon dann entfallen, wenn die gesamte Kommunikation eines Rechtsanwalts oder einer Rechtsanwältin überwacht werden würde, weil die Überwachung aufgrund der miterfassten Privatkommunikation keine „ausschließliche“ Erhebung von Daten aus einer Vertraulichkeitsbeziehung wäre.

*e) Gesteigerte Anforderungen an die Überwachung von Berufsgeheimnisträgern*

Der DAV begrüßt im Grundsatz ebenfalls, dass die gezielte Überwachung von Personen i.S. des § 53 StPO nur unter den restriktiven Voraussetzungen des § 21 Abs. 2 BNDG-E zulässig sein soll. Gemäß § 21 Abs. 2 S. 1 BNDG-E ist die Verwendung von Suchbegriffen nach Absatz 1 ausnahmsweise zulässig, sofern tatsächliche Anhaltspunkte dafür vorliegen, dass die in Absatz 1 Satz 2 aufgeführte Person Täter oder Teilnehmer einer der in § 29 Abs. 3 genannten Straftaten ist oder dies zur Verhinderung einer dort näher ausgeführten erheblichen Gefahr notwendig ist. Allerdings laufen diese gesteigerten Anforderungen aufgrund der dargestellten (unzulässigen) Beschränkung des Anwendungsbereichs von § 21 BNDG-E ins Leere.

## **5. Ausufernde Überwachungskapazität (§§ 19 Abs. 8, BNDG-E)**

Auch die vom Regierungsentwurf in vorgesehene Beschränkung des Volumens der strategischen Ausland-Ausland-Fernmeldeaufklärung auf 30 Prozent der bestehenden Telekommunikationsnetze ist nach wie vor unzureichend, § 19 Abs. 8 BNDG-E.<sup>84</sup>

Nach der Rechtsprechung des BVerfG liegt ein übergreifendes Ziel der sich aus dem Verhältnismäßigkeitsgrundsatz ergebenden Anforderungen darin, die strategische Telekommunikationsüberwachung trotz ihrer Streubreite als hinreichend fokussiertes Instrument auszugestalten und damit begrenzt zu halten. Eine globale und pauschale

---

<sup>84</sup> Der § 26 BNDG-E als Pendant enthält keine entsprechende Regelung..

Überwachung lässt das Grundgesetz auch zu Zwecken der Auslandsaufklärung nicht zu. Dafür hat der Gesetzgeber zunächst einschränkende Maßgaben zum Volumen der für die jeweiligen Übertragungswege auszuleitenden Daten vorzugeben und sicherzustellen, dass das von der Überwachung abgedeckte geographische Gebiet begrenzt bleibt. Da sich die technischen Möglichkeiten der Datenverarbeitung schnell ändern, reicht es nicht, hierfür allein auf tatsächlich bestehende Kapazitätsgrenzen zu verweisen.<sup>85</sup>

Nach §§ 19 Abs. 8 S. 2, BNDG-E sollen bis zu 30 Prozent der weltweiten Telekommunikationsnetze überwacht werden dürfen. § 19 Abs. 8 S. 2 BNDG-E enthält damit nicht die vom BVerfG geforderte Beschränkung des Überwachungsvolumens, sondern faktisch eine Erweiterung.

Auch wenn der Regierungsentwurf im Vergleich zum Referentenentwurf eine Herabsetzung des Anteils der überwachten Kommunikation von 50 Prozent auf 30 Prozent vorsieht, überschreitet er die in § 10 Abs. 4 S. 2 G 10 vorgesehene Kapazitätsgrenze von 20 Prozent um einen Drittel.

Zudem fehlt dem Regierungsentwurf die vom BVerfG geforderte Begrenzung der Überwachungsmaßnahme auf ein bestimmtes geographisches Gebiet. Der DAV fordert deshalb, die Überwachungskapazität in Gleichlauf mit § 10 Abs. 4 S. 2 G 10 auf 20 Prozent zu reduzieren und eine Pflicht zur geographischen Beschränkung der Überwachung einzuführen. Andernfalls könnte etwa 100 Prozent der Telekommunikation eines kleinen Staates überwacht werden, ohne dass dies dazu führen würde, dass das Überwachungsvolumen von 30 Prozent der *weltweiten* Kommunikation ausgeschöpft würde.

