



---

**Ausschussdrucksache 21(4)233 G**  
vom 12. Oktober 2026

---

**Schriftliche Stellungnahme**

von Luca Manns, M.A., LL.M., Universität zu Köln  
vom 12. Oktober 2026

zu dem

Gesetzentwurf der Bundesregierung  
*Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts*  
**BT-Drucksache 21/7868**



Forschungsstelle Nachrichtendienste, 50923 Köln

Innenausschuss des  
Deutschen Bundestages  
11011 Berlin

Köln, 12.10.2026

**Schriftliche Stellungnahme  
zum Gesetzentwurf der Bundesregierung  
zur Reform des Nachrichtendienstrechts (Drs. 21/7868)**

|      |                                                                                |    |
|------|--------------------------------------------------------------------------------|----|
| A.   | Rahmen der Novelle und dieser Stellungnahme .....                              | 5  |
| I.   | Gegenstand, Anlass .....                                                       | 5  |
| II.  | Prüfungsmaßstab .....                                                          | 6  |
| III. | Umfang .....                                                                   | 7  |
| B.   | Art. 2 – BNDG-E .....                                                          | 8  |
| I.   | Aufgabe, Eingriffsschwellen, allgemeine Befugnisse,<br>Zugänge (§§ 1–18) ..... | 8  |
| 1.   | Aufgabe (§ 2) .....                                                            | 8  |
| 2.   | Eingriffsschwellen (§§ 3, 4) .....                                             | 9  |
| 3.   | Allgemeine Befugnisse, Vorgaben (§§ 5, 6) .....                                | 11 |
| 4.   | Informationszugänge (§§ 10–17) .....                                           | 13 |
| 5.   | Heimliches Betreten von Wohnungen (§ 18 Abs. 2) ..                             | 20 |
| II.  | Nachrichtendienstliche Verbindungen (§§ 20, 22, 23) ..                         | 23 |
| III. | Strategische Aufklärung (§§ 30–34, 47) .....                                   | 26 |
| 1.   | Zusammenführung der Regime .....                                               | 26 |
| 2.   | Erhebung, Volumengrenze (§§ 31, 32) .....                                      | 26 |
| 3.   | Einsicht, Inlandsbezug, Eignungsprüfung (§§ 33, 34) ..                         | 29 |
| 4.   | Anordnung, Kontrolle (§ 47, § 97) .....                                        | 30 |
| 5.   | Speicherfristen (§§ 65, 66) .....                                              | 34 |
| 6.   | Mitteilung, Rechtsweg (§§ 100–103) .....                                       | 36 |
| IV.  | Individualisierte technische Aufklärung (§§ 35–39) .....                       | 37 |
| V.   | Kooperationen mit ausländischen Stellen (§§ 40–45) ..                          | 40 |
| VI.  | Erweiterte nachrichtendienstliche Maßnahmen (§§ 49–51)<br>.....                | 41 |
| 1.   | Regelungskonzept und Erscheinungsformen .....                                  | 41 |

**Forschungsstelle  
Nachrichtendienste**

**Prof. Dr. Markus Ogorek, LL.M.**  
Direktor

Telefon: 0221 470-76545  
Telefax: 0221 470-76570  
Markus.Ogorek@uni-koeln.de

**Luca Manns, M.A., LL.M.**  
Geschäftsführer

Telefon: 0221 470-90835  
Telefax: 0221 470-76570  
Luca.Manns@uni-koeln.de

**Postanschrift**  
FS Nachrichtendienste  
50923 Köln

**Besuchsanschrift**  
Universitätsstraße 22a  
50937 Köln

**KVB** (Sülz) Universität



|       |                                                                                       |    |
|-------|---------------------------------------------------------------------------------------|----|
| 2.    | Grundsätzliche Bewertung und Anordnungsarchitektur.....                               | 42 |
| 3.    | Kompetenzordnung des Grundgesetzes .....                                              | 43 |
| 4.    | Konkrete Maßnahmenarten .....                                                         | 44 |
| a)    | Digitale Maßnahmen.....                                                               | 44 |
| b)    | Realweltliche Maßnahmen .....                                                         | 46 |
| c)    | Absenken nachrichtendienstlicher Schwellen als „erweiterte Maßnahme“ .....            | 50 |
| 5.    | Verhältnis zu anderen Eingriffsbefugnissen.....                                       | 51 |
| VII.  | Weiterverarbeitung, insbesondere automatisierte Auswertung (§§ 52, 53).....           | 52 |
| VIII. | Übermittlung (§§ 70–94).....                                                          | 54 |
| 1.    | Katalog gleichwertiger Delikte einer „besonders schweren Straftat“ .....              | 54 |
| 2.    | Übermittlungen an die Bundeswehr.....                                                 | 56 |
| IX.   | Kontrolle, Auskunft, Rechtsschutz (§§ 95–103) .....                                   | 57 |
| 1.    | Vorabkontrolle und Einzelfallkontrolle.....                                           | 57 |
| 2.    | Auskunft (§ 102) .....                                                                | 58 |
| X.    | Eigensicherung, Schutz von Verschlusssachen (§§ 104–124) .....                        | 61 |
| 1.    | Einordnung und Zulässigkeit .....                                                     | 61 |
| 2.    | Räumlicher Anwendungsbereich (§§ 106–108).....                                        | 61 |
| 3.    | Anknüpfung, Festhalten, Durchsuchung (§§ 104, 109–111).....                           | 63 |
| 4.    | Schutz von Verschlusssachen (§§ 115–119) .....                                        | 64 |
| 5.    | Tätigkeit von Ruhestandsbeamten .....                                                 | 65 |
| C.    | Art. 1 – BVerfSchG-E .....                                                            | 66 |
| I.    | Aufgabe, Begriffsbestimmungen (§§ 1–3).....                                           | 66 |
| 1.    | Aufgabe, Kompetenz, Trennungsklauseln (§§ 1–3).....                                   | 66 |
| 2.    | Eingriffsschwellen (§ 3 Abs. 4–10).....                                               | 68 |
| II.   | Beobachtungsobjekt-Regime (§ 4): Prüffall, Verdachtsfall, gesicherte Bestrebung ..... | 72 |
| 1.    | Kodifikation und Einstufungsvorbehalt.....                                            | 72 |
| 2.    | Fristenregime, Ministervorbehalt (Abs. 3).....                                        | 72 |
| 3.    | Rechtsschutz (Art. 15, § 50 Abs. 1 Nr. 2a VwGO).....                                  | 73 |
| III.  | Datenerhebung unter Mitwirkung Dritter (§§ 8–15).....                                 | 73 |
| IV.   | Nachrichtendienstliche Mittel (§§ 16–32) .....                                        | 75 |
| 1.    | Systematik (§§ 16, 29).....                                                           | 75 |
| 2.    | Adressatenkreis (§ 16 Abs. 5).....                                                    | 76 |
| 3.    | Vertrauenspersonen und Verdeckte Bedienstete (§§ 17–19).....                          | 76 |
| 4.    | Observation, Standortfeststellung (§§ 20, 21) .....                                   | 79 |
| 5.    | Brief-, Post- und Telekommunikationsüberwachung (§ 22) .....                          | 79 |
| 6.    | Eingriffe in informationstechnische Systeme (§§ 23–26).....                           | 80 |
| a)    | Auslesen informationstechnischer Geräte (§ 23).....                                   | 80 |
| b)    | Eingriff in private informationstechnische Systeme (§ 25).....                        | 81 |
| c)    | Abgegrenzter Eingriff (§ 26).....                                                     | 83 |



|       |                                                                                        |     |
|-------|----------------------------------------------------------------------------------------|-----|
| d)    | Angriffsinfrastruktur (§ 24) .....                                                     | 84  |
| 7.    | Heimliches Betreten von Wohnungen (§ 16 Abs. 6) .....                                  | 84  |
| 8.    | Wohnraumüberwachung, Einsatzsicherung (§§ 27, 28) .....                                | 85  |
| 9.    | Kernbereich und Berufsgeheimnisträger (§§ 31, 32) .....                                | 86  |
| V.    | Anordnung, Vorabkontrolle, Mitteilung (§§ 33–35) .....                                 | 87  |
| VI.   | Weiterverarbeitung (§§ 36–44) .....                                                    | 89  |
| VII.  | Übermittlung (§§ 45–58) .....                                                          | 91  |
| VIII. | Schutzmaßnahmen (§§ 59–62) .....                                                       | 92  |
| 1.    | Tatbestand, Maßnahmenkatalog .....                                                     | 92  |
| 2.    | Verhältnismäßigkeit auf Schwellenebene .....                                           | 93  |
| 3.    | Kompetenz, Regelungsvorschlag .....                                                    | 96  |
| 4.    | Subsidiarität, Kontrolle .....                                                         | 98  |
| IX.   | Eigensicherung (§§ 28, 63–67) .....                                                    | 99  |
| 1.    | Aufgabe, Kompetenz .....                                                               | 99  |
| 2.    | Befugnisse im Eigensicherungsbereich (§§ 63, 64) .....                                 | 100 |
| 3.    | Einsatzsicherung, Waffen, Drohnenabwehr (§§ 28, 63 Abs. 7, 65) .....                   | 101 |
| 4.    | Vergleich mit dem BNDG-E, Regelungslücken .....                                        | 101 |
| X.    | Kontrolle, Auskunft, Übergang (§§ 69, 70, 79) .....                                    | 102 |
| D.    | Art. 3 – UKRatG-E .....                                                                | 103 |
| I.    | Verfassungsrechtlicher Rahmen .....                                                    | 103 |
| 1.    | Gerichtsäquivalente Ersatzkontrolle bei Eingriffen in Art. 10 GG .....                 | 103 |
| 2.    | Unabhängige Vorabkontrolle bei sonstigen eingriffsintensiven Maßnahmen .....           | 104 |
| 3.    | Bedeutung des Wegfalls nachträglichen Rechtsschutzes .....                             | 105 |
| II.   | Bündelung der Kontrollzuständigkeiten .....                                            | 106 |
| 1.    | Zentralisierung und Gesamtüberblick .....                                              | 106 |
| 2.    | Verlagerung der Anordnungszuständigkeit auf die Dienste .....                          | 107 |
| 3.    | Prüfungsmaßstab .....                                                                  | 108 |
| III.  | Besetzung (§ 14 UKRatG-E) .....                                                        | 109 |
| 1.    | Erweiterung des Kreises richterlicher Mitglieder .....                                 | 109 |
| 2.    | Öffnung für nichtrichterliche Mitglieder .....                                         | 109 |
| a)    | Bundesanwälte .....                                                                    | 110 |
| b)    | Beamte oberster Bundesbehörden .....                                                   | 110 |
| c)    | Künftig ehemalige Mitglieder der G 10-Kommission .....                                 | 111 |
| IV.   | Altersgrenze (§ 20 Abs. 1 S. 1 UKRatG-E) .....                                         | 111 |
| V.    | Wahl (§§ 16, 17 UKRatG-E) .....                                                        | 111 |
| VI.   | Verfahren der Vorabkontrolle und Einzelentscheidung (§§ 23, 27, 28, 30 UKRatG-E) ..... | 113 |
| VII.  | Begründungspflicht (§ 23 Abs. 6 UKRatG-E) .....                                        | 114 |
| VIII. | Verfahrensstellung der Mitglieder (§ 23 Abs. 5, § 28 Abs. 3, § 30 UKRatG-E) .....      | 114 |



|       |                                                                            |     |
|-------|----------------------------------------------------------------------------|-----|
| 1.    | Begrenzte individuelle Verfahrensrechte .....                              | 114 |
| 2.    | Grenzen der Gerichtsähnlichkeit .....                                      | 115 |
| 3.    | Ergebnis: Minderheitsvotum, Stimmengleichheit, Besetzung der Kammern ..... | 115 |
| IX.   | Gefahr im Verzug (§ 31 UKRatG-E) .....                                     | 115 |
| X.    | Administrative Kontrolle und Prüfaufträge (§§ 25, 26, 32 UKRatG-E) .....   | 116 |
| XI.   | Befugnisse (§ 13 UKRatG-E) .....                                           | 117 |
| XII.  | Rechtsfolgen festgestellter Verstöße (§§ 33, 34 UKRatG-E) .....            | 118 |
| XIII. | Individuelles Ersuchen (§ 38 UKRatG-E) .....                               | 119 |
| XIV.  | Berichte und Parlament (§§ 35, 36 UKRatG-E) .....                          | 120 |
| XV.   | Veröffentlichung von Entscheidungen .....                                  | 121 |
| XVI.  | Öffnungsklauseln und Parlamentsvorbehalt .....                             | 122 |
| XVII. | Ausstattung und Kontrolldichte .....                                       | 122 |
| E.    | Spannungs-, Verteidigungs- und Besonderer Feststellungsfall .....          | 123 |
| I.    | Auslösetatbestände (§ 75 Abs. 1 BVerfSchG-E, § 125 BNDG-E) .....           | 123 |
| II.   | BND (§§ 126–133 BNDG-E) .....                                              | 124 |
| III.  | BfV (§ 75 BVerfSchG-E) .....                                               | 126 |
| IV.   | Besonderer Feststellungsfall .....                                         | 128 |
| V.    | Kontrolle und Rechtsschutz im Ausnahmezustand .....                        | 129 |
| F.    | Änderung des MAD-Gesetzes und Folgeänderungen .....                        | 129 |
| I.    | Art. 5 – MAD-Gesetz .....                                                  | 129 |
| II.   | Folgeänderungen mit Eigengewicht .....                                     | 131 |
| G.    | Querschnittsfragen .....                                                   | 131 |
| I.    | Befristung und Evaluierung .....                                           | 131 |
| II.   | Haushaltsausgaben .....                                                    | 132 |
| III.  | Redaktionelles .....                                                       | 132 |
| H.    | Zusammenfassung und wesentliche Thesen .....                               | 133 |

## A. Rahmen der Novelle und dieser Stellungnahme

### I. Gegenstand, Anlass

Gegenstand dieser Stellungnahme ist der Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts (BT-Drs. 21/7868). Der Entwurf löst das Bundesverfassungsschutzgesetz (BVerfSchG) und das Bundesnachrichtendienstgesetz (BNDG) von 1990 vollständig ab. Zudem hebt er das Artikel 10-Gesetz (G 10; Art. 23) auf und stellt die Rechtskontrolle der Nachrichtendienste des Bundes in einem eigenen Stammgesetz auf eine neue Grundlage (Art. 3). Hinzu treten auch materiell bedeutende Änderungen des Gesetzes über den Militärischen Abschirmdienst (MADG), insbesondere zur Telekommunikationsüberwachung (Art. 5), und Folgeänderungen in weiteren Gesetzen und Verordnungen (Art. 6–22). Es steht zu erwarten, dass auf Grundlage dieser Novelle in näherer Zukunft das in einer Art Zwischenstadium der Überarbeitung befindliche MAD-Gesetz weiterführend reformiert wird, insbesondere betreffend die Kontrollstrukturen und eventuelle erweiterte nachrichtendienstliche Befugnisse.

Wir halten den Anlass der Reform für sehr gut nachvollziehbar. Das geltende Recht ist durch drei Jahrzehnte anlassbezogener Änderungen in einigen Teilen unlesbar geworden, was auch darin begründet ist, dass die mitunter bis auf Mikroebene in einer ersatzgesetzgeberischen Weise konstruierten Maßgaben des Bundesverfassungsgerichts zu neuartigen und nicht immer passenden Schwellen geführt haben. Freilich ist die intensive verfassungsrichterliche Ausprägung auch dem Umstand geschuldet, dass die Nachrichtendienstgesetze in ihren Anfangsjahren sehr fragmentarisch ausfielen und es innerhalb der Dienste und ihrer Aufsichtsbehörden eine gewisse Neigung gab, gerade heikle Eingriffe und Verfahren lieber nicht oder nur sehr rudimentär zu normieren, obwohl gerade diese der normenklaren und mit hinreichenden Schwellen versehenen Regelung bedurft hätten.

Zudem hat sich die Gefahrenlage spätestens seit dem Jahr 2022 grundlegend verändert. Zwar hat sich auch die Gefährdung durch gewalttätigen Extremismus und Terrorismus in mehreren Phänomenbereichen verschärft, im auslandsbezogenen Extremismus zuletzt geprägt durch die Angriffe der „Hamas“ vom 7. Oktober 2023 mit dem Iran als mutmaßlich steuernder Hintermacht. Zumindest auf einzelne Phänomenbereiche begrenzten Terrorismus hat es gleichwohl schon seit jeher gegeben, man denke nur an die „Rote-Armee-Fraktion“ und den prägenden Einfluss ihrer Gewalttaten auf die damalige westdeutsche Gesellschaft. Der primäre Anlass für die aktuelle Novellierung muss daher in der Bedrohung durch fremde Mächte gesucht (und gefunden) werden, namentlich jener durch die Russische Föderation. Innere und äußere Sicherheit werden durch den „hybriden Krieg“ der russischen Staatsmacht zwangsläufig immer enger miteinander verschränkt.<sup>1</sup> Da die Aufklärung von geheimdienstlich gesteuerten Operationen nochmals intensiverer Fähigkeiten in der Strukturanalyse und im internationalen Austausch mit anderen Diensten verlangt, als sie es gegenüber dem „klassischen“ Terrorismus tut, wächst in diesem Bereich der Bedarf an Intervention, welcher über die polizeilichen Befugnisse im Inland hinausgeht. Ihn will das Bundesamt für Verfassungsschutz (BfV) im Sinne seiner seit einiger Zeit verwendeten Selbstzuschreibung als „Abwehrdienst“ intensiviert abdecken. Erst recht machen es die operativen Interventionen unterhalb der Schwelle des bewaffneten Angriffs mit der Gefahr einer daraus erwachsenden regulären militärischen Auseinandersetzung durch Russland nötig, über Reaktionsmöglichkeiten des deutschen Staates außerhalb seiner

---

<sup>1</sup>Zur Bandbreite hybrider Angriffe und zu den strafrechtlichen Reaktionsmöglichkeiten Engelstätter, GSZ 2025, 257 (257 ff.).

Territorialgrenzen nachzudenken. Dies schließt es ein, nötigenfalls gegnerische Staaten in ihrer Fähigkeit einzuschränken, bevor sie gegen Deutschland aktiv werden können. Damit sind der Bundesnachrichtendienst (BND) und die ihm künftig im Sicherheitsgefüge der Bundesrepublik zugedachte Rolle angesprochen.

Daneben treten strukturelle Veränderungen in der internationalen Sicherheitsarchitektur: Dürfen deutsche Dienste bestimmte Informationen nicht selbst erheben, hat sie das seit jeher nicht davon abgehalten, entsprechende Zulieferungen von „potenteren“ Partnerdiensten dankend anzunehmen, vor allem aus den Vereinigten Staaten. Dass diese Kontaktbeziehungen erheblich bedroht sind, lässt sich angesichts der Verhaltensweisen der Trump-Administration kaum bestreiten.<sup>2</sup> Oft vergessen, stehen weitere zentrale Partner wie das Vereinigte Königreich mit „Reform UK“ oder die Französische Republik mit dem „Rassemblement National“ jedenfalls an einer Schwelle, als verlässliche Informationslieferanten mittelfristig nur noch eingeschränkt zur Verfügung zu stehen. Neben ihrer nachrichtendienstlichen Komponente schließen diese Partnerschaften eine militärisch sehr wirkmächtige Unterstützung durch den jeweiligen strategischen Atomschirm ein, deren Wanken oder gar Wegfallen zulasten Deutschlands die Risikobereitschaft gegnerischer Kräfte wie Russland steigern könnte, von staatsterroristischen Aktionen über paramilitärische Verhaltensweisen hin in eine breit angelegte militärische Auseinandersetzung zu driften.

All dies sind zwar keine unmittelbar verfassungsrechtlich zu verarbeitenden Umstände, aber in Teilen durchaus konkretisiert erfassbare Verschiebungen der Rechtsgutsbedrohungen. Da das geheime Nachrichtenwesen – anders als in der politisch-medialen Debatte bisweilen anklingend – kein Selbstzweck ist, sondern dem Schutz elementarer Verfassungsgüter dient, kann eine Veränderung in der Bedrohungsanalyse durchaus gesteigerte Grundrechtseingriffe begründen. In diesem Sinne eröffnet sich die Notwendigkeit, dem Nachrichtendienstrecht aus gesetzgeberischer Sicht ein neues Gepräge zu geben. Sinnbildlich dafür steht die derzeitige justizielle Zuordnung des geheimen Nachrichtenwesens zum Datenschutzrecht. Künftig sollte das Recht der Nachrichtendienste wie das Polizei- und Ordnungsrecht einem breiter zu denkenden Sicherheitsrecht zugeordnet werden, um die mit der vorliegenden Novelle ausgebaute Grundrechtsinvasivität zutreffend zu kategorisieren und die Bedeutung der Nachrichtendienste innerhalb der Sicherheitsarchitektur adäquat abzubilden.

Dass der vorliegende Regierungsentwurf die Aufklärungsfähigkeiten vor allem des Auslandsnachrichtendienstes stärkt und die Kontrolle von BND und BfV bei einer Stelle bündelt, entspricht ebenfalls dem, was wir seit Längerem vertreten. Eine solche grundsätzliche Zustimmung entbindet indes nicht von Kritik im Einzelnen, sowohl bezogen auf vorgesehene Instrumente und Eingriffsschwellen als auch auf „rechtshandwerkliche“ Aspekte. Diese Kritik ist in den Abschnitten B.–G. niedergelegt.

## II. Prüfungsmaßstab

Rechtlicher Maßstab dieser Stellungnahme ist insbesondere die umfangreiche Judikatur des Bundesverfassungsgerichts. Das Gericht hat das Nachrichtendienstrecht seit 2020 in vier Grundsatzentscheidungen neu vermessen. Das Urteil zur Ausland-Ausland-Fernmeldeaufklärung bindet die deutsche Staatsmacht auch im Ausland an die Grundrechte und verlangt eine unabhängige Kontrolle in gerichtsähnlicher Form.<sup>3</sup> Das Urteil zum Bayerischen Verfassungsschutzgesetz verpflichtet den

<sup>2</sup> Vgl. auch Flade, Partnerschaft auf dem Prüfstand, tagesschau.de v. 20.9.2025, <https://tagesschau.de/ausland/amerika/geheimdienste-deutschland-usa-bnd-fbi-nsa-cia-100.html>.

<sup>3</sup> BVerfGE 154, 152 (Urt. v. 19.5.2020, 1 BvR 2835/17), Leitsatz 1 und Rn. 272 ff.

Gesetzgeber, die Eingriffsschwellen nach dem Gewicht der jeweiligen Befugnis abzustufen und normenklar zu fassen.<sup>4</sup> Der Beschluss zum Hessischen Verfassungsschutzgesetz überträgt das Kriterium der hypothetischen Datenneuerhebung auf die Übermittlung nachrichtendienstlicher Erkenntnisse und begrenzt operative Anschlussmaßnahmen der Empfänger.<sup>5</sup> Der Beschluss vom 8. Oktober 2024 schließlich betrifft die strategische Inland-Ausland-Fernmeldeaufklärung nach dem Artikel 10-Gesetz.<sup>6</sup> Der vorliegende Regierungsentwurf versteht sich ausdrücklich auch als Umsetzung dieser Rechtsprechung.<sup>7</sup> Aus dem letztgenannten Beschluss folgt zugleich eine Frist. Die beanstandete Befugnis zur strategischen Überwachung im Bereich der Cybergefahren (§ 5 Abs. 1 S. 3 Nr. 8 G 10) gilt nur bis zum 31. Dezember 2026 fort. Tritt das Gesetz nicht rechtzeitig in Kraft, entfällt diese Befugnis ab dem 1. Januar 2027 ersatzlos. Hinzu treten die Vorgaben zur automatisierten Datenanalyse,<sup>8</sup> zum Kernbereichsschutz bei Eingriffen in informationstechnische Systeme,<sup>9</sup> zum informationellen Trennungsprinzip<sup>10</sup> sowie jene Grenzen, die die grundgesetzliche Kompetenzordnung (Art. 73 Abs. 1 Nr. 10, Art. 87 Abs. 1 S. 2 GG) und die Ausnahmezustandsverfassung (Art. 80a, Art. 115a ff. GG) dem Bundesgesetzgeber ziehen.

Soweit die Europäische Menschenrechtskonvention und das Unionsrecht über das Grundgesetz hinausweisen, ziehen wir sie ergänzend heran (näher B.I.4 und B.III.4; zum Prüfumfang vgl. unten). Zweiter Maßstab ist die Praxistauglichkeit. Ein Nachrichtendienstgesetz, das in Karlsruhe Bestand hat, im Dienst aber nicht vollziehbar ist, verfehlt seinen Zweck ebenso wie ein Gesetz, das vollziehbar ist, aber die nächste Verfassungsbeschwerde nicht überlebt. Wir haben den Entwurf deshalb nach unseren Möglichkeiten als von außen auf das geheime Nachrichtenwesen blickende Rechtswissenschaftler daraufhin geprüft, ob seine Schwellen, Verfahren und Kontrollmechanismen im Alltag der Dienste und des Unabhängigen Kontrollrats (UKRat) voraussichtlich handhabbar wären.

Schließlich müssen wir auf folgenden Umstand hinweisen: Einige Regelungen bewegen sich aus unserer Sicht jenseits der bisherigen, recht rigiden verfassungsgerichtlichen Maßstäbe.<sup>11</sup> Ob die veränderte Bedrohungslage eine angepasste verfassungsrechtliche Abwägung trägt, wird sich erst anlässlich der sicher zu erwartenden Überprüfung dieser Novelle in Karlsruhe erweisen. Wir halten die im Entwurf erdachte Argumentation für begründet, weil sie der durch das Gericht selbst herangezogenen Grundlogik von Rechtsgüterabwägungen abseits der Menschenwürdegarantie entspricht und die realen Bedrohungsverschiebungen aus unserer Sicht evident sind.

### III. Umfang

Den über sechshundertseitigen Regierungsentwurf, der gleich mehrere komplexe Gesetze neu fasst oder erst errichtet, kann unsere mit Schreiben vom 7.10.2026 sehr kurzfristig durch den Deutschen

<sup>4</sup> BVerfGE 162, 1 (Urt. v. 26.4.2022, 1 BvR 1619/17), Rn. 190 ff., 199.

<sup>5</sup> BVerfGE 169, 130 (Beschl. v. 17.7.2024, 1 BvR 2133/22), Rn. 106 ff.

<sup>6</sup> Vgl. BVerfGE 170, 79 (Beschl. v. 8.10.2024, 1 BvR 1743/16 und 1 BvR 2539/16); zur Übergangsfrist BGBl. 2024 I Nr. 398. Beanstandet wurden unter anderem die Aussonderung rein inländischer Telekommunikation und der Kernbereichsschutz.

<sup>7</sup> Begr. A.II, BT-Drs. 21/7868, S. 202.

<sup>8</sup> BVerfGE 165, 363 (Urt. v. 16.2.2023, 1 BvR 1547/19, 1 BvR 2634/20), Rn. 99 ff.

<sup>9</sup> BVerfGE 141, 220 (Urt. v. 20.4.2016, 1 BvR 966/09 u.a.), Rn. 224; BVerfG, Beschl. v. 24.6.2025, 1 BvR 180/23 (Trojaner II), Rn. 264 ff.

<sup>10</sup> BVerfGE 133, 277, Rn. 113, 123; BVerfGE 162, 1, Leitsatz 1 und Rn. 171.

<sup>11</sup> Kritisch zur Dichte dieser Maßstäbe Unterreitmeier, GSZ 2026, 13 (15 f.); für eine Neujustierung angesichts der veränderten Bedrohungslage Benamor, Verfassungsrechtliches Ballett, VerfBlog v. 7.9.2026, <https://verfassungsblog.de/geheimdienstreform-bnd-streitkräfte>.

Bundestag erbetene Stellungnahme zur Anhörung am 12.10.2026 keinesfalls vollständig würdigen.<sup>12</sup> Wir fokussieren uns daher auf jene Regelungen, die das neue Recht tragen oder verfassungsrechtlich das größte Gewicht haben dürften: die Schwellendogmatik beider Fachgesetze (B.I.2, C.I.2), die strategische Fernmeldeaufklärung des BND (B.III), die Eingriffe in informationstechnische Systeme (B.IV, C.IV.6), die Interventionsbefugnisse (B.VI, C.VIII), die Übermittlungsvorschriften (B.VIII, C.VII), die Eigensicherung mitsamt dem Schutz von Verschlusssachen (B.X, C.IX), das Beobachtungsobjekt-Regime des BfV (C.II), das UKRat-Gesetz (D.) und den Spannungs- und Verteidigungsfall (E.). Auch innerhalb dieser Bereiche werden wir nicht sämtliche Aspekte aufgreifen können. Der Gesamtschwerpunkt liegt bei alledem auf dem BND-Gesetz.

## **B. Art. 2 – BNDG-E**

Das BNDG-E verweist bewusst nicht mehr auf das BVerfSchG, sondern wird ein echtes Fachgesetz. Das ist ein Gewinn an Lesbarkeit, der sich ebenfalls in der insgesamt verbesserten Struktur von BNDG-E und BVerfSchG-E zeigt. Auch wenn Kernbereichsschutz<sup>13</sup>, Berufsgeheimnisträgerschutz<sup>14</sup>, Eingriffe in informationstechnische Systeme<sup>15</sup> und Übermittlungsvorschriften<sup>16</sup> parallel geregelt sind, bestehen jedoch im Regierungsentwurf gewisse terminologische Unterschiede bei gleich gemeinten Regelungen. Darin wurzeln (kleinere, aber gehäufte) Auslegungsrisiken, weil jede Abweichung im Wortlaut künftig als Sachentscheidung gelesen werden könnte.<sup>17</sup> Ihnen sollte mit einer fachlichen Zwischenredaktion, die die Bundesregierung dem Parlament aufgrund ihrer Ressourcen vor der zweiten Lesung anbieten kann, abgeholfen werden. In der Regel sind nach unserer kursorischen Durchsicht die Formulierungen und die zugehörigen Begründungsteile des BNDG-E übernehmenswerter.

### **I. Aufgabe, Eingriffsschwellen, allgemeine Befugnisse, Zugänge (§§ 1–18)**

#### **1. Aufgabe (§ 2)**

Durch § 2 Abs. 1 S. 2 BNDG-E wird die Auslandsaufklärung erstmals über ihr Ziel definiert: die Früherkennung von Bedrohungen für besonders gewichtige Rechtsgüter. Das ist mehr als eine terminologische Präzisierung des bisherigen § 1 Abs. 2 BNDG. Die außen- und sicherheitspolitisch bedeutsame Aufklärung wird ausdrücklich auf den Schutz derjenigen Rechtsgüter ausgerichtet, auf die das Bundesverfassungsgericht in seinen Entscheidungen zum Nachrichtendienstrecht verstärkt rekurriert. Zugleich erhält der BND das geschärfte Profil einer eigenständigen Sicherheitsbehörde, die weder verlängerter diplomatischer Informationsdienst noch – in nachgeordnetem Rang – bloßer Zubringer der Polizei ist.<sup>18</sup> Die unter B.I.2 angesprochene weite Rechtsgüterliste, etwa die außenpolitische Handlungsfähigkeit, berücksichtigt weiterhin dabei die politische Aufklärung als Primärziel.

Verfassungsrechtlich ist diese Ausrichtung tragfähig, und rechtspolitisch ist sie ausdrücklich zu begrüßen. Das Bundesverfassungsgericht hat die Auslandsaufklärung in seiner Entscheidung von

---

<sup>12</sup> Aus den vorbezeichneten Gründen ist auch eine ordentliche Schlussredaktion nach strengem wissenschaftlichem Maßstab nicht mehr vollständig Rechnung zu tragen gewesen; entsprechende Fehler etwa im Belegapparat oder der internen Verweisung sind vor diesem Hintergrund freundlicherweise nachzusehen.

<sup>13</sup> § 31 BVerfSchG-E, § 21 BNDG-E.

<sup>14</sup> § 32 BVerfSchG-E, § 22 BNDG-E.

<sup>15</sup> §§ 23–26 BVerfSchG-E, §§ 36–39 BNDG-E.

<sup>16</sup> §§ 45–58 BVerfSchG-E, §§ 70–88 BNDG-E.

<sup>17</sup> Zur abweichenden Vorlagepflicht bei kernbereichsrelevanten Informationen § 31 Abs. 4 Nr. 3 BVerfSchG-E („soweit Zweifel bestehen“) und § 21 Abs. 5 S. 2 BNDG-E („tatsächliche Anhaltspunkte“); dazu C.IV.6.

<sup>18</sup> BT-Drs. 21/7868, S. 73 ff.

2020 vom Primärzweck der politischen Unterrichtung der Bundesregierung her gedacht und Gefahrenfrüherkennung und Kriminalitätsbekämpfung nur als Sekundärzwecke eingeordnet.<sup>19</sup> Diese Verortung der Pole ist zu hart ausgefallen. Sie verdeckt, dass der BND schon nach geltendem Recht etwa Gefahren für Leib, Leben und Freiheit oder die organisierte Kriminalität aufklärt und seine Erkenntnisse an Gefahrenabwehr- und Strafverfolgungsbehörden übermitteln darf, bei unmittelbar bevorstehender Gefahr sogar übermitteln muss.<sup>20</sup> Auch das Grundgesetz legt den Dienst nicht auf eine bloß informationssammelnde Tätigkeit für die Regierung fest. Die Kompetenz für die auswärtigen Angelegenheiten umfasst die Aufklärung von Bedrohungen mit internationaler Dimension, auch soweit sie sich schon zu Gefahren verdichtet haben, und sie greift regelmäßig nicht in Zuständigkeiten der Landespolizeien ein, die für Gefahren auf fremdem Hoheitsgebiet nicht zuständig sind.<sup>21</sup> Ein Auslandsdienst, der allein Lagebilder für die Bundesregierung liefert, ist jedenfalls seit dem Ausbruch des großen Landkrieges gegen die Ukraine nicht mehr geeignet, den Bedrohungen durch fremde Mächte für die Bundesrepublik frühzeitig zu begegnen. Wir sind uns sicher, dass dies auch die Karlsruher Richter in einem heutigen Judikat so vertreten und die sicherheitsbehördliche Rolle des BND deutlich stärken würden. Der Entwurf zieht daraus mit der Ausrichtung auf die Früherkennung auch von Einzelfällen die richtige Konsequenz. (Zur Frage aktiver (Gegen-)Maßnahmen vgl. unter B.VI.)

## 2. Eingriffsschwellen (§§ 3, 4)

Sowohl das BVerfSchG-E als auch das hier besprochene BNDG-E sehen eine von Grund auf neue, erstmals gestufte Schwellendogmatik vor. Diese Entscheidung ist richtig, weil so die Gewichtungen im Gesetz einmal vorangestellt und nicht in jeder Befugnisnorm neu ausgehandelt werden.<sup>22</sup> Spätere verfassungsrichterliche Überprüfungen können dadurch zu vereinfacht umzusetzenden Beanstandungen führen, wenn etwa die Geltung einer jeweils höheren Schwelle der im Gesetz vorgesehenen Schrankentrias eingefordert wird. Durch die geplanten drei Stufen wird zudem der durch die Entscheidungen des Bundesverfassungsgerichts geschaffene Flickenteppich an Eingriffsvoraussetzungen zumindest für die nächste Zeit bereinigt, was Rechtssicherheit und Normenklarheit stärkt.

Für den BND soll neben der Grundschwelle („zur nachrichtendienstlichen Auslandsaufklärung erforderlich“) in der ersten Steigerungsstufe die erhebliche Bedrohung (§ 3 Abs. 1 BNDG-E) und in der finalen Steigerungsstufe die Bedrohung von herausgehobener Bedeutung (§ 4 Abs. 1 BNDG-E) vorgesehen werden. Die Bedrohungsziele, -felder und -lagen (§ 3 Abs. 3 und 4, § 4 Abs. 3–5 BNDG-E) sind weit gefasst und die aufgeführten Kataloge (§ 3 Abs. 2, § 4 Abs. 2 BNDG-E) sind nicht abschließend, sondern sollen nur „besonders“ herangezogen werden. Sie rekurren teils auf Bedrohungsarten (Ziele, Methoden etc.) und teils auf bedrohte Schutzgüter (Verfassungsordnung, staatliche Funktionsfähigkeit usw.). Im Ansatz lässt sich das durchaus hören und für einen Auslandsdienst mit dem breiten Auftrag des § 2 Abs. 1 BNDG-E ist die Abstraktion einerseits und der Umfang der Katalogbeispiele andererseits wohl auch noch vertretbar, obgleich die Novelle an dieser Stelle sowohl an der rechtlichen Unbestimmtheit als auch der praktischen Überkomplexität kratzt.

Die Kataloge begründen dabei keine Vermutung, sondern benennen Indizien, die bei der Einstufung einer Bedrohung besonders zu berücksichtigen sind (§ 3 Abs. 2, § 4 Abs. 2 BNDG-E). Das ist der richtige Weg. Das Bundesverfassungsgericht verlangt, die Potentialität einer Bedrohung im Einzelfall

<sup>19</sup> Vgl. BVerfGE 154, 152; kritisch Arts, NVwZ 2026, 455 (456 f., 458).

<sup>20</sup> § 11b Abs. 1 und 7 BNDG; Arts, NVwZ 2026, 455 (458).

<sup>21</sup> Art. 73 Abs. 1 Nr. 1 GG; Arts, NVwZ 2026, 455 (458).

<sup>22</sup> Vgl. BVerfGE 162, 1, Rn. 190 ff., 199. Zur Entscheidung Wissenschaftliche Dienste des Deutschen Bundestages, WD 3 - 3000 - 069/22.

zu prüfen, und lässt etwa ein erkennbar dilettantisches Vorgehen nicht schon deshalb in eine höhere Stufe fallen, weil es einem bestimmten Phänomenbereich angehört.<sup>23</sup> Ein offener Berücksichtigungskatalog bildet das besser ab als eine Fiktion, wie sie das BVerfSchG-E für die Anknüpfung an Straftaten vorsieht (dazu C.I.2). Der Preis ist, dass die Kataloge die Einstufung nur anleiten und sie sich nicht aus ihnen unmittelbar heraus ergibt. Umso wichtiger ist, dass der BND die Gründe der Bedrohungszuweisung dokumentiert und der UKRat ggf. nachvollziehen kann.

Trotz der grundsätzlichen Zustimmung zu den erdachten Schwellenzuordnungen sind besonders zwei Zuordnungen aus hiesiger Sicht problematisch:

| §                   | Stufe                                                     | Be-<br>reich             | Gegenstand                                                                                                                         | Kritik                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------|-----------------------------------------------------------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3 Abs. 4<br>Nr. 5   | Erhebliche<br>Bedrohung                                   | Bedro-<br>hungs-<br>feld | „Aufkommende<br>disruptive Tech-<br>nologien“                                                                                      | „Aufkommende disruptive Technologien“, die nach der Begründung schon in ihrer Entwicklung beobachtet werden sollen, <sup>24</sup> können durchaus ein legitimes Aufklärungsziel des BND darstellen. Nach dem BNDG-E sollen die Technologien aber als Merkmal einer „erheblichen Bedrohung“ herhalten, die Eingriffe gegen Personen eröffnet (etwa § 35 Abs. 1 S. 2 BNDG-E). Dem kann so pauschal nicht zugestimmt werden – vielmehr ist eine Begrenzung auf potenziell sicherheitsrelevante oder besonders sabotagebedrohte/-bedrohende Technologien erforderlich. Dabei kann der Sicherheitsbegriff durchaus weit gedacht werden, wie aktuelle Beispiele von „ausbrechenden“ KI-Tools und ihr Datendiebstahl aus ausländischen Regierungsnetzen belegen. Ohne diese Begrenzung ist die Einordnung in die Kategorie der „erheblichen Bedrohung“ verfassungsrechtlich abzulehnen. |
| § 4 Abs.<br>5 Nr. 3 | Bedrohung<br>von her-<br>ausgehobe-<br>ner Be-<br>deutung | Bedro-<br>hungs-<br>lage | Lage, die „zu einer Gefährdung wesentlicher außen- oder sicherheitspolitischer Belange der Bundesrepublik Deutschland führen kann“ | § 4 Abs. 5 Nr. 3 BNDG-E will bereits eine solche Lage als „Bedrohung von herausgehobener Bedeutung“ führen. Das Kriterium liegt allerdings – den als Hürde nicht allzu hohen Wesentlichkeitsbezug ausklammernd – sehr nahe an der allgemeinen Aufgabenbeschreibung des BND (§ 2 Abs. 1 BNDG-E). Eine Beibehaltung in der Spitzenkategorie der Bedrohungslevel ist aus unserer Sicht verfassungsrechtlich nicht vertretbar. Eine Lage, die „zu einer Gefährdung wesentlicher außen- oder sicherheitspolitischer Belange der Bundesrepublik Deutschland führen kann“, ist vielmehr (nur) als „erhebliche Bedrohung“ einzuordnen und damit auf der Mittelebene der Schwellentrias zu verorten.                                                                                                                                                                                      |

Der Deutsche Bundestag sollte diese beiden Beispiele zum Anlass nehmen, die jeweiligen Schwellen noch einmal sorgsam vor der zweiten Lesung durchzuschauen, weil Fehlzuordnungen an einer so zentralen „Weichensteller“-Position des Gesetzes im Falle der späteren verfassungsgerichtlichen Verwerfung zu weitreichenden Umstellungsprozessen im BND führen würden, die unnötig sind. Aus

<sup>23</sup>BVerfGE 169, 130, Rn. 156, 179.

<sup>24</sup> Begr. zu § 3 Abs. 4 Nr. 5 BNDG-E, BT-Drs. 21/7868, S. 352.

hiesiger Sicht wären mit Behebung der zwei vorbezeichneten Stellen die sich aufdrängenden fehlerhaften Schwellenzuordnungen geheilt. Ob aber weitere abstrakte Begriffe wie die „Funktionsfähigkeit staatlicher Einrichtungen“ oder die „inländische oder europäische Wirtschaft“ hinreichend begrenzt sind, um die an entsprechende Schwellenzuordnungen geknüpften Grundrechtseingriffe zu ermöglichen, mag dahinstehen.

Abschließend sei darauf hingewiesen, dass sich die Voraussetzungen der einzelnen dem BND zugedachten Befugnisse nach Staatsangehörigkeit und Inlandsaufenthalt der betroffenen Person und nach der Richtung der Maßnahme unterscheiden, die Adressatenregeln – anders als im BVerfSchG-E – aber auf die einzelnen Befugnisse verteilt sind (etwa § 13 Abs. 1 und 2, § 20 Abs. 2 und 3, §§ 35, 37–39 BNDG-E). Eine allgemeine Regel, nach der für Ausländer stets eine Stufe niedriger gilt, enthält der Entwurf somit nicht. Die Streuung erschwert aber Anwendung und Kontrolle, weshalb wir eine systematisierende Bündelung oder jedenfalls klare Verweisungen empfehlen.

### **3. Allgemeine Befugnisse, Vorgaben (§§ 5, 6)**

§ 5 Abs. 3 BNDG-E erlaubt künftig neben den bislang aus dem BNDG bekannten allgemeinen Befugnissen auch den biometrischen Abgleich von Daten aus allgemein zugänglichen Quellen einschließlich der Durchführung über öffentliche und nichtöffentliche Stellen in Drittstaaten, wenn der Abgleich nicht gleichermaßen im Inland oder in der Europäischen Union erfolgen kann. Angesprochen dürften damit in der Praxis insbesondere Tools von US-Unternehmen wie das Identifikationssystem „PimEyes“ sein, mit denen das öffentliche Internet nach Personen durchsucht werden kann. Kommerzielle biometrische Suchverfahren eröffnen damit zusätzliche und zeitgemäße Möglichkeiten zur Identifizierung – dass der Dienst solche Werkzeuge nutzen darf, ist daher richtig. Gibt der BND aber die Information, für welche Personen er sich interessiert, an einen Anbieter in einem Drittstaat weiter, der dort eigenen Auskunftspflichten unterliegt (insbesondere nach CLOUD Act und FISA 702 in den Vereinigten Staaten), vertieft das den an sich geringen Eingriff einer Recherche in offenen Quellen erheblich. Denkbar ist vor diesem Hintergrund, die konkreten Kennungen durch zusätzliche nicht aussagekräftige Abfragen oder gleich wirksame technische Vorkehrungen zu verbergen. Solche Schutzverfahren setzen die Dienste bei anderen Auswertungsmethoden mit Bezug zu externen Dritten bereits im Rahmen der operativen Sicherheit ein, sie sollten aber im Gesetz selbst zumindest dem Rahmen nach normiert und nicht allein BND-internen Vorschriften überlassen werden. Konkret sollte § 5 Abs. 3 eine risikoadäquate technische Gestaltung vorschreiben, die Rückschlüsse auf das konkrete Aufklärungsinteresse möglichst verhindert, und eine dokumentierte Prüfung der Zugriffsmöglichkeiten im Drittstaat verlangen.

