



Ausschussdrucksache 21(4)233 B
vom 9. Oktober 2026

Schriftliche Stellungnahme

von Prof. Dr. Matthias Bäcker, Johannes Gutenberg-Universität Mainz
vom 9. Oktober 2026

zu dem

Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts
BT-Drucksachen 21/7868, 21/8295

JOHANNES GUTENBERG-UNIVERSITÄT MAINZ - 55099 Mainz

FACHBEREICH 03
RECHTSWISSENSCHAFT
Lehrstuhl für Öffentliches Recht
und Informationsrecht,
insbesondere Datenschutzrecht

Universitätsprofessor
Dr. Matthias Bäcker, LL.M.

Johannes Gutenberg-
Universität Mainz
Jakob-Welder-Weg 9
55128 Mainz

Tel. +49 6131 39 28173
Fax +49 6131 39 28172

matthias.baecker@uni-mainz.de
www.baecker.jura.uni-mainz.de

Stellungnahme

zu dem Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts
(BT-Drs. 21/7868)

Gliederung

Ergebnisse.....	3
I. Telekommunikationsbezogene Überwachungsmaßnahmen	4
1. Verarbeitung der Inhalte und Metadaten nicht-interpersoneller Kommunikation	4
2. Strategische Aufklärung	6
a) Aufklärungsziel	6
b) Bevorratung von Inhalten der ausländischen und internationalen interpersonellen Kommunikation	8
c) Bevorratung inländischer Kommunikationsdaten.....	10
d) Einsichtnahme	11
II. Nutzung von Künstlicher Intelligenz	11
III. Datenübermittlungen.....	14
1. Übermittlungsbefugnisse des BfV.....	14
a) Datenübermittlung zum administrativen Rechtsgüterschutz.....	14
b) Datenübermittlung zur Strafverfolgung.....	16
c) Datenübermittlung an nicht-öffentliche Stellen	17
2. Übermittlungsbefugnisse des BND	18
a) Datenübermittlung zur Strafverfolgung.....	18
b) Datenübermittlung zur Gefahrenabwehr	18
c) Datenübermittlung im Gefahrvorfeld.....	19
IV. Aktionelle Maßnahmen	19
1. „Schutzmaßnahmen“ des BfV.....	20
a) Regelungsgehalt und Reichweite von §§ 59 ff. BVerfSchG-E	20
b) Rechtsstaatliche Unvertretbarkeit heimlicher Eingriffe in Freiheit und Eigentum	23
c) Weitere verfassungsrechtliche Einwände	27
2. „Erweiterte nachrichtendienstliche Maßnahmen“ des BND	28

Ergebnisse

1. Der sowohl im BVerfSchG-E als auch im BNDG-E vorgesehene schwächere Schutz von Inhalten und Metadaten der Mensch-Maschine- und der intermaschinellen Kommunikation im Vergleich zu Inhalten und Metadaten der interpersonellen Kommunikation ist mit dem Fernmeldegeheimnis nicht vereinbar.
2. Die Regelungen über die strategische Aufklärung des BND sind hinsichtlich der zulässigen Aufklärungsziele zu weit gefasst, erlauben die Bevorratung der erhobenen Daten in zu großem Ausmaß und knüpfen die Einsichtnahme in diese Daten nicht durchweg an hinreichend gehaltvolle Voraussetzungen.
3. Die Regelungen im BVerfSchG-E und im BNDG-E zur Nutzung komplexer Analysetechnik, insbesondere von Künstlicher Intelligenz, tragen dem Eingriffsgewicht der Datenanalyse nicht durchweg Rechnung.
4. Die Ermächtigungen des BfV und des BND zu Datenübermittlungen reichen teils zu weit.
5. Die Ermächtigung des BfV zu „Schutzmaßnahmen“ ist rechtsstaatlich nicht vertretbar.
6. Die Ermächtigung des BND zu „erweiterten nachrichtendienstlichen Maßnahmen“ sollte hinsichtlich der bedrohten Rechtsgüter präziser gefasst, weitergehend als vorgesehen auf Maßnahmen im Ausland beschränkt, klar auf aktionelle Maßnahmen zugeschnitten und mit den wehrverfassungsrechtlichen Vorgaben abgestimmt werden. Im Übrigen erscheint es sinnvoll, diese Regelungen durch einen (deklaratorischen) Hinweis auf die völkerrechtlichen Grenzen solcher Maßnahmen zu ergänzen.

Eine umfassende Stellungnahme zu dem 609 Seiten umfassenden Gesetzentwurf ist mir als Einzelperson generell nicht mit vertretbarem Aufwand möglich und jedenfalls in der kurzen Frist bis zu der Anhörung nicht zu leisten. Die folgenden Ausführungen beschränken sich schlaglichtartig auf einzelne Regelungskomplexe, die zudem teilweise nicht in allen Facetten erörtert werden. Es sei ausdrücklich betont, dass der Entwurf im Übrigen neben zweifellos beachtlichen Verbesserungen sowohl eine Reihe von Defiziten des geltenden Rechts fortschreibt (beispielsweise werden nach wie vor die zulässigen nachrichtendienstlichen Mittel nicht abschließend reguliert, fehlen belastbare Vorgaben zum Umgang mit IT-Schwachstellen und verletzt die aus dem G 10 übernommene Ermächtigung der Landesverfassungsschutzbehörden zu Telekommunikationsüberwachungen die bundesstaatliche Kompetenzordnung) als auch weitere Zweifelsfragen aufwirft, die im Folgenden nicht näher erörtert werden können (beispielhaft sei auf die niedrigschwelligen Ermächtigungen zu OSINT-Maßnahmen einschließlich biometrischer Abgleiche, die fragwürdige Differenzierung zwischen teils eingriffsintensiven Auskunftersuchen und nachrichtendienstlichen Mitteln oder die sehr weit gefassten Verstrickungsregelungen im Zusammenhang mit dem Schutz von Berufsgeheimnissen verwiesen).

I. Telekommunikationsbezogene Überwachungsmaßnahmen

1. Verarbeitung der Inhalte und Metadaten nicht-interpersoneller Kommunikation

Die Regelungen zu telekommunikationsbezogenen Überwachungsmaßnahmen sowohl im BVerfSchG-E als auch im BNDG-E beruhen auf – im Ansatz ähnlichen, im Detail unterschiedlichen – Differenzierungen unterschiedlicher Kategorien von Telekommunikationsdaten, die sich durch telekommunikationsbezogene Überwachungsmaßnahmen erlangen lassen. Dabei handelt es sich erstens um Inhalte interpersoneller Kommunikation, an der mindestens zwei natürliche Personen als Kommunikationspartner beteiligt sind, zweitens um die Metadaten interpersoneller Kommunikation, drittens um Inhalte und Metadaten einer Mensch-Maschine-Kommunikation und viertens um Inhalte und Metadaten rein intermaschineller Kommunikation. Diese Differenzierung wird genutzt, um unterschiedliche Eingriffsschwellen für telekommunikationsbezogene Überwachungsmaßnahmen festzulegen:

Nach § 22 Abs. 1 Satz 2 und 3 BVerfSchG-E darf das BfV die Inhalte interpersoneller Telekommunikation nur zur Aufklärung einer besonders erheblich beobachtungsbedürftigen Bedrohung überwachen, während eine auf Metadaten und die Mensch-Maschine-Kommunikation beschränkte Überwachung auch im Fall einer erheblich beobachtungsbedürftigen Bedrohung zulässig ist. Die Überwachung rein intermaschineller Kommunikation richtet sich gemäß § 22 Abs. 2 Satz 2 BVerfSchG-E nach den Vorschriften über das Auslesen informationstechnischer Geräte oder über Eingriffe in die Integrität informationstechnischer Systeme (§ 23, § 25 und § 26 BVerfSchG-E), was nach der

Entwurfsbegründung regelmäßig ebenfalls zu dem Erfordernis einer erheblich beobachtungsbedürftigen Bedrohung führen soll.¹

Nach §§ 33 ff. BNDG-E richten sich die Anforderungen sowohl an die Einsichtnahme in Kommunikationsdaten bei der strategischen Aufklärung als auch an die individualbezogene Telekommunikationsüberwachung gleichfalls nach der Datenkategorie.

Bei der strategischen Aufklärung gelten die strengsten Anforderungen für die Einsichtnahme in die Inhalte interpersoneller Kommunikation (§ 33 Abs. 2, § 34 Abs. 2 BNDG-E). Weniger strenge, aber immer noch kommunikationsspezifische Anforderungen gelten mit Blick auf die Metadaten interpersoneller Kommunikation (§ 33 Abs. 1, § 34 Abs. 1). Keine besonderen Vorgaben gelten schließlich für die Einsichtnahme in die Inhalte und Metadaten der Mensch-Maschine- und der rein intermaschinellen Kommunikation. Soweit solche Daten bei der strategischen Aufklärung anfallen, darf der BND sie nach den allgemeinen Regeln in §§ 52 ff. BNDG-E weiterverarbeiten, also sie insbesondere langfristig bevorraten und unter niedrigschwelligen Voraussetzungen einsehen.² Dies gilt insbesondere auch für Daten aus einer reinen Inlandskommunikation.³

Bei der individualbezogenen Telekommunikationsüberwachung differenziert der Entwurf zwischen Überwachungen, die sich auch auf die Inhalte interpersoneller Kommunikation beziehen (§ 35 Abs. 1 Satz 2, Abs. 2 Satz 2 BNDG-E), und sonstigen Überwachungen, die unter niedrigeren Voraussetzungen zulässig sind (§ 35 Abs. 1 Satz 1, Abs. 2 Satz 1 BNDG-E). Mit Blick auf die Weiterverarbeitung der erhobenen Daten finden sich wiederum besondere Regelungen für Inhalte und Metadaten der interpersonellen Kommunikation (§§ 64 ff. BNDG-E), während sich die Weiterverarbeitung sonstiger Inhalte und Metadaten auch insoweit nach den allgemeinen Regelungen richtet.⁴

Die Differenzierung im Schutzniveau zwischen Inhalten und Metadaten der interpersonellen Kommunikation einerseits und sonstiger Telekommunikation andererseits findet im Text des Grundgesetzes und in der Rechtsprechung des Bundesverfassungsgerichts keine Stütze. Sie überzeugt auch in der Sache nicht.

Art. 10 GG schützt das Fernmeldegeheimnis unabhängig davon, wer kommuniziert und welche Inhalte übertragen werden. Wie die Entwurfsbegründung verschiedentlich anerkennt, unterfallen daher auch die Mensch-Maschine- und die intermaschinelle Telekommunikation dem Fernmeldegeheimnis. Dies hat das Bundesverfassungsgericht in seinem Trojaner-I-Beschluss ausdrücklich festgehalten.⁵ Weder in diesem Beschluss noch an anderer Stelle in der Rechtsprechung des Bundesverfassungsgerichts finden sich hingegen Ausführungen, die einen differenzierten Schutz unterschiedlicher Kommunikationsformen anlegen. Vielmehr hat das Gericht auch in seiner jüngsten Rechtsprechung

¹ BT-Drs. 21/7868, S. 254 f. Ob der Verweis auf § 23, § 25 und § 26 BVerfSchG-E aufgeht, erscheint mir allerdings fragwürdig. Das BfV verschafft sich bei einer netzbasierten Überwachung der Maschine-Maschine-Kommunikation zumindest in der Regel weder einen unmittelbaren Zugriff auf die kommunizierenden Maschinen noch auf die IT-Systeme der Kommunikationsinfrastruktur, sondern erhält die Inhalte und Metadaten von einem Kommunikationsdiensteanbieter in Kopie übermittelt. Da der Regelungsansatz des § 22 BVerfSchG-E allerdings ohnehin verfehlt ist, wie sogleich zu zeigen ist, kann diese Frage hier auf sich beruhen.

² BT-Drs. 21/7868, S. 424.

³ Vgl. BT-Drs. 21/7868, S. 431.

⁴ BT-Drs. 21/7868, S. 484.

⁵ BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 2466/19 –, Rn. 91.

6

die Anforderungen an die Verhältnismäßigkeit inhaltsbezogener (Quellen-)Telekommunikationsüberwachungen einheitlich bestimmt, ohne dabei zwischen unterschiedlichen Kommunikationsformen und Inhalten zu differenzieren.⁶

Eine solche Differenzierung liegt in der Sache auch fern. Das Fernmeldegeheimnis knüpft an die spezifische Verwundbarkeit der Fernkommunikation und nicht an die Sensibilität der übermittelten Inhalte an. Selbst wenn dies anders zu sehen wäre, sind zudem entgegen der Entwurfsbegründung Inhalte und Metadaten der Mensch-Maschine- und der intermaschinellen Kommunikation nicht typischerweise weniger schutzbedürftig als gleichartige Daten der interpersonellen Kommunikation. Vielmehr kann bei beiden Kommunikationsformen die Sensibilität dieser Daten im Einzelfall stark divergieren. So dürfte ein quantitativ großer Teil der Sprachtelefonie oder der Instant-Messaging-Kommunikation darin bestehen, dass die Beteiligten banale Alltagsvorgänge besprechen. Dies ändert nichts daran, dass diese interpersonellen Kommunikationsdienste gerade auch zum vertraulichen Austausch mit engsten Bezugspersonen genutzt werden können. Ebenso können Inhalte und Metadaten der Mensch-Maschine- wie auch der intermaschinellen Kommunikation eine sehr hohe Sensibilität aufweisen, die hinter der interpersonellen Kommunikation nicht regelhaft zurückbleibt. Beispielsweise können bei der Nutzung eines auf einem komplexen Sprachmodell beruhenden Chatbots oder bei der Nutzung einer Suchmaschine (Mensch-Maschine-Kommunikation) hochgradig sensible Inhalte anfallen. Eine Analyse der von einem menschlichen Nutzer aufgerufenen Webseiten (Metadaten der Mensch-Maschine-Kommunikation) kann weitreichende Schlüsse über die betroffene Person ermöglichen. Gleiches gilt etwa für die durch Gesundheitsapps oder Kartendienste übermittelten Daten (intermaschinelle Kommunikation).

2. Strategische Aufklärung

a) Aufklärungsziel

Der Entwurf gibt die aus dem BNDG-Urteil des Bundesverfassungsgerichts stammende Differenzierung im geltenden Recht zwischen Aufklärungsprojekten zur politischen Information und zur Gefahrfrüherkennung auf. Die strategische Aufklärung soll stattdessen umfassend auf die Früherkennung von Bedrohungen ausgerichtet werden. Dementsprechend muss die Ermächtigung vollständig den für die Gefahrfrüherkennung geltenden verfassungsrechtlichen Maßstäben genügen.⁷ Eine strategische Aufklärung zur Gefahrfrüherkennung muss auf den Schutz hochrangiger Gemeinschaftsgüter gerichtet sein, deren Verletzung schwere Schäden für den äußeren und inneren Frieden oder die Rechtsgüter Einzelner zur Folge hätte.⁸ Diesem Erfordernis genügt der Entwurf nicht.

Nach § 32 Abs. 1 BNDG-E darf der BND personenbezogene Daten im Rahmen strategischer Aufklärungsmaßnahmen erheben, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dies zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist. Damit ist die Datenerhebung im gesamten durch § 2 Abs. 1 Satz 1 BNDG-E definierten Aufgabenbereich des BND zulässig. Die strategische

⁶ Vgl. BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 2466/19 –, Rn. 122 ff.; Beschluss vom 24. Juni 2025 – 1 BvR 180/23 –, Rn. 176 ff.

