



Ausschussdrucksache 21(4)208
vom 4. September 2026

Schriftliche Stellungnahme
des Deutschen Anwaltvereins vom 3. September 2026

zu dem

Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts
BT-Drucksache 21/...

Von: Rychlikowski, Diana (DAV) <rychlikowski@anwaltverein.de> im Auftrag von Gröning, Max (DAV) <groening@anwaltverein.de>
Gesendet: Donnerstag, 3. September 2026 12:44
Betreff: DAV-Stellungnahme Nr. 60/2026 zum Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts
Anlagen: DAV-SN 60-26_BND.pdf
Kennzeichnung: Zur Nachverfolgung
Kennzeichnungsstatus: Gekennzeichnet



Deutscher**Anwalt**Verein

Gesetzgebungsausschüsse Recht der Inneren Sicherheit und Informationsrecht DAV-SN 60/2026 zum Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts

Sehr geehrte Damen und Herren,
sehr geehrte Kolleginnen und Kollegen,

beigefügt übersende ich Ihnen die [Stellungnahme Nr. 60/2026](#) des Deutschen Anwaltvereins (DAV), vorbereitet durch die Ausschüsse Recht der Inneren Sicherheit und Informationsrecht zum Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts.

Zwar erkennt der DAV einzelne Verbesserungen – etwa beim Kernbereichsschutz – an; insgesamt sieht er aber erhebliche verfassungsrechtliche Defizite und die deutliche Ausweitung nachrichtendienstlicher Befugnisse. Er kritisiert insbesondere die Schwächung anwaltlicher Kommunikation.

Bundesamt für Verfassungsschutz und Bundesnachrichtendienst sollen eigene operative Eingriffsbefugnisse erhalten. Dies gefährdet aus Sicht des DAV die verfassungsrechtlich gebotene Trennung zwischen Nachrichtendiensten und Polizei und stellt zugleich die Rechtfertigung weitreichender nachrichtendienstlicher Vorfeldbefugnisse infrage.

Auch wenn der Entwurf den Schutz von Vertraulichkeitsbeziehungen in mehreren Punkten verbessert, sieht der DAV einige Punkte gleichwohl sehr kritisch. Insbesondere bedeuten die geplanten Regelungen eine Schwächung des Schutzes anwaltlicher Kommunikation, weil die Ausnahmen des § 22 Abs. 2 BNDG-E die Erfassung auch typischer Mandatstätigkeit ermöglichen könnten, ohne dass der Rechtsanwalt selbst Täter oder Teilnehmer einer Straftat sein muss.

Mitteilungs-, Auskunft- und Rechtsschutzmöglichkeiten der Betroffenen bewertet der DAV als unzureichend. Besonders problematisch ist, dass heimliche Maßnahmen teilweise ohne wirksame nachträgliche Rechtsschutzmöglichkeit bleiben.

Die Regelungen zur Weitergabe nachrichtendienstlicher Erkenntnisse an Verwaltungs- und Strafverfolgungsbehörden sind aus Sicht des DAV teilweise zu unbestimmt und unterschreiten bei bestimmten Straftaten die vom BVerfG geforderte Schwelle der „besonders schweren Straftat“. Auch das abgestufte System der Zweckbindung wird aus Sicht des DAV teilweise unterlaufen.

Die Bündelung der Kontrolle beim Unabhängigen Kontrollrat (UKRat) sieht der DAV grundsätzlich als Chance, der Entwurf gewährleistet aber weder eine hinreichend umfassende Kontrolle noch ausreichende Durchsetzungsbefugnisse. Die Beschränkung auf längerfristige Prüfprogramme schafft aus Sicht des DAV zudem kontrollfreie Bereiche.

Die Verfassungsschutzbehörden sollen nicht mehr nur Informationen sammeln und auswerten, sondern Bestrebungen aktiv „entgegenwirken“. Nach Auffassung des DAV müsste eine solche Ausweitung spiegelbildlich mit stärkeren Betroffenenrechten einhergehen.

Zudem kritisiert der DAV den Einsatz staatlicher Trojaner, insbesondere auch gegen Rechtsanwält:innen. Er beanstandet u.a. die vergleichsweise niedrigen Eingriffsschwellen bei nicht privat genutzten IT-Systemen und eine fehlende eigenständige Verhältnismäßigkeitsprüfung. Der DAV äußert insoweit erhebliche Zweifel an der Vereinbarkeit mit Art. 10 Abs. 1 GG und dem IT-Grundrecht.

Weitere Einzelheiten bitte ich der anliegenden Stellungnahme zu entnehmen.

Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur [Registernummer R000952](#) eingetragen.

Der Deutsche Anwaltverein ist mit der Veröffentlichung seiner Stellungnahme einverstanden. Gleiches gilt für die in der Stellungnahme namentlich genannten Mitglieder hinsichtlich ihrer personenbezogenen Daten.

Bei Rückfragen stehen wir Ihnen sehr gerne zur Verfügung.

Mit freundlichen Grüßen

Max Gröning

Deutscher Anwaltverein

Syndikusrechtsanwalt Max Gröning
Geschäftsführer
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152 106
Mail: groening@anwaltverein.de

Assistentin: Diana Rychlikowski

Tel.: +49 30 726152 171
Mail: rychlikowski@anwaltverein.de

www.anwaltverein.de
[Organigramm der Geschäftsstelle /](#)
[Organization chart](#)

Nicole Narewski

Deutscher Anwaltverein

Rechtsanwältin Nicole Narewski
Geschäftsführerin
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152 128
Mail: narewski@anwaltverein.de

Assistentin: Anne Lasmar

Tel.: +49 30 726152 138
Mail: lasmar@anwaltverein.de

www.anwaltverein.de
[Organigramm der Geschäftsstelle /](#)
[Organization chart](#)



Stellungnahme

**des Deutschen Anwaltvereins vorbereitet durch
die Ausschüsse Recht der Inneren Sicherheit und
Informationsrecht**

**zum Entwurf eines Gesetzes zur Reform des
Nachrichtendienstrechts**

Stellungnahme Nr.: 60/2026

Berlin, im September 2026

Mitglieder des Ausschusses Recht der Inneren Sicherheit

- Rechtsanwältin Lea Voigt, Bremen (Vorsitzende und Berichterstatlerin)
- Rechtsanwalt Wilhelm Achelpöhl, Münster (Berichterstatler)
- Rechtsanwältin Dr. Lea Babucke, Düsseldorf
- Prof. Dr. Annika Dießner, Berlin (ständiges Gastmitglied im Ausschuss)
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln
- Rechtsanwalt Dr. Tobias Groscurth, Frankfurt
- Rechtsanwalt Dr. Andreas Grözing, Köln (Berichterstatler)
- Rechtsanwalt Dr. Mayeul Hiéramente, Hamburg
- Rechtsanwalt Dr. Saleh Ihwas, Frankfurt am Main
- Rechtsanwalt Dr. Arne Klaas (Berichterstatler)
- Rechtsanwältin Dr. Regina Michalke, Frankfurt am Main
- Prof. Dr. Mark A. Zöller, München (ständiges Gastmitglied im Ausschuss)

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwalt Max Gröning, Geschäftsführer, Berlin
- Rechtsanwältin Katharina Schmidt-Matthäus, Referentin, Berlin

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: 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
EU-Transparenz-Registernummer:
87980341522-66

Mitglieder des Ausschusses Informationsrecht

- Rechtsanwalt Prof. Niko Härting, Berlin (Vorsitzender und Berichterstatter)
- Rechtsanwalt Dr. Simon Assion, Frankfurt
- Rechtsanwältin Dr. Christiane Bierekoven, Düsseldorf
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Prof. Dr. Malte Grützmaker, LL.M., Hamburg
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf
- Rechtsanwalt Dr. Helmut Redeker, Bonn
- Rechtsanwältin Dr. Kristina Schreiber, Köln
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Nicole Narewski, Geschäftsführerin, Berlin

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt ca. 60.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 253 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene. Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

Inhalt

A. Kritik am Gesetzgebungsverfahren	6
B. Stellungnahme	7
I. Trennungsgebot	7
II. Schutz von Berufsgeheimnisträger*innen	9
1. § 22 BNDG-E — Schutz der Vertraulichkeitsbeziehung	9
a. Regelungsgehalt	9
b. Kritik	10
aa) Anwaltliche Mandatsführung	10
bb) Verschwiegenheit	11
cc) Kein Erhebungs-, sondern nur ein Zielrichtungsverbot	11
dd) Die Verfahrenssicherungen greifen zu punktuell	11
ee) Ausländische Berufsträger	12
ff) Folgewirkung	12
c. Fazit	12
d. Forderungen	13
2. § 32 BVerfSchG-E	13
a. Regelungsgehalt	13
b. Kritik	14
c. Forderung	15
III. UKRatG	15
1. Eine „gerichtsähnliche Kontrolle“ ohne gerichtsähnliches Verfahren?	16
2. Die „administrative Kontrolle“: ein zahnloser Tiger?	17
3. Eine lückenhafte Kontrolle	18
4. Eine weitgehende personelle sowie fachliche Verknappung	19
IV. BNDG	20

1. Schutz von Vertraulichkeitsbeziehungen nach § 22 BNDG-E	20
a. Ausland-Ausland-Kommunikation	21
b. Ausland-Inland-Kommunikation	22
c. Fazit	24
2. Online-Durchsuchungen nach §§ 36 ff. BNDG-E	25
a. Einsatz von Trojanern gegen Rechtsanwältinnen und Rechtsanwälte	25
aa) Geringe Hürden	25
bb) Kein Eingreifen von § 22 BNDG-E	27
cc) Mangelnde Kontrolle durch den Unabhängigen Kontrollrat	27
dd) Fazit	28
b. Umkehrung des Schutzzwecks des BSI	28
3. Strategische Aufklärung	29
a. De facto wirkungslose Volumengrenze - § 10 Abs. 4 S. 3 G10 / § 31 Abs. 3 S. 2 Nr. 2 BNDG-E	30
b. Löschpflicht als Speicherbefugnis - § 66 Abs. 1 S. 1 BNDG-E	30
c. Wegfall des Suchbegriffsverbots - § 5 Abs. 2 G10 / §§ 33 Abs. 3, 34 Abs. 2 BNDG-E	31
d. Entgrenzung der Erkenntniszwecke - § 5 Abs. 1 S. 2 G10 / §§ 32 Abs. 1, 33 Abs. 1 BNDG-E	31
4. § 7 Befugnis zur Datenerhebung unter Mitwirkung anderer Stellen	32
a. Regelungsgehalt	32
b. Kritik	32
5. § 8 i. V. m. §§ 134, 136, 137 BNDG-E — Strafbewehrtes Mitteilungsverbot ohne Ausnahme für Rechtsrat	33
a. Regelungsgehalt	33
b. Kritik	34
aa) Konsultation eines Rechtsanwalts	34
bb) Bestimmtheit	34
cc) Zusammenspiel mit § 103	34
dd) Verweisungsfehler in der Bußgeldnorm	35
c. Fazit	35
d. Forderungen	35
6. §§ 100–103 BNDG-E — Mitteilung, Auskunft und Rechtsweg	36
a. Regelungsgehalt	36
b. Kritik	36
aa) Anknüpfung an die Staatsangehörigkeit (§ 100 Abs. 3 Satz 1)	36
bb) Ausschluss Drittbetroffener (§ 100 Abs. 3 Satz 2)	37
cc) Mitteilungspflicht	37
dd) Auskunftsanspruch	37

ee) Rechtswegausschluss.....	38
ff) Gesamtwirkung	38
c. Fazit	39
d. Forderungen	39
7. § 81 i. V. m. Anlage 2 BNDG-E — Übermittlung zur Strafverfolgung	40
a. Regelungsgehalt	40
b. Kritik	40
aa) Äußerungsdelikte als „besonders schwere Straftaten“	40
bb) Lückenhafte Regelung in § 77.....	41
cc) Verknüpfung von Desinformationsabwehr und Äußerungsstrafrecht.....	41
dd) Verdeckte Herkunft	42
ee) Verweisungsfehler.....	42
c. Fazit	42
d. Forderungen	43
V. BVerfSchG	43
1. Aufgaben der Verfassungsschutzämter	44
2. Legaldefinitionen / Eingriffsschwellen	44
a. Freiheitlich demokratische Grundordnung	44
b. Erhebliche Beobachtungsbedürftigkeit und Gewaltbegriff	45
c. Besonders erhebliche Beobachtungsbedürftigkeit	47
3. Datenübermittlungsbefugnisse	47
a. Maßstab des BVerfG an die Verwendung nachrichtendienstlich erhobener Daten	47
aa) Reichweite des Erhebungszwecks.....	48
bb) Anforderungen an zweckändernde Verarbeitungen	48
cc) Spezifische Anforderungen an Übermittlungen	49
b. §§ 45 ff. BVerfSchG-E	51
aa) § 47 BVerfSchG-E.....	51
bb) § 48 BVerfSchG-E.....	53
cc) § 49 BVerfSchG-E	54
dd) § 58 BVerfSchG-E.....	55

Stellungnahme des Deutschen Anwaltvereins zum Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts¹

Die Bundesregierung legt einen Entwurf für eine „umfassende Reform“² des Nachrichtendienstrechts vor. Der Bundesnachrichtendienst (BND) und das Bundesamt für Verfassungsschutz (BfV) sollen weitreichende neue Befugnisse erhalten.

A. Kritik am Gesetzgebungsverfahren

Angesichts der besonderen Problemstellung, die mit der Einrichtung und dem Unterhalt von Geheimdiensten im Rechtsstaat generell einhergeht und mit Blick auf die Erfahrungen in der deutschen Geschichte mit Geheimpolizei und Geheimdiensten im Besonderen, ist es befremdlich, dass das Bundesinnenministerium das Verbändeverfahren und damit die Chance einer kritischen öffentlichen Revision des Entwurfs, obstruiert hat. Die Verbände wurden am Freitag, den 03.07.2026 um 13:55 Uhr angeschrieben. Unter Beifügung des über 700 Seiten umfassenden Gesetzesentwurf erhielten sie Gelegenheit zur Stellungnahme bis zum 14.07.2026, also binnen nur sechs voller Werktagen. Wer das Verbändeverfahren so ausgestaltet, muss sich den Vorwurf gefallen lassen, es zum Feigenblatt zu degradieren. Dies ist gerade in Zeiten, in denen parlamentarische Verfahren und Institutionen besonders unter Druck stehen, problematisch.

Die Gesetzesbegründung erhält erneut keine Synopse, mit der die bestehenden Regelungen den beabsichtigten Neuregelungen gegenübergestellt werden. Solche Synopsen werden im Zuge der Entwurfserstellung regelmäßig angefertigt. Ob sie der Öffentlichkeit zur leichteren Orientierung über die geplanten Änderungen zur Verfügung gestellt werden, wird unterschiedliche gehandhabt. Ministerien, die – wie hier – davon absehen, setzen sich dem Verdacht aus, die Öffentlichkeit nicht umfassend über ihr Vorhaben informieren zu wollen. Der Deutsche Anwaltverein fordert die

¹ Regierungsentwurf vom 12.08.2026, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/OES12/GE-ND-Reform.pdf?__blob=publicationFile&v=2.

² S. 239 des Entwurfs.

Bundesregierung auf, das Vorgehen zu vereinheitlichen und die Änderungssynopse stets mit dem Entwurf zu veröffentlichen.

B. Stellungnahme

Der Deutsche Anwaltverein hat sich entschlossen, zum Ende der parlamentarischen Sommerpause eine Stellungnahme zu dem Entwurf vorzulegen. Diese greift aus Sicht der Anwaltschaft zentrale Probleme des Entwurfs auf. Soweit sie sowohl das BNDG als auch das BVerfSchG betreffen, werden sie vor die Klammer gezogen.