## **6. Unzulässige Überschreitung der zulässigen Höchstspeicherdauer von Verkehrsdaten (§ 26 Abs. 5 S. 2 BNDG-E)**

§ 26 Abs. 5 S. 2 BNDG-E sieht die Möglichkeit zur Speicherung von Verkehrsdaten über den Zeitraum von sechs Monaten hinaus vor, „*soweit sie für die Aufgabenerfüllung des Bundesnachrichtendienstes erforderlich ist*“.

---

<sup>85</sup> BVerfG NJW 2020, 2235 (2251).

Auf diese Weise schafft § 26 Abs. 5 S. 2 BNDG-E die Möglichkeit zur faktisch unbegrenzten Vorratsdatenspeicherung, weil eine Überprüfung der Erforderlichkeit der weiteren Speicherung gem. § 26 Abs. 5 S. 2 i.V.m. § 29 BNDG-E nur alle 7 Jahre vorgesehen ist. Die Unzulässigkeit einer solchen grenzenlosen Vorratsdatenspeicherung ist evident.

Der DAV fordert daher § 26 Abs. 5 S. 2 BNDG-E als Ausnahme zur Höchstspeicherfrist von 6 Monaten ersatzlos zu streichen. Eine Ausnahme von der Höchstspeicherfrist ist nach der Rechtsprechung des BVerfG auch nicht vorgesehen. Dort heißt es lediglich:

*„Der Gesetzgeber hat sicherzustellen, dass die hierfür erfassten Datenströme substantiell begrenzt bleiben und eine Höchstspeicherungsdauer von sechs Monaten (vgl. auch BVerfGE 125, 260 <322>) nicht überschritten werden darf.“<sup>86</sup>*

Die Einführung einer Ausnahme aus dem schlichten Grund ihrer „Erforderlichkeit“ ist offenkundig unzulässig. Auch hier werden die Vorgaben des BVerfG missachtet.

## **7. Unzureichende Dokumentationspflichten**

Eine wirksame Kontrolle ist auf eine detaillierte, ausreichende Dokumentation angewiesen. Wo eine solche nicht vorhanden ist, kann nicht wirksam kontrolliert werden. Der vorgelegte Gesetzesentwurf schwächt eine effektive Kontrolle an vielen Stellen bereits systemisch durch fehlende oder mangelhafte Dokumentations- und Kennzeichnungspflichten. Dies betrifft vor allem die verwendeten Selektoren (s. dazu bereits oben unter I.1.c.) Sie erfasst jedoch auch andere Bereiche. Ein legitimer Sachgrund für die fehlende Kennzeichnungspflicht bei Daten aus einer Online-Durchsuchung (§ 34 BNDG-E) ist ebenso wenig ersichtlich. Die fehlende Kennzeichnungspflicht von Daten aus einer strategischen Fernmeldeüberwachung macht zudem allenfalls bei Übermittlungen ins Ausland Sinn, um den BND zu schützen, nicht jedoch bei Übermittlungen im Inland, insbesondere wenn eine solche an andere deutsche Nachrichtendienste erfolgt. Ohne Kennzeichnungspflicht läuft der Zweckbindungsgrundsatz ins Leere. So kann etwa das Bundesamt für

---

<sup>86</sup> BVerfG NJW 2020, 2235 (2253).

Verfassungsschutz (BfV), das Daten durch den BND übermittelt bekommt, besondere Übermittlungsbeschränkungen nicht beachten, wenn es nicht weiß, wo die personenbezogenen Daten herrühren. Das BfV könnte dann – faktisch ungefiltert – alle Daten nach seinen eigenen Übermittlungsvorschriften an Polizei und Staatsanwaltschaft weitergeben. Hierdurch würden – auch verfassungsrechtlich zwingend vorgesehene – Übermittlungsschwellen umgangen.

## II. Übermittlung und Kooperation

Die Übermittlungsvorschriften werden im BNDG-E in den §§ 29, 38 und 39 geregelt. Während § 29 und § 38 BNDG-E die Übermittlung an inländische Stellen normieren, enthält § 39 BNDG-E eine Befugnis zur Datenübermittlung an ausländische Stellen. Die Übermittlungsvorschriften genügen nicht durchgängig den verfassungsrechtlichen Anforderungen. Die Monita werden nachfolgend nur pars pro toto skizziert.