⁷ Insoweit ebenso die Entwurfsbegründung, BT-Drs. 21/7868, S. 433.

⁸ BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 176.

Aufklärung wird demnach, obwohl sie als Maßnahme der Gefahrfrüherkennung konzipiert ist, wie eine Maßnahme zur politischen Information behandelt.⁹

Zwar soll die Auslandsaufklärung nach § 2 Abs. 1 Satz 2 BNDG-E generell nur Bedrohungen für besonders gewichtige Rechtsgüter zum Gegenstand haben. Der in § 2 Abs. 2 BNDG-E enthaltene, ohnehin nicht abschließende Katalog besonders gewichtiger Rechtsgüter begrenzt jedoch die Aufklärungstätigkeit des BND nicht durchweg auf Rechtsgüter, die den Anforderungen an eine strategische Aufklärung zur Gefahrfrüherkennung genügen.

Grund hierfür ist vor allem das in § 2 Abs. 2 Nr. 3 BNDG-E genannte Rechtsgut der außenpolitischen Handlungsfähigkeit der Bundesrepublik Deutschland. Dieser für sich genommen wenig klare Begriff wird im BNDG-E nicht definiert. Seine Bedeutung erschließt sich erst aus der Entwurfsbegründung. Danach geht es bei der außenpolitischen Handlungsfähigkeit generell um die „auswärtigen Belange“ der Bundesrepublik und um Vorgänge im staatlichen oder nichtstaatlichen Bereich, die „außenpolitische Reaktionen erforderlich“ machen. Der BND solle in diesem Zusammenhang „die Bundesregierung in außen- und sicherheitspolitischen Fragen mit Informationen... versorgen“.¹⁰ Die außenpolitische Handlungsfähigkeit der Bundesrepublik könne dementsprechend „auch durch Unkenntnis über politische oder wirtschaftliche Ereignisse und Entwicklungen in aufklärungsbedürftigen Staaten bedroht sein“.¹¹

Wird die außenpolitische Handlungsfähigkeit derart offen verstanden, so grenzt dieses Rechtsgut den Befugnisbereich des BND nicht erkennbar ein. Abhängig von den jeweiligen außenpolitischen Interessen der Bundesrepublik kann nahezu jeder Vorgang im Ausland, der über den privaten Bereich einzelner Menschen hinausgeht, außenpolitisch relevant sein. Nach den Erläuterungen in der Entwurfsbegründung erfordert die außenpolitische Handlungsfähigkeit der Bundesrepublik möglichst umfassende Informationen über außenpolitisch relevante Vorgänge. Die drohende Unkenntnis über einen solchen Vorgang beinhaltet in der Folge eine Bedrohung für die außenpolitische Handlungsfähigkeit der Bundesrepublik. Dementsprechend fügt das Erfordernis einer solchen Bedrohung der allgemeinen Aufgabe des BND, Informationen von außen- oder sicherheitspolitischer Relevanz zu sammeln und auszuwerten, nichts hinzu. Diese Aufgabe wiegt jedoch gerade nicht generell schwer genug, um eine strategische Aufklärung zur Gefahrfrüherkennung zu legitimieren.¹²

Die zu offene Fassung des Rechtsguts der außenpolitischen Handlungsfähigkeit wirkt sich im Übrigen auch auf zahlreiche weitere Ermächtigungen aus, die für Grundrechtseingriffe von teils erheblicher Intensität gleichfalls lediglich voraussetzen, dass sie aufgrund tatsächlicher Anhaltspunkte im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich sind (vgl. etwa § 13 Abs. 1 Satz 1, § 24 Abs. 1 Nr. 1 BNDG-E). Solche Maßnahmen sind in der Folge bereits dann zulässig, wenn durch sie überhaupt außenpolitisch relevante Informationen erlangt werden können. Dem

⁹ Vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 177.

¹⁰ BT-Drs. 21/7868, S. 343 f.

¹¹ BT-Drs. 21/7868, S. 337.

¹² Vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 305.

Erfordernis einer gesteigerten Eingriffsschwelle für eingriffsintensivere Maßnahmen¹³ trägt dies nicht Rechnung.

b) Bevorratung von Inhalten der ausländischen und internationalen interpersonellen Kommunikation

Weder mit Art. 10 GG noch mit Art. 8 EMRK oder – soweit mittelbar relevant – mit Art. 7 und Art. 8 GRCh vereinbar ist die im Gesetzentwurf neu vorgesehene Bevorratung von Inhalten der ausländischen und internationalen interpersonellen Kommunikation.

Der BND darf die im Rahmen der strategischen Aufklärung erhobenen Inhaltsdaten der ausländischen und internationalen Kommunikation gemäß § 66 Abs. 1 Satz 1 BNDG-E bis zu sechs Monate lang ohne weitere Voraussetzungen speichern.¹⁴ Hierin liegt – wie auch die Entwurfsbegründung verschiedentlich hervorhebt – eine erhebliche Ausweitung der strategischen Aufklärung, da gegenwärtig Inhalte bei der Erfassung mit Suchbegriffen abzugleichen sind und nur die dabei resultierenden Treffer weiterverarbeitet werden dürfen (§ 19 Abs. 5 BNDG, § 5 Abs. 2 Satz 1 G 10).

Die Rechtsprechung des Bundesverfassungsgerichts bietet keinen Anhaltspunkt dafür, dass diese Ausweitung mit dem Fernmeldegeheimnis in Einklang stehen könnte. Das Gericht hat vielmehr in seinem Urteil zum BNDG die Auswahl der Suchbegriffe als wesentlichen Parameter hervorgehoben, der die Verhältnismäßigkeit der strategischen Aufklärung gewährleistet.¹⁵ Dementsprechend sah es das Gebot einer „unverzöglichen Auswertung der erfassten Daten“ anhand solcher Suchbegriffe als notwendigen Bestandteil einer gesetzlichen Regulierung an.¹⁶ Die „gesamthaft bevorratende Speicherung“ von Verkehrsdaten, wie sie bereits das geltende Recht vorsieht, hat das Bundesverfassungsgericht als intensitätssteigernden Umstand gewertet¹⁷ und nur unter einengenden Voraussetzungen für verfassungsgemäß gehalten.¹⁸ Dass das Gericht nunmehr die noch deutlich eingriffsintensivere Bevorratung von Inhalten, wie sie der Entwurf vorsieht, für gerechtfertigt halten wird, erscheint unwahrscheinlich.

Gleichläufige Indizien finden sich in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte. Der Gerichtshof hatte bisher nur Überwachungsprogramme zu beurteilen, in denen Inhalte unmittelbar mit Suchbegriffen abgeglichen und lediglich Verkehrsdaten ohne einen solchen

¹³ Vgl. zum Verfassungsschutzrecht BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 190 ff.; Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, Rn. 96 f.

¹⁴ Dies ist jedenfalls die aus der Entwurfsbegründung ersichtliche Regelungsintention, vgl. BT-Drs. 21/7868, S. 487. Dem Wortlaut nach enthält § 66 Abs. 1 BNDG-E keine Ermächtigung zur Datenspeicherung, sondern legt eine Höchstfrist für die Löschung der Daten fest. Hieraus könnte gefolgert werden, dass die Speicherung der Inhalte sich nach der allgemeinen Weiterverarbeitungsermächtigung in § 52 Abs. 1 BNDG-E richtet. Diese Norm knüpft an eine Erforderlichkeitsprüfung an, was sich so verstehen ließe, dass der BND vor der (längerfristig angelegten) Speicherung von Daten konkret prüfen muss, ob sich ihnen Informationen über bestimmte Bedrohungen entnehmen lassen (vgl. die Erläuterung zu den Voraussetzungen von § 52 Abs. 1 BNDG-E, aus der zumindest mir nicht deutlich geworden ist, was genau wann genau der BND im Zusammenhang mit einer Datenspeicherung zu prüfen hat, in BT-Drs. 21/7868, S. 466 f.). Diese vom Wortlaut her möglichen oder sogar naheliegenden, aber ersichtlich nicht gemeinten Norminterpretationen bleiben hier außer Betracht.

¹⁵ BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 182.

¹⁶ BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 192.

¹⁷ BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 153.

¹⁸ BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 166, 191.

Abgleich bevorratet wurden.¹⁹ Lediglich für Verkehrsdaten hat der Gerichtshof eine derartige Bevorratung unter strengen Kautelen grundsätzlich für hinnehmbar erachtet.²⁰ Ob demnach eine Bevorratung sogar von Inhalten konventionsrechtlich zulässig sein kann, erscheint bestenfalls offen.

Schließlich liegt nahe, dass sich eine solche Bevorratung nicht mit unionsrechtlichen Vorgaben vereinbaren lässt.

Entgegen der Entwurfsbegründung²¹ sind solche Vorgaben für die vorgesehenen Regelungen nicht von vornherein irrelevant. Ob tatsächlich die gesamte Tätigkeit des BfV und des BND als Schutz der nationalen Sicherheit im Sinne von Art. 4 Abs. 2 EUV begriffen werden kann, ist fragwürdig,²² kann hier aber dahinstehen. Mit Blick auf die strategische Aufklärung ergeben sich jedenfalls mittelbar unionsrechtliche Anforderungen aus der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation. Grund hierfür ist, dass der BND die im Rahmen der technischen Aufklärung erhobenen Daten in der Regel unter Mitwirkung bestimmter Anbieter von Telekommunikationsdiensten erhebt, die etwa Datenströme an den BND ausleiten oder dem BND ermöglichen, eigene Überwachungsvorrichtungen an ihre Vermittlungstechnik anzuschließen.

Die Diensteanbieter benötigen zu ihrer Mitwirkung eine datenschutzrechtliche Erlaubnis nach dem durch die Richtlinie 2002/58/EG vorgeprägten Telekommunikations-Datenschutzrecht, da sie ansonsten Dritten keinen Zugriff auf die Inhalte und Umstände der von ihnen vermittelten Kommunikation einräumen dürfen. Art. 15 Abs. 1 RL 2002/58/EG ermöglicht den Mitgliedstaaten, solche Erlaubnisse (und zugehörige Mitwirkungspflichten) der Diensteanbieter zu schaffen. Aus Art. 15 Abs. 1 RL 2002/58/EG ergeben sich nicht allein Anforderungen an die Erlaubnisnormen für die Diensteanbieter, sondern mittelbar auch Anforderungen an die korrespondierenden Ermächtigungen der Sicherheitsbehörden zur Erhebung und Weiterverarbeitung der ausgeleiteten Daten. Denn nach der Rechtsprechung des Gerichtshofs der Europäischen Union steht die Mitwirkungserlaubnis mit Art. 15 Abs. 1 RL 2002/58/EG nur in Einklang, wenn sie einem der dort genannten Zwecke – unter anderem dem Schutz der nationalen Sicherheit – dient und in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Dies lässt sich nur mit Blick auf die Verarbeitung der Daten beurteilen, an deren Erhebung der Diensteanbieter mitwirkt. Ist die Erhebung und Weiterverarbeitung der Daten durch den BND nicht hinreichend restriktiv geregelt, so kann auch ihre Ausleitung durch die Diensteanbieter nicht gerechtfertigt werden. Ist wiederum die Mitwirkung unzulässig, so darf auch die Weiterverarbeitung der ausgeleiteten Daten nicht zugelassen werden.

Dieser mittelbare Kontrollansatz ist auch dann zu beachten, wenn die Weiterverarbeitung der Daten durch die Empfangsbehörde für sich genommen nicht in den Anwendungsbereich des Unionsrechts fällt. Die strategische Aufklärung ist daher ungeachtet von Art. 4 Abs. 2 Satz 3 EUV mittelbar auch

¹⁹ Vgl. die Darstellungen bei EGMR, Urteil vom 25. Mai 2021, Nos. 58170/13, 62322/14 und 24960/15 – Big Brother Watch u.a. v. United Kingdom, Rn. 293, 297, 403, 419; Urteil vom 25. Mai 2021, No. 35252/08 – Centrum för Rättvisa v. Sweden, Rn. 26.

²⁰ EGMR, Urteil vom 25. Mai 2021, Nos. 58170/13, 62322/14 und 24960/15 – Big Brother Watch u.a. v. United Kingdom, Rn. 363 f., 416 ff.

²¹ BT-Drs. 21/7868, S. 204.

²² Näher Bäcker, in: BeckOK Datenschutzrecht, Stand 1. August 2026, Art. 2 DSGVO Rn. 10 ff.

10

insoweit an den Unionsgrundrechten zu messen, als sie dem Schutz der nationalen Sicherheit dient.²³

Der Gerichtshof der Europäischen Union hatte auf dieser konstruktiven Grundlage ein nachrichtendienstliches Programm zu beurteilen, bei dem einzelne Anbieter von Telekommunikationsdiensten durch Anordnungen verpflichtet wurden, bestimmte Verkehrsdaten *en bloc* auszuleiten.²⁴ Der Gerichtshof hielt diese Ausleitung von Verkehrsdaten mit dem Ziel, sie für nachrichtendienstliche Zwecke zu bevorraten und auszuwerten, für unionsrechtswidrig. Da die Diensteanbieter die von der Anordnung betroffenen Daten allgemein und unterschiedslos übermittelten, betreffe ihre Übermittlung pauschal sämtliche Personen, die elektronische Kommunikationsdienste nutzten. Sie gelte somit auch für Personen, bei denen keinerlei Anhaltspunkt dafür bestehe, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit dem Ziel der Wahrung der nationalen Sicherheit stehen könnte, und setze insbesondere keinen Zusammenhang zwischen den Daten, deren Übermittlung vorgesehen sei, und einer Bedrohung der nationalen Sicherheit voraus. Sie könne daher nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden.²⁵ Erst recht dürfte dies für eine Bevorratung der bei der strategischen Aufklärung anfallenden Inhaltsdaten gelten, wie sie der Entwurf vorsieht.²⁶

c) Bevorratung inländischer Kommunikationsdaten

Verfassungswidrig sind die vorgesehenen Regelungen auch insoweit, als sie dem BND eine weitreichende Bevorratung von Inhalten und Metadaten der inländischen Telekommunikation erlauben, soweit es sich um Daten der Mensch-Maschine- oder der intermaschinellen Kommunikation handelt (siehe oben I. 1.). Wie oben ausgeführt, gewährleistet Art. 10 GG die Vertraulichkeit dieser Daten im selben Maß wie die Vertraulichkeit der gleichartigen Daten der interpersonellen Kommunikation. Dementsprechend gilt auch für diese Daten die verfassungsrechtliche Vorgabe, dass inländische Kommunikationsdaten bei der Erfassung auszufiltern und unverzüglich spurlos zu löschen sind.²⁷ Erst recht dürfen sie nicht über einen längeren Zeitraum für nachrichtendienstliche Auswertungen gespeichert werden, wie es der Entwurf vorsieht.

²³ Vgl. zur Ausleitung von Verkehrsdaten EuGH, Urteil vom 6. Oktober 2020, Rs. C-623/17 – Privacy International, Rn. 34 ff.

²⁴ Das Überwachungsverfahren wird näher dargestellt bei Anderson, Report of the Bulk Powers Review, 2016, S. 29 ff., abrufbar unter <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf>; vgl. auch die Schilderung in dem Vorabentscheidungsersuchen des Investigatory Powers Tribunal, Urteil vom 8. September 2017, No. IPT/15/110/CH, abrufbar unter <https://www.ipt-uk.com/docs/Privacy%20International%20v%20SSFCA%20and%20Ors%20September%202017.pdf>.