I. Trennungsgebot

Das Trennungsgebot zwischen Nachrichtendiensten und Polizeibehörden ist grundrechtlich begründet. Nachrichtendiensten können nur deshalb Befugnisse zustehen, Informationen weit im Vorfeld einer Gefahrenlage zu erheben, weil sie keine Exekutivbefugnisse haben. Das BVerfG hat dies wie folgt formuliert:

„Die weitreichenden Überwachungsbefugnisse der Verfassungsschutzbehörden können verfassungsrechtlich nur gerechtfertigt werden, wenn die aus der Überwachung gewonnenen Informationen nicht ohne Weiteres an andere Behörden mit operativen Anschlussbefugnissen übermittelt werden dürfen („informationelles Trennungsprinzip“³). Ansonsten böte der Umstand, dass die Verfassungsschutzbehörde selbst nicht über operative Anschlussbefugnisse verfügt, den Überwachten am Ende doch kaum Schutz: Die der Verfassungsschutzbehörde verschlossenen eingriffsintensiven Folgemaßnahmen könnten dann von operativ ausgestatteten Behörden durchgeführt werden, die dabei die durch die Verfassungsschutzbehörde erlangten Informationen weiternutzten, ohne dass die für sie selbst als operative Behörden geltenden Datenerhebungsvoraussetzungen erfüllt sein müssten. Aufseiten der empfangenden Behörde würden so die grundrechtsschützenden Eingriffsschwellen der Befugnisse operativer Behörden umgangen; zugleich

³ vgl. BVerfGE 133, 277 (329) Rn. 123; BVerfGE 156, 11 (50, 51 f.).

verlöre aufseiten der Verfassungsschutzbehörden der Umstand, dass diese ohne operative Anschlussbefugnisse sind, seinen schützenden Effekt“.⁴

§§ 59 ff. BVerfSchG-E begründet mit dem neuen Abschnitt 4 indessen operative Anschlussbefugnisse der Gefahrenabwehr mit den dort vorgesehenen „Schutzmaßnahmen“. Die dem Verfassungsschutz nunmehr eingeräumten operativen Eingriffsbefugnisse werden durch den Begriff der „Schutzmaßnahmen“ verschleiert, sind doch alle Maßnahmen der Gefahrenabwehrbehörden „Schutzmaßnahmen“, die davor schützen sollen, dass sich eine Gefahr für ein geschütztes Rechtsgut verwirklicht. Tatsächlich sind die Schutzmaßnahmen „operative Anschlussbefugnisse“ und sind als „Eingriffsbefugnisse“ deutlich besser bezeichnet. Denn mit diesen Befugnissen werden dem Verfassungsschutz vergleichbar den Polizeibehörden Eingriffsbefugnisse eingeräumt. Zulässig ist die Einwirkung auf Gegenstände, die für eine Bedrohung eingesetzt werden könnten, wenn eine solche Bedrohung nur absehbar sein soll. Gestattet ist jede Einwirkung, der Katalog des § 59 Abs. 2 Nr. 1 ist nicht abschließend, umfasst auch nicht körperliche Gegenstände, einzig der unmittelbare Zwang gegen Personen bleibt ausgeschlossen, „Gewalt gegen Sachen“ gehört künftig zum Repertoire des Verfassungsschutzes. Zulässig sind diese Maßnahmen, wenn der Verfassungsschutz der Ansicht ist, dass eine Übermittlung der Erkenntnisse an die zum Eingriff befugten Polizeibehörden nach § 51 nicht möglich ist. Das ist bereits dann der Fall, wenn der Übermittlung „überwiegende Sicherheitsinteressen“ entgegenstehen.

Die klare Trennung von Polizei und Geheimdiensten wird damit aufgehoben. Damit werden zugleich nachrichtendienstliche Befugnisse des Verfassungsschutzes zur Datenerhebung in Frage gestellt. Auf diesem Weg zur Geheimpolizei werden auch dem BND mit §§ 49 ff. BNDG-E unbestimmt gefasste Eingriffsbefugnisse gewährt, dem nunmehr ein „aktives Einwirken“ gestattet wird, die insoweit einzusetzenden Mittel werden nicht begrenzt. Das „aktive Einwirken“ darf sich nicht „gezielt gegen Leib und Leben einer Person“ richten. Die Begründung verweist zutreffend darauf, dass damit allein „gezielte Verletzungen oder Tötungen ausgeschlossen sind“ (S. 562). Damit sind dem BND etwa Drohnenangriffe auf Frachtflugzeuge gestattet. Wenn dabei Menschen zu Schaden kommen, steht dies der Maßnahme nur dann entgegen, wenn auf deren Verletzung gezielt wurde, nicht aber, wenn sie nur in Kauf genommen wurde.

⁴ BVerfG Urteil vom 26.4.2022 – 1 BvR 1619/17 Rn. 171.

Das BVerfG hat die Rechtfertigung der Befugnisse des BND zu Informationserhebungen im Vorfeld einer Gefahr gerade in den fehlenden Eingriffsbefugnissen gesehen:

*„Ein wichtiger Gesichtspunkt für die Rechtfertigungsfähigkeit der strategischen Telekommunikationsüberwachung liegt schließlich darin, dass die Folgen der anlasslosen Durchführung dadurch etwas abgemildert werden, dass sie durch eine Behörde vorgenommen werden, die selbst grundsätzlich keine operativen Befugnisse hat“.*⁵

Auch im Inland können diese Maßnahmen nach § 51 Abs. 2 BNDG-E durchgeführt werden, wenn die Datenübermittlung an andere Behörden aus Gründen der Geheimhaltung nicht möglich ist, was bei einem Geheimdienst, der mit anderen Geheimdiensten zusammenarbeitet die Regel sein dürfte.

Der ersatzlose Wegfall der bisherigen Regelung des § 2 Abs. 3 BNDG „Polizeiliche Befugnisse oder Weisungsbefugnisse stehen dem Bundesnachrichtendienst nicht zu“ bringt den Übergang zu einem Geheimdienst mit Eingriffsbefugnissen auf den Punkt.

II. Schutz von Berufsgeheimnisträger*innen

1. § 22 BNDG-E — Schutz der Vertraulichkeitsbeziehung

a. Regelungsgehalt

Gegenüber der bisherigen Rechtslage begrüßt der DAV, dass der Schutz von Vertraulichkeitsbeziehung auf sämtliche nachrichtendienstliche Mittel ausgedehnt werden soll.

⁵ BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, BVerfGE 154, 152-312 (LT 1-8), Rn. 165.

§ 22 Abs. 1 verbietet die Erhebung personenbezogener Daten „zum Zweck der gezielten Erlangung“ von Daten aus einer Vertraulichkeitsbeziehung und schützt Seelsorger, Rechtsanwälte und Verteidiger, Journalisten sowie Mandatsträger.

b. Kritik

Abs. 2 lässt die Erhebung gleichwohl zu, wenn der Berufsträger in die Bedrohung verstrickt ist (Nr. 1) oder eine erhebliche Gefahr für ein besonders gewichtiges Rechtsgut abzuwenden ist (Nr. 2).

aa) Anwaltliche Mandatsführung

Die Klausel des Abs. 2 Nr. 1 Buchst. c beschreibt die Mandatsführung. Danach genügt es, dass der Berufsträger „in Zusammenhang“ mit einer zumindest erheblichen Bedrohung steht; als Regelbeispiel nennt die Vorschrift den Fall, dass er „für eine Person nach Buchstaben a und b bestimmte oder von ihr herrührende Mitteilungen entgegennimmt oder weitergibt“.

Genau das gehört zum Kernbereich anwaltlicher Tätigkeit.

Ist der Mandant Zielperson — und Buchst. a verlangt lediglich „Unterstützen“ —, kann der Ausnahmetatbestand durch die Berufsausübung selbst erfüllt sein. Die Schutznorm wird dann durch ihre eigene Ausnahme aufgehoben. Der Eingriff in Art. 12 Abs. 1 GG des Anwalts und in das faire Verfahren des Mandanten tritt damit nicht als eng begrenzte Ausnahme ein, sondern als Regelfall. Das ist schon deshalb unverhältnismäßig, weil die Norm kein Kriterium enthält, das eine Abwägung überhaupt steuern könnte. Dies zeigt auch ein Vergleich mit § 160a Abs. 1 StPO. Dieser nimmt den Verteidiger demgegenüber gerade deshalb von der Maßnahme aus, weil er Mitteilungen des Beschuldigten zwangsläufig entgegennimmt.

Entsprechend erläutert die Entwurfsbegründung allein den Fall des an Anschlagsplänen beteiligten Anwalts — also Buchst. a — und schweigt zu Buchst. c, der die eigentliche Ausweitung enthält.

bb) Verschwiegenheit

Der Verweis in Abs. 2 Nr. 2 auf § 2 Abs. 2 stellt die Verschwiegenheit unter außenpolitischen Vorbehalt. § 2 Abs. 2 nennt neben Leben, Freiheit und körperlicher Unversehrtheit auch die „außenpolitische Handlungsfähigkeit der Bundesrepublik Deutschland“ (Nr. 3) und „Sachen von bedeutendem Wert“ (Nr. 5); der Katalog ist zudem nicht abschließend („insbesondere“). Anwaltliche Kommunikation kann danach zur Abwehr einer Gefahr für die außenpolitische Handlungsfähigkeit überwacht werden. Für Eingriffe von diesem Gewicht verlangt die Rechtsprechung indes den Schutz überragend wichtiger Rechtsgüter. Ein Staatsinteresse ohne individualrechtlichen Bezug genügt nicht.

cc) Kein Erhebungs-, sondern nur ein Zielrichtungsverbot

Abs. 1 verbietet allein die gezielte Erlangung; die Begründung stellt ausdrücklich klar, dass bei ungeklärter Vertraulichkeit „eine Erhebung zulässig“ ist und erst Abs. 3 eingreift. Der Schutz wird damit von der Erhebungs- auf die Verwertungsebene verlagert. Gerade diese Verlagerung hat das Bundesverfassungsgericht für den absolut geschützten Bereich für unzureichend gehalten.⁶ Der Entwurf selbst kennt die alternative Gestaltung: § 21 Abs. 1 Satz 2 und 3 sehen für den Kernbereich eine Vorwirkung auf Planung und Anordnung vor; in § 22 fehlt sie.

dd) Die Verfahrenssicherungen greifen zu punktuell.

Eine berufsgeheimnisspezifische Vorabkontrolle besteht nur für Suchbegriffe in der strategischen Aufklärung (§ 97 Abs. 1 Nr. 12 Buchst. b). Für V-Personen-Einsatz, Observation, Postkontrolle, Telekommunikationsüberwachung und Online-Durchsuchung gegen einen Berufsträger gibt es keine. § 97 Abs. 3 Nr. 1 erfasst erst die Weiterverarbeitung, also einen Zeitpunkt nach dem Bruch der Vertraulichkeit. Über Zweifelsfälle entscheidet nach § 22 Abs. 3 Satz 3 i. V. m. § 21 Abs. 2 ein Bediensteter des behördlichen Datenschutzes des BND - die erhebende Behörde also über sich selbst.

⁶ BVerfGE 109, 279.

ee) Ausländische Berufsträger

Ob Abs. 1 Satz 2 Nr. 2 ausländische Rechtsanwälte erfasst, bleibt offen. Bei einem Auslandsnachrichtendienst ist das jedoch die praktisch wichtigste Konstellation. In grenzüberschreitenden Wirtschaftsstraß-, Sanktions- und Exportkontrollmandaten verläuft die Mandatskommunikation typischerweise über bzw. mit ausländischen Kanzleien.

ff) Folgewirkung

Da § 22 Abs. 2 den Zugriff bereits bei einer erheblichen Bedrohung zulässt, die Mitteilungspflicht nach § 100 Abs. 1 Nr. 2 aber erst bei einer Bedrohung von herausgehobener Bedeutung entsteht, erfährt der Berufsträger von der Überwachung seiner Mandatskommunikation regelmäßig nichts.

c. Fazit

Die gerügten Punkte führen zu einer Verletzung mehrerer Grundrechte zugleich. Beim Rechtsanwalt ist Art. 12 Abs. 1 GG betroffen: Die Verschwiegenheitspflicht ist konstitutiver Bestandteil des anwaltlichen Berufsbildes.⁷ Weil die Verstrickungsklausel des Abs. 2 Nr. 1 Buchst. c durch die bloße Mandatsführung erfüllt wird, ist der Eingriff nicht die eng begrenzte Ausnahme, sondern der Regelfall — und die Norm enthält kein Kriterium, das eine Abwägung überhaupt steuern könnte. Beim Mandanten ist das Recht auf ein faires Verfahren (Art. 2 Abs. 1 i. V. m. Art. 20 Abs. 3 GG; Art. 6 Abs. 3 Buchst. b und c EMRK) verletzt, dessen Funktionsbedingung die Vertraulichkeit der Verteidigerkommunikation ist; je nach eingesetztem Mittel treten Art. 10 Abs. 1 GG, Art. 13 Abs. 1 GG und das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) hinzu. Der Kernbereich privater Lebensgestaltung (Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG) ist nur berührt, soweit höchstpersönliche Inhalte betroffen sind — Gespräche über konkrete Straftaten zählen gerade nicht dazu⁸; insoweit trägt der Kernbereich den absoluten Verteidigerschutz nicht allein, wohl aber gemeinsam mit dem fairen Verfahren, worauf das

⁷ BVerfGE 113, 29.

⁸ nach BVerfGE 109, 279.

Bundesverfassungsgericht auch die Zweiteilung des § 160a StPO gestützt hat⁹. Dass über Zweifelsfälle der behördliche Datenschutz des Dienstes entscheidet und eine Mitteilung regelmäßig unterbleibt, verletzt zusätzlich Art. 19 Abs. 4 GG. Für Journalisten ist Art. 5 Abs. 1 Satz 2 GG, für Mandatsträger Art. 38 Abs. 1 Satz 2 GG betroffen.

d. Forderungen

- Absoluter Schutz für Verteidiger, Seelsorger und Mandatsträger nach dem Vorbild des § 160a Abs. 1 StPO. Klarstellend: Die Verstrickungsannahme darf sich nicht allein auf die Wahrnehmung der geschützten Tätigkeit stützen.
- Streichung des Regelbeispiels in Abs. 2 Nr. 1 Buchst. c.
- Beschränkung von Abs. 2 Nr. 2 auf Leben, Leib, Freiheit und den Bestand des Bundes oder eines Landes.
- Übernahme der Vorwirkungsregelung des § 21 Abs. 1 Satz 2 und 3 in § 22.
- Vorabkontrolle für jede gegen eine geschützte Person gerichtete Maßnahme; Zweifelsentscheidung durch den Unabhängigen Kontrollrat statt durch den behördlichen Datenschutz.
- Klarstellung, dass ausländische Berufsträger erfasst sind.
- Mitteilungspflicht bei jeder Maßnahme, die zur Erhebung von Daten aus einer Vertraulichkeitsbeziehung geführt hat; Verwertungsverbot für solche Daten in Straf-, Bußgeld- und Verwaltungsverfahren.

2. § 32 BVerfSchG-E

a. Regelungsgehalt

Gem. § 32 Abs. 1 ist eine Maßnahme gegen einen Rechtsanwalt oder bestimmte andere Berufsheimnisträger unzulässig, wenn sie voraussichtlich Informationen erbringen würde, über die der Berufsheimnisträger das Zeugnis verweigern dürfte.

⁹ BVerfGE 141, 220.

Abs. 4 enthält allerdings eine Ausnahmeregelung, die das vermeintlich umfassende Schutzniveau in nicht hinnehmbarer Weise zurückbaut. Es heißt dort:

“Die Absätze 1 bis 3 sind nicht anzuwenden, wenn die Maßnahme wegen tatsächlicher Anhaltspunkte dafür, dass die Person an den aufzuklärenden Bedrohungen beteiligt ist, durchgeführt wird.”

In der Entwurfsbegründung heißt es auf S. 326:

Der Beteiligtenbegriff ist gefahrenabwehrrechtlich zu verstehen, erfasst also Sachverhalte der objektiven Förderung der Bedrohungen, wobei auch mehrstufige Wirkungsketten einbezogen sind, beispielsweise verschleiende Transaktionsketten bei Finanzierungssachverhalten oder Nachrichtenmittler. Gefahrenabwehrrechtlich ist eine subjektive Tatseite grundsätzlich unmaßgeblich.

Es wird somit auch das Entgegennehmen von Nachrichten oder Geldern als “Beteiligung” angesehen, wobei es nicht darauf ankommt, ob der Nachrichtenmittler bzw. Zahlungsempfänger von der Bedrohung bzw. von dem Zusammenhang mit der Bedrohung Kenntnis hat.

b. Kritik

Durch die Ausnahme in Abs. 4 wird der Schutz des Mandatsgeheimnisses von Rechtsanwältinnen und Rechtsanwälten ausgehebelt. Anwaltliche Standardtätigkeiten, wie die Entgegennahme und Weitergabe von Nachrichten oder Zahlungen, können als (objektive) Beteiligung eingestuft und beim Rechtsanwalt direkt überwacht werden.

Der Entwurf versäumt die Chance, ein angemessenes Schutzniveau für Berufsgeheimnisträger, u. a. Rechtsanwältinnen und Rechtsanwälte, zu etablieren. Dies ist angesichts des geplanten massiven Ausbaus der Befugnisse des Bundesamts für Verfassungsschutz besonders beklagenswert.

c. Forderung

Der Schutz von Berufsgeheimnisträgern sollte analog zu § 62 BKAG unter die alleinige Ausnahme gestellt werden, dass unmittelbar von dem Berufsgeheimnisträger eine relevante Bedrohung ausgeht.