### 1. Verfassungswidrigkeit der Übermittlungsvorschriften und Reformbedarf

Das Bundesverfassungsgericht hat in seinem BND-Urteil zwar nur die mit der Verfassungsbeschwerde angegriffenen Übermittlungsvorschriften des BNDG (§ 24 Abs. 1 Satz 1, 24 Abs. 2 Satz 1 BNDG) für verfassungswidrig erklärt. Der Erste Senat hat jedoch klar gemacht, dass nahezu sämtliche Übermittlungsvorschriften in den Nachrichtendienstgesetzen die verfassungsrechtlichen Anforderungen verfehlen:<sup>87</sup>

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

---

<sup>87</sup> BVerfG NJW 2020, 2235 (2268) Rn. 319 – Hervorhebung diesseits.

Derzeit erfolgen nahezu sämtliche Übermittlungen des BND, aber auch aller anderen deutschen Nachrichtendienste, auf weitgehend verfassungswidrigen Rechtsgrundlagen.

Es besteht daher dringender Anlass zur Behebung des aktuell verfassungswidrigen Zustandes der Übermittlungsvorschriften in allen Nachrichtendienstgesetzen, namentlich im BVerfSchG, im BNDG, im MADG und im G10. Diese enthalten schon seit jeher Wertungswidersprüche. Vor allem genügen sie jedoch weitgehend materiell nicht den verfassungsrechtlichen Anforderungen an den Grundsatz der Verhältnismäßigkeit und den Bestimmtheitsgrundsatz bzw. das Gebot der Normenklarheit.<sup>88</sup> In formaler Hinsicht fehlt es an der verfassungsrechtlich gebotenen Protokollierungspflicht. Diese Feststellung, die spätestens seit dem Urteil des Bundesverfassungsgerichts zum ATDG<sup>89</sup> klar erkennbar wurde, ist durch das BNDG-Urteil des Bundesverfassungsgerichts nunmehr offenkundig angesprochen worden.

Nach Ansicht des DAV muss der verfassungswidrige Zustand wegen der zum Teil gravierenden Grundrechtseingriffe, die mit einer Übermittlung einhergehen,<sup>90</sup> dringend behoben werden. Der DAV bedauert, dass die Bundesregierung und mit ihr der aktuelle Gesetzgeber diese wichtige und aktuell weitgehend verfassungswidrige Materie offensichtlich dem Gesetzgeber der neuen Legislaturperiode zur verfassungsrechtlich angemahnten Überarbeitung überlassen will. Dadurch dürfte der verfassungswidrige Zustand um mindestens ein weiteres Jahr, wenn nicht noch länger aufrechterhalten bleiben. Bei Licht betrachtet dürften aktuell wegen der erklärten Verfassungswidrigkeit Übermittlungen durch die Nachrichtendienste weitgehend nicht mehr stattfinden, was natürlich kein tragbarer Zustand ist.

---

<sup>88</sup> Eingehend zu den einzelnen Übermittlungsvorschriften aller Nachrichtendienstgesetze und zu Fragen der Verfassungswidrigkeit *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 286 ff., 560 ff. *et passim*.

<sup>89</sup> BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07, Rn. 123 (ATDG).

<sup>90</sup> S. dazu nur *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 286 ff.

## 2. Übermittlung personenbezogener Daten an inländische Stellen

§§ 29 Abs. 1 Nr. 1, 38 Abs. 1 Nr. 1 BNDG-E sehen eine verfassungsrechtlich so nicht zulässige Privilegierung für Daten aus einer strategischen Ausland-Fernmeldeaufklärung vor. Ausweislich der Vorgaben des BVerfG ist Voraussetzung für eine Übermittlung zu Zwecken der Gefahrenabwehr eine konkretisierte Gefahrenlage und im Falle einer Übermittlung zu Zwecken der Strafverfolgung ein hinreichend konkretisierter Tatverdacht. Diese Übermittlungsschwellen werden in dem RegE nicht beachtet. § 29 Abs. 1 Nr. 1 BNDG-E knüpft das Vorliegen tatsächlicher Anhaltspunkte lediglich an die Erforderlichkeit der Übermittlung zum Schutz der Rechtsgüter an. Die vom BVerfG geforderte konkretisierte Gefahrenlage als qualifizierte Übermittlungsschwelle wird hierdurch unterlaufen. Dasselbe gilt für die Übermittlungsbefugnis in § 38 Abs. 1 Nr. 1 BNDG-E und für die Übermittlung zu repressiven Zwecken. Hier sollten „bestimmte Tatsachen“ als Anknüpfungspunkt gewählt werden, um den verfassungsrechtlichen Anforderungen an einen hinreichend konkretisierten Tatverdacht zu genügen.