²⁵ EuGH, Urteil vom 6. Oktober 2020, Rs. C-623/17 – Privacy International, Rn. 78 ff.

²⁶ Sogar den Wesensgehalt des Unionsgrundrechts auf Achtung des Privat- und Familienlebens (Art. 7 i.V.m. Art. 52 Abs. 1 Satz 1 GRCh) sieht durch eine Ermächtigung zur generellen Erfassung von Telekommunikationsinhalten verletzt EuGH, Urteil vom 8. April 2014, Rs. C-293/12 und C-594/12 – Digital Rights Ireland u.a., Rn. 39; Urteil vom 6. Oktober 2015, Rs. C-362/14 – Schrems I, Rn. 94.

²⁷ BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 170 ff.; Beschluss vom 8. Oktober 2024 – 1 BvR 1743/16, 1 BvR 2539/16 –, Rn. 165.

d) Einsichtnahme

Die Regelungen über die Einsichtnahme in die mit der strategischen Aufklärung erhobenen Daten genügen gleichfalls nicht vollständig den verfassungsrechtlichen Anforderungen. Wie bereits zum Aufklärungsziel ausgeführt (siehe oben I. 2. a)), lässt sich die strategische Aufklärung angesichts ihrer hohen Eingriffsintensität nur als Maßnahme zur Früherkennung von Gefahren für hochrangige Gemeinschaftsgüter rechtfertigen, deren Verletzung schwere Schäden für den äußeren und inneren Frieden oder die Rechtsgüter Einzelner zur Folge hätte. Dementsprechend darf der BND die durch die Aufklärung erlangten Inhalte und Metadaten nur einsehen und auswerten, um eine solche Bedrohung im Einzelfall aufzuklären. Die differenziert geregelten Voraussetzungen für die Einsichtnahme in die erlangten Daten genügen diesem Erfordernis teils nicht.

Der BND darf nach § 33 Abs. 1 BNDG-E Metadaten der ausländischen interpersonellen Kommunikation einsehen, wenn dies zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist. Damit ist die Einsichtnahme – insbesondere wegen des offen gefassten Rechtsguts der außenpolitischen Handlungsfähigkeit der Bundesrepublik (siehe oben I. 2. a)) – generell zulässig, um Informationen von außenpolitischer Bedeutung zu gewinnen. Auf eine gesteigerte Bedrohung für hochrangige Gemeinschaftsgüter kommt es nicht an.

Mit dem Fernmeldegeheimnis nicht zu vereinbaren ist zudem, dass der BND Inhalte und Metadaten der (inländischen wie ausländischen) nicht-interpersonellen Kommunikation unter den niedrigen Voraussetzungen der §§ 52 ff. BNDG-E einsehen und weiterverarbeiten darf (siehe oben I. 1.).

II. Nutzung von Künstlicher Intelligenz

Der Entwurf soll sowohl dem BfV als auch dem BND ermöglichen, bei der Analyse vorhandener Datenbestände auf komplexe Analysetechnik unter Einschluss von Künstlicher Intelligenz (nach der Legaldefinition in § 52 Abs. 4 BNDG-E also von Anwendungen auf der Grundlage selbstlernender Systeme, die anpassungsfähig auf einen autonomen Betrieb ausgelegt sind) zurückzugreifen.

Die Nutzung derartiger Analysetechnik unterliegt besonderen verfassungsrechtlichen Bindungen, wenn die Datenanalyse ein eigenständiges besonderes Eingriffsgewicht erreicht. Nach dem zu polizeilichen Anwendungen ergangenen Datenanalyse-Urteil des Bundesverfassungsgerichts kommt es neben Art und Umfang der verwendeten Daten vor allem auf die Auswertungsmethode und die daraus resultierenden (möglichen) Analyseergebnisse an.²⁸ Ein hohes Eigengewicht weisen etwa Anwendungen auf, die „die Erstellung von genaueren Bewegungs-, Verhaltens- oder Beziehungsprofilen zu[lassen] oder [...] vermehrt Personen, die objektiv nicht zurechenbar in das relevante Geschehen verfangen sind, dem Risiko aus[setzen], aufgrund der Ergebnisse der automatisierten Datenanalyse oder -auswertung weiteren, gezielt gegen sie gerichteten, polizeilichen Ermittlungsmaßnahmen unterzogen zu werden“.²⁹ Der Einsatz einer solchen Anwendung ist wie eine eingriffsintensive Datenerhebung zu behandeln und an die dafür maßgeblichen Eingriffsschwellen zu binden.³⁰

²⁸ BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 –, Rn. 66 ff.

²⁹ BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 –, Rn. 73.

³⁰ BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 –, Rn. 104 ff.

Nach dem Entwurf sollen das BfV und der BND grundsätzlich alle vorhandenen Daten – mit Ausnahme der durch Wohnraumüberwachungen und „echte“ Online-Durchsuchungen erlangten Daten (vgl. § 36 Abs. 1 Satz 2 Nr. 2 BVerfSchG-E, § 52 Abs. 1 Satz 2 BNDG-E) – mit Hilfe komplexer Analysetechnik auswerten dürfen. Der Einsatz solcher Technik wird zweistufig reguliert:

Die Datenanalyse selbst soll sich nach den gesetzlichen Generalklauseln für die Weiterverarbeitung vorhandener Daten richten. Sie ist darum nach § 36 Abs. 1 Satz 2 BVerfSchG-E beziehungsweise § 52 Abs. 1 Satz 1 BNDG-E niedrighschwellig zulässig, wenn dies im Einzelfall zur Erfüllung der Aufgaben des BfV beziehungsweise zur nachrichtendienstlichen Auslandsaufklärung, also zur Aufgabenerfüllung des BND, erforderlich ist.

Erhöhte Anforderungen sieht der Entwurf erst auf der als Abruf bezeichneten zweiten Stufe vor. Der missverständliche³¹ Begriff des Abrufs wird in den vorgesehenen Regelungen nicht definiert. Aus der Entwurfsbegründung ergibt sich, dass unter einem Abruf die „Verfügbarkeit der Erkenntnis zur Weiterverarbeitung“³² beziehungsweise „der an eine inhaltliche Prüfung anschließende Verarbeitungsschritt, welcher das Auswertungsprodukt für die weitere Verwendung zugänglich macht“,³³ zu verstehen ist. Der Abruf wird in Fällen, in denen das Auswertungsprodukt besonders weitreichende oder sensible Informationen enthält, durch § 37 BVerfSchG-E und § 53 BNDG-E differenziert an qualifizierte Voraussetzungen gebunden.

Der zweistufige Regulierungsansatz hat somit zur Folge, dass das BfV und der BND zunächst weitgehend ohne konkreten Anlass nahezu beliebige Analysetechnik über ihre Datenbestände laufen lassen dürfen. Erst der Umgang mit den durch die Analyse erzeugten Erkenntnissen („Produkten“) wird strenger reguliert. Die Entwurfsbegründung führt hierzu insbesondere aus, erst mit dem Abruf und nicht schon durch den vorgelagerten vollautomatischen Auswertungsprozess erhöhe sich die Eingriffsintensität, sodass es einer qualifizierten Eingriffsschwelle bedürfe.³⁴ In der juristischen Literatur wird zudem vorgebracht, die Eingriffsintensität der Verarbeitung des Produkts lasse sich im Voraus nicht absehen.³⁵ Diese Argumentation überzeugt jedoch nicht. Der Regulierungsansatz des Entwurfs ist verfassungsrechtlich unzureichend, da er auch eine unzulässige „weder im Einzelfall durch einen konkreten Anlass getragene noch durch Vorgaben zur Verarbeitungsmethode inhaltlich eingeschränkte automatisierte Durchsuchung großer Bestände personenbezogener Daten auf bislang unbekannte Gesetzmäßigkeiten und gefahrenabwehrrechtlich bedeutende Zusammenhänge“³⁶ ermöglicht.

Zwar mag sich die Eingriffsintensität einer Datenanalyse mitunter erst an deren Ergebnis zeigen. Mit Blick auf solche Fälle ist es verfassungsrechtlich akzeptabel, eine prima facie nicht besonders eingriffsintensive Analysemethode unter niedrigen Voraussetzungen zuzulassen und erst die Weiterverarbeitung des Produkts strenger zu regulieren. Allerdings gibt es auch Analysemethoden, die von

³¹ Kritisch Hornung/Kostov, in: Dietrich u.a., Nachrichtendienstrecht im Wandel der Technik, im Erscheinen, unter III. 3. b).

³² BT-Drs. 21/7868, S. 289.

³³ BT-Drs. 21/7868, S. 470.

³⁴ So zu § 53 BNDG-E BT-Drs. 21/7868, S. 470.

³⁵ Zumindest in diese Richtung Hornung/Kostov, in: Dietrich u.a., Nachrichtendienstrecht im Wandel der Technik, im Erscheinen, unter IV. 2. b) bb).

³⁶ BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 –, Rn. 95.

vornherein auf die Gewinnung von hochgradig sensiblen Informationen gerichtet sind, sodass bei ihrem Einsatz in jedem Fall von einer hohen Eingriffsintensität auszugehen ist. Beispielsweise befassen sich § 37 Abs. 2 Nr. 1 lit. a BVerfSchG-E und § 53 Abs. 4 Nr. 2 BNDG-E mit Analysen, die gezielt zur „Gewinnung von tatsächlichen Anhaltspunkten für eine Beteiligung von Personen, zu denen individuell kein Anlass zu solcher Prüfung bestand“, beziehungsweise zur „Gewinnung von tatsächlichen Anhaltspunkten erstellt werden, dass eine Person, bei der individuell kein Anlass für eine Prüfung bestand, in einem Zusammenhang mit einer zumindest erheblichen Bedrohung steht, der Grund zu der Annahme gibt, dass durch die Aufklärung der Person auch Erkenntnisse über die Bedrohung gewonnen werden können“. Derartige Maßnahmen der gezielten Verdächtigengewinnung weisen in jedem Fall eine – ex ante ohne weiteres ersichtliche – hohe Eingriffsintensität auf. Sie sind darum auch im Rahmen der nachrichtendienstlichen Aufklärung nur bei einem herausgehobenen, hinreichend konkreten Anlass zulässig.³⁷ Es gibt keinen Grund, solche Datenanalysen niedrigschwellig zuzulassen, wenn die Weiterverarbeitung des Produkts in jedem Fall an qualifizierte Voraussetzungen gebunden werden muss. Eine solche Regelungstechnik schafft ohne erkennbaren Grund nicht hinnehmbare Risiken für die betroffenen Personen.

Darüber hinaus wirft der im Entwurf eher entgegen dem üblichen Sprachgebrauch verwendete, nicht legaldefinierte und aus sich heraus wenig klare Begriff des Abrufs die Frage auf, welche Weiterverarbeitungen von Analyseprodukten genau besonders reguliert werden und welche nicht. Wenn der Abruf die Datenverarbeitungshandlung sein soll, durch deren Regulierung die verfassungsrechtlichen Anforderungen an komplexe Datenanalysen umgesetzt werden, muss der Begriff des Abrufs auch alle hierfür relevanten Handlungen erfassen. Jedoch ist zumindest unklar, ob die gesetzlichen Abrufermächtigungen diesem Erfordernis genügen.

Insbesondere muss ausgeschlossen sein, dass das Produkt einer Datenanalyse für Folgehandlungen mit gehobenem Eingriffsgewicht genutzt wird, ohne dass ein Abruf stattfindet, dessen Regulierung diesem Eingriffsgewicht Rechnung trägt. Die vorgesehenen Regelungen weisen insoweit Leerstellen auf oder lassen zumindest Fragen offen. So soll zwar die automatisierte Veranlassung bestimmter Anschlussmaßnahmen nur ausnahmsweise zulässig sein. Insoweit bedarf es also vor den betreffenden Anschlussmaßnahmen eines Abrufs nach Maßgabe der Abrufermächtigungen. Diese Regelungen beziehen sich jedoch nicht auf alle denkbaren Handlungen, die an die Generierung eines Analyseprodukts anknüpfen: § 37 Abs. 6 BVerfSchG-E schließt lediglich „Schutzmaßnahmen“ grundsätzlich aus. Der strenger gefasste § 53 Abs. 7 BNDG-E bezieht sich auf Datenerhebungen und bestimmte aktionelle Maßnahmen. Beide Normen lassen jedoch offen, ob und inwieweit eine automatisierte Durchführung anderer Anschlusshandlungen ohne vorherigen Abruf zulässig ist. Vielmehr nennt die Entwurfsbegründung zu § 37 BVerfSchG-E sogar ausdrücklich eine „automatisierte Neuqualifikation“ als zulässiges Szenario, die anscheinend auch durch einen „technischen Hintergrundprozess“ ohne Abrufqualität bewirkt werden kann.³⁸ Eine solche Neuqualifikation, etwa – so

³⁷ Vgl. zur präventivpolizeilichen Rasterfahndung, die einen gleichläufigen Zweck verfolgt und nur zur Abwehr einer konkreten (nicht konkretisierten) Gefahr zulässig ist, BVerfGE 115, 320 (356 ff.); BVerfG, Beschluss vom 9. Dezember 2022 – 1 BvR 1345/21 –, Rn. 186 ff.

³⁸ BT-Drs. 21/7868, S. 288. Die Begründung zu § 53 BNDG-E ist insoweit weniger klar, geht aber anscheinend gleichfalls davon aus, dass ein Abruf erst bei einer „Kenntnisnahme durch Mitarbeitende des

das Beispiel in der Entwurfsbegründung – von einem Beteiligungsverdacht zur gesicherten Beteiligung, kann für die betroffene Person erhebliche Folgen haben, indem sich Speicherfristen verlängern oder die Wahrscheinlichkeit von Anschlussmaßnahmen steigt. Sie kann daher nicht als Grundrechtseingriff niedrigeren Gewichts durch die Generalklauseln zur Weiterverarbeitung gerechtfertigt werden.

Nicht überzeugend erscheint schließlich, dass die qualifizierenden Abrufvoraussetzungen in § 53 BNDG-E von vornherein nur zum Schutz von Inländern greifen. Auch wenn – nicht unproblematisch, aber im Einklang mit der Binnenlogik des BNDG-E – eine generelle Absenkung des grundrechtlichen Schutzniveaus für Ausländer im Ausland akzeptiert wird, geht es zu weit, Abrufe ihnen gegenüber unabhängig vom Eingriffsgewicht des Produkts nur an die niedrigen Voraussetzungen des § 52 Abs. 1 Satz 1 BNDG-E zu binden.

Zusammenfassend müssen daher ex ante eingriffsintensive Analysen bereits in der Auswertungsphase an qualifizierte Anforderungen gebunden werden. Zudem muss der Begriff des Abrufs präzisiert werden, um alle angezeigten Fallkonstellationen (Datenerhebungen, aktionelle Maßnahmen und Datenveränderungen mit intensitätssteigernder Wirkung) zu erfassen, in denen das Eingriffsgewicht des Auswertungsprodukts relevant ist.

Um die Verwendung³⁹ komplexer Analysetechnik kontrollierbar zu halten, ist darüber hinaus eine vorherige Dokumentation der eingesetzten Analysemethoden und der damit verfolgten Analysezwecke geboten, wie sie § 41 BVerfSchG-E, nicht aber die Parallelregelung in § 61 BNDG-E vorsieht.