III. UKRatG

Die Datenschutzkontrolle durch den Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) soll abgeschafft werden, soweit es um nachrichtendienstliche Tätigkeiten des BfV, des BND und des Militärischen Abschirmdienstes (MAD) geht. Die G10-Kommission und das G10-Gesetz sollen abgeschafft werden. Soweit es um das BfV und den BND geht, sollen alle Kontrollaufgaben stattdessen durch den Unabhängigen Kontrollrat (UKRat) ausgeübt werden, den es erst seit 2021 gibt und der bislang ausschließlich für die reinen Auslandsaktivitäten des BND zuständig war. Die Aufgaben und Befugnisse des UKRat sollen in einem eigenen Gesetz – dem UKRatG – geregelt werden.

Zwar bietet eine Zusammenführung von Kompetenzen grundsätzlich die Chance, eine „echte“ Kontrollinstanz zu schaffen, welche die Befugnisse der Nachrichtendienste wirksam zu begrenzen vermag, indem Kompetenzlücken zwischen den einzelnen Kontrollinstanzen geschlossen werden. Diese Chance wird jedoch durch den Entwurf nicht genutzt. Eine wirksame Nachrichtendienstkontrolle setzt voraus, dass die Kontrollinstanz über ausreichende verfahrensrechtliche Befugnisse verfügt, ihre Entscheidungen tatsächlich durchsetzen kann und personell wie technisch so ausgestattet ist, dass sie den Umfang und die Komplexität der zu kontrollierenden Maßnahmen bewältigen kann. Diesbezüglich bestehen gravierende Bedenken, zumal die Kontrollexpertise und -erfahrung, die im Hause der BfDI über viele Jahre gewonnen wurde, weder sachlich noch personell in den UKRat überführt werden soll.

1. Eine „gerichtsähnliche Kontrolle“ ohne gerichtsähnliches Verfahren?

Nach § 5 UKRatG-E soll der UKRat – wie bereits derzeit im BNDG geregelt – aus einem „gerichtsähnlichen Kontrollorgan“ und einem „administrativen Kontrollorgan“ bestehen. Die Bezeichnung als „gerichtsähnliches“ Kontrollorgan ist jedoch irreführend. Mit einem Gericht hat der UKRatG wenig gemein.

Das gerichtsähnliche Kontrollorgan wird auf Antrag der Nachrichtendienste tätig, etwa nach § 27 Abs. 2 UKRatG-E und § 29 Abs. 2 UKRatG-E, wobei die Dienste zu einem Antrag auf „Vorabkontrolle“ nur in den Fällen verpflichtet sind, die in § 27 Abs. 3 UKRatG-E abschließend aufgeführt sind. Die betroffenen Personen erhalten demgegenüber grundsätzlich keine Möglichkeit, ihre Interessen in diesem Verfahren durch eine Vertretung geltend zu machen. Damit besteht ein strukturelles Ungleichgewicht: Der Nachrichtendienst kennt die beabsichtigte Maßnahme, ihre tatsächlichen Grundlagen und ihre Zielrichtung. Die betroffene Person hat dagegen – wenn sie überhaupt Kenntnis von der Maßnahme erlangt – keine Gelegenheit zur Stellungnahme. Dies steht im Widerspruch zu einem ein Gericht kennzeichnendes kontradiktorischen Verfahren. Der Deutsche Anwaltverein hält es deshalb für fraglich, ob die Bezeichnung der Stelle als „gerichtsähnliches Kontrollorgan“ der verfahrensrechtlichen Ausgestaltung hinreichend Rechnung trägt. Wenn die besonderen Geheimhaltungsinteressen der Nachrichtendienste eine unmittelbare Beteiligung Betroffener ausschließen, sollte zumindest geprüft werden, ob bei einem „gerichtsähnlichen Kontrollorgan“ nicht doch eine unabhängige Vertretung der Betroffeneninteressen Einzug finden soll in Form eines „Anwalts der Betroffenen“, den der Deutsche Anwaltverein bereits in der Vergangenheit für unverzichtbar erachtet hat, um eine rechtsstaatliche Kontrolle der Nachrichtendienste zu gewährleisten.

Das in § 38 UKRatG-E vorgesehene Petitionsrecht für Personen, die der Auffassung sind, durch einen Nachrichtendienst in eigenen Rechten verletzt worden zu sein, vermag diesen Mangel an Rechtsschutz nicht zu beheben. Eine bloße Prüfpflicht ist im Hinblick auf das Gebot effektiven Rechtsschutzes aus Art. 19 Abs. 4 GG ungenügend. Zwar können bei geheimen nachrichtendienstlichen Maßnahmen durchaus besondere verfahrensrechtliche Anforderungen gelten. Diese Besonderheiten rechtfertigen jedoch nicht, die Kontrolle auf eine unverbindliche Prüfung ohne Rechtsfolge zu beschränken. Der Gesetzgeber sollte daher klarstellen, welche Rechtsfolgen sich aus einer

erfolgreichen Petition ergeben. Insbesondere sollte vorgesehen werden, dass der UKRat bei festgestellten Rechtsverletzungen verbindliche Maßnahmen zu deren Beseitigung treffen muss.

2. Die „administrative Kontrolle“: ein zahloser Tiger?

Besondere Bedenken bestehen auch hinsichtlich § 33 UKRatG-E. Danach kann das „administrative Kontrollorgan“ bei einem einfachen Verstoß eine Beanstandung gegenüber der zuständigen Aufsichtsbehörde aussprechen und eine Stellungnahme einholen. Eine ausdrückliche Befugnis zur Beseitigung des festgestellten Rechtsverstoßes ist damit jedoch nicht verbunden. Dies schwächt die Wirksamkeit der Kontrolle erheblich. Eine unabhängige Kontrollinstanz sollte nicht darauf beschränkt sein, einer anderen staatlichen Stelle mitzuteilen, dass sie einen Rechtsverstoß festgestellt hat. Wird eine Maßnahme als rechtswidrig erkannt, muss grundsätzlich auch gewährleistet sein, dass die Kontrollinstanz die Rechtsverletzung beenden und ihre Folgen beseitigen kann.

Für qualifizierte Verstöße sieht § 34 UKRatG-E zwar weitergehende Reaktionen vor. Danach kann das administrative Kontrollorgan, wenn es einen qualifizierten Verstoß feststellt und der zuständige Nachrichtendienst dem Verstoß nicht nach § 33 UKRatG-E abhilft, gem. § 34 Abs. 1 UKRatG-E den Senat des UKRat anrufen. Dieser kann nach eigener Prüfung gem. § 34 Abs. 2 UKRatG-E eine Anweisung ggü. dem betroffenen Nachrichtendienst erlassen. Problematisch ist auch hier, dass der Gesetzesentwurf im Falle der Nichtbefolgung dem Senat keine Durchsetzungsinstrumente an die Hand gibt. Kommt der Nachrichtendienst der Anweisung nicht nach, sieht Abs. 2 allein die Unterrichtung des Parlamentarischen Kontrollgremiums (PKGr) als Möglichkeit vor. Dies kann die fehlende rechtliche Durchsetzbarkeit einer Anweisung jedoch nicht annähernd kompensieren. Zwar kann das PKGr ggf. politischen Druck ausüben, ist jedoch nicht befugt, eine konkrete rechtswidrige Maßnahme zu beenden.

Der Deutsche Anwaltverein hält deshalb eine Ergänzung von §§ 33, 34 UKRatG-E für erforderlich. Zum einen muss § 33 UKRatG-E um eine Durchsetzungsinstrumente ergänzt werden. Auch im Rahmen des § 34 UKRatG-E müssen für den Fall, dass ein

Nachrichtendienst einer verbindlichen Anweisung des Kontrollrats nicht nachkommt, wirksame Folgemaßnahmen vorgesehen werden.

3. Eine lückenhafte Kontrolle

Allgemeine Bestimmungen zur Reichweite der Kontrolle der Rechtmäßigkeit regelt der Entwurf in § 2 UKRatG-E. Diese Kontrolle weist aus Sicht des Deutschen Anwaltvereins erhebliche Lücken auf.

Dies betrifft zum einen ihren Anwendungsbereich. Gem. § 2 Abs. 1 UKRatG-E beschränkt sich diese auf die Verarbeitung personenbezogener Daten.

Grundrechtsintensive Maßnahmen können aber bereits in der Art und Weise der technischen oder operativen Durchführung liegen. Hierfür nehme man beispielhaft die Erhebung von Daten aus informationstechnischen Systemen nach § 37 Abs. 1 BNDG-E. Bei genauer Betrachtung darf der BND zweierlei: zum einen auf das IT-System zugreifen, zum anderen – nach dem Zugriff – personenbezogene Daten erheben. Dass eine Kontrolle der Rechtmäßigkeit durch den UKRatG allein bei der Erhebung der Daten, aber nicht beim Zugriff erfolgt, steht im Widerspruch zur Grundrechtsintensität des Zugriffs. Laut dem BVerfG schützt das IT-Grundrecht aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG „nicht nur die Vertraulichkeit der Daten, die durch Datenerhebungsvorgänge verletzt wird, sondern verlagert diesen Schutz nach vorne und umfasst schon die abstrakt-systembezogene Vertraulichkeitserwartung im Vorfeld konkreter Datenerhebungen“. Daher besteht „bereits mit dem Zugriff auf ein IT-System [...] eine besondere Gefährdungslage“.¹⁰ Der Eingriff in das IT-Grundrecht liegt somit bereits im Zugriff selbst. Das gleiche Problem betrifft Maßnahmen, die in die von Art. 13 GG geschützte räumliche Sphäre eingreifen. Auch hier liegt in einem Eindringen in eine Wohnung oder einen Geschäftsraum noch nicht die Erhebung personenbezogener Daten. Dennoch greift die Maßnahme in Art. 13 GG ein. Warum die Rechtskontrolle allein auf die Verarbeitung personenbezogener Daten beschränkt ist und alle sonstigen Maßnahmen, mögen sie auch noch so grundrechtssensibel sein, der Kontrolle nicht unterliegen, erschließt sich nicht. Die Gesetzesbegründung zu § 2 Abs. 1 UKRatG-E (S. 612 f.) betont, dass die „staatliche Überwachungstätigkeit“ auf die Verarbeitung personenbezogener Daten gerichtet sei. Dass auch schon ohne Verarbeitung von

¹⁰ BVerfG, Beschl. v. 24.06.2025 – 1 BvR 2466/19 – Trojaner I, Rn. 100.

personenbezogenen Daten durch Maßnahmen in Grundrechte eingegriffen werden kann, erwähnt sie hingegen nicht.

Die Reichweite der vorgesehenen Vorabkontrolle begegnet darüber hinaus eigenständigen Bedenken. Nach § 2 Abs. 2 Nr. 1 UKRatG-E ist das gerichtsähnliche Kontrollorgan nur für die „gesetzlich bestimmte[n] Maßnahmen“ zuständig. Die gesetzlich bestimmten Fälle sind jedoch vergleichsweise begrenzt. So soll beispielsweise dem BND im Umkehrschluss zu § 97 Abs. 1 Nr. 14 i.V.m. § 37 Abs. 1 BNDG-E der Einsatz von Trojanern ohne Vorabkontrolle möglich sein, wenn sich die Maßnahme gegen ein nicht privates genutztes Gerät richtet – eine schier unbegrenzte Anzahl von Geräten, verfügt doch mittlerweile die überwiegende Zahl der Arbeitnehmer an ihrem Arbeitsplatz über einen Computer oder ein zusätzliches Smartphone. Im Wege eines effektiven Grundrechtsschutzes darf eine Vorabkontrolle jedoch nicht allein davon abhängen, ob der Gesetzgeber eine bestimmte Maßnahme ausdrücklich in den Katalog der kontrollierten Maßnahmen aufgenommen hat, sondern wie grundrechtsintensiv die Maßnahme ist.

Besonders kritisch zu sehen ist die Beschränkung der „administrativen Kontrolle“ auf ein „Prüfprogramm“ (§ 32 Abs. 2 UKRatG-E), das das „gerichtsähnliche Kontrollorgan“ nach § 26 UKRatG-E für einen Zeitraum von 24 Monaten beschließt (§ 26 Abs. 1 UKRatG-E). Dies schützt die Nachrichtendienste vor überraschenden Prüfungen, wie sie in der Vergangenheit der Praxis der BfDI entsprach. Zugleich schafft die Beschränkung auf ein „Prüfprogramm“ erhebliche kontrollfreie Zonen, da die Mitarbeiter der Nachrichtendienste darauf vertrauen können, dass es außerhalb des „Prüfprogramms“ (und der Fälle, in denen eine „Vorabkontrolle“ vorgeschrieben ist), keine Kontrolle der Rechtmäßigkeit nachrichtendienstlicher Maßnahmen gibt.

4. Eine weitgehende personelle sowie fachliche Verknappung

Bisher bestehende Kompetenzen der BfDI sowie der G10-Kommission fallen nun dem UKRat zu. Somit endet die nach § 28 BVerfSchG, § 63 BNDG bestehende Zuständigkeit der BfDI für die datenschutzrechtliche Kontrolle der Nachrichtendienste. Ebenso endet die Kompetenz der Vorabkontrolle von Maßnahmen durch die G10-Kommission nach § 15 Abs. 6 G 10.

Hiermit müsste zwingend eine proportionale Aufstockung der Ressourcen des UKRat einhergehen – diese bleibt jedoch aus. Zwar soll das gerichtsähnliche Kontrollorgan gem. § 14 UKRatG-E nun aus 8 statt aus bislang 6 Mitgliedern bestehen. Ob diese zwei Mitglieder bei einem erheblich gewachsenen Aufgabenkreis einen Unterschied machen, darf bezweifelt werden. Ein Blick in die Gesetzesbegründung (S. 222) schafft keine Abhilfe: für den UKRatG werden allein 37 Planstellen veranschlagt, wobei auch nur 27 für die gerichtsähnliche und administrative Rechtskontrolle zuständig sind. Kosten soll dies jährlich 8,86 Mio. Euro. Ein kleiner Vergleich: Für das Jahr 2026 werden dem BND vom Bund ca. 1,5 Mrd. Euro und somit das 170-fache an finanziellen Mitteln zur Verfügung gestellt – ein durchaus bemerkenswerter Größenunterschied, der eine künftige Unterbesetzung des UKRat zumindest nicht unwahrscheinlicher macht.

Doch es fehlen nicht nur personelle Mittel. Auch die bei der BfDI im Bereich der Kontrolle vorhandene große juristische und technische Expertise setzt sich nicht zwangsläufig fort beim UKRat. Diese war jedoch notwendig angesichts der komplexen technischen Befugnisse des BND. Eine Lösung für diesen Verlust an Sachverstand bietet der Entwurf nicht – weder durch die Einbindung technischer Sachverständiger noch durch eine punktuelle Einbindung der BfDI.

IV. BNDG

1. Schutz von Vertraulichkeitsbeziehungen nach § 22 BNDG-E

Der Deutsche Anwaltverein hegt insbesondere Bedenken hinsichtlich des in § 22 BNDG-E geregelten Schutzes von Vertraulichkeitsbeziehungen.

§ 22 BNDG-E ersetzt zum einen den bisherigen § 21 BNDG, der die Verarbeitung von Daten aus Vertraulichkeitsbeziehungen von ausländischen Personen im Ausland regelte (sog. Ausland-Ausland-Kommunikation). Zum anderen soll die Vorschrift künftig auch für die Kommunikation zwischen Personen im Ausland und Inland gelten (sog. Ausland-Inland-Kommunikation). Damit ersetzt § 22 BNDG-E den Schutz der Ausland-

Inland-Kommunikation aus § 3b Abs. 2 und 4 G 10. Der Schutz des Anwaltsgeheimnisses würde erheblich geschwächt.

a. Ausland-Ausland-Kommunikation

§ 22 Abs. 1 BNDG-E untersagt zwar grundsätzlich die gezielte Erhebung personenbezogener Daten zum Zweck der Erlangung von Erkenntnissen aus einer Vertraulichkeitsbeziehung. Dieser Schutz wird jedoch durch den in Absatz 2 vorgesehenen Ausnahmekatalog erheblich relativiert. Das Regel-Ausnahme-Verhältnis des Absatzes 1 droht dadurch gegenüber der bisherigen Rechtslage faktisch umgekehrt zu werden.