Soweit § 29 Abs. 4 BNDG-E durch das Wort „insbesondere“ eine nicht abschließende Aufzählung der Übermittlungszwecke beabsichtigt, dürfte dies gegen den Bestimmtheitsgrundsatz verstoßen und zudem die Übermittlungsschwellen des § 29 Abs. 4 Nr. 2 BNDG-E umgehen. Die Öffnungsklausel „insbesondere“ sollte daher gestrichen werden.

Der gewählte Straftatenkatalog für die Übermittlung personenbezogener Daten an Strafverfolgungsbehörden in § 29 Abs. 3 genügt den verfassungsrechtlichen Anforderungen nicht durchgängig. Nr. 1 ist verfassungsrechtlich nicht zu beanstanden. Hier wird an den Katalog der besonders schweren Straftaten angeknüpft, wie sie in § 100b Abs. 2 StPO legaldefiniert sind. Die in § 29 Abs. 3 Nr. 2 BNDG vorgesehene Übermittlung zur Verfolgung von „vorsätzlichen Straftaten nach den §§ 17 und 18 des Außenwirtschaftsgesetzes“ unterschreitet hingegen die verfassungsrechtlichen Mindestanforderungen und verstößt damit gegen den Grundsatz der Verhältnismäßigkeit. Denn § 17 Abs. 4 und § 18 Abs. 1-6 AWG enthalten Straftaten, die zum Teil nur dem Bereich der einfachen bis mittleren Kriminalität zuzuordnen sind, so

etwa § 18 Abs. 5a AWG, der einen Strafraum von bis zu einem Jahr Freiheitsstrafe oder Geldstrafe vorsieht. Die Verfolgung einer solchen Straftat dient ersichtlich keinem herausragenden öffentlichen Interesse, das den mit der Übermittlung verbundenen gravierenden Grundrechtseingriff verfassungsrechtlich zu rechtfertigen geeignet ist.<sup>91</sup> Dies ist bei dem Katalog in Nr. 2 allein bei § 18 Abs. 7 und 8 AWG der Fall. Der Straftatenkatalog muss daher zwingend entsprechend angepasst werden, um nicht dem Verdikt der Verfassungswidrigkeit zu unterfallen.

### **3. Insbesondere: Übermittlung personenbezogener Daten an Private**

§§ 29 Abs. 6, 30 Abs. 4, 39 Abs. 5 BNDG-E lassen eine Übermittlung von Informationen an „andere inländische Stellen“ bzw. „andere ausländische Stellen“ und somit private Unternehmen zu. Nach der Entwurfsbegründung sind insoweit insbesondere private Stiftungen, Vereine und Kapitalgesellschaften gemeint.<sup>92</sup>

Zwar ist die Übermittlung personenbezogener Daten an andere Stellen nur unter strengen Voraussetzungen möglich, namentlich dann, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung erforderlich ist zur Verhinderung einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person, lebenswichtige Güter der Allgemeinheit oder den Bestand oder die Sicherheit des Bundes oder eines Landes oder die Sicherheit eines Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages. Allerdings wird die Art und Weise der Überlassung der Daten unzureichend geregelt. Insbesondere bleibt unklar, für welche Dauer Privaten die übermittelten personenbezogenen Daten zur Verfügung gestellt werden.

Der DAV fordert daher, die Übermittlung von geheimdienstlichen Informationen an Private zu konkretisieren und damit in Übereinstimmung mit dem verfassungsrechtlich gebotenen Bestimmtheitsgrundsatz auszugestalten.

---

<sup>91</sup> Vgl. BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07, Rn. 123 (ATDG); s. zu den verfassungsrechtlich zulässigen Straftatenkatalogen *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 275 ff., 327 ff., 566 ff.

<sup>92</sup> RegE S. 94.