III. Datenübermittlungen

1. Übermittlungsbefugnisse des BfV

a) Datenübermittlung zum administrativen Rechtsgüterschutz

Die in § 47 Abs. 1 BVerfSchG-E vorgesehenen Erweiterungen der geltenden Ermächtigung zu Datenübermittlungen zum administrativen Rechtsgüterschutz (§ 20 BVerfSchG) stehen mit den verfassungsrechtlichen Vorgaben teils nicht in Einklang.

Wenn ein Nachrichtendienst personenbezogene Daten, die er durch Grundrechtseingriffe oberhalb einer Bagatellschwelle erlangt hat, an eine Behörde übermittelt, die über operative Anschlussbefugnisse verfügt – also unmittelbar Verhaltensfreiheit oder Eigentum von Personen beschränken darf⁴⁰ –, so handelt es sich um einen eigenständigen schwerwiegenden Grundrechtseingriff. Hierunter fallen alle in § 47 Abs. 1 BVerfSchG-E geregelten Datenübermittlungen. Nimmt die Empfangsbehörde

Bundesnachrichtendienstes“ vorliegt, sodass rein automatisierte Vorgänge nicht unter diesen Begriff fallen, vgl. BT-Drs. 21/7868, S. 470.

³⁹ Vgl. daneben zu der Regulierung der hier nicht erörterten Trainingsphase Hornung/Kostov, in: Dietrich u.a., Nachrichtendienstrecht im Wandel der Technik, im Erscheinen, IV. 2. a).

⁴⁰ Vgl. zum verfassungsrechtlichen Begriff der operativen Befugnis unter Korrektur zwischenzeitlich in der juristischen Literatur aufgekommener Missverständnisse BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, Rn. 230 f.

Aufgaben des präventiven Rechtsgüterschutzes wahr, so muss die Übermittlung grundsätzlich mindestens an eine konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut gebunden werden.⁴¹

Eine Ausnahme von diesem Grundsatz hat das Bundesverfassungsgericht in seinem Beschluss zum Hessischen Verfassungsschutzgesetz angenommen, wenn eine Übermittlung „auf [...] Ersuchen [der Empfangsbehörde] oder zur Erfüllung einer dieser gegenüber bestehenden Nachberichts- oder Unterrichtungspflicht im Rahmen personen- oder gruppenbezogener Risikoprävention“ erfolge. In „gesetzlich geregelten, herausgehobenen Zusammenhängen mit besonders hohem Gefahrenpotential für hochrangige Rechtsgüter und einer engen Verbindung zu den Schutzgütern des Verfassungsschutzes“ sei dann „auf Grundlage entsprechender tatsächlicher Anhaltspunkte im Einzelfall eine Übermittlung grundsätzlich möglich“. Als Anwendungsfälle nennt das Gericht Übermittlungen zu „Prüfzwecken im Waffen- oder Luftsicherheitsrecht sowie bei personenbezogenen Eignungs- oder Sicherheitsüberprüfungen im öffentlichen Dienst oder in den Fällen, in denen – basierend auf der verfassungsrechtlichen Grundentscheidung für eine wehrhafte Demokratie (vgl. Art. 9 Abs. 2, Art. 18, Art. 21 GG) – schon einer nur potentiellen Gefährdung der freiheitlichen demokratischen Grundordnung begegnet werden soll, wie etwa der Vorbereitung von Vereinsverboten“.⁴²

Die in § 47 Abs. 1 BVerfSchG-E vorgesehenen Übermittlungsermächtigungen, die durchweg nicht an eine konkretisierte Gefahr anknüpfen, gehen über diese Ausnahme teils deutlich hinaus.

Die behördlichen Aufgaben nach dem Staatsangehörigkeitsrecht (§ 47 Abs. 1 Nr. 3 lit. a BVerfSchG-E) und dem Aufenthaltsrecht (§ 47 Abs. 1 Nr. 5 BVerfSchG-E), die Gewerbeaufsicht (§ 47 Abs. 1 Nr. 8 BVerfSchG-E) und die Finanzdienstleistungsaufsicht (§ 47 Abs. 1 Nr. 9 BVerfSchG-E) wiegen nicht generell schwer genug und weisen nicht generell eine hinreichend enge Verbindung mit den Schutzgütern des Verfassungsschutzes auf, um eine Übermittlung unterhalb der Schwelle der konkretisierten Gefahr zu rechtfertigen. Ein Abweichen von dieser allgemeinen Schwelle kommt nur in Betracht, soweit diese Regime des Sonderordnungsrechts Eingriffsmaßnahmen zum Schutz hochrangiger Rechtsgüter gerade an eine personenbezogene Eignungs- oder Zuverlässigkeitsprüfung binden. Darüber hinaus bedarf es teils eines in der Übermittlungsermächtigung niederzulegenden näheren Bezugs zu den Schutzgütern des Verfassungsschutzrechts, wie ihn das geltende Recht für das Gewerbe (Beschränkung auf das Sicherheitsgewerbe) und für die Finanzdienstleistungsaufsicht (Beschränkung auf die Terrorismusfinanzierung) vorsieht. Diese Bezugnahmen mögen sich noch ausbauen lassen. Eine pauschale Absenkung der Übermittlungsschwelle, wie sie der Entwurf vorsieht, kommt mit Blick auf die genannten behördlichen Aufgaben jedoch nicht in Betracht.

Generell keinen Grund für eine Absenkung der Eingriffsschwelle gibt es mit Blick auf die Versammlungsaufsicht (§ 47 Abs. 1 Nr. 3 lit. c BVerfSchG-E). Eingriffsmaßnahmen der Versammlungsbehörden knüpfen nicht an personen- oder gruppenbezogene Risiken an – dies wäre vor dem Hintergrund von Art. 8 GG auch nicht verfassungsgemäß –, sondern setzen eine konkrete Gefahr oder eine besonders normierte, gleichfalls konkrete Krisenlage voraus (vgl. § 5, § 12a Abs. 1 Satz 1, § 13 Abs. 1

⁴¹ BVerfG, Urteil vom 22. April 2022 – 1 BvR 1619/17 –, Rn. 245 ff., 258; Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, Rn. 107 ff., 111.

⁴² BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, Rn. 113.

Satz 1, § 15 VersammlG). Es ist daher ausreichend und verfassungsrechtlich geboten, Datenübermittlungen vom BfV an eine Versammlungsbehörde an das allgemeine Erfordernis einer konkretisierten Gefahr zu binden.

Viel zu unbestimmt und zu weit gefasst ist schließlich die in § 47 Abs. 1 Nr. 11 BVerfSchG-E vorgesehene Übermittlungsermächtigung zur Verhinderung der Beschaffung von Mitteln, die geeignet und dazu bestimmt sind, die Ausführung von wenigstens erheblich beobachtungsbedürftigen Bedrohungen erheblich zu fördern. Der Übermittlungsempfänger und die konkreten Maßnahmen, denen die Übermittlung dienen soll, bleiben in dieser Norm weitgehend offen. Eine nähere tatbestandliche Begrenzung wäre jedoch bereits darum erforderlich, weil die Beschaffung von Mitteln zur Ausführung erheblich beobachtungsbedürftiger Bedrohungen eine legale Tätigkeit darstellen kann, zu deren unmittelbarer wie mittelbarer Verhinderung die hoheitliche Gewalt nicht berufen ist. Erst recht gibt es keinen Grund, Übermittlungen zu diesem Ziel ohne besondere Eingriffsschwelle potenziell bereits weit im Vorfeld konkretisierter Gefahren zuzulassen.

b) Datenübermittlung zur Strafverfolgung

Die vorgesehene Ermächtigung zu Datenübermittlungen zur Strafverfolgung in § 48 BVerfSchG-E steht weitgehend, aber nicht vollständig mit den verfassungsrechtlichen Anforderungen in Einklang.

Nach der Rechtsprechung des Bundesverfassungsgerichts ist eine Übermittlung nachrichtendienstlich erlangter Daten nur zur Verfolgung einer besonders schweren Straftat zulässig.⁴³ In erster Linie sind besonders schwer solche Straftaten, deren Strafraum eine Höchststrafe von mehr als fünf Jahren Freiheitsstrafe umfasst.⁴⁴ Daneben kann eine Straftat mit einer angedrohten Höchstfreiheitsstrafe von mindestens fünf Jahren auch dann als besonders schwer eingestuft werden, „wenn dies nicht nur unter Berücksichtigung des jeweils geschützten Rechtsguts und dessen Bedeutung für die Rechtsgemeinschaft, sondern auch unter Berücksichtigung der Tatbegehung und Tatfolgen vertretbar erscheint“.⁴⁵ Allerdings „können Straftaten nicht allein deshalb als besonders schwer angesehen werden, weil sie für bestimmte Kriminalitätsfelder typisch sind, wenn in diesem Feld sowohl schwere als auch leichte Straftaten begangen werden können. Erforderlich ist stets, dass sich insbesondere eine bestimmte Begehungsform im Tatbestand selbst niederschlägt und zugleich das besonders schwere Unrecht der Tat begründet“.⁴⁶ Dies gilt insbesondere auch für Staatsschutzdelikte, selbst wenn diese „besonders gewichtige Rechtsgüter mit hoher Bedeutung für die Rechtsgemeinschaft“ schützen.⁴⁷ Dementsprechend sind Staatsschutzdelikte oder sonstige im Einzelfall gegen Verfassungsschutzgüter gerichtete Delikte nicht etwa „aus einem übergreifenden präventiven Interesse an der Strafverfolgung im Aufgabenbereich der Verfassungsschutzbehörden im Sinne einer ‚materialen Auftragskontinuität‘ bei der Übermittlung privilegiert [...], so dass letztlich alle Straftaten, die gegen die Schutzgüter des § 3 Abs. 1 BVerfSchG gerichtet sind, übermittlungsfähig wären“.⁴⁸

⁴³ BVerfG, Urteil vom 22. April 2022 – 1 BvR 1619/17 –, Rn. 251; BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, Rn. 110, 201 ff.

⁴⁴ BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, Rn. 203 f.

⁴⁵ BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, Rn. 205.

⁴⁶ BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, Rn. 207.

⁴⁷ BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, Rn. 208.

⁴⁸ BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, Rn. 210.

Nach diesen Maßstäben bestehen keine verfassungsrechtlichen Bedenken gegen die Übermittlungsermächtigung in § 48 Abs. 1, Abs. 2 Nr. 1 BVerfSchG-E, die vom gesetzlichen Strafraumen ausgeht. Auch die Ermächtigung in § 48 Abs. 1, Abs. 2 Nr. 2 BVerfSchG-E zu Datenübermittlungen zur Verfolgung der in der Anlage zum BVerfSchG-E aufgezählten Straftaten, die im Höchstmaß mit Freiheitsstrafe von lediglich fünf Jahren bedroht sind, ist weitgehend verfassungskonform. Allerdings nennt die Anlage einzelne Straftatbestände, die nach den Kriterien des Bundesverfassungsgerichts nicht als besonders schwere Straftaten eingeordnet werden können.

Dies gilt insbesondere für die Verunglimpfung des Bundespräsidenten (§ 90 Abs. 1 und 3 StGB, Nr. 8 der Anlage) und die Verunglimpfung des Staates und seiner Symbole für extremistische Bestrebungen (§ 90a Abs. 3 StGB, Nr. 9 der Anlage), die zwar einen Staatsschutzbezug aufweisen, aber als reine Kommunikationsdelikte ausgestaltet sind. Ein Verstoß gegen diese Straftatbestände setzt eine besondere Beeinträchtigung oder zumindest Gefährdung staatsschutzrelevanter Rechtsgüter weder voraus noch führt er sie typischerweise herbei. Verfassungsrechtlich noch vertretbar erscheint mir hingegen die Einbeziehung der verfassungsfeindlichen Verunglimpfung von Verfassungsorganen (§ 90b Abs. 1 StGB, Nr. 10 der Anlage), da diese Norm tatbestandlich eine das Ansehen des Staates gefährdende Handlungsweise voraussetzt. Dass sich eine solche Gefährdung in der Praxis kaum je begründen lassen wird und ohnehin angesichts des grundrechtlichen Schutzes der Machtkritik Meinungsäußerungen allenfalls in seltenen Ausnahmefällen die Tatbestände von §§ 90 ff. StGB verwirklichen,⁴⁹ ist bei der Anwendung der Übermittlungsermächtigung zu beachten.

c) Datenübermittlung an nicht-öffentliche Stellen

Zu weit gefasst ist schließlich die vorgesehene Ermächtigung zu Datenübermittlungen an nichtöffentliche Stellen in § 50 BVerfSchG-E, soweit sie über die gegenwärtige Rechtslage (§ 22a BVerfSchG) hinausgeht.

Die in § 50 Abs. 1 Nr. 4 und 5 BVerfSchG-E vorgesehenen Übermittlungsermächtigungen verfolgen im Kontext des Verfassungsschutzrechts bereits keinen legitimen Zweck. Sie sollen dem BfV ermöglichen, bestimmte Gewerbetreibende oder Organisationen über einzelne Beteiligte von Bedrohungen zu informieren. Auf der Grundlage dieser Information sollen die Übermittlungsempfänger eine „informierte Entscheidung in gesellschaftlicher Verantwortung“ über die „objektive Förderung“ dieser Bedrohungen treffen können.⁵⁰

Dieser Übermittlungszweck ist von den Aufgaben des Verfassungsschutzes nicht umfasst. Der Verfassungsschutz dient zum einen als strukturorientiertes Frühwarnsystem für Politik und Gesellschaft, zum anderen als Informationsdienstleister für die Sicherheitsgewähr durch andere Behörden und subsidiär durch Private. Eine unmittelbare und zielgerichtete Störung der geschäftlichen, politischen, kulturellen und privaten sozialen Beziehungen einzelner Personen, wie sie durch § 50 Abs. 1 Nr. 4 und 5 BVerfSchG-E angelegt wird, wechselt die Bezugsebene und lässt sich entgegen der Entwurfsbegründung nicht mehr als „Verfassungsschutz durch Aufklärung“ auf der Linie der jährlichen

⁴⁹ So hat das Bundesverfassungsgericht Verfassungsbeschwerden gegen Eingriffsmaßnahmen, die sich auf § 90a StGB stützten, in allen veröffentlichten Entscheidungen nach BVerfG (Vorprüfungsausschuss), NJW 1985, 263, stattgegeben, vgl. BVerfGE 81, 278; 81, 298; BVerfG (K), NJW 1999, 204; NJW 2001, 596; NJW 2009, 908; NJW 2012, 1273; BVerfG (K), Beschluss vom 9. Juli 2008 – 1 BvR 519/08.

⁵⁰ BT-Drs. 21/7868, S. 302.

Verfassungsschutzberichte darstellen. Es geht hier gerade nicht mehr um Aufklärung der Gesellschaft über verfassungsfeindliche Bestrebungen in allgemeiner Form, sondern um das gezielte „Anschwärzen“ Einzelner in ihrem persönlichen Umfeld.