Nach geltendem Recht sind Eingriffe in den Schutz von Vertraulichkeitsbeziehungen im Bereich der Ausland-Ausland-Kommunikation nur unter engen Voraussetzungen zulässig. Nach § 21 Abs. 2 Nr. 1 i.V.m. § 11a Abs. 1 BNDG musste die betroffene Person Täter oder Teilnehmer einer schweren Straftat oder einer Straftat im unmittelbaren Zusammenhang mit einem nachrichtendienstlich relevanten Gefahrenbereich – etwa der Gefährdung kritischer Infrastrukturen – sein. Alternativ muss nach § 21 Abs. 2 Nr. 2 BNDG die Maßnahme zur Abwehr einer Gefahr für ein besonders gewichtiges Rechtsgut, etwa Leib oder Leben, erforderlich sein. Der Deutsche Anwaltverein sieht mit erheblicher Sorge, dass § 22 BNDG-E den Schutz dieser Vertraulichkeitsbeziehungen gegenüber der bisherigen Rechtslage in wesentlichen Punkten abschwächt. Künftig soll es nach § 22 Abs. 2 Nr. 1 BNDG-E nicht mehr erforderlich sein, dass die betroffene Rechtsanwältin oder der betroffene Rechtsanwalt selbst Täter oder Teilnehmer einer Straftat ist. Vielmehr soll bereits ein Zusammenhang mit einer „erheblichen Bedrohung“ im Sinne des § 3 Abs. 1 BNDG-E ausreichen. Damit werden neben den für eine Bedrohung selbst verantwortlichen Personen auch Personen erfasst, die Mitglieder eines Netzwerks sind, welches die Bedrohung unterstützt.

Besonders problematisch ist § 22 Abs. 2 Nr. 1 lit. c BNDG-E. Danach genügt bereits ein „Zusammenhang [...], der „Grund zu der Annahme gibt, dass durch die Maßnahme Erkenntnisse über diese Bedrohung gewonnen werden können, die nicht gleichermaßen durch eine Maßnahme gegen eine Person nach Buchstaben a und b zu

gewinnen sind“. Die Vorschrift erfasst dabei ausdrücklich auch Personen, die Mitteilungen für entsprechende Personen entgegennehmen oder weitergeben, ohne dass ein Bewusstsein über die Bedeutung dieses Kontakts vorausgesetzt wird. Für Rechtsanwältinnen und Rechtsanwälte ist diese Regelung von besonderer Brisanz. Die anwaltliche Tätigkeit bringt es gerade bei international ausgerichteten Mandaten zwangsläufig mit sich, dass Rechtsanwälte mit einer Vielzahl von Personen in unterschiedlichen Staaten kommunizieren. In bestimmten Mandaten ist es nicht ausgeschlossen, dass diese Kontakte auch Personen betreffen können, die sich in politisch oder sicherheitsrechtlich sensiblen Regionen aufhalten oder zu Personen mit nachrichtendienstlicher Relevanz in Verbindung stehen. Besonders bedenklich ist dabei, dass § 22 Abs. 2 Nr. 1 lit. c BNDG-E keinen konkreten Nachweis verlangt, dass die betroffene Rechtsanwältin oder der betroffene Rechtsanwalt tatsächlich mit einer konkret bedrohungsrelevanten Person eine entsprechende Beziehung unterhält. Es genügt, dass die Person zu der Bedrohung in einem „Zusammenhang [steht], der Grund zu der Annahme gibt, dass durch die Maßnahme Erkenntnisse über diese Bedrohung gewonnen werden können“. Für die Anwaltschaft ist dies besonders problematisch, weil gerade die anwaltliche Tätigkeit darauf angelegt ist, auch mit Personen zu kommunizieren, die selbst Gegenstand staatlicher Ermittlungen oder nachrichtendienstlicher Beobachtung sein können. Insbesondere besteht die Sorge, dass der BND bei der Kommunikation mit potenziell straffällig gewordenen Personen oder politisch sensiblen Mandanten immer davon ausgehen kann, Erkenntnisse zu gewinnen. Bereits die Kenntnis, dass eine bestimmte Person anwaltlichen Rat bei einer bestimmten Rechtsanwältin oder einem bestimmten Rechtsanwalt sucht, kann höchst sensible Informationen offenbaren. Ein Rechtsanwalt kann und darf aber nicht zum bloßen Überwachungsobjekt werden, weil er seine berufliche Pflicht erfüllt und einem Mandanten rechtlichen Beistand leistet.

b. Ausland-Inland-Kommunikation

Besonders gravierend sind die Auswirkungen auf die Ausland-Inland-Kommunikation. Betroffen sind hier insbesondere in Deutschland tätige Rechtsanwältinnen und Rechtsanwälte, die mit Mandanten oder anderen am Mandat beteiligten Personen im Ausland kommunizieren. Bislang waren Maßnahmen nach § 3b Abs. 4 G 10

grundsätzlich daran geknüpft, dass die betroffene Person selbst einer Straftat verdächtig war oder diese bewusst unterstützte. Der Gesetzentwurf gibt diese hohe Eingriffsschwelle auf. Auch für die Ausland-Inland-Kommunikation soll künftig bereits nach § 22 Abs. 2 Nr. 1 BNDG-E ein Zusammenhang mit einer erheblichen Bedrohung oder die Annahme genügen, dass über die betroffene Person relevante Erkenntnisse gewonnen werden können. Ob die Rechtsanwältin oder der Rechtsanwalt tatsächlich Kenntnis von einer etwaigen Gefährdungslage hat oder diese bewusst unterstützt, ist danach nicht mehr entscheidend. Dies steht im diametralen Widerspruch zur vertraulichen anwaltlichen Tätigkeit. Wie die anwaltliche Schweigepflicht aus § 43a Abs. 2 BRAO und die strafrechtliche Sanktionierung der Offenbarung eines Geheimnisses durch einen Anwalt nach § 203 Abs. 1 Nr. 3 StGB, insbesondere aber auch der verfassungsrechtliche Rang des Anwaltsgeheimnisses in Deutschland und Europa belegen, ist die Vertraulichkeit der Kommunikation zwischen Anwalt und Mandant unerlässlich. Mandantinnen und Mandanten müssen darauf vertrauen können, dass sie ihre Rechtsanwältin oder ihren Rechtsanwalt auch zu sensiblen, möglicherweise strafrechtlich oder sicherheitsrechtlich relevanten Sachverhalten uneingeschränkt informieren können. Nur unter dieser Voraussetzung kann die Anwaltschaft ihre Funktion bei der Durchsetzung und Wahrung von Rechten wirksam erfüllen. Genau das Vertrauen in diese Beziehung wird jedoch durch § 22 BNDG-E erheblich erschüttert. Hinzu kommt, dass gem. § 22 Abs. 2 Nr. 2 BNDG-E bei Ausland-Inland-Kommunikation eine Maßnahme bereits zulässig sein soll, wenn sie „zur Abwendung einer erheblichen Gefahr für ein besonders gewichtiges Rechtsgut“ notwendig ist. Damit wird eine Eingriffsmöglichkeit, die bislang nur für die Ausland-Ausland-Kommunikation vorgesehen war, auf die Kommunikation mit in Deutschland tätigen Rechtsanwältinnen und Rechtsanwälten erstreckt. Diese Erweiterung ist aus Sicht des Deutschen Anwaltvereins besonders kritisch. Die Entscheidung darüber, wann eine solche Maßnahme „notwendig“ ist, wird in erheblichem Umfang in den Beurteilungsspielraum des Nachrichtendienstes verlagert. Dies beinhaltet ein erhebliches Missbrauchspotenzial. Besonders problematisch ist die Angleichung der Ausland-Inland-Kommunikation an das bislang deutlich niedrigere Schutzniveau der Ausland-Ausland-Kommunikation. Die anwaltliche Vertraulichkeitsbeziehung droht damit von einem grundsätzlich geschützten Bereich zu einem Schutzgut zu werden, welches bereits bei vergleichsweise weit definierten Gefahrenlagen zurücktreten muss. Auch kann dieses Missbrauchspotenzial Mandantinnen und Mandanten davon abschrecken,

bestimmte Sachverhalte gegenüber ihrer Rechtsanwältin oder ihrem Rechtsanwalt offenzulegen, wenn sie nicht sicher sein können, dass die Kommunikation tatsächlich vertraulich bleibt. Dies betrifft gerade Mandate, in denen eine umfassende und offene Kommunikation besonders erforderlich ist. Für das Mandatsgeheimnis bedeutet dies eine strukturelle Schwächung.

Auffallend ist schließlich, dass die Gesetzesbegründung zu § 22 Abs. 2 BNDG-E diese erheblichen Auswirkungen der Neuregelung auf die anwaltliche Vertraulichkeitsbeziehung nicht hinreichend nachvollziehbar darstellt. Eine derart weitreichende Absenkung der Eingriffsschwellen bedarf einer ausdrücklichen Auseinandersetzung mit den gegenläufigen grundrechtlichen Belangen. Dies gilt insbesondere angesichts der zentralen Bedeutung der anwaltlichen Verschwiegenheit für den effektiven Zugang zum Recht und für eine funktionierende Rechtspflege.

c. Fazit

Der Gesetzentwurf nutzt die Zusammenführung des BND-Gesetzes und des G-10-Gesetzes in § 22 BNDG-E, um die bislang unterschiedlichen Schutzregime für Ausland-Ausland- und Ausland-Inland-Kommunikation anzugleichen. Statt auf das Schutzniveau der Ausland-Inland-Kommunikation wurde sich mit dem Entwurf jedoch dazu entschieden, den wesentlich geringeren Schutz der Ausland-Ausland-Kommunikation als einheitliches Regime zu wählen. Richtigerweise hätte die Vereinheitlichung der beiden Regelungsregime jedoch in die entgegengesetzte Richtung erfolgen müssen. Der Gesetzgeber hätte das höhere Schutzniveau der Ausland-Inland-Kommunikation konsequent auf die gesamte anwaltliche Kommunikation mit ihren Mandanten ausweiten müssen. Der Gesetzentwurf verpasst damit die Chance, den durch die Verfassungsgerichtsrechtsprechung ohnehin gebotenen Systemwechsel zu nutzen, um den Schutz des Anwaltsgeheimnisses in beiden Konstellationen auf ein einheitlich hohes Niveau zu heben. Stattdessen wird der bislang bestehende, wenn auch nicht lückenlose, Schutz der Ausland-Inland-Kommunikation faktisch preisgegeben.

2. Online-Durchsuchungen nach §§ 36 ff. BNDG-E

Der Deutsche Anwaltverein sieht die im Entwurf in §§ 36 ff. BNDG-E geregelten Online-Durchsuchungen sehr kritisch. Hierzu tragen auch die in diesem Zusammenhang bestehenden neuen Pflichten des BSI bei.

a. Einsatz von Trojanern gegen Rechtsanwältinnen und Rechtsanwälte

§ 37 BNDG-E stellt gemeinsam mit § 38 BNDG-E die künftige Regelung für Maßnahmen dar, die bislang nach § 34 BNDG im Bereich der Ausland-Ausland-Kommunikation sowie nach § 11 Abs. 1a G 10 im Bereich der Ausland-Inland-Kommunikation zulässig waren. Der Gesetzentwurf erweckt zunächst den Eindruck, für Eingriffe in informationstechnische Systeme ein abgestuftes und differenziertes Schutzkonzept zu schaffen. Bei genauerer Betrachtung zeigt sich jedoch, dass die vorgesehenen Schutzvorkehrungen dahinter zurückbleiben.

aa) Geringe Hürden

Besonders deutlich wird dies am Beispiel eines deutschen Rechtsanwalts, dessen dienstlich genutztes Arbeitshandy mittels eines staatlichen Trojaners ausgespäht wird. Bei einem solchen Arbeitshandy handelt es sich um ein informationstechnisches System im Sinne der Vorschrift. Da das Gerät nicht dem privaten Bereich zugeordnet wird, ist allein § 37 Abs. 1 BNDG-E einschlägig. Die erhöhten Voraussetzungen der Absätze 2 und 3 greifen dagegen nicht ein, da diese ausschließlich für private informationstechnische Systeme vorgesehen sind. Dies hat zur Folge, dass für den Einsatz eines Trojaners gegen einen deutschen Rechtsanwalt bereits genügt, dass tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme erforderlich ist, um Informationen über zumindest erhebliche Bedrohungen im Sinne des § 3 Abs. 1 BNDG-E zu gewinnen.

Zwar definiert § 3 Abs. 1 BNDG-E eine erhebliche Bedrohung als eine Gefährdung, die geeignet ist, ein besonders gewichtiges Rechtsgut in besonderem Maße zu beeinträchtigen. Die eigentliche Eingriffsschwelle liegt jedoch nicht in diesem

Bedrohungsbegriff, sondern in dem Merkmal der Erforderlichkeit. Gerade weil ein Trojaner aufgrund seines umfassenden Zugriffs auf gespeicherte und laufende Kommunikationsdaten regelmäßig das effektivste Mittel zur Informationsgewinnung darstellen wird, eröffnet die Vorschrift dem BND einen erheblichen Beurteilungsspielraum. Je weitreichender die technische Zugriffsmöglichkeit ist, desto leichter lässt sich argumentieren, dass gerade diese Maßnahme zur Erlangung relevanter Erkenntnisse erforderlich sei. Eine eigenständige Verhältnismäßigkeitsprüfung sieht § 37 Abs. 1 BNDG-E hingegen nicht vor. Dies überrascht umso mehr, als dem Gesetzgeber entsprechende Schutzmechanismen durchaus bekannt sind. So enthält etwa § 32 Abs. 2 Satz 2 Nr. 2 BVerfSchG-E zumindest noch Ansätze einer – wenn auch gegenüber der bisherigen Rechtslage bereits deutlich abgeschwächten – Verhältnismäßigkeitsprüfung.

Diese niedrige Eingriffsschwelle steht in einem deutlichen Spannungsverhältnis zur außergewöhnlichen Eingriffsintensität der Maßnahme. Auf einem Arbeitshandy befinden sich regelmäßig zahlreiche personenbezogene Daten des betroffenen Rechtsanwalts. Hierzu zählen etwa Standortdaten, Fotos, Kalender- und Kontaktdaten sowie sonstige Informationen über seine beruflichen und privaten Lebensumstände. Von noch größerer Bedeutung ist jedoch die Möglichkeit, auf die Kommunikation mit Mandantinnen und Mandanten zuzugreifen. Gerade diese Kommunikation enthält häufig besonders sensible Informationen über die persönlichen, wirtschaftlichen und rechtlichen Verhältnisse der Mandantschaft sowie über vertrauliche Mitteilungen und die anwaltliche Beratung. Durch die Infiltration eines solchen Geräts werden daher sowohl das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG hinsichtlich laufender Kommunikation als auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hinsichtlich gespeicherter Daten in erheblichem Maße berührt.

Problematisch erscheint in diesem Zusammenhang auch die gesetzgeberische Begründung der Differenzierung zwischen privaten und nicht privaten informationstechnischen Systemen. Die Gesetzesbegründung (S. 487) verweist insoweit auf die Entscheidung des Bundesverfassungsgerichts zum IT-Grundrecht¹¹ und leitet daraus ab, dass allein privat genutzte informationstechnische Systeme in den

¹¹ BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 und 1 BvR 595/07, BVerfGE 120, 274 ff., Rn. 206.

Schutzbereich dieses Grundrechts fallen. Eine solche Lesart überzeugt jedoch nicht. Das Bundesverfassungsgericht spricht allein davon, dass die betroffene Person das IT-System „überwiegend als eigenes nutzt“. Damit stellt es gerade nicht schematisch auf die Unterscheidung zwischen privaten und dienstlichen Geräten ab. Vielmehr knüpft es den Schutz an die berechnete Erwartung der betroffenen Person, dass die Vertraulichkeit und Integrität des informationstechnischen Systems gewahrt bleibt. Eine solche Schutz- und Vertraulichkeitserwartung kann jedoch selbstverständlich auch bei einem dienstlich genutzten Arbeitshandy bestehen. Dies gilt insbesondere für Rechtsanwältinnen und Rechtsanwälte, deren berufliche Tätigkeit gerade auf der vertraulichen Kommunikation mit Mandantinnen und Mandanten beruht.

bb) Kein Eingreifen von § 22 BNDG-E

Nun könnte man auf den ersten Blick meinen, dass § 22 BNDG-E als zusätzliche Schutzvorschrift eingreift. Bei näherer Betrachtung erweist sich jedoch auch diese Hürde als nur begrenzt wirksam. Nach § 22 Abs. 1 BNDG-E ist die Erhebung personenbezogener Daten unzulässig, wenn sie zum Zweck der „gezielten“ Erlangung von Informationen aus einer anwaltlichen Vertraulichkeitsbeziehung erfolgt. Die Vorschrift erfasst damit lediglich Maßnahmen, die gerade auf die Vertraulichkeitsbeziehung als solche gerichtet sind. Dem BND bleibt es hingegen möglich, die Maßnahme formal auf die Gewinnung sonstiger personenbezogener Daten auszurichten. Werden im Rahmen einer solchen Maßnahme zugleich Informationen aus der Kommunikation zwischen Rechtsanwalt und Mandant bekannt, greift das Verbot des § 22 Abs. 1 BNDG-E nicht ohne Weiteres. Der Schutz anwaltlicher Vertraulichkeitsbeziehungen droht dadurch in der praktischen Anwendung erheblich an Wirksamkeit zu verlieren.

cc) Mangelnde Kontrolle durch den Unabhängigen Kontrollrat

Hinzu kommt, dass Maßnahmen nach § 37 Abs. 1 BNDG-E nicht einmal einer vorgelagerten Kontrolle durch den Unabhängigen Kontrollrat (UKR) unterliegen. Nach § 97 Abs. 1 Nr. 14 BNDG-E ist eine solche Vorabkontrolle lediglich für Maßnahmen nach § 37 Abs. 2 und 3 BNDG-E vorgesehen. Gerade die hier einschlägige Standardmaßnahme des § 37 Abs. 1 BNDG-E bleibt hiervon ausgenommen. Selbst die wenigen verbliebenen Kontrollmechanismen greifen somit nicht zugunsten des

betroffenen Rechtsanwalts ein. Gleiches gilt für die Mitteilung an betroffene Personen nach § 100 Abs. 1 Nr. 2 BNDG-E. Wie bereits bei der Vorabkontrolle durch den Unabhängigen Kontrollrat ist für die Standardmaßnahme nach § 37 Abs. 1 BNDG-E keine Mitteilungspflicht vorgesehen. Ohne eine solche Mitteilung bleibt dem betroffenen Rechtsanwalt auch die Möglichkeit verwehrt, die Maßnahme nachträglich gerichtlich überprüfen zu lassen.