### **III. Kontrolle**

#### **1. Unabhängiger Kontrollrat**

Der DAV begrüßt die vorgeschlagene Schaffung eines Unabhängigen Kontrollrats, der als Fortentwicklung des Unabhängigen Gremiums sowohl für die gerichtsähnliche als auch für die administrative Rechtskontrolle zuständig sein soll (§ 40 Abs. 2 BNDG-E). Dieser sollte allerdings stärker ausgestaltet werden, da andernfalls die Gefahr besteht, dass eine effektive Kontrolle von vornherein faktisch vereitelt wird.

Der Regierungsentwurf hält die Schaffung von 62 Planstellen zur Deckung des Bedarfs von gerichtsähnlicher Rechtskontrolle, administrativer Rechtskontrolle und Verwaltung für ausreichend. Dem ist zu widersprechen.

In der Praxis soll der BND in die Lage versetzt werden, 30 Prozent des gesamten weltweiten Telekommunikationsverkehrs zu überwachen. Unabhängig davon, dass die avisierte Überwachungskapazität mit 30 Prozent weiterhin zu hoch ist,<sup>93</sup> ist kaum vorstellbar, wie eine Handvoll Personen die Rechtmäßigkeit der Überwachung von täglich mehreren Milliarden Daten überprüfen können soll. Selbst wenn man unterstellt, dass der Regierungsentwurf dem Unabhängigen Kontrollrat effektive Kontrollmöglichkeiten an die Hand gibt, besteht die Gefahr, dass eine effektive Kontrolle schon mangels ausreichender Personalausstattung nicht vorgenommen werden kann. Der Mitarbeiterstab des Unabhängigen Kontrollrats ist daher deutlich auszubauen. Aufgrund der erheblichen Überwachungskapazität des BND muss der Mitarbeiterstab des Unabhängigen Kontrollrats in einer vergleichbaren Größenordnung zum Mitarbeiterstab des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit liegen, der gegenwärtig etwa 320 Planstellen umfasst.

Außerdem sollte eine dreijährige Evaluationsfrist eingeführt werden, so dass gesteigerter Bedarf rechtzeitig erkannt und zeitnah gedeckt werden kann.

Die Auswahl der Mitglieder des Unabhängigen Kontrollrats, wie sie im Entwurf vorgesehen ist, ist ebenso zu kritisieren wie der eingeschränkte Kreis, aus dem sie gewählt werden sollen. Warum nur Richterinnen und Richter des BGH und nicht auch

---

<sup>93</sup> Siehe oben, S. 13 ff.

solche des BVerwG zu Mitgliedern des gerichtsähnlichen Kontrollorgans ernannt werden können, ist mitnichten nachvollziehbar. Über eine sachnahe besondere Kompetenz auf diesen Rechtsgebieten verfügen Richterinnen und Richter am BVerwG zweifelsohne. Nicht nachvollziehbar ist zudem, warum – in Fortschreibung des Unabhängigen Gremiums – eine Vertreterin bzw. ein Vertreter des Generalbundesanwalts das richterähnliche Amt bekleiden soll, ohne dass es einen entsprechenden Gegenpol gibt. Als größtes Manko in der vorgesehenen Besetzung ist nach Ansicht des DAV zu monieren, dass – wie auch bisher im Unabhängigen Gremium – keine Vertreterin oder Vertreter für die Interessen der von den Überwachungsmaßnahmen Betroffenen vorgesehen ist. Ein solcher Vertreter als Bürgeranwalt/Bürgeranwältin, Menschenrechtsanwältin/Menschenrechtsanwalt oder Ombudsperson wäre schon deshalb essentiell, um eine Gerichtsähnlichkeit zu erreichen und eine ausgewogene unabhängige Kontrolle sicherzustellen. Zwar sieht die Entscheidung des BVerfG die Einführung eines „Anwalts“ des Betroffenen und somit die Einführung eines streitigen Verfahrens nicht ausdrücklich vor. Für die Ermöglichung eines streitigen Verfahrens spricht aber der vom BVerfG bemühte Grundgedanke, dass die gerichtsähnliche Kontrolle gerade eine Kompensation dafür sein soll, dass dem Betroffenen mangels Kenntnis von der Überwachung oder anschließender Benachrichtigung ein individueller Rechtsschutz gerade versagt sein wird. Auch die (negativen) Erfahrungen ausländischer Jurisdiktionen sprechen für die Schaffung eines streitigen Verfahrens.<sup>94</sup> So forderte der ehemalige Vorsitzende Richter des US-amerikanischen Foreign Intelligence Surveillance Court (FISC), *James Robertson*, der am 20.12.2005 aus Protest gegen die damals gängige Überwachungspraxis zurückgetreten war, die Einführung des streitigen Verfahrens, in dem den Regierungsvertretern eine Partei gegenübersteht, die die Interessen der vom Behördenhandeln Betroffenen vertritt.<sup>95</sup> Nur ein Streitiges Verfahren stellt aus Sicht des DAV sicher, dass die Rechte der von den Maßnahmen Betroffenen nicht unverhältnismäßig stark eingeschränkt werden. Überdies ist daran zu erinnern, dass es nicht Ziel des Gesetzgebers sein sollte, nur das Mindestmaß des verfassungsrechtlich Notwendigen zu beachten. Die entsprechenden Vorschläge in den Anträgen der Fraktion der FDP (BT-Drs. 19/19509, S. 3) und BÜNDNIS 90/DIE GRÜNEN (BT-Drs. 19/26221, S. 8) sind zu begrüßen.