Darüber hinaus fehlt eine ausdrückliche Voraussetzung für den Abgleich selbst. § 5 Abs. 3 verlangt nicht, dass der Abgleich im Einzelfall erforderlich ist, und die allgemeine Aufgabenbindung ersetzt diese Klarstellung nicht ausdrücklich. Wir empfehlen daher – zumindest aus rechtspolitischen Erwägungen –, den Abgleich nur zuzulassen, „soweit dies im Einzelfall zur nachrichtendienstlichen Auslandsaufklärung erforderlich ist“. Für den entsprechenden Abgleich des BfV verlangt schon § 8 Abs. 1 S. 2 Nr. 2 BVerfSchG-E tatsächliche Anhaltspunkte im Einzelfall. Bei der Prüfung, ob der Abgleich im Inland oder in der Union gleichermaßen möglich ist (§ 5 Abs. 3 S. 2), und bei der Beschaffung von Software (§ 52 Abs. 5) sollten zudem Datensicherheit und digitale Souveränität ausdrücklich zu berücksichtigen sein, weil technisch gleiche Leistung allein nicht genügt.

Eine Sonderregel enthält § 6 Abs. 3 BNDG-E. Er senkt die Schwellen gegenüber Deutschen und Personen im Bundesgebiet um jeweils eine Bedrohungsstufe ab, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Person hoheitliche Aufgaben einer fremden Macht wahrnimmt und die zu veranlassende nachrichtendienstliche Maßnahme ausschließlich oder ganz überwiegend Erkenntnisse zu dieser Tätigkeit verspricht. Verfassungsrechtlich ist das nicht offensichtlich unzulässig, aber auch nicht gesichert. Gegen eine Absenkung von Eingriffsschwellen bei nachweislich gesteigerter Bedrohung ist nach unserer Auffassung zwar nichts Grundsätzliches einzuwenden. Das Bundesverfassungsgericht leitet die Anforderungen aus dem Verhältnismäßigkeitsgrundsatz ab, so dass bei gesteigertem Gewicht der bedrohten Rechtsgüter auch die umgekehrte Bewegung möglich sein muss.<sup>25</sup> Zudem spricht das jetzt vorgesehene „Hoheitsträgerprinzip“ anders als die frühere Funktionsträgertheorie des BND einem bestimmten Personenkreis den Grundrechtsschutz nicht kategorial hinsichtlich seiner Berufstätigkeit ab.<sup>26</sup> Es nimmt stattdessen nur eine Abstufung vor, wie sie das Bundesverfassungsgericht etwa bei Ausländern im Ausland für zulässig befunden hat,<sup>27</sup> und verlangt wenigstens tatsächliche Anhaltspunkte für die Agenten- bzw. Sabotagetätigkeit im Einzelfall. Die Absenkung setzt aber voraus, dass das Gesetz die Tatsachengrundlage der gesteigerten Bedrohung sichert, und hier liegt die Schwäche der Regelung. Mit der Einschlägigkeit von § 6 Abs. 3 BNDG-E entfallen die an ihn anknüpfenden Vorabkontrollen (etwa § 97 Abs. 1 Nr. 13 i.V.m. § 35 Abs. 2 BNDG-E), und ob ein Deutscher als Funktionsträger einer fremden Macht zu behandeln ist, entscheidet zunächst der Dienst allein. Dadurch könnte der BND, wenngleich es sich um eine abstrakte Besorgnis handelt, Personen und sie betreffende Maßnahmen von der strengen Vorabkontrolle des UKRats ausnehmen, falls er ansonsten ein Scheitern in der aufsichtlichen Prüfung besorgen müsste. Aus rein grundrechtsschonender Sicht läge deshalb eine obligatorische Vorabentscheidung des Kontrollrats zur Bestätigung der tatsächlichen Anhaltspunkte nahe. Mit Blick auf die gegen die Belange der Betroffenen abzuwägende Schlagkraft des Auslandsdienstes halten wir eine solche Vorgabe indes nicht für zwingend – und die Regelung für gewagt, aber verfassungsrechtlich noch tragfähig. Aus rechtspolitischer Sicht sollte der BND die Tatsachengrundlage seiner Entscheidung aber verpflichtend dokumentieren und der UKRat sie administrativ nachträglich stichprobenartig prüfen können, was zugleich das der Konstruktion immanente Missbrauchsrisiko senkt.

Eine weitere Absenkung im Schutzniveau enthält § 6 Abs. 4 BNDG-E. Wird eine Maßnahme gegen eine Person ohne deutsche Staatsangehörigkeit angeordnet, während sie sich im Ausland aufhält, darf sie unter den Voraussetzungen der Anordnung längstens 72 Stunden im Bundesgebiet fortgeführt werden, wenn ihr Zweck sonst vereitelt oder wesentlich erschwert würde. Nach der Gesetzesbegründung sollen hier Fälle der örtlichen Nachteile abgedeckt werden, etwa im Transitbereich eines Flughafens.<sup>28</sup> In Betracht kommen zudem reisende Agenten, die innerhalb Europas durch den BND überwacht werden und Deutschland bloß durchfahren bzw. durchstreifen. Der auslandsnachrichtendienstliche Bedarf einer solchen Regelung ist nachvollziehbar und die Frist fällt angemessen kurz aus. Zwar beschränkt sich der Wortlaut weder auf den Transit noch unterscheidet er nach dem Gewicht der Maßnahme, wäre die Fortführung einer Telekommunikationsüberwachung über einen Zwischenstopp hinweg doch eher hinnehmbar als etwa der Zugriff auf privat genutzte informationstechnische Systeme durch die auf deutschem Boden erleichterten Zugriffsmöglichkeiten. Man könnte somit der Auffassung sein, dass die Fortgeltung der niedrigeren Auslands-Schwellen nach dem Eingriffsgewicht abzustufen ist und für besonders intensive Maßnahmen jene Anforderungen mitsamt

<sup>25</sup> So überzeugend Arts/Jipp, GSZ 2026, 7 (9).

<sup>26</sup> Vgl. BVerfGE 154, 152, Rn. 68 ff.

<sup>27</sup> BVerfGE 154, 152, Rn. 104.

<sup>28</sup> Begr. zu § 6 Abs. 4 BNDG-E, BT-Drs. 21/7868, S. 364.

dem Kontrollregime zu übernehmen sind, die für Personen im Inland gelten. Verfassungsrechtlich zwingend erscheint uns dies aber nicht, da das Bundesverfassungsgericht generell gesprochen eine Absenkung des Schutzniveaus für Ausländer im Ausland ermöglicht und dies mit den geringer ausgeprägten Schutzpflichten sowie dem geringeren Vertrauen der Betroffenen in ihre Nichtüberwachung durch die deutsche Staatsmacht begründet hat. Genau ein solches schutzwürdiges Vertrauen kann bei einer Durchreise aber kaum aufgebaut werden – anders als wenn Ausländer vielleicht über viele Jahre in Deutschland leben und durch Familie, Arbeit usw. letztlich wie deutsche Staatsangehörige in das hiesige Gesellschaftsgefüge eingebunden sind.

#### 4. Informationszugänge (§§ 10–17)

Einen bedeutsamen Teil der Befugnisweiterungen bilden die ausgebauten Informationszugänge der §§ 10 bis 17 BNDG-E. Sie erschließen dem Dienst erhebliche Daten, die bei anderen Stellen vorhanden sind, und verpflichten diese weitgehend zur Antwort.<sup>29</sup> Der Entwurf unterscheidet dabei nach dem Adressaten: Inländische öffentliche Stellen dürfen dem BND von sich aus Informationen übermitteln, wenn tatsächliche Anhaltspunkte für ihre Erforderlichkeit zur Auslandsaufklärung bestehen. Für die Verfassungsschutzbehörden und den MAD, für das BSI (mit Ausnahme für die Meldestellenaufgaben), für die Zentralstelle für Finanztransaktionsuntersuchungen, für den Justizvollzug, für die Staatsanwaltschaften, für Polizeien und Zoll, für das BAMF und für die Finanzbehörden wird daraus eine Übermittlungspflicht, die nur in eng umschriebenen Konflikten zurücktritt – etwa bei überwiegenden Sicherheitsinteressen der Verfassungsschutzbehörden oder zum Schutz verdeckt eingesetzter Personen (§ 10 Abs. 1, 2 und 4).<sup>30</sup> Zu Recht nimmt der Entwurf das BSI aus, soweit eine Übermittlung im Widerspruch zu seinen Aufgaben als Meldestelle stünde (§ 10 Abs. 4 Nr. 2).<sup>31</sup> Wäre die Meldestelle einbezogen, drohte das BSI zum Schwachstellenlieferanten der Dienste zu werden. Wer Sicherheitslücken oder Angriffe meldet, tut das im Vertrauen darauf, dass das BSI hilft, die Lücke zu schließen, und sie nicht für fremde Zwecke offenhält. Eine Übermittlungspflicht hätte dieses Vertrauen untergraben und die Meldebereitschaft von Forschern, Herstellern und Betreibern gerade dort geschwächt, wo der Staat auf sie angewiesen ist. Dahinter steht auch die alte Frage, ob das BSI, das aus der Zentralstelle für das Chiffrierwesen hervorgegangen ist, eine Sicherheitsbehörde mit Informationsauftrag oder eine Behörde für Informationssicherheit sein soll. Für die Meldestelle beantwortet der Entwurf sie richtig.

Daten, die eine Behörde unter einer bestimmten Zweckbindung erhoben hat, werden nach dem Gesetzentwurf wie soeben dargestellt in potentiell großem Stil für die Auslandsaufklärung umgewidmet. Jede solche Umwidmung ist ein eigener Grundrechtseingriff, dessen Gewicht sich nach dem Gewicht der ursprünglichen Erhebung und der geplanten Folgeverarbeitung richtet.<sup>32</sup> Für Daten aus eingriffsintensiven Maßnahmen verlangt das Bundesverfassungsgericht deshalb, der neue Zweck müsse dem Schutz von Rechtsgütern eines solch hohen Gewichts dienen, dass er nach den Wertungen des Grundgesetzes ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnte (Grundsatz der hypothetischen Datenneuerhebung), und dass sich aus den Daten ein

<sup>29</sup> BT-Drs. 21/7868, S. 78 ff.

<sup>30</sup> Der Bundesrat bittet zu prüfen, ob auf die Übermittlungspflicht der Finanzbehörden (§ 10 Abs. 2 S. 1 Nr. 6) verzichtet werden kann; die Bundesregierung hält an ihr fest, BT-Drs. 21/8295, S. 8, 14. Kritisch zur Einbeziehung des BSI, das dadurch an Vertrauen als neutrale Ansprechstelle verlieren dürfte, Höning, Ein legislativer Rundumschlag, VerfBlog v. 14.8.2026, <https://verfassungsblog.de/geheimdienstreform-rundumschlag>. Ihre Sorge betrifft nach der Ausnahme für die Meldestelle allerdings nur noch Erkenntnisse, die das BSI außerhalb dieser Aufgabe gewinnt.

<sup>31</sup> Begr. zu § 10 BNDG-E, BT-Drs. 21/7868, S. 367.

<sup>32</sup> Vgl. BVerfGE 141, 220 (324 ff.) (BKAG); BVerfG, Urt. v. 1.10.2024, 1 BvR 1160/19 (BKAG II).

konkreter Ermittlungsansatz ergibt.<sup>33</sup> Gemessen daran halten wir die Übermittlungspflichten im Grundsatz für tragfähig: Erstens hat der neue Zweck hohes Gewicht, weil die Auslandsaufklärung nach § 2 Abs. 1 S. 2 auf die Früherkennung von Bedrohungen besonders gewichtiger Rechtsgüter festgelegt ist (B.I.1). Zweitens bleibt die Schutzwirkung der ursprünglichen Zweckbindung erhalten, weil auch die Übermittlungspflicht nur greift, soweit besondere gesetzliche Übermittlungsregelungen nicht entgegenstehen (§ 10 Abs. 1 und 2). Die Übermittlungsschranken des abgebenden Fachrechts, etwa für Daten aus heimlichen strafprozessualen oder polizeilichen Maßnahmen, setzt der Entwurf also nicht außer Kraft. Drittens folgen auf die Übermittlung keine unmittelbaren Exekutivmaßnahmen, sondern die Daten werden im Auslandsnachrichtendienst verarbeitet. Möchte der BND sie wiederum an andere Strafverfolgungs- und Gefahrenabwehrbehörden weiterleiten oder den gleichen Stellen in aufbereiteter Form zur Verfügung stellen, so unterliegt er wiederum den entsprechenden Schwellen. Übermittlungspflichten zwischen Behörden sind der Rechtsordnung zudem auch sonst geläufig, etwa im Strafverfahren. Entscheidend muss bei alledem sein, ob die Schwellen nach dem Gewicht des jeweiligen Zugriffs abgestuft sind, und das ist jedenfalls nach kursorischer Durchsicht der Fall. Auch der automatisierte Abruf, den § 10 Abs. 2 S. 3 ermöglicht, beseitigt keine Übermittlungsvoraussetzung.

Auf Ersuchen muss zudem jede inländische öffentliche Stelle vorhandene und künftig anfallende Informationen übermitteln, soweit keine besondere Übermittlungsregel entgegensteht (§ 11 Abs. 1). Das ist angesichts der Schutzvorschriften der jeweiligen Fachgesetze, etwa Übermittlungsverboten und Zweckbindungen, unschädlich und wird die nachrichtendienstliche Praxis kaum verändern. Hinzu tritt die Einsicht des BND in amtliche Register, wenn ein Ersuchen den Zweck gefährden oder den Betroffenen unverhältnismäßig belasten würde oder Personen identifiziert werden sollen (§ 11 Abs. 2). Sie vertieft den Eingriff nicht typischerweise, sondern dient vor allem der operativen Sicherheit, weil der Dienst nicht durch ein Ersuchen offenlegen muss, auf wen er abzielt, während sich die materiellen Zugriffsvoraussetzungen unverändert aus dem jeweiligen Registerrecht ergeben. Weiter soll der BND bei tatsächlichen Anhaltspunkten für eine zumindest erhebliche Bedrohung Personen und Sachen im polizeilichen Informationsverbund verdeckt ausschreiben lassen dürfen (§ 11 Abs. 3). Darin liegt keine polizeiliche Maßnahme, die der Dienst selbst nicht vornehmen dürfte, denn die verdeckte Ausschreibung fordert weder eine Ingewahrsamnahme noch eine Festnahme, sondern zielt auf eine Informationsmitteilung ab (zum Beispiel, dass eine Person eine bestimmte Übertrittsstelle passiert hat). Zwar könnten sich zum Beispiel Grenzpolizeibeamte bei einer auslösenden verdeckten Ausschreibung motiviert sehen, eingehendere Personen- oder Gepäckkontrollen durchzuführen oder andere polizeiliche Folgemaßnahmen auszulösen. Diese stützten sich aber nicht auf die Ausschreibung des Dienstes selbst, sondern müssten die eigenen polizeirechtlichen Eingriffsschwellen in der Verantwortung der handelnden Beamten erfüllen. Grob gesprochen ergänzt die geplante verdeckte Ausschreibung in INPOL vor allem die bereits zulässige Ausschreibung im Schengener Informationssystem.<sup>34</sup> Die verdeckte Ausschreibung ist deshalb verfassungsrechtlich zulässig und angesichts ihres Erkenntnisgewinns rechtspolitisch sinnvoll. Schließlich soll der BND öffentliche Videoüberwachung mitbenutzen und ihre Daten in Echtzeit ausleiten (§ 11 Abs. 4).<sup>35</sup> Maßstab ist auch hier der Gedanke der hypothetischen Datenneuerhebung, also die Frage, ob der Dienst für seine Aufgabe selbst Videoanlagen aufstellen dürfte. Das wird man bejahen müssen, wenn schon örtliche Polizei- und Kommunalbehörden solche Anlagen zu geringeren Schutzzwecken wie der Verfolgung allgemeiner Straftaten oder Ordnungswidrigkeiten aufstellen dürfen, während der BND auf

<sup>33</sup> Vgl. BVerfGE 141, 220 (328 f.), wobei damit keine „konkrete“ Gefahr o. Ä. gemeint ist.

<sup>34</sup> Vgl. hierzu, auch für den BND, § 17 Abs. 3 BVerfSchG (geltende Fassung).

<sup>35</sup> Kritisch zur weiter reichenden Parallelbefugnis des BfV (§ 15 BVerfSchG-E) Höning, VerBlog v. 14.8.2026 (Fn. oben).

den Schutz besonders gewichtiger Rechtsgüter festgelegt ist. Werden Ausschreibungen oder Videodaten mit biometrischen Verfahren verknüpft, gelten nach der Regelungstechnik des Entwurfs zudem die besonderen befugnisrechtlichen Hürden dieser Verfahren (die allerdings sehr niedrig sind).

Gewichtiger als die gegenüber staatlichen Stellen ermöglichten Informationserhebungen sind die geplanten Ersuchen an nichtöffentliche Stellen – denn hier greift der Staat auf Datenbestände Privater zu, die für ganz andere Zwecke angelegt wurden. Das geltende Recht kennt besondere Auskunftsverlangen nur gegenüber einzelnen Branchen wie Luftfahrtunternehmen, Kreditinstituten und Telekommunikationsanbietern (§§ 3, 4 BNDG i.V.m. § 8a BVerfSchG), die Stück für Stück aus aktuellem Anlass eingeführt wurden, namentlich nach den Anschlägen vom 11. September 2001 für Fluggastdaten. Künftig kann der BND nach dem Regierungsentwurf alle Stellen ersuchen, die öffentlich zugängliche Leistungen im Personen- oder Güterverkehr erbringen, ferner Kraftfahrzeughersteller und subsidiär Werkstätten, die nach dem Geldwäschegesetz Verpflichteten, Post- und Warenverkehrsdienste, Telekommunikationsanbieter, digitale Dienste und technische Zahlungsdienste (§ 12 Abs. 2 S. 1 Nr. 1 bis 7). Auf der ersten Stufe fragt er nach Bestandsdaten, also den Daten des Nutzungsverhältnisses, und nach Sachinformationen über den angebotenen Dienst, wofür genügt, dass die Auskunft im Einzelfall zur Auslandsaufklärung oder zum Schutz des Betroffenen erforderlich ist (§ 12 Abs. 1). Bei Telekommunikations- und digitalen Diensten darf er außerdem anhand einer IP-Adresse, eines Zahlungsmittels oder von Anmeldedaten den Nutzer ermitteln lassen und nach Zugangssicherungen wie Passwörtern fragen (sofern irgendein Provider diese tatsächlich noch offen, also ohne Umwandlung in eine Hash-Prüfsumme, speichern sollte). Letzteres gilt allerdings nur, wenn er die geschützten Daten auch nutzen dürfte (Abs. 4 und 5). Die ersuchte Stelle muss unverzüglich und vollständig antworten (§ 16 Abs. 1 und 3).

Für Bestandsdaten ist die niedrige Schwelle *im Grundsatz* tragfähig, weil ihr Eingriffsgewicht vergleichsweise gering ist und das Bundesverfassungsgericht es für nachrichtendienstliche Auskünfte dieser Art genügen lässt, dass sie zur Aufklärung einer bestimmten beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten sind.<sup>36</sup> Namentlich bei Verkehrsunternehmen sowie Kraftfahrzeugherstellern und -werkstätten ist die Erweiterung konsequent: Wieso wird der Bahnreisende bislang mehr geschützt als der Fluggast? Auch die Einbeziehung digitaler Dienste ist eine Anpassung an die Wirklichkeit, denn dass das geltende Recht sie nicht erfasst, hat historische Gründe und wurzelt nicht im Eingriffsgewicht selbst. Auch liegt es auf der Hand, dass die verbreiterte Erkenntnismöglichkeit in die sozialen Netzwerke eine Reaktion auf deren Nutzung als Aktionsraum von Extremisten, Terroristen und fremden Mächten darstellt – von der Desinformation bis zur Anwerbung von Terroristen. Anders liegt die verfassungsrechtliche Wertung bei der Zuordnung einer IP-Adresse, die die Karlsruher Richter an einen gesteigerten Rechtsgüterschutz gebunden haben.<sup>37</sup> § 12 Abs. 4 stellt dafür keine eigenen Anforderungen auf, so dass die allgemeine Schwelle des Absatzes 1 gilt. Verfassungsrechtlich dürfte die Ausrichtung der Aufgabe auf besonders gewichtige Rechtsgüter (§ 2 Abs. 1 S. 2, B.I.1) diese Anforderung wohl tragen, die Begründung sollte darauf aber ausdrücklich Bezug nehmen und sich damit erkennbar an der Verfassungsrechtsprechung ausrichten.

Über Bestandsdaten deutlich hinaus reichen die qualifizierten Ersuchen des § 13. Mit ihnen kann der BND bei denselben Stellen alle dort vorhandenen Informationen erfragen, wobei er nicht auf Bestands- oder Sachdaten beschränkt ist (Abs. 1). Je nach Adressat sind das Reise- und

<sup>36</sup> Begr. zu § 12 BNDG-E, BT-Drs. 21/7868, S. 371, unter Hinweis auf BVerfGE 130, 151, Rn. 122, und BVerfGE 156, 11, Rn. 119.

<sup>37</sup> BVerfGE 155, 119 (Bestandsdatenauskunft II), dort zur Zuordnung dynamischer IP-Adressen.

Buchungsdaten, Telemetrie- und Standortinformationen von Fahrzeugen, Kontobewegungen, Sendungsdaten, die Verkehrsdaten der Telekommunikation und bei digitalen Diensten die Nutzungsdaten bis hin zu den Inhalten, die Nutzer dort hinterlegt oder ausgetauscht haben. Solche qualifizierten Ersuchen stuft der Entwurf nach dem Inlandsbezug ab: Betrifft das Ersuchen Ausländer im Ausland oder Informationen ohne Personenbezug, genügt wie bei Bestandsdaten die Erforderlichkeit im Einzelfall (Abs. 1 S. 1). Sind hingegen Deutsche, Personen im Bundesgebiet oder inländische juristische Personen betroffen, müssen tatsächliche Anhaltspunkte dafür bestehen, dass Informationen zu zumindest erheblichen Bedrohungen erlangt werden (Abs. 1 S. 2). Das Ersuchen darf sich in diesem Fall zudem nur auf Verantwortliche und Unterstützer, auf Mitglieder eines entsprechenden Netzwerks oder auf Personen beziehen, deren Zusammenhang mit der Bedrohung Erkenntnisse verspricht, etwa weil sie für einen Verantwortlichen Leistungen in Anspruch nehmen oder Mitteilungen weitergeben (Abs. 2 S. 1). Damit geht der Entwurf über das geltende BNDG hinaus, das – sofern eine solche Abfrage überhaupt geregelt ist – Tatsachen für schwerwiegende Gefahren in bestimmten Gefahrenbereichen verlangt.<sup>38</sup>

Jene Absenkung folgt der neuen Schwellendogmatik (vgl. unter B.I.2). Bei Telekommunikationsanbietern genügt zudem eine räumlich und zeitlich hinreichende Bezeichnung der Daten, wenn die Maßnahme sonst aussichtslos oder wesentlich erschwert wäre (Abs. 2 S. 2). Das nähert sich dem Eingriffsgewicht einer Funkzellenabfrage an, die unbeteiligte Dritte in großer Zahl erfasst, unterliegt aber immerhin der Vorabkontrolle (§ 97 Abs. 1 Nr. 1). Insgesamt drängt sich die Frage auf, ob die entsprechenden Schwellen angesichts der potentiell sehr weitreichenden Persönlichkeitserfassungen nicht jeweils eine Stufe zu niedrig liegen. Sie lässt sich – freilich – nicht pauschal beantworten, sondern nur nach den ersuchten Stellen und den dort zu erwartenden Erkenntnissen. Maßstab ist, dass die Eingriffsschwelle mit dem Gewicht des Zugriffs adäquat steigen muss (vgl. unter B.I.2), wobei sich ein Vergleich mit jenen technischen Befugnissen und ihren Schwellen anbietet, mit denen der Dienst dieselben Erkenntnisse selbst gewinnen könnte. Gegenüber Ausländern im Ausland rechtfertigt zudem der Gedanke, dass Erkenntnisse dort in der Regel (erst recht) nicht unmittelbar zu Folgemaßnahmen führen, das Absenken der rechtlichen Anforderungen, worauf sich die Gesetzesbegründung zu Recht stützt.<sup>39</sup>

Gemessen daran scheinen die Schwellen überwiegend tragfähig: Reise- und Buchungsdaten der Verkehrsunternehmen zeigen, wer wann wohin gereist ist und mit wem, und stellen damit Ausschnitte des Bewegungsverhaltens im öffentlichen Raum dar. Sie kennt das geltende Recht für Flugpassdaten schon und ihr Gewicht trägt die mittlere Bedrohungs-Stufe ohne Weiteres. Kontobewegungen wiegen zwar schwerer, weil sich aus dem Zahlungsverkehr gerade bei häufiger Nutzung auch für kleinere Summen die Lebensführung mitsamt dem Beziehungsleben und privaten Gewohnheiten ablesen lässt. Für die Aufklärung von Terrorismusfinanzierung, Proliferationsnetzwerken und verdeckter staatlicher Einflussnahme sind sie aber oft der einzige erfolgversprechende Zugang. Zudem kennt das geltende Recht bereits Auskünfte der Kreditinstitute. Die Schwelle scheint daher ebenfalls (noch) vertretbar, wobei eine Klausel rechtspolitisch zu empfehlen ist, wonach als besonderer Ausfluss aus dem Verhältnismäßigkeitsgrundsatz kein vollständiges Persönlichkeitsprofil erstellt werden darf und sich auch tiefeschürfendes Profiling stets auf Umstände beschränken muss, die zur nachrichtendienstlichen Aufklärung erforderlich sind. Sendungsdaten der Post- und Warenverkehrsdienste betreffen wiederum die Umstände der Verkehre, deren Inhalt dem Öffnen und

<sup>38</sup> Begr. zu § 13 Abs. 1 BNDG-E, BT-Drs. 21/7868, S. 375 f.; zum geltenden Recht § 3 Abs. 1 BNDG i.V.m. § 8a BVerfSchG.

<sup>39</sup> Begr. zu § 13 Abs. 1 BNDG-E, BT-Drs. 21/7868, S. 376, unter Berufung auf BVerfGE 154, 152.

Einsehen nach § 28 mit höheren Schwellen vorbehalten bleibt, worauf § 13 Abs. 4 die Herausgabe von Sendungen folgerichtig beschränkt. Die Einbeziehung ist daher unproblematisch. Für die Verkehrsdaten der Telekommunikation schließlich, die nach der Rechtsprechung tiefe Einblicke in soziale Beziehungen und Bewegungen erlauben,<sup>40</sup> stimmt die Schwelle mit der Telekommunikationsüberwachung überein, die Metadaten ebenso gestuft zulässt (§ 35 Abs. 1 S. 1, Abs. 2 S. 1). Mit Inlandsbezug unterliegt das Ersuchen zudem der Vorabkontrolle. Die Zuordnung ist somit ebenfalls vertretbar. Positiv hervorzuheben ist ferner § 13 Abs. 3: Er erlaubt Ersuchen an Güterverkehrs- sowie Post- und Warenverkehrsdienstleister ohne konkreten Personenbezug, um grenzüberschreitende Transportwege und Beschaffungsrouten aufzuklären. Obwohl die Norm vergleichsweise geringe Persönlichkeitserfassungen vorhersehen lässt, sind solche Ersuchen nur bei tatsächlichen Anhaltspunkten für eine zumindest erhebliche Bedrohung zulässig. Damit erfüllt sie einen präzise auf strukturelle nachrichtendienstliche Auslandsaufklärung zugeschnittenen Auftrag, besonders im Bereich von Proliferationsnetzwerken<sup>41</sup>, und ist schwellenmäßig eher hoch angesiedelt.

Nicht alle Schwellenzuordnungen können derart überzeugen. So sollen Telemetrie- und Standortdaten aus vernetzten Fahrzeugen rückwirkend und, mit der Erstreckung auf künftig anfallende Daten, über bis zu ein Jahr erfasst werden können, woraus sich bei intensiver Fahrzeugnutzung ein quasi-lückenloses Bewegungsprofil gewinnen lässt (§ 9). Dieselbe Erkenntnis aus einer eigenen Standortfeststellung über mehr als 30 Tage darf der Auslandsnachrichtendienst dagegen nur bei einer erheblichen Bedrohung bzw. gegenüber Deutschen sogar erst bei einer Bedrohung von herausgehobener Bedeutung vornehmen (§ 26 Abs. 1 Nr. 2, Abs. 2 Nr. 2). Die Schwellen für fahrzeugbezogene Ersuchen, soweit sie einen vergleichbaren Zeitraum erschließen, liegen deshalb im In- wie im Ausland eine Stufe zu tief. Noch deutlicher ist das Gefälle bei den digitalen Diensten. Ein soziales Netzwerk oder ein Messengerdienst verwahrt nicht nur Nutzungsdaten, sondern auch die Inhalte privater Kommunikation über Direktnachrichten für Jahre. § 13 Abs. 1 erfasst diese Inhalte, weil er alle Informationen zulässt, die über Bestandsdaten hinausgehen, und Absatz 6 schränkt den Zugriff nur bei clouddartigen Diensten ein, die Nutzern Speicherplatz und Anwendungen für eigene Daten bereitstellen.<sup>42</sup> Für das BfV erstreckt die Begründung die qualifizierte Auskunft ausdrücklich auch auf Inhalte von Nutzungen und hält das für unbedenklich, weil bei sozialen Medien nur enge Ausschnitte von Kommunikation erschlossen würden.<sup>43</sup> Für Kaufvorgänge und öffentlich sichtbare Beiträge mag das überzeugen, nicht aber bezüglich gespeicherter privater Nachrichten. Sie stehen auch bei nicht-klassischen Anbietern von Telekommunikationsverkehren unter dem Schutz des Art. 10 GG.<sup>44</sup> Da ein Ersuchen einen vollständigen Kommunikationsverlauf erschließen kann, übersteigt es sogar den typischerweise zu erwartenden Ertrag einer befristeten Telekommunikationsüberwachung und nähert sich insoweit einer auf Kommunikationsverkehre begrenzten Online-Durchsuchung an. Diese Eingriffsintensivität zeichnet der Regierungsentwurf nicht nach, da er für den Abruf solcher Inhalte die Erforderlichkeit gegenüber Ausländern im Ausland und die erhebliche Bedrohung bei Inlandsbezug genügen will. Für Kommunikationsinhalte verlangt er in § 35 jeweils eine Stufe mehr, nämlich die erhebliche Bedrohung im Ausland und die Bedrohung von herausgehobener Bedeutung im Inland (§ 35 Abs. 1 S. 2, Abs. 2 S. 2). Dies wäre auch für die qualifizierten Ersuchen bei Online-Diensten die angemessene Schwellenzuordnung; alternativ müsste klargestellt werden, dass auch Kommunikation über Online-Dienste nur dem § 35 als *lex specialis* unterfällt. Für Post und

<sup>40</sup> BVerfGE 125, 260 (319) (Vorratsdatenspeicherung).

<sup>41</sup> Begr. zu § 13 Abs. 3 BNDG-E, BT-Drs. 21/7868, S. 377 f.

<sup>42</sup> Begr. zu § 13 Abs. 6 BNDG-E, BT-Drs. 21/7868, S. 378 f.

<sup>43</sup> Begr. zu § 11 Abs. 3 BVerfSchG-E, BT-Drs. 21/7868, S. 232.

<sup>44</sup> BVerfGE 124, 43 (54 ff.) (E-Mails beim Provider).

Telekommunikation vermeidet der Entwurf dieses Gefälle übrigens, indem er die Herausgabe von Inhalten an die jeweilige Überwachungsbefugnis bindet (§ 13 Abs. 4 und 5).

Die Absätze 4 und 5 verpflichten Post- und Telekommunikationsanbieter schließlich, bei der Durchführung angeordneter Maßnahmen mitzuwirken. Dies umfasst auch die Unterstützung beim Einbringen technischer Mittel durch Umleitung der Telekommunikation. Damit übernimmt der Entwurf die bekannten Mitwirkungspflichten der Anbieter aus § 2 G 10.<sup>45</sup> Die Überwachungsbefugnis selbst, also das Gegenstück zu den §§ 1, 3 G 10, enthält § 35 BNDG-E (dazu unter B.IV).<sup>46</sup> Absatz 6 beschränkt den Zugriff auf Daten, die Nutzer in Clouddiensten verarbeiten, auf die Durchführung informationstechnischer Eingriffe nach den §§ 36 bis 38. Der Ausschuss sollte die Klarstellung der Bundesregierung, dass die Mitwirkungspflichten weder zur Entschlüsselung noch zur Schaffung oder Offenhaltung von Schwachstellen verpflichten, in seinem Bericht festhalten. Das gibt den Anbietern Rechtssicherheit, ohne den Umkehrschluss zu eröffnen, den die Bundesregierung bei einer Regelung im Gesetz befürchtet. Diese Mitwirkungspflichten teilen das Kontrollregime der jeweiligen Hauptmaßnahme, was sachgerecht ist. Eng gefasst sind auch die besonderen Ersuchen bei informationstechnischen Angriffen – deren letzte Stufe, die Herausgabe einer Systemkopie, konsequenterweise der Vorabkontrolle unterliegt (§ 14, § 97 Abs. 1 Nr. 2) – und die Mitbenutzung privater Videoüberwachung, die eine zumindest erhebliche Bedrohung voraussetzt (§ 15).

Auf alle Ersuchen hin ist die Stelle zur Auskunft oder Mitwirkung verpflichtet, sofern sie in Deutschland eine Niederlassung hat oder ihre Leistung hier erbringt (§ 16 Abs. 1 und 4). Die Pflicht erfasst vorhandene Daten, kann aber auch auf Daten erstreckt werden, die binnen zwölf Monaten anfallen, und mit der Pflicht verbunden werden, künftig anfallende Daten zu speichern (§ 9). So konsequent diese aus dem G 10-Bereich schon bekannte Heimlichkeitspflicht zur nachrichtendienstlichen Zielerreichung ist, erhöht die langfristige klandestine Informationshortung beim Anbieter doch das Eingriffsgewicht nicht unerheblich. Weder können Betroffene mangels Kenntnis des Sachverhalts rechtliche Überprüfungen anstrengen noch die auskunftspflichtige Stelle, weil die Voraussetzungen jedenfalls nach dem Willen der Gesetzesbegründung allein der BND verantwortet.<sup>47</sup> Umso mehr kommt es auf das Verfahren an. Eine Anordnung der Behördenleitung und die Vorabkontrolle durch den UKRat verlangt der Entwurf aber nur für qualifizierte Ersuchen mit Inlandsbezug an Post- und Telekommunikationsanbieter (§ 17 Abs. 1, § 97 Abs. 1 Nr. 1), weil nur dort besonders schützenswerte Daten betroffen seien.<sup>48</sup> Das überzeugt nicht. Konto- und Reisebewegungen sowie Nutzungsinformationen digitaler Dienste und Standortdaten vernetzter Fahrzeuge lassen in einem derart langen Zeitraum potentiell ähnlich genaue Rückschlüsse auf das Privatleben zu wie die Verkehrsdaten der Telekommunikation. Von Verfassungen wegen muss das Eingriffsgewicht aus der Art der Daten und der Dauer des möglichen Zugriffs bestimmt werden, nicht aber aus der Branche des Adressaten. Anordnung und Vorabkontrolle sollten deshalb jedenfalls auf qualifizierte Ersuchen mit Inlandsbezug erstreckt werden, die Finanz-, Bewegungs- oder Nutzungsdaten mit profilbildender Nähe betreffen

---

<sup>45</sup>Eine Pflicht zur Entschlüsselung oder zur Schaffung, Offenhaltung oder Nutzung von Zugängen und Schwachstellen begründen die Mitwirkungspflichten nach der Gegenäußerung der Bundesregierung nicht. Den Vorschlag des Bundesrates, dies ausdrücklich zu regeln, hält sie wegen der Gefahr von Umkehrschlüssen für entbehrlich, BT-Drs. 21/8295, S. 4 f., 8, 13 f. (dort zu Nummer 13 mit Verweis auf die Ausführungen zu Nummer 7, gemeint ist ersichtlich Nummer 6).

<sup>46</sup>Für das BfV vgl. § 22 BVerfSchG-E, das daneben Ersuchen um Kommunikationsinhalte unmittelbar an die Anbieter kennt (§ 13 Abs. 4 BVerfSchG-E, dazu unter C.III).

<sup>47</sup>Begr. zu § 13 Abs. 1 BNDG-E, BT-Drs. 21/7868, S. 376.

<sup>48</sup>Begr. zu § 17 Abs. 1 BNDG-E, BT-Drs. 21/7868, S. 382.

und entweder eine Speicherung über mehr als sechs Monate in die Zukunft anordnen oder vergleichbar umfangreiche bereits gespeicherte Informationen erfassen.

Gegenüber Anbietern elektronischer Kommunikationsdienste könnte eine solche Kontrolle zudem unionsrechtlich geboten sein. Für die Anwendbarkeit des Unionsrechts spricht zumindest die Rechtsprechung des Gerichtshofs der Europäischen Union in ähnlichen Konstellationen. Nur solche Maßnahmen zum Schutz der nationalen Sicherheit sollen dabei ausschließlich dem nationalen Recht unterfallen, die die Dienste selbst und ohne Inanspruchnahme privater Anbieter durchführen. Verpflichtet der Staat dagegen Anbieter elektronischer Kommunikationsdienste, Daten zu speichern, an Sicherheitsbehörden zu übermitteln oder Zugang zu gewähren, ist die Datenschutzrichtlinie für elektronische Kommunikation anwendbar, auch wenn die Pflicht dem Schutz der nationalen Sicherheit dient.<sup>49</sup> Das gilt – im Grundsatz – selbst für SIGINT- und HUMINT-Auslandsnachrichtendienste<sup>50</sup>, und es gilt unabhängig von Staatsangehörigkeit und Aufenthaltsort der Betroffenen, weil die Richtlinie an die Tätigkeit des Anbieters in der Union anknüpft. Gegen die Anwendbarkeit im konkreten Rechtssetzungsfall lässt sich jedoch anführen, dass das Bundesverfassungsgericht die datenschutzbezogenen Rechtsakte der Union auf die strategische Inland-Ausland-Fermeldeaufklärung des BND für nicht anwendbar hält,<sup>51</sup> obwohl gerade diese Aufklärung auch durch eine Ausleitung der Anbieter nach § 2 G 10 durchgeführt wird. Die Auffassung des Bundesverfassungsgerichts ist zumindest ein gewichtiges Ergebnis bei der Auslegung des Unionsrechts. Hinzu kommt, dass Auskunftersuchen an Anbieter zum Standardrepertoire der Dienste gehören: Mit Art. 4 Abs. 2 S. 3 EUV hat die Union die nationale Sicherheit und damit die Arbeit der Nachrichtendienste den Mitgliedstaaten vorbehalten – jene Grundentscheidung liefe leer, wenn undifferenziert jede Mitwirkung eines Anbieters den Anwendungsbereich des Unionsrechts eröffnete. Ob die Richtlinie auf die Auskunftspflicht und Mitwirkungspflichten des BNDG-E anwendbar ist, lässt sich insofern nicht abschließend beantworten. Betroffen wären die Pflichten der Telekommunikationsanbieter nach den §§ 12, 13 Abs. 1 und 5 sowie Messenger und andere nummernunabhängige interpersonelle Kommunikationsdienste, die als digitale Dienste i.S.v. § 12 Abs. 2 S. 1 Nr. 6 zählen dürften.<sup>52</sup>

Zudem verlangt der Gerichtshof für die Echtzeiterhebung von Verkehrs- und Standortdaten zum Schutz der nationalen Sicherheit eine vorherige Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle mit bindender Entscheidung und beschränkt sie auf Personen, bei denen ein triftiger Grund für den Verdacht einer Beteiligung an terroristischen Aktivitäten besteht. Für die automatisierte Analyse verlangt er eine wirksame Kontrolle.<sup>53</sup> Eine vorherige Kontrolle für den Zugang zu gespeicherten Verkehrs- und Standortdaten hat er bislang für die Strafverfolgung ausgesprochen,<sup>54</sup> wohingegen er für den Zugang zu Identitätsdaten, die einer IP-Adresse zugeordnet sind, unter engen Voraussetzungen auf sie verzichtet hat.<sup>55</sup> Ob der Gerichtshof entsprechende Vorgaben bei Zugriffen auf gespeicherte Verkehrsdaten durch Nachrichtendienste zum Schutz der nationalen Sicherheit ebenso verlangt, hat er nicht entschieden – nach der Linie seiner Rechtsprechung ist es weder zwingend noch ausgeschlossen. Vor diesem Hintergrund sei darauf hingewiesen, dass

<sup>49</sup> EuGH (GK), Urt. v. 6.10.2020, C-511/18 u.a., La Quadrature du Net u.a.; EuGH (GK), Urt. v. 6.10.2020, C-623/17, Privacy International.

<sup>50</sup> Das vorbezeichnete Verfahren Privacy International betraf wesentlich den britischen Signalerfassungsdienst Government Communications Headquarters (GCHQ), daneben waren der HUMINT-orientierte Auslandsdienst Secret Intelligence Service (MI6) und der Inlandsdienst Security Service (MI5) verfahrensgegenständlich.

<sup>51</sup> BVerfGE 170, 79, Rn. 77.

<sup>52</sup> Für das BfV gilt dasselbe für die Auskunftspflichten der §§ 11 ff. BVerfSchG-E (vgl. unter C.III).

<sup>53</sup> EuGH (GK), Urt. v. 6.10.2020, C-511/18 u.a., La Quadrature du Net u.a., Tenor Nr. 2.

<sup>54</sup> EuGH (GK), Urt. v. 2.3.2021, C-746/18, Prokuratuur.

<sup>55</sup> EuGH (Plenum), Urt. v. 30.4.2024, C-470/21, La Quadrature du Net u.a.

Echtzeitausleitungen bei Telekommunikationsanbietern gegenüber Ausländern im Ausland (§ 13 Abs. 5 i.V.m. § 35 Abs. 1) nach dem Regierungsentwurf bislang keiner Vorabkontrolle unterliegen, weil § 97 Abs. 1 Nr. 13 nur die Überwachung nach § 35 Abs. 2 erfasst und § 97 Abs. 1 Nr. 1 nur Ersuchen mit Inlandsbezug an Post- und Telekommunikationsanbieter der Vorabkontrolle unterwirft. Gerade eine Differenzierung nach In- und Ausländern sieht die Richtlinie jedoch nicht vor. Zumindest die Begründung sollte die unionsrechtliche Einordnung der Anbieterpflichten deshalb vertieft behandeln und die legislativen Wertungen der Bundesrepublik für eine eventuelle Überprüfung vor dem Gerichtshof der Europäischen Union dokumentieren. Rechtssicherer wäre es, die Vorabkontrolle auf Echtzeitausleitungen und auf Ersuchen um gespeicherte Verkehrs- und Standortdaten bei Anbietern elektronischer Kommunikationsdienste auch ohne Inlandsbezug zu erstrecken. Gleichwohl ist uns klar, dass damit eine nicht unwesentliche Mehrarbeit auf den UKRat zukäme und vor allem die Schlagkraft des auswärtigen Nachrichtenwesens unter den zeitlichen Folgen leiden würde. Hier abzuwägen ist vorrangige Aufgabe des Bundesgesetzgebers.