Zudem bleibt fraglich, ob sich die Mitteilungspraxis des BND durch die Neuregelung tatsächlich verbessert. Der BND kann nach § 100 Abs. 4 Nr. 4 bereits von vornherein (ohne den Umweg über eine Zurückstellung) endgültig von einer Mitteilung absehen, wenn schon zu Beginn "mit an Sicherheit grenzender Wahrscheinlichkeit" feststeht, dass eine dauerhafte Nichtmitteilung geboten sein wird. Diese Feststellung ist zwar an die Zustimmung des Unabhängigen Kontrollrats gebunden, schafft jedoch einen zusätzlichen, in dieser Form bislang nicht bestehenden Ausnahmetatbestand.

dd) Fazit

Insgesamt drängt sich daher der Eindruck auf, dass der Gesetzentwurf die verfassungsrechtliche Tragweite des Einsatzes staatlicher Trojaner gegenüber Rechtsanwältinnen und Rechtsanwälten erheblich unterschätzt. Die Kombination aus niedriger Eingriffsschwelle, fehlender Verhältnismäßigkeitsprüfung, eingeschränktem Schutz anwaltlicher Vertraulichkeitsbeziehungen und dem Fehlen einer unabhängigen Vorabkontrolle sowie der Mitteilungspflicht als Anstoß für eine ex-post Kontrolle eröffnet einen weitreichenden Überwachungsrahmen. Vor diesem Hintergrund bestehen erhebliche Zweifel an der Vereinbarkeit der Regelung mit dem Fernmeldegeheimnis aus Art. 10 Abs. 1 GG sowie dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

b. Umkehrung des Schutzzwecks des BSI

Bedenken begegnen der in § 10 Abs. 2 Nr. 2 BNDG-E vorgesehenen Verpflichtung des Bundesamts für Sicherheit in der Informationstechnik (BSI), dem BND auch ohne vorheriges Ersuchen von sich aus Informationen zu übermitteln. Nach der Gesetzesbegründung (S. 400) umfasst dies ausdrücklich auch Erkenntnisse über 0-

Day-Schwachstellen. Aus der Begründung wird zugleich ersichtlich, welchem Zweck die Übermittlung eigentlich dienen soll: Die Zeitspanne zwischen der Entdeckung einer Schwachstelle durch das BSI, ihrer Mitteilung an die Hersteller, der Entwicklung eines Patches und dessen flächendeckender Installation soll dem BND ermöglichen, die Schwachstelle nachrichtendienstlich „in Wert zu bringen“ – mithin offensiv auszunutzen, etwa für die in §§ 36 ff. BNDG-E vorgesehene Online-Durchsuchung. Dies steht in einem grundlegenden Spannungsverhältnis zum gesetzlichen Auftrag des BSI, das nach dem BSI-Gesetz gerade die IT-Sicherheit in Deutschland stärken und bekannte Schwachstellen möglichst schnell beseitigen soll. Statt dem Grundsatz des „Responsible Disclosure“ zu folgen und Sicherheitslücken unverzüglich den Herstellern zu melden, schafft der Entwurf damit faktisch einen Anreiz zur Schwachstellenhortung im Interesse des BND. Die Konsequenz wäre, dass ungepatchte Sicherheitslücken länger offenbleiben und dadurch auch kriminellen Akteuren oder ausländischen Nachrichtendiensten als Angriffsmöglichkeit zur Verfügung stehen, sofern diese dieselbe Schwachstelle unabhängig entdecken. Besonders problematisch ist, dass das BSI – anders als etwa die Verfassungsschutzbehörden nach § 10 Abs. 4 Nr. 1 BNDG-E – selbst bei entgegenstehenden überwiegenden Sicherheitsinteressen – keine Befreiung von der Übermittlungspflicht erhalten kann. Ein Ausnahme- oder Widerspruchsrecht ist nicht vorgesehen, obwohl gerade angesichts des Spannungsverhältnisses zwischen dem gesamtgesellschaftlichen Interesse an einer sicheren IT-Infrastruktur und dem nachrichtendienstlichen Interesse an der Offenhaltung von Angriffsvektoren eine Abwägung erforderlich wäre. Die Gesetzesbegründung erkennt diesen Konflikt zwar, löst ihn jedoch einseitig zugunsten der nachrichtendienstlichen Nutzung auf und sieht zugleich kein höchststrichterlich gefordertes Schwachstellenmanagement vor.¹² Damit wird ein strukturelles Defizit geschaffen, bei dem die Cybersicherheit der Allgemeinheit hinter den operativen Interessen des BND zurücktritt.

3. Strategische Aufklärung

Die §§ 31 ff. BNDG-E sollen die in §§ 5 ff. G10 und § 19 BNDG geregelte „strategische Fernmeldeüberwachung“ unter dem neuen Namen „strategische Aufklärung“ ersetzen. Wie bereits bei § 22 BNDG-E (s.o.) wird der Schutz von Ausland-Ausland-

¹² BVerfG, Urteil vom 08.06.2021 - 1 BvR 2771/18.

Kommunikation und Ausland-Inland-Kommunikation zusammengeführt – und wiederum orientieren sich die neuen Eingriffsschwellen an den niedrigen Hürden der Ausland-Ausland-Kommunikation.

a. De facto wirkungslose Volumengrenze - § 10 Abs. 4 S. 3 G10 / § 31 Abs. 3 S. 2 Nr. 2 BNDG-E

Während § 10 Abs. 4 S. 3 G10 die Ausleitung auf 20 % der verfügbaren Kapazität eines Übertragungswegs begrenzt, soll § 31 Abs. 3 S. 2 Nr. 2 BNDG-E künftig die Erfassung von bis zu 15 % des Datenvolumens erlauben, das in „allen Telekommunikationsnetzen“ übertragen werden kann. Problematisch sind dabei insbesondere die unklare Bezugsgröße und die Orientierung an der theoretisch möglichen statt der tatsächlich genutzten Kapazität. Bei entsprechend weiter Auslegung durch den BND könnte die 15-%-Grenze faktisch nahezu den gesamten tatsächlichen Datenverkehr erfassbar machen. Die vorgesehene Volumengrenze droht damit ihre effektive Begrenzungswirkung zu verlieren und zu einer bloßen Rechengröße zu werden. Zugleich steigt das Risiko, dass auch vertrauliche Mandatskommunikation in großem Umfang erfasst wird.

b. Löschpflicht als Speicherbefugnis - § 66 Abs. 1 S. 1 BNDG-E

§ 66 Abs. 1 S. 1 BNDG-E sieht die Löschung von Inhaltsdaten spätestens nach sechs Monaten vor und ermöglicht damit zugleich deren sechsmonatige Speicherung und nachträgliche Auswertung. Insbesondere können nachträglich gewonnene Suchbegriffe auf den gespeicherten Datenbestand angewendet werden. Ob anwaltliche Kommunikation von der nachrichtendienstlichen Auswertung erfasst wird, entscheidet sich damit nicht mehr abschließend im Zeitpunkt ihrer Erhebung. Auch zunächst unauffällige Mandats- und Verteidigerkommunikation kann nachträglich in den Fokus der Auswertung geraten, wodurch insbesondere die Vertraulichkeit des Mandatsverhältnisses gefährdet wird.

c. Wegfall des Suchbegriffsverbots - § 5 Abs. 2 G10 / §§ 33 Abs. 3, 34 Abs. 2 BNDG-E

§ 5 Abs. 2 S. 2 Nr. 1 G10 verbietet bislang bestimmte personenbezogene Suchbegriffe zur gezielten Überwachung einzelner Personen. Diese Einschränkung soll nach § 33 Abs. 3 BNDG-E weitgehend entfallen. Damit könnten etwa Namen, E-Mail-Adressen, Telefonnummern oder Messenger-Kennungen von Anwälten gezielt zur Filterung ihrer Kommunikation eingesetzt werden. § 34 Abs. 2 BNDG-E ermöglicht dies unter bestimmten Voraussetzungen auch bei qualifiziertem Inlandsbezug. Die bisherige konkrete Schutzschranke wird weitgehend durch eine allgemeine Verhältnismäßigkeitsprüfung ersetzt. Dies schwächt nach Auffassung des Deutschen Anwaltvereins den Schutz des Berufsgeheimnisses und der anwaltlichen Vertraulichkeit erheblich.

d. Entgrenzung der Erkenntniszwecke - § 5 Abs. 1 S. 2 G10 / §§ 32 Abs. 1, 33 Abs. 1 BNDG-E

Schließlich entfällt die abschließende Zweckbestimmung des § 5 Abs. 1 S. 2 G10. Nach §§ 32 Abs. 1 und 33 Abs. 1 BNDG-E soll künftig grundsätzlich genügen, dass die Maßnahme für die „nachrichtendienstliche Auslandsaufklärung“ erforderlich ist. Dadurch können auch Kommunikationsvorgänge von Anwälten erfasst werden, wenn sie thematisch in Bereiche der Auslandsaufklärung fallen. Die weite Zweckbestimmung vergrößert damit den Entscheidungsspielraum des BND und schwächt die gesetzliche Vorababgrenzung der Überwachung. In Verbindung mit den Änderungen der §§ 22, 33 und 66 BNDG-E steigt damit insbesondere das Risiko für die vertrauliche Kommunikation zwischen Anwalt und Mandant.

4. § 7 Befugnis zur Datenerhebung unter Mitwirkung anderer Stellen

a. Regelungsgehalt

Nach § 7 BNDG-E soll der BND „andere Stellen“ um Übermittlung von Informationen einschließlich personenbezogener Daten ersuchen, „soweit dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist“. Mit „anderen Stellen“ sind sowohl Behörden („öffentliche Stellen“) als auch Unternehmen und andere privatrechtliche Organisationen („nichtöffentliche Stellen“) gemeint. Betroffene Personen werden von der Übermittlung von Daten und Informationen nie erfahren, da es „inländischen Stellen“ durch § 8 Abs. 1 Nr. 1 BNDG-E verboten werden soll, Betroffene zu informieren - dies sogar dann, wenn gesetzliche Meldepflichten bestehen.

b. Kritik

Dies geht viel zu weit und würde dem BND die heimliche Sammlung von Informationen über Bürgerinnen und Bürger immer dann ermöglichen, wenn der BND der Auffassung ist, die Informationen seien zur Erfüllung seiner Aufgaben „erforderlich“. Eine Kontrolle gleich welcher Art ist nicht vorgesehen – auch nicht durch den Unabhängigen Kontrollrat. Die bislang für Übermittlungsersuchen an Behörden vorgeschriebene Dokumentation (vgl. § 18 Abs. 5 BVerfSchG) soll abgeschafft werden, dies bezeichnet die Gesetzesbegründung auf Seite 441 als „Bürokratieentlastung“.

Falsch ist es, wenn es in der Gesetzesbegründung weiter heißt, „eine generelle Dokumentationspflicht“ sei laut BVerfG vom 27.5.2020, 1 BvR 1873/13, Rn. 218 (gemeint ist wohl Rn. 248 ff.) „nicht erforderlich“. In Rn. 250 heißt es in dieser Entscheidung:

„Dagegen kann die Zuordnung dynamischer IP-Adressen angesichts ihres erhöhten Eingriffsgewichts nur dann als verhältnismäßig angesehen werden, wenn die Entscheidungsgrundlagen für die Durchführung einer solchen Maßnahme nachvollziehbar und überprüfbar dokumentiert werden. Die rechtlichen und tatsächlichen Grundlagen entsprechender

Auskunftsbegehren sind aktenkundig zu machen (BVerfGE 125, 260 <344>). Zum einen rationalisiert und mäßigt es die Entscheidung, wenn die entscheidende Behörde sich selbst über ihre Entscheidungsgrundlagen Rechenschaft ablegen muss. Zum anderen ermöglicht erst die Dokumentation eine aufsichtliche Kontrolle durch die Datenschutzbeauftragten. Schließlich wird durch die Dokumentation die verwaltungsgerichtliche Kontrolle erleichtert (vgl. BVerfGE 150, 244 <303 Rn. 157>). Für den Abruf von Zugangsdaten bedarf es demgegenüber keiner Regelung genereller Dokumentationspflichten. Soweit sie aufgrund des Eingriffsgewichts im Einzelfall geboten sein sollten, ergeben sich entsprechende Anforderungen regelmäßig aus den jeweiligen Ermächtigungsgrundlagen zur Nutzung der Daten.“

Dokumentationspflichten rationalisieren und mäßigen nach Auffassung des BVerfG Überwachungsentscheidungen und ermöglichen überhaupt erst die (nachträgliche) Kontrolle heimlicher Maßnahmen. Die Streichung jeglicher Dokumentationspflichten, die geplant ist, ist mit den Maßgaben des BVerfG somit unvereinbar.

5. § 8 i. V. m. §§ 134, 136, 137 BNDG-E — Strafbewehrtes Mitteilungsverbot ohne Ausnahme für Rechtsrat

a. Regelungsgehalt

§ 8 Abs. 1 Nr. 1 untersagt der ersuchten Stelle und ihren Beschäftigten, „der betroffenen Person oder Dritten“ Informationen über das Ersuchen oder dessen Durchführung mitzuteilen.

Der Verstoß ist nach § 136 mit Freiheitsstrafe bis zu zwei Jahren, im Qualifikationsfall mit drei Monaten bis fünf Jahren bedroht; § 137 sieht Geldbußen bis 500.000 €, § 134 Abs. 2 die Untersagung des Geschäftsbetriebs vor. Der Adressatenkreis reicht von Telekommunikations- und Digitaldiensteanbietern über sämtliche Verpflichtete nach § 2 Abs. 1 GwG bis zu Kraftfahrzeugherstellern und -werkstätten (§ 12 Abs. 2).

b. Kritik

aa) Konsultation eines Rechtsanwalts

Das Verbot erfasst nach seinem Wortlaut die Konsultation eines Rechtsanwalts. „Dritter“ ist jeder außer dem Bundesnachrichtendienst. Eine Ausnahme für Rechtsrat oder Rechtsschutz fehlt. Das ist kein Redaktionsversehen: Denn § 47 Abs. 2 GwG kennt eine solche Ausnahme ausdrücklich. Zugleich muss der Verpflichtete die Reichweite des Ersuchens selbst beurteilen - § 137 Abs. 1 Nr. 1 sanktioniert die Zuwiderhandlung gegen ein „vollziehbares“ Ersuchen. Er soll also rechtlich bewerten, sich aber nicht beraten lassen dürfen.

bb) Bestimmtheit

Art. 103 Abs. 2 GG. § 136 ist ein Blankett, das seinen Unrechtsgehalt vollständig aus § 8 Abs. 1 Nr. 1 bezieht. Ob „Dritte“ auch den Abschlussprüfer (§ 320 HGB), den Aufsichtsrat (§ 90 AktG), die Konzernmutter, den Betriebsrat oder Beschäftigte außerhalb des nach § 13 Abs. 6 ausgewählten Kreises erfasst, bleibt offen. In sämtlichen Konstellationen kollidiert das Verbot mit gesetzlichen Auskunft- oder Berichtspflichten. Die Begründung löst den Konflikt nur für die geldwäscherechtliche Verdachtsmeldung (§ 43 GwG) - und zwar zulasten der Meldepflicht.

cc) Zusammenspiel mit § 103

Für Ersuchen nach § 13 Abs. 1 Satz 2 ist der Rechtsweg gegen „die Anordnung und den Vollzug“ bis zur Mitteilung an die betroffene Person ausgeschlossen. Die Norm unterscheidet nicht nach dem Rechtsschutzsuchenden. Erfasst der Ausschluss auch den Verpflichteten selbst, kann dieser das an ihn gerichtete Ersuchen weder gerichtlich überprüfen lassen noch sich darüber beraten lassen, haftet aber mit Geldbuße bis 300.000 € und im Wiederholungsfall mit der Untersagung seines Geschäftsbetriebs.