Insbesondere ist zu beachten, dass das BfV Informationen über die betreffenden Personen in Fällen, in denen ein rechtswidriges Verhalten droht oder sich sonst eine konkretisierte Gefahr abzeichnet, in weitem Umfang nach den anderen Übermittlungsermächtigungen des geltenden wie des vorgesehenen Verfassungsschutzrechts auch an nichtöffentliche Stellen weiterleiten kann. In § 50 Abs. 1 Nr. 4 und 5 BVerfSchG-E geht es demgegenüber zumindest in erster Linie um eine Übermittlung von Informationen über Personen, die sich im Rahmen der betreffenden sozialen Kontakte legal verhalten. Durch den intendierten Appell an ihre „gesellschaftliche Verantwortung“ werden die Übermittlungsempfänger dahingehend beeinflusst, dass sie diese Kontakte abbrechen sollen. Hieran ändert es nichts, dass die Entscheidung über den Abbruch bei den Übermittlungsempfängern verbleibt, zumal diese mitunter nicht ganz grundlos befürchten werden, ansonsten selbst in die Beobachtung einbezogen, im Extremfall sogar Objekt von „Schutzmaßnahmen“ zu werden.

Der Umgang privater Einrichtungen mit (möglichen) Beteiligten von Bedrohungen ist, soweit es nicht um konkretisierte Gefahren oder sonst sich abzeichnende Schäden für Rechtsgüter geht, kein Thema der hoheitlichen Sicherheitsgewähr. Es geht hier um eine weitergehende Steuerung zulässigen Verhaltens und erlaubter sozialer Beziehungen, die besonders rechtfertigungsbedürftig und jedenfalls dem behördlichen Verfassungsschutz auf der individuellen Ebene nicht anvertraut ist.

2. Übermittlungsbefugnisse des BND

a) Datenübermittlung zur Strafverfolgung

Die vorgesehene Übermittlungsermächtigung in § 81 BNDG-E stimmt weitgehend mit § 48 BVerfSchG-E überein und reicht daher ebenfalls teils zu weit (siehe oben III. 1. b)).

b) Datenübermittlung zur Gefahrenabwehr

Die vorgesehene Übermittlungsermächtigung in § 82 Abs. 1 Satz 1 BNDG-E setzt eine zumindest konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut voraus und erscheint daher auf den ersten Blick unbedenklich. Jedoch wird die Ermächtigung dadurch bedenklich ausgedehnt, dass zu den besonders wichtigen Rechtsgütern gemäß § 2 Abs. 2 Nr. 3 BNDG-E auch die außenpolitische Handlungsfähigkeit der Bundesrepublik gehört. Diese wenig klare Formulierung soll nach der Entwurfsbegründung im Ergebnis alle außenpolitischen Interessen umfassen (siehe oben I. 2. a)). Eine konkretisierte Gefahr für die außenpolitische Handlungsfähigkeit der Bundesrepublik ließe sich daher bereits bejahen, wenn ein zumindest in groben Konturen absehbares Ereignis diese Interessen in irgendeiner Weise beeinträchtigen könnte. Damit ist jedoch nicht in jedem Fall ein drohender Schaden beschrieben, der den verfassungsrechtlichen Anforderungen an den Rechtsgüterschutz genügt.

Die Entwurfsbegründung erkennt die Operationalisierungsprobleme, die das Erfordernis einer konkretisierten Gefahr für die außenpolitische Handlungsfähigkeit und auch für die anderen „eher abstrakten“ Kollektivgüter wie die freiheitliche Grundordnung oder die Sicherheit des Bundes, eines Landes oder einer internationalen Organisation aufwirft. Sie will hieraus jedoch den Schluss ziehen, dass der Begriff der konkretisierten Gefahr in Verbindung mit diesen Rechtsgütern extensiv zu verstehen sei, sodass ein „mittelbarer Bezug, der daraus entsteht, dass die tatbestandliche Verwirklichung sich gegen diese Schutzgüter richtet“, ausreichen soll. Als Beispiel nennt die Entwurfsbegründung

eine drohende Sachbeschädigung, die gegen eine Botschaft gerichtet ist. Hierin liege eine konkretisierte Gefahr für die außenpolitische Handlungsfähigkeit der Bundesrepublik.⁵¹ Auf diese Weise wird ein bevorstehendes Bagatelldelikt in die bevorstehende Schädigung eines besonders gewichtigen Rechtsguts umgedeutet.

Diese Ausführungen in der Entwurfsbegründung zeigen die verfassungsrechtlich nicht hinnehmbare Ausdehnungstendenz exemplarisch auf, die eine Bezugnahme insbesondere auf die außenpolitische Handlungsfähigkeit im Rahmen einer Ermächtigung zur Gefahrenabwehr mit sich bringt.⁵² Andererseits ist nicht erkennbar, in welchen Fällen eine drohende Beeinträchtigung der außenpolitischen Handlungsfähigkeit ein besonders gewichtiges Rechtsgut gefährden soll, ohne dass zugleich eines der anderen Rechtsgüter des § 2 Abs. 2 BNDG-E gefährdet ist. Wenn daher an diesem Rechtsgut überhaupt festgehalten werden soll, muss es jedenfalls aus der Übermittlungsermächtigung in § 82 Abs. 1 Satz 1 BNDG-E ausgeklammert werden.

c) Datenübermittlung im Gefahrenvorfeld

§ 83 BNDG-E ermöglicht Datenübermittlungen an Behörden mit operativen Anschlussbefugnissen unterhalb der Schwelle einer konkretisierten Gefahr. Die vorgesehene Regelung beschränkt – ähnlich wie die Parallelnorm in § 47 BVerfSchG-E (siehe oben III. 1. a)) – die geregelten Übermittlungen nicht durchweg auf herausgehobene Rechtsgutsgefährdungen und verfehlt daher zum Teil die verfassungsrechtlichen Anforderungen.

Die Ermächtigung zu Übermittlungen mit dem Ziel, ein Lagebild zu erstellen (§ 83 Abs. 1 Nr. 1 BNDG-E) beschreibt ein allgemeines behördliches Anliegen, das weder durchweg besonders gewichtig ist noch in einem spezifischen Zusammenhang zu den durch den BND geschützten Rechtsgütern steht. Hinnehmbar wäre sie allenfalls, wenn eine Nutzung der so entstandenen Lagebilder für operative Anschlussmaßnahmen eng begrenzt würde. Gerade dies ist jedoch nach der Entwurfsbegründung nicht intendiert.⁵³

Die Ermächtigungen zur Unterstützung von Aufgaben nach dem Staatsangehörigkeitsrecht (§ 83 Abs. 1 Nr. 2 BNDG-E) und dem Aufenthaltsrecht (§ 83 Abs. 1 Nr. 3 BNDG-E) entsprechen § 47 Abs. 1 Nr. 3 lit. a BVerfSchG-E und § 47 Abs. 1 Nr. 5 BVerfSchG-E und weisen dieselben Mängel auf (siehe oben III. 1. a)).

IV. Aktionelle Maßnahmen

Der Entwurf soll dem BfV und dem BND erstmals aktionelle Maßnahmen erlauben, mit denen sie schadensträchtige Kausalverläufe unmittelbar beeinflussen können. Die vorgesehenen Ermächtigungen sind differenziert zu beurteilen. Die geplante Befugnis des BfV zu „Schutzmaßnahmen“ ist rechtsstaatlich nicht vertretbar. Die Ermächtigung des BND zu „erweiterten nachrichtendienstlichen Maßnahmen“ lässt sich durch – allerdings nicht unerhebliche – Änderungen verfassungskonform

⁵¹ BT-Drs. 21/7868, S. 386.

⁵² Allgemein zu den Bedenken gegen eine polizeirechtliche Inbezugnahme von Kollektivgütern Bäcker, Kriminalpräventionsrecht, 2015, S. 310 ff.

⁵³ Vgl. BT-Drs. 21/7868, S. 496.

ausgestalten. Im Übrigen muss der BND innerstaatlich verbindliche völkerrechtliche Vorgaben beachten, die seinen Spielraum für solche Maßnahmen deutlich einengen.

1. „Schutzmaßnahmen“ des BfV

Im Ganzen und ohne Möglichkeit einer Nachbesserung verfassungswidrig ist die vorgesehene Ermächtigung des BfV zu „Schutzmaßnahmen“ in §§ 59 ff. BVerfSchG-E. Diese Ermächtigung ermöglicht dem BfV weitreichende Eingriffe in Verhaltensfreiheit und Eigentum, die gegenüber den betroffenen Personen dauerhaft geheim gehalten werden. Dies ist schon im Ansatz rechtsstaatlich unvertretbar. Selbst wenn eine solche Ermächtigung im deutschen Recht überhaupt vorstellbar wäre, wiese jedenfalls die konkrete Ausgestaltung im Gesetzentwurf zahlreiche, teils unbehebbarer verfassungsrechtliche Mängel auf. §§ 59 ff. BVerfSchG müssen daher ersatzlos gestrichen werden.

a) Regelungsgehalt und Reichweite von §§ 59 ff. BVerfSchG-E

Die vorgesehene Ermächtigung zu „Schutzmaßnahmen“ erlaubt potenziell eine große Vielfalt aktioneller Maßnahmen über einen beträchtlichen Zeitraum.

Das BfV darf „Schutzmaßnahmen“ durchführen, wenn es zunächst eine besondere Bedrohung im Sinne von § 59 Abs. 3 BVerfSchG-E festgestellt hat. Diese Feststellung setzt gegenüber dem allgemeinen Begriff der Bedrohung (§ 3 Abs. 4 BVerfSchG-E) eine hinsichtlich des Schadenspotenzials qualifizierte Bedrohung voraus, hingegen nach dem Gesetzeswortlaut keine besonders verdichtete Bedrohungslage. Es muss also insbesondere noch kein konkretes Geschehen absehbar sein, in dem sich das besondere Schadenspotenzial zu verwirklichen droht.⁵⁴ So kommt es nach der Entwurfsbegründung für eine terroristische Bedrohung im Sinne von § 59 Abs. 3 Nr. 1 BVerfSchG-E nicht darauf an, dass die Beteiligten bereits konkrete terroristische Straftaten planen. Ausreichend ist vielmehr, dass sie (mutmaßlich) den Übergang zu einem terroristischen *Modus Operandi* planen.⁵⁵ Dementsprechend kann die Bedrohung über einen längeren Zeitraum andauern – nach § 60 Abs. 2 BVerfSchG-E ist die Einstufung auf bis zu ein Jahr zu befristen, wobei nach Fristablauf eine erneute Einstufung möglich ist.

Die Anordnung einer „Schutzmaßnahme“ setzt des Weiteren nach § 59 Abs. 1 Satz 1 BVerfSchG-E voraus, dass die Einwirkung erforderlich ist, um eine von der betreffenden Bedrohung ausgehende Gefährdung für ein besonders gewichtiges Rechtsgut abzuwenden. Diese Voraussetzung geht über das stets zu beachtende Erforderlichkeitsgebot nicht erkennbar hinaus. Insbesondere liegt es fern, den Begriff der Gefährdung synonym mit dem polizeirechtlichen Begriff der (konkreten) Gefahr zu verstehen. Dieser Begriff beschreibt vielmehr lediglich das Potenzial der Bedrohung, ein Rechtsgut tatsächlich zu verletzen.⁵⁶ Ebenso ergeben sich aus dem Erfordernis, dass ein besonders

⁵⁴ Vgl. gleichläufig die Entwurfsbegründung, BT-Drs. 21/7868, S. 307 f.

⁵⁵ BT-Drs. 21/7868, S. 307.

⁵⁶ So in der Sache auch die Entwurfsbegründung, BT-Drs. 21/7868, S. 307: Der Schutz müsse „strukturell ansetzen, darf sich nicht allein auf die Verhinderung eines isolierten Einzelereignisses ausrichten, sondern muss das Aktionspotenzial der operierenden Strukturen vorzugsweise insgesamt schwächen, dadurch dann auch die Realisierung jeden einzelnen künftigen Angriffs erschweren, hierdurch auch Angriffe verhindern und Schadenspotenzial eingrenzen.“

gewichtiges Rechtsgut betroffen sein muss, keine zusätzlichen Voraussetzungen, da die einstuftungsfähigen Bedrohungen ohnehin stets solche Rechtsgüter gefährden.

Eine „Schutzmaßnahme“ ist des Weiteren zwar nach § 59 Abs. 1 Satz 2 BVerfSchG-E nur subsidiär zulässig. Die Voraussetzungen der Subsidiaritätsklausel werden jedoch häufig erfüllt sein:

Nach § 59 Abs. 1 Satz 2 Nr. 1 BVerfSchG-E sind „Schutzmaßnahmen“ zulässig, wenn ihr Zweck durch Einwirkung einer anderen Stelle nicht erreicht werden kann. Maßnahmen anderer Stellen werden insbesondere in akuten Krisenlagen in Betracht kommen, in denen der polizeiliche Handlungskreis eröffnet ist. „Schutzmaßnahmen“ sollen jedoch ausweislich der Entwurfsbegründung gerade auch unabhängig von solchen Krisenlagen durchgeführt werden und strukturell wirken, verfolgen also Zwecke, die der polizeilichen Tätigkeit zumindest tendenziell fremd sind. In einer derartigen Vorfeldlage können hingegen bereits Befugnisse von Sonderordnungsbehörden bestehen, etwa der Gewerbeaufsicht oder der Migrationsverwaltung. Solche Befugnisse werden allerdings den Zweck einer „Schutzmaßnahme“ vielfach dann nicht erreichen können, wenn der Zweck gerade auch darin gesehen wird, eine Gefährdung zu entschärfen, ohne die Betroffenen zu warnen, um so weitere Erkenntnisse gewinnen zu können.

Zudem lässt § 59 Abs. 1 Satz 2 Nr. 2 BVerfSchG-E „Schutzmaßnahmen“ auch zu, wenn eine Übermittlung der zur Abwehr erforderlichen Informationen nach § 51 BVerfSchG-E nicht möglich ist. Aufgerufen ist damit insbesondere der durch § 51 Abs. 1 Nr. 2 BVerfSchG-E gewährleistete Quellen- und Methodenschutz. Ob die verbreitete Annahme zutrifft, dass das BfV sich derzeit eher häufig auf diesen Ausschlussstatbestand beruft, mag hier dahinstehen. Jedenfalls enthält § 51 Abs. 1 Nr. 2 BVerfSchG-E mit den „überwiegenden Sicherheitsinteressen“ einen unbestimmten Rechtsbegriff, dessen Auslegung im Wesentlichen in der Hand des BfV liegt. Die Verfügbarkeit von „Schutzmaßnahmen“ könnte rein tatsächlich einen Anreiz zu einer eher (zu) großzügigen Interpretation setzen, zumal der Entwurf die im gegenwärtigen Recht enthaltenen Klarstellungen in § 23 Abs. 1 Nr. 4 BVerfSchG und die Unterrichtungspflicht in § 23 Abs. 2 BVerfSchG streichen will.

Der Kreis der in Betracht kommenden „Schutzmaßnahmen“ wird in § 59 Abs. 2 BVerfSchG-E überaus weit gefasst. Insbesondere erlaubt § 59 Abs. 2 Satz 1 Nr. 1 BVerfSchG-E generell ein „Einwirken“ auf „Gegenstände, die für die Bedrohung gegenwärtig oder absehbar eingesetzt werden“. Die anschließend katalogartig aufgezählten Einwirkungsmodi sind lediglich Beispiele. Sie verdeutlichen allerdings, dass als „Gegenstand“ jedes manipulierbare Objekt in Betracht kommt, also neben physischen Sachen auch etwa Informationen oder Informationszusammenhänge sowie virtuelle Entitäten jeder Art. Ein Gegenstand muss auch nicht in einem engeren Sinne als (potenzielles) Tatmittel einzustufen sein, damit das BfV auf ihn einwirken kann, sondern nur überhaupt zu der Bedrohung beitragen können. Schließlich umfasst der Begriff des „Einwirkens“ jede Handlung, mit der ein solches Objekt manipuliert wird, also etwa gleichermaßen das Verändern, Sicherstellen oder Vernichten.