---

<sup>94</sup> Vgl. bereits DAV Stellungnahme 65/2016.

<sup>95</sup> <https://www.theguardian.com/law/2013/jul/09/fisa-courts-judge-nsa-surveillance>.

Überdies sollte erwogen werden, ob nicht dem PKGr selbst ein originäres Vorschlagsrecht für Mitglieder des Unabhängigen Kontrollgremiums eingeräumt werden sollte, statt dieses Vorschlagsrecht originär und exklusiv der Präsidentin/dem Präsidenten des BGH sowie dem Generalbundesanwalt zu überlassen. Dies gilt auch für den Fall, dass der Kreis der zu wählenden Mitglieder sinnvollerweise um Richterinnen und Richter aus der Verwaltungsgerichtsbarkeit ergänzt wird.

## **2. Anordnungs- statt Vollzugsvorbehalt**

Schließlich ist die Art und Weise der Kontrollbefugnisse unzureichend ausgestaltet. Das BVerfG hat entschieden, dass vor bestimmten besonders eingriffsintensiven Maßnahmen eine gerichtsähnliche ex-ante Kontrolle einzuführen ist. Im Regierungsentwurf ist diese Anforderung nunmehr derart umgesetzt worden, dass die Maßnahmen weiterhin vom BND selbst angeordnet werden dürfen und lediglich der Vollzug unter den Vorbehalt gerichtsähnlicher Kontrolle gestellt wird (§ 23 Abs. 4 BNDG-E). Diese Konstruktion wird erhebliche Auswirkungen auf die Entscheidungspraxis haben, weil eine gerichtsähnliche Person, die eine eingriffsintensive Maßnahme selbst anordnen muss, eher geneigt sein wird, die Maßnahme vorher umfassend zu prüfen als eine Person, die eine bereits angeordnete Maßnahme lediglich freizeichnen muss.

Der DAV fordert daher, die besonders eingriffsintensiven Maßnahmen, die bisher lediglich einem Vollzugsvorbehalt unterstehen, in der Form umzugestalten, dass nur der Unabhängige Kontrollrat diese Maßnahmen auf Antrag der Verantwortlichen des BND anordnen kann.

## **3. Parlamentarische Kontrolle als zentrales Kontrollinstrument**

Bei alledem ist zu bedenken, dass das Parlament das wichtigste Kontrollorgan der Nachrichtendienste bleibt. Denn die Kontrolle durch das Parlament geht viel weiter als eine bloße Kontrolle der Rechtmäßigkeit, wie sie durch den Unabhängigen Kontrollrat vorgesehen ist. Der DAV hält einen Ausbau der parlamentarischen Kontrolle daher für sinnvoll und nötig. Hierbei müssen vor allem die faktischen Kontrollmöglichkeiten insbesondere durch das PKGr verbessert werden. Der DAV begrüßt insoweit die beiden

Anträge der Fraktionen der FDP (BT-Drs. 19/19509) und BÜNDNIS 90/DIE GRÜNEN (BT-Drs. 19/26221) und die darin unterbreiteten Vorschläge. Der DAV empfiehlt, sich damit näher auseinander zu setzen.