dd) Verweisungsfehler in der Bußgeldnorm

§ 137 Abs. 1 Nr. 1 verweist auf „§ 15 Satz 1“, obwohl § 15 in Absätze gegliedert ist; Nr. 5 und 6 verweisen auf § 136 (Strafvorschrift) statt auf § 135 (Anzeige- und Genehmigungspflichten). Über § 3 OWiG gilt auch für Bußgeldtatbestände, dass der Normadressat der Regelung selbst entnehmen können muss, welches Verhalten sanktioniert ist.

c. Fazit

Das strafbewehrte Mitteilungsverbot verletzt in seiner jetzigen Fassung Art. 12 Abs. 1 GG: Auskunfts-, Mitwirkungs- und Schweigepflichten sind Berufsausübungsregelungen, und die Untersagung des Geschäftsbetriebs nach § 134 Abs. 2 erreicht berufswahlnahe Intensität, ohne dass der Verpflichtete die Reichweite seiner Pflichten rechtssicher ermitteln könnte. Weil das Verbot die Weitergabe wahrer Tatsachen untersagt und auch Transparenzberichte erfasst, liegt zugleich ein Eingriff in Art. 5 Abs. 1 Satz 1 GG vor. Der Ausschluss anwaltlicher Beratung verletzt das aus Art. 2 Abs. 1 i. V. m. Art. 20 Abs. 3 GG folgende Recht, in eigener Sache Rechtsrat einzuholen; erfasst § 103 auch Rechtsbehelfe des Verpflichteten, tritt eine Verletzung von Art. 19 Abs. 4 GG hinzu, denn die Ausnahme des Art. 10 Abs. 2 Satz 2 GG greift für ihn nicht — er ist nicht in seinem Fernmeldegeheimnis, sondern in seiner Berufsfreiheit betroffen. Die Unbestimmtheit des Begriffs „Dritte“ und die fehlerhaften Verweisungen in § 137 Abs. 1 verletzen Art. 103 Abs. 2 GG, der über § 3 OWiG auch für den Bußgeldtatbestand gilt.

d. Forderungen

- Ausdrückliche Ausnahme für die Mitteilung an Rechtsanwälte zum Zweck der Beratung über das Ersuchen und für die Wahrnehmung von Rechtsschutz, verbunden mit der Erstreckung des Verbots auf die beratende Person.
- Enumerative Bestimmung des Adressatenkreises statt des offenen Begriffs „Dritte“; ausdrückliche Regelung des Verhältnisses zu §§ 90 AktG, 320 HGB, §

43 GwG und zu Unterrichtungspflichten gegenüber Betriebsräten, jeweils mit Freistellung von der Verantwortlichkeit nach §§ 130, 30 OWiG.

- Klarstellung in § 103, dass der Rechtswegausschluss Rechtsbehelfe der verpflichteten Stelle nicht erfasst.

6. §§ 100–103 BNDG-E — Mitteilung, Auskunft und Rechtsweg

a. Regelungsgehalt

§ 100 Abs. 1 und 2 begründen Mitteilungspflichten für eingriffsintensive Maßnahmen; Abs. 3 beschränkt sie auf deutsche Staatsangehörige, inländische juristische Personen und nicht nur vorübergehend im Bundesgebiet aufhältige Personen sowie auf Personen, gegen die die Maßnahme gerichtet war; Abs. 4 nimmt sechs Fallgruppen aus. § 102 gewährt einen Auskunftsanspruch unter engen Voraussetzungen. § 103 schließt den Rechtsweg vor der Mitteilung aus gegen Auskunftersuchen nach § 13 Abs. 1 Satz 2, gegen die strategische Aufklärung nach § 32 und gegen die Telekommunikationsüberwachung nach § 35.

b. Kritik

aa) Anknüpfung an die Staatsangehörigkeit (§ 100 Abs. 3 Satz 1)

Die Anknüpfung an die Staatsangehörigkeit (§ 100 Abs. 3 Satz 1) ist verfassungswidrig. Die Begründung nimmt „Ausländer im Ausland“ ausdrücklich von der Mitteilungspflicht aus und begründet dies mit dem Schutz der Betroffenen vor Repressionen ihres Heimatstaats. Das Argument ist überschießend: Für diesen Fall greift bereits § 100 Abs. 4 Nr. 5 - und zwar mit Zustimmung des Kontrollrats. Der Entwurf ersetzt eine kontrollierte Einzelfallprüfung durch eine pauschale Statusregel. Sachwidrig ist die Anknüpfung zudem deshalb, weil für Ausländer im Ausland durchgehend die niedrigste Eingriffsschwelle gilt (§§ 24 Abs. 1, 26 Abs. 1, 35 Abs. 1, 37 Abs. 1); die Gruppe mit dem geringsten materiellen Schutz erhält damit auch keinen prozeduralen. Die deutsche Staatsgewalt ist bei der Auslandsaufklärung nach Art. 1 Abs. 3 GG an die

Grundrechte gebunden.¹³ Die Rechtsschutzgarantie des Art. 19 Abs. 4 GG knüpft zudem nicht an die Staatsangehörigkeit an.

bb) Ausschluss Drittbetroffener (§ 100 Abs. 3 Satz 2)

Betroffener im Sinne des Art. 19 Abs. 4 GG ist, wer durch die Maßnahme in seinen Grundrechten berührt wird - bei einer Wohnraumüberwachung also auch der Gesprächspartner. Das Bundesverfassungsgericht hat Benachrichtigungspflichten auch gegenüber identifizierbaren Drittbetroffenen gefordert.¹⁴ Verschärfend erlauben § 46 Abs. 5 und § 48 Abs. 4 die Erstreckung einer Maßnahme auf nicht in der Anordnung genannte Personen; diese sind Zielpersonen, fallen aber möglicherweise aus der Mitteilungspflicht heraus.

cc) Mitteilungspflicht

§ 100 Abs. 4 Nr. 1 hebt die Mitteilungspflicht praktisch auf. Die Ausnahme greift, wenn eine Steuerung durch eine fremde Macht „nicht vollständig ausgeschlossen werden kann“. Tatbestandsvoraussetzung ist damit nicht die Feststellung eines Sachverhalts, sondern die Unmöglichkeit seiner Widerlegung - bei einem Auslandsnachrichtendienst, dessen Auftrag sich weitgehend auf staatlich gesteuerte Bedrohungen richtet, ein praktisch nie zu führender Negativbeweis. Entscheidend ist die Verfahrensfolge: § 100 Abs. 4 Satz 2 verlangt die Zustimmung des Kontrollrats nur für Nr. 4 und 5. Über die praktisch bedeutsamste Ausnahme entscheidet der Dienst allein. Gleiches gilt für Nr. 2 (Einsatz einer nachrichtendienstlichen Verbindung): Das Quellenschutzinteresse ist legitim, rechtfertigt aber keine kategorische Ausnahme ohne unabhängige Prüfung, ob eine Mitteilung ohne Offenlegung der Durchführungsart möglich wäre.

dd) Auskunftsanspruch

§ 102 knüpft den Auskunftsanspruch an eine Kenntnis, die er erst verschaffen soll. Verlangt werden die Benennung eines konkreten Sachverhalts und die Darlegung eines besonderen Interesses; wer von einer heimlichen Maßnahme nichts weiß, kann beides

¹³ BVerfGE 154, 152.

¹⁴ BVerfGE 109, 279; 141, 220.

nicht leisten. Hinzu kommen der Ausschluss der Auskunft über Herkunft und Empfänger (Abs. 2 Nr. 1), der vollständige Ausschluss der Akteneinsicht (Abs. 6) und der Verzicht auf jede Begründung (Abs. 5 Satz 1). Der Verweis auf den Kontrollrat ist kein Rechtsschutz im Sinne des Art. 19 Abs. 4 GG: Denn der Betroffene ist am Verfahren nicht beteiligt, der Kontrollrat entscheidet nicht über seine Rechte, und die Mitteilungen dürfen keine Rückschlüsse zulassen.

ee) Rechtswegausschluss

§ 103 überschreitet die Ermächtigung des Art. 10 Abs. 2 Satz 2 GG. Die Begründung beschränkt sich auf den Hinweis, die Regelung übernehme den bisherigen § 13 G10. Das trifft in zweifacher Hinsicht nicht zu:

Zum einen erfasst § 103 Nr. 1 Auskunftersuchen über Daten, die nicht durchweg dem Fernmeldegeheimnis unterfallen. Insoweit ist Art. 10 Abs. 2 Satz 2 GG von vornherein nicht einschlägig.

Zum anderen erlaubt die Verfassungsnorm den Rechtswegausschluss nur, soweit die Beschränkung dem Schutz der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes dient. Die strategische Aufklärung nach § 32 dient demgegenüber dem gesamten Zweckspektrum des § 2 — einschließlich der außenpolitischen Handlungsfähigkeit, der Wirtschaft und Wissenschaft, der Rohstoffversorgung und „krisenhafter Entwicklungen im Ausland“. Ein Ausschluss, der an die Maßnahmenart statt an den verfassungsrechtlich zugelassenen Zweck anknüpft, ist von der Ermächtigung nicht gedeckt. Das bisherige Recht war insoweit präziser, weil das Artikel 10-Gesetz die zulässigen Beschränkungszwecke selbst festlegte; mit dessen Aufhebung (Artikel 20 Nr. 3) verändert die scheinbare Übernahme den Regelungsgehalt substantiell.

ff) Gesamtwirkung

Wer keine Mitteilung erhält, erhält auch auf Antrag keine Auskunft, keine Angabe zu Herkunft und Empfängern, keine Akteneinsicht und keine Begründung. Somit ist für die

drei praktisch wichtigsten Maßnahmenarten der Rechtsweg verschlossen. Der Rechtsschutz ist damit nicht zeitlich verschoben, sondern für den Regelfall aufgehoben.

c. Fazit

Die gerügten Punkte verletzen in ihrer Zusammenschau Art. 19 Abs. 4 GG. Die Benachrichtigung ist bei heimlichen Maßnahmen nicht datenschutzrechtliches Beiwerk, sondern die Bedingung, unter der die Rechtsschutzgarantie überhaupt wirksam werden kann¹⁵; entfällt sie in den praktisch wichtigsten Fällen und ist der Rechtsweg zusätzlich versperrt, ist der Rechtsschutz nicht verzögert, sondern beseitigt.

Die Anknüpfung an die Staatsangehörigkeit verletzt Art. 3 Abs. 1 GG, weil sie nach einem für das Schutzbedürfnis unerheblichen Merkmal differenziert, und erkennt die aus Art. 1 Abs. 3 GG folgende Grundrechtsbindung bei der Auslandsaufklärung.¹⁶ Die Ausgestaltung des Auskunftsanspruchs verletzt das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG), weil sie Voraussetzungen aufstellt, deren Erfüllung die Kenntnis dessen verlangt, was der Anspruch erst verschaffen soll. Der Rechtswegausschluss des § 103 überschreitet die Ermächtigung des Art. 10 Abs. 2 Satz 2 GG, soweit er an die Maßnahmenart statt an den dort abschließend benannten Zweck anknüpft und Daten außerhalb des Fernmeldegeheimnisses erfasst. Fließen nachrichtendienstliche Erkenntnisse über § 83 in Verwaltungsverfahren ein, ohne dass Herkunft und Entstehungszusammenhang offengelegt werden, ist zusätzlich Art. 103 Abs. 1 GG betroffen.

d. Forderungen

- Streichung von § 100 Abs. 3 Satz 1; Schutzinteressen der Betroffenen sind über § 100 Abs. 4 Nr. 5 mit Zustimmung des Kontrollrats zu wahren.
- Mitteilungspflicht auch gegenüber erheblich betroffenen, ohne unverhältnismäßigen Aufwand identifizierbaren Dritten, jedenfalls gegenüber

¹⁵ BVerfGE 100, 313; 141, 220.

¹⁶ BVerfGE 154, 152.

Personen, auf die die Maßnahme nach § 46 Abs. 5 oder § 48 Abs. 4 erstreckt wurde.

- Streichung von § 100 Abs. 4 Nr. 1, hilfsweise Anknüpfung an Tatsachen, die die Annahme einer Tätigkeit für eine mit nachrichtendienstlichen Aufgaben betraute Stelle einer fremden Macht rechtfertigen.
- Zustimmung des Unabhängigen Kontrollrats für jede Nichtmitteilung.
- Streichung des Erfordernisses eines „besonderen Interesses“ in § 102 Abs. 1.
- Beschränkung des Rechtswegausschlusses in § 103 auf Maßnahmen, die tatsächlich dem Schutz der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherheit des Bundes oder eines Landes dienen.
- Als Ausgleich für die Verkürzung des Individualrechtsschutzes: Einführung eines Verfahrens vor dem Bundesverwaltungsgericht, in dem die Interessen des nicht benachrichtigten Betroffenen durch einen sicherheitsüberprüften anwaltlichen Sonderbevollmächtigten wahrgenommen werden.

7. § 81 i. V. m. Anlage 2 BNDG-E — Übermittlung zur Strafverfolgung

a. Regelungsgehalt

§ 81 Abs. 1 erlaubt die Übermittlung an Strafverfolgungsbehörden bei Verdacht einer „besonders schweren Straftat“. Abs. 2 definiert diese als Straftaten mit einer Höchststrafe von mehr als fünf Jahren (Nr. 1) sowie als die in der Anlage aufgeführten Delikte (Nr. 2). § 77 begrenzt für Daten aus bestimmten Erhebungsarten die Übermittlung zusätzlich auf den Katalog des § 100b Abs. 2 StPO.

b. Kritik

aa) Äußerungsdelikte als „besonders schwere Straftaten“

Anlage 2 enthält unter anderem die Verunglimpfung des Bundespräsidenten (§ 90 Abs. 1 und 3 StGB), die Verunglimpfung des Staates und seiner Symbole (§ 90a Abs. 3 StGB), die verfassungsfeindliche Verunglimpfung von Verfassungsorganen (§ 90b Abs. 1 StGB) und die Störpropaganda gegen die Bundeswehr (§ 109d Abs. 1 StGB).

Sämtliche dieser Tatbestände sind mit einer Höchststrafe von fünf Jahren bedroht und würden die Schwelle des § 81 Abs. 2 Nr. 1 gerade nicht erreichen; die Anlage dient also dazu, Delikte einzubeziehen, die die selbst gesetzte Schwereschwelle verfehlen. Die Begründung leitet die „besondere Schwere“ allein aus der Abstraktion des Schutzguts ab - ein Maßstab, der jedes Staatsschutzdelikt erfasste.

Zum Vergleich: Keines dieser Delikte ist im Katalog des § 100b Abs. 2 StPO enthalten. Der Entwurf erlaubt damit die Übermittlung von Erkenntnissen zur Verfolgung von Taten, für die dieselben Erkenntnisse strafprozessual nicht hätten erhoben werden dürfen — der Kernfall dessen, was der Grundsatz der hypothetischen Datenneuerhebung¹⁷ ausschließen soll.

bb) Lückenhafte Regelung in § 77

Die Lücken des § 77 verschärfen den Befund. Die Begrenzung auf § 100b Abs. 2 StPO gilt nur für Daten aus § 29 Abs. 2, § 113 Abs. 2 und § 37 Abs. 3. Nicht erfasst sind insbesondere § 29 Abs. 1 (Wohnraumüberwachung im Ausland gegenüber Nichtdeutschen), § 37 Abs. 1 und 2 (Zugriff auf komplexe informationstechnische Systeme, auch privat genutzte), § 38, § 35 sowie §§ 32 und 33. Für diese Erhebungsarten gilt allein § 81 Abs. 2 samt Anlage 2. Konkret bedeutet das: Erkenntnisse aus einer Wohnraumüberwachung im Ausland oder aus einer Online-Durchsuchung dürfen zur Verfolgung einer Verunglimpfung des Bundespräsidenten übermittelt werden. Das ist mit der Rechtsprechung des BVerfG¹⁸ nicht vereinbar und überschreitet für die Wohnraumüberwachung zugleich die Schranke des Art. 13 Abs. 3 GG.

cc) Verknüpfung von Desinformationsabwehr und Äußerungsstrafrecht

Die Begründung nennt für § 90 und § 90a Abs. 3 StGB ausdrücklich „Desinformation (Bsp.: Fake-News)“ und „hybride Maßnahmen Dritter“ als Anwendungsfall — ein Bedrohungsfeld, das § 3 Abs. 4 Nr. 2 als Aufklärungsgegenstand benennt. Damit wird die Abwehr staatlich gesteuerter Einflussnahme in das Individualstrafrecht verschoben,

¹⁷ BVerfGE 141, 220; 154, 152; 163, 43.