Darüber hinaus beschränkt § 59 Abs. 2 BVerfSchG-E den Kreis der von „Schutzmaßnahmen“ Betroffenen nicht, insbesondere nicht auf Beteiligte an der betreffenden Bedrohung im Sinne von § 3 Abs. 5 BVerfSchG-E. Die in der Entwurfsbegründung vertretene Auffassung, der (nicht abschließende) Maßnahmenkatalog impliziere „eine Beschränkung der Maßnahmerichtung auf

Verantwortliche der Bedrohungssituation“,⁵⁷ findet im Gesetzeswortlaut keine Stütze. Sie trifft in der Sache allenfalls dann zu, wenn als „verantwortlich“ jede Person angesehen wird, die als Betroffene einer „Schutzmaßnahme“ überhaupt in Betracht kommt, weil sie mit der Bedrohung in dem Sinne zu tun hat, dass eine Maßnahme ihr gegenüber etwas an der Bedrohung ändern kann. In diesem Sinne dürfte auch der terminologisch schiefe, aber instruktive Verweis der Entwurfsbegründung auf eine „Zustandsverantwortlichkeit“ zu verstehen sein.⁵⁸ Gleiches gilt für den Hinweis auf mögliche Manipulationen eines (potenziellen) Tatmittels auf der Lieferkette, der sich gleichfalls einer Parallelwertung zu den polizeirechtlichen Verantwortungskategorien entzieht.⁵⁹

Angesichts der weit im Gefahrvorfeld angesiedelten Voraussetzungen und des offenen Betroffenenkreises von „Schutzmaßnahmen“ schöpfen die gesetzlichen Beispielstatbestände wie auch die in der Entwurfsbegründung genannten Beispiele den potenziellen Anwendungsbereich von §§ 59 ff. BVerfSchG-E nicht aus. Als „Schutzmaßnahmen“ darstellbar sind etwa die heimliche Entziehung von physischen oder virtuellen Vermögensgegenständen, die für die Finanzierung einer Bedrohung genutzt werden könnten, die legendierte Veröffentlichung unzutreffender Informationen oder die Verfälschung bereits veröffentlichter Informationen, um die Beteiligten einer Bedrohung zu verunsichern oder auf eine falsche Fährte zu locken, die Beeinflussung sozialer Kontakte durch individualisierte Falschinformationen, um Zwietracht unter den Beteiligten einer Bedrohung zu säen, oder die Unbrauchbarmachung von Räumlichkeiten, die den Beteiligten einer Bedrohung als Treffpunkt oder Operationsbasis dienen.

Für die Kontrolle von „Schutzmaßnahmen“ finden sich Sonderregelungen. Gemäß § 60 Abs. 2 Satz 2 BVerfSchG-E unterliegt die Einstufung einer Bedrohung als besondere Bedrohung der Vorabkontrolle durch den Unabhängigen Kontrollrat. Für die Anordnung der einzelnen „Schutzmaßnahmen“ ist eine solche Vorabkontrolle hingegen gemäß § 60 Abs. 4 Satz 2 BVerfSchG-E nur in den Sonderfällen vorgesehen, dass das BfV zum Zweck der Einwirkung in ein privates informationstechnisches System eingreift oder heimlich eine Wohnung betritt. Stattdessen sieht § 62 BVerfSchG-E eine jährliche Kontrolle durch den Unabhängigen Kontrollrat und jährliche Berichte des Bundesministeriums des Innern und des Unabhängigen Kontrollrats an das Parlamentarischen Kontrollgremium vor. Im

⁵⁷ BT-Drs. 21/7868, S. 306.

⁵⁸ Der polizeirechtliche Begriff der Zustandsverantwortlichkeit passt auf „Schutzmaßnahmen“ von vornherein nicht, da die polizeirechtliche Verantwortlichkeit eine konkrete Gefahr voraussetzt. Darüber hinaus lässt sich der Begriff auf das Verfassungsschutzrecht auch nicht sinnvoll übertragen. Dem Verfassungsschutzrecht geht es um die Früherkennung von Bedrohungen, die von (individuellen oder aggregierten) menschlichen Handlungen ausgehen. Wer an solchen Handlungen zurechenbar – also nicht lediglich kausal – beteiligt ist, ist in polizeirechtlicher Terminologie Verhaltensstörer. Dies kann auch etwa für eine Person gelten, die einer anderen Person eine Sache überlässt, damit die Empfängerin die Sache zu Schädigungshandlungen einsetzen kann. Die an die reine Sachherrschaft anknüpfende Zustandsverantwortlichkeit erfasst hingegen in der Regel gerade nicht die Gefahr eines Missbrauchs der für sich genommen harmlosen Sache durch Dritte, näher Bäcker, in: Liskin/Denninger/ders., Handbuch Polizei- und Sicherheitsrecht, 8. Aufl. 2026, Kap. 3 Rn. 183 ff., m.w.N.

⁵⁹ Wer *zulässigerweise* eine Sache an jemanden liefert, der diese Sache sodann für sicherheitsgefährdende Handlungen nutzt, ist polizeirechtlich grundsätzlich weder Verhaltens- noch Zustandsstörer und kann nur unter den Voraussetzungen des polizeilichen Notstands in Anspruch genommen werden. Anders liegt es, wenn eine Rechtsnorm eine Verantwortlichkeit des Lieferanten positiv begründet, näher zu den Grenzen der Verantwortlichkeit in den Fällen der sogenannten Zweckveranlassung Bäcker, in: Liskin/Denninger/ders., Handbuch Polizei- und Sicherheitsrecht, 8. Aufl. 2026, Kap. 3 Rn. 164 ff., m.w.N.

Rahmen dieser „besonderen Kontrolle“ kann allerdings im Regelfall keine der Kontrollstellen verbindliche Entscheidungen über „Schutzmaßnahmen“ treffen, selbst soweit diese im Kontrollzeitpunkt noch andauern. Das Parlamentarische Kontrollgremium hat generell keine Weisungsrechte gegenüber den Nachrichtendiensten. Bei dem Unabhängigen Kontrollrat unterfällt die laufende Kontrolle von „Schutzmaßnahmen“ gemäß § 32 Abs. 1 Nr. 1 UKRatG-E der administrativen Kontrolle. Das administrative Kontrollorgan hat in diesem Rahmen gemäß § 33 Abs. 1 UKRatG-E eine Beanstandungsbefugnis, kann das BfV jedoch nicht verbindlich anweisen, bestimmte „Schutzmaßnahmen“ abzubrechen oder zu unterlassen. Eine Befassung des Senats nach § 34 UKRatG-E, in deren Rahmen solche Anweisungen möglich wären, ist für diese Fallkonstellation grundsätzlich nicht vorgesehen.

Vorstellbar erscheint, dass das gerichtsähnliche Kontrollorgan im Rahmen der Vorabkontrolle einer Einstufung als besondere Bedrohung Maßgaben und Einschränkungen für die Durchführung der darauf bezogenen „Schutzmaßnahmen“ nach § 27 Abs. 1 Satz 2 UKRatG-E vorsieht, die dann gegebenenfalls gemäß § 34 Abs. 1 Satz 2 Nr. 2 UKRatG-E Gegenstand eines Senatsverfahren werden könnten. Allerdings ist fragwürdig – und wird in den vorgesehenen Normen nicht klar geregelt, in der Entwurfsbegründung nicht einmal erwähnt –, ob die Vorabkontrolle der Einstufung überhaupt § 34 UKRatG-E unterfällt oder ob es sich um einen Fall der Einzelfallkontrolle im Sinne von § 29 UKRatG-E handelt, bei der derartige Maßgaben und Einschränkungen nicht vorgesehen sind. Maßgaben und Einschränkungen dürften jedenfalls möglich sein, soweit das gerichtsähnliche Kontrollorgan ausnahmsweise gemäß § 60 Abs. 2 Satz 2 BVerfSchG-E die Anordnung einzelner „Schutzmaßnahmen“ vorab zu kontrollieren hat.

Betroffene können theoretisch gegen „Schutzmaßnahmen“ verwaltungsgerichtlich mit einer Unterlassungs- oder Feststellungsklage vorgehen. Praktisch ist dies jedoch nahezu ausgeschlossen. Die Zulässigkeit einer solchen Klage setzt voraus, dass der Kläger eine konkrete vollzogene, andauernde oder bevorstehende Verwaltungshandlung benennen kann, die ihn möglicherweise in seinen Rechten verletzt hat, verletzt oder verletzen wird. Dies wird den Betroffenen von „Schutzmaßnahmen“ in aller Regel nicht möglich sein, da die Maßnahmen verdeckt durchgeführt werden und eine spätere Benachrichtigung im Gesetz nicht vorgesehen ist. Ein verwaltungsgerichtlicher Rechtsschutz gegen eine „Schutzmaßnahme“ kommt daher faktisch nur in Betracht, wenn der Betroffene zufällig von der Maßnahme erfährt, was das BfV nach Kräften zu vermeiden suchen wird. Die selbst in einem solchen Fall für den Betroffenen bestehenden Substantiierungs- und Nachweisprobleme seien lediglich erwähnt.

b) Rechtsstaatliche Unvertretbarkeit heimlicher Eingriffe in Freiheit und Eigentum

Das Vorbringen in der Entwurfsbegründung, „Schutzmaßnahmen“ sollten lediglich Schutzlücken schließen und verblieben ansonsten „im nachrichtendienstlichen Gepräge“,⁶⁰ überzeugt nicht. Sollten die vorgesehenen Regelungen in Kraft treten, so läge hierin ein Paradigmenwechsel, der das BfV als neuen Akteur der aktionellen Sicherheitsgewähr installiert, mit Befugnissen, über die keine andere deutsche Behörde verfügt. Hiervon sollte Abstand genommen werden. Die vorgesehene

⁶⁰ BT-Drs. 21/7868, S. 305.

Ermächtigung zu „Schutzmaßnahmen“ verletzt elementare rechtsstaatliche Grundsätze und ist verfassungsrechtlich unvertretbar.

„Schutzmaßnahmen“ können je nach betroffenem Gegenstand und Einwirkungsmodus an zahlreichen Grundrechten zu messen sein. Beispielsweise beeinträchtigt eine Manipulation von Sachen das Eigentum, berührt die Verbreitung personenbezogener Fehlinformationen das allgemeine Persönlichkeitsrecht oder kann die Beeinflussung von Kommunikationsprozessen durch falsche oder verfälschte Informationen in die Meinungsfreiheit eingreifen. Eingriffe in weitere Grundrechte wie Religionsfreiheit, Versammlungsfreiheit, Freizügigkeit oder Berufsfreiheit sind ebenfalls vorstellbar. Sie werden nicht dadurch ausgeschlossen, dass „Schutzmaßnahmen“ nach § 59 Abs. 2 Satz 2 BVerfSchG-E nicht durch unmittelbaren Zwang gegen Personen vollzogen werden dürfen, da alle diese Grundrechte auch gegen mittelbar-faktische Beeinträchtigungen schützen. Darüber hinaus können vorbereitende Handlungen etwa die Unverletzlichkeit der Wohnung oder das IT-System-Grundrecht berühren.

„Schutzmaßnahmen“ stellen somit, allgemein gesprochen, Eingriffe in Verhaltensfreiheit und Eigentum dar. Diese Eingriffe oder zumindest ihre hoheitliche Natur sollen den betroffenen Personen dauerhaft verborgen bleiben. Diese Vorgehensweise ist mit der demokratischen und rechtsstaatlichen Ordnung, wie sie das Grundgesetz errichtet, nicht vereinbar.

Die andauernde Heimlichkeit von „Schutzmaßnahmen“ enthält den betroffenen Personen die grundlegende Orientierung darüber vor, inwieweit die hoheitliche Gewalt auf ihre Rechte zugreift. Diese Orientierung hat einen demokratischen und rechtsstaatlichen Eigenwert. Der demokratische Rechtsstaat des Grundgesetzes zeichnet sich dadurch aus, dass er den Bürgerinnen und Bürgern nach Maßgabe rechtlicher Bindungen offen entgegentritt,⁶¹ so den Betroffenen hoheitlicher Eingriffsmaßnahmen ermöglicht, ihre Anliegen zu artikulieren, und sich individueller wie öffentlicher Kritik aussetzt.

Zudem ist die Kenntnis hoheitlicher Eingriffe in Verhaltensfreiheit und Eigentum elementare Voraussetzung dafür, dass die betroffenen Personen selbstbestimmt ihre Rechte durch behördliche und gerichtliche Rechtsschutzverfahren wahren können. Die Ermächtigung zu heimlichen „Schutzmaßnahmen“ nimmt den betroffenen Personen diese Möglichkeit und unterläuft so die Rechtsweggarantie des Art. 19 Abs. 4 GG praktisch umfassend.

Diesem Befund lässt sich nicht entgegenhalten, dass als Kompensation für den Ausfall des individuellen Rechtsschutzes eine Rechtskontrolle durch den Unabhängigen Kontrollrat eingerichtet ist. Da die Verfahren des Unabhängigen Kontrollrats ihrerseits geheim sind, können sie eine öffentliche Diskussion von vornherein nicht ersetzen. Darüber hinaus erfüllt eine Rechtskontrolle ohne Beteiligung der betroffenen Person nicht die Anforderungen, die Art. 19 Abs. 4 GG an den zu eröffnenden Rechtsweg stellt. Teil der Rechtsweggarantie ist die autonome Entscheidung darüber, ob und mit welchen prozessual verfügbaren Mitteln die betroffene Person gegen mögliche Rechtsverletzungen

⁶¹ Vgl. sogar mit Blick auf die Beschaffung von Informationen BVerfGE 118, 168 (197): „In einem Rechtsstaat ist Heimlichkeit staatlicher Eingriffsmaßnahmen die Ausnahme und bedarf besonderer Rechtfertigung.“

vorgehen will.⁶² Dementsprechend ist ihr eine aktive Stellung im gerichtlichen Verfahren einzuräumen. Nur so kann die betroffene Person ihr eigenes Tatsachenwissen und ihre rechtlichen Argumente in das Verfahren einbringen. Auch der systematische Vergleich mit Art. 10 Abs. 2 Satz 2 GG zeigt, dass der Ausschluss des Rechtswegs und seine Ersetzung durch ein Organ der objektiven Rechtskontrolle einer besonderen verfassungsrechtlichen Erlaubnis bedürfen.⁶³ Für den faktischen Ausschluss des Rechtswegs, der sich aus der dauerhaften Heimlichkeit hoheitlicher Grundrechtseingriffe ergibt, kann nichts anderes gelten.