## **5. Heimliches Betreten von Wohnungen (§ 18 Abs. 2)**

Die Befugnis, Wohnungen heimlich zu betreten, hat in der öffentlichen Debatte besondere Aufmerksamkeit gefunden. Der Entwurf gesteht sie BND und BfV in nahezu gleicher Gestalt (§ 18 Abs. 2 BNDG-E, § 16 Abs. 6 BVerfSchG-E) zu,<sup>56</sup> weshalb die Befugnisserweiterung hier insgesamt betrachtet wird. Entgegen politisch-medialen Besorgnissen stellt sie keinen historischen „Dammbruch“ dar, indem Nachrichtendienstangehörige in kriminalpolizeilicher Manier und im landläufig verstandenen Sinne Wohnungen „durchsuchen“ dürfen. Das im Rahmen der vorliegenden Novelle den Diensten zugestandene Betreten dient hingegen ausschließlich der Vorbereitung und Durchführung einer Überwachung mit spezifisch nachrichtendienstlichen Mitteln, typischerweise dem Aufspielen von Spähsoftware auf ein elektronisches Gerät, das aus der Ferne nicht zu erreichen ist. Die rechtliche Möglichkeit hierzu ist beispielsweise im Rahmen der Quellen-Telekommunikationsüberwachung bereits eröffnet, allerdings scheitert das Aufspielen praktisch bisweilen daran, dass moderne Geräte (etwa neue iPhones im „Blockierungsmodus“) selbst über sehr teure und überdies nicht unproblematische Anwendungen wie „Pegasus“ oder „Predator“ nicht sicher mit Spähsoftware zu infizieren sind. Auch sind diese Befugnisse kein Neuland: Mehrere deutsche Länder haben ihren Verfassungsschutzbehörden in den letzten Jahren entsprechende Eingriffe zugestanden, die praktisch ein Instrument für wenige Ausnahmefälle bleiben.<sup>57</sup> Das Bundesverfassungsgericht hatte jedenfalls die bayerische Regelung 2022 nicht beanstandet.<sup>58</sup>

Hinsichtlich der für den BND nun geplanten befugnisrechtlichen Schwellen setzt § 18 Abs. 2 S. 2 BNDG-E eine erhebliche Bedrohung voraus, knüpft also nur an die mittlere Stufe der dreistufigen Schrankenlogik des neuen Gesetzes an. Für alle Wohnungen im Bundesgebiet und für Wohnungen Deutscher im Ausland gelten nach Satz 3 darüber hinaus die Erfordernisse einer konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut, verbunden mit dem Erfordernis einer besonderen Anordnung. Nur jene Inlands-Fälle unterwirft § 97 Abs. 1 Nr. 3 einer eigenständigen Vorabkontrolle des Betretens durch den UKRat, auch wenn das vorbereitete Mittel selbst keiner Vorabkontrolle bedarf. Die Inlandsschwelle entspricht damit im Grundsatz der des BfV und der Vorgabe des

<sup>56</sup> BT-Drs. 21/7868, S. 85 f., 133 ff.

<sup>57</sup> Sehl, Geheimdienste: Warum der Verfassungsschutz schon jetzt heimlich in Wohnungen einbrechen darf, Legal Tribune Online v. 24.8.2026, [https://lto.de/persistent/a\\_id/60707](https://lto.de/persistent/a_id/60707).

<sup>58</sup> Art. 9 Abs. 1 S. 2, Art. 11 BayVSG; § 23 Abs. 2 S. 4, § 13 VSG NRW (dort nur zur Wohnraumüberwachung und mit Anordnung des Amtsgerichts). In BVerfGE 162, 1 wurden Art. 9 Abs. 1 S. 1 und Art. 10 Abs. 1 BayVSG a.F. beanstandet; die Betretensbefugnis war nicht Gegenstand der Prüfung (Rn. 91) und erscheint nur in der Wiedergabe der Norm.

Bundesverfassungsgerichts<sup>59</sup> (zur Problematik des UKRats gleich gesondert). Die abgesenkte Schwelle für Wohnungen von Ausländern im Ausland bedarf hingegen noch einer eigenen verfassungsrechtlich rechtfertigenden Begründung, weil die für Art. 10 GG anerkannten Differenzierungen nicht automatisch Abweichungen beim Schutz der Wohnung nach Art. 13 GG zulassen. Anders als bei der *Fernmeldeaufklärung*, wo die reduzierte Grundrechtsbindung von Drittstaatenbehörden durch den Maßnahmedressaten typischerweise zu erwarten ist, dürfte bei einem verständigen Dritten kein gleichartiges Verständnis dafür vorherrschen, dass die Bundesrepublik Deutschland als insofern fremde Macht nach dortigem Recht illegal in Wohnobjekte auf ausländischem Boden eindringt. Andererseits werden wohl wenige Auslandsausländer überhaupt davon ausgehen, dass sie nach dem Recht fremder Staaten grundrechtlich geschützt sind, wenn Auslandsnachrichtendienste auf externem Terrain operieren. Zudem ist eine allgemeine Grundrechtsbindung gegenüber Auslandsausländern nicht in gleichem Maße wie innerhalb der deutschen Staatsgrenzen zu erwarten. Wir erachten die niedrigere Schwelle nach alledem als verfassungsrechtlich riskant, halten sie aus gesetzgeberischer Sicht aber (noch) für vertretbar.

Über die Schwelle hinaus stellt sich die Frage, wie die Vorabkontrolle ausgestaltet sein muss und ob hierfür ein Richter im institutionellen Sinne zu bemühen ist. Verfassungsrechtlich ist das heimliche Betreten jedenfalls kein Fall der Schranke des Art. 13 Abs. 2 GG (ebenso wenig der Abs. 3 bis 5), sondern ein sonstiger Eingriff nach Art. 13 Abs. 7 GG. Das Bundesverfassungsgericht hat ausdrücklich offengelassen, ob das Betreten zur Infiltration eines informationstechnischen Systems begrifflich eine Durchsuchung darstellt, und eine Einschlägigkeit des Abs. 2 unabhängig davon verneint, weil dieser nur offene Durchsuchungen erfassen soll. Anders als Art. 13 Abs. 2 und 4 GG verlangt Abs. 7 seinem Wortlaut nach keine Vorabkontrolle durch den Richter. Insofern ist es missverständlich, dass das Bundesverfassungsgericht das heimliche Betreten zur Vorbereitung einer Online-Durchsuchung oder Quellen-Telekommunikationsüberwachung dennoch an eine „richterliche Anordnung“ gebunden hat.<sup>60</sup> Tatsächlich meinten die Karlsruher Richter, wie es sich aus den Entscheidungsgründen eindeutig ergibt, jedoch nur eine unabhängige Vorabkontrolle, die aus dem Verhältnismäßigkeitsgrundsatz heraus das besonders hohe Eingriffsgewicht eines solchen Betretens abfedert, und räumten dem Gesetzgeber Spielraum ein, wie er die unabhängige Stelle ausgestaltet.<sup>61</sup>

*Auch unabhängig von Art. 13 Abs. 2 GG dürfte aus allgemeinen Gründen der Verhältnismäßigkeit ein so schwerwiegender heimlicher Grundrechtseingriff grundsätzlich nicht ohne richterliche Anordnung erfolgen. Bewirkt eine heimliche Ermittlungsmaßnahme einen schwerwiegenden Grundrechtseingriff, so ist eine **vorbeugende Kontrolle durch eine unabhängige Instanz** verfassungsrechtlich geboten, weil die Betroffenen sonst ungeschützt blieben [...] Der Gesetzgeber hat allerdings bei der Gestaltung der Kontrolle im Einzelnen, etwa bei der **Entscheidung über die kontrollierende Stelle** und das anzuwendende Verfahren, grundsätzlich einen Spielraum. Bei einem Grundrechtseingriff von besonders hohem Gewicht reduziert sich dieser dahingehend, dass die Maßnahme grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen ist. Der Gesetzgeber **darf eine andere Stelle nur dann mit der Kontrolle betrauen, wenn diese gleiche Gewähr für ihre Unabhängigkeit und Neutralität bietet** [...].*

<sup>59</sup> Vgl. hierzu schon BVerfGE 165, 1 (Beschl. v. 9.12.2022, 1 BvR 1345/21), Leitsatz 2 und Rn. 147 ff. (SOG MV).

<sup>60</sup> Vgl. BVerfGE 165, 1, Leitsatz 2 und Rn. 147 ff. Die Entscheidung betraf zwar die Polizei, ihre Übertragung auf die Nachrichtendienste liegt aber nahe, weil das Gewicht eines heimlichen Betretens nicht davon abhängt, wer diesen Schritt vornimmt.

<sup>61</sup> BVerfGE 165, 1, Rn. 149; dazu sogleich.

*BVerfGE 165, 1 (Beschl. v. 9.12.2022, 1 BvR 1345/21), Rn. 149; Hervorhebungen durch Verf.*

Die hier einschlägige Anforderung, dass nicht dem institutionellen Richter entsprechende Kontrolleure die gleiche Gewähr für ihre Unabhängigkeit und Neutralität bieten müssen, erfüllt der UKRat (anders als wohl die G 10-Kommission) zweifellos. Auch der Gesetzentwurf fußt ausweislich seiner Begründung auf der These, dass die Vorabkontrolle durch den UKRat den Richtervorbehalt ersetzt und dessen Schutzaufgabe erfüllt.<sup>62</sup> In der Tat sind die Senatsmitglieder bei der Rechtskontrolle unabhängig und nur dem Gesetz unterworfen (§ 15 UKRatG-E). Zudem müssen mindestens sieben der neun Mitglieder des gerichtsähnlichen Kontrollorgans langjährig erfahrene Richter an obersten Bundesgerichten gewesen sein (§ 14 UKRatG-E, dazu D.III), deren Richteramt bloß ruht. Dauerhafte Spezialisierung, technische Unterstützung, eine Geheimschutzinfrastruktur sowie die Kenntnis der Maßnahmenzusammenhänge und die Verzahnung mit der Vollzugskontrolle entsprechen überdies in nahezu idealer Weise den Qualitätsmaßstäben, die das Bundesverfassungsgericht an eine wirk-same Vorabkontrolle stellt.<sup>63</sup> Verglichen besonders mit den Amtsgerichten, denen die Länder die Vorabkontrolle eingriffsintensiver Maßnahmen ihrer Verfassungsschutzbehörden übertragen haben, dürfte der UKRat die deutlich wirksamere Kontrolle bieten.<sup>64</sup> Sollte das Bundesverfassungsgericht, aus hiesiger Sicht wider Erwarten, später doch einen Richter im institutionellen Sinne fordern, lässt sich die Zuständigkeit ohne Systembruch auf das Bundesverwaltungsgericht verlagern, das nach dem Entwurf ohnehin über Anwendungsfälle der Wohnraumüberwachung nach Art. 13 GG entscheiden soll (§ 97 Abs. 6 und 7 BNDG-E, § 34 Abs. 4 BVerfSchG-E).

Nach dieser weitgehenden gutachterlichen Billigung der Neuregelung sei einschränkend auf Folgendes hingewiesen: Der Gesetzentwurf erlaubt neben dem Betreten zum Zwecke der Vorbereitung nachrichtendienstlicher Maßnahmen an anderer Stelle die heimliche Inbesitznahme von Sachen zur Auswertung, nicht immer mit anschließender Rückgabe (§ 18 Abs. 1 S. 2 und 3 BNDG-E, § 16 Abs. 1 S. 2 Nr. 4 BVerfSchG-E). Zusammen lassen beide Befugnisse theoretisch zu, einen Laptop oder ein Handy sogar vorübergehend aus einer Wohnung herauszutragen; der Betroffene erführe, falls von einer nachträglichen Mitteilung abgesehen wird, niemals etwas vom Verbleib seines Geräts. Das kommt einer heimlichen Beschlagnahme nahe und weckt zudem ungünstige – wenngleich angesichts der fortbestehenden Zweckbindung auf die Informationsgewinnung des BND falsche – Erinnerungen an Einschüchterungsstrategien, wie sie durch die Geheimdienste der Russischen Föderation zur Anwendung gebracht werden.<sup>65</sup> Zumindest aus rechtspolitischer Sicht sollte die heimliche Inbesitznahme in Wohnungen entweder ausgeschlossen oder – vermutlich praxisnäher – nur zur sehr kurzzeitigen Mitnahme gestattet sein, um nicht in der Wohnung als Risikoraum selbst die Spähsoftware aufspielen zu müssen. Hilfsweise wäre als Mindeststandard zu verlangen, dass die Maßnahme der besonderen Nachkontrolle durch den Senat des UKRats unterworfen wird.

<sup>62</sup> Begr. zu § 37 BNDG-E, BT-Drs. 21/7868, S. 444; Begr. zu § 27 Abs. 2 UKRatG-E, S. 578.

<sup>63</sup> BVerfGE 154, 152, Rn. 272 ff., 286 ff.; BT-Drs. 21/7868, S. 93 f., 167 f. Zu diesen Maßstäben beim verdeckten Zugriff auf IT-Systeme Peuker, GSZ 2026, 101 (105).

<sup>64</sup> Sehl, Legal Tribune Online v. 24.8.2026, dort auch zur Zuständigkeit der Amtsgerichte in den Ländern. Für einen klassischen Richtervorbehalt als ressourcenschonendere Alternative dagegen Löffelmann, Hoffnungsanker im Paradigmenwechsel, VerfBlog v. 20.8.2026, <https://verfassungsblog.de/nachrichtendienstreform-kontrolle-unabhaengerigerkontrollrat>.

<sup>65</sup> Vgl. Fröhlich, „Klassischer Fall von Einschüchterung“: Sabotiert Russlands Geheimdienst Ukraine-Helfer in Berlin?, Tagesspiegel v. 23.3.2022, <https://tagesspiegel.de/berlin/sabotiert-russlands-geheimdienst-ukraine-helfer-in-berlin-5422288.html>.

## II. Nachrichtendienstliche Verbindungen (§§ 20, 22, 23)

Auch menschliche Quellen, die im BND seit jeher als nachrichtendienstliche Verbindungen bezeichnet werden, erfahren künftig eine eigenständige fachgesetzliche Regelung. Diese unterscheidet nach dem Inlandsbezug. So dürfen Deutsche und Personen im Bundesgebiet nicht als nachrichtendienstliche Verbindung geführt werden, wenn sie nicht voll geschäftsfähig, insbesondere minderjährig sind (§ 23 Abs. 2 Nr. 1 BNDG-E). Die Behördenleitung kann für Personen ab 16 Jahren eine Ausnahme anordnen, wenn die Aufgabenerfüllung sonst aussichtslos oder wesentlich erschwert wäre und Belange der Fürsorge besonders berücksichtigt werden (Abs. 3 S. 1 Nr. 1). Anders als beim BfV dürfte dies aufgrund des Fokus des BND auf das Ausland aber die Ausnahme bleiben. Relevanter sind daher die für Ausländer im Ausland geltenden Absenkungen, sollen doch die gesetzlichen Ausschlussgründe nicht für sie gelten, weil diese auf die Lebenssituation im Bundesgebiet zugeschnitten seien. Bislang galten die Ausschlussgründe des § 9b BVerfSchG über § 5 BNDG pauschal auch für den BND.<sup>66</sup> Die Differenzierung ist im Ansatz richtig. Ein Auslandsdienst gewinnt Quellen in Konfliktgebieten und Milieus, in denen auch Jugendliche Zugang zu Informationen haben und vielfach sogar selbst unter Waffen stehen, so dass die jugendfürsorgenden Maßstäbe des Bundesgebiets in der Tat nicht ohne Weiteres passen.

Zwei Punkte sind aber zu bedenken: Zum einen bleibt die Ausnahme für Minderjährige ab 16 Jahren im Inland hinter der künftig für das BfV geplanten Schwelle zurück, wonach die Werbung und Führung jugendlicher Quellen an die Unerlässlichkeit zur Aufklärung besonders erheblich beobachtungsbedürftiger Bestrebungen und damit an die höchste Bedrohungsstufe gebunden wird (§ 18 Abs. 1 S. 3 BVerfSchG-E). Jedenfalls aus rechtspolitischer Sicht sollte die Ausnahme im Inland deshalb an die Schwelle des BfV angeglichen werden. Zum anderen fehlt für Minderjährige im Ausland jede gesetzliche Vorgabe zur Fürsorge. Die Konflikte der gesetzlichen Vertretung und der erforderlichen elterlichen Zustimmung, die wir für das BfV benannt haben (vgl. unter C.IV.3), stellen sich hier in verschärfter Form, weil Eltern durch die Zusammenarbeit mit einem ausländischen Dienst in ihrer Heimatregion selbst eine Straftat begehen oder auf andere Weise gefährdet werden können. Für Minderjährige im Ausland sollte daher jedenfalls eine dokumentierte Abwägung unter Berücksichtigung der Fürsorgeaspekte für die minderjährige Quelle und ihr nahes Umfeld im Rahmen der vorhandenen Erkenntnisse erfolgen, die der administrativen Kontrolle des UKRats zugänglich wird. Ein generelles Verbot der Werbung und Führung minderjähriger nachrichtendienstlicher Verbindungen erachten wir in Abwägung mit dem daraus erwachsenden Verlust an Schlagkraft des BND nicht als erforderlich.

Es liegt auf der Hand, dass der BND vor der Werbung einer Person als nachrichtendienstliche Verbindung ihre Zuverlässigkeit und erwartete Quellenehrlichkeit ebenso erforschen muss wie den Umstand, ob sie womöglich für einen fremden Dienst wirkt (außer bei der Überwerbung von Countertermen) und ob dem Einsatz Eigensicherungsgründe entgegenstehen. Dafür darf der Dienst nach § 20 Abs. 4 BNDG-E nachrichtendienstliche Mittel gegen die erforschte Person einsetzen, sie etwa observieren oder Auskünfte über sie einholen (vgl. § 13 Abs. 2 S. 3). Insofern muss die entsprechende Person nicht – wie nach den allgemeinen Bestimmungen gefordert – mit einem Aufklärungsziel in Zusammenhang stehen. Auch entfällt die ansonsten geltende Vorgabe, dass eingriffsintensive Mittel gegenüber Deutschen und Personen im Bundesgebiet nur angeordnet werden dürfen, wenn sie für eine zumindest erhebliche Bedrohung verantwortlich sind, diese unterstützen oder Akteure

---

<sup>66</sup> Begr. zu § 23 Abs. 2 und 3 BNDG-E, BT-Drs. 21/7868, S. 399.

derartiger Bedrohungen in einer Weise nahestehen, die Erkenntnisse über sie versprechen. Auf den ersten Blick könnte man vor diesem Hintergrund meinen, dass die erforschte Person – der selbst nicht zwingend etwas „vorgeworfen“ werden muss – nicht zum Gegenstand heimlicher Überwachungen werden dürfe. Ein solches Verständnis würde allerdings verkennen, dass nachrichtendienstliche Beobachtungen nicht von klassischen „Schuld“- und Verantwortlichkeits-Zurechnungen geprägt sind, sondern eines legitimen Zwecks im Rahmen der nachrichtendienstlichen Aufgabenerfüllung bedürfen. Operativ sind die geplanten Befugnisse vor diesem Hintergrund berechtigt, denn eine ungeprüfte Quelle gefährdet den Dienst und nicht selten sich selbst, so dass die Prüfung auch in ihrem eigenen Interesse liegt. Schrankenlos ist sie zudem nicht, gelten die besonderen Voraussetzungen des jeweiligen nachrichtendienstlichen Mittels doch ebenso weiter wie die allgemeinen Grundsätze der Zweckbindung und der Verhältnismäßigkeit. Ebenfalls nachvollziehbar ist, dass die Erhebungsschwelle nicht an ein Handeln der erforschten Person anknüpft, sondern an die Schwere jener Bedrohung, die die nachrichtendienstliche Verbindung aufklären soll,<sup>67</sup> da ansonsten keine praktische Handhabung der Bestimmungen des Gesetzes möglich ist. Diese Regelung führt allerdings zu durchaus invasiven Eingriffsmöglichkeiten gegenüber Personen, die lediglich geworben werden könnten: Sollen sie nach dem Willen des BND etwa eine Bedrohung von herausgehobener Bedeutung aufklären, dürfte gegen die möglichen künftigen Quellen sogar eine mehr als einwöchige optische und akustische Überwachung (§ 27 Abs. 1 Nr. 2, Abs. 2 Nr. 2) oder das Öffnen und Einsehen ihrer Briefe und Postsendungen (§ 28 Abs. 2) angeordnet werden. Der Gesetzgeber sollte darüber nachdenken, ob er im Sinne eines Negativkatalogs nicht zumindest bestimmte besonders eingriffsintensive Maßnahmen ausschließt, auch weil sie zur Quellenerforschung wenig geeignet sind.

Seit jeher ist der Schutz von Vertraulichkeitsbeziehungen von zentraler Bedeutung bei der Ausgestaltung verfassungsmäßiger und in einer (wehrhaften) Demokratie politisch vertretbarer Befugnisnormen im Bereich der heimlichen Quellenführung. § 22 BNDG-E versucht, sich dieses Komplexes anzunehmen und schützt Vertraulichkeitsbeziehungen zu Geistlichen, Rechtsanwälten, Journalisten und Abgeordneten einschließlich ihrer Mitarbeiter. Absatz 1 verbietet es, Daten mit dem Ziel zu erheben, an das zu gelangen, was diesen Personen in ihrer beruflichen Eigenschaft anvertraut wurde. Absatz 2 hebt das Verbot allerdings wieder auf, wenn der Berufsträger selbst für eine zumindest erhebliche Bedrohung verantwortlich ist oder sie unterstützt (Nr. 1 lit. a), wenn er einem Netzwerk angehört, das eine solche Bedrohung trägt (lit. b), oder wenn er lediglich in einem Zusammenhang mit der Bedrohung steht, der Erkenntnisse verspricht, die sich bei den Verantwortlichen nicht gleichermaßen gewinnen lassen, etwa weil er Mitteilungen für sie entgegennimmt oder weitergibt (lit. c).<sup>68</sup> Die ersten beiden Fallgruppen betreffen Berufsträger, die selbst in die Bedrohung verstrickt sind, und sind unbedenklich. Lit. c reicht dagegen weiter und erfasst gerade typische Konstellationen innerhalb der Tätigkeitsentfaltung der angesprochenen Berufsgruppen – etwa Journalisten, die mit ihren Quellen aus terroristischen Kreisen sprechen, oder Verteidiger, die mit ihrem Mandanten über potentielle schwere Straftaten in vermeintlich „geschütztem Raum“ sprechen. Würde dieser Normentwurf Gesetz, liefe der Schutz dort leer, wo er aus einer grundrechtlichen Perspektive der Betroffenen am dringendsten gebraucht wird. Auch die Subsidiaritätsklausel in lit. c hilft dabei nicht weiter, weil sie nur fragt, ob sich die Erkenntnisse anders gewinnen lassen, und das eigenständige Gewicht des Vertrauensschutzes nicht in die Abwägung einstellt. Wir empfehlen deshalb, lit. c tatbestandlich so einzugrenzen, dass berufstypischer Kontakt allein nicht genügt, und eine ausdrückliche Einzelfallabwägung mit dem Gewicht der Vertrauensbeziehung vorzuschreiben, wobei gezielte

<sup>67</sup> Begr. zu § 20 Abs. 4 BNDG-E, BT-Drs. 21/7868, S. 390.

<sup>68</sup> BT-Drs. 21/7868, S. 88; zur Kontrolle § 97 Abs. 1 Nr. 12 und Abs. 3 Nr. 2 BNDG-E, S. 134.

Erhebungen nach lit. c vorab dem UKRat zur Entscheidung vorzulegen sind. Für die strategische Aufklärung sieht § 97 Abs. 1 Nr. 12 lit. b eine solche Vorabkontrolle bereits vor, und für erst nachträglich als geschützt erkannte Daten genügt die vorgesehene Einzelfallkontrolle nach § 22 Abs. 3 und § 97 Abs. 3 Nr. 2.

Eine zweite Lücke betrifft den Ort der Erhebung. Absatz 3 regelt zwar den Fall, dass sich erst bei der Auswertung zeigt, dass Daten aus einer Vertraulichkeitsbeziehung stammen, erfasst aber nur Daten, die beim Berufsträger selbst erhoben wurden. Wird dieselbe Kommunikation beim Mandanten, bei der Quelle oder bei einem Dienstleister erfasst, greift er nicht, so dass die vertrauliche Gegenseite je nach Erhebungsort schwächer geschützt ist. Wir empfehlen, den Schutz auf ihrem Inhalt nach geschützte Vertraulichkeitskommunikation unabhängig vom Erhebungsort zu erstrecken, unter denselben eng gefassten Ausnahmen und Kontrollregeln. Er sollte deshalb auch Daten erfassen, die erkennbar einer geschützten Berufsbeziehung oder dem Redaktionsgeheimnis zuzuordnen sind und bei Kanzleien, Redaktionen, Medienunternehmen, Kammern, beruflichen Cloudsystemen oder sonstigen Dienstleistern liegen, bei Notarkammern und der Bundesnotarkammer insbesondere Daten, die der notariellen Verschwiegenheit unterliegen. Einer pauschalen Gleichstellung sämtlicher Organisations- und Verwaltungsdaten bedarf es dagegen nicht.

Schließlich fällt der Schutz hinsichtlich des betroffenen Personenkreises noch nicht weit genug aus. Hierzu bedarf es zunächst eines Hinweises auf die unterschiedliche Systematik in BVerfSchG-E und BNDG-E. Indem § 32 BVerfSchG-E dem Vorbild des § 160a StPO folgt und an die Zeugnisverweigerungsrechte des § 53 StPO anknüpft, macht er zumindest Maßnahmen gegen Geistliche, Verteidiger, Rechtsanwälte, Kammerrechtsbeistände und Abgeordnete absolut unzulässig, soweit sie voraussichtlich Informationen erbringen, über die diese das Zeugnis verweigern dürften. Bei den übrigen Berufsgeheimnisträgern, darunter Ärzten, Psychotherapeuten und Journalisten, relativiert er den Schutz. Maßnahmen erfordern hier aber wenigstens eine erheblich beobachtungsbedürftige Bedrohung (was im Hinblick darauf, dass diese Schwelle fast bei allen Beobachtungsobjekten erreicht sein dürfte, ebenfalls sehr weit reicht, vgl. dazu unter C.I.2 und C.IV.9). § 22 BNDG-E kennt diese Abstufung hingegen nicht. Er verbietet die gezielte Erhebung aus einer Vertraulichkeitsbeziehung, beschränkt den geschützten Kreis aber auf Seelsorger, Rechtsanwälte und Verteidiger, Journalisten und Abgeordnete samt ihren Mitarbeitern (Abs. 1 S. 2 und 3) und lässt selbst für alle von ihnen die Ausnahmen des Absatzes 2 zu.<sup>69</sup> Ärzte, Psychotherapeuten und Notare bleiben somit gegenüber dem Auslandsdienst ohne eigenständigen berufsbezogenen Schutz.

Durch den Kernbereichsschutz des § 21 BNDG-E, der auch in Stellungnahmen der betroffenen Fachverbände bisweilen übersehen wurde,<sup>70</sup> erfolgt zwar eine Art Grundsicherung.<sup>71</sup> Er erfasst aber nur höchstpersönliche Inhalte und gewährt keinen besonderen Vertrauensschutz für die Berufsbeziehung als solche. Warum ein Therapeut gegenüber dem Auslandsdienst schutzloser sein soll als gegenüber dem Inlandsdienst, erklärt die Gesetzesbegründung auch nicht. Obgleich eine Erweiterung des Berufsgeheimnisträgerschutzes nach unserer Auffassung nicht verfassungsrechtlich

<sup>69</sup> § 21 Abs. 1 S. 2 BNDG; BT-Drs. 21/7868, S. 88; Begr. S. 396 f.

<sup>70</sup> So etwa die gemeinsame Stellungnahme von DGPPN, DGKJP und DGPM zum Regierungsentwurf v. 9.9.2026, Nr. 2, die zu § 22 BNDG-E den fehlenden Schutz der Behandlungsbeziehung rügt, ohne § 21 BNDG-E anzusprechen, <https://dgkjp.de/stellungnahme-gesetz-zur-reform-des-nachrichtendienstrechts>. Zur Forderung nach absolutem Schutz ferner Bundespsychotherapeutenkammer, Stellungnahme zum Gesetzentwurf v. 31.8.2026; Kassenärztliche Bundesvereinigung, Stellungnahme v. 13.8.2026 zum Referentenentwurf v. 5.7.2026.

<sup>71</sup> Sie gilt für alle Personen und nach der Begründung auch für die strategische Aufklärung (Begr. zu § 21 BNDG-E, BT-Drs. 21/7868, S. 390). Damit ist zugleich die Vorgabe umgesetzt, die gezielte Kernbereichserfassung auch gegenüber Ausländern im Ausland auszuschließen, BVerfGE 170, 79, Rn. 196 ff.

zwingend ist und sich durchaus mit Unterschieden im Aufklärungsprofil zugunsten des Auslandsnachrichtendienstes argumentieren ließe, empfehlen wir rechtspolitisch ein Nachbessern durch den Gesetzgeber. Entweder übernimmt das BNDG-E an dieser Stelle die Regelungslogik des BVerfSchG-E oder Ärzte, Psychotherapeuten und Notare werden in den Kreis des § 22 Abs. 1 BNDG-E aufgenommen, dessen Ausnahmen nach Absatz 2 den relativen Charakter dieses Schutzes wahren. Für psychotherapeutische Sitzungskommunikation sollte zudem – in beiden Gesetzen – klargestellt werden, dass sie absolutem Kernbereichsschutz unterfällt. Hierzu genügt die Gesetzesbegründung (dazu auch unter C.IV.9).

### **III. Strategische Aufklärung (§§ 30–34, 47)**

#### **1. Zusammenführung der Regime**

Bei der strategischen Aufklärung wagt der Regierungsentwurf den großen Wurf. Bislang finden sich die beiden technisch verwandten Formen strategischer Telekommunikationsaufklärung in zwei Verfahren: Die Ausland-Ausland-Fermeldeaufklärung nach den §§ 19 ff. BNDG erfasst Kommunikation, an der auf beiden Seiten Ausländer im Ausland stehen, und wird vom UKRat kontrolliert. Die strategische Beschränkung nach den §§ 5, 8 G 10 richtet sich in Abgrenzung dazu auf Kommunikation mit Inlandsbezug und wird von der G 10-Kommission kontrolliert. Beide Verfahren laufen technisch über dieselben Erfassungsansätze, führen aber unter abweichenden Schwellen zu getrennten Datenbeständen unter getrennter Aufsicht. Für die operative Wirksamkeit ist das ebenso hinderlich wie für die Kontrolle, die additive Eingriffe gegen dieselbe Person nur erkennen kann, wenn sie beide Bestände sieht. Der Entwurf beendet diese Teilung und regelt die strategische Aufklärung einheitlich in den §§ 30–34 BNDG-E. Dass das G 10 in die Fachgesetze integriert wird, ist erfreulich und schafft mehr Normenklarheit, zumal die Aufspaltung ein historisches Relikt war.<sup>72</sup>

Das BNDG-E bildet mit seinem einheitlichen Ansatz den Inlandsbezug nicht mehr über getrennte Normen zur Ausland-Ausland-Aufklärung ab, sondern sorgt über den Begriff des qualifizierten Inlandsbezugs (§ 30 Nr. 6) und über die Sonderregeln des § 34 für eine trennscharfe Abgrenzung. Diese Entscheidung des Gesetzgebers überzeugt stark, zumal sie zugleich den Beschluss des Bundesverfassungsgerichts vom 8. Oktober 2024 umsetzt, der die bisherige Regelung der strategischen Beschränkung im G 10 beanstandet hatte.<sup>73</sup> Künftig erhebt der Dienst einheitlich für seine Aufgabenerfüllung und unterscheidet erst bei der späteren Verwendung, was erhebliche Operativgewinne verspricht. Die Schranken der Verwendung entfallen dadurch nicht, denn die Zweckbindung des § 68 und die Übermittlungsschwellen der §§ 70 ff. bleiben eigenständig bestehen. Die Angemessenheit der Erhebung sollte aber schon auf dieser ersten Stufe begründet werden und nicht erst in einer späteren Schrankenprüfung Beachtung finden (dazu im Folgenden).

#### **2. Erhebung, Volumengrenze (§§ 31, 32)**

§ 31 Abs. 3 BNDG-E beschränkt die Fermeldeaufklärung auf Netzbestandteile, für die tatsächliche Anhaltspunkte einer besonderen Ergiebigkeit bestehen, und auf höchstens 15 Prozent des Datenvolumens, das in allen Telekommunikationsnetzen übertragen werden kann. Das geltende Recht begrenzt die Erfassung auf „nicht mehr als 30 Prozent der bestehenden Telekommunikationsnetze“ (§ 19 Abs. 8 S. 2 BNDG). Die Prozentwerte sind nicht unmittelbar vergleichbar, weil der

<sup>72</sup>Begr. A.II, BT-Drs. 21/7868, S. 203.

<sup>73</sup> Vgl. BVerfGE 170, 79. Zur geltenden strategischen Ausland-Fermeldeaufklärung weiterführend Vogt, DÖV 2023, 689.

Regierungsentwurf auf die Übertragungskapazitäten abstellt und nicht auf die tatsächliche Last in den Netzen. Einer näheren Betrachtung bedarf es allerdings nicht, da die Volumengrenze lediglich der abstrakten verfassungsgerichtlichen Anforderung begegnen soll, die Erfassung nicht global und pauschal anzulegen. In der Praxis werden die neuen Grenzwerte ebenso wenig je auch nur im Ansatz durch die dem BND zur Verfügung stehenden Rechnerkapazitäten abgedeckt werden können wie die bislang möglichen Volumina. Die eigentliche Begrenzung leisten deshalb Thema und geografischer Fokus der Anordnung (§ 31 Abs. 2, § 47), die neu geschaffene Ergiebigkeitsprüfung je Netzbestandteil und die Vorabkontrolle. Dass Bezugsgröße, Messzeitraum, Berechnung des möglichen Gesamtvolumens und Dokumentation der Auslastung so bestimmt werden, dass der UKRat Einhaltung und tatsächliche Schutzwirkung prüfen kann, ist eine Frage der praktischen Verständigung.<sup>74</sup> Da BND und Kontrollrat dem Vernehmen nach eine zwar intensive, aber stets konstruktive Arbeitsbeziehung führen, wird davon ausgegangen, dass dies unproblematisch gelingt.

Inhaltlich begrenzt wird die Fernmeldeaufklärung wie angesprochen maßgeblich über die Anordnung mit der Angabe des Aufklärungsthemas und ihres geografischen Fokus. Aus der Anordnung muss sich ergeben, welchen erheblichen Bedrohungen die nachrichtendienstliche Früherkennung begegnen soll (§ 47 Abs. 2 Nr. 1 und 2 lit. a). Damit tritt die nicht abschließend beschriebene mittlere Bedrohungsstufe des neuen Gesetzes an die Stelle der bisherigen Kataloge (vgl. unter B.I.2). Der immerhin abschließende Katalog für die Inland-Ausland-Fernmeldeaufklärung nach § 5 G 10 sieht zwar eine Vielzahl von Beobachtungskriterien vor – vom bewaffneten Angriff über internationale Terroranschläge und die Verbreitung von Kriegswaffen bis zum organisierten Rauschgifthandel. Weiterhin umfasst er Geldfälschung, Geldwäsche oder Schleusungen sowie Cybergefahren, wobei das Bundesverfassungsgericht im letztgenannten Fall die bereits angesprochenen Nachbesserungen bis zum 31.12.2026 eingefordert hat. Über § 8 G 10 wurden darüber hinaus strategische Beschränkungen bei einer Gefahr für Leib oder Leben einer Person im Ausland abgedeckt (Entführungsfälle mit Zustimmungsfiktion). Das Regime des § 5 G 10 umfasst damit bei zusammenfassender Würdigung zwar eine Vielzahl von Szenarien, denen aber ein Bezug auf häufig illegales, jedenfalls Bedrohungen von höherem Gewicht hervorrufendes Verhalten gemein ist. Die derzeitige Ausland-Ausland-Fernmeldeaufklärung nach § 19 Abs. 4 BNDG ist demgegenüber deutlich breiter angelegt. Sie umfasst neben Landes- und Bündnisverteidigung, Terrorismus, Extremismus, Cyberangriffen, organisierter Kriminalität und Proliferation auch vage Themenfelder wie krisenhafte Entwicklungen im Ausland, Gefährdungen Kritischer Infrastrukturen und hybride Bedrohungen sowie den Schutz von potentiell häufig betroffenen Rechtsgütern wie der außenpolitischen Handlungsfähigkeit. Über den Begriff der politischen Unterrichtung der Bundesregierung aus § 19 Abs. 1 Nr. 1 BNDG, den das Bundeskanzleramt (BKAm) über das eingestufte Auftragsprofil der Bundesregierung steuern konnte, wurde dieser Katalog schließlich schier grenzenlos ausgedehnt. Gemessen an diesen Vorbildern ist der Entwurf im Hinblick auf das bisherige Regime nach § 19 BNDG teils enger, weil die Einsichtnahme in Inhalte stets eine erhebliche Bedrohung voraussetzt (§ 33 Abs. 2, § 34 Abs. 1), und teils weitergehend, weil die offenen Bedrohungsstufen für Kommunikation mit Inlandsbezug an die Stelle des geschlossenen Katalogs des § 5 G 10 treten. Unter Würdigung der strukturellen Eingriffshürden, die durch den neuen Katalog der „erheblichen Bedrohungen“ erfüllt sein müssen, halten wir diese Regelungsweise im Ergebnis für verfassungsrechtlich zulässig, zumal die eigentliche Steuerung über die Anordnungskriterien und ihre Vorabkontrolle erfolgt (vgl. dazu unter B.III.4).

---

<sup>74</sup> BVerfGE 154, 152, Rn. 169.

Rechtlich sensibler ist § 32 Abs. 2 BNDG-E. Er erlaubt, die strategische Aufklärung auch so durchzuführen, dass sich der Auslandsdienst ohne Wissen eines Telekommunikations- oder Digitaldiensteanbieters Zugang zu dessen Systemen verschafft und dort Daten aus laufenden Übertragungen sowie kurzzeitig gespeicherte Daten und Bestandsdaten erhebt. Der BND darf Anbieter also heimlich infiltrieren, wobei zwei Aspekte ins Auge stechen: Zum einen dürfen beim Anbieter zwischengespeicherte Daten künftig erhoben werden, wenn sie nicht älter als 72 Stunden sind, statt bisher 48 Stunden (§ 32 Abs. 2 S. 3 BNDG-E, § 19 Abs. 6 S. 2 BNDG). Das mag man damit begründen, dass Angriffe nicht selten – gerade am Wochenende – erst mit Verzögerung entdeckt werden. Es wäre gut, die Gesetzesbegründung würde eine solche Argumentation noch liefern. Zum anderen erstreckt der Entwurf die Befugnis auch auf inländische Anbieter, nachdem das geltende Recht diese Befugnis nur gegenüber ausländischen Anbietern kennt (§ 19 Abs. 6 BNDG). Gegenüber inländischen juristischen Personen setzt Satz 2 voraus, dass sie einem Auskunftersuchen nicht nachgekommen sind oder tatsächliche Anhaltspunkte dafür bestehen, dass die Offenlegung des Ersuchens dessen Zweck gefährden würde. Erstere Regelung überzeugt im Ansatz, weil ein Verstoß gegen das schon bestehende Mitwirkungsregime des § 170 TKG zwar sanktioniert werden kann, einer auslandsnachrichtendienstlichen Operation aber trotzdem zunächst im Wege stünde. Die Voraussetzungen des Satzes 2 bedürfen allerdings – als sachverständige Empfehlung ausgesprochen – noch der Konkretisierung, ab wann einem Ersuchen „nicht nachgekommen“ wird und ob schon eine unvollständige Erfüllung genügt. Vermutlich geht es hier ohnehin nur um renitente „Vollverweigerer“. Für reine Digitaldiensteanbieter greift die Selbsterhebungsmöglichkeit darüber hinaus bedauerlicherweise nicht, weil diese an ein nicht befolgtes Ersuchen nach § 13 Abs. 5 anknüpft, das nur an Telekommunikationsanbieter (§ 12 Abs. 2 S. 1 Nr. 5) gerichtet werden kann.<sup>75</sup> Richtigerweise sollte diese Maßnahme vorabkontrollpflichtig werden, damit sie nicht wie eine Umgehung des TKG wirkt und das Schutzniveau erhalten bleibt – damit würden die Anbieter im Gegenzug unter die Providermaßnahmen des BNDG-E fallen, was systematisch konsequent wäre.

Auch wenn die Offenlegung im Sinne des zweiten Selbsteingriffsgrundes „den Zweck gefährden würde“, sagt die Norm nicht. Die Begründung versteht diese Variante als Schutz vor der Offenlegung des Ersuchens,<sup>76</sup> im Wortlaut selbst wurde bislang jedoch auf nähere Umschreibungen verzichtet. Verfassungsrechtlich wäre es zudem sicherer, beide Varianten des Selbstzugriffs auf inländische Anbietersysteme in den Katalog der Vorabkontrolle (§ 97 Abs. 1) aufzunehmen; allerdings entstünde damit ein Systembruch gegenüber den bislang noch nicht kontrollpflichtigen Regelungen von Zugriffen auf nicht-private IT-Geräte (§ 37 Abs. 1). Bislang ist er dort nur mittelbar über die Anordnung der strategischen Aufklärungsmaßnahme erfasst, die den Zugriff auf einen konkreten Anbieter nicht benennt.

Wie schon das Bestandsrecht untersagt auch das BNDG-E die Erfassung reiner Inlandskommunikation über die Fernmeldeaufklärung. Sie darf nach § 32 Abs. 3 BNDG-E nicht erhoben werden und ist automatisiert herauszufiltern.<sup>77</sup> Die Ausnahmen, die Satz 5 davon zulässt, sind nachvollziehbar und im Grundsatz auch hinreichend begrenzt. Überwiegend betreffen sie Konstellationen, in denen keine Ausrichtung der Maßnahme gegen den Betroffenen erfolgt, sondern ihre Durchführung gerade dem Schutz der Person dient. Dies betrifft Fälle der mutmaßlichen Einwilligung (Nr. 1) ebenso wie Fälle von Cyberangriffen, da es im Interesse Deutscher sein dürfte, dass ihre Endgeräte nicht unbemerkt von ausländischen Hackern als Plattform für die weitere Ausführung von IT-Angriffen genutzt

<sup>75</sup> BT-Drs. 21/7868, S. 80 ff., 96 f.

<sup>76</sup> Begr. zu § 32 Abs. 2 BNDG-E, BT-Drs. 21/7868, S. 430.

<sup>77</sup> Damit setzt der Entwurf BVerfGE 170, 79, Rn. 164, 190 ff., um.

und dieser „digitale Hausfriedensbruch“ durch die Sicherheitsbehörden aufgeklärt wird (Nr. 2). Einzig Nr. 3 richtet sich gegen den Betroffenen der Überwachungsmaßnahme, ist aber auf die Abwehr erheblicher Gefahren begrenzt und entspricht als eine Art Notkompetenz weitgehend geltendem Recht gemäß § 19 Abs. 7 S. 4 BNDG. Richtigerweise fordert der Tatbestand auch die Begehung durch eine fremde Macht, was den Bezug zum BND eindeutig eröffnet, oder terroristische Bestrebungen. Hier könnte der Gesetzgeber gerne noch nachschärfen und eine Beschränkung auf den „internationalen Terrorismus“ vornehmen.

Auf den ersten Blick irritieren mag darüber hinaus die nach Nummer 4 zulässige Verarbeitung von Daten. Hierbei handelt es sich um *nicht kommunikationsbezogene* Inhaltsdaten, bei denen eine Identifizierung von Absender und Empfänger durch automatisierte Unkenntlichmachung jedenfalls mit vertretbarem Aufwand auszuschließen ist. Das Verfahren der Unkenntlichmachung kennt bereits das geltende Recht für Verkehrsdaten Deutscher und Inländer, bindet deren Weiterverarbeitung aber an zwei benannte Zwecke (§ 26 Abs. 3 S. 2 Nr. 2, S. 3 und 4 BNDG). Die im BNDG-E nun vorgesehene Erfassung kommt hingegen ohne eine solche Zweckbindung aus. Die Begründung nennt als Zweck hierfür die Erkennung internationaler Kommunikationsnetzwerke, zu der auch inländische Kommunikationsdaten beitragen können.<sup>78</sup> In rechtlicher Hinsicht ist vor allem darauf hinzuweisen, dass es fraglich sein dürfte, ob es sich – nach strikter Anonymisierung – überhaupt noch um personenbezogene und nicht nur um Sachdaten handelt, für die wohl keine Rechtsgrundlage erforderlich wäre. Jedenfalls sind die Daten von recht geringem Gewicht, weshalb der Normentwurf ihre geplante Verarbeitung tragen dürfte.

Schließlich erhält der Dienst mit § 31 Abs. 6 BNDG-E eine eigene Abwehrbefugnis, im Rahmen der laufenden Erfassung Daten zu verändern oder zu löschen, Datenverkehre umzuleiten oder zu unterbinden und den Betrieb informationstechnischer Systeme einzuschränken, wenn eine unmittelbar bevorstehende Gefahr für ein besonders gewichtiges Rechtsgut anders nicht abgewehrt werden kann. Das ist, um es klar auszusprechen, eine absolut sinnvolle Eilbefugnis: Wer einen Angriff in der laufenden Erfassung erkennt, soll ihn am Ansatz abwehren dürfen, bevor er sein Ziel erreicht. Die Befugnisnorm ist eine eigene erfassungsbezogene Annexbefugnis und gehört nicht zu den erweiterten Maßnahmen der §§ 49–51 (zu den drei Regimen vgl. unter B.VI.4). Sie kommt ohne Grundanordnung und ohne besondere Vorab- oder obligatorische nachträgliche Einzelfallkontrolle aus, was sich aus der Eile leicht erklärt. Die allgemeine Kontrolle nach § 98 Abs. 1 BNDG-E und die administrative Kontrolle der Datenverarbeitung nach § 32 Abs. 1 Nr. 1 UKRatG-E bleiben erfreulicherweise bestehen. Ungeregelt sind Erforderlichkeit und Verhältnismäßigkeit dabei nicht, wir bitten den Gesetzgeber aber, sie in zwei Punkten technisch zu konkretisieren: Erstens sollte die Veränderung von Daten (Nummer 1) ausdrücklich auf das zur Abwehr des Angriffs Erforderliche begrenzt werden. Eine begrenzte Veränderung kann gegenüber der vollständigen Löschung das mildere Mittel sein, sie kann aber auch weiter reichen, als die Abwehr es verlangt. Zweitens würde eine nachträgliche Vorlage an den UKRat zur Einzelfallkontrolle (§ 97 Abs. 3) die Eile nicht behindern, sondern die allgemeine Kontrolle um eine obligatorische Prüfung des einzelnen Eingriffs ergänzen.

### **3. Einsicht, Inlandsbezug, Eignungsprüfung (§§ 33, 34)**

Auf die Erfassung folgt als zweite Stufe der strategischen Aufklärung die Einsichtnahme. Erst hier entscheidet sich, welche der erfassten Daten durch spezialisierte Prüfmitarbeiter tatsächlich zur Kenntnis genommen werden. Der Entwurf stuft diesen Schritt ab: Metadaten darf das BND-Personal

<sup>78</sup> Begr. zu § 32 Abs. 3 BNDG-E, BT-Drs. 21/7868, S. 432.

einsehen, soweit dies für die Auslandsaufklärung erforderlich ist, Inhaltsdaten hingegen nur bei tatsächlichen Anhaltspunkten für eine zumindest erhebliche Bedrohung (§ 33 Abs. 1 und 2). Weist die Kommunikation einen qualifizierten Inlandsbezug auf, gilt die höhere Schwelle auch für Metadaten. Suchbegriffe, die solchen Personen zugeordnet sind, dürfen nur in den Fällen des § 34 Abs. 2 S. 3 verwendet werden. Ohne besondere Schwelle bleibt dagegen die Einsichtnahme in Daten, an deren Übermittlung auf einer oder beiden Seiten kein Mensch beteiligt ist. Sie fallen unter die allgemeinen §§ 52 ff. Da das Fernmeldegeheimnis auch sie erfasst und ihr Aussagegehalt im Einzelfall an den eines Gesprächs heranreicht (dazu unter C.IV.5), sollte die Schwelle des § 33 Abs. 2 auch hier gelten, sobald sich die Daten bestimmten Personen zuordnen lassen.

Der Einsichtnahme geht die bereits heute praktizierte Eignungsprüfung voraus (§ 30 Nr. 1, § 33 Abs. 4), mit der der Dienst ermittelt, welche Telekommunikationsnetze ergiebig und welche Suchbegriffe geeignet sind. Dafür erlaubt schon das geltende Recht eine befristete Speicherung von zwei beziehungsweise vier Wochen (§ 24 Abs. 5 und 6 BNDG), und bereits nach § 24 Abs. 7 BNDG dürfen die dabei gewonnenen Daten unter besonderen Voraussetzungen zur Gefahrenabwehr und zum Schutz der Bundeswehr weiterverarbeitet werden. Wesentlich größeres Gewicht erhält die Einsichtnahme indes künftig dadurch, dass durch die verlängerten Speicherfristen des Entwurfs eine fortdauernde Auswertung und Anwendung von Selektoren auf den erhobenen Datenpool über einen deutlich längeren Zeitraum ermöglicht wird (dazu genauer unter B.III.5).

#### **4. Anordnung, Kontrolle (§ 47, § 97)**

Mit der Zusammenführung der Regime werden auch Anordnung und Kontrolle vereinheitlicht. Strategische Aufklärungsmaßnahmen sind von der Behördenleitung anzuordnen. Dabei ist neben einer Befristung von höchstens 36 Monaten die Angabe des Aufklärungsthemas und seines geografischen Fokus vorzunehmen. Die Benennung von einzelnen Selektoren entfällt dagegen (§ 47 Abs. 1–3). Die Vorabkontrolle durch Senatsmitglieder des UKRats erfasst in dieser Logik konsequent zunächst auch nur die Anordnung (§ 97 Abs. 1 Nr. 11). Zusätzlich verlangt das Gesetz eine Einbindung der unabhängigen Kontrolleure bei Selektoren zu EU-Stellen oder zu Personen mit Vertraulichkeitsbeziehungen, die ausnahmsweise einer gesonderten Anordnung bedürfen (§ 97 Abs. 1 Nr. 12). Im Übrigen beaufsichtigt das administrative Kontrollorgan die BND-seitige Eigensteuerung von Selektoren.

Fraglich ist, ob die Einspeisung von Suchbegriffen ohne Vorabkontrolle durch den Senat des UKRats auskommen darf, und zwar künftig nicht nur bei Ausland-Ausland-, sondern auch bei Inland-Ausland-Verkehren. Für erstere Erhebungsart hat das Bundesverfassungsgericht nur eine gerichtsähnliche Kontrolle der wesentlichen Verfahrensschritte verlangt, nicht aber jedes einzelnen Suchbegriffs. Ausdrücklich zugewiesen hat es ihr allerdings Suchbegriffe, die gezielt auf mögliche Gefahrverursacher gerichtet sind oder voraussichtlich vertraulichkeitsgeschützte Kommunikation erfassen.<sup>79</sup> Das geltende BNDG setzt dies mit gesonderten Anordnungen um, die der UKRat vorab prüft. Sie betreffen EU-Stellen, Vertraulichkeitsbeziehungen und die gezielte Erhebung gegen Gefahrverursacher, deren Daten für Folgemaßnahmen mit unmittelbarer Außenwirkung übermittelt werden sollen.<sup>80</sup> Der Entwurf übernimmt nur die ersten beiden Fallgruppen (§ 47 Abs. 4, § 97 Abs. 1 Nr. 12). Für die Inland-Ausland-Aufklärung reicht die im geltenden Recht angeordnete Kontrolle noch weiter:

<sup>79</sup> BVerfGE 154, 152, Rn. 278; BT-Drs. 21/7868, S. 98 f., 134.

<sup>80</sup> § 20 Abs. 1 und 2, § 21 Abs. 2, § 23 Abs. 5 und 7 BNDG (geltende Fassung).

Dort sind alle Suchbegriffe in der Anordnung zu benennen, über die die G 10-Kommission vor dem Vollzug entscheidet.<sup>81</sup> Eine solche Benennung entfällt wie dargestellt künftig (§ 47 Abs. 2 S. 2).<sup>82</sup>

Den Verzicht auf die Benennung aller Suchbegriffe halten wir für verfassungsrechtlich tragfähig, auch soweit er Inland-Ausland-Verkehre erfasst. Die derzeitige Benennungspflicht des G 10 geht über das nach dem Grundgesetz Gebotene hinaus. Das Bundesverfassungsgericht hat sie 2024 zwar als bestehende Sicherung der gezielt personenbezogenen Überwachung herangezogen, aber nicht als Mindestanforderung formuliert.<sup>83</sup> Auch bei Inland-Ausland-Verkehren richten sich die Suchbegriffe gegen einen ausländischen Teilnehmer mit nach der Spruchpraxis abgesenktem Schutzniveau, und für Kommunikation mit qualifiziertem Inlandsbezug greifen weiterhin höhere Einsichtsschwellen (§ 34 Abs. 1 und 2). Die Anordnung bindet die Suchbegriffe überdies an ein vorab kontrolliertes Aufklärungsthema und muss angeben, ob und in welchem Umfang personenbezogene Suchbegriffe verwendet werden (§ 33 Abs. 3, § 47 Abs. 2 Nr. 2 lit. c). Hinzu treten die administrative Kontrolle und das Verbot, die gesamte Telekommunikation einer Person strategisch zu überwachen, ohne dass die Voraussetzungen des § 35 vorliegen (§ 33 Abs. 5).

Anders als bisher sieht der Entwurf keine vorab kontrollierte Sonderanordnung für die gezielte Erhebung gegen „Gefahrverursacher“ mehr vor. Das Bundesverfassungsgericht hatte für diese Fallgruppe eine gerichtsähnliche Kontrolle verlangt, weil gegenüber Personen, die als mögliche Verursacher von Gefahren im unmittelbaren Interesse des Dienstes stehen, belastende Folgemaßnahmen wahrscheinlicher seien.<sup>84</sup> Dennoch ist der Wegfall dieser Privilegierung in der Sache gut begründbar: Die strategische Aufklärung steuert ganz überwiegend Telekommunikationsmerkmale, die bestimmten Personen zugeordnet sind, etwa Rufnummern oder E-Mail-Adressen. Inhaltliche Suchbegriffe wie „Bombe“ sind dagegen meist untauglich, weil sie, soweit verschlüsselte Verkehre überhaupt Inhalte erkennen lassen, eine nicht mehr sinnvoll auswertbare Masse an Treffern erzeugen. Die personenbezogene Steuerung ist damit der Regelfall der strategischen Aufklärung. Sie richtet sich, dem Aufklärungsauftrag entsprechend, teils auf mögliche Gefahrverursacher und teils auf andere Personen von Interesse, die in keinem so konkreten Bedrohungsverdacht stehen. Eine Sonderkategorie für Gefahrverursacher in der bisherigen Logik des Bundesverfassungsgerichts stellte deshalb gerade diejenigen unter einen besonderen Schutz, von denen Gefahren ausgeht – nicht aber jene Personen, die der Dienst wegen eines vergleichsweise unverdächtigen Verhaltens ansonsten überwacht. Das kehrt die Logik der Verhältnismäßigkeit um, nach der der Eingriff mit der Nähe zur Gefahr gewichtiger ausfallen darf. Das Risiko belastender Folgemaßnahmen, auf das das Gericht abstellt, sichert bereits die Übermittlungsschwelle der konkretisierten Gefahr (vgl. dazu unter B.VIII).<sup>85</sup> Die Grenze zur Individualüberwachung zieht das Gericht zudem ohnehin nach der Wirkung des Suchbegriffs,<sup>86</sup> und der Entwurf übernimmt sie in § 33 Abs. 5. Nach alledem kann die Karlsruher Spruchpraxis dogmatisch nicht überzeugen und der Gesetzgeber sieht sich zurecht veranlasst, dem Gericht Gelegenheit zu geben, seine Rechtsprechung insoweit fortzuentwickeln und zu präzisieren. Dem Anliegen, die gezielte Überwachung einzelner Personen nicht unkontrolliert zu lassen, wird eine dokumentierte interne Freigabe personenbezogener Suchbegriffe sogar besser gerecht (dazu

---

<sup>81</sup>§ 10 Abs. 4 S. 1, § 15 Abs. 6 G 10 (geltende Fassung).

<sup>82</sup>BVerfGE 154, 152, Rn. 272 ff.

<sup>83</sup>BVerfGE 170, 79, Rn. 118.

<sup>84</sup>BVerfGE 154, 152, Rn. 188.

<sup>85</sup>BVerfGE 154, 152, Leitsatz 6.

<sup>86</sup>BVerfGE 154, 152, Rn. 189.

sogleich). Dass der BND Erkenntnisse künftig auch für erweiterte Maßnahmen nutzen kann (§ 51), ändert daran nichts, weil dort eigene Schwellen und die Grundanordnung greifen (vgl. unter B.VI).

Daneben ist die in der Anordnung vorgesehene Dauer anzusprechen. Dass das neue BNDG-E eine Höchstfrist von 36 Monaten vorsieht, ist gegenüber der bisherigen Ausland-Ausland-Aufklärung grundrechtlich eine unzweifelhafte Verbesserung, weil § 23 BNDG überhaupt keine Höchstfrist kennt und nur die Angabe (irgend)einer Dauer verlangt. Für die bisherige Inland-Ausland-Aufklärung nach § 5 G 10, die künftig in derselben Anordnung aufgeht, geht mit der Novelle dagegen eine erhebliche Ausweitung der Befristung einher, gilt dort doch bislang eine solche auf drei Monate mit der Möglichkeit der Verlängerung um jeweils drei Monate.<sup>87</sup> Wer beide Regime zusammenführt, musste sich zwangsläufig für einen Maßstab entscheiden, und der Entwurf wählt im Sinne der Reformziele der Regierungskoalition nachvollziehbarerweise einen eher großzügigen. Jedenfalls für Anordnungen, die Suchbegriffe mit qualifiziertem Inlandsbezug nach § 34 Abs. 2 zulassen, könnte der Gesetzgeber zur Verbesserung seiner verfassungsrechtlichen Absicherung dennoch etwas nach unten greifen und etwa dreizehn Monate vorsehen.<sup>88</sup> Somit würde er einmal mehr abstufen und damit dem Bundesverfassungsgericht ein Signal senden. Ob das angesichts dessen, dass diese Kategorie den ganz weitgehenden Anteil innerhalb der vorbezeichneten Anordnungen ausmacht, aus gesetzgeberischer Sicht hingenommen werden soll, ist keine rechtswissenschaftlich zu beantwortende Frage.

Über das Grundgesetz hinaus sind bei der Anordnung die Anforderungen des Europäischen Gerichtshofs für Menschenrechte zu beachten. Er verlangt für die strategische Aufklärung sogenannte End-to-End-Sicherungen. Dazu zählen eine unabhängige Genehmigung zu Beginn, wenn Gegenstand und Umfang der Maßnahme festgelegt werden, ebenso wie Angaben zu den Kategorien der Suchbegriffe. Weiterhin fordert der Gerichtshof eine interne Vorabgenehmigung für werthaltige, einzelnen Personen zugeordnete Suchbegriffe und eine unabhängige nachträgliche Kontrolle. Die gezielte Erfassung vertraulichen journalistischen Materials oder ihre hohe Wahrscheinlichkeit bedarf sogar einer unabhängigen Vorabgenehmigung.<sup>89</sup> Diesen doch recht rigiden Straßburger Maßgaben genügen nur wenige SIGINT-Gesetze in Europa, und auch das vorliegende BNDG-E erfüllt die Forderungen des Gerichtshofs nur teilweise.<sup>90</sup> So sieht das BNDG-E zwar die unabhängige Genehmigung zu Beginn einer Maßnahme im Rahmen der Anordnung durch den UKRat vor. Für Suchbegriffe, die Vertraulichkeitsbeziehungen betreffen, tritt zudem die Vorabkontrolle der gesonderten Anordnung nach § 47 Abs. 4 hinzu, was der Straßburger Spruchpraxis nach einer unabhängigen Vorabgenehmigung für journalistisches Material entspricht.

Problematisch ist derzeit noch, dass die §§ 30–34 und 47 BNDG-E keine interne Vorabfreigabe der einzelnen Suchbegriffe vorsehen, die bestimmten Personen zugeordnet sind; bislang ist dies nur untergesetzlich geregelt. Hier sollte entsprechend im Gesetzeswortlaut nachgebessert werden. Die Freigabe sollte verlangen, dass die Stelle, die einen personenbezogenen Suchbegriff einsetzen will, dessen Verwendung anhand von Erforderlichkeit und Verhältnismäßigkeit begründet und dokumentiert und dass eine von der Auswahlentscheidung getrennte Stelle innerhalb des BND die

<sup>87</sup> § 10 Abs. 5 G 10 (geltende Fassung).

<sup>88</sup> Dreizehn statt zwölf Monate erfassen auch jährlich wiederkehrende Ereignisse, die nicht an einem festen Datum, sondern in einem bestimmten Zeitraum des Jahres stattfinden. Zur entsprechenden Überlegung bei den Speicherfristen unter B.III.5.

<sup>89</sup> EGMR (GK), Urte. v. 25.5.2021, Nr. 58170/13 u.a., Big Brother Watch u.a./Vereinigtes Königreich, Rn. 350 ff.; vgl. auch EGMR (GK), Urte. v. 25.5.2021, Nr. 35252/08, Centrum för rättsvisa/Schweden.

<sup>90</sup> EGMR (GK), Urte. v. 25.5.2021, Nr. 58170/13 u.a., Big Brother Watch u.a./Vereinigtes Königreich, Rn. 354 f., 381 ff., 448.

Rechtfertigung vor dem Einsatz prüft.<sup>91</sup> Die materiellen Anforderungen des § 33 Abs. 3 und die allgemeine Pflicht zu Dienstvorschriften nach § 95 Abs. 2 gewährleisten diese Verfahrenssicherung für sich genommen nicht, und die Dokumentationspflicht des § 47 Abs. 7 S. 2 ersetzt weder die selektorenbezogene Rechtfertigung noch ihre vorherige Prüfung.<sup>92</sup> Die Pflicht gehört deshalb in das Gesetz; zuständige Stelle und das Verfahren können hingegen weiterhin durch eine Dienstvorschrift bestimmt werden.

Zudem ist vor dem Hintergrund der bisherigen Spruchpraxis des Gerichtshofs unklar, ob seine Anforderungen nach einer verpflichtenden Angabe über die „Kategorien“ von einzusetzenden Suchbegriffen<sup>93</sup> durch den Regierungsentwurf erfüllt werden. Nach § 47 Abs. 2 Nr. 2 lit. c BNDG-E muss eine Anordnung des BND nach dem Regierungsentwurf zwar angeben, ob und in welchem Umfang Selektoren verwendet werden, die sich auf bestimmbare Personen beziehen. Mit anderen Worten wird also zwischen eingriffsrechtlich betrachtet „starken“ und „schwachen“ Suchbegriffen unterschieden. Ob diese Beschreibung dem entspricht, was der Gerichtshof unter Kategorien versteht, lässt sich nicht abschließend unter Rekurs auf seine bisherige Judikatur ergründen. Für eine bloße Unterscheidung nach dem Personenbezug, also zwischen starken und schwachen Suchbegriffen, spricht, dass das Gericht Selektoren im Kern selbst an anderer Stelle so zweiteilt.<sup>94</sup> Andererseits behandelt der Gerichtshof die Angabe der Kategorien und die Vorabfreigabe personenbezogener Suchbegriffe als zwei getrennte Anforderungen, und die Angabe soll ermöglichen, Erforderlichkeit und Verhältnismäßigkeit schon bei der Anordnung zu prüfen.<sup>95</sup> Inwieweit der bloße Hinweis auf die Selektorenstärke bzw. -schwäche dem entspricht, ist unklar. Hinzu kommt, dass der Gerichtshof in seiner maßgeblichen, zum Vereinigten Königreich ergangenen Entscheidung auf das schwedische Recht verwies, das die „categories of selectors“ in der gerichtlichen Genehmigung neben einer eigenen Regel für personenbezogene Suchbegriffe kennt.<sup>96</sup> Dort finden offenbar abstrakte Beschreibungen nach Art des Suchbegriffs und seines Bezugsobjekts Verwendung, etwa als Telekommunikationskennungen von Einrichtungen fremder Streitkräfte und Dienste, Kennungen bestimmter Organisationen oder inhaltliche Suchbegriffe zum Aufklärungsthema. Es muss letztlich dem Gesetzgeber überlassen bleiben, eine Bewertung des Konventionsrechts hierzu vorzunehmen. Nicht erforderlich ist es jedenfalls auch nach der konventionsrechtlichen Judikatur, jeden einzelnen Suchbegriff dem UKRat vorzulegen.<sup>97</sup> Verfassungsrechtlich steht dem Verzicht auf eine selektorengenaue Vorabkontrolle ebenfalls nichts entgegen. Das Bundesverfassungsgericht verlangt nicht, dass die Suchbegriffe bei Festlegung der Maßnahme abschließend bestimmt sind, sondern dass ihre spätere Auswahl an den Aufklärungsrahmen gebunden bleibt und einer wirksamen Kontrolle zugänglich ist.<sup>98</sup> Für die strategische Ausland-Ausland-Fernmeldeaufklärung ist zudem eine sechsstellige Zahl verwendeter Suchbegriffe festgestellt worden, ganz überwiegend formale Selektoren wie Anschlusskennungen.<sup>99</sup> Eine Prüfung jedes einzelnen durch ein gerichtsähnliches Organ wäre kaum sinnvoll zu leisten. Auch die G 10-Kommission, bei der die Suchbegriffe formal Bestandteil der Anordnung

<sup>91</sup>EGMR (GK), Urt. v. 25.5.2021, Nr. 58170/13 u.a., Big Brother Watch u.a./Vereinigtes Königreich, Rn. 355.

<sup>92</sup>Vgl. § 33 Abs. 3, § 47 Abs. 7 S. 2 und § 95 Abs. 2 BNDG-E, BT-Drs. 21/7868, S. 98, 107, 133.

<sup>93</sup>EGMR (GK), Urt. v. 25.5.2021, Nr. 58170/13 u.a., Big Brother Watch u.a./Vereinigtes Königreich, Rn. 353 f., 381, 383.

<sup>94</sup>EGMR (GK), Urt. v. 25.5.2021, Nr. 58170/13 u.a., Big Brother Watch u.a./Vereinigtes Königreich, Rn. 292 f. („strong selectors“ und „complex queries“).

<sup>95</sup>EGMR (GK), Urt. v. 25.5.2021, Nr. 58170/13 u.a., Big Brother Watch u.a./Vereinigtes Königreich, Rn. 354 f., 381, 383.

<sup>96</sup>EGMR (GK), Urt. v. 25.5.2021, Nr. 58170/13 u.a., Big Brother Watch u.a./Vereinigtes Königreich, Rn. 353; zum schwedischen Recht EGMR (GK), Urt. v. 25.5.2021, Nr. 35252/08, Centrum för rättsvisa/Schweden, Rn. 265 ff.

<sup>97</sup>EGMR (GK), Urt. v. 25.5.2021, Nr. 58170/13 u.a., Big Brother Watch u.a./Vereinigtes Königreich, Rn. 354 („may not be feasible in practice“).

<sup>98</sup>Vgl. BVerfGE 154, 152, Rn. 179 f.

<sup>99</sup>Vgl. BVerfGE 154, 152, Rn. 23 f.

sind, konnte sie als ehrenamtliches und nur monatlich tagendes Gremium (§ 15 Abs. 1 S. 4, Abs. 4 S. 1 G 10) nicht vertieft prüfen, sodass hier bei praktischer Betrachtung nichts verloren geht.

## 5. Speicherfristen (§§ 65, 66)

Der Schwerpunkt der Neuregelung liegt nicht auf der Erhebung, sondern auf der Speicherung. Das geltende Recht erlaubt zwar die befristete Pufferung auch von Inhaltsdaten zur Eignungsprüfung (§ 24 Abs. 5 und 6 BNDG), ermöglicht ansonsten aber keine Speicherung von Inhaltsdaten ohne sofortigen Treffer bei der Selektoranwendung unmittelbar nach der Erhebung. Nur für Verkehrsdaten sieht § 26 Abs. 5 BNDG grundsätzlich sechs Monate Pufferfrist vor und lässt dabei schon heute eine längere Speicherung im Einzelfall zu, soweit sie weiterhin erforderlich ist. Nach dem Regierungsentwurf stehen hier markante Ausweitungen ins Haus: Nicht weiterverarbeitete Inhaltsdaten dürften künftig allgemein für höchstens sechs Monate gespeichert werden (§ 66 Abs. 1) und für nicht weiterverarbeitete Metadaten würde die heute schon eröffnete Puffermöglichkeit auch ohne sofortigen Selektortreffer auf zwölf Monate ausgeweitet (§ 66 Abs. 4 S. 1 Nr. 1), wobei Satz 2 wie im geltenden Recht eine längere Speicherung erlaubt, soweit sie im Einzelfall erforderlich ist. In dieser Zeit blieben die Inhalts- und Metadaten laufend durchsuchbar, was die Möglichkeiten gegenüber der zeitlich und inhaltlich begrenzten Eignungsprüfung wesentlich erweitert. Daten einer Person, die bei der Erfassung noch keinem Suchbegriff unterfiel, blieben so auffindbar, wenn diese erst später in das Blickfeld des Dienstes gerät.

Für die verfassungsrechtliche Bewertung dieser Erweiterungen sind insbesondere Zweckbindung, Einsichtnahmeschwellen, Kontrolle und Ausnahmen von den Regelfristen maßgeblich.<sup>100</sup> Wir halten die Fristen von sechs und grundsätzlich zwölf Monaten für mit dem Grundgesetz noch vereinbar. Neu ist dabei vor allem die längere Regelfrist für Inhaltsdaten, die zudem nicht mehr nur der Eignungsprüfung dient, sondern eine durchsuchbare Bevorratung der Daten erlaubt. Dem stehen in dessen gewichtige praktische Gründe entgegen: Wird dem Dienst ein neuer Suchbegriff bekannt, etwa durch den Hinweis eines Partnerdienstes, kann er auf einen vorhandenen Datenbestand zurückgreifen, statt auf eine neue Erfassung hoffen zu müssen. Diese Kaltstartfähigkeit hat die Bundesregierung schon im Verfahren zum geltenden BND-Gesetz für Verkehrsdaten als unabdingbar beschrieben.<sup>101</sup> Zudem müssen Verkehre, die bei der Eignungsprüfung als relevant erkannt werden, nicht mehr grundsätzlich gelöscht werden, nur weil ihr Suchbegriff zuvor nicht gesteuert war. Hinzu kommt, dass Inhaltsdaten besonders geeignet sind, werthaltige Erkenntnisse für mindestens erhebliche Bedrohungen zu generieren, und durch den Einzug von Ende-zu-Ende-Verschlüsselungen in breit genutzten Applikationen wie WhatsApp droht keine weitgehende Ausforschung des Internets, die den Karlsruher Vorgaben insofern eindeutig zuwiderliefe. Die Verlängerungsmöglichkeit des § 66 Abs. 4 S. 2, die an das geltende Recht anknüpft, bedarf zudem weiterhin einer eigenständigen Rechtfertigung im Einzelfall. Ob das Bundesverfassungsgericht die Ausweitung mitträgt, ist dennoch eine offene Frage, weil sie auf Verhältnismäßigkeitswertungen fußt, die nicht vorab seriös vorherzusehen sind. Das Gericht hat 2020 zwar verlangt, dass die seinerzeit geltenden Speicherfristen eingehalten werden. Diese Forderung steht aber nur im Nachsatz zu seiner eigentlichen Forderung, dass eine umfassende Bevorratung von Daten gesetzlich begrenzt werden müsse.<sup>102</sup> Die konkreten Fristen hat das Gericht also nicht selbst aufgestellt, sondern nur als Grenze des damals geltenden

<sup>100</sup> Zu Zweckbindung und Einsichtnahme §§ 31–34 BNDG-E, zu den Löschfristen § 66 Abs. 1 und 4 BNDG-E, zur Kontrolle § 97 Abs. 1 Nr. 11 und 12 BNDG-E.

<sup>101</sup> BVerfGE 154, 152, Rn. 44 (Vortrag der Bundesregierung).

<sup>102</sup> BVerfGE 154, 152, Rn. 191.

Gesetzes vor dem Hintergrund seiner abstrakten Anforderungen bestätigt. Wir meinen deshalb, dass sich die Karlsruher Richter nicht fortan und dauerhaft auf bestimmte Fristen festlegen wollten, wodurch die hier angesprochene neuerliche Verhältnismäßigkeitsprüfung eröffnet würde. Der Einwand, der Entwurf bevorratete in zu großem Ausmaß, verkennt zudem, dass das Gewicht der Speicherung nicht allein von ihrer Dauer abhängt, sondern von den Einsichtnahmeschwellen, die der Entwurf nach Datenart abstuft (vgl. unter B.III.3). Dass eine solche Prüfung zugunsten des BND ausfallen könnte, wird durch einen innereuropäischen Vergleich getragen, in dem der Entwurf weiterhin zurückhaltend bleibt. So erlaubt Frankreich die Speicherung von Inhaltsdaten bis zu vier und von Metadaten bis zu sechs Jahre.<sup>103</sup> Die Niederlande halten noch nicht ausgewertete Daten undifferenziert bis zu drei Jahre vor, Norwegen Metadaten aus der grenzüberschreitenden Kommunikation bis zu achtzehn Monate<sup>104</sup> und das Vereinigte Königreich kennt sogar überhaupt keine gesetzliche Höchstfrist<sup>105</sup>.

Bleibt man der Logik des Gesetzentwurfs treu, stellt sich indes die Frage, weshalb Metadaten regelmäßig „nur“ 12 Monate gespeichert werden sollten. Hier drängt sich etwas der Verdacht auf, dass der bisherige Wert von sechs Monaten schlicht verdoppelt wurde, um einen Abstand in der Schutzwürdigkeit zu den diesem Zeitraum künftig unterfallenden Inhaltsdaten vorzusehen. Eine solche Justierung von Speicherfristen wäre dem Gesetzgeber zwar nicht verwehrt, weil er im Rahmen der rechtlich kaum greifbaren Verhältnismäßigkeitsabwägungen riesiger Datenmengen gegen zwar besonders gewichtige, in ihrer Früherkennung aber doch mitunter noch abstrakt auftretende Bedrohungen keine mathematischen Formeln anwenden kann. Eine leichte Anpassung der regelmäßigen Höchstspeicherdauer von 12 auf 13 Monate würde in operativer Hinsicht jedoch den gewichtigen Vorteil eröffnen, dass jährlich wiederkehrende Ereignisse, die allerdings nicht genau am gleichen Datum im Jahr, sondern nur in einem bestimmten Zeitraum des Jahres stattfinden, nicht aus der Überwachung fielen. Der Unterschied zwischen 12 und 13 Monaten ist grundrechtlich kaum zu fassen und insofern verfassungsrechtlich unwesentlich. Eine Anpassung schlagen wir daher vor.

Näherer Sicherungen bedarf noch § 66 Abs. 2 BNDG-E: Daten der technischen Aufklärung, deren Inhalte bei der Erhebung aus technischen Gründen nicht lesbar gemacht werden können (Nr. 1), und Daten, bei denen sich nicht erforderliche Teile nur mit unverhältnismäßigem Aufwand von unlesbaren Teilen trennen ließen (Nr. 2), sind ihm zufolge spätestens nach fünfzehn Jahren zu löschen. Im Einzelfall ist eine längere Speicherung zulässig, soweit sie weiterhin erforderlich ist (S. 2). Gemeint sind vor allem die vielen verschlüsselten Verkehre, die der Dienst aufbewahrt, bis er sie möglicherweise über aufgedeckte Kryptografiefehler oder vor allem mittels künftiger Quantenrechner entschlüsseln kann. Nummer 2 erfasst daneben Beifang, der mit solchen Daten untrennbar verbunden ist. Der tatsächliche Umfang ist dabei begrenzt: Anders als die bekannt gewordenen Programme etwa der National Security Agency ist die strategische Aufklärung des BND nicht auf eine umfassende Erfassung angelegt, sondern die begrenzten Speicher- und Auswertungskapazitäten verwehren dem deutschen Auslandsdienst schon auf technischer Ebene eine quasi wahllose Bevorratung.<sup>106</sup> Aufbewahrt werden deshalb vor allem Daten mit erkennbarem Aufklärungswert, etwa

<sup>103</sup>Art. L. 854-1 ff. Code de la sécurité intérieure i.d.F. der Loi n° 2015-1556 v. 30.11.2015 (Inhalte zwölf Monate ab erster Auswertung, höchstens vier Jahre ab Erhebung; Verbindungsdaten sechs Jahre; verschlüsselte Daten bis zu acht Jahre); dazu Conseil constitutionnel, Décision n° 2015-722 DC v. 26.11.2015.

<sup>104</sup>§ 7-7 Lov om Etterretningstjenesten v. 19.6.2020 nr. 77 (Löschung der massenhaft gespeicherten Metadaten spätestens nach 18 Monaten); Inhalte nur nach gezielter Erhebung mit vorheriger gerichtlicher Genehmigung (§§ 7-9, 8-1).

<sup>105</sup>Sec. 150(5) Investigatory Powers Act 2016 (Löschung, sobald keine maßgeblichen Gründe für die Aufbewahrung mehr bestehen).

<sup>106</sup>Zur Begrenzung des Volumens der überwachten Übertragungswege vgl. BVerfGE 154, 152, Rn. 169.

verschlüsselte technische Dokumentationen ausländischer Waffensysteme, die personenbezogene Daten allenfalls beiläufig enthalten. Schon das geltende Recht erlaubt, unlesbare Daten aus der Eignungsprüfung zu Forschungszwecken bis zu zehn Jahre zu speichern (§ 24 Abs. 6 S. 2 und 3 BNDG). Der Entwurf erstreckt diesen Zeitraum indes auf alle Daten der technischen Aufklärung, verzichtet auf die Bindung an Forschungszwecke und verlängert die Frist auf fünfzehn Jahre. Die Frist von sechs Monaten, die der Entwurf für lesbare Inhaltsdaten setzt, wird für eine im Angesicht zunehmender Kryptierung von Verkehren immer größere Datenmenge um das Dreißigfache überschritten. Hieraus ergeben sich auf den ersten Blick verfassungsrechtliche Bedenken. Allerdings ist in die Bewertung einzustellen, dass die Daten gerade nicht durchgesehen, also aus ihnen kommunikationserfassende Schlüsse gezogen werden können, und dass die Sechsmonatsfrist mit der Lesbarmachung regulär beginnt (Abs. 2 S. 4). Insofern ist der Gesetzesbegründung zuzustimmen, dass sich das Eingriffsgewicht nicht wesentlich manifestiert, solange die Daten unlesbar sind.<sup>107</sup> Auch die allgemeine verfassungsrechtliche Wertung, wonach das Eingriffsgewicht mit der Dauer von Datenspeicherungen wächst, trifft hier aufgrund der Unlesbarkeit nicht eindeutig zu.<sup>108</sup> Auf der einen Seite wird man vertreten können, dass der Dienst zunehmend weniger Interesse an den Daten haben könne, weil darin theoretisch enthaltene Hinweise auf Ereignisse und Personen zunehmend unattraktiv würden. Andersherum sinkt – abgesehen von intimen und dadurch ohnehin vom Kernbereichsschutz abgedeckten Handlungen – aber auch das schützenswerte Maß der Ausprägung des Persönlichkeitsrechts von Betroffenen an ihrer veralteten Kommunikation. Man denke sinnbildlich daran, was einem unangenehmer wäre: Wenn der Staat aktuelle private Kommunikation seiner Person abfange oder solche heute zur Kenntnis erhalte, die man vor 20 oder vielleicht sogar 30 Jahren gepflegt habe? Im Lichte dieser recht eindeutigen Erwägungen halten wir die Bestimmung in verfassungsrechtlicher Hinsicht für zulässig und empfehlen allein in rechtspolitischer Hinsicht eine regelmäßige dokumentierte Prüfung. Dabei sollte der Dienst überblickartig und gerne knapp festhalten, warum die Daten noch einen Aufklärungswert haben und ob ihre Entschlüsselung realistisch erscheint. Ist beides nicht der Fall, sind sie frühzeitig zu löschen.

## 6. Mitteilung, Rechtsweg (§§ 100–103)

Der Rechtswegausschluss vor Mitteilung (§ 103 Nr. 2) und die Mitteilungspflichten der §§ 100, 101 BNDG-E übernehmen die Struktur des G 10.<sup>109</sup> denfortgesetzt nochmals zu hinterfragen (Zur Frage, ob der UKRat das Organ ist, das Art. 10 Abs. 2 S. 2 GG als Ersatz für den Rechtsweg verlangt, nehmen wir unter D.V im Ergebnis zustimmend Stellung.) Rechtspolitisch empfehlen wir gleichwohl, auf den ausdrücklichen Rechtswegausschluss zu verzichten. Art. 10 Abs. 2 S. 2 GG erlaubt ihn, verlangt ihn aber nicht. Praktisch bleibt er ohne Bedeutung, weil ohne Kenntnis der Maßnahme ohnehin kaum geklagt wird. Zugleich belastet er die Legitimation der Maßnahmen nach den Maßstäben des Europäischen Gerichtshofs für Menschenrechte, der dem offenstehenden Rechtsweg erhebliches Gewicht beimisst. Entsprechendes gilt für § 22 Abs. 5 BVerfSchG-E.

Neu gefasst sind die Ausnahmen von der Mitteilungspflicht. Nach § 100 Abs. 4 S. 1 BNDG-E unterbleibt die Mitteilung unter anderem, wenn Tatsachen die Annahme rechtfertigen, dass die Bedrohung von einer fremden Macht ausging oder gesteuert wurde (Nr. 1), oder wenn die Maßnahme unter Einsatz einer nachrichtendienstlichen Verbindung erfolgte (Nr. 2). Der Zustimmung des UKRats

<sup>107</sup> Begr. zu § 66 Abs. 2 BNDG-E, BT-Drs. 21/7868, S. 487.

<sup>108</sup> Vgl. BVerfGE 125, 260, Rn. 215 zur Bedeutung der Speicherdauer.

<sup>109</sup> Kritisch zum Ausschluss der originären gerichtlichen Kontrolle und zur Beschränkung der Mitteilung auf Fälle mit Inlandsbezug Löffelmann, VerfBlog v. 20.8.2026 (Fn. oben); zur Frage der Ungleichbehandlung von Ausländern vgl. Sosna, ZD 2026, 657 (657).

bedarf die Nichtmitteilung nur in den Fällen der Nummern 4 und 5 (Satz 2). Die Begründung verweist darauf, dass eine Mitteilung im ersten Fall den Gegner warnen und im zweiten die Gewinnung menschlicher Quellen nahezu ausschließen würde.<sup>110</sup> Gegen den Verzicht auf eine Einzelzustimmung spricht, dass der Dienst damit selbst über das Entfallen einer grundrechtlich gebotenen Verfahrenssicherung entscheidet. Für ihn spricht gleichwohl, dass beide Tatbestände an den Aufklärungsgegenstand und die Art der Maßnahme anknüpfen und keine Prognose im Einzelfall verlangen, der UKRat also kaum einen sinnvollen Prüfstoff vorfände. Zudem entlastet die Regelung von wiederholten, aussichtslosen Prüfungen der Mitteilung. Gerade Akteure, die für fremde Mächte wirken, haben in aller Regel wenig bis kein schutzwürdiges Vertrauen in ihre Kommunikation, da ihnen entsprechende Counter-Überwachungshandlungen bekannt sind. Sie verlieren dadurch selbstredend nicht ihren Persönlichkeitsrechtsschutz, als Abwägungsgrund kann man diese Erwartungen aber legitimerweise einbeziehen. Wir halten die gesetzliche Nichtmitteilung ohne individuelle Zustimmung nach alledem für hinnehmbar. Die *allgemeine* Kontrolle durch den UKRat sollte sich aber ausdrücklich auch auf die Anwendung der Nummern 1 und 2 erstrecken, zumal dies vermutlich ohnehin so intendiert und nur nicht hinreichend deutlich ausbuchstabiert ist.

#### IV. Individualisierte technische Aufklärung (§§ 35–39)

Für die Telekommunikationsüberwachung gegenüber Ausländern im Ausland enthält das geltende Recht keine spezifische Befugnis, die § 35 BNDG-E nun schafft. Metadaten dürfen bei Erforderlichkeit für die Auslandsaufklärung erhoben werden, Inhaltsdaten bei tatsächlichen Anhaltspunkten für eine zumindest erhebliche Bedrohung (Abs. 1). Gegenüber Deutschen und Personen mit Inlandsaufenthalt greift jeweils die nächsthöhere Stufe (Abs. 2). Insoweit tritt § 35 Abs. 2 an die Stelle der Individualüberwachung nach den §§ 1, 3 G 10, die bislang dem BND ebenso offenstand wie den Verfassungsschutzbehörden. Die Mitwirkungspflichten der Anbieter, bislang in § 2 G 10 geregelt, übernimmt § 13 Abs. 4 und 5 (vgl. unter B.I.4). Schon § 3 Abs. 1 S. 1 G 10 verlangte dabei keinen strafprozessualen Tatverdacht, sondern ließ tatsächliche Anhaltspunkte für den Verdacht einer Katalogtat genügen. Er erfasste deshalb seit jeher auch Verhaltensweisen im Vorfeld einer Rechtsgutsverletzung.<sup>111</sup> Der Wechsel von Katalogtaten zu Bedrohungsstufen verlagert die Überwachung deshalb nicht erstmals ins Vorfeld (vgl. unter B.I.2). Die Stufung nach dem Inlandsbezug ist im ersten Leitsatz des Urteils zur Ausland-Ausland-Fernmeldeaufklärung angelegt, wonach sich die Schutzwirkungen der einzelnen Grundrechte im Inland und Ausland unterscheiden können.<sup>112</sup> Der Entwurf hält an der Grundrechtsbindung auch im Ausland fest und stuft lediglich das Schutzniveau innerhalb dieser Bindung ab. § 35 Abs. 3 erlaubt die Überwachung zudem mit Mitteln der strategischen Aufklärung (gewissermaßen als „milderes Mittel“). Die technische Methode ersetzt dabei aber nicht die Voraussetzungen, die für die Überwachung der einzelnen Person gelten (dazu B.III.4), sondern fußt nur auf dem organisatorischen Problem, dass Telekommunikationsanbieter im Ausland weder rechtlich zur Mitwirkung verpflichtet werden können noch eine solche aus Gründen der operativen Sicherheit stets angezeigt wäre. Auch das überzeugt, denn wer laufende Kommunikation an der Quelle abgreift, greift zugleich in Art. 10 GG und in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme ein. Der Zugriff auf bereits gespeicherte Kommunikation ist ohnehin allein am IT-Grundrecht zu messen.<sup>113</sup>

<sup>110</sup> Begr. zu § 100 Abs. 4 BNDG-E, BT-Drs. 21/7868, S. 516.

<sup>111</sup> § 3 Abs. 1 S. 1 Nr. 3 G 10 (geltende Fassung) erfasst die §§ 94–96 und 97a–100a StGB.

<sup>112</sup> BVerfGE 154, 152, Leitsatz 1.

<sup>113</sup> BVerfG, Beschl. v. 24.6.2025, 1 BvR 180/23 (Trojaner II), Leitsätze 1 und 2a.

Die Erhebung von Daten aus informationstechnischen Systemen (§ 37 BNDG-E) ist dreistufig konstruiert. Auf der ersten Stufe setzt der Zugriff auf komplexe Systeme, die einen Einblick in wesentliche Teile der Lebensgestaltung einer Person ermöglichen können, eine erhebliche Bedrohung voraus (Abs. 1). Für Systeme, die die betroffene Person als eigene privat nutzt, gilt auf der zweiten Stufe die Bedrohung von herausgehobener Bedeutung (Abs. 2). Geht es um privat genutzte Systeme Deutscher, verlangt die dritte Stufe zusätzlich eine konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut und die Subsidiarität gegenüber anderen Behörden mit Ausnahme anderer Nachrichtendienste, beim Inlandsaufenthalt außerdem einen grenzüberschreitenden Zusammenhang (Abs. 3). Unterhalb dieser Stufen liegen „einfache“ Systeme, die nur punktuelle Daten zu einem Lebensbereich enthalten. Der Zugriff auf sie berührt nach der Begründung nicht das IT-Grundrecht und richtet sich nach der allgemeinen Befugnis des § 18.<sup>114</sup> Das ist folgerichtig, solange beachtet wird, dass auch einfache Geräte über ihre Vernetzung in den Anwendungsbereich des § 37 Abs. 1 rücken können, den der Wortlaut ausdrücklich auf technisch vernetzte Systeme erstreckt. Für den Zugriff auf privat genutzte Systeme Deutscher entspricht die gewählte Schwellenkonstruktion nicht nur jenem Standard, den das Bundesverfassungsgericht für die Online-Durchsuchung durch Inlandsdienste gesetzt hat und der sich auf den BND ohne Weiteres übertragen lässt. Vielmehr übertrifft der Gesetzgeber diesen Standard sogar, weil der besondere Auslandsbezug hinzutritt, der verfassungsgerichtlich nicht gefordert wird. Für die übrigen Systeme von Deutschen richtet sich ihr Schutz nach den allgemeinen Regeln des neuen BNDG-E, insbesondere nach § 6. Dass die Schwelle für Ausländer im Ausland unter jener für Deutsche liegt, ist ebenfalls vertretbar, weil die Grundrechtsbindung auch im Ausland besteht, ihre konkreten Schutzanforderungen nach dem Urteil von 2020 aber wie mehrfach dargestellt von denen im Inland abweichen können. Auch bei konkreter Betrachtung der vorgesehenen Schwelle erscheint die Auswahl vertretbar, denn die für Deutsche geltende konkretisierte Gefahr beschreibt eine polizeirechtliche Einstiegshürde, die nicht auf den Zugriff auf Geräte von Auslandsausländern passt. Zwar ergibt sich das sehr hohe Eingriffsgewicht von Erhebungen aus informationstechnischen Systemen auch aus dem Inhalt der Daten selbst und den daraus zu erlangenden weitgehenden Persönlichkeitsinformationen. Dem wird das Gesetz – wohl – aber dadurch gerecht, dass es immerhin die Spitzenstufe der auslandsnachrichtendienstlichen Befugnisschwellen mit der Bedrohung von herausgehobener Bedeutung in Bezug nimmt. Zudem besteht im Gegensatz zu Erhebungen eines Inlandsnachrichtendienstes beim BND deutlich weniger das Risiko für den Betroffenen, dass seine Daten an Strafverfolgungs- oder andere Exekutivbehörden weitergeleitet werden und dadurch belastende Folgemaßnahmen getroffen werden könnten. Dass § 97 Abs. 1 Nr. 14 nur Zugriffe nach den Absätzen 2 und 3 der Vorabkontrolle unterwirft, folgt aus der im Regierungsentwurf gewählten Stufung. Offen bleibt damit aber, ob nicht auch ein Zugriff nach Absatz 1 im Einzelfall so schwer wiegt, dass er vorab kontrolliert werden sollte. Zum Kernbereichsschutz nach § 21 BNDG-E gilt das unter C.IV.6 Ausgeführte.

Nachzuschärfen sind darüber hinaus vier kleinere Punkte. Erstens verlangt § 37 Abs. 3 Nr. 1, dass „bestimmte Tatsachen die Annahme rechtfertigen“, eine zumindest konkretisierte Gefahr liege vor. Die konkretisierte Gefahr setzt aber schon selbst eine Tatsachengrundlage voraus. Die Doppelung könnte deshalb so gelesen werden, als verlange das Gesetz hier einen zusätzlichen, strengeren oder jedenfalls doppelten Nachweis. Die Vorschrift sollte sprachlich vereinheitlicht werden (vgl. auch unter C.I.2). Zweitens regelt Absatz 4 den Fall, dass sich erst während des Zugriffs herausstellt, dass das System einer höheren Kategorie angehört. Die Maßnahme darf dann nur fortgeführt werden,

---

<sup>114</sup>Begr. zu § 37 BNDG-E, BT-Drs. 21/7868, S. 440 ff. Zum Rückgriff auf Generalklauseln jenseits der grundrechtssensiblen Standardmaßnahmen Peuker, GSZ 2026, 101 (106 f.).

wenn die Voraussetzungen dieser Kategorie vorliegen. Wer das feststellt und wie der Übergang verläuft, lässt sich dem Wortlaut des Regierungsentwurfs allerdings nicht entnehmen. Das Gesetz sollte daher ausdrücklich bestimmen, dass die Behördenleitung oder eine von ihr betraute Stelle (Abteilungs- oder Direktorsleitung) die höhere Einstufung vornimmt und die Maßnahme vor allem unverzüglich dem UKRat vorlegen lässt, um insbesondere Umgehungsmodelle durch bewusstes „Zu-Niedrig-Bewerten“ der Zielsysteme strukturell auszuschließen. Drittens ist die Löschfrist von 36 Monaten für nicht weiterverarbeitete Daten aus IT-Systemen zumindest als lang zu bezeichnen (§ 66 Abs. 4 S. 1 Nr. 2). Das geltende Recht verlangt die unverzügliche Prüfung und lässt einen Prüfzeitraum von bis zu drei Jahren nur mit Zustimmung des UKRats zu (§ 34 Abs. 7 S. 2 BNDG). Der Entwurf macht diesen Ausnahmezeitraum allerdings zur Regelfrist. Zumindest rechtspolitisch, wohl aber auch verfassungsrechtlich vorzugswürdig wäre eine Regelfrist von rund zwölf Monaten. Viertens erlaubt § 39 Abs. 3 Nr. 2, technische Veränderungen bestehen zu lassen, wenn eine Wiederverwendung absehbar ist. Ein offen gehaltener Zugang bleibt aber ein dauerhaftes Risiko für die Integrität des Systems, weil ihn auch Dritte ausnutzen können. Damit das Merkmal „absehbar“ nicht zur unbegrenzten Vorratshaltung von Zugängen führt, empfehlen wir eine einheitliche Höchstfrist, eine vollständige Dokumentation und eine regelmäßige Überprüfung. Das Gesetz sollte vor allem vorsehen, dass die Veränderungen nach technischen Möglichkeiten zurückzubauen sind, sofern die Erforderlichkeit entfällt.

Neben der vollständigen Online-Durchsuchung gestattet § 38 BNDG-E eine abgegrenzte Erhebung. Sie limitiert den Zugriff auf bestimmte Datenarten sowie technisch abgesicherte Teile der Verarbeitung innerhalb des Zielgeräts. Eine solche, auf die tatsächlich erhebungsnotwendigen Systemteile zugeschnittene Befugnis kann praktisch bedeutsamer sein und ist grundrechtsschonender als die Vollausswertung, weshalb ihre Schaffung im Grundsatz Beifall findet. Zulässig sein soll eine solche abgegrenzte Erhebung nach dem Regierungsentwurf schon bei erheblichen Bedrohungen (Abs. 1). Richtet sie sich gegen Deutsche oder Personen im Bundesgebiet und soll sie umfassend Kommunikationsinhalte oder vergleichbar gewichtige Einblicke in die Lebensführung erfassen, gilt hingegen die Schwelle der Bedrohung von herausgehobener Bedeutung (Abs. 2), und nur in diesem Fall unterliegt die Maßnahme auch der Vorabkontrolle (§ 97 Abs. 1 Nr. 15). Das geltende BNDG verlangt demgegenüber für jeden Eingriff in informationstechnische Systeme entsprechende Anhaltspunkte von herausgehobener Bedeutung (§ 34 Abs. 2 und 3 BNDG). Insbesondere gegenüber Ausländern im Ausland wird die abgegrenzte Erhebung also erleichtert. Zwar lässt sich dies in der Karlsruher Logik der Abstufungen bei Auslandsausländern wiederum im Ansatz hören, wenn man im Wege des Erst-Recht-Schlusses zur vollständigen Online-Durchsuchung auch hier die Auffassung des Gesetzgebers teilt, dass sich aus der Erhebung als solcher noch kein so schwerwiegender Eingriff ergibt, dass er nur durch polizeigleiche Schwellen abzufedern wäre. Es scheint schwer absehbar, wie das Bundesverfassungsgericht hierzu Position beziehen wird. Gegenüber Deutschen bleibt der Abstand zur vollständigen Online-Durchsuchung mit ihrem Erfordernis der konkretisierten Gefahr (§ 37 Abs. 3) ferner beträchtlich, worauf an dieser Stelle zumindest hingewiesen werden soll. Für Maßnahmen gegen Deutsche und Personen im Inland gilt das zum BfV Gesagte, wonach eine Vorabkontrolle zumindest rechtspolitisch empfehlenswert wäre (C.IV.6.c).

Für alle individualisierten Maßnahmen stellen sich zudem zwei Verfahrensfragen. Die erste betrifft die Dauer der Anordnung. Nach § 48 Abs. 3 BNDG-E gelten Anordnungen grundsätzlich bis zu zwölf Monate, für Maßnahmen nach § 37 Abs. 3 bis zu sechs Monate. Gegenüber der bisherigen Telekommunikationsüberwachung, deren Anordnung auf drei Monate befristet war (§ 10 Abs. 5 G 10), geht damit eine deutliche Verlängerung einher, die möglicherweise auf der Komplexität und mitunter

Langwierigkeit bei Zugriffsversuchen auf die herstellerseitig immer besser abgeschirmten Endgeräte beruht. Damit diese lange Frist nicht allzu leicht dazu führt, dass im nachrichtendienstlichen Vollzug während der Anordnungsdauer keine internen Kontrollen mehr erfolgen, empfehlen wir eine dokumentierte Überprüfung, die der administrativen Kontrolle des UKRats unterliegt, sobald sich die tatsächlichen Umstände erheblich ändern. Die zweite Frage betrifft vorbereitende Eingriffe: Nach § 48 Abs. 5 darf der Dienst schon vor der Anordnung in die Integrität eines Systems eingreifen, wenn der Erfolg der Maßnahme sonst gefährdet wäre. Personenbezogene Daten darf er dabei noch nicht erheben. Auch ohne Datenerhebung hat ein solcher Eingriff aber eigenes grundrechtliches Gewicht. Er ist zudem vom Eilverfahren nach § 31 UKRatG-E zu unterscheiden, denn dieses setzt eine bereits getroffene Anordnung voraus, während § 48 Abs. 5 gerade vor der Anordnung greift. Gesetzlich abgesichert werden sollten deshalb ein objektiver Anlass, ein enger zeitlicher Rahmen, die unverzügliche Nachholung der Anordnung und der Rückbau, wenn die Genehmigung ausbleibt (vgl. zu § 33 Abs. 1 S. 2 BVerfSchG-E unter C.V).<sup>115</sup> Eine solche Lösung könnte auch unmittelbar über die Aufnahme eines Verweises auf § 39 Abs. 3 erfolgen.

## **V. Kooperationen mit ausländischen Stellen (§§ 40–45)**

Die Vorschriften zur Zusammenarbeit mit ausländischen Stellen können wir aufgrund des eingangs angesprochenen sehr knappen Ersuchens des Deutschen Bundestages um Stellungnahme nicht umfassend würdigen. Auf zwei Aspekte möchten wir allerdings hinweisen:

Der erste ist § 45 BNDG-E. Er erstreckt Kooperationen ausdrücklich auf die Telekommunikationsüberwachung und die Erhebung aus informationstechnischen Systemen nach den §§ 37 und 38, einschließlich automatisierter Übermittlung. Das ist ein operativer Zugewinn, bedeutet aber zugleich die Weitergabe hochsensibler individualisierter Daten (man erinnere sich daran, wie sensibel bislang sogar darauf geachtet wurde, überall die „G 10“-Markierungen auf entsprechenden Auswerteprodukten konsequent abzdrukken). Eine kontrollfreie Kooperationszone entsteht dadurch gleichwohl nicht. Daten aus einem Zugriff auf IT-Systeme von Deutschen oder Personen im Inland (§ 37 Abs. 3) darf der BND nur automatisiert weitergeben, wenn dessen strenge Voraussetzungen auch im Zeitpunkt der Übermittlung noch vorliegen. Für Daten aus der Telekommunikationsüberwachung gelten dieselben Regeln wie für selektierte Daten aus der strategischen Kooperation (§ 45 Abs. 2 S. 2 und 3 i.V.m. § 43).<sup>116</sup>

Darüber hinaus hat die Übergangsregel für bestehende Absichtserklärungen unsere Aufmerksamkeit gewonnen. Während die Übermittlung unselektierter Metadaten an Kooperationspartner (§ 44 BNDG-E) im Wesentlichen die schon nach § 33 BNDG heute bestehende Rechtslage übernimmt, sorgt § 140 Abs. 5 BNDG-E für eine tatsächliche Ergänzung. Danach gelten Absichtserklärungen, die der Dienst nach den §§ 13 und 31 BNDG mit ausländischen öffentlichen Stellen geschlossen hat, bis zu zehn Jahre fort. Die Begründung verweist auf den erheblichen Aufwand jeder Neuverhandlung, der auch die Partner trifft. Zudem ändere sich der vorgeschriebene Inhalt der Absichtserklärungen nur geringfügig, und die Änderungen beruhen nicht auf verfassungsrechtlichen Vorgaben.<sup>117</sup> Dafür spricht zudem, dass jede Neuverhandlung einem Partner Anlass geben kann, die Zusammenarbeit insgesamt zu überdenken. Dagegen steht allerdings, dass Kooperationen über so viele Jahre auf Grundlage von rechtlichen Gegebenheiten in den Vertragsstaaten erfolgen, die sich

<sup>115</sup> BT-Drs. 21/7868, S. 108, 156.

<sup>116</sup> BT-Drs. 21/7868, S. 105.

<sup>117</sup> Begr. zu § 140 Abs. 5 BNDG-E, BT-Drs. 21/7868, S. 546.

etwa durch verfassungsgerichtliche Judikatur längst geändert haben. Dem lässt sich wahlweise dadurch entgegenreten, dass dem Regierungsentwurf noch eine vorzeitige Anpassungspflicht im Falle solcher, die Vereinbarung wesentlich infrage stellender Rechtsänderungen hinzugefügt wird – oder aber dadurch, dass man das Auseinanderdriften hinnimmt, weil eine über das jeweils geltende Recht hinausgehende Absichtserklärung den Dienst ohnehin nicht zu (dann rechtswidrigem) Verhalten verbindlich veranlassen kann.

## **VI. Erweiterte nachrichtendienstliche Maßnahmen (§§ 49–51)**

Bislang ist der BND ein reiner Auslandsnachrichtendienst, der Erkenntnisse sammelt und weitergibt, aber nicht selbst gegen jene Bedrohungen vorgehen darf, die er aufklärt. Der Entwurf hebt die primär nachrichtendienstliche Aufgabe des BND nicht auf, erweitert seinen Instrumentenkasten aber im Zuge einer grundlegenden Neuausrichtung um geheimdienstliche Eingriffsmittel.

### **1. Regelungskonzept und Erscheinungsformen**

Stellt der Auslandsdienst eine spezifische Gefährdungslage fest, obliegt ihm nach dem Regierungsentwurf künftig ein aktives Einwirken zu deren Abwendung oder Einschränkung (§ 49 Abs. 1 S. 1). Eine solche Lage liegt vor, wenn tatsächliche Anhaltspunkte dafür bestehen, dass besonders gewichtige Rechtsgüter durch eine fremde Macht anhaltend, planvoll und in besonderem Maße gefährdet werden (§ 49 Abs. 2). Sie ist halbjährlich zu überprüfen. Auf ihr gründende Maßnahmen setzen eine auf zwölf Monate befristete Grundanordnung der Behördenleitung voraus, die Ziel, Art und Umfang der Aktionen begrenzt (§ 50) und der Vorabkontrolle durch den Senat des UKRats unterliegt (§ 97 Abs. 2, § 27 Abs. 3 Nr. 2 lit. b UKRatG-E). Konkrete Einzelmaßnahmen ordnet der Dienst im Rahmen der Grundanordnung selbst an (§ 51 Abs. 1). Sie sind grundsätzlich im Ausland durchzuführen, gegen die verantwortliche fremde Macht zu richten, dürfen nicht gezielt gegen Leib und Leben gerichtet sein und müssen verhältnismäßig bleiben (§ 51 Abs. 2–4). Zur Abwehr von Cyberangriffen dürfen erweiterte Maßnahmen automatisiert ausgelöst werden (§ 53 Abs. 7 S. 2). Dritte können zur Hilfe verpflichtet werden (Abs. 5). Im Spannungs- und Verteidigungsfall gilt die Gefährdungslage als gegeben, die Zustimmung des BKAmt ersetzt hier die durch den UKRat zu billigende Grundanordnung, und die Inlandssubsidarität sowie die Grenze für Leib und Leben entfallen (§ 129, dazu unter E.).

Die Befugnis selbst soll nach der Gesetzesbegründung grundsätzlich jede Durchführungsform decken. Was unter dem Begriff der erweiterten Maßnahme möglich wird, lässt sich dennoch in drei wesentliche Erscheinungsformen fassen: Die erste stellen „Hackbacks“ dar, also digitale Einwirkungen auf Systeme und Datenverkehre, von denen hybride Operationen ausgehen, und das sonstige Handeln im Informationsraum. Die zweite sind realweltliche Maßnahmen gegen Personen, Sachen und Infrastrukturen in einem potentiell geheimdienstlichen Sinne. Als dritte Erscheinungsform treten schließlich klassisch-nachrichtendienstliche Tätigkeitsformen hinzu, die dem Auslandsdienst bereits offenstehen, für die aber die entsprechenden Schwellen abgesenkt werden. Dies umfasst beispielsweise auch den Einsatz nachrichtendienstlicher Verbindungen ohne die Grenzen des § 23 und Übermittlungen ohne Einhaltung der Vorgaben des sechsten Abschnitts.<sup>118</sup>

Die erweiterten Maßnahmen sind dabei nicht die einzigen Befugnisse, mit denen der BND über die Aufklärung hinaus einwirken darf. Daneben stehen die Abwehr während laufender Aufklärung (§ 28

---

<sup>118</sup>Begr. zu § 51 BNDG-E, BT-Drs. 21/7868, S. 464.

Abs. 3 S. 2, § 31 Abs. 6, § 39 Abs. 4, ergänzt um § 36 für Schadsoftware) und die Eigensicherung (§§ 104 ff.). Beide kommen ohne Grundanordnung aus, sind dafür aber an eigene Schwellen, an die Subsidiarität und an die Verhältnismäßigkeit gebunden.<sup>119</sup>

## 2. Grundsätzliche Bewertung und Anordnungsarchitektur

Im Grundsatz ist der nun auf politische Mehrheiten stoßende Schritt, den Auslandsdienst aus seiner internationalen Rolle als „Vegetarier“ zu befreien, konsequent und angesichts der gewachsenen hybriden Bedrohungslage auch überfällig, wie wir bereits zu Beginn unserer Stellungnahme festgestellt haben (siehe dazu unter A.I).<sup>120</sup> Anders als beim BfV, das im Inland neben den zu Exekutivmaßnahmen berechtigten Polizeibehörden steht, verfügt die Bundesrepublik im Ausland unterhalb der rechtlich wie politisch sehr hohen Schwelle, ab der die Streitkräfte eingesetzt werden können, über keine Eingriffsoptionen. Dieser Umstand hat Auswirkungen auf die Aktivitäten fremder Mächte gegen die Bundesrepublik: Indem besonders durch die Russische Föderation statt eigener Nachrichtendienstoffiziere zunehmend lose geworbene „Low-Level-Agents“ nach Deutschland entsandt werden, lassen sich durch inländische Maßnahmen wie Verhaftungen und justizielle Verurteilungen keine dauerhaften Abwehrerfolge erzielen. Die Auftraggeber werben aus sicherer Entfernung schlicht die nächsten Helfer an, deren Scheitern auf deutschem Boden sie taktisch wenig kostet. Dieses Vorgehen der steuernden Dienste legt es operativ nahe, gegen sie selbst vorzugehen, etwa indem ihre digitalen oder physischen Infrastrukturen gestört werden. Dazu kann es auch gehören, die Herstellung und Nutzung von Einsatzmitteln zu beeinträchtigen und so die Kosten hybrider Operationen gegen Deutschland in die Höhe zu treiben. Zugleich erhielte der BND bei der lange vernachlässigten Gegenspionage, die sich nicht allein „vom Schreibtisch aus“ erfüllen lässt, wieder eine klarere Rolle neben der Spionageabwehr des BfV.

Auch die gewählte Anordnungsarchitektur ist durchdacht. Dass der UKRat unabhängig über eine Gefährdungslage befinden soll, führt dazu, dass der BND ohne dessen Zustimmung nicht „erweitert“ tätig werden darf. Zugleich werden die einzelnen Operationen dem Dienst überlassen, was den faktischen Unwägbarkeiten eines Handelns im Ausland entspricht, dessen Einzelheiten sich vorab nicht hinreichend absehen und in eine verschriftlichte Form gießen lassen. Eine Voraboffenlegung würde zudem den Kenntniskreis konkreter Operationspläne vergrößern, obwohl den eingesetzten Kräften bei physischen Maßnahmen auf fremdem Boden im Enttarnungsfall eine innerhalb des BND so bislang nicht gekannte Lebensgefahr droht. Kontrollierbar bleibt das Modell angesichts des sehr hohen Eingriffsgewichts aber nur, wenn die Grundanordnung dennoch hinreichend konkret ausgestaltet ist. Dem wird das BNDG-E in § 50 Abs. 3 Nr. 2 gerecht, indem es die Nennung von Art und Umfang der Maßnahmen einfordert, was Zielrichtung, Maßnahmentypen und wesentliche Eingriffsgrenzen beinhaltet. Insbesondere durch die Maßnahmentypen und die wesentlichen Eingriffsgrenzen wird sich der UKRat ein angereichertes Bild davon machen können, was der Auslandsdienst konkret ausführen will. In Ermangelung eines Rechtsbehelfs des BND oder des BKAm gegen ablehnende Senatentscheidungen dürfte auch nicht die Gefahr bestehen, dass vonseiten des BND die vorbezeichneten Kriterien zu abstrakt verstanden werden und dadurch eine unzureichende Information erfolgt.

<sup>119</sup>BT-Drs. 21/7868, S. 93, 96 f., 99 ff.

<sup>120</sup>Näher Arts/Jipp, GSZ 2026, 7; dies., GSZ 2026, 147. A.A. Schantz, Stellungnahme zum Entwurf des Gesetzes zur Reform der Nachrichtendienste – Reform des BND-Gesetzes (für die Gesellschaft für Freiheitsrechte), 14.7.2026, Rn. 13 ff., der von einem „bedenklichen Paradigmenwechsel“ spricht; ebenso Gesellschaft für Freiheitsrechte, Stellungnahme zum Referentenentwurf eines Gesetzes zur Reform des Nachrichtendienstrechts, 14.7.2026, die eine Verwischung der Trennung zwischen Nachrichtendiensten und Polizei rügt, welche bei Handeln des BND im Ausland allerdings von vornherein wie dargestellt fernliegt.

Dass das Gesetz selbst keinen Katalog zulässiger Maßnahmenarten enthält, ist deshalb nicht von vornherein zu beanstanden. Der Verzicht hat aber eine Kehrseite. Ohne Positivkatalog muss jede Maßnahmenart, die besondere verfassungsrechtliche Fragen aufwirft, im Gesetz eigens abgesichert sein, namentlich Freiheitsbeschränkungen, Einwirkungen in der realen Welt und die Zurechnung von Stellvertretern (dazu unter B.VI.4.b). Ein Katalog mit je eigenen Maßgaben machte diese Einzelabsicherungen entbehrlich. Er würde die Befugnis zugleich vorhersehbarer machen, allerdings auch für fremde Mächte, und er könnte den dynamischen Veränderungen der Einwirkungsmittel, insbesondere durch Künstliche Intelligenz und andere disruptive Technologien, nur mit Verzögerung folgen. Welchen Weg der Gesetzgeber wählt, steht ihm frei. Nicht frei steht ihm, beides offen zu lassen. Nachzuschärfen ist dagegen der Anlass. § 49 Abs. 2 verweist auf die Rechtsgüter des § 2 Abs. 2 und damit auch auf die außenpolitische Handlungsfähigkeit der Bundesrepublik (Nr. 3). Für Maßnahmen, die bis zur in Kauf genommenen Schädigung Einzelner reichen können, ist dieses Rechtsgut zu unscharf, weil es im Grunde jedes außenpolitische Interesse umfasst. § 49 Abs. 2 sollte es deshalb entweder ausnehmen oder nur bei Gefährdungen von erheblichem Gewicht genügen lassen.

### 3. Kompetenzordnung des Grundgesetzes

Der Entwurf stützt das BNDG-E auf Art. 73 Abs. 1 Nr. 1 GG und auf eine kompetenzielle Zuordnung kraft Natur der Sache.<sup>121</sup> Das Bundesverfassungsgericht hat dem BND unter dem Titel der auswärtigen Angelegenheiten die Früherkennung von Gefahren mit internationaler Dimension als eigene Aufgabe zugewiesen. Zugleich hat es betont, dass der Bund ihn nicht allgemein mit der Gewährleistung der *inneren* Sicherheit betrauen darf und die Gefahrenabwehr grundsätzlich Sache der Länder bleibt.<sup>122</sup> Daraus abzuleiten, dass aktive Maßnahmen als Gefahrenabwehr von der Kompetenz für auswärtige Angelegenheiten nicht gedeckt seien,<sup>123</sup> ist allerdings sehr fraglich. Zum einen gehen die Wertungen des Gerichts schlicht auf das damalige Aufgabenprofil des Dienstes zurück, das sie bestätigt haben, und sollten sicherlich keine absolute Verengung auf die Aufgabe der Früherkennung darstellen. Zum anderen sind Maßnahmen gegen eine fremde Macht, die Deutschland aus dem Ausland anhaltend und planvoll bedroht, der Sache nach auswärtige Angelegenheiten und berühren zugleich die Verteidigung, die Art. 73 Abs. 1 Nr. 1 GG ebenfalls dem Bund zuweist.<sup>124</sup> Den internationalen Bezug, den das Gericht verlangt, sichert der Tatbestand durch die Zielrichtung auf die fremde Macht (§ 51 Abs. 3).

Anders liegt es nach hiesiger Sicht nur dann, wenn der BND aktionell im Inland tätig zu werden gedenkt. Dort trifft er auf die Gefahrenabwehrbehörden der Länder (und des Bundes). Ob allein der Auslandsbezug einer Bedrohung die Kompetenz zu aktivem Einschreiten eröffnet, muss vor diesem Hintergrund kritisch hinterfragt werden. Zwar federt der Gesetzentwurf die Aufgabenzuweisung im Inland dadurch ab, dass sie subsidiär (§ 49 Abs. 1 S. 2) ausgestaltet wird und die Anordnung zusätzlich den Ort der Einzelmaßnahme (§ 51 Abs. 2) zu bezeichnen hat. Das ist sinnvoll, ersetzt aber keine Kompetenzbegründung (zur parallelen Frage beim BfV vertieft unter C.VIII).<sup>125</sup> In diesem Zusammenhang fällt auf, dass der Entwurf § 2 Abs. 3 BNDG nicht übernimmt, der dem BND polizeiliche

<sup>121</sup>Begr. A.V, BT-Drs. 21/7868, S. 204.

<sup>122</sup>BVerfGE 154, 152, Leitsatz 4 und Rn. 126–128.

<sup>123</sup>Schantz, Stellungnahme v. 14.7.2026 (Fn. oben), Rn. 17, der Art. 73 Abs. 1 Nr. 1 GG allein in seiner ersten Alternative heranzieht. Ebenso Rieger, GSZ 2026, 86 (87, 89).

<sup>124</sup>Für einen Rückgriff auf diesen Titel auch Arts/Jipp, GSZ 2026, 7; a.A. Rieger, GSZ 2026, 86 (87 ff.), der darin eine Umgehung der wehrverfassungsrechtlichen Organisationstrennung sieht.

<sup>125</sup>BT-Drs. 21/7868, S. 109 f.

Befugnisse versagt und ihm untersagt, die Polizei um Maßnahmen zu ersuchen, zu denen er selbst nicht befugt ist.<sup>126</sup> Da es sich hierbei allerdings aufgrund der Übermittlungsschwellendogmatik des Bundesverfassungsgerichts sowie der sich aus dem Polizeirecht ergebenden eigenen Anforderungen für dortiges Tätigwerden (Doppeltürprinzip) wohl nur noch um deklaratorische Bestimmungen handelte, ist ihr Wegfall mit keinen materiellen Nachteilen verbunden. Der Schritt entspricht im Übrigen den in der „vorgezogenen“ Novelle des MADG erfolgten Anpassungen.

#### **4. Konkrete Maßnahmearten**

##### **a) Digitale Maßnahmen**

Digitale Maßnahmen dürften künftig vermutlich am häufigsten als erweiterte Maßnahmen des BND beantragt und angeordnet werden. Derartige Handlungen können vom Löschen oder Verändern von Daten über das Umleiten und Unterbinden von Datenverkehren bis zur Einwirkung auf Systeme, von denen hybride Operationen ausgehen, reichen. Kompetenzrechtlich bereiten sie am wenigsten Schwierigkeiten, wenn man der Logik des Regierungsentwurfs folgt, wonach die Zielrichtung der fremden Macht und nicht der Belegenheitsort des Systems maßgeblich sein soll. Eine Maßnahme gegen einen gegnerischen Server wäre danach auch dann keine Inlandsmaßnahme, wenn der Server im Bundesgebiet steht.<sup>127</sup> Das überzeugt, solange das System der fremden Macht zuzurechnen ist, weil es in der Praxis häufig vom Zufall abhängt und in der „Cloud-Gesellschaft“ bisweilen als Endnutzer gar nicht mehr möglich ist, die Routingwege und Speicherorte seiner eigenen Daten nachzuhalten. Grundrechtlich berühren digitale Maßnahmen Rechte Dritter vor allem dann, wenn fremde Dienste die Systeme Unbeteiligter als Zwischenstationen nutzen oder wenn eine Infrastruktur zugleich zivil genutzt wird (dazu unten 5.). Da die entsprechend betroffenen Deutschen oder Inländer ihre Infrastruktur allerdings kaum bewusst für eine fremde Macht zur Verfügung stellen, sondern diese entsprechende Endgeräte „gekapert“ haben dürfte, würde eine strenge Anknüpfung an den Serverstandort sogar dazu führen können, dass vermehrt innerdeutsche Router- oder Smarthome-Geräte für Botnetze verwendet werden.<sup>128</sup>

Im Hinblick auf das Kriterium der operativen Anschlussbefugnisse dürften „Hackbacks“ nach hiesiger Auffassung zudem eher selten dazu führen, dass eine eventuelle vorgelagerte nachrichtendienstliche Überwachungsmaßnahme derart „infiziert“ wird, dass sich ihre Schwellen erhöhen. Nach der Rechtsprechung des Bundesverfassungsgerichts handelt es sich bei operativen Befugnissen um solche staatlichen Eingriffe, die gegenüber Einzelnen erforderlichenfalls mit Zwang durchzusetzen sind.<sup>129</sup> Digitale Gegenmaßnahmen setzen jedoch keinen Zwang durch, handeln egalitär im selben Raum wie der Angreifer und erlassen – im Netz ohnehin abwegig – keine Duldungsverfügung, weshalb der vorherige Angreifer den Gegenschlag rechtlich nicht hinnehmen muss.<sup>130</sup> Wir bezweifeln deshalb, dass digitale Gegenabwehr im Regelfall überhaupt operative Anschlussbefugnisse

<sup>126</sup>Darauf weist Schantz, Stellungnahme v. 14.7.2026 (Fn. oben), Rn. 23, hin.

<sup>127</sup>Begr. zu Abschnitt 4 BNDG-E, BT-Drs. 21/7868, S. 462.

<sup>128</sup>Auf das Beispiel eines als Zwischenstation missbrauchten Krankenhaussystems verweist Schantz, Stellungnahme v. 14.7.2026 (Fn. oben), Rn. 40.

<sup>129</sup>BVerfGE 162, 1, Rn. 154, 159, 171, 302; BVerfGE 169, 130, Rn. 231. Zur Funktion der operativen Befugnisse als „Datenscheide“ Friehe/Wallrath, NVwZ 2025, 201 (202); zur Übermittlung an Waffenbehörden zu Prüfzwecken trotz ihrer Durchsuchungs- und Sicherstellungsbefugnisse zudem BVerfGE 169, 130, Rn. 112 f.; kritisch zur diesbezüglichen Abgrenzung Manns, ZRP 2026, 63 (64 f.).

Wie hier Manns, ZRP 2026, 63 (65). <sup>130</sup>A.A. für die Schutzmaßnahmen des BfV Timu, Vom Aufklären zum Abwehren, VerBlog v. 27.8.2026, <https://verfassungsblog.de/nachrichtendienste-reform-operativ-bka>, der operatives Handeln nicht auf Zwang gegenüber Personen beschränkt, sondern jede eigene Verwendung der Erkenntnisse zur Einwirkung auf den Geschehensablauf erfasst.

begründet, sofern sie nicht ausnahmsweise zu unmittelbaren physischen Schädigungen führt (näher C.VIII.2, auch zu BVerfGE 169, 130, Rn. 231).<sup>131</sup>

Zwei Punkte bleiben: Erstens erlaubt es § 53 Abs. 7 S. 2, Maßnahmen zur Abwehr von Cyberangriffen automatisiert auszulösen, sofern diese auf das Verändern oder Löschen von Daten und das Umleiten oder Unterbinden von Datenverkehren beschränkt bleiben. Dagegen wird eingewandt, die Entscheidung über das Vorliegen eines Angriffs und über seine Zurechnung dürfe nicht einem autonomen System überlassen werden.<sup>132</sup> Der Einwand hat Gewicht, soweit es um die Zurechnung zu einer fremden Macht geht. Die automatisierte Auslösung bleibt aber an eine Grundanordnung gebunden, die Lage und Zielrichtung vorab festlegt (§ 50 Abs. 1), und sie ist auf Datenveränderungen und Umleitungen beschränkt. Dadurch dürften die Bedenken auf verfassungsrechtlicher Ebene weitgehend ausgeräumt sein. Wir empfehlen nichtsdestoweniger, in § 53 Abs. 7 die Protokollierung jeder automatisierten Auslösung vorzuschreiben, um sie menschlichen Nachkontrollen etwa durch das administrative Kontrollorgan zugänglich zu machen. Zweitens fehlt eine Pflicht, in diesen Fällen das Bundesamt für Sicherheit in der Informationstechnik einzubinden, obwohl Rückwirkungen auf die IT-Sicherheit im Inland naheliegen (dazu unten 7.).

Völkerrechtlich stellt die Begründung fest, der Entwurf sei mit den Verpflichtungen der Bundesrepublik und mit Völkergewohnheitsrecht vereinbar.<sup>133</sup> Sie macht es sich mit dieser pauschalen Feststellung allerdings zu leicht, weil sie die maßgeblichen Vorgaben nicht benennt und abwägt. Für digitale Maßnahmen gilt zunächst, dass sie von Deutschland aus geführt nicht mit dem Betreten von fremdem Hoheitsgebiet einhergehen. Die territoriale Integrität des Zielstaats verletzen sie deshalb nach unserer Auffassung in aller Regel nicht.<sup>134</sup> Geltende Maßstäbe sind darüber hinaus das Interventionsverbot und das Gewaltverbot. Das Interventionsverbot untersagt Einwirkungen mit Zwangsscharakter auf Angelegenheiten, über die der andere Staat frei entscheiden darf.<sup>135</sup> Die Störung einer Infrastruktur, die ein fremder Dienst für Operationen gegen Deutschland einsetzt, betrifft keine solche Angelegenheit. Anders liegt es bei Maßnahmen im Informationsraum, die auf die politische Willensbildung im Zielstaat einwirken, etwa durch verdeckte Desinformation. Sie liegen nahe an einer verbotenen Intervention und sollten in der Grundanordnung ausdrücklich bezeichnet werden müssen.<sup>136</sup> Das sich seinem Namen gemäß selbsterklärende Gewaltverbot (Art. 2 Nr. 4 UN-Charta) ist nach den Wirkungen einer Maßnahme zu beurteilen, nicht nach ihrer Form. Eine Cyberoperation, die unmittelbar physische Schäden verursacht, kann es ebenso berühren wie eine physische Sabotage. Ohne physische Wirkung erreichen digitale Schläge diese Schwelle wohl nie, und das Löschen von Daten, das Umleiten von Datenverkehren oder das Lahmlegen einer Angriffsinfrastruktur als für den BND vorgesehene Cybermaßnahmen bleiben jedenfalls deutlich darunter.<sup>137</sup> Nach alledem halten wir

<sup>131</sup>A.A. Schantz, Stellungnahme v. 14.7.2026 (Fn. oben), Rn. 24, der die Hackback-Befugnisse vor dem Hintergrund des Trennungsprinzips für „hochproblematisch“ hält.

<sup>132</sup>Schantz, Stellungnahme v. 14.7.2026 (Fn. oben), Rn. 42 („unverantwortlich“); kritisch auch Gesellschaft für Freiheitsrechte, Stellungnahme v. 14.7.2026 (Fn. oben) (fehlende technische Kontrollkompetenz des UKRats).

<sup>133</sup>Begr. A.VI, BT-Drs. 21/7868, S. 204.

<sup>134</sup>Schmitt (Hrsg.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017, Rules 1–4; Aust, AVR 52 (2014), 375 (381 ff.). A.A. Wissenschaftliche Dienste des Deutschen Bundestages, Sachstand „Aktive Cyberabwehr – Völkerrechtliche Rahmenbedingungen“, EU 6 - 3000 - 079/26 v. 19.6.2026, S. 8; ebenso dies., Verfassungsrechtlicher Rahmen staatlicher Cyberabwehr: Verbot friedensstörender Handlungen und Kompetenzverteilung, WD 3 - 3000 - 056/26 v. 6.7.2026, S. 4 f.

<sup>135</sup>IGH, Military and Paramilitary Activities in and against Nicaragua, Urt. v. 27.6.1986, ICJ Reports 1986, S. 14, Rn. 205.

<sup>136</sup>UN-Generalversammlung, Res. 2625 (XXV) v. 24.10.1970 (Friendly Relations Declaration); Chesterman, Michigan Journal of International Law 27 (2006), 1071 (1081 ff.).

<sup>137</sup>Tallinn Manual 2.0 (Fn. oben), Rule 69; Bundesregierung, On the Application of International Law in Cyberspace, Positionspapier, März 2021; Roscini, Cyber Operations and the Use of Force in International Law, 2014, S. 44 ff.

erweiterte Maßnahmen des Auslandsdienstes im Informationsraum für grundsätzlich vom Völkerrecht gedeckt. Soweit eine digitale Maßnahme gleichwohl Völkerrecht verletzt, kann sie als Gegenmaßnahme gerechtfertigt sein. Das setzt eine vorangegangene Völkerrechtsverletzung des Zielstaats voraus, verlangt Verhältnismäßigkeit und grundsätzlich eine vorherige Aufforderung und Notifikation, von der bei dringlichen Gegenmaßnahmen abgesehen werden kann.<sup>138</sup> Gerade digitale Maßnahmen gegen hybride Operationen fügen sich in dieses Schema, weil die hybride Operation ihrerseits regelmäßig das Interventionsverbot oder die Souveränität Deutschlands verletzt.

## **b) Realweltliche Maßnahmen**

Am meisten diskutiert wurden hingegen die realweltlichen Maßnahmen. Hierunter fallen etwa physische Einwirkungen auf Personen, Sachen und Infrastrukturen. Sie sind vorrangig im Ausland durchzuführen, können nach dem Entwurf aber doppelt subsidiär auch im Inland zulässig sein. Einen Positivkatalog sieht § 51 BNDG-E nicht vor, sodass lediglich gezielte Einwirkungen auf Leib und Leben<sup>139</sup> untersagt sind (Abs. 3 S. 2). In Betracht kommen damit die Sabotage von Infrastrukturen und Einsatzmitteln, die eine fremde Macht für ihre Operationen gegen Deutschland nutzt, aber auch Beschränkungen der Freiheit einer Person, von der kurzzeitigen Ingewahrsamnahme, um sie von der Fortsetzung der Bedrohungshandlungen abzuhalten, bis zur dauerhaft angelegten Extraktion aus dem Zielstaat. Richten müssen sich die Maßnahmen gegen jene fremde Macht, die für die Lage verantwortlich ist (Abs. 3 S. 1). Hybride Bedrohungen werden aber typischerweise über Stellvertreter ausgeführt, etwa kriminelle Gruppen, Scheinfirmen oder terroristische Proxys. Die Begründung bezieht sie funktional ein,<sup>140</sup> der Normtext sagt aber nicht, ob und wann diese Akteure der fremden Macht zuzurechnen sind. Nach der Rechtsprechung des Bundesverfassungsgerichts muss der Gesetzgeber besonders bei heimlichen und eingriffsintensiven Befugnissen die wesentlichen Grenzen selbst im Wortlaut ziehen. Wir ermutigen ihn deshalb, abstrakte Zurechnungskriterien unmittelbar in § 51 Abs. 3 BNDG-E aufzunehmen und dabei ruhig einen großzügigen Zurechnungsansatz zu wählen, der dem vielseitigen Verhalten geheimdienstlicher Helfer praktisch gerecht wird.

Nach dem Regierungsentwurf sollen auch realweltliche Maßnahmen im Inland doppelt subsidiär statthaft sein, und zwar wie angesprochen nur dann, wenn nicht-nachrichtendienstliche, insbesondere polizeiliche Stellen nicht informiert werden können und wenn ein Einschreiten nicht bereits im Ausland möglich war. Nach der Gesetzesbegründung soll die Subsidiarität gegenüber eigentlich zuständigen Stellen nicht nur gewahrt sein, wenn eine Benachrichtigung namentlich der Polizei kein rechtzeitiges Einschreiten mehr erwarten lässt, sondern auch dann, wenn Informationen aus Gründen des Geheimschutzes (besonders der Third Party Rule) nicht weitergegeben werden dürfen. Dagegen wird eingewandt, dass dem BND hierdurch faktisch weite Zugriffsrechte auf die Subsidiaritätsentscheidung zur Hand stünden, weil er die Third Party Rule interpretieren kann und andere Dienste naturgemäß an einer Informationsausleitung aus der globalen Intelligence Community wenig Interesse haben.<sup>141</sup> Dieser Einwand mag zutreffen, wenngleich ihm entgegenzuhalten ist, dass die Third Party Rule nun einmal existiert und durch das Bundesverfassungsgericht sogar als Begründung für Informationsverweigerungen gegenüber dem Deutschen Bundestag anerkannt

<sup>138</sup>Art. 22, 49–53 der Artikel der ILC zur Staatenverantwortlichkeit (ARSIWA), A/RES/56/83 v. 12.12.2001; zur Dringlichkeit Art. 52 Abs. 2, zum Ausschluss von Gewalt Art. 50 Abs. 1 lit. a ARSIWA; daneben kommt der Notstand in Betracht (Art. 25 ARSIWA).

<sup>139</sup>Für den Spannungs- und Verteidigungsfall nennt die Begründung ausdrücklich auch kinetische Mittel; Begr. zu § 129 BNDG-E, BT-Drs. 21/7868, S. 541.

<sup>140</sup>Begr. zu § 51 Abs. 3 BNDG-E, BT-Drs. 21/7868, S. 465.

<sup>141</sup>Vgl. im Ansatz Schantz, Stellungnahme v. 14.7.2026 (Fn. oben), Rn. 22.

wurde.<sup>142</sup> Eine weitergehende inhaltliche Auseinandersetzung kann jedoch insoweit ausbleiben, als der Einwand nur die Gesetzesbegründung, nicht aber den Normtext betrifft. Gerade in jüngerer Zeit haben die Verfassungs- und Verwaltungsgerichtsbarkeit Begründungssätze mit regelndem Charakter nur als Orientierung, nicht aber als normtextgleiche Regelung verstanden.<sup>143</sup>

Verfassungsrechtlich stellt sich bei realweltlichen Maßnahmen zuerst die Grundsatzfrage, ob ein Nachrichtendienst im Inland überhaupt eingreifend tätig werden darf. Ein Trennungsgebot, das dies ausschliesse, findet sich im einfachen Recht (etwa in § 2 Abs. 3 BNDG), in dieser Strenge aber richtigerweise nicht im Grundgesetz.<sup>144</sup> Verfassungsrechtlich maßgeblich ist vielmehr (nur) das informationelle Trennungsprinzip, das das Bundesverfassungsgericht aus den Grundrechten ableitet. Einen Ausfluss dieser Judikatur stellt das Kriterium der operativen Anschlussbefugnisse dar. Das Gericht billigt den Diensten niedrigere Erhebungsschwellen als der Polizei gerade deshalb zu, weil es ihnen an operativen Anschlussbefugnissen fehlt.<sup>145</sup> Erhielte der BND solche Befugnisse, müssten nach dieser Logik schon die Erhebungsschwellen auf polizeiliches Niveau steigen, und gerade die strategische Aufklärung würde dadurch möglicherweise entwertet.<sup>146</sup> Die Gesetzesbegründung verneint eine Zuordnung der realweltlichen Maßnahmen aus § 51 BNDG-E zum Rechtsbegriff der operativen Anschlussbefugnisse indes mit zwei Argumenten: Die erweiterten Befugnisse hätten Ausnahmecharakter, weshalb sie nicht wie bei der Polizei regelmäßig auf eine Datenerhebung folgen könnten, und es handle sich nicht um klassische Operativmaßnahmen, weil der BND im Ausland weder mit verwaltungsrechtlichen Mitteln noch mit polizeilichem Zwang handle.<sup>147</sup> Dies überzeugt zwar nicht – denn nach dem Grund des Trennungsprinzips kommt es nicht auf die Rechtsform des exekutiven Handelns an, sondern darauf, dass umfassendes Wissen mit Eingriffsmacht gegenüber dem Einzelnen zusammentrifft. Zudem setzen die erweiterten Maßnahmen nach § 49 Abs. 1 ausdrücklich auf der Aufklärung auf und beruhen damit wohl doch typischerweise auf nachrichtendienstlich erhobenen Daten. Die Argumente der Gesetzesbegründung tragen gleichwohl, soweit sich Maßnahmen nur gegen die fremde Macht selbst und ihre Einrichtungen richten, weil es dann an Maßnahmen gegenüber Einzelnen fehlt (etwa Zerstörung von Infrastrukturen). Operativen Charakter haben dagegen Maßnahmen, die gezielt in Rechtsgüter bestimmter Personen eingreifen, etwa in das Eigentum oder die Freiheit von Individualpersonen. Bezogen auf derartige realweltliche Folgen würde die Rechtsprechung zu den operativen Anschlussmaßnahmen greifen – wenn man sie denn auch gegenüber dem Auslandsdienst für einschlägig erachtet. Dagegen könnte sprechen, dass das informationelle Trennungsprinzip, aus dem sich die Rechtsfigur der operativen Anschlussbefugnisse begründet, mit Blick auf den Verfassungsschutz entwickelt worden ist, in dessen inländischem Wirkungsraum die Polizei zur Gefahrenabwehr bestimmt ist, während der BND im Ausland allein steht. Zudem hat das Bundesverfassungsgericht den Grundrechtsschutz im Ausland zwar anerkannt,

<sup>142</sup>BVerfGE 143, 101, Rn. 162.

<sup>143</sup>BVerwG, Urt. v. 26.3.2026, 5 C 7.24, Rn. 21; BVerwG, Beschl. v. 18.11.2025, 4 BN 4.25, Rn. 6. Danach ist der Wille des Gesetzgebers nur maßgeblich, soweit er im Gesetzestext wenigstens andeutungsweise einen Niederschlag gefunden hat; grundlegend BVerfGE 86, 59 (64).

<sup>144</sup>Vgl. Nehm, NJW 2004, 3289 (3290 f.); Arts/Jipp, GSZ 2026, 7; Manns, ZRP 2026, 63; Unterreitmeier, GSZ 2022, 251; Gusy, GSZ 2021, 141 (jeweils zum informationellen Trennungsprinzip als judikativ entwickelter Grenze). Differenzierend Wolff, DÖV 2009, 602 (jedenfalls ein organisatorisches Trennungsgebot aus Art. 87 Abs. 1 Satz 2 GG herleitbar); a.A. Bantlin/Graulich, GSZ 2023, 179. Verfassungsgerichtlich bislang offengelassen in BVerfGE 97, 198 (217); zum informationellen Trennungsprinzip weiterführend BVerfGE 133, 277, Rn. 123; BVerfGE 162, 1, Rn. 159.

<sup>145</sup>BVerfGE 162, 1, Rn. 154, 159, 171, 302; BVerfGE 169, 130, Rn. 231.

<sup>146</sup>In diesem Sinne Schantz, Stellungnahme v. 14.7.2026 (Fn. oben), Rn. 18, 24; ähnlich wohl Löffelmann, VerfBlog v. 20.8.2026 (Fn. oben).

<sup>147</sup>Begr. zu Abschnitt 4 BNDG-E, BT-Drs. 21/7868, S. 461 f., unter Berufung auf BVerfGE 154, 152, Rn. 149. Ebenso BVerfGE 170, 79, Rn. 158, wonach der BND „jedenfalls selbst grundsätzlich nicht über eigene operative Befugnisse verfügt“.

seinen Gehalt wie mehrfach erwähnt zumindest im Hinblick auf Artikel 10 GG aber abgestuft.<sup>148</sup> Ob dies ausreicht, um keine polizeigleichen Schwellen für realweltliches Handeln des BND im Rahmen des § 51 BNDG-E zu verlangen, lässt sich kaum seriös abschätzen, aber auch nicht klar verneinen. Es liegt am Gesetzgeber, das hinnehmbare prozessuale Risiko in Karlsruhe hier selbst zu wägen.

Um zumindest ansonsten zu verfassungsgemäßen, insbesondere zu verhältnismäßigen Wertungen zu kommen, müssen die Inlandsbefugnisse im Rahmen der erweiterten Maßnahmen noch begrenzt werden. Die gewählte Regelungsweise, nur gezielte Leib- und Lebensschäden bereits im Gesetz auszuschließen und alles weitere über die Grundanordnungen zu beschränken, mag im Ausland noch rechtmäßig sein und erweist sich jedenfalls als zweckmäßig. Nach der aktuellen „Bauweise“ des § 51 BNDG-E wäre es allerdings theoretisch nicht ausgeschlossen, auch in die Freiheit eingreifende Maßnahmen durchzuführen, wenn sich diese im Inland gegen den Akteur einer fremden Macht richten. Damit kämen dem BND potentiell genau jene Verhaftungsbefugnisse abseits der Polizeibehörden zu, die in der öffentlichen Debatte fälschlicherweise dem BVerfSchG-E zugewiesen und dort mit „Stasi“- sowie „Gestapo“-Vergleichen skandalisiert werden. Es liegt auf der Hand, dass der Regierungsentwurf nicht wirklich intendiert, seinem Wortlaut nach schließt er es derzeit aber auch nicht aus. Für das Inland bedarf es daher in irgendeiner Weise Beschränkungen – entweder, indem man doch einen Positivkatalog nur für realweltliches Handeln im Inland schafft oder zumindest einen sehr gründlich ausgearbeiteten Negativkatalog vorsieht, der ganz erheblich über das allgemeine Verbot gezielter Leib- und Lebensschäden hinausgeht.

Besonderer Regelung bedürfen unseres Erachtens darüber hinaus die Eingriffe in die Freiheit der Person auch unabhängig vom spezifischen Inlandsbezug. Zwar kann in vielen denkbaren Anwendungsszenarien eine Verhältnismäßigkeit zu bejahen sein. Dies schließt aber Zweifel daran nicht aus, ob die Norm verfassungsrechtlich hinreichend bestimmt ist. Art. 104 GG verlangt bereits für Freiheitsbeschränkungen ein förmliches Gesetz und stellt an Freiheitsentziehungen zusätzliche Anforderungen, namentlich den Richtervorbehalt. Welche dieser Anforderungen deutsche Stellen im Ausland in welcher Form binden, ist – einmal mehr – nicht abschließend geklärt. Falls sich der Gesetzgeber nicht auf das Wagnis einer unvorhersehbaren Klärung aus Karlsruhe einlassen möchte, könnte er trotz der Entscheidung, auf Positivkataloge zu verzichten, für derartige Fälle bestimmte Grundpfeiler setzen. Zu regeln wären die erfassten Maßnahmen und Personen, Anlass und Eingriffsvoraussetzungen, eine enge zeitliche Begrenzung, die Beendigung der Maßnahme oder die Übergabe an zuständige Stellen und die erforderlichen gerichtlichen Sicherungen.<sup>149</sup> Dies sollte jeweils gesondert für das Ausland und das Inland geschehen, in dem die Vorgaben des Art. 104 GG unstreitig in vollem Umfang gelten. Möchte der Gesetzgeber keine Kriterien für freiheitsbeschränkende Eingriffe vorsehen, sollte zumindest das Inland als Aktionsraum ausgenommen werden. Dort steht den Angehörigen des Auslandsdienstes ohnehin das vorläufige Jedermann-Festnahmerecht aus § 127 Abs. 1 StPO zu, wenn die Polizei nicht rechtzeitig einschreiten kann, sodass keine wesentlichen Lücken in der Bedrohungsbekämpfung drohen.

---

<sup>148</sup>BVerfGE 154, 152, Leitsatz 1.

<sup>149</sup>Art. 104 GG dürfte mit seiner Schranke im Wortlaut den institutionell abgesicherten Richter meinen, sodass der UKRat nicht ohne Weiteres hier eine Vorabkontrolle durch seinen Senat vornehmen könnte. Angesichts der ohnehin erheblichen verfassungsrechtlichen Wagnisse könnte der Gesetzgeber auch dieses Risiko aber in Kauf nehmen, gegebenenfalls durch das Bundesverfassungsgericht auf die Justiz zurückgeworfen zu werden und dann vermutlich das Bundesverwaltungsgericht mit der Kontrolle zu betrauen. Ein inhaltliches Minus an Kontrolle, das einem solchen Wagnis aus grundrechtlicher Sicht entgegenstehen würde, ist beim UKRat gegenüber der institutionellen Justiz nicht zu besorgen.

Verhältnismäßigkeitsfragen wirft ferner die Einwirkung auf Infrastrukturen (im Ausland, da es niemand von fremden Mächten in Deutschland genutzte Infrastrukturen außerhalb von Kriegsszenarien geben wir) auf, die auch der Zivilbevölkerung dienen. Sinnvoll wäre zumindest eine Klarstellung in § 51 Abs. 3, wonach das Ziel einer Maßnahme nur Infrastruktur sein darf, die von der verantwortlichen fremden Macht für die Gefährdung genutzt wird. Wird eine solche Einrichtung parallel zivil genutzt, wäre zudem eine besonders sorgfältige Abwägung vorzuschreiben. Prüfparameter sollten die zivile Versorgungsfunktion, die technische Abtrennbarkeit und die Auswirkungen auf unbeteiligte Dritte sein. Ein solches Mindestmaß an Begrenzung folgt aus dem Schutzauftrag für die Zivilbevölkerung, der auch für Abwehrhandlungen unterhalb eines bewaffneten Konflikts nicht pauschal unberücksichtigt bleiben darf. Eine vollständige Abtrennbarkeit sollte aber nicht zur Voraussetzung jener bundesnachrichtendienstlichen Maßnahmen werden, weil ein Einschreiten gegen hybride Angriffe sonst faktisch unmöglich würde. Das soeben Gesagte gilt entsprechend für digitale Maßnahmen.

Mitunter wird für realweltliche Maßnahmen mit militärähnlicher Wirkung, etwa den Einsatz von Sprengstoff, über die allgemeinen verfassungsrechtlichen Vorgaben hinaus ein wehrverfassungsrechtlicher Parlamentsvorbehalt erwogen.<sup>150</sup> Dieser Vorbehalt knüpft an den Einsatz bewaffneter Streitkräfte an und passt auf Operationen eines Nachrichtendienstes nicht.<sup>151</sup> Das Eskalationsrisiko, das hinter dem Gedanken steht, ist dennoch real. Ihm trägt der Entwurf durch die Grundanordnung, die Vorabkontrolle und die Unterrichtung des Parlamentarischen Kontrollgremiums (PKGr) Rechnung. Zudem ist über die Fachaufsicht, die unmittelbar beim Bundeskanzleramt liegt, eine direkte und hochrangige politische Rückkoppelung vorhanden. Für Maßnahmen mit kinetischer Wirkung stellt der Ausschluss gezielter Leib- und Lebensschädigungen außerhalb des Verteidigungsfalls zudem hinreichend klar, dass keine kriegerischen bzw. kriegsähnlichen Handlungen durch den BND vorgenommen werden sollen.

In völkerrechtlicher Hinsicht wiegen realweltliche Maßnahmen schwerer als digitale. Sie verlangen deshalb eine intensivere Prüfung, die die Gesetzesbegründung derzeit noch nicht leistet (vgl. bereits unter B.VI.4.a). Physische Einwirkungen auf fremdem Hoheitsgebiet verletzen ohne Zustimmung des betroffenen Staates dessen territoriale Souveränität und Integrität.<sup>152</sup> Sie bedürfen deshalb stets einer Rechtfertigung, die das Völkerrecht in engen Grenzen bereithält, namentlich als Gegenmaßnahme gegen eine vorangegangene Völkerrechtsverletzung des Zielstaats oder im Notstand.<sup>153</sup> Handlungen von Stellvertretern können gegnerischen Staaten dabei zugerechnet werden, wenn diese auf Weisung handeln oder unter effektiver Kontrolle der entsprechenden Hoheitsträger stehen.<sup>154</sup> Auch bedarf es keiner gerichtsförmigen Gewissheit: Vereitelt der verantwortliche Staat den unmittelbaren Beweis, darf die Zurechnung auf Indizien gestützt werden, die in ihrer Gesamtheit nur einen Schluss zulassen.<sup>155</sup> Sind nach einer entsprechenden, durch den BND vorzunehmenden Gesamtbewertung dessen Gegenmaßnahmen statthaft, dürfen diese grundsätzlich nach dem Völkerrecht keine Gewalt einschließen. Dass gezielte Leib- und Lebensschäden nach dem Regierungsentwurf ausgeschlossen werden, ist somit gleichermaßen richtig wie wichtig. Auch eine Sabotage mit erheblichen physischen Schäden kann jedoch das Gewaltverbot tangieren, was entsprechende

<sup>150</sup>Schantz, Stellungnahme v. 14.7.2026 (Fn. oben), Rn. 19.

<sup>151</sup>BVerfGE 90, 286 (381 ff.); BVerfGE 121, 135 (153 ff.). Zur wehrverfassungsrechtlichen Organisationstrennung (Art. 87a GG) vgl. Rieger, GSZ 2026, 86 (88); für ein funktionales Verständnis des Streitkräftebegriffs dagegen Benamor, VerfBlog v. 7.9.2026 (Fn. oben).

<sup>152</sup>Matz-Lück, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, § 2 Rn. 24 ff.

<sup>153</sup>Art. 22, 25, 49–53 ARSIWA (dazu bereits oben).

<sup>154</sup>Art. 8 ARSIWA; IGH, Nicaragua (Fn. oben), Rn. 115.

<sup>155</sup>IGH, Corfu Channel (Vereinigtes Königreich/Albanien), Urt. v. 9.4.1949, ICJ Reports 1949, S. 4 (18).

Prüfungen erfordert. Sie muss der Gesetzgeber allerdings nicht im Vorhinein vornehmen. Vielmehr genügt es, dass die Befugnis im Einzelfall durch den BND völkerrechtskonform angewendet werden kann, zumal Art. 25 GG den Dienst ohnehin an die allgemeinen Regeln des Völkerrechts bindet. Dass der Gesetzgeber mit der eher weiten Ausgestaltung von § 51 BNDG-E kein Neuland auf dem internationalen Parkett betritt, zeigt auch der Blick auf andere europäische Staaten, die ihre Dienste durch Generalklauseln zu aktiven Maßnahmen ermächtigen.<sup>156</sup> Abschließend sei, um mögliche Missverständnisse zu vermeiden, darauf hingewiesen, dass in den geplanten erweiterten Maßnahmen des BND wohl niemals ein bewaffneter Angriff, der das Selbstverteidigungsrecht auslöst (Art. 51 UN-Charta), zu erblicken wäre, selbst wenn die Maßnahme im Nachhinein nicht als völkerrechtliche Gegenmaßnahme anerkannt würde. Denn das Selbstverteidigungsrecht ist aufgrund seiner enormen Konsequenzen nach einem deutlich höheren Maßstab zu beurteilen und trifft selbst auf schweren Staatsterrorismus wohl kaum je zu.

### **c) Absenken nachrichtendienstlicher Schwellen als „erweiterte Maßnahme“**

Nach der Begründung soll § 51 auch Übermittlungen tragen. Der BND soll personenbezogene Daten ohne die Vorgaben des sechsten Abschnitts übermitteln dürfen, wenn dies zur Abwendung oder Einschränkung der Gefährdung erforderlich ist.<sup>157</sup> Die Übermittlung würde damit selbst zur erweiterten Maßnahme, obwohl der Wortlaut des § 51 sie nicht nennt, und im Anwendungsbereich einer Grundanordnung würden die Übermittlungsschwellen des BNDG-E abgesenkt. Das ist nur teilweise zulässig. Die §§ 70 ff. setzen die Schwellen um, die das Bundesverfassungsgericht für die Weitergabe nachrichtendienstlicher Daten an Stellen mit operativen Befugnissen verlangt, nämlich eine zumindest konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut.<sup>158</sup> Für Übermittlungen an ausländische Stellen verlangt es zudem eine Vergewisserung über den rechtsstaatlichen Umgang mit den Daten.<sup>159</sup> Die spezifische Gefährdungslage kann beides nicht ersetzen, weil sie eine sicherheitspolitische Lage beschreibt und weder eine Gefahr im Einzelfall noch eine Prüfung des Empfängers enthält. Hinzu kommt, dass eine Gesetzesbegründung gesetzliche Schwellen nicht außer Kraft setzen kann. Verfassungsrechtlich bedenklich ist das Modell deshalb, soweit Daten an inländische Stellen mit operativen Anschlussbefugnissen oder an ausländische Stellen gehen. Vertretbar ist es dagegen, wenn die Weitergabe selbst die Abwehrhandlung ist, etwa die Warnung eines betroffenen Unternehmens oder der Hinweis an einen Plattformbetreiber auf eine gesteuerte Kampagne. Dann bereitet sie keine fremden Eingriffe vor, sondern wirkt unmittelbar auf die Gefährdung ein. Wir empfehlen deshalb, in § 51 klarzustellen (wie es ohnehin bereits gemeint sein dürfte), dass Übermittlungen an inländische öffentliche Stellen und an ausländische Stellen den Vorschriften des sechsten Abschnitts unterliegen, soweit sie nicht selbst Teil der Abwehrhandlung sind. Die nach § 51 Abs. 6 vorgeschriebene Dokumentation sollte bei solchen Übermittlungen Anlass, Empfänger und Zweck ausweisen, damit der UKRat sie nachträglich prüfen kann.

Dass die Hilfe Dritter auch bei geheimdienstlichen Operationen wichtig ist, wird kaum überraschen. Nach § 51 Abs. 5 soll sie jedoch nicht durchweg freiwillig erfolgen, wie es etwa bei der Nutzung von Gewährspersonen der Fall ist. Öffentliche Stellen, Anbieter öffentlich zugänglicher Telekommunikationsdienste und Anbieter öffentlich zugänglicher digitaler Dienste sollen vielmehr zur Hilfe verpflichtet werden können (Satz 3). Hierbei dürfte es in der Sache vor allem um digitale Gegenschläge

<sup>156</sup>Etwa sec. 1(1)(b) Intelligence Services Act 1994 (Vereinigtes Königreich); Art. D. 3126-2 Code de la défense (Frankreich).

<sup>157</sup>Begr. zu § 51 Abs. 1 BNDG-E, BT-Drs. 21/7868, S. 464.

<sup>158</sup>BVerfGE 154, 152, Leitsatz 6; BVerfGE 162, 1, Rn. 230 ff., 235.

<sup>159</sup>BVerfGE 154, 152, Leitsatz 6.

gehen. Die verpflichteten Stellen sollen dem Regierungsentwurf zufolge den Anlass des Hilfeersuchens nicht selbst nachprüfen müssen, sodass die Verantwortung für eingeforderte Unterstützungshandlungen beim BND verbleibt.<sup>160</sup> Dies ist bei der Arbeit eines Auslandsdienstes allgemein und bei geheimdienstlichen Operationen besonders nachvollziehbar. Dem stehen die Belastung der Verpflichteten und mögliche Folgen für die Nutzer fremder Systeme gegenüber. Die Begründung sollte deshalb erläutern, wie der BND Art und Dauer der verlangten Hilfe auf das Erforderliche begrenzt und unverhältnismäßige Belastungen und Beeinträchtigungen unbeteiligter Nutzer vermeidet. Ebenso sollte sie das Verhältnis zwischen der Verschwiegenheitspflicht (Satz 2 i.V.m. § 8), den Ausnahmegründen (Satz 4) und der Entschädigung nichtöffentlicher Stellen (Satz 5) klarstellen.

## 5. Verhältnis zu anderen Eingriffsbefugnissen

Die drei über nachrichtendienstliche Tätigkeit hinausgehenden Eingriffsregime des BNDG-E – also die hier diskutierten erweiterten Maßnahmen, die Annexbefugnisse (besonders die Abwehr von Cybergefahren während laufender Aufklärung) und die Eigensicherung – ergänzen einander, ohne dass eines das andere ersetzen dürfte.<sup>161</sup> Die Cyberabwehr während laufender Aufklärung verlangt die Identifikation einer unmittelbar bevorstehenden Gefahr und sieht damit eine Schwelle vor, unter der auch eine operativ tätige Behörde wie die Polizei handeln dürfte. Sie ist mit der Judikatur zum informationellen Trennungsprinzip jedenfalls vereinbar, ohne dass es auf die Klärung ankäme, ob digitale Abwehr überhaupt operative Anschlussbefugnisse begründet. Die Eigensicherung wiederum dient nicht der nachrichtendienstlichen Tätigkeit und begründet schon insofern keine *Folgemaßnahmen*.

Außerhalb des BNDG-E kommen die Schutzmaßnahmen des BfV (§ 59 BVerfSchG-E) hinzu und die Cyberabwehrbefugnisse, die der parallel beratene Entwurf eines Gesetzes zur Stärkung der Cybersicherheit dem Bundeskriminalamt und der Bundespolizei zubilligen will. Diese geplanten Erweiterungen reichen von der Untersagung des Betriebs von Systemen über die Umleitung und Unterbindung von Datenverkehr bis zur Löschung und Veränderung von Daten auf fremden Systemen.<sup>162</sup> Bei einem Cyberangriff aus dem Ausland auf ein Ziel im Inland können damit bis zu vier Bundesbehörden zuständig sein, jeweils mit eigenen Schwellen und eigener Kontrolle. Dass das Polizeirecht einen Teil dieser Maßnahmen dem Richtervorbehalt beim Amtsgericht unterstellt und das Nachrichtendienstrecht der Vorabkontrolle des UKRats, folgt aus der unterschiedlichen Kontrollarchitektur und ist für sich kein Widerspruch. Gemeinsame Mindeststandards sollten aber für alle gelten, nämlich eine Dokumentation, eine Abschätzung der Folgen für unbeteiligte Dritte und die Unterrichtung der jeweils anderen Behörden – beim BND insbesondere des Bundesamts für Sicherheit in der Informationstechnik, sofern dem keine operativen oder Geheimhaltungsgründe entgegenstehen. Eine gesetzliche Kollisionsregel empfehlen wir dagegen nicht. Sie müsste die Zuständigkeiten nach Inland und Ausland trennen, und gerade diese Trennung trägt im Cyberraum nicht, weil viele Angriffe aus dem Ausland kommen und im Inland wirken. Eine Regel, die dem BND das Inland und dem BfV das Ausland verschließt, würde beide in dem Moment lähmen, in dem der Angriff die Grenze überschreitet. Gleiches gilt für Unterscheidungen zwischen polizeilichem und nachrichtendienstlichem Wirken, wobei insbesondere der BND mit seiner strategischen Erfassung von Netzen über

<sup>160</sup>Begr. zu § 51 Abs. 5 BNDG-E, BT-Drs. 21/7868, S. 465.

<sup>161</sup>Daneben enthält das BNDG-E einzelne weitere Befugnisse, die über die Aufklärung hinaus wirken, namentlich die automatisierte Auslösung von Abwehrmaßnahmen gegen Cyberangriffe (§ 53 Abs. 7, dazu oben und B.VII) und den Eingriff in fremde Systeme zur Löschung abgeflüssener Verschlusssachen (§ 119, dazu B.X.4).

<sup>162</sup>BT-Drs. 21/6585 (Entwurf eines Gesetzes zur Stärkung der Cybersicherheit); BT-Drs. 21/7406 (Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung).

Möglichkeiten verfügt, die den Polizeien des Bundes nicht offenstehen (und jenen der Länder erst recht nicht). Die Abgrenzung muss und kann deshalb operativ erfolgen, also durch Absprachen der Behörden etwa im Nationalen Cyber-Abwehrzentrum, in dem alle Beteiligten vertreten sind. Wir empfehlen, diesen Abstimmungsauftrag in der Begründung zu § 51 BNDG-E und § 59 BVerfSchG-E festzuhalten und die Dienste zu verpflichten, einander und die Polizeien des Bundes über Einwirkungen nach Maßgabe der operativen Sicherheit und des Geheimschutzes zu unterrichten. Das dient nicht nur der Effizienz – wirken mehrere Behörden auf dasselbe System ein oder überwachen sie dieselben Personen, addieren sich die Eingriffe, und das Bundesverfassungsgericht rechnet sie in einer von ihm vor wenigen Jahren ersonnenen Überwachungsgesamtrechnung möglicherweise zusammen.<sup>163</sup>

## VII. Weiterverarbeitung, insbesondere automatisierte Auswertung (§§ 52, 53)

Weiterverarbeitung meint alles, was der BND nach der Erhebung mit personenbezogenen Daten tut, also Speichern, Auswerten, Verknüpfen, Prüfen und Löschen (Abschnitt 5, §§ 52–67 BNDG-E; zu den Speicher- und Löschrufen für Daten aus der technischen Aufklärung vgl. unter B.III.5). Die §§ 52 und 53 sehen dabei auch einen neuen Fall der Weiterverarbeitung vor: die automatisierte Auswertung großer Datenbestände, auch mit Anwendungen der künstlichen Intelligenz. Der Entwurf trennt dabei zwei Schritte. Nach § 52 Abs. 4 darf der BND Auswertungsprodukte zunächst automatisiert im technischen Hintergrund erstellen. Abrufen darf er Produkte mit qualifiziertem Eingriffsgewicht dagegen nur unter den Schwellen des § 53, der das Gegenstück zur qualifizierten Auswertung des § 37 BVerfSchG-E bildet (C.VI). Qualifiziert sind Produkte, die über einen Datenabgleich hinausgehen und neue Erkenntnisse über die Beziehungen oder die Persönlichkeit von Deutschen oder Personen mit Inlandsaufenthalt gewinnen lassen (Abs. 2). Für ihren Abruf sind die Schwellen nach Eingriffsgewicht gestuft (Abs. 3–5), was zu begrüßen ist.<sup>164</sup>

Nachrichtendienstlich interessante Verbindungen und merkwürdige Muster lassen sich in digitalen Spuren oftmals schon finden, bevor ein konkreter Verdacht formuliert werden kann. Dass der BND stark auf Künstliche Intelligenzen und ähnlich leistungsfähige Anwendungen setzen muss, um insbesondere im SIGINT-Bereich wieder eine Erkenntnisdichte und -qualität zu garantieren, die den horrenden Kosten der Signalerfassung einerseits und dem damit verfolgten Schutzzweck andererseits entspricht, ist vor diesem Hintergrund nur allzu verständlich. Eine menschliche Sichtung jedes Zwischenschritts wäre ineffizient und würde sogar zu einem deutlich erhöhten Grundrechtseingriff führen, weil Auswertungspersonal dann mehr Daten zur Kenntnis nähme als notwendig. Dies stellte bereits in der Vergangenheit ein Problem dar, weil die eingesetzten Selektoren mitunter so vage ausfielen, dass mit ihrer Einsteuerung eine hohe Streuwirkung entstand, die zu fehlerhaften Vorwieldeprodukten führte. Folgerichtig ist im ersten Schritt eine vertiefte technische Vorauswahl vorgesehen, für die die qualifizierte Schwelle (sofern sie abseits der Auslandsausländer anwendbar ist) noch nicht gilt, sondern erst bei dem Verarbeitungsschritt hinzutritt, der ein Produkt für die weitere Verwendung zugänglich macht.<sup>165</sup> Dass zunächst kein Mensch die Daten zur Kenntnis nimmt, mindert das Eingriffsgewicht in dieser Frühphase der Auswertung, beseitigt den dadurch entstehenden Grundrechtseingriff aber nicht, was auch die Gesetzesbegründung anerkennt.<sup>166</sup> Die für polizeiliche Datenanalysen in der HessenData-Entscheidung entwickelten Maßstäbe lassen sich zwar nicht

<sup>163</sup>BVerfGE 125, 260, Rn. 218; BVerfGE 141, 220, Rn. 130.

<sup>164</sup>Zur Vorgabe BVerfGE 165, 363, Rn. 99 ff.

<sup>165</sup>BT-Drs. 21/7868, S. 111 f.; Begr. S. 469 ff.

<sup>166</sup>Begr. zu § 53 BNDG-E, BT-Drs. 21/7868, S. 470.

schematisch auf Nachrichtendienste übertragen, ihr Grundgedanke gilt aber auch hier.<sup>167</sup> Danach muss – erstens – auch eine automatisierte Freigabe oder Zweckzuweisung als Abruf im Sinne des § 53 gelten, obgleich nicht jeder Analysevorgang manuell ausgelöst werden muss. Andernfalls ließen sich Ergebnisse maschinell weiterleiten und so an der Schranke vorbeiführen. Zweitens sollte das Gesetz genauer bestimmen, wo die Erzeugung eines Produkts endet, wann es abgeschirmt vorgehalten wird und wann es freigegeben ist. Technische Zugriffssperren, die es aus Gründen der operativen Sicherheit im BND ohnehin längst gibt, sollten gesetzlich vorgeschrieben werden, und vor jeder Freigabe sollte eine dokumentierte Schwellenprüfung stattfinden. Für ungenutzte Produkte müssten zudem überprüfbare Prüf- und Löschfristen gelten. Der UKRat sollte administrativ kontrollieren, ob dieses Modell praktisch trägt, ohne dass ihm einzelne technische Zwischenergebnisse vorgelegt werden müssen.

Eine Ausnahme von der Abrufschranke bildet die sogenannte automatisierte Reaktion. Nach § 53 Abs. 7 darf ein Auswertungsprodukt für sich genommen grundsätzlich nur Auskunftersuchen an öffentliche Stellen automatisiert auslösen. Satz 2 macht davon jedoch eine Ausnahme für die Abwehr von Cyberangriffen. Das eingesetzte System darf hierfür im Einzelfall selbst Daten verändern oder löschen und Datenverkehre umleiten oder unterbinden, wenn der Angriff anders nicht oder nicht rechtzeitig abgewehrt werden kann. Nach der Begründung ist dann auch die Entscheidung, ob ein Angriff vorliegt und welche Maßnahme geeignet ist, dem autonomen System überlassen.<sup>168</sup> Im Ansatz ist das hinzunehmen, denn automatisierte Angriffe laufen spätestens seit dem Einzug flächendeckender Hackerangriffe durch KI-Systeme Mitte des Jahres 2026 und wohl auf absehbare Zeit in Zeiträumen ab, in denen kein Mensch rechtzeitig entscheiden kann. Zudem sind die zulässigen Reaktionen eng umschrieben. Greift eine automatisierte Maßnahme als eigenständige Intervention erheblich in Grundrechte ein, sollte sie dem UKRat jedoch unverzüglich zur nachträglichen Prüfung vorgelegt werden. Paketfilter und vergleichbare Zwischenschritte sollten nicht darunter fallen (vgl. unter D.XVII).

Einen eigenen Verarbeitungsweg eröffnet § 60 BNDG-E für Forschung und Entwicklung. Er erlaubt die Weiterverarbeitung personenbezogener Daten zu Forschungs- und Entwicklungszwecken einschließlich des Trainings von KI-Anwendungen. Die Daten sind grundsätzlich unkenntlich zu machen, es sei denn, dies widerspricht dem Forschungs- und Entwicklungszweck oder erfordert einen unverhältnismäßigen Aufwand (Abs. 1 S. 2). Die Speicherfrist beträgt grundsätzlich fünfzehn Jahre, wobei eine längere Speicherung zulässig sein kann, soweit sie im Einzelfall erforderlich ist (Abs. 4). Absatz 2 erlaubt für diesen Zweck die Einsichtnahme in Daten aus der strategischen Aufklärung „abweichend von den §§ 33 und 34“. Das ist der Zugriff auf erfasste Kommunikation ohne Suchbegriff, ohne Bedrohungsbezug und ohne Rücksicht auf den Inlandsbezug, zum Zweck der Systementwicklung. Der Bedarf für eine solche Regelung ist nachvollziehbar, weil Erkennungsverfahren an echten Daten trainiert werden müssen, um schlagkräftig und präzise zu wirken. Damit weicht die Norm jedoch von einem Kernprinzip der strategischen Aufklärung ab, wonach erfasste Daten nur ausgewertet werden dürfen, nachdem eine Einsichtnahme unter bestimmten Voraussetzungen erfolgt ist. Die grundsätzlich gebotene Unkenntlichmachung und die Beschränkung auf Systementwicklung statt Aufklärung mindern diesen Eingriff zwar ab. Durch die Ausnahmetatbestände von der Unkenntlichmachung und die Möglichkeit einer Speicherung über fünfzehn Jahre hinaus werden diese Sicherungen aber geschwächt. Prägendes Schutzmerkmal ist somit (nur noch) die

---

<sup>167</sup> Vgl. BVerfGE 165, 363; die Entscheidung betrifft nicht das Modell des BND-Gesetzes.

<sup>168</sup> Begr. zu § 53 Abs. 7 BNDG-E, BT-Drs. 21/7868, S. 474.

Zweckbindung des Absatzes 5. Ihre Ausnahme für unmittelbar bevorstehende Gefahren eröffnet allerdings wiederum einen Zweckwechsel ohne die regulären Einsichtnahmeschwellen der §§ 33 und 34 und ohne besondere Vorabkontrolle. Auch wenn für die Ausnahme spricht, dass im Forschungsbestand ein konkreter Hinweis auf eine unmittelbar bevorstehende Gefahr auftauchen kann, obwohl der operative Datenbestand bereits gelöscht ist, sorgt das Zusammenwirken der verschiedenen Ausnahmetatbestände im Ergebnis dafür, dass mit einem großen Datenpool potentiell rechtmäßig die Schwellenlogik der neuen Fernmeldeaufklärung unterlaufen werden könnte. Wir regen deshalb eine engere Fassung der Norm an. Ein Zweckwechsel sollte nur zulässig sein, soweit konkret bezeichnete Daten für die Abwehr der unmittelbar bevorstehenden Gefahr unerlässlich und nicht rechtzeitig aus einem anderen zulässigen Bestand zu gewinnen sind. Zudem muss dieser Sonderfall begründet und protokolliert werden. Über die Zweck- und Rechtmäßigkeit sollte zunächst die Behördenleitung entscheiden, überführte Daten müssten dem UKRat anschließend zur Einzelfallkontrolle vorgelegt werden, wofür § 97 Abs. 3 BNDG-E entsprechend zu ergänzen ist.

Missverständlich ist schließlich die Frist von fünfzehn Jahren in § 56 Abs. 2 BNDG-E. Sie bezeichnet ein Höchstintervall für die Prüfung der Erforderlichkeit, keine allgemeine Höchstspeicherfrist und keine Garantie, Daten so lange behalten zu dürfen. Entfallen die Voraussetzungen der Speicherung früher, verlangt § 56 Abs. 1 grundsätzlich auch die frühere Löschung. Absatz 2 enthält zudem Ausnahmen.<sup>169</sup> Wir empfehlen gleichwohl kürzere Prüfintervalle, die sich am Risiko des jeweiligen Datenbestands orientieren. Für die langfristige Aufklärung fremder Mächte können dabei längere Intervalle gerechtfertigt sein als für andere Bestände. (Zum Auslesen von Speichern nach § 54 siehe unter C.IV.6.a.)

## VIII. Übermittlung (§§ 70–94)

### 1. Katalog gleichwertiger Delikte einer „besonders schweren Straftat“

Die Übermittlungsvorschriften übernehmen im Wesentlichen das geltende Recht. Dabei sorgt der Gesetzentwurf an einzelnen Stellen für feine Nachjustierungen im Sinne der sehr intensiven verfassungsrichterlichen Judikatur zum Übermittlungswesen. Dies betrifft besonders die Schaffung eines Katalogs von Straftaten in § 81 BNDG-E, die neben der „besonders schweren Straftat“ stehen, welche zutreffend als ein solches Delikt bezeichnet ist, dessen Höchststrafe *mehr* als fünf Jahre umfasst, sodass der fünfjährige Höchststrafen einen Tatbestand nicht bereits aus sich heraus hinreichend qualifiziert. Ob die in den Katalog aufgenommenen Delikte allesamt der Qualität einer besonders schweren Straftat entsprechen, ist an den Entscheidungslinien des Bundesverfassungsgerichts zu prüfen. Danach hat der Strafrahmen nur eine – freilich maßgebliche – Indizwirkung. Auch ein Delikt mit einer Höchststrafe von fünf Jahren kann daher besonders schwer sein, wenn neben dem Rechtsgut auch Tatbegehung und Tatfolgen diese Wertung tragen und die Strafnorm selbst entsprechende Umstände objektiviert.<sup>170</sup> Ein bloßer Staatsschutzbezug genügt dagegen nicht, ebenso wenig eine gegen Verfassungsschutzgüter gerichtete Zielsetzung des Täters.<sup>171</sup> Zudem scheiden Delikte mit einer Höchststrafe von unter fünf Jahren, also drei Jahren oder (noch) niedriger, von vornherein aus.<sup>172</sup>

<sup>169</sup> BT-Drs. 21/7868, S. 113 f.

<sup>170</sup> BVerfGE 169, 130, Rn. 204–207.

<sup>171</sup> BVerfGE 169, 130, Rn. 208–210.

<sup>172</sup> BVerfGE 169, 130, Rn. 208, 216.

Gemessen daran ist ein großer Teil des vorgesehenen Katalogs unproblematisch. Das gilt für Tatbestände, die eine konkrete Gefahr eines schweren Nachteils für die äußere Sicherheit voraussetzen (§§ 95, 96 Abs. 2, 97, 100a StGB), für Delikte mit Taterfolg oder konkreter Gefährdung wie Sabotage und die Störung wichtiger Anlagen (§§ 88, 109e, 305a, 315b, 316b, 317, 318 StGB) und für Delikte mit Gewalt oder Drohung als Begehungsform (§§ 83 Abs. 2, 106, 107 StGB). Ebenso liegt es bei den Verbrechenstatbeständen des Kriegswaffen-, Waffen- und Chemiewaffenrechts und bei § 111 und § 127 StGB, die nur bei einer besonders schweren Bezugstat erfasst sind.

Bei anderen Delikten trägt dagegen vor allem das Rechtsgut die Qualifizierung als einer besonders schweren Straftat entsprechendes Delikt, während Begehungsmerkmale und Tatfolgen nicht zwingend für eine solche Kategorisierung streiten. Dies betrifft etwa die landesverräterische Agententätigkeit und den sicherheitsgefährdenden Nachrichtendienst (§§ 98, 109f StGB), die beide den Auftrag einer fremden Macht, aber keinen Gefahrerfolg verlangen. Es betrifft ferner den Angriff auf Organe ausländischer Staaten (§ 102 StGB), der auch eine einfache Körperverletzung erfasst, und die Störpropaganda gegen die Bundeswehr (§ 109d StGB). Für diese Delikte sollte die Gesetzesbegründung zumindest darlegen, worin aus Sicht des Parlamentes die objektivierte besondere Schwere liegt, um ihre sicher anstehende verfassungsgerichtliche Überprüfung zu fördern. Trotz der bei den vorgenannten Tatbeständen bestehenden Rechtsrisiken ist aus hiesiger Sicht zumindest der operative Sinn derartiger Übermittlungen sehr nachvollziehbar, sodass dem Gesetzgeber eine vorseilende Kürzung in Erwartung möglicher begrenzender Rechtsprechung kaum zu empfehlen ist.

Nicht zu halten sind dagegen die Verunglimpfungsdelikte (§§ 90, 90a Abs. 3, 90b StGB). Hierbei handelt es sich um reine Äußerungsdelikte, deren Schwere allein auf dem Staatsschutzbezug und einer bestimmten Begehungsabsicht beruht. Das Bundesverfassungsgericht hatte gerade die öffentliche Verleumdung der mittleren Kriminalität zugeordnet und ihr die Eignung einer ausnahmsweisen Anerkennung als besonders schwere Straftat somit sakrosankt versagt.<sup>173</sup> Gleiches gilt für den besonders schweren Fall der kriminellen Vereinigung (§ 129 Abs. 5 S. 1 und 2 StGB), der keinen Qualifikationstatbestand darstellt, sondern eine Strafzumessungsregel begründet. Ob sich ein nach diesem Tatbestand zu entscheidender Fall als besonders schwer erweist, ergibt sich erst aus einer Gesamtwürdigung durch das Gericht, und das Regelbeispiel des Satzes 2 begründet nur eine widerlegliche Vermutung. Die besondere Schwere findet damit gerade nicht den objektivierten Ausdruck in der Strafnorm, den das Bundesverfassungsgericht verlangt.<sup>174</sup> Darüber hinaus entfallen § 84 Abs. 2 und § 182 Abs. 2 StGB von vornherein, weil sie nur mit bis zu drei Jahren bedroht sind. Die vom Bundesrat geforderte Aufnahme der Volksverhetzung (§ 130 StGB) lehnt die Bundesregierung aus den genannten Gründen zu Recht ab.<sup>175</sup> Ihr Tatbestand verlangt insbesondere nur die Eignung zur Störung des öffentlichen Friedens, also weder einen Erfolg noch eine besondere Begehungsform.

Der besonderen Behandlung von Daten aus der Wohnraumüberwachung im Inland und der Online-Durchsuchung gegenüber Deutschen und Inländern, für die nach der Rechtsprechung eine Höchststrafe von fünf Jahren nie genügt,<sup>176</sup> trägt der Entwurf bereits Rechnung, indem § 77 ihre Übermittlung zur Strafverfolgung auf die Katalogtaten des § 100b Abs. 2 StPO beschränkt.<sup>177</sup> Für entsprechende Maßnahmen gegenüber Ausländern im Ausland (§ 29 Abs. 1, § 37 Abs. 2) gilt dagegen § 81

<sup>173</sup>BVerfGE 169, 130, Rn. 204, 208 f.

<sup>174</sup>BVerfGE 169, 130, Rn. 206 f.

<sup>175</sup>BT-Drs. 21/8295, S. 7, 14.

<sup>176</sup>BVerfGE 169, 130, Rn. 205.

<sup>177</sup>§ 77 Nr. 1 lit. a, Nr. 2 lit. a BNDG-E; Begr. zu § 77, BT-Drs. 21/7868, S. 492.

einschließlich der im Katalog aufgeführten Straftatbestände. Ob der abgestufte Grundrechtsschutz im Ausland das verfassungsrechtlich trägt, kann schwer vorhergesagt werden.

## 2. Übermittlungen an die Bundeswehr

Materiell im Vergleich zum geltenden Recht deutlich weitergehend gefasst ist § 80 BNDG-E. Nach Absatz 1 soll der BND der Bundeswehr Daten übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass sie zu den genannten militärischen Zwecken erforderlich sind. Eine zusätzliche qualifizierte Gefahrenschwelle verlangt die Norm nicht. Tragender Grund ist, dass der BND als militärischer Auslandsnachrichtendienst der Bundesrepublik gerade auch für die Bundeswehr entsprechende Aufklärungsmaßnahmen durchführt und insoweit (neben dem streitkräfteeigenen militärischen Nachrichtenwesen) gerade für die Bundeswehr aufklärt. Die regelmäßige militärische Lageversorgung ist deshalb nicht mit der Weitergabe an eine gewöhnliche inländische Gefahrenabwehrbehörde gleichzusetzen, was die Gesetzesbegründung zu Absatz 2 zu Recht anbringt.<sup>178</sup> Davon zu trennen ist der zweite Schritt: Nach § 31 Abs. 2 S. 1 sind Übermittlungen gemäß § 80 Abs. 2 von einer vorherigen Sichtung durch den BND befreit (vgl. S. 2 Nr. 1), der für gewöhnlich keine Rohdaten, sondern aufbereitete Auswerteprodukte oder sogar erst „Finished Intelligence“ weitergibt. Durch diese Sondervorschrift wird die automatisierte, nach der Begründung auch echtzeitnahe Übermittlung von Rohdaten zugelassen, die der BND noch nicht gesichtet hat. Zwar kennt auch das geltende BNDG bereits automatisierte Übermittlungen an die Bundeswehr für bestimmte, anhand von Suchbegriffen erhobene Daten der strategischen Aufklärung (§ 11b Abs. 4 Nr. 1 BNDG) sowie für Daten aus individuellen Aufklärungsmaßnahmen nach § 34 BNDG (§ 11b Abs. 4 Nr. 2 BNDG) und für Daten aus der Eignungsprüfung (§ 24 Abs. 7 S. 1 Nr. 2, S. 2 BNDG). Auch das geltende Recht schreibt dafür nicht stets eine vorherige persönliche Einsichtnahme vor, wählt aber durch Suchbegriffe und Zweckbindungen aus. Demgegenüber reicht die Neuregelung deutlich weiter und ist daher verfassungsrechtlich unweigerlich sensibler.

Wir halten § 80 BNDG-E dennoch für verfassungsrechtlich (noch) vertretbar. Für ihn sprechen zunächst militärische Zwecke und die besondere Stellung der Bundeswehr und das aus der Rolle des BND als dem militärischen Auslandsnachrichtendienst zwingend erwachsenden engen Kooperationsverhältnis. Dem steht auch nicht entgegen, dass das militärische Nachrichtenwesen selbst ebenfalls Informationserhebungen strategischer Art durchführt. An die Bundeswehr gerichtete Übermittlungen sind an die Einsatzbereitschaft und den Schutz der Streitkräfte, die Landes- und Bündnisverteidigung sowie die Vorbereitung von Auslandseinsätzen zweckgebunden (§ 80 Abs. 1) – also an elementare Aufgaben, die der Truppe durch Art. 87a GG ausdrücklich zugewiesen sind. Gerade für zeitkritische militärische Lagebilder kann die automatisierte Übermittlung vor der Einsichtnahme des BND erforderlich sein, um das gebotene Maß an Effektivität der Streitkräfte sicherzustellen. Letztlich würde eine Überdehnung von Schwellen aus einem streng institutionellen Blick heraus, der BND und Bundeswehr als gänzlich verschiedene Stellen betrachtet, auch nur zu einer Verlagerung zugunsten des militärischen Nachrichtenwesens führen, dessen Aufklärungstätigkeit keiner gesetzlichen Regelung und ebenso wenig einer spezifischen Kontrolle unterliegt.

Ein Empfänger ohne jede Anschlussbefugnis ist die Bundeswehr trotz alledem nicht.<sup>179</sup> Sogar im Inland kann sie in den Fällen der Art. 35 und 87a Abs. 3 und 4 GG tätig werden und im begrenzten

<sup>178</sup> BT-Drs. 21/7868, S. 124 f.; Begr. S. 493 ff. Zur vorherigen Neuordnung der Übermittlungsvorschriften des BNDG vgl. Thiel, ZRP 2023, 234.

<sup>179</sup> Zum Maßstab vgl. BVerfGE 169, 130, Rn. 107, 113.

Anwendungsbereich des UZwGBw auch Zwang ausüben, wobei Letzterer eher dem Eigensicherungsregime der Dienste entspricht. Schon das geltende BNDG rechnet naheliegenderweise damit, dass übermittelte Daten zur operativen Anwendung unmittelbaren Zwangs verwendet werden können (vgl. § 11b Abs. 3 BNDG). Maßgeblich für eine verfassungskonforme Ausgestaltung des § 80 BNDG-E sind deshalb der streng militärische Verwendungszweck und wirksame Sicherungen innerhalb der Streitkräfte. Für ihr Handeln im Ausland gelten zwar das Einsatzrecht, der Parlamentsvorbehalt für bewaffnete Einsätze und, soweit ein bewaffneter Konflikt vorliegt, das humanitäre Völkerrecht. Weil diese Bestimmungen aber nicht spezifisch auf Datenhaltung und -verarbeitung ausgerichtet sind, sollte der Deutsche Bundestag ausdrücklich regeln, dass die §§ 33, 34 und die Prüf- und Löschpflichten der §§ 65, 66 für die übermittelten Daten in der Bundeswehr entsprechend gelten.

Zuletzt sei darauf hingewiesen, dass der Katalog des § 81 bislang keine qualifizierten Erpressungs- und Geldwäschekonstellationen (§§ 253, 261 StGB) erfasst. Derartige Konstellationen liegen nicht eindeutig unter den sonstigen, in § 81 geregelten Tatbeständen, ordnen sich hinsichtlich ihrer Erheblichkeit aber klar am unteren Rand ein. Als rein rechtspolitischer Vorschlag erwägenswert könnte es angesichts dessen sein, etwa staatliche Steuerung oder die drohende Verletzung besonders gewichtiger Gemeinwohlüter durch Folgehandlungen im vagen Verdachtssinne tatsächlicher Anhaltspunkte hinzuzunehmen.

## **IX. Kontrolle, Auskunft, Rechtsschutz (§§ 95–103)**

### **1. Vorabkontrolle und Einzelfallkontrolle**

Der Katalog an vorabkontrollpflichtigen Maßnahmen in § 97 Abs. 1 BNDG-E fällt umfangreicher aus als jener des BVerfSchG-E, was den gegenüber dem Inlandsdienst mitunter weitergehenden Befugnissen des BND Rechnung trägt. Er erfasst die strategische Aufklärung, die Telekommunikationsüberwachung mit Inlandsbezug, die Eingriffe in private und in inländische IT-Systeme, die Feststellung des qualifizierten Aufklärungsbedarfs für die unselektierte Übermittlung von Metadaten (§ 44 Abs. 2) und die Eingriffe zum Schutz von Verschlusssachen. Nicht erfasst sind der biometrische Abgleich (§ 5 Abs. 3), der Zugriff auf komplexe, nicht privat genutzte Systeme (§ 37 Abs. 1), der heimliche Zugang zu Anbietersystemen (§ 32 Abs. 2), die Gefahrenabwehr in der Erfassung (§ 31 Abs. 6) und die einzelne erweiterte Maßnahme (§ 51). Für den heimlichen Zugang zu Anbietersystemen und die Gefahrenabwehr in der Erfassung haben wir Ergänzungen vorgeschlagen (vgl. unter B.III.2). Ergänzungsbedürftig ist der Katalog zudem bei der optischen und akustischen Überwachung im nichtöffentlichen Raum außerhalb von Wohnungen (§ 27 Abs. 3). Sie erfasst das nichtöffentlich gesprochene Wort und steht in ihrer Eingriffsintensität der Telekommunikationsüberwachung nicht nach, ist aber schon zur allgemeinen Auslandsaufklärung zulässig und unterliegt der Vorabkontrolle nur, wenn sie längerfristig angelegt ist (§ 97 Abs. 1 Nr. 8). Wir empfehlen, ihre Schwelle an die der Telekommunikationsüberwachung anzugleichen und sie unabhängig von der Dauer in § 97 Abs. 1 Nr. 8 aufzunehmen.

Für die übrigen Maßnahmen halten wir die bestehende Kontrolle für ausreichend.

Eine Besonderheit des Kontrollkatalogs betrifft die Ausdehnung einer angeordneten Maßnahme auf weitere Personen. Die Anordnung eines Auskunftersuchens oder einer gegen eine Person gerichteten Maßnahme kann den Zusatz enthalten, dass sie sich auch gegen andere als die genannten Personen richten darf, wenn bei dem Aufklärungsziel mit weiteren Beteiligten zu rechnen ist und die

Voraussetzungen auch ihnen gegenüber vorliegen werden (§ 17 Abs. 4, § 46 Abs. 5, § 48 Abs. 4 S. 1 BNDG-E). Bei der Telekommunikationsüberwachung kann der Zusatz zudem weitere Rufnummern und Anschlüsse erfassen (§ 48 Abs. 4 S. 2). Macht der Dienst von einem solchen Zusatz Gebrauch, legt er eine tatsächlich vollzogene Ausdehnungshandlung später nicht erneut zur Vorabkontrolle vor, sondern unverzüglich zur Einzelfallkontrolle (§ 97 Abs. 3 S. 1 Nr. 4). Stellt der UKRat fest, dass sie unzulässig war, sind die erhobenen Daten zu löschen (§ 97 Abs. 3 S. 2). Dieses Modell mag auf den ersten Blick, weil es von den bekannten Verfahren etwa nach §§ 1, 3 G 10 abweicht, vielleicht irritieren. Verfassungsrechtlich dürfte es allerdings tragen, weil die Hinzunahme weiterer Personen bereits Teil der vorab kontrollierten Anordnung ist und die konkrete Anwendung des insoweit erfolgenden Anordnungsvollzugs dennoch, wenngleich nachträglich, geprüft wird. Die Verweisung in § 97 Abs. 3 S. 1 Nr. 4 ist allerdings um § 17 Abs. 4 zu ergänzen (vgl. Anlage Nr. 1).<sup>180</sup> Beim BfV setzt die entsprechende Kontrolle deutlich später ein (vgl. dazu unter C.V).

## 2. Auskunft (§ 102)

Deutlich verändert wird das Auskunftsrecht der Betroffenen. Es ist ein Instrument der Kontrolle und zugleich der Schlüssel zu den übrigen Betroffenenrechten, können Betroffene diese praktisch doch erst ausüben, wenn sie wissen, welche Daten über sie bei den Diensten gespeichert sind. § 102 BNDG-E löst das Auskunftsrecht gegenüber dem BND erstmals von seiner verfassungsschutzrechtlichen Vorbildnorm aus § 15 BVerfSchG, auf die § 9 BNDG bislang verweist. Der Regierungsentwurf trennt die Regelungsregime jedoch nicht nur, sondern ändert für den BND auch materiell dreierlei: den Gegenstand der Auskunft (Abs. 1), die Ausschlussgründe (Abs. 2) und die Beschwerdeinstanz (Abs. 5). Die Neuregelung überzeugt im Grundsatz stark, bedarf aber an einzelnen Stellen der Klarstellung.

Voraussetzungen der Auskunft bleiben die Benennung eines konkreten Sachverhalts und die Darlegung eines besonderen Auskunftsinteresses durch den Petenten. Neu gefasst wird indes der Gegenstand des Auskunftsanspruchs. Erfasst sind künftig nur solche Daten, die in einer Personendatenbank gespeichert oder über sie auffindbar sind. Andere Informationen erfasst der Anspruch ausnahmsweise dann, wenn die betroffene Person Angaben macht, mit denen sie sich mit angemessenem Aufwand eindeutig auffinden lassen (Abs. 1). Dies mag nach einer Verengung klingen, überträgt aber im Wesentlichen auf den modernen Behördenalltag mit seiner elektronischen Aktenführung jene Begrenzungen, die das Bundesverwaltungsgericht dem geltenden Recht schon in verfassungskonformer Auslegung entnommen hat.<sup>181</sup> Ein verfassungsrechtlich geringes Restrisiko bleibt darin bestehen, dass der Dienst selbst bestimmt, was er in eine Personendatenbank einspeichert, und dadurch systematisch bestimmte Auskunftersuchen sperren könnte. Da er sich durch eine Austragung entsprechender Informationen aus den bundesnachrichtendienstlichen IT-Systemen aber auch selbst des Zugriffs auf sie berauben würde, weil bei der Vielzahl seiner Mitarbeiter schon rein praktisch keine Information „unter der Hand“ über ihr Vorhandensein an einem Ort außerhalb der Datenbankstrukturen möglich wäre, bleibt dieses Missbrauchsszenario abstrakt. Freilich schadet es nichts, wenn das administrative Kontrollorgan des UKRats vielleicht gelegentlich stichprobenhaft prüft, dass operative Recherchierbarkeit und Auskunftsumfang übereinstimmen.

<sup>180</sup> BT-Drs. 21/7868, S. 134 f.

<sup>181</sup> BVerwG, NVwZ 2008, 580 (582) zur „missverständlichen Verweisung“ in § 9 i.V.m. § 6 Abs. 1 BNDG. Zum Auskunftsrecht nach dem Entwurf vgl. Ogorek/Manns, Was der BND künftig nicht mehr sagen muss, VerfBlog v. 24.9.2026, <https://verfassungsblog.de/nachrichtendienstreform-auskunftsrecht>.

Kern der Neuregelung ist die Erweiterung der Ausschlussgründe. Neben Herkunft und Empfängern der Daten (Abs. 2 Nr. 1, bisher § 15 Abs. 3 BVerfSchG) sind künftig solche Daten von vornherein vom Auskunftsanspruch ausgenommen, deren Weitergabe nachrichtendienstliche Verbindungen offenlegen würde (Nr. 2), oder deren Offenlegung eine Gefährdung operativer Vorgänge oder der Funktions- und Kooperationsfähigkeit des Dienstes besorgen lässt (Nr. 3). Die Versagungsgründe des Absatzes 3, die eine Abwägung im Einzelfall verlangen, entsprechen dagegen nahezu wörtlich § 15 Abs. 2 BVerfSchG. Dass der Regierungsentwurf ausgerechnet die Ausschlussgründe ausweitet, ist insofern rechtlich raffiniert angelegt, als nach der Rechtsprechung des Bundesverwaltungsgerichts das behördliche Ermessen bei ihrer Einschlägigkeit zulasten des Petenten vorstrukturiert ist. Dem Geheimhaltungsinteresse kommt somit regelmäßig der Vorrang zu, und eine Einzelfallabwägung ist nur geboten, wenn der Betroffene Anhaltspunkte dafür aufzeigt, dass eine Auskunft zur Vermeidung gewichtiger Nachteile ausnahmsweise erforderlich ist.<sup>182</sup> Die Erweiterung des Katalogs entlastet die Dienste damit – hoffentlich – von aufwändigen Einzelfallprüfungen und, bezogen auf spätere gerichtliche Auseinandersetzungen, vom Erlass jener Sperrerklärungen nach § 99 Abs. 1 S. 3 VwGO, die nach den Anforderungen des bundesverwaltungsgerichtlichen In-Camera-Senats mittlerweile absatzweise Begründungen selbst bei sehr langen Aktenstücken oder Konvoluten verlangen.

Um von dem Regelungskonzept zu profitieren, müssen Ausschlussgründe allerdings auch tatsächlich jene typisierende Wertung zugunsten des BND tragen, die diese Vorstrukturierung voraussetzt. Für die Kooperationsfähigkeit mit ausländischen Diensten liegt das auf der Hand: Ohne Partnerdienste kann der BND seinen Auftrag nicht erfüllen, und wer die Third Party Rule bricht, nach der übermittelte Erkenntnisse nur mit Zustimmung des Herkunftsdienstes weitergegeben werden dürfen, riskiert den Zugang zu mitunter lebenswichtigen Informationen.<sup>183</sup> Den Geheimschutz operativer Vorgänge lässt das Bundesverwaltungsgericht sogar gegenüber dem verfassungsunmittelbaren Auskunftsanspruch der Presse regelmäßig überwiegen.<sup>184</sup> Auch der Quellenschutz dürfte bei typisierender Betrachtung regelmäßig eine Informationsversagung des BND rechtfertigen. Er dient nicht nur der Sicherheit der geführten Person, sondern wahrt zugleich die Fähigkeit des Dienstes, künftig Informanten zu gewinnen.<sup>185</sup> Dass der Entwurf den Ausschluss auf die drohende Offenlegung nachrichtendienstlicher Verbindungen beschränkt und den übrigen Quellenschutz in der Abwägung des Absatzes 3 Nr. 2 belässt, ist dabei eine aner kennenswert enge und somit grundrechtsfreundliche Lösung.

Anders liegen die Dinge beim Begriff der Gefährdung der Funktionsfähigkeit des BND (Abs. 2 Nr. 3 Var. 2). Sie lässt sich begrifflich kaum von der Gefährdung der Aufgabenerfüllung des Dienstes unterscheiden, die Absatz 3 Nr. 1 lediglich als Versagungsgrund anerkennt und dadurch einer individuellen Abwägung jedes Petentenersuchens unterwirft. Wären beide materiell deckungsgleich, liefe die Abwägung leer. Die Gesetzesbegründung legt jedoch nahe, dass die Funktions- und die bereits angesprochene Kooperationsfähigkeit des BND als Einheit zu verstehen sind. In dieser Lesart ist der Tatbestand eng genug, ergibt sich aber nicht eindeutig aus dem Gesetzestext. Der Gesetzgeber sollte daher begrifflich nachschärfen, etwa durch die Formulierung „Funktionsfähigkeit im Rahmen der Zusammenarbeit mit anderen [alternativ: ausländischen] Stellen“.

<sup>182</sup>BVerwG, NJW 1990, 2761 (2764); NVwZ 2016, 1487 (1489) Rn. 21 ff.; NVwZ 2018, 590 (593) Rn. 29.

<sup>183</sup>BVerfGE 143, 101, Rn. 146 ff., 162.

<sup>184</sup>BVerwG, NVwZ 2025, 1184 (1185) Rn. 19.

<sup>185</sup>BVerfGE 146, 1, Rn. 112.

Klarstellungsbedürftig ist ferner die Gesetzesbegründung selbst, soweit sie formuliert, bei den Ausschlussgründen bestehe kein Ermessen.<sup>186</sup> Das klingt nach einer Bereichsausnahme. Eine Gesetzesbegründung kann den Anspruch auf ermessensfehlerfreie Entscheidung aber nicht beseitigen, der nach der Rechtsprechung des Bundesverwaltungsgerichts unmittelbar aus der Verfassung greifen soll, sofern kein oder nur ein nicht einschlägiger einfachgesetzlicher Auskunftsanspruch besteht.<sup>187</sup> Er besteht deshalb auch gegenüber den neuen Ausschlussgründen fort. Gemeint sein kann daher nur die Vorstrukturierung, nach der das Geheimhaltungsinteresse im Regelfall überwiegt und die eine Einzelfallprüfung nur bei gewichtigen Anhaltspunkten verlangt, die der Antragsteller selbst aktiv vorbringen muss. Das hätte die Gesetzesbegründung ausdrücklich klarstellen sollen, zumal eine gegenläufige Auffassung in ihr ohnehin keinen Regelungscharakter beanspruchen kann.

Beschwerdeinstanz gegen ablehnende Entscheidungen ist künftig der UKRat anstelle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI; Abs. 5). Für den Betroffenen ändert sich dadurch insofern wenig, als der UKRat ihm ebenso wenig Mitteilungen machen darf, die Rückschlüsse auf den Erkenntnisstand des Dienstes zulassen, wie es der BfDI durfte. Dass der Europäische Gerichtshof für Menschenrechte das Fehlen einer begründeten Entscheidung der zuständigen Aufsichtsorgane gegenüber Betroffenen nachrichtendienstlicher Maßnahmen beanstandet hatte,<sup>188</sup> greift der Entwurf somit nicht auf. Zumindest nach der Gesetzesbegründung soll der BND zudem auch die Mitteilung unterlassen dürfen, dass zu einer Person keine auskunftspflichtigen Daten gespeichert sind, wenn ein Versagungsgrund nach Absatz 3 Nr. 1 oder 3 vorliegt.<sup>189</sup> In der Sache ist das die aus dem US-Recht bekannte „Glomar“-Antwort („neither confirm nor deny“), welche der BND als Reaktion auf sensible Presseanfragen bereits in leicht abgewandelter Form einsetzt.<sup>190</sup> Der Bedarf für eine solche Nichtauskunft in Petentensachen lässt sich unter Verweis auf die operative Sicherheit und die Eigensicherung des Auslandsdienstes durchaus nachvollziehen, weil sich aus systematisch eingeholten Negativauskünften der Erkenntnisstand des BND kartieren lässt. Für den Betroffenen stellte eine „Glomar“-Regelung aber eine spürbare Verschlechterung dar, die – rechtlich gesprochen – als Vertiefung des mit der Nichtauskunft einhergehenden Grundrechtseingriffs einer Verankerung im Gesetzestext und nicht nur in seiner Begründung bedarf.

An anderer Stelle wird die Kontrolle stärker, da gegenüber dem UKRat der Staatswohlvorbehalt entfällt, unter dem das BKAm bislang selbst dem BfDI gegenüber die Auskunft mit Verweis auf Staatswohlgefährdungen verweigern konnte. Dies wurzelt unter anderem im Umstand, dass der UKRat nicht der Third Party Rule unterfällt und belegt nochmals die Qualität des Kontrollgremiums für die zentrale Aufsicht über den BND und das BfV.

Rechtspolitisch erschließt sich nicht, warum das BVerfSchG-E in § 70 Abs. 3 BVerfSchG-E keine parallele Regelung zu § 102 BNDG-E vorsieht und namentlich die Ausschlussgründe ebenso erweitert. Denn die Ausforschung durch fremde Mächte bedroht den Inlandsdienst ebenso wie den BND, und auch der Prüfaufwand bei Sperrerkklärungen und In-camera-Verfahren wird künftig gleichartig ausfallen, wenn Verfahren gegen das BfV ebenfalls beim Bundesverwaltungsgericht anhängig

<sup>186</sup>Begr. zu § 102 Abs. 2 BNDG-E, BT-Drs. 21/7868, S. 518.

<sup>187</sup>BVerwG, Urt. v. 24.1.2018, 6 A 8.16, Rn. 13; NVwZ 2016, 1487 (1489); NVwZ 2018, 590 (592 f.); vgl. auch BVerwG, NVwZ 2020, 1439; BVerfG, NVwZ 2001, 185 (186); Wolff, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, VIII § 1 Rn. 27.

<sup>188</sup>EGMR (GK), Urt. v. 25.5.2021, Nr. 35252/08, Centrum för rättsvisa/Schweden, Rn. 369 ff.

<sup>189</sup>Begr. zu § 102 Abs. 3 BNDG-E, BT-Drs. 21/7868, S. 520.

<sup>190</sup> So die Standardantwort des BND auf Presseanfragen: „Der Bundesnachrichtendienst nimmt zu Angelegenheiten, die etwaige nachrichtendienstliche Erkenntnisse oder Tätigkeiten betreffen, grundsätzlich nicht öffentlich Stellung. Damit ist keine Aussage darüber getroffen, ob der Sachverhalt zutreffend ist oder nicht.“

gemacht werden sollen (vgl. unter F.II). Der Gesetzgeber sollte diesen Schritt nachholen (vgl. auch unter C.X).

## **X. Eigensicherung, Schutz von Verschlussachen (§§ 104–124)**

### **1. Einordnung und Zulässigkeit**

Die Eigensicherung ist vom Schutz des BND als Teil seiner nachrichtendienstlichen Aufgabe zu unterscheiden. Dort geht es um die Aufklärung von Bedrohungen, die sich auch gegen den Dienst richten könnten, hier um Befugnisse, mit denen er seine Einrichtungen und Bediensteten vor Ort schützt. Zwar überlappen sich diese Regime in der Praxis womöglich, rechtlich trennt sie aber die Stoß- bzw. Blickrichtung. Die Abgrenzung entscheidet zudem darüber, wie weit Daten aus der Eigensicherung für die Aufklärung umgewidmet werden dürfen (§ 123 Abs. 3 BNDG-E).

Bereits nach den Eigensicherungsbefugnissen des geltenden BNDG kann der Auslandsdienst Maßnahmen treffen, wie sie klassischerweise der Polizei zugewiesen sind. Dass der Dienst etwa Personenkontrollen auf seinem Gelände vornehmen darf, dient dem Schutz von Bediensteten, Quellen und Methoden. Eine solche Kontrolle kann ohne Gefährdung der Funktionsfähigkeit des geheimen Nachrichtenwesens nicht durch Polizeibeamte vorgenommen werden. Würde eine Person etwa beim Verlassen einer Dienststelle des BND durchsucht, weil der Verdacht besteht, dass eingestuftes Material ausgeschleust wird, könnten dieses Material und der Verratsfall an dienstfremde Kräfte geraten. Durch die Eigensicherungsbefugnisse kommen hingegen nur eigene, nach der höchsten Stufe sicherheitsüberprüfte und der Leitung des Dienstes unterstellte Bedienstete mit etwaigen Verschlussachen in Berührung.

Gerechtfertigt wird dies bislang damit, dass die Eigensicherung – anders als die nachrichtendienstliche Aufklärung – nicht im Grunde jeden Bürger treffen kann. Sie ist vielmehr räumlich auf die Dienststellen des BND beschränkt, welche Betroffene freiwillig und, bei klarer Abgrenzung und hinreichender Belehrung, in Kenntnis des dort geltenden Rechts betreten.<sup>191</sup> Auch begründet sie keine operativen Anschlussbefugnisse nach der Karlsruher Spruchpraxis: Zwar darf der Dienst insoweit Zwang ausüben, diese Befugnisse schließen aber nicht an Erkenntnisse aus der verdeckten Aufklärung an, um den nachrichtendienstlichen Auftrag gegenüber Bürgern durchzusetzen, sondern knüpfen an ein isoliertes Verhalten im Eigensicherungsbereich selbst an.<sup>192</sup> Im Interesse eines wirksamen Geheim-schutzes, der verfassungsrechtlich hoch zu gewichtenden Gütern des Staatswohls dient, und angesichts der nur einfachgesetzlichen Stellung des Trennungsgebots überzeugt die Eigensicherung deshalb als Grundkonzept.<sup>193</sup>

Der Regierungsentwurf regelt sie für den BND in einem eigenen Abschnitt und in größerer Tiefe als für das BfV. Er erweitert sie räumlich (2.) und bei den Befugnissen (3.) und baut den Schutz von Verschlussachen aus (4.).

### **2. Räumlicher Anwendungsbereich (§§ 106–108)**

Gelungen ist die räumliche Erweiterung dort, wo sie offen erfolgen soll. § 106 BNDG-E erlaubt, Örtlichkeiten außerhalb der Dienststellen des BND vorübergehend zu besonderen

<sup>191</sup>Manns, GSZ 2025, 30 (31 f.), zum Eigensicherungsrecht des BfV nach § 26b BVerfSchG.

<sup>192</sup>Zum Begriff der operativen Befugnis BVerfGE 169, 130, Rn. 231; näher C.VIII.2.

<sup>193</sup>Manns, GSZ 2025, 30 (32).

Sicherheitsbereichen zu erklären. Dies setzt grundsätzlich die vorherige Zustimmung des BKAm voraus, von der die Norm nur in Eilfällen absieht. Die Bereiche sind entsprechend zu beschildern (§ 107). Das ist die richtige Lösung, weil sie sichtbar macht, wo besondere Befugnisse gelten, und dem Bürger die Entscheidung lässt, ob er sich ihnen aussetzt.<sup>194</sup>

Weiter reicht § 108 Nr. 4 BNDG-E, der die räumlichen Grenzen der Eigensicherung ohne ein solches Verfahren verschiebt. Die Befugnisse zur Sicherung der Bediensteten und Dienststellen dürfen sich ihm zufolge auch gegen Personen richten, die sich in unmittelbarer Nähe einer Dienststelle aufhalten, wenn tatsächliche Anhaltspunkte für eine qualifiziert funktionsgefährdende Tätigkeit bestehen. Damit reicht der Eigensicherungsbereich in den öffentlichen Raum – und über Nacheile-Situationen hinaus, in denen ausschließlich solche Personen im unmittelbaren Umfeld umfasst sind, die sich einer Maßnahme innerhalb des Eigensicherungsbereichs entziehen (so vorgesehen in § 63 Abs. 6 Nr. 1 BVerfSchG-E).

Diese doch deutliche räumliche Erweiterung ist im Zusammenspiel mit den ausgebauten Eingriffsbefugnissen alles andere als unproblematisch. Sie nimmt den Diensten die eingangs genannte Rechtfertigung (vgl. unter B.X.1), wonach sich Personen freiwillig und in Kenntnis des dort geltenden Rechts in den Bereich einer Sicherheitsbehörde begeben, die sie von Gesetzes wegen nicht aufsuchen müssen.<sup>195</sup> Wer die Straße vor einer BND-Liegenschaft nutzt, tut das nicht, und er weiß nicht einmal in jedem Fall, wer in den dortigen Gebäuden residiert, zumal ihn keine entsprechende Informationspflicht trifft. Durch das Fehlen dieser Begrenzungen nähert sich das im BNDG-E skizzierte Eigensicherungsrecht zunehmend denjenigen allgemeinen Zugriffsmöglichkeiten an, die das Polizeirecht vorsieht. Damit verschärfen sich ohnehin im Schrifttum<sup>196</sup> vorhandene Vorbehalte gegenüber der nachrichtendienstlichen Eigensicherung.

Der Bedarf ist gleichwohl real, wie jüngere Versuche mutmaßlicher Ausforschungen der BND-Zentrale dokumentiert haben<sup>197</sup>: Wer Bedienstete beim Verlassen der Dienststelle fotografiert oder zu ihrer Verfolgung ansetzt, tut das von außen. In derartigen Verdachtsfällen stets die Polizei herbeizurufen, ist wenig zweckmäßig und dürfte im Falle der (naturgemäß zu erwartenden) Negativtreffer nach allgemeiner Lebenserfahrung zu einer gewissen „Abstumpfung“ im Reaktionsverhalten der Polizei führen. Eine Subsidiaritätsklausel ohne Ausnahme wäre deshalb unpraktikabel. Handhabbar bliebe sie jedoch vielleicht mit einer Ausnahme für den Fall, dass polizeiliche Hilfe nicht rechtzeitig erlangt werden kann, wie sie der Entwurf an anderer Stelle kennt (§ 119 Abs. 2). Würde § 108 Nr. 4 so gefasst, könnte dies die Rechtssicherheit erhöhen. Will der Gesetzgeber hierauf verzichten, sollte er mindestens die Erkennbarkeit der Umfeldbefugnis ausdrücklich festschreiben. § 107 S. 1 Nr. 2 erstreckt die Hinweispflicht ausdrücklich auf die unmittelbare Nähe der Dienststellen, Satz 2 nimmt aber Dienststellen aus, deren Zugehörigkeit zum BND nicht offen erkennbar ist. Der Hintergrund für das Aufrechterhalten abgetarnter Dienststellen leuchtet ohne Weiteres ein; allerdings ist jedenfalls hier ein Kippen der erweiterten Eigensicherungsbefugnisse in die Verfassungswidrigkeit zu

---

<sup>194</sup>Vgl. § 2 Abs. 2 UZwGBw.

<sup>195</sup> So schon Manns, GSZ 2025, 30 (31 f.), auf den auch die Gesetzesbegründung mit der in der Sache zutreffenden Wertung verweist: „Die Befugnisse zur Sicherung von Bediensteten und Dienststellen stehen im engen räumlichen Zusammenhang mit den Dienststellen des Bundesnachrichtendienstes und sind auf diesen engen räumlichen Zusammenhang gleichermaßen beschränkt.“ (Begr. zu Abschnitt 8 BNDG-E, BT-Drs. 21/7868, S. 521).

<sup>196</sup> Siehe etwa Poscher, Stellungnahme zu dem Gesetzentwurf der Bundesregierung zum ersten Teil der Reform des Nachrichtendienstrechts und zu dem Referentenentwurf des Bundeskanzleramts zur Änderung des BND-Gesetzes, BT-Aussch.-Drs. 20(4)324 B, 1 (22).

<sup>197</sup> Vgl. Flade, Die Spione sorgen sich um ihre Sicherheit, tagesschau.de v. 24.6.2026, <https://tagesschau.de/investigativ/wdr/spione-sicherheit-100.html>.

besorgen. Zusätzlich empfehlen wir eine Unterrichtung der örtlichen Polizei über Maßnahmen nach § 108 Nr. 4, sofern dem nicht ausnahmsweise Staatswohlgründe entgegenstehen, damit die Zuständigkeiten nicht (noch) mehr verschwimmen.

Dass Eigensicherung und nachrichtendienstliche Aufklärung zu unterscheiden sind, hält § 123 Abs. 3 Nr. 1 BNDG-E nicht davon ab, Daten aus Maßnahmen zur Sicherung der Bediensteten und Dienststellen zur Auslandsaufklärung weiterzuverarbeiten, wenn das im Einzelfall erforderlich ist (für das BfV gilt über § 36 Abs. 1 S. 2 Nr. 1 lit. a BVerfSchG-E Entsprechendes). Dass Erkenntnisse über eine Person, die vor der Dienststelle eine Straftat gegen den Dienst vorbereitet, in die Aufklärung einfließen dürfen, ist in der Sache richtig, denn wer Bedienstete ausspäht, handelt häufig für einen fremden Dienst, dessen Aufklärung wiederum dem BND unter bestimmten Umständen unterliegt. Dass die Eigensicherung hier „sperrend“ gegenüber den nachrichtendienstlichen Erhebungsmitteln wirkte, könnte kaum gewollt sein. Die mit der Umwidmung einhergehende Zweckänderung ist zudem an tatsächliche Anhaltspunkte im Einzelfall gebunden und kennzeichnungspflichtig (§ 123 Abs. 1 S. 2 BNDG-E). Eine spätere Verwendung zur Auslandsaufklärung bedarf gleichwohl einer gesondert dokumentierten Zweckprüfung, und zur Qualitätssicherung sollte die Zweckänderung an eine Entscheidung der Behördenleitung gebunden werden.

### **3. Anknüpfung, Festhalten, Durchsuchung (§§ 104, 109–111)**

Besonders eingriffsintensive Befugnisse, die den Eigensicherungskräften eröffnet werden sollen, knüpft § 104 Nr. 2 BNDG-E an „qualifiziert funktionsgefährdende Tätigkeiten“. Gemeint sind im Kern strafbares Handeln gegen Bedienstete, Dienststellen und Gegenstände des Dienstes sowie Straftaten mit unmittelbarem Bezug zu sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten. Hinzu tritt unzulässiger Drohnenbetrieb nach § 21h Abs. 3 Nr. 4 LuftVO (lit. d), der nicht notwendig eine Straftat darstellt. Damit erhalten die Durchsuchung (§ 110), der Platzverweis (§ 111 Abs. 1) und der Zugriff auf private Geräte (§ 118 Abs. 2) einen deutlich begrenzteren und „härteren“ Anknüpfungspunkt, als es für die reguläre bundesnachrichtendienstliche Aufklärungstätigkeit nach Maßgabe der vorgestellten Bedrohungsschwellen erforderlich ist. Das ist zu begrüßen.

Als Teil dieser Maßnahmen erlauben § 109 Abs. 3 und § 111 Abs. 2 BNDG-E das Festhalten von Personen zur Identitätsfeststellung und bei Gefahr im Verzug bis zur Überstellung an die Polizei. Je nach Art, Intensität und Dauer des Festhaltens kann dies eine Freiheitsentziehung darstellen (Art. 104 Abs. 2 GG). Für § 111 Abs. 2 sichert die entsprechende Anwendung der §§ 40–42 BPolG (S. 4) die nach dem Grundgesetz in solchen Fällen erforderliche richterliche Entscheidung, wohingegen für § 109 Abs. 3 eine entsprechende Verweisung offensichtlich als „rechtshandwerkliches“ Versehen nicht eingefügt wurde. Da die Maßnahmen nach § 109 Abs. 3 jedoch ihrem Wesen nach zeitlich noch enger begrenzt sind, dürfte gegen eine entsprechende Verweisungsergänzung nichts streiten.

Die Befugnisnormen zur Durchsuchung mit Sicherstellung und Beschlagnahme (§ 110) verweisen auf die §§ 96, 97 und 110 StPO. Sichergestellte Gegenstände sind danach grundsätzlich unverzüglich, spätestens binnen drei Tagen, an Polizei oder Staatsanwaltschaft zu übergeben; für Rückgabe- und Besitzkonstellationen gelten Sonderregeln. Damit entsteht eine saubere Schnittstelle zum Strafverfahren. Für den Schutz von Bediensteten bei offener Tätigkeit und für den Personenschutz besonders gefährdeter Bediensteter sollte beim BND dasselbe gelten wie beim BfV (C.IV.8). Bei der Drohnenabwehr (§ 112) sollte das Gesetz zudem klarstellen, welche Zwangsmittel zur Durchsetzung einer Sicherstellung zulässig sind. Ausgeschlossen sein sollten nur Schusswaffen (vgl. C.IX.3).

#### 4. Schutz von Verschlusssachen (§§ 115–119)

Den Schutz von Verschlusssachen regelt der Entwurf in einem eigenen Unterabschnitt. Nachdem bereits der mutmaßliche Verratsfall um Carsten L., dem das Ausschleusen von Verschlusssachen aus dem BND vorgeworfen wird,<sup>198</sup> das Bedrohungspotential durch derartige Abflüsse eindrücklich belegt hat, verdeutlichen jüngste Ermittlungen des Generalbundesanwalts wegen mutmaßlichen Geheimnisverrats durch (vormalige) BND-Angehörige<sup>199</sup> neuerlich, wie stark der Schutz von Leib und Leben der im BND eingesetzten Mitarbeiter und ihrer Quellen sowie die internationale Kooperationsfähigkeit im Verbund der westlichen Auslandsdienste von vermuteten Innentätern bedroht werden kann.

Zu begrüßen ist zunächst, dass § 115 Abs. 3 BNDG-E eine Belehrung der Personen verlangt, die sich in den Dienststellen aufhalten, und zwar nicht nur über den Umgang mit Verschlusssachen, der schon nach den Maßgaben von SÜG und VSA erfolgt, sondern auch über mögliche Kontrollen. Sie macht vorhersehbar, womit Bedienstete und Besucher rechnen müssen. Die IT-Kontrollen zur Sicherung von Verschlusssachen (§ 118) übernehmen im Ansatz jene des geltenden § 65d BNDG und unterscheiden zwischen dienstlichen, privatdienstlichen und vorschriftswidrig eingebrachten Geräten. Allerdings wird der Zugriff auf unrechtmäßig eingebrachte privatdienstliche Geräte insofern erweitert, als das Gerät bei tatsächlichen Anhaltspunkten für eine Straftat nach § 104 Nr. 2 lit. c nicht mehr nur gespiegelt und dem Betroffenen wieder ausgehändigt werden muss, der die gespeicherten Daten dann vermutlich rasch beseitigen und so eine nachträgliche Strafverfolgung behindern könnte. Vielmehr darf es für einen begrenzten Zeitraum einbehalten und gegebenenfalls an die Strafverfolgungsbehörden weitergeleitet werden (§ 118 Abs. 2 S. 2, Abs. 3 S. 3). Weiter geht das BVerfSchG-E, das die Untersuchung vorschriftswidrig eingebrachter Geräte einschließlich der gespeicherten Daten schon wegen des verbotenen Einbringens erlaubt (§ 63 Abs. 5 S. 1 Nr. 2, S. 2 BVerfSchG-E). Diese Regelung sollte das BNDG-E übernehmen. Wer sein privates Gerät trotz Hinweis und Belehrung (§§ 107, 115 Abs. 3) heimlich in die Dienststelle mitnimmt, begründet die naheliegende Besorgnis heimlicher Ton- oder Bildaufnahmen, sodass Spiegeln und Einbehalten für die Dauer der Untersuchung gerechtfertigt sind, ohne dass zusätzlich Anhaltspunkte für eine Straftat vorliegen müssten (näher C.IX.2). Dass die Auswertung eines Abbilds vorschriftswidrig eingebrachter Geräte unter den dort genannten Voraussetzungen auch Nachrichtensmittler umfasst, gegen die kein eigener Straftatverdacht bestehen muss, ist im Sinne der gefahrenabwehrenden Ausrichtung der Eigensicherung konsequent.

Am weitesten reicht die Befugnis zum Eingriff in fremde Computer und Server außerhalb der Liegenschaften und sonstigen Eigensicherungsbereiche des BND. § 119 BNDG-E erlaubt dem Dienst, in derartige informationstechnische Systeme einzugreifen, wenn der dringende Verdacht besteht, dass dort unbefugt Verschlusssachen oder sonstige geheimhaltungsbedürftige Informationen des Dienstes gespeichert sind. Kann polizeiliche Hilfe nicht rechtzeitig erlangt werden, darf er diese Informationen auch löschen. Die Gesetzesbegründung nennt als denkbare Anwendungsszenario den Fall, dass Informationen (wie Klarnamen) über Bedienstete oder Quellen auf Servern im Ausland gespeichert sind und deren Leben gefährden. Für diesen Fall ist die Befugnis einleuchtend und sind die bedrohten Schutzgüter hinreichend gewichtig – der Normwortlaut reicht aber weiter. Er erfasst

<sup>198</sup> PM des KG Berlin Nr. 28/2023 v. 30.11.2023, <https://berlin.de/gerichte/presse/pressemitteilungen-der-ordentlichen-gerichtsbarkeit/2023/pressemitteilung.1391278.php>.

<sup>199</sup> PM des GBA v. 6.10.2026, <https://generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2026/Pressemitteilung-vom-06-10-2026.html>.

jedes System, auf dem sich eine Verschlussache des Dienstes befindet, also im Grundsatz auch eine Redaktion oder einen Journalisten, dem ein Dokument zugespielt wurde (zu den Schutzbestimmungen sogleich). Die Begründung räumt das ein und verweist auf die Verhältnismäßigkeit und auf die entsprechende Anwendung des § 39 Abs. 1 S. 2, wonach eine Verantwortlichkeit des Betreibers für den Abfluss bestehen müsse. Journalisten seien deshalb regelmäßig nicht erfasst, und wo doch, sei Art. 5 Abs. 1 GG abzuwägen.<sup>200</sup> Im Normtext findet sich diese Grenze allerdings nicht.

Der Entwurf schützt die Presse vor diesem Eingriff tatsächlich auf zwei Wegen, die aber beide nicht zuverlässig greifen. Der erste ist der Schutz von Vertraulichkeitsbeziehungen: § 119 Abs. 3 erklärt § 22 für entsprechend anwendbar, und dieser § 22 wiederum verbietet Maßnahmen, die gezielt auf Informationen aus dem Vertrauensverhältnis eines Berufsgeheimnisträgers gerichtet sind. Ob die Suche nach einer Verschlussache auf einem Redaktionssystem eine solche Maßnahme ist, lässt sich aber unterschiedlich beantworten. Der Dienst sucht nicht nach dem Inhalt eines Vertrauensverhältnisses, sondern nach seinem eigenen Dokument. Für den Journalisten ist diese Unterlage dagegen gerade das, was ihm sein Informant anvertraut hat. Gesetzesbegründung und vor allem Normtext lassen offen, welche Perspektive gilt. Als zweiter, nur lose geregelter Schutzfaktor steht daneben § 119 Abs. 3. Er erklärt § 39 Abs. 1 S. 2 für entsprechend anwendbar, wonach sich ein Eingriff in fremde Systeme nur gegen Systeme verantwortlicher Personen und bestimmter Dritter richten darf. Daraus schließt die Begründung, Journalisten seien regelmäßig nicht erfasst. Nach § 39 Abs. 1 S. 2 Nr. 3 lit. a genügt aber, dass eine Person Informationen entgegennimmt, die von einem Verantwortlichen herrühren. Genau das tut der Journalist, dem ein Informant ein Dokument zugespielt hat. Für die Löschung nach Absatz 2 fehlt selbst diese Begrenzung, weil § 119 Abs. 3 nur auf den Eingriff nach Absatz 1 verweist. Dort bleibt allein der Schutz des § 22, der über § 123 Abs. 1 S. 3 für die gesamte Datenverarbeitung des Abschnitts gilt und dessen Reichweite gerade offen ist. Greift ein Nachrichtendienst in ein Redaktionssystem ein, um dort ein Dokument zu löschen, beeinträchtigt er die Pressefreiheit in einer Intensität, die das Bundesverfassungsgericht schon bei der Durchsuchung von Redaktionsräumen nur unter engsten Voraussetzungen zugelassen hat.<sup>201</sup> Eine Löschung ist potentiell irreversibel und trifft den Kern journalistischer Arbeit, die Verfügung über das Material. Die Vorabkontrolle nach § 97 Abs. 1 Nr. 17 erfasst die Maßnahme bereits, ersetzt aber keine materielle Grenze. Wir empfehlen deshalb, in Absatz 1 Systeme auszunehmen, die von Personen nach § 22 Abs. 1 S. 2 BNDG-E in dieser Eigenschaft genutzt werden, sofern nicht tatsächliche Anhaltspunkte für deren Beteiligung am unbefugten Abfluss bestehen.

## 5. Tätigkeit von Ruhestandsbeamten

Aufgrund der aktuellen Verratsfalldiskussionen im BND sollte dringend eine Anpassung von § 105 Abs. 3 BBG erfolgen. Die Anzeigepflicht nach Absatz 2 (der in Nr. 1 speziell politische Beamte und in Nr. 2 bisherige Personen mit Sicherheitsüberprüfung einbezieht) endet demzufolge fünf Jahre nach Beendigung des Beamtenverhältnisses, wenn die Beamtin oder der Beamte mit Erreichen der Regelaltersgrenze in den Ruhestand tritt, und in den übrigen Fällen sieben Jahre nach Beendigung des Beamtenverhältnisses. Die Norm sollte demgegenüber künftig wie folgt lauten:

(3) <sup>1</sup>Die Anzeigepflicht nach Absatz 2 endet

<sup>200</sup>Begr. zu § 119 Abs. 1 BNDG-E, BT-Drs. 21/7868, S. 533.

<sup>201</sup>BVerfGE 117, 244 (258 ff.) (Cicero).

*1. fünf Jahre nach Beendigung des Beamtenverhältnisses, wenn die Beamtin oder der Beamte mit Erreichen der Regelaltersgrenze in den Ruhestand tritt,*

*2. und in den übrigen Fällen sieben Jahre nach Beendigung des Beamtenverhältnisses.*

*<sup>2</sup>Die zeitliche Befristung der Anzeigepflicht gilt nicht für Personen nach Absatz 2 Nr. 2, soweit für die dort geforderte sicherheitsempfindliche Tätigkeit eine erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen nach § 10 des Sicherheitsüberprüfungsgesetzes erforderlich gewesen ist.*

Zudem sollte § 105 Abs. 6 S. 1 BBG wie folgt neugefasst werden:

*(6) <sup>1</sup>Die Erwerbstätigkeit oder sonstige Beschäftigung ist zu untersagen, soweit zu besorgen ist, dass durch sie dienstliche Interessen beeinträchtigt werden; in den Fällen des § 3 Satz 2 auch dann, wenn nicht ausgeschlossen werden kann, dass hierdurch dem Wohl des Bundes oder eines Landes oder der Funktionsfähigkeit des geheimen Nachrichtenwesens Nachteile entstehen können.*

## **C. Art. 1 – BVerfSchG-E**

Auch das Verfassungsschutzrecht des Bundes wird im Zuge der durch die Novellierungen beim Bundesnachrichtendienst angestoßenen Großreform von Grund auf neu gefasst. Es wird dadurch, wie bereits zum BNDG-E ausgeführt, zumindest für die nächste Zeit von verfassungsgerichtlich veranlassten Einfügungen befreit und auch ansonsten besser verständlich. Teils regelt das BVerfSchG-E zudem auch Gegenstände, derer es verfassungsrechtlich nicht bedurft hätte, die aber sehr zu begrüßen sind (etwa die Beobachtungsstufen). Daneben stehen Befugniserweiterungen, die wir hinsichtlich des operativen Bedarfs im Ansatz durchgehend nachvollziehen können. Größtenteils sind sie, gegebenenfalls mit den hier vorgeschlagenen Anpassungen, auch von vertretbarem Risiko hinsichtlich ihrer möglichen Verwerfung durch das Bundesverfassungsgericht. Vereinzelt überschießende Regelungen werden folgend gesondert aufgegriffen.

### **I. Aufgabe, Begriffsbestimmungen (§§ 1–3)**

#### **1. Aufgabe, Kompetenz, Trennungsklauseln (§§ 1–3)**

Die Aufgaben- und Begriffsnormen für das BfV enthalten mehrere Neuerungen, von denen drei hervorzuheben sind. Zunächst benennt § 2 Abs. 2 S. 1 Nr. 1 BVerfSchG-E die bereits bestehende Informationsfunktion, auch gegenüber der Öffentlichkeit, erstmals ausdrücklich im allgemeinen Aufgabenkatalog und verdeutlicht damit ihren Bezug zur nachrichtendienstlichen Aufklärung.<sup>202</sup> Das schafft eine klarere gesetzliche Struktur, begründet aber keine eigene Befugnis zur Informationsweitergabe; für jede Übermittlung bleiben vielmehr die Übermittlungsvorschriften mit ihren eigenen Ermächtigungen und Schwellen maßgeblich. Neu ist ferner die Legaldefinition sicherheitsgefährdender und geheimdienstlicher Tätigkeiten (§ 2 Abs. 1 Nr. 3). Die Begründung versteht sie als Erläuterung der bisher schon verwendeten Begriffe und stellt zugleich klar, dass auch Akte transnationaler Repression erfasst sind, bei denen ein fremder Staat gegenüber Regimegegnern gerade nicht verdeckt

<sup>202</sup> BT-Drs. 21/7868, S. 209 f.; zum geltenden Recht §§ 5 Abs. 2 S. 2, 16 Abs. 1, 19 ff. BVerfSchG.

auftritt (lit. a).<sup>203</sup> Diese Klarstellung ist hilfreich, weil sie eine zunehmend bedeutsame Erscheinungsform fremdstaatlicher Einflussnahme erfasst.<sup>204</sup>

Schließlich übernimmt der Entwurf in § 3 Abs. 3 die Grundsätze der freiheitlichen demokratischen Grundordnung aus dem zweiten NPD-Verfahren und ergänzt sie folgerichtig um das staatliche Gewaltmonopol.<sup>205</sup> Ob der engere Begriff aus der Rechtsprechung zum Parteiverbot die Beobachtung übermäßig verengt, ist zwar umstritten. Dafür lässt sich anführen, dass das Bundesverfassungsgericht die Reduzierung auf wenige Grundprinzipien gerade mit dem Ausnahmecharakter des Parteiverbots begründet hat und die Nachweislast sich zu Lasten der Verfassungsschutzbehörden verschieben könnte.<sup>206</sup> Die besseren Gründe sprechen aber für die Übernahme: Die Schutzgüter sind für alle Instrumente des präventiven Verfassungsschutzes dieselben, und das Bundesverwaltungsgericht greift sie auch bei Vereinsverboten auf. Das höhere Eingriffsgewicht des Parteiverbots wirkt sich nicht bei den Schutzgütern aus, sondern erst bei den Anforderungen an Erkenntnisdichte und Potentialität, die für die nachrichtendienstliche Aufklärung niedriger liegen.<sup>207</sup> Eine spürbare Verringerung der Beobachtungsobjekte ist deshalb nicht zu erwarten. Konsequenterweise haben die Gerichte die Grundprinzipien in ihrer Anwendung auf verfassungsschutzrechtliche Sachverhalte weiterhin zureichend eng verstanden – etwa wenn der ethnisch-kulturelle Volksbegriff nach verwaltungsrechtlicher Judikatur in seiner Ausprägung als Forderung rechtlicher Diskriminierung nicht nur gegen Art. 3 GG, sondern auch gegen die Menschenwürdegarantie aus Art. 1 GG gerichtet sein soll. Dass Kritik an staatlichen Zwangsbefugnissen für sich genommen keine Bestrebung gegen das Gewaltmonopol im Sinne der Judikatur des Bundesverfassungsgerichts ist, stellt das Gesetz dadurch nicht infrage.

Die Begründung stützt das BVerfSchG-E auf Art. 73 Abs. 1 Nr. 10 lit. b und c GG und für die nicht auf die Bund-Länder-Zusammenarbeit bezogenen Aufgaben des BfV auf die Natur der Sache.<sup>208</sup> Dabei sind Gesetzgebungs- und Verwaltungskompetenz zu trennen. Art. 87 Abs. 1 S. 2 GG trägt die Einrichtung des BfV als Zentralstelle, aber nicht schon jede Befugnis dieser Stelle (näher dazu unter C.VIII.3). In welchem Umfang Art. 73 Abs. 1 Nr. 10 lit. b und c GG neben der Zusammenarbeit auch Aufgaben und Befugnisse des BfV trägt und wo eine ungeschriebene Bundeskompetenz benötigt wird, bedarf einer gegenstandsbezogenen Begründung. Zumindest aus „rechtshandwerklicher“ Sicht sollte die Bundesregierung im weiteren Verfahren die Kompetenzgrundlagen deshalb getrennt für die einzelnen Aufgaben und Befugnisgruppen darlegen und die Berufung auf die Natur der Sache nur dort beibehalten, wo sie eigenständig begründet wird.<sup>209</sup> (Für die materiellen Problemfelder in der Kompetenzzuweisung, also für die Eigensicherung und insbesondere für die Schutzmaßnahmen, vgl. hierzu unter C.VIII.3 und C.IX.1.) Eine Ergänzung ist auch in den Aufgabennormen für das BfV selbst nötig: So erstreckt § 2 Abs. 1 Nr. 2 lit. c BVerfSchG-E die Aufgabe auf Bestrebungen gegen die Sicherheit der Europäischen Union, der NATO und anderer internationaler

<sup>203</sup> Begr. zu § 2 Abs. 1 Nr. 3 BVerfSchG-E, BT-Drs. 21/7868, S. 210.

<sup>204</sup> Weiterführend Pawlowsky/Evans/Manns, GSZ 2025, 107.

<sup>205</sup> BVerfGE 144, 20, Rn. 535 ff., zum Gewaltmonopol und zur gewaltsamen Durchsetzung politischer Ziele dort Rn. 547.

<sup>206</sup> Stellungnahme des Bundesrates, BT-Drs. 21/8295, S. 2 f., unter Hinweis auf BVerfGE 144, 20, Rn. 535.

<sup>207</sup> Gegenäußerung der Bundesregierung, BT-Drs. 21/8295, S. 12, unter Hinweis auf BVerfGE 144, 20, Rn. 535, und BVerwG, Urt. v. 24.6.2025, 6 A 4.24, Rn. 72.

<sup>208</sup> Begr. A.V, BT-Drs. 21/7868, S. 203.

<sup>209</sup> Zu Art. 73 Abs. 1 Nr. 10 lit. b und c GG als Zusammenarbeitskompetenz und Art. 87 Abs. 1 S. 2 GG als Verwaltungskompetenz für das BfV als Zentralstelle Dietrich, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, III § 3 Rn. 59.

Organisationen. Art. 73 Abs. 1 Nr. 10 lit. b GG benennt diese Schutzgüter jedoch nicht. Vermutlich ließe sich die Bündnisfähigkeit als Element der Sicherheit des Bundes begreifen (vgl. § 2 Abs. 2 Nr. 2 BNDG-E).

Durch die Novelle tritt eine ausdrückliche Normierung der Aufklärungspflichten des BfV hinzu: Nach § 2 Abs. 3 S. 1 BVerfSchG-E muss der Inlandsdienst entsprechend der bisherigen Rechtslage<sup>210</sup> aufklärend tätig werden, sobald tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten in seinem Aufgabenfeld vorliegen. Erstmals wird dabei auch das Ermessen geregelt. Es verbleibt nach Satz 2 nur bei Bestrebungen und Tätigkeiten gegen die Sicherheit der Europäischen Union, der NATO und anderer internationaler Organisationen (Nr. 1), bei Bestrebungen von Einzelpersonen (Nr. 2) und bei Angehörigen des Geschäftsbereichs des Bundesministeriums der Verteidigung, für die der MAD zuständig ist (Nr. 3). In letzterem Fall ist die Aufklärung nur im Benehmen mit dem MAD zulässig (Satz 3). Dient die Aufklärung überragenden Gemeinwohlinteressen, ist eine solche Pflicht folgerichtig und die Ausnahmen erweisen sich zugleich als tauglich, weil im internationalen Bereich oder, soweit es andere Ressortbereiche in der Bundesregierung betrifft, besonders viele politische Erwägungen zu beachten sind, die eine Beobachtung ausnahmsweise untunlich machen können. Der Gesetzgeber sollte aber anlässlich der ausdrücklichen Regelung klarstellen, dass § 2 Abs. 3 kein subjektives Recht vermittelt, so wie es auch das bisherige Verfassungsschutzrecht nicht tut. Kompetenzrechtlich ist zudem offen, ob die Zusammenfassungen den Ausschluss des Entschließungsermessens auch der Landesbehörden trägt, die § 2 Abs. 3 S. 1 ebenfalls entsprechend verpflichtet.<sup>211</sup>

Eine eigene Aufgabe zur Beobachtung der organisierten Kriminalität sieht der Entwurf nicht vor. Strukturen der organisierten Kriminalität, die für eine fremde Macht handeln oder von ihr genutzt werden, erfasst § 2 Abs. 1 Nr. 3 aber bereits über die geheimdienstliche Tätigkeit für eine fremde Macht. Das sollte der Gesetzgeber klarstellen und dabei festhalten, dass das BfV solche Strukturen bei tatsächlichen Anhaltspunkten für ihre Nutzung daraufhin prüfen darf. Eine darüber hinausgehende Aufgabe würde die Abgrenzung zur Polizei erschweren. Unvertretbar erschiene aber auch sie nicht. Organisierte Kriminalität kann staatliche Institutionen systematisch unterwandern und selbst Regierungen bedrohen, wie Italien und zuletzt die Niederlande zeigen, und mehrere Länder weisen ihren Verfassungsschutzbehörden eine solche Aufgabe schon heute zu.<sup>212</sup>

## 2. Eingriffsschwellen (§ 3 Abs. 4–10)

Zur Grundentscheidung für eine gestufte Schwellendogmatik gilt das zum BNDG-E Gesagte (B.I.2), wonach das Modell ausdrücklich zu begrüßen ist. Für das BfV sieht der Regierungsentwurf konkret neben einer (Grund-)„Bedrohung“ (§ 3 Abs. 4 BVerfSchG-E) die wie im BNDG-E als „erhebliche Bedrohung“ bezeichnete erste Steigerungsstufe (Abs. 7) und die „besonders erheblich beobachtungsbedürftige Bedrohung“ als Spitzenstufe (Abs. 8) vor. Hinzu treten, ebenfalls wie im BNDG-E, die konkretisierte und die dringende Gefahr (§ 3 Abs. 10, § 27 Abs. 1 Nr. 1 BVerfSchG-E). Rechtspolitisch empfehlen wir, auch die Spitzenstufen beider Gesetze gleichlautend zu bezeichnen, wie es bei der „erheblichen Bedrohung“ bereits gelungen ist (vgl. Anlage Nr. 3).

<sup>210</sup> Warg, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, V § 4 Rn. 11, 13.

<sup>211</sup> Zu den Grenzen funktionaler Mischverwaltung vgl. BVerfGE 119, 331. Zur Reichweite des Art. 73 Abs. 1 Nr. 10 lit. b und c GG für Befugnisse des BfV vgl. BVerfGE 155, 119 (174); 163, 43 (79); dazu Wissenschaftliche Dienste des Deutschen Bundestages, WD 3 - 3000 - 056/26 v. 6.7.2026, S. 16 f.

<sup>212</sup> Vgl. Art. 3 S. 2 BayVSG; § 2 Abs. 2 Nr. 5 HVSG; § 2 SächsVSG.

Gewisse, wenngleich nicht durchgreifende Zweifel begründet dagegen die inhaltliche Ausformung der „erheblichen Bedrohung“. Nach § 3 Abs. 7 S. 2 BVerfSchG-E „ist“ die Eignung einer Bestrebung zur erheblichen Beeinträchtigung anzunehmen, wenn sie zur Zielverfolgung Straftaten begeht. Die Zuordnung ist nicht widerleglich und erfasst nach ihrem Wortlaut auch geringfügige Delikte. Für sie spricht zwar, dass die Straftaten der Zielverfolgung dienen müssen. Dieser Zusammenhang grenzt den Tatbestand ein und unterscheidet solche Bestrebungen aussagekräftig von legalistisch agierenden. Das Bundesverfassungsgericht hat aber eine Regelung beanstandet, die Bestrebungen normativ als erheblich beobachtungsbedürftig einstufte, ohne ihre tatsächliche Potentialität im Einzelfall zu prüfen. Die Anknüpfung an Straftaten hat es nur als Anhaltspunkt einer gewissen Potentialität gebilligt und ein engeres Verständnis über Regelbeispiele verlangt.<sup>213</sup> Dass Satz 1 weiterhin tatsächliche Anhaltspunkte einer Bedrohung verlangt und jede Maßnahme eigens verhältnismäßig sein muss, beseitigt die Fiktion nicht. Sie ist deshalb verfassungsrechtlich riskant. Zumindest rechtspolitisch empfehlen wir eine widerlegliche, auf eine Gesamtbetrachtung gerichtete Fassung, etwa: „Bei der Beurteilung der Eignung ist insbesondere zu berücksichtigen, ob zur Zielverfolgung Straftaten begangen werden.“ In diese Gesamtbetrachtung gehören Gewicht, Häufigkeit und Zurechenbarkeit der Straftaten.

Nach Satz 3 kann sich die Eignung auch aus der Vorgehensweise, dem Aktionspotenzial oder dem Umfang gesellschaftlicher Einflussnahme ergeben. Bei gewaltorientiertem, zu Hass anstachelndem, kämpferisch-aggressivem und „planmäßig verschleiern dem“ Vorgehen (Satz 3 Nr. 1 lit. a–d) ist sie nach Satz 4 in der Regel anzunehmen.<sup>214</sup> Damit wird die erste Steigerungsstufe faktisch zum Regelfall. Observationen (§ 20 Abs. 1), längerfristige Quelleneinsätze (§ 18 Abs. 2), Standortfeststellungen (§ 21 Abs. 1 Nr. 1), das Auslesen von Geräten (§ 23 Abs. 1) und abgegrenzte Eingriffe in private informationstechnische Systeme (§ 26 Abs. 1) sind gegenüber fast jeder Bestrebung möglich, die nicht als unvernetzte Einzelperson legalistisch agiert. Mit Ausnahme der Quelleneinsätze und des Auslesens nach § 23 Abs. 2 und 3 unterliegen diese Maßnahmen keiner Vorabkontrolle (§ 34 Abs. 1, insbesondere Nr. 7 BVerfSchG-E), sodass regelmäßig der Dienst allein entscheidet, ob die Einordnung trägt. Für die Regelung spricht allerdings, dass die Vermutung widerleglich ist und sich auch legalistisch, aber abgeschottet agierende Bestrebungen ohne verdeckte Mittel oft nicht aufklären lassen. Zudem fordert die Rechtsprechung den Einsatz nachrichtendienstlicher Mittel mitunter implizit ein, so in der Eilentscheidung des Verwaltungsgerichts Köln zur Einstufung der „Alternative für Deutschland“ als „gesichert rechtsextremistisch“,<sup>215</sup> die schon wegen ihres gesellschaftlichen Einflusspotenzials als erheblich beobachtungsbedürftig gelten dürfte. Gegen die Regelvermutung für das planmäßig verschleiern Vorgehen spricht aber, dass Konspiration jeder Beobachtungsklientel eigen ist, die sich einer Beobachtung entziehen will, und dass das Bundesverfassungsgericht das Maß der Abschottung nur als einen Gesichtspunkt neben anderen anerkannt hat.<sup>216</sup> Verfassungsrechtlich stabiler wäre es deshalb, die Regelvermutung auf lit. a–c zu beschränken und Verschleierung nur zusammen mit einem weiteren Merkmal genügen zu lassen. Der Gesetzgeber sollte

<sup>213</sup> BVerfGE 169, 130, Rn. 151 f. (Beanstandung der automatischen Einstufung), Rn. 153 f. (Straftaten als Anhaltspunkt), Rn. 244 und Tenor Nr. 3 lit. b (Regelbeispiele); im Ergebnis ebenso Gesellschaft für Freiheitsrechte, Stellungnahme v. 14.7.2026 (Fn. oben).

<sup>214</sup> Kritisch zur Trennschärfe des Merkmals der planmäßigen Verschleierung Höning, VerfBlog v. 14.8.2026 (Fn. oben). Die Bundesregierung sieht in der Stufung gegenüber den bisherigen Voraussetzungen des G 10 keine praxisrelevanten Einschränkungen, BT-Drs. 21/8295, S. 12.

<sup>215</sup> Vgl. Ogorek, Mit Geheimplänen ist nicht zu rechnen, F.A.Z. v. 9.4.2026, S. 12.

<sup>216</sup> BVerfGE 162, 1, Rn. 196.

zudem klarstellen, dass bloße Verschlossenheit ohne Anhaltspunkte für Aktionspotenzial oder gesellschaftliche Einflussnahme die Vermutung nicht auslöst.

Der Spitzenstufe der „besonders erheblich beobachtungsbedürftigen Bedrohung“ ordnet der Entwurf alle Straftaten mit einer Höchststrafe von mindestens fünf Jahren (§ 3 Abs. 8 Nr. 1 lit. a BVerfSchG-E), die Fortführung verbotener Vereine (lit. b) und geheimdienstliche Tätigkeiten (Nr. 2) zu. Er knüpft damit an Wertungen des G 10 an, setzt sie aber nicht einfach fort. § 3 Abs. 1 G 10 kombiniert einen bestimmten Straftatenkatalog mit einer gesonderten Vereinigungsalternative, § 3 Abs. 8 Nr. 1 lit. a BVerfSchG-E arbeitet dagegen mit einer abstrakten Strafrahmengrenze. Gegen diese Neuordnung lässt sich einwenden, dass sie das System wechselt. Zudem wird kritisiert, Ersatzorganisationen verbotener Vereine würden pauschal der Spitzenstufe zugeschlagen.<sup>217</sup> Beide Einwände überzeugen als solche nicht. Lit. b setzt die erhebliche Beobachtungsbedürftigkeit des verbotenen Vereins voraus. Und dass das Gesetz mit einer Strafrahmengrenze arbeitet, ist im Ansatz tragfähig, weil sie das Gewicht der zur Zielverfolgung begangenen Taten an einem objektiven Maßstab festmacht. Ob die gewählte Höhe genügt, ist allerdings eine eigene Frage (dazu sogleich). Sie betrifft zudem allein die Datenerhebung und ist von den strengeren Anforderungen an die Übermittlung zur Strafverfolgung zu unterscheiden.

Kritischer ist die pauschale Anknüpfung an alle Straftaten mit einem Höchstmaß von mindestens fünf Jahren. Das Bundesverfassungsgericht versteht als besonders schwere Straftaten im Grundsatz Delikte mit einer Höchststrafe von mehr als fünf Jahren, was in der Systematik des StGB regelmäßig eine Höchststrafe von zehn Jahren bedeutet.<sup>218</sup> Ob es diese Schwelle auch für die Spitzenstufe nachrichtendienstlicher Befugnisse verlangen würde, ist nicht ausgemacht. Eine Straftatanknüpfung unterhalb dieser Schwelle ist aber mit verfassungsrechtlichen Unwägbarkeiten verbunden.<sup>219</sup> Ausgeschlossen ist ein niedrigerer Strafrahmen zwar nicht, weil ihm nur eine, wenn auch maßgebende, Indizwirkung zukommt.<sup>220</sup> Er genügt aber nur, wenn neben dem geschützten Rechtsgut auch Tatbegehung und Tatfolgen eine Gleichwertigkeit mit den schweren Straftaten begründen und der Tatbestand diese Umstände selbst objektiviert.<sup>221</sup> Die mit höchstens fünf Jahren bedrohten Delikte des StGB gehören dagegen häufig nur zum mittleren Kriminalitätsbereich<sup>222</sup>. Zumindest rechtspolitisch empfehlen wir deshalb, die Grenze in § 3 Abs. 8 Nr. 1 lit. a auf eine Höchststrafe von mehr als fünf Jahren anzuheben. Delikte mit geringerem Strafrahmen sollten nur erfasst werden, wenn ihr Tatbestand besondere Begehungsformen oder Tatfolgen objektiviert (vgl. B.VIII.1).

Neu ist die Zuordnung funktionsgefährdender Tätigkeiten zur Spitzenstufe (§ 3 Abs. 8 Nr. 3 BVerfSchG-E). Erfasst sind Tätigkeiten gegenwärtiger oder ehemaliger Bediensteter, verdeckter Hilfspersonen, mit sicherheitsempfindlichen Tätigkeiten beauftragter Personen und Zugangsberechtigter (lit. a), Tätigkeiten durch unerlaubten Zugriff auf die informationstechnischen Systeme des BfV (lit. b) und funktionsgefährdende Tätigkeiten, bei denen zur Zielverfolgung Straftaten begangen werden, die im Höchstmaß mit mindestens fünf Jahren Freiheitsstrafe bedroht sind (lit. c). Das geltende Recht erlaubt den Einsatz besonderer Mittel gegen eigene Beschäftigte und Beauftragte nur zur

<sup>217</sup> Gesellschaft für Freiheitsrechte, Stellungnahme v. 14.7.2026 (Fn. oben).

<sup>218</sup> BVerfGE 169, 130, Rn. 203.

<sup>219</sup> Vgl. *Kluckert*, in: Epping/Hillgruber, BeckOK GG, 62. Ed. 15.6.2025, Art. 13 Rn. 15a; *Papier*, in: Dürig/Herzog/Scholz, Grundgesetz, 106. EL Oktober 2024, Art. 13 Rn. 71.

<sup>220</sup> *Löffelmann/Zöller*, Nachrichtendienstrecht, 2. Aufl. 2025, S. 267, Rn. 48.

<sup>221</sup> BVerfGE 169, 130, Rn. 205.

<sup>222</sup> Zum Kriterium bereits BVerfGE 109, 279 (347 f.).

Aufklärung sicherheitsgefährdender Tätigkeiten.<sup>223</sup> Für die Zuordnung spricht zunächst die besondere Gefährlichkeit von Innentätern. Wer für den Dienst arbeitet oder Zugang zu ihm hat, kennt Quellen, Methoden und laufende Operationen. Er kann sie mit geringem Aufwand und oft lange unentdeckt preisgeben und richtet damit Schäden an, die sich kaum rückgängig machen lassen. Gerade Vorbereitungshandlungen wie das unauffällige Sammeln von Material sind dabei häufig noch nicht strafbar. Angriffe auf die Systeme des Dienstes wiederum zielen auf seinen Kern.<sup>224</sup> Lit. b und c sind deshalb gut begründet. Bei lit. a ergeben sich dagegen aus den Folgeeingriffen verfassungsrechtliche Bedenken, die sich aber durch eine Anbindung an strafbares Verhalten ausräumen lassen. Die Zuordnung zur Spitzenstufe öffnet die schwersten nachrichtendienstlichen Mittel, namentlich die Telekommunikationsüberwachung (§ 22 Abs. 1). Zugleich knüpft sie an einen denkbar weiten Grundbegriff an. Funktionsgefährdend ist nämlich jede Tätigkeit, die geeignet ist, die ordnungsgemäße Aufgabenwahrnehmung zu beeinträchtigen (§ 2 Abs. 4). Wo ein Innentäter Dienstgeheimnisse verletzt, greift schon lit. c, weil § 353b Abs. 1 StGB Freiheitsstrafe bis zu fünf Jahren androht. Eigenständige Bedeutung hat lit. a daher gerade unterhalb der Strafbarkeit. Schon nicht strafbares Verhalten eines Bediensteten würde damit die schwersten Eingriffe eröffnen. Das verträgt sich schlecht mit der Abstufung nach dem Gewicht der Bedrohung, die das Bundesverfassungsgericht für nachrichtendienstliche Befugnisse verlangt. Es widerspricht zudem der Linie, die der Entwurf an anderer Stelle selbst verfolgt. Das geltende BNDG bindet den Eingriff in Geräte von Mitarbeitern an den Verdacht bestimmter Straftaten (§ 65d Abs. 2 BNDG), der Entwurf die eingriffsintensiven Eigensicherungsbefugnisse an strafbares Handeln (§ 104 Nr. 2 BNDG-E). Wir empfehlen deshalb, lit. a auf Fälle zu beschränken, in denen tatsächliche Anhaltspunkte für eine Straftat bestehen. Daneben kann ein abschließender Katalog nicht strafbarer Handlungen treten, die typischerweise einen Geheimnisverrat vorbereiten, etwa das unbefugte Kopieren oder Ausleiten von Verschlusssachen, sofern er deutlich enger bleibt als der Begriff der Funktionsgefährdung.

Der Entwurf definiert zudem mehrere Begriffe, die das Bundesverfassungsgericht geprägt hat. Zwei dieser Definitionen sollten überdacht werden. § 3 Abs. 9 Nr. 4 BVerfSchG-E erweitert den Katalog der besonders gewichtigen Rechtsgüter um die sexuelle Selbstbestimmung und um „vergleichbar besonders gewichtige Rechtsgüter einer Person“. Die Begründung nennt als Beispiele Gesundheit und Kindeswohl.<sup>225</sup> Die Öffnungsklausel sollte gestrichen werden. Sie ist nach unserer Auffassung verfassungsrechtlich bedenklich und auch unnötig, weil die Beispiele der Begründung bereits vom Schutz der „körperlichen Unversehrtheit“ umfasst sind. § 3 Abs. 10 BVerfSchG-E definiert ferner die konkretisierte Gefahr im Anschluss an das Bundesverfassungsgericht, dessen Definition den Nachweisgrad bereits enthält, nämlich tatsächliche Anhaltspunkte für das Entstehen einer konkreten Gefahr.<sup>226</sup> Wenn § 37 Abs. 3 Nr. 1 BNDG-E darüber hinaus „bestimmte Tatsachen“ verlangt, die die Annahme einer „zumindest konkretisierten Gefahr“ rechtfertigen, legt er eine gegenüber der Rechtsprechung veränderte Hürde nahe. Im Interesse der Normenklarheit empfehlen wir die einheitliche Formel „im Falle einer konkretisierten Gefahr“.

<sup>223</sup> § 26b Abs. 8 BVerfSchG (geltende Fassung).

<sup>224</sup> Begr. zu § 3 Abs. 8 Nr. 3 BVerfSchG-E, BT-Drs. 21/7868, S. 219.

<sup>225</sup> Begr. zu § 3 Abs. 9 Nr. 4 BVerfSchG-E, BT-Drs. 21/7868, S. 220.

<sup>226</sup> BVerfGE 141, 220, Rn. 112; 162, 1, Rn. 158.

## II. Beobachtungsobjekt-Regime (§ 4): Prüffall, Verdachtsfall, gesicherte Bestrebung

### 1. Kodifikation und Einstufungsvorbehalt

Im Mittelpunkt dieses Abschnitts steht die Einstufung der Beobachtungsobjekte. § 4 Abs. 2–4 BVerfSchG-E kodifiziert das Stufenmodell aus Prüffall, Verdachtsfall und gesicherter Bestrebung entsprechend jenen Bezeichnungen, die die Verwaltungsgerichte in den gegen Parteien gerichteten Verfahren zum Maßstab gemacht haben.<sup>227</sup> Das ist zu begrüßen, denn von der Einstufung hängt etwa ab, ob das BfV die Öffentlichkeit informieren darf (§ 45) und wie lange eine Beobachtung zumutbar ist. Eine so folgenreiche Kategorisierung gehört in das Gesetz, wie es nun erfolgt. Aus gleichem Grund ist es richtig, dass ihre Anordnung der Amtsleitung vorbehalten bleibt (§ 4 Abs. 2 S. 2).

Für den Prüffall schließt der Entwurf den Einsatz nachrichtendienstlicher Mittel aus und bildet damit die heutige Praxis ab. Aus allgemein zugänglichen Quellen darf das BfV zwar auch verdeckt erheben, dabei aber kein schutzwürdiges Vertrauen in Anspruch nehmen (§ 4 Abs. 4 S. 2 und 3), was überzeugt. Neu ist die Befristung: So soll die Prüfung zwei Jahre nicht überschreiten, kann durch die Amtsleitung aber um jeweils höchstens zwei Jahre verlängert werden (S. 4 und 5). Dass eine Obergrenze fehlt, halten wir für vertretbar, dient der Prüffall doch der Klärung, ob überhaupt eine Bestrebung vorliegt, was sich gerade in größeren und dynamischen Vereinigungen über die Zeit verändern mag. Zudem begrenzt der Ausschluss nachrichtendienstlicher Mittel den Eingriff ohnehin stark. Es fehlt aber eine Zweckbindung, wie sie heute bereits gelebt wird: Das Gesetz sollte daher klarstellen, dass Daten aus dem Prüffall nur für die Prüfung verwendet werden dürfen und zu löschen sind, wenn die Einstufung ausbleibt (d.h. Anlegung gesonderter Prüffallakten). Darüber hinaus sollte angeordnet werden, dass die Verlängerung schriftlich begründet werden muss.

### 2. Fristenregime, Ministervorbehalt (Abs. 3)

Auch für den Verdachtsfall führt der Entwurf feste Fristen ein: Er ist nach spätestens drei Jahren zu überprüfen und in der Regel aufzuheben, wenn die Bestrebung nicht nach spätestens fünf Jahren als gesichert verfassungsfeindlich bewertet ist (§ 4 Abs. 3 S. 1–3 BVerfSchG-E). Damit wird die Verhältnismäßigkeit der Beobachtungsdauer praxistauglich umgesetzt,<sup>228</sup> die bereits heute – wenn gleich zeitlich unbestimmt – durch die Rechtswissenschaften aus dem Verhältnismäßigkeitsgebot abgeleitet wurde.

Nicht überzeugend ist dagegen, dass die Beobachtung über fünf Jahre hinaus mit Zustimmung des Bundesministeriums des Innern (BMI) fortgeführt werden kann (S. 4). Sie ist zwar insofern regelungstechnisch logisch angelegt, als der dem Behördenleiter übergeordnete Minister die gegenüber der durch Ersteren anzuordnenden Prüffallbearbeitung schwerwiegendere Verdachtsfalleinstufung verantworten würde. Die Begründung sieht darin zu Recht eine parlamentsverantwortliche Verfahrenssicherung.<sup>229</sup> Ihre Logik geht aber an der politischen Realität vorbei, in der Verlängerungen von Verdachtsfällen wie bereits angesprochen typischerweise Parteien, Parteiflügel und bundesweite Vereinigungen betreffen, die besonders im Blickfeld der medialen Aufmerksamkeit stehen. Dass über ihre weitere Beobachtung ein Mitglied der Bundesregierung entscheidet, das mit der

<sup>227</sup> VG Köln, Urt. v. 8.3.2022, 13 K 326/21, BeckRS 2022, 3817; OVG Münster, Urt. v. 13.5.2024, 5 A 1218/22, NVwZ-Beilage 2024, 94; 5 A 1216/22, BeckRS 2024, 10025. Zur Unterscheidung von Verdachtsfall und Prüffall im geltenden Recht Warg, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, V § 1 Rn. 19.

<sup>228</sup> Vgl. BVerfGE 162, 1, Rn. 220 zum Gewicht, das Überwachungsmaßnahmen mit ihrer Dauer gewinnen.

<sup>229</sup> Begr. zu § 4 Abs. 3 BVerfSchG-E, BT-Drs. 21/7868, S. 221.

beobachteten Partei in einem faktischen politischen Wettbewerb steht, könnte somit leicht als Kampagnenargument gegen die Sachentscheidung verwendet werden. Untersagen könnte das Ministerium die Fortführung der Beobachtung zwar schon kraft Fachaufsicht – neu ist aber, dass seine Zustimmung zur Voraussetzung wird. Politisch klüger wäre daher, die Fortführung der Einstufung an eine Feststellung des UKRats zu binden, dass der Verdachtsfallnachweisgrad weiterhin vorliegt und es sich um eine Bestrebung handelt, die aufgrund ihrer inneren Veränderungen über die Regelfrist hinaus zu beobachten ist. Hält der Gesetzgeber an der ministeriellen Entscheidung fest, sollte dessen Zustimmung jedenfalls schriftlich begründet und dem PKGr unverzüglich mitgeteilt werden.

### 3. Rechtsschutz (Art. 15, § 50 Abs. 1 Nr. 2a VwGO)

Neu geordnet wird ferner der Rechtsschutz gegen die Einstufung. Art. 15 des Entwurfs weist Klagen gegen die Einstufung (§ 4 Abs. 2 BVerfSchG-E) und gegen die gesondert zu prüfende Information der Öffentlichkeit hierüber (§ 45 BVerfSchG-E) dem Bundesverwaltungsgericht im ersten und letzten Rechtszug zu (§ 50 Abs. 1 Nr. 2a VwGO-E). Dafür sprechen bundesweit einheitliche Maßstäbe, die Einheit von Hauptsache und (oftmals zu erwartendem) In-camera-Verfahren nach § 99 Abs. 2 VwGO sowie die bislang überlange Dauer zweier Tatsacheninstanzen bei Aktenbeständen im fünfstelligen Seitenbereich.<sup>230</sup> Dagegen streitet indes eben jener Verlust einer Tatsacheninstanz. Er ist aber hinnehmbar, wenn das Bundesverwaltungsgericht die Einstufung vollständig überprüft, was der Gesetzgeber klarstellen sollte. Den Einwand, das Leipziger Bundesgericht werde damit weiter von seiner primären Aufgabe als Revisionsgericht entfernt,<sup>231</sup> erachten wir zwar als nachvollziehbar, halten ihn aber nicht für durchgreifend. Der Gesetzgeber hat dem Gericht in (zu?) vielen Bereichen, etwa im Planungsrecht, erstinstanzliche Zuständigkeiten allein aus Gründen der Beschleunigung zugewiesen. Für Verfahren über besonders eingriffsintensive Maßnahmen der Nachrichtendienste des Bundes, in denen regelmäßig Verschlussachen eine Rolle spielen, liegt eine solche Zuweisung im Vergleich deutlich näher, zumal das Gericht über Sperrerkklärungen oberster Bundesbehörden in diesen Verfahren wie dargestellt ohnehin entscheidet (§ 99 Abs. 2 VwGO).

Regelungsbedürftig bleibt die Klageart. Ob eine Einstufung bekanntgegeben wird, ob sie rechtliche Außenwirkung hat und wie man gegen sie vorgehen kann, sind unterschiedliche Fragen, die der Entwurf noch offenlässt. Das Gesetz sollte zudem selbst bestimmen, ob Anfechtungs-, Feststellungs- oder Unterlassungsklage statthaft ist.<sup>232</sup>

### III. Datenerhebung unter Mitwirkung Dritter (§§ 8–15)

Wie der BND (vgl. unter B.I.4) erhält auch das BfV deutlich breitere Informationszugänge, die einen wesentlichen Teil der Novelle des Verfassungsschutzrechts darstellen. Inländische öffentliche Stellen müssen ihm auf Ersuchen vorliegende Informationen übermitteln, soweit keine besonderen Übermittlungsregeln entgegenstehen (§ 10 Abs. 1). Zudem darf das BfV amtliche Register einsehen, verdeckte Ausschreibungen im polizeilichen Informationsverbund veranlassen (§ 10 Abs. 2 und 3) und Videoüberwachungsanlagen mitbenutzen (§ 15). Für diese Zugänge gilt das zum BNDG-E mit

<sup>230</sup>Ebenso Schwarz, Zwischen effektivem Rechtsschutz und Verfahrenseffizienz, VerBlog v. 26.8.2026, <https://verfassungsblog.de/verfassungsschutz-einstufung-bverwg>; kritischer hingegen Kraft, Von der Revisions- zur Tatsacheninstanz, VerBlog v. 2.9.2026, <https://verfassungsblog.de/bverwg-tatsacheninstanz-verfassungsschutz>, der die Grenzen aus Art. 92, 95 Abs. 1 und Art. 101 Abs. 1 S. 2 GG überschritten sieht.

<sup>231</sup>Kraft, VerBlog v. 2.9.2026 (Fn. oben).

<sup>232</sup>Zu den Rechtsschutzformen bei nachrichtendienstlichen Realakten weiterführend Wöckel, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, VII § 3; zur bisherigen verwaltungsgerichtlichen Behandlung vgl. VG Köln, Urt. v. 8.3.2022, 13 K 326/21.

seinem Inlandsbezug Gesagte entsprechend, einschließlich der Bewertung der damit verbundenen Zweckänderungen (B.I.4). Ausschreibungen und Videomitbenutzung sind konsequenterweise hier wie da an eine wenigstens erheblich beobachtungsbedürftige Bedrohung gebunden (§ 10 Abs. 3, § 15 Abs. 2). Eine engere Führung des BfV gegenüber dem BND ist insoweit nicht angezeigt. Die §§ 11–15 BVerfSchG-E führen zudem die bislang verstreuten Auskunftsbefugnisse zusammen und erweitern sie, insbesondere um Auskünfte von Kraftfahrzeugherstellern und -werkstätten zu Telemetriedaten (§ 11 Abs. 1 Nr. 2) und um alle Dienste des Güter- und Personenverkehrs (§ 11 Abs. 1 Nr. 1 lit. a). Das sind zeitgemäße und passgenaue Erhebungsmethoden: Wer eine Reiseroute nachvollziehen will, muss etwa nicht mehr den Umweg über eine verdeckte Kontrolle im Schengener Informationssystem gehen. Qualifizierte Auskünfte setzen eine wenigstens erheblich beobachtungsbedürftige Bedrohung voraus (§ 11 Abs. 5, § 13 Abs. 3). Bei Telekommunikations- und Postdiensten unterliegen sie zudem ebenso wie Systemkopien der Vorabkontrolle (§ 34 Abs. 1 Nr. 6 lit. a, Nr. 8).

Zwei Punkte sind aber analog zum BNDG-E nachzuschärfen: Erstens erstreckt sich die qualifizierte Auskunft ausdrücklich auch auf Inhalte von Nutzungen (§ 11 Abs. 3 Nr. 2 lit. b), also auch auf gespeicherte private Nachrichten in sozialen Netzwerken und Messengerdiensten. Dafür genügt die erhebliche Beobachtungsbedürftigkeit. Für Inhalte interpersoneller Telekommunikation verlangt das Gesetz sonst eine besonders erhebliche Beobachtungsbedürftigkeit und Subsidiarität (§ 13 Abs. 4, § 22 Abs. 1). Die Schwelle liegt hier aus den unter B.I.4 genannten Gründen eine Stufe zu niedrig und sollte auf die besonders erhebliche Beobachtungsbedürftigkeit angehoben werden. Gleiches gilt für Telemetrie- und Standortdaten über längere Zeiträume, gemessen an der technischen Bewegungsüberwachung (§ 21). Zweitens sollte die Vorabkontrolle auch beim BfV auf qualifizierte Auskünfte erstreckt werden, die künftig anfallende Daten erfassen oder Finanz-, Bewegungs- oder Nutzungsdaten betreffen. Soweit die Auskunftspflichten Anbieter elektronischer Kommunikationsdienste treffen, gilt für die unionsrechtlichen Anforderungen ebenfalls das zum BNDG-E Gesagte (vgl. B.I.4).

Nicht geregelt ist, ob Hersteller und Dienstleister auch Informationen und Mittel herausgeben müssen, die zur verdeckten Überwindung von Schließ-, Sicherungs- und Alarmsystemen eines Fahrzeugs erforderlich sind. § 11 Abs. 3 erfasst nach der Begründung nur Sachinformationen. Eine solche Mitwirkungspflicht wäre vertretbar, wenn sie akzessorisch an eine vorab kontrollierte Einzelmaßnahme anknüpft, sich auf das betroffene Fahrzeug beschränkt und weder Generalschlüssel noch neue Schwachstellen verlangt. Hinzukommen sollten eine Geheimhaltungspflicht und eine Entschädigung.

Ebenfalls nicht vorgesehen ist eine Sicherungsanordnung für Verkehrsdaten. Anbieter speichern Verkehrsdaten oft nur wenige Tage, sodass eine spätere Auskunft ins Leere läuft, wenn sich ein Verdacht erst nach Wochen erhärtet. Eine einzelfallbezogene Sicherung ist deutlich grundrechtsschonender