¹⁸ BVerfGE 109, 279 und BVerfGE 120, 274.

und zwar mit Tatbeständen, die auf Meinungsäußerungen zugreifen und deren verfassungskonforme Anwendung ohnehin engster Grenzen bedarf. Hier bedürfte es wohl zunächst der Schaffung von entsprechenden Straftatbeständen, die ein staatlich gesteuerte Einflussnahme auf Meinungsbildung durch Desinformation zum Gegenstand haben und entsprechende Sanktionen vorsehen.

dd) Verdeckte Herkunft

Nach § 29 Abs. 7 Satz 2 kann die Behördenleitung anordnen, dass bei der Übermittlung auf die Kennzeichnung verzichtet wird. Die Herkunft aus einer Wohnraumüberwachung kann damit gegenüber der empfangenden Stelle verschleiert werden. Das hat unmittelbare Folgen für die Prüfung von Verwertungsverböten im Strafverfahren.

ee) Verweisungsfehler

§ 81 Abs. 2 Nr. 2 verweist auf „Anlage 1“; ausweislich der Anlagenüberschrift ist Anlage 2 gemeint (Anlage 1 gehört zu § 48 Abs. 2 Nr. 2 BVerfSchG).

c. Fazit

Die Zweckänderung ist ein eigenständiger Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG); ihr Gewicht bemisst sich nach dem Grundrecht, in das die Erhebung eingegriffen hat. Weil § 77 die Begrenzung auf § 100b Abs. 2 StPO nur lückenhaft anordnet, wirken bei der Übermittlung Art. 13 Abs. 1 GG (Daten aus § 29 Abs. 1), das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme (Daten aus §§ 37, 38) und Art. 10 Abs. 1 GG (Daten aus §§ 32, 33, 35) fort - und werden durch einen Katalog entwertet, der Delikte mit fünfjähriger Höchststrafe einbezieht. Für Erkenntnisse aus der Wohnraumüberwachung liegt darin zugleich eine Überschreitung des Art. 13 Abs. 3 GG, der die akustische Wohnraumüberwachung von Verfassungswegen auf besonders schwere Straftaten begrenzt; das ist ein unmittelbarer Verfassungsverstoß und nicht erst eine Frage der hypothetischen Datenneuerhebung. Die Aufnahme der Äußerungsdelikte verletzt Art. 5 Abs. 1 Satz 1 GG, weil die Aussicht, wegen einer Meinungsäußerung auf Grundlage

nachrichtendienstlicher Überwachung verfolgt zu werden, weit über den Einzelfall hinaus abschreckend wirkt und die verfassungskonform enge Auslegung des § 90a StGB auf Übermittlungsebene nicht abgebildet wird. Der Kennzeichnungsverzicht nach § 29 Abs. 7 Satz 2 verletzt schließlich das Recht auf ein faires Verfahren (Art. 2 Abs. 1 i. V. m. Art. 20 Abs. 3 GG), weil die Verteidigung ohne Kenntnis von Erhebungsart und Rechtsgrundlage die Verwertbarkeit nicht prüfen kann.

d. Forderungen

- Streichung der Nummern 8, 9, 10, 21, 24 und 25 der Anlage 2 (Äußerungsdelikte).
- Ausweitung des § 77 auf sämtliche Erhebungsarten mit gesteigertem Eingriffsgewicht, insbesondere § 29 Abs. 1, § 37 Abs. 1 und 2, § 38 sowie § 35.
- Streichung der Kennzeichnungsausnahme des § 29 Abs. 7 Satz 2 für Übermittlungen an Strafverfolgungsbehörden.
- Pflicht zur Mitteilung von Erhebungsart und Rechtsgrundlage bei der Übermittlung nach § 81 sowie zur Unterrichtung der Verteidigung; ohne diese Angaben ist die Verwertbarkeit im Strafverfahren nicht prüfbar.
- Korrektur des Verweises in § 81 Abs. 2 Nr. 2.

V. BVerfSchG

Der Deutsche Anwaltverein sieht es mit Besorgnis, wie weitreichend die Befugnisse des Bundesamts für Verfassungsschutz ausgebaut werden sollen.

Der Aufrüstung des Inlandsnachrichtendienstes steht keine Ertüchtigung der Rechtsschutzmöglichkeiten gegenüber. Wo kein Individualrechtsschutz verwirklicht werden kann, fehlt es auch an der gerichtlichen Kontrolle. Es liegt auf der Hand, dass dem herkömmlichen Rechtsweg im Nachrichtendienstrecht wegen der Geheimhaltungsbedürftigkeit Grenzen gesetzt sind. Es wäre aber Aufgabe des Gesetzgebers, möglichst äquivalente Mechanismen zu etablieren, um eine rechtsstaatliche Kontrolle trotzdem zu gewährleisten. Dies lässt der Entwurf nicht im Ansatz erkennen.

1. Aufgaben der Verfassungsschutzämter

Die Aufgabenzuweisung, die bisher im § 3 des BVerfSchG geregelt ist, soll in § 2 des Entwurfs grundlegend neu geregelt werden. Während es bisher heißt, dass „die Sammlung und Auswertung von Informationen“ Aufgabe des BfV und der Landesämter ist, heißt es nun in § 2 Abs. 1 des Entwurfs, es sei ihre Aufgabe, bestimmten „Bestrebungen und Tätigkeiten entgegenzuwirken“. Dies tun sie nach der Vorstellung des Entwurfs, indem sie „über die Bestrebungen und Tätigkeiten informieren“ und „diese dazu bereits frühzeitig aufklären“ (§ 2 Abs. 2 d. Entwurfs). Darin liegt eine proaktivere Rolle der Verfassungsschutzämter. Wird der Entwurf Gesetz, stellen die Verfassungsschutzämter nicht mehr „nur“ Informationen zusammen, die andere Behörden unter bestimmten Voraussetzungen abrufen können, sondern sollen selbst Bestrebungen entgegenwirken, indem sie proaktiv informieren.

Es liegt auf der Hand, dass ein solcher Wandel einhergehen müsste mit einer spiegelbildlichen Stärkung der Betroffenenrechte. Andernfalls gerät das Gleichgewicht zwischen Eingriffsbefugnissen und Grundrechtsschutz aus den Fugen.

2. Legaldefinitionen / Eingriffsschwellen

a. Freiheitlich demokratische Grundordnung

In § 3 Abs. 3 des Entwurfs findet sich eine Definition der freiheitlich demokratischen Grundordnung, welche die neuere Rechtsprechung des Bundesverfassungsgerichts¹⁹ aufgreift. Die Umsetzung ist allerdings ungenau und sollte korrigiert werden. Laut § 3 Abs. 3 Nr. 3 c) des Entwurfs ist „das Gewaltmonopol des Staates“ Bestandteil der freiheitlich demokratischen Grundordnung. Das Bundesverfassungsgericht hat dies aber differenzierter formuliert. In der genannten Leitentscheidung heißt es in Rn. 547:

¹⁹ Urteil vom 17.01.2017, Az. 2 BvB 1/13, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2017/01/bs20170117_2bvb000113.html.

„Zugleich erfordert der Schutz der Freiheit des Einzelnen, dass die Anwendung physischer Gewalt den gebundenen und gerichtlicher Kontrolle unterliegenden staatlichen Organen vorbehalten ist. Das Gewaltmonopol des Staates [...] ist deshalb ebenfalls als Teil der freiheitlichen demokratischen Grundordnung im Sinne des Art. 21 Abs. 2 Satz 1 GG anzusehen.“

Das Bundesverfassungsgericht stellt damit klar, dass nicht jede Staatsgewalt für sich ein Monopol reklamieren kann, sondern sich die Legitimität des Gewaltmonopols erst aus der rechtsstaatlichen Einhegung der staatlichen Gewalt ergibt. § 3 Abs. 3 Nr. 3 c) sollte daher wie folgt gefasst werden:

dass die Anwendung physischer Gewalt den gebundenen und gerichtlicher Kontrolle unterliegenden staatlichen Organen vorbehalten ist (staatliches Gewaltmonopol).

b. Erhebliche Beobachtungsbedürftigkeit und Gewaltbegriff

§ 3 Abs. 7 des Entwurfs lautet,

Erheblich beobachtungsbedürftig sind Bedrohungen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass sie geeignet sind, die in § 2 Absatz 1 genannten Schutzgüter erheblich zu beeinträchtigen. Die Eignung ist anzunehmen, wenn zur Zielverfolgung Straftaten begangen werden.

Diese Formulierung geht zu weit. Indem eine Eignung zur erheblichen Beeinträchtigung u. a. der freiheitlich demokratischen Grundordnung mit der Begehung von Straftaten identifiziert wird, ohne dies auf Straftaten einer bestimmten Schwere zu begrenzen, wird die konkrete Gefahr geschaffen, dass auch gesellschaftskritische Akteure, die etwa Plakate im öffentlichen Raum anbringen (in bestimmten Konstellationen eine strafbare Sachbeschädigung), einer nachrichtendienstlichen Beobachtung unterworfen und beispielsweise zur verdeckten polizeilichen Kontrolle ausgeschrieben werden, § 10 Abs. 3 BVerfSchG-E. Auch die heimliche Ausleitung von Verkehrs- und Inhaltsdaten aus digitalen Diensten und den Verkehrsdaten von Kommunikationsdiensten für einen Zeitraum von bis zu einem Jahr sowie die heimliche Überwachung durch eine V-Person

soll schon beim Vorliegen einer “erheblichen Beobachtungsbedürftigkeit” möglich sein, vgl. §§ 11, 13, 18 des Entwurfs.

Auch die in Abs. 7 S. 2 Nr. 1 a) verwendete Formulierung

Die Eignung kann anzunehmen sein nach Maßgabe

1. der Vorgehensweise bei der Zielverfolgung, nämlich

a) gewaltorientiert, indem Gewalt angewendet wird oder dazu Bereitschaft besteht oder Gewalt unterstützt oder befürwortet wird [...]

ist zu weitgehend. Der Gewaltbegriff wurde in der strafrechtlichen Rechtsprechung vom Alltagssprachgebrauch abgekoppelt. Entsteht infolge einer Sitzblockade ein Stau aus Fahrzeugen, so wird in der Verursachung dieser physischen Barriere Gewalt im Sinne des § 240 StGB gesehen.²⁰ Stemmt sich jemand im Rahmen seiner Festnahme mit den Füßen gegen den Boden oder klebt sich jemand mit Sekundenkleber an den Asphalt einer Straße, so erkennen darin manche Strafgerichte bereits Gewalt im Sinne des § 113 StGB.²¹ Der Entwurf täte daher gut daran, klarzustellen, dass hier nur Gewalt jenseits der Bagatellgrenze gemeint ist, etwa „Gewalt, die geeignet ist, Personen erheblich zu verletzen“.

Außerdem sollte der Entwurfstext wie folgt ergänzt werden (Einschübe unterstrichen):

1. der Vorgehensweise bei der Zielverfolgung, nämlich

a) gewaltorientiert, indem Gewalt angewendet wird oder dazu Bereitschaft besteht oder Gewalt aktiv unterstützt oder aktiv befürwortet wird [...]

Durch das Erfordernis einer *aktiven* Unterstützung bzw. Befürwortung würde klargestellt, dass eine indifferente Haltung nicht ausreicht. Es mag zwar sprachlich eindeutig sein, dass eine fehlende Distanzierung nicht mit der Unterstützung oder Befürwortung gleichgesetzt werden kann. Die Praxis zeigt aber, dass es hier immer wieder Anwendungsunsicherheiten gibt.

²⁰ BGH, Urt. v. 20.07.1995 - 1 StR 126/95.

²¹ KG, Beschl. v. 10.07.2024, NStZ 2025, 361.

c. Besonders erhebliche Beobachtungsbedürftigkeit

In Abs. 8 des Entwurfs heißt es

Besonders erheblich beobachtungsbedürftig sind Bedrohungen, wenn tatsächliche Anhaltspunkte vorliegen für

1. verfassungsfeindliche Bestrebungen, die

a) zur Zielverfolgung Straftaten begehen, die im Höchstmaß mit Freiheitsstrafe von mindestens 5 Jahren bedroht sind,

Auch diese Eingriffsschwelle ist zu niedrig. Die besonders erheblich beobachtungsbedürftige Bedrohung ist Voraussetzung für weitreichende Grundrechtseingriffe wie die Überwachung von Kommunikationsinhaltsdaten, vgl. § 13 Abs. 4 des Entwurfs. Straftaten, die im Höchstmaß mit Freiheitsstrafen von mindestens 5 Jahren bestraft werden, sind etwa auch einfache Körperverletzungsdelikte gem. § 223 StGB oder Diebstahlsdelikte gem. § 242 StGB. Dem Gesetzgeber wird empfohlen, hier auf den Katalog des § 100a StPO Bezug zu nehmen oder die Schwelle durch eine abstrakt generelle Formulierung zu erhöhen.

3. Datenübermittlungsbefugnisse

a. Maßstab des BVerfG an die Verwendung nachrichtendienstlich erhobener Daten

Das BVerfG unterscheidet im Ausgangspunkt – so weit so bekannt – zwischen zweckentsprechender und zweckändernder Verarbeitung.²²

- Nach dem BVerfG können (Weiter-)Verarbeitungshandlungen auf die Erhebungsgrundlage gestützt werden, wenn die erhebende Behörde die Daten „im Rahmen des konkreten Anlasses des Erhebungseingriffs“ verarbeitet.²³

²² BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 101 ff. – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 225 ff. – Bayerisches VerfassungsschutzG.

²³ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 102 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 226 – Bayerisches VerfassungsschutzG.

- Dagegen bedarf es einer eigenständigen Rechtsgrundlage, wenn die erhebende Behörde selbst die Daten „zu anderen Zwecken als denen der ursprünglichen Datenerhebung“ nutzt.²⁴ Dabei sei die „Übermittlung von Daten an eine andere Behörde (...) ein Unterfall der zweckändernden Nutzung, weil eine weitere Nutzung nur dann innerhalb der ursprünglichen Zwecksetzung bleiben kann, wenn sie seitens derselben Behörde erfolgt“.²⁵
- Darüber hinaus bedarf es ebenfalls einer eigenständigen Rechtsgrundlage, wenn die Daten durch die erhebende Behörde „im Rahmen der ursprünglichen Zwecke“ aber „zu einem anderen konkreten Anlass“ verarbeitet.²⁶

aa) Reichweite des Erhebungszwecks

Daneben korrespondiert die Reichweite eines Erhebungszwecks mit der vorgelagerten Eingriffstiefe. Grundsätzlich soll es genügen, „dass die erhobenen Daten für ein neues Verfahren derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter einen hinreichenden Spurenansatz bieten“.²⁷ Bei Daten aus Wohnraumüberwachungen und Online-Durchsuchungen muss dagegen eine „den Erhebungsvoraussetzungen entsprechende[...] dringende[...] bzw. zumindest konkretisierte[...] Gefahr erforderlich“ sein.²⁸

bb) Anforderungen an zweckändernde Verarbeitungen

Bei einer zweckändernden Verarbeitung gilt der Grundsatz der hypothetischen Datenneuerhebung.²⁹ Der neue Nutzungszweck muss so gewichtig sein, dass er „eine

²⁴ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 102 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 226 – Bayerisches VerfassungsschutzG.

²⁵ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 102 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 226, 232 – Bayerisches VerfassungsschutzG.

²⁶ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 102 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 227 – Bayerisches VerfassungsschutzG.

²⁷ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 103 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 227 – Bayerisches VerfassungsschutzG.

²⁸ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 103 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 228 – Bayerisches VerfassungsschutzG.

²⁹ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 104 f. – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 229 – Bayerisches VerfassungsschutzG.

*Neuerhebung durch die empfangende Stelle mit vergleichbar schwerwiegenden Mitteln wie die vorangegangene nachrichtendienstliche Überwachung rechtfertigen könnte“.*³⁰

Dabei gilt: „*Verfügt die empfangende Behörde über operative Anschlussbefugnisse, sind an eine Datenneuerhebung – und entsprechend an eine Übermittlung – wegen unmittelbar möglicher Folgemaßnahmen grundsätzlich strengere Anforderungen zu stellen, als wenn die empfangende Behörde keine weiteren operativen Befugnisse hat*“.³¹

Bei nachrichtendienstlich erhobenen Informationen weicht das BVerfG von den ansonsten geltenden Grundsätzen der hypothetischen Datenneuerhebung ab und misst dem Eingriffsgewicht der jeweiligen Einzelmaßnahme keine Bedeutung zu.³²

cc) Spezifische Anforderungen an Übermittlungen

Das BVerfG unterscheidet nach den Aufgaben und den Befugnissen der empfangenden Behörden:

- **Gefahrenabwehrbehörden:** Sollen nachrichtendienstlich ersterhobene personenbezogene Daten/daraus abgeleitete Informationen an Gefahrenabwehrbehörden mit „*operativen Anschlussbefugnissen*“ übermittelt werden, bedarf es (1) ein „*besonders gewichtiges Rechtsgut*“ bzw. ein „*herausragendes öffentliches Interesse*“³³ und (2) eine „*wenigstens konkretisierte Gefahr*“.³⁴ Besonders gewichtige Rechtsgüter: „*Leib, Leben und Freiheit der Person*“, „*der Bestand oder die Sicherheit des Bundes oder eines Landes*“, „*Schutz von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist*“ (bspw. „*wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen*“).³⁵

³⁰ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 105 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 230 – Bayerisches VerfassungsschutzG.