Allerdings ließe sich eine Ermächtigung zu dauerhaft heimlichen „Schutzmaßnahmen“ angesichts des potenziellen Eingriffsgewichts solcher Maßnahmen nach meiner Einschätzung selbst durch verfassungsänderndes Gesetz nicht einführen, da eine solche Verfassungsänderung den durch Art. 79 Abs. 3 GG gewährleisteten Kernbestand des Demokratie- und des Rechtsstaatsprinzips sowie das aus der Menschenwürdegarantie folgende Recht auf eigenverantwortliche Verteidigung elementarer Freiheiten verletzen würde.⁶⁴ Bereits der durch verfassungsänderndes Gesetz eingeführte Art. 10 Abs. 2 Satz 2 GG ist nur deshalb mit Art. 79 Abs. 3 GG vereinbar, weil er gerade keine generell und dauerhaft heimlichen Grundrechtseingriffe erlaubt, sondern zumindest eine Benachrichtigung der betroffenen Person fordert, wenn dadurch keine Gefährdungen für gewichtige hoheitliche Belange mehr drohen.⁶⁵

Im Übrigen ist zwar nach der Rechtsprechung des Bundesverfassungsgericht mit Blick auf eingriffsintensive verdeckte Überwachungsmaßnahmen der Nachrichtendienste keine vollständige, aber doch eine weitreichende dauerhafte Heimlichkeit durch die Beschränkung von Benachrichtigungspflichten und Auskunftsrechten hinzunehmen.⁶⁶ Diese Rechtsprechung lässt sich jedoch auf „Schutzmaßnahmen“ nicht übertragen.

Bei verdeckten Überwachungsmaßnahmen gibt es zwei Gründe, die – sofern es um hoheitliche Belange von hohem Gewicht geht – eine weitreichende Geheimhaltung rechtfertigen können: Erstens müssen die meisten Überwachungsmaßnahmen notwendig verdeckt durchgeführt werden, um ihren Zweck zu erfüllen. Selbst nachträglich ansetzende Transparenzschaffende Vorkehrungen können die durch Überwachungsmaßnahmen verfolgten Ziele erheblich beeinträchtigen, da sie Betroffene warnen oder Informationen über die verdeckte behördliche Vorgehensweise erschließen können. Zweitens greift die verdeckte Überwachung zwar – möglicherweise schwerwiegend – in die Privatheit der betroffenen Person ein. Sie tastet jedoch Verhaltensfreiheit und Eigentum unmittelbar nicht an. Überwachung ist zudem kein Selbstzweck, sondern auf hoheitliche Anschlusshandlungen gerichtet, die – möglicherweise in einer mehrgliedrigen Maßnahmenkette – in der Regel auf Eingriffe in Verhaltensfreiheit und Eigentum hinauslaufen. Führt eine Überwachungsmaßnahme nicht zu einem solchen Eingriff, so bleibt sie für die betroffene Person ohne unmittelbare physische oder psychische

⁶² Vgl. Schmidt-Aßmann, in: Dürig/Herzog/Scholz, GG, Stand August 2020, Art. 19 Abs. 4 Rn. 30: Recht auf „eigenverantwortliche Verteidigung“ eigener Rechte.

⁶³ Vgl. auch BVerfGE 101, 397 (408), wonach der vollständige Ausschluss des Rechtswegs durch einfaches Recht verfassungsrechtlich stets unzulässig ist.

⁶⁴ Vgl. Schmidt-Aßmann, in: Dürig/Herzog/Scholz, GG, Stand August 2020, Art. 19 Abs. 4 Rn. 30.

⁶⁵ Vgl. BVerfGE 30, 1 (21).

⁶⁶ Vgl. etwa BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17 –, Rn. 267 ff.; Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 289; Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, Rn. 118.

Folgen. Hat die Überwachung einen Eingriff in Verhaltensfreiheit oder Eigentum zur Folge, kann sich die betroffene Person hiergegen zur Wehr setzen und in diesem Rahmen gegebenenfalls auch die vorausgehende Überwachung thematisieren.

Beide Gründe treffen auf dauerhaft heimliche „Schutzmaßnahmen“ nicht zu. Erstens müssen Eingriffe in Verhaltensfreiheit und Eigentum, die schädigende Kausalverläufe abbrechen oder bereits die Entstehung von Gefahren vermeiden sollen, anders als viele Überwachungsmaßnahmen nicht notwendigerweise geheim durchgeführt werden. Im Gegenteil beruht die gesamte gegenwärtige Eingriffsverwaltung auf offenen, diskutierbaren und rechtsschutzfähigen Eingriffsmaßnahmen. Einen unabdingbaren praktischen Bedarf für dauerhaft heimliche „Schutzmaßnahmen“ zeigt auch die Entwurfsbegründung – jenseits einer pauschalen und nicht substantiierten Sorge vor „Schutzlücken“ – nicht auf. Zweitens – und vor allem – beschränken „Schutzmaßnahmen“ Verhaltensfreiheit und Eigentum der betroffenen Personen unmittelbar. Sie bewirken immer einen physischen oder psychischen Nachteil, der sich bei einer dauerhaften Heimlichkeit weder öffentlich thematisieren noch individuell abwehren lässt. Ein Verweis auf die Transparenz nachgelagerter Maßnahmen kommt hier nicht in Betracht. Die dauerhafte Heimlichkeit nimmt den betroffenen Personen vielmehr Orientierung und Rechtsschutz dauerhaft und vollständig.

In einem demokratischen Rechtsstaat ist daher für verdeckte Eingriffe in Verhaltensfreiheit und Eigentum nur in sehr engen Grenzen Raum. Solche Eingriffe kommen meiner Ansicht nach nur unter drei kumulativen, jeweils restriktiv zu verstehenden Voraussetzungen in Betracht:

Erstens muss der verdeckte Eingriff dazu dienen, schwerwiegende Schäden zu verhindern, die in einer akuten Krisenlage konkret absehbar sind. In polizeirechtlicher Terminologie geht es um eine gegenwärtige Gefahr beziehungsweise eine unmittelbar bevorstehende Schädigungshandlung. Synonym dürfte die in dem Gesetzentwurf gelegentlich vorkommende (vgl. etwa § 46 Abs. 2 BVerfSchG-E), wenngleich ungebräuchliche und terminologisch schiefe⁶⁷ Formulierung „unmittelbar bevorstehende Gefahr“ zu verstehen sein.

Zweitens muss gerade ein verdecktes Vorgehen erforderlich sein, um hochrangige Sicherheitsbelange zu gewährleisten. Dies kommt insbesondere in Betracht, wenn die bestehende Krisenlage zwar ein unverzügliches Einschreiten erfordert, zugleich jedoch noch weitere, nur verdeckt zu gewinnende Informationen benötigt werden, um diese Lage nachhaltig zu beenden.

Drittens sind die betroffenen Personen über den verdeckten Eingriff unverzüglich zu informieren, sobald die – allein auf die konkrete Krisenlage zu beziehenden – Gründe für das verdeckte Vorgehen entfallen sind. Eine Ausnahme von der Benachrichtigungspflicht scheidet aus den oben ausgeführten Gründen aus. Indem sich die hoheitliche Gewalt entschließt, Verhaltensfreiheit oder Eigentum einer Person zu beschränken, entschließt sie sich unaufgebbar auch zur Ermöglichung einer öffentlichen Diskussion und zur Gewährung von wenigstens nachträglichem Rechtsschutz.

Ein Anschauungsbeispiel für ein derartiges zeitweise verdecktes Vorgehen bildet der Fall der sogenannten Sauerlandgruppe. Hierbei handelte es sich um eine islamistische terroristische Zelle, deren

⁶⁷ Der Begriff der Gefahr verweist auf die Prognose eines zukünftigen Schadensereignisses. Die Formulierung „unmittelbar bevorstehende Gefahr“ erweckt den Eindruck, es gehe nicht um ein unmittelbar bevorstehendes Schadensereignis, sondern um die unmittelbar bevorstehende Prognose oder Prognostizierbarkeit.

Mitglieder große Mengen einer Chemikalie beschafften, um daraus Bomben zu bauen. Ende Juli 2007 tauschten Polizeibeamte diese Chemikalien gegen eine harmlose Ersatzflüssigkeit aus, um die Gruppe weiter überwachen und ihre Vernetzungen klären zu können, ohne einen Schaden zu riskieren. Eine letzte Lieferung bestand von vornherein lediglich aus einer harmlosen Lösung. Anfang September 2007 wurden die Angehörigen der Sauerlandgruppe festgenommen.⁶⁸

Die fachrechtliche Bewertung dieses Vorgehens nach damaligem Rechtsstand mag hier dahinstehen. Es erscheint mir jedenfalls verfassungsrechtlich hinnehmbar. Die Ermächtigung zu „Schutzmaßnahmen“ geht jedoch über derartige temporär verdeckte Maßnahmen in akuten Krisenlagen weit hinaus und soll dies nach der Entwurfsbegründung auch gerade. Es wäre im Übrigen kaum verständlich, warum gerade das BfV und nicht eine Polizeibehörde mit der temporär verdeckten Bewältigung akuter Krisenlagen betraut sein soll. In einer Lage, wie sie sich im Fall der Sauerlandgruppe darstellt, ist der Handlungskreis der weitaus schlagkräftigeren und operativ erfahreneren Polizei zwanglos eröffnet. Ein Zurückhalten von Informationen aufgrund überwiegender Sicherheitsinteressen kommt gleichfalls nicht in Betracht, wenn zahllose Menschenleben gefährdet sind.

c) Weitere verfassungsrechtliche Einwände

Selbst wenn sich dauerhaft verdeckte aktionelle Eingriffsmaßnahmen verfassungsrechtlich überhaupt legitimieren ließen, wäre die konkrete gesetzliche Ausgestaltung in §§ 59 ff. BVerfSchG-E in vielfacher Hinsicht verfassungsrechtlich defizitär. Diese Einwände seien im Folgenden in geraffter Form dargestellt.

Erstens stehen §§ 59 ff. BVerfSchG-E mit der bundesstaatlichen Kompetenzordnung nicht in Einklang. Es fehlt bereits an einer Gesetzgebungskompetenz des Bundes. Die für den Verfassungsschutz einschlägigen Kompetenztitel in Art. 73 Abs. 1 Nr. 10 lit. b und c GG decken allein informationelle Aufgaben und darauf bezogene Befugnisse ab. Dies ergibt sich zum einen aus einer historischen Auslegung. Ungeachtet mancher Kontroversen⁶⁹ sind diese Normen immer nur auf die Auswertung von Erkenntnissen bezogen worden. Zum anderen zeigt der systematische Vergleich von Art. 73 Abs. 1 Nr. 10 GG mit Art. 73 Abs. 1 Nr. 9a GG, dass es für eine bundesrechtliche Regelung der aktionellen Gefahrenabwehr eines besonderen Kompetenztitels bedarf. Diese Norm ist hier allerdings nicht einschlägig, da sie allein eine Betrauung des BKA mit der präventiven Terrorismusabwehr ermöglicht. Das Fehlen einer Gesetzgebungskompetenz des Bundes lässt sich weder mit einem – sachlich nicht überzeugenden – Verweis auf das „nachrichtendienstliche Gepräge“ der „Schutzmaßnahmen“ noch durch eine Berufung auf die Natur der Sache überspielen. Eine Gesetzgebungskompetenz kraft Natur der Sache für aktionelle Maßnahmen der Gefahrenverhütung kommt nicht in Betracht, wie sich bereits an der unstreitigen grundsätzlichen Gesetzgebungszuständigkeit der Länder für das allgemeine Gefahrenabwehrrecht zeigt. Diese Kompetenz schließt die Abwehr von staatsschutzrelevanten Gefahren, die von besonderen Bedrohungen im Sinne des § 59 Abs. 3 BVerfSchG-E ausgehen, ohne weiteres ein.

⁶⁸ Vgl. <https://archive.ph/2012.09.13-134827/http://www.ruhrnachrichten.de/nachrichten/region/hierund-heute/Sauerland-Gruppe-Terroristen-kaufen-monatelang-Wasserstoffperoxid;art1544,559696>.

⁶⁹ Vgl. Bäcker, in: Lisken/Denninger/ders., Handbuch Polizei- und Sicherheitsrecht, 8. Aufl. 2026, Kap. 2 Rn. 324 ff., m.w.N.

Zweitens sind die materiellen Eingriffsvoraussetzungen und Rechtsfolgen von „Schutzmaßnahmen“ viel zu weit und offen formuliert. Sie verletzen daher den Verhältnismäßigkeitsgrundsatz. Entgegen der Entwurfsbegründung weisen „Schutzmaßnahmen“ in der Regel bereits wegen ihrer dauerhaft heimlichen Durchführung eine hohe Eingriffsintensität auf. Manche „Schutzmaßnahmen“ können darüber hinaus Verhaltensfreiheit und Eigentum schwerwiegend beeinträchtigen, etwa wenn sie der betroffenen Person wesentliche Vermögenswerte entziehen oder ihr soziales Umfeld erheblich manipulieren. Selbst wenn solche Maßnahmen überhaupt für rechtfertigungsfähig gehalten werden, bedürfen sie daher einer normenklaren Regulierung und gehaltvoller Voraussetzungen. Demgegenüber gestattet § 59 Abs. 2 BVerfSchG-E beliebige Einwirkungen auf Gegenstände in einem – wie gezeigt – äußerst weiten Sinn gegenüber jeder Person, bei der solche Einwirkungen überhaupt irgendeinen Erfolg zeitigen können.

Drittens ist die Kontrolle von „Schutzmaßnahmen“ unzureichend ausgestaltet. Eine Vorabkontrolle einzelner Maßnahmen ist nur in Sonderfällen vorgesehen, die das Spektrum eingriffsintensiver Maßnahmen nicht annähernd ausschöpfen. Die Ex-Post-Kontrolle durch das administrative Kontrollorgan ist zu durchsetzungsschwach, da es grundsätzlich an einer verbindlichen Weisungsbefugnis fehlt.

Viertens stört die Ermächtigung zu „Schutzmaßnahmen“ den Regelungskontext des Verfassungsschutzrechts. Nach der Rechtsprechung des Bundesverfassungsgerichts darf der Gesetzgeber die Eingriffsschwellen für die nachrichtendienstliche Aufklärung verfassungsschutzrelevanter Bedrohungen nur deshalb im Vergleich zu polizeilichen Maßnahmen absenken, weil im Gegenzug die Verfassungsschutzbehörden nicht über operative Befugnisse, also Befugnisse zur unmittelbaren Verkürzung von Verhaltensfreiheit und Eigentum verfügen.⁷⁰ Gerade solche Befugnisse werden durch die Ermächtigung zu „Schutzmaßnahmen“ jedoch geschaffen. In der Folge müssten die Eingriffsschwellen für den Einsatz eingriffsintensiver Aufklärungsmaßnahmen auf ein polizeirechtliches Niveau angehoben werden – was den nachrichtendienstlichen Verfassungsschutz sinnlos machen würde. Die einzige gangbare Alternative besteht darin, die Ermächtigung zu „Schutzmaßnahmen“ zu streichen.

2. „Erweiterte nachrichtendienstliche Maßnahmen“ des BND

Im Ansatz für noch vertretbar halte ich hingegen die vorgesehene Ermächtigung des BND zur Durchführung aktioneller Maßnahmen in §§ 49 ff. BNDG-E. Maßgeblich hierfür sind zwei Erwägungen:

Erstens lassen sich rechtsstaatliche Anforderungen nur begrenzt aus dem innerstaatlichen Bereich auf die Auslandstätigkeit deutscher hoheitlicher Stellen übertragen. Im Ausland verfügen diese Stellen nicht über hoheitliche Befugnisse, sodass rechtsförmige hoheitliche Maßnahmen ausscheiden. Zudem würde eine offene Durchführung aktioneller Maßnahmen im Ausland den Zweck dieser Maßnahmen, in manchen Fällen möglicherweise auch die betroffenen Personen gefährden. Als Alternative verbleiben mit Blick auf das Ausland im Wesentlichen Kooperationsmechanismen wie die Rechtshilfe in Strafsachen, die allerdings in den Fällen der §§ 49 ff. BNDG-E praktisch nicht greifen werden.

Zweitens beschränkt sich die vorgesehene Ermächtigung gemäß § 51 Abs. 3 Satz 1 BNDG-E auf Maßnahmen gegen fremde Mächte, von denen spezifische Gefährdungen ausgehen. Ausländische

⁷⁰ Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 153 ff.; Beschluss vom 17. Juli 2024 – 1 BvR 2133/22 –, Rn. 88 ff.

Staaten als solche sind keine Grundrechtsträger. Dies schließt zwar nicht aus, dass eine „erweiterte nachrichtendienstliche Maßnahme“ im Einzelfall gleichwohl in Grundrechte eingreift, etwa indem sie gegenüber einzelnen betroffenen Personen zu Sach- oder Personenschäden führt. Die primäre Stoßrichtung gegen eine fremde Macht macht solche Eingriffe allerdings meiner Ansicht nach hinnehmbar, da gemäß § 51 Abs. 3 Satz 2 BNDG-E zumindest eine gezielte Verletzung von Leib und Leben unzulässig ist. „Erweiterte nachrichtendienstliche Maßnahmen“ etwa zur Bekämpfung terroristischer Gruppierungen oder von Strukturen der organisierten Kriminalität im Ausland, die nicht zugleich als Teile einer fremden Macht zu begreifen sind, erschienen mir hingegen verfassungsrechtlich ausgeschlossen.

Im Detail weist die gesetzliche Ausgestaltung der „erweiterten nachrichtendienstlichen Maßnahmen“ allerdings einige – teils nicht triviale, aber prinzipiell behebbare – verfassungsrechtliche Mängel auf.

Erstens ist der in § 49 Abs. 2 BNDG-E in Bezug genommene Katalog von Rechtsgütern in § 2 Abs. 2 Nr. 1 bis 5 BNDG-E teils zu weit gefasst, um „erweiterte nachrichtendienstliche Maßnahmen“ zu rechtfertigen.

„Erweiterte nachrichtendienstliche Maßnahmen“ können in Grundrechte eingreifen. Zwar sollen sie Gefährdungen durch fremde Mächte abwenden, die als solche keine Grundrechtsträger sind. Soweit sich „erweiterte nachrichtendienstliche Maßnahmen“ unmittelbar gegen einzelne Personen richten, können sie gleichwohl in Grundrechte eingreifen. Für Personen, die unmittelbar ausländische hoheitliche Gewalt ausüben, gilt dies zumindest insoweit, als eine Maßnahme höchstpersönliche Rechtsgüter beeinträchtigt. Hierzu zählen insbesondere Leib und Leben, deren Gefährdung oder auch in Kauf genommene Verletzung § 51 Abs. 3 Satz 2 BNDG-E nicht ausschließt. Darüber hinaus können „erweiterte nachrichtendienstliche Maßnahmen“ auch Personen einbeziehen, die sich nicht selbst einer fremden Macht zuordnen lassen, sondern derer sich eine fremde Macht lediglich – möglicherweise ohne ihr Wissen – im Zusammenhang mit einer Gefährdung bedient. Solche Personen sind vollumfänglich grundrechtsberechtigt. Wegen des breiten Spektrums möglicher Maßnahmen, die bis zu schweren Schäden für Einzelne reichen, wegen ihrer dauerhaften Heimlichkeit und wegen der Zulässigkeit von Maßnahmen erheblich im Vorfeld konkreter Gefährdungen ist zumindest in manchen Fällen von einer hohen Eingriffsintensität auszugehen.

Angesichts dessen lassen sich „erweiterte nachrichtendienstliche Maßnahmen“, soweit das Spektrum der zulässigen Maßnahmen nicht enger begrenzt wird, nur rechtfertigen, wenn sie dem Schutz besonders herausragend bedeutsamer Rechtsgüter dienen. Demgegenüber kann nach § 49 Abs. 2 i.V.m. § 2 Abs. 2 Nr. 3 BNDG-E eine spezifische Gefährdungslage, in der solche Maßnahmen zulässig sind, bereits bei einer Gefährdung der außenpolitischen Handlungsfähigkeit der Bundesrepublik vorliegen. Dieses Rechtsgut umfasst letztlich alle außenpolitischen Interessen (siehe oben I. 2. a)). Selbst anhaltend und planvoll herbeigeführte, besonders schwerwiegende Gefährdungen der so verstandenen außenpolitischen Handlungsfähigkeit können jedoch schwere Grundrechtseingriffe, die bis zur in Kauf genommenen Tötung von Menschen reichen können, nicht in jedem Fall legitimieren. Dafür ist dieses Rechtsgut nicht trennscharf genug formuliert. Die pauschale Bezugnahme auf die außenpolitische Handlungsfähigkeit als Schutzgut von §§ 49 ff. BNDG-E droht die Ermächtigung zu entgrenzen und „erweiterte nachrichtendienstliche Maßnahmen“ unabhängig von ihrer Eingriffsintensität zum Standardmittel des BND zu machen.

Um die Eingriffsvoraussetzungen angemessen zu konturieren, könnten etwa die „erweiterten nachrichtendienstlichen Maßnahmen“ näher spezifiziert oder zumindest enger begrenzt werden, soweit

sie dem Schutz der außenpolitischen Handlungsfähigkeit der Bundesrepublik dienen. Zusätzlich oder alternativ könnte § 49 Abs. 2 BNDG-E statt einer Bezugnahme auf § 2 Abs. 2 Nr. 3 BNDG-E die Gefährdungen für die außenpolitische Handlungsfähigkeit näher beschreiben, denen solche Maßnahmen begegnen sollen. Sofern etwa „erweiterte nachrichtendienstliche Maßnahmen“ dazu dienen sollen, gegenüber ausländischen Staaten Wehrhaftigkeit durch Vergeltungsmaßnahmen zu demonstrieren, könnte und müsste dieser Zweck ausdrücklich in die Ermächtigung aufgenommen werden.

Zweitens eröffnen § 49 Abs. 1 Satz 2 und § 51 Abs. 2 Satz 2 BNDG-E dem BND in zu großem Ausmaß „erweiterte nachrichtendienstliche Maßnahmen“ im Inland. Hier gilt für den BND ebenso wie für das BfV, dass dauerhaft heimliche aktionelle Maßnahmen mit elementaren demokratischen und rechtsstaatlichen Anforderungen nicht in Einklang stehen. Die gesetzlich vorgesehene bloße Subsidiarität solcher Maßnahmen gegenüber Maßnahmen im Ausland sowie gegenüber Maßnahmen anderer inländischer Behörden behebt diesen Einwand nicht, sondern begrenzt lediglich den Anwendungsbereich „erweiterter nachrichtendienstlicher Maßnahmen“ im Inland. Auch die Vorgabe in § 51 Abs. 3 Satz 1 BNDG-E, dass sich „erweiterte nachrichtendienstliche Maßnahmen“ gegen die betreffende fremde Macht richten müssen, behebt das rechtsstaatliche Defizit nicht, da diese Vorgabe lediglich die Zielsetzung der Maßnahme beschreibt, den Betroffenenkreis aber nicht trennscharf begrenzt. So sollen nach der Entwurfsbegründung Maßnahmen auch gegen Ziele zulässig sein, die „von fremden Mächten für die (quasi-)staatliche Aufgabenwahrnehmung beauftragt wurden oder gesteuert werden“.⁷¹ Diese Beschreibung schließt inländische Kriminelle wie auch „nützliche Idioten“ ein, denen gegenüber sich ein dauerhaft heimliches Vorgehen nicht legitimieren lässt. Eine Durchführung „erweiterter nachrichtendienstlicher Maßnahmen“ im Inland erscheint vielmehr jenseits akuter Krisenlagen (siehe oben IV. 1. b)) nur dann hinnehmbar, wenn es sich gleichwohl um auslandsbezogene Maßnahmen handelt, bei denen die oben angesprochenen Besonderheiten zum Tragen kommen. Dies ist zumindest grundsätzlich nur anzunehmen, wenn der BND zwar im Inland handelt, die Wirkungen dieser Handlung jedoch im Ausland eintreten sollen. Ein Beispiel bildet die Manipulation von Exportgütern vor der Ausfuhr, wenn der ausländische Empfänger der betreffenden ausländischen Macht zugerechnet werden kann. Andere Kriterien, die gesetzlich näher zu konkretisieren wären, mögen für Maßnahmen ohne klar lokalisierbaren Handlungs- und/oder Erfolgsort angezeigt sein, etwa für aktive Cyberoperationen.

Drittens schränkt § 51 Abs. 1 BNDG-E den Kreis der zulässigen „erweiterten nachrichtendienstlichen Maßnahmen“ in zweifacher Hinsicht nicht hinreichend ein.

Zum einen können nach der Gesetzesbegründung „erweiterte nachrichtendienstliche Maßnahmen“ praktisch beliebige Handlungen umfassen, neben aktionellen Eingriffen auch etwa Datenerhebungen oder Datenübermittlungen.⁷² Auf diese Weise werden §§ 49 ff. BNDG-E zum Instrument, um die Voraussetzungen aller anderen im Gesetz geregelten Maßnahmen auszuhebeln. Die Ermächtigung nähert sich so einer Regelung des Ausnahmezustands an. Hierfür gibt es auch dann, wenn eine spezifische Gefährdungslage festgestellt ist, keinen plausiblen Grund, zumal wenn es dabei bleibt, dass der BND nach §§ 49 ff. BNDG-E auch im Inland tätig werden kann. Die „erweiterten

⁷¹ BT-Drs. 21/7868, S. 465.

⁷² BT-Drs. 21/7868, S. 464: „alle denkbaren Durchführungsformen“.

nachrichtendienstlichen Maßnahmen“ lassen sich als auf das Ausland begrenzte aktionelle Ergänzung des informationellen Handlungskreises des BND rechtsstaatlich (noch) hinnehmen, nicht aber als Freibrief dafür, sich aller sonstigen Bindungen zu entledigen.

Zum anderen steht die aktionelle Auslandstätigkeit des BND in einem latenten Konkurrenzverhältnis zu genuin militärischen Operationen, die den besonderen verfassungsrechtlichen Anforderungen an den Einsatz der Streitkräfte im Ausland unterliegen. Als „erweiterte nachrichtendienstliche Maßnahmen“ kommen nach dem Entwurfswortlaut neben punktuellen Handlungen wie der Löschung bestimmter Daten oder der Manipulation einzelner technischer Geräte auch groß angelegte Sabotagehandlungen in Betracht. Schäden an Leib und Leben dürfen dabei gemäß § 51 Abs. 2 Satz 2 BNDG-E zwar nicht Maßnahmeziel sein, wohl aber als Kollateralschäden in Kauf genommen, je nach Norminterpretation sogar wissentlich herbeigeführt werden. Beispielsweise ließe sich nach dem vorgesehenen offenen Normwortlaut eine Aktion wie der Sprengstoffanschlag auf die Nord Stream-Pipelines, durch den Schäden an bedeutsamen Infrastruktureinrichtungen im (mindestens) dreistelligen Millionenbereich verursacht wurden und etwa 500.000 Tonnen eines hochentzündlichen starken Treibhausgases in die Atmosphäre gelangten, als „erweiterte nachrichtendienstliche Maßnahme“ darstellen. Bei solchen Aktionen handelt es sich um Mittel der hybriden Kriegsführung, die sich – so sie denn überhaupt ergriffen werden sollen – jedenfalls nicht im Wege eines fachbehördlichen Anordnungs- und quasi-gerichtlichen Kontrollverfahrens legitimieren lassen.

Im Übrigen verdeutlicht dieses Beispiel, dass der BND bei der Durchführung „erweiterter nachrichtendienstlicher Maßnahmen“ neben rechtsstaatlichen insbesondere auch völkerrechtliche Vorgaben zu beachten hat. Die damit aufgerufenen Interventions- und Gewaltverbote sind als allgemeine Regeln des Völkerrechts⁷³ gemäß Art. 25 GG für den BND unmittelbar verbindlich. Gleichfalls unmittelbar verbindlich sind völkervertragliche Regelungswerke, die der Gesetzgeber in innerstaatliches Recht umgesetzt hat. Zudem sind die völkerrechtlichen Verpflichtungen der Bundesrepublik, insbesondere soweit sie dem Grund- und Menschenrechtsschutz dienen, wegen der Völkerrechtsfreundlichkeit des Grundgesetzes generell bei der Verfassungsinterpretation zu beachten und insoweit mittelbar auch innerstaatlich relevant.⁷⁴

Aufgrund der innerstaatlich wirksamen völkerrechtlichen Vorgaben sind dem BND verdeckte Sabotagehandlungen im Ausland, zumindest wenn sie eine Bagatellschwelle überschreiten, ungeachtet der vorgesehenen gesetzlichen Regelung nur in besonderen Krisenlagen oder als Reaktion auf vergleichbare Handlungen der betreffenden ausländischen Macht ausnahmsweise erlaubt.⁷⁵ Angesichts dessen erstaunt es, dass die Entwurfsbegründung das Völkerrecht im Zusammenhang mit „erweiterten nachrichtendienstlichen Maßnahmen“ nicht erwähnt. Die völkerrechtlichen Vorgaben sind sowohl bei der Grundanordnung als auch bei den Entscheidungen über einzelne Maßnahmen zu beachten. Insbesondere besteht eine Krisenlage, die solche Maßnahmen rechtfertigen kann, nicht in jedem Fall schon dann, wenn eine spezifische Gefährdungslage im Sinne von § 49 Abs. 2 BNDG-E

⁷³ König, in: Huber/Voßkuhle, GG, 8. Aufl. 2024, Art. 25 Rn. 63; Aust, in: v. Münch/Kunig, GG, 8. Aufl. 2025, Art. 25 Rn. 66.

⁷⁴ Vgl. etwa BVerfG, Urteil vom 15. Juli 2025 – 2 BvR 508/21 –, Rn. 84 f.; stRspr.

⁷⁵ Vgl. beispielhaft zur völkerrechtlichen Beurteilung des Anschlags auf die Nord Stream-Pipelines BGH, Beschluss vom 10. Dezember 2025 – StB 60/25 3 BJs 297/25-2.

vorliegt, da die Feststellung einer solchen Gefährdungslage deutlich weiter im Vorfeld konkreter Gefährdungen ansetzt.

Die Ermächtigung zu „erweiterten nachrichtendienstlichen Maßnahmen“ sollte daher an die völkerrechtlichen Anforderungen angeglichen werden. Zumindest erscheint es sinnvoll, in die Ermächtigung zu „erweiterten nachrichtendienstlichen Maßnahmen“ einen Verweis auf die zu beachtenden völkerrechtlichen Normen aufzunehmen. Ein solcher Verweis wäre rein deklaratorisch und würde an den rechtlichen Bindungen des BND nichts ändern. Er würde aber den Rechtsrahmen für Anordnungen und Maßnahmen des BND und für ihre Kontrolle durch den Unabhängigen Kontrollrat in übersichtlicher Weise klarstellen. So würde der ausdrückliche Verweis auf die völkerrechtlichen Verpflichtungen der Bundesrepublik dem etwaigen Missverständnis vorbeugen, der BND sei aufgrund von §§ 49 ff. BNDG-E von diesen Verpflichtungen freigestellt.