³¹ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 106 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 234 – Bayerisches VerfassungsschutzG.

³² BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 108 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 238 – Bayerisches VerfassungsschutzG.

³³ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 108 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 235 – Bayerisches VerfassungsschutzG.

³⁴ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 107 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 235 – Bayerisches VerfassungsschutzG.

³⁵ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 108 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 243 – Bayerisches VerfassungsschutzG.

- **Strafverfolgungsbehörden:** Sollen nachrichtendienstlich ersterhobene personenbezogene Daten/daraus abgeleitete Informationen an Strafverfolgungsbehörden übermittelt werden, ist das Gewicht der Straftat entscheidend.³⁶ Vom Verfassungsschutz ersterhobene Daten dürfen nur zum Schutz eines „*herausragenden öffentlichen Interesses*“ (d.h. „besonders schwere Straftaten“) an Strafverfolgungsbehörden übermittelt werden.³⁷ Erfasst werden Strafnormen, „*wenn sie mit einer Höchstfreiheitsstrafe von mehr als fünf Jahren bedroht ist*“.³⁸ Eine Höchstfreiheitsstrafe von mindestens fünf Jahren reicht dagegen an und für sich noch nicht aus.³⁹ Die „besondere Schwere“ muss hier „*unter Berücksichtigung des jeweils geschützten Rechtsguts und dessen Bedeutung für die Rechtsgemeinschaft*“ und „*unter Berücksichtigung der Tatbegehung und Tatfolgen*“ vertretbar erscheinen⁴⁰ und „*in der Strafnorm selbst einen objektivierten Ausdruck finden*“⁴¹.

Als Schwelle sind „*bestimmte, den Verdacht begründende Tatsachen*“ erforderlich; d.h. es bedarf „*konkrete[r] und in gewissem Umfang verdichtete[r] Umstände als Tatsachenbasis für den Verdacht*“.⁴²

- **Sonstige Stellen:** Sollen nachrichtendienstlich ersterhobene personenbezogene Daten/daraus abgeleitete Informationen an sonstige Stellen – unabhängig ob diese operative Handlungsbefugnisse besitzen oder nicht – übermittelt werden, muss das „*zum Schutz eines Rechtsguts von besonderem Gewicht*“ erfolgen.⁴³ Die Anlassschwelle soll davon abhängen, ob die sonstige Stelle operative Handlungsbefugnisse (dann: „*wenigstens konkretisierte Gefahr*“) oder keine besitzt (dann: Absenken möglich).⁴⁴

³⁶ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 110 – Hessisches VerfassungsschutzG.

³⁷ BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 251 – Bayerisches VerfassungsschutzG.

³⁸ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 203 – Hessisches VerfassungsschutzG.

³⁹ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 204 – Hessisches VerfassungsschutzG.

⁴⁰ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 205 – Hessisches VerfassungsschutzG.

⁴¹ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 206 – Hessisches VerfassungsschutzG.

⁴² BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 110 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 252 – Bayerisches VerfassungsschutzG.

⁴³ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 111 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 255 – Bayerisches VerfassungsschutzG.

⁴⁴ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 111 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 257 f. – Bayerisches VerfassungsschutzG.

Gleichzeitig betont das BVerfG, dass diese Vorgaben nicht „schematisch abschließend“ gelten.⁴⁵ „Unberührt“ soll die Möglichkeit bleiben, „für die Verknüpfung von an verschiedenen Stellen vorhandenen Informationen und die Anbahnung ihres Austausches auf Verbunddateien zurückzugreifen“.⁴⁶

Auch sollen „im Einzelfall“ Informationen an inländische öffentliche Stellen übermittelt werden dürfen, wenn dies „auf deren Ersuchen oder zur Erfüllung einer dieser gegenüber bestehenden Nachberichts- oder Unterrichtungspflicht im Rahmen personen- oder gruppenbezogener Risikoprävention“ und ein „besonders hohe[s] Gefahrenpotenzial für hochrangige Rechtsgüter und einer engen Verbindung zu den Schutzgütern des Verfassungsschutzes“ besteht.⁴⁷ Folgende Beispiele werden genannt:

- „Prüfzwecke im Waffen- oder Luftsicherheitsrecht“
- „Eignungs- oder Sicherheitsüberprüfungen im öffentlichen Dienst“
- „Vorbereitung von Vereinsverboten“

b. §§ 45 ff. BVerfSchG-E

Der Abschnitt 3 des BVerfSchG-E regelt die Übermittlung von nachrichtendienstlich erhobenen Informationen durch das Bundesamt für Verfassungsschutz an Dritte. Gemessen an den Vorgaben des BVerfG sind einige der Regelungen in ihrer konkreten Ausgestaltung verfassungs- sowie unionsrechtswidrig.

aa) § 47 BVerfSchG-E

Der § 47 BVerfSchG-E regelt die „Übermittlung an inländische öffentliche Stellen zum administrativen Rechtsgüterschutz“. Regelungstechnisch setzt der Entwurf – insoweit „schematisch“ – die formellen Anforderungen für die Weitergabe von nachrichtendienstlichen Erkenntnissen an öffentliche Stellen mit „operativen

⁴⁵ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 112 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 232 – Bayerisches VerfassungsschutzG.

⁴⁶ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 112 – Hessisches VerfassungsschutzG.

⁴⁷ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 113 – Hessisches VerfassungsschutzG.

Handlungsbefugnissen“ um. Der Entwurf übernimmt damit den abstrakten, durch das BVerfG verfassungsrechtlich abgesteckten Rahmen – nimmt jedoch keinerlei Konkretisierung innerhalb dieses Rahmens vor. Es wird nicht bestimmt, welche *konkreten* verwaltungsrechtlichen (Anschluss-)Maßnahmen auf der Grundlage dieser Informationen ergriffen werden dürfen. Das lässt sich zwar für juristisch geschulte Personen – theoretisch – auslegungstechnisch anhand der Vorgaben des BVerfG bestimmen. Für einen juristischen Laien ist jedoch nicht klar ersichtlich, welche Maßnahmen im Bereich der Gewerbeaufsicht (§ 47 Abs. 1 Nr. 8 BVerfSchG-E) oder der Finanzdienstleistungsaufsicht (§ 47 Abs. 1 Nr. 9 BVerfSchG-E) auf der Grundlage nachrichtendienstlich erlangter Informationen ergriffen werden dürfen. Damit scheitert die Norm nicht an den datenschutzrechtlichen Vorgaben zur Zweckbindung/-änderung, sondern an denen der Normenklarheit und -bestimmtheit.⁴⁸

Auch systematisch ist § 47 BVerfSchG-E nicht gelungen. Während im bisherigen § 20 BVerfSchG in Absatz 2 nur die mit nachrichtendienstlichen Mitteln erhobenen Daten angesprochen waren, ist diese Einschränkung im vorgeschlagenen § 47 Abs. 2 entfallen⁴⁹. Dadurch behandelt sowohl Abs. 1 als auch Abs. 2 den selben Anwendungsfall mit minimalen sprachlichen Abweichungen:

Abs. 1

Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an eine inländische öffentliche Stelle übermitteln, soweit dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zum Schutz besonders gewichtiger Rechtsgüter vor Bedrohungen erforderlich ist [...]

⁴⁸ GFF, Stellungnahme vom 14. Juli 2026, S. 22.

⁴⁹ Was von der Entwurfsbegründung aber verneint wird. Dort heißt es auf S. 359 “Der Absatz entspricht der Übermittlungsbefugnis im bisherigen § 20 Absatz 2.”

Abs. 2

Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an eine inländische öffentliche Stelle übermitteln [...] wenn dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall zum Schutz besonders gewichtiger Rechtsgüter erforderlich ist.

Es erschließt sich nicht, warum die in Abs. 2 enthaltende Datenweitergabe “zur Vorbereitung, Durchführung oder Überprüfung einer begünstigenden Maßnahme” eines eigenen Absatzes bedarf, wenn sie nun unter den selben Voraussetzungen zulässig sein soll, wie die Weitergabe nach Abs. 1.

Die Grundrechts- und Praxisrelevanz des bisherigen § 20 Abs. 2 BVerfSchG und eines etwaigen künftigen § 47 Abs. 2 ist erheblich, denn diese Norm wird als Rechtsgrundlage des sog. Haber-Verfahrens herangezogen.

bb) § 48 BVerfSchG-E

§ 48 BVerfSchG-E regelt die Übermittlung an Strafverfolgungsbehörden. Der in § 48 Abs. 2 Nr. 2 BVerfSchG-E festgelegte Katalog an Straftaten genügt nicht den Anforderungen des BVerfG an eine „*besonders schwere Straftat*“. In der Anlage finden sich einige Delikte, die lediglich eine Höchstfreiheitsstrafe von mindestens fünf Jahren aufweisen und sich die „*besondere Schwere*“ auch nicht objektiv im Tatbestand selbst ausdrückt, weil dies „*unter Berücksichtigung des jeweils geschützten Rechtsguts und dessen Bedeutung für die Rechtsgemeinschaft*“ und „*unter Berücksichtigung der Tatbegehung und Tatfolgen*“ vertretbar erscheint, bspw.:

- Verunglimpfung des Bundespräsidenten, § 90 Abs. 1 und 3 StGB
- Aussetzung, § 221 Abs. 1 StGB
- Zerstörung wichtiger Arbeitsmittel, § 305a Abs. 1 StGB
- Gefährliche Eingriffe in den Straßenverkehr, § 315b Abs. 1 und 2 StGB
- Störung öffentlicher Betriebe, § 316b Abs. 1, 2 StGB

cc) § 49 BVerfSchG-E

Der § 49 BVerfSchG-E regelt die Übermittlung personenbezogener Daten an inländische öffentliche Stellen ohne Möglichkeit operativer Anschlussmaßnahmen.

Die Regelung in Absatz 4 steht im Widerspruch zu den Vorgaben des BVerfG.⁵⁰

§ 49 Abs. 4 BVerfSchG-E sieht vor, dass der Empfänger die übermittelten Daten nicht für operative Anschlussmaßnahmen zu Lasten der betroffenen Person nutzen darf, wenn die Voraussetzungen nach den §§ 46 und 48 BVerfSchG-E nicht vorliegen.

Zum einen möchte die Norm nur die Verwendung „zu Lasten der betroffenen Personen“ ausschließen; nicht aber zu Lasten Dritter. Positiv gewendet erlaubt die Norm die Verwendung der personenbezogenen Daten für operative Anschlussmaßnahmen gegenüber Dritten. Das steht im Widerspruch zu den Zweckbindungsvorgaben des BVerfG. Auch bei einer Verwendung zu Lasten Dritter werden die personenbezogenen Daten – welche den Bezugspunkt der Zweckbindungsvorgaben bilden – verarbeitet.

Zum anderen wird hiermit die generelle Statik des vom BVerfG errichteten, feingliedrigen Systems ins Wanken gebracht. Eine Übermittlung unter den niedrigschwelligen Voraussetzungen soll nur deshalb möglich sein, weil die empfangende Behörde keine „Möglichkeiten“ für operative Anschlussmaßnahmen besitzen soll. Nach dem Willen des Reformgesetzgebers sollen diese Möglichkeiten jedoch (1) bestehen und (2) unter den Voraussetzungen der §§ 46–48 BVerfSchG-E in Bezug auf die übermittelten personenbezogenen Daten auch genutzt werden dürfen. Hiermit wird das abgestufte Schutzgefüge schlicht unterlaufen.

Systematisch und teleologisch fehlt geht daher auch die in Absatz 2 vorgesehene Übermittlung an den Bundesnachrichtendienst. Dieser wird im Rahmen des Legislativpaketes gerade mit operativen Handlungsbefugnissen ausgestattet.

⁵⁰ BVerfG Beschl. v. 17.7.2024 – 1 BvR 2133/22 Rn. 106 – Hessisches VerfassungsschutzG; BVerfG Urt. v. 26.4.2022 – 1 BvR 1619/17 Rn. 234 – Bayerisches VerfassungsschutzG.

dd) § 58 BVerfSchG-E

§ 58 BVerfSchG-E ist unionsrechtswidrig. Danach sind personenbezogene Daten unverzüglich gegenüber dem Empfänger zu berichtigen, wenn sie sich nach ihrer Übermittlung nach den Vorschriften dieses Gesetzes als unvollständig oder unrichtig erweisen. Dies gilt jedoch dann nicht, wenn dies für die Beurteilung eines Sachverhalts ohne Bedeutung ist.

Unrichtige personenbezogene Daten sind jedoch nach den zwingenden unionsrechtlichen Vorgaben ohne Rückausnahme zu berichtigen.

Nach Art. 4 lit. d) RL (EU) 2016/680 („JI-RL“) sehen die Mitgliedsstaaten vor, dass personenbezogene Daten *„sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden“*.

Art. 7 Abs. 3 JI-RL regelt:

„Wird festgestellt, dass unrichtige personenbezogene Daten übermittelt worden sind oder die personenbezogenen Daten unrechtmäßig übermittelt worden sind, so ist dies dem Empfänger unverzüglich mitzuteilen. In diesem Fall ist gemäß Artikel 16 eine Berichtigung oder Löschung oder die Einschränkung der Verarbeitung der personenbezogenen Daten vorzunehmen.“

Erwägungsgrund 47 Satz 7, 8 JI-RL:

„Entsprechende Berichtigungen oder Löschungen personenbezogener Daten oder Einschränkungen der Verarbeitung sollten den Empfängern, gegenüber dem die personenbezogenen Daten offengelegt wurden, und den zuständigen Behörden, von denen die unrichtigen Daten stammen, mitgeteilt werden. Der Verantwortliche sollte auch von jeglicher Weiterverbreitung dieser Daten Abstand nehmen.“

Der unionsrechtliche Richtliniengeber sieht daher keinen Umsetzungsspielraum für die Mitgliedsstaaten vor.

Verteiler

- Bundesministerium der Justiz und für Verbraucherschutz
- Bundesministerium des Innern
- Bundesministerium für Wirtschaft und Energie
- Bundesministerium für Digitales und Staatsmodernisierung
- Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages
- Innenausschuss des Deutschen Bundestages
- Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
- Ausschuss Digitale Agenda im Deutschen Bundestag
- Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien
- Arbeitsgruppen Inneres der im Deutschen Bundestag vertretenen Parteien
- Fraktionen des Deutschen Bundestages
- Justizministerien der Länder
- Innenministerien der Länder
- Rechts- und Innenausschüsse der Landtage
- Europäische Kommission – Vertretung in Deutschland
- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Landesdatenschutzbeauftragte

- Bundesrechtsanwaltskammer
- Bundesverband der Freien Berufe
- Deutsches Institut für Menschenrechte
- Gesellschaft für Freiheitsrechte
- Institut für Deutsches und Europäisches Strafprozessrecht und Polizeirecht (ISP) der Universität München
- Deutscher Richterbund, Bund der Richterinnen und Richter, Staatsanwältinnen und Bund Deutscher Verwaltungsrichter und Verwaltungsrichterrinnen Staatsanwälte e.V. (DRB)
- Gewerkschaft der Polizei
- Deutsche Polizeigewerkschaft
- Stiftung neue Verantwortung e.V.
- Republikanischer Anwältinnen- und Anwälteverein e. V.

- Mitglieder des Vorstandes des Deutschen Anwaltvereins
- Vorsitzenden der Landesverbände des Deutschen Anwaltvereins
- Vorsitzenden der Gesetzgebungsausschüsse des Deutschen Anwaltvereins
- Mitglieder des Ausschusses Recht der Inneren Sicherheit des Deutschen Anwaltvereins
- Mitglieder des Ausschusses Informationsrecht
- Vors. des FORUM Junge Anwaltschaft des DAV

Presse

- NJW
- Frankfurter Allgemeine Zeitung
- Süddeutsche Zeitung
- Berliner Verlag GmbH
- Hamburger Abendblatt
- Der Tagesspiegel
- Der Spiegel

- Juris Newsletter
- JUVE Verlag für juristische Information GmbH
- Redaktion Anwaltsblatt
- JurPC
- Netzpolitik.org
- Heise
- LTO
- Neue Zürcher Zeitung
- Frankfurter Rundschau
- Zeit
- Neue Zeitschrift für Verwaltungsrecht
- Die Öffentliche Verwaltung
- Redaktion MultiMedia und Recht (MMR)
- Redaktion Zeitschrift für Datenschutz ZD
- Computer und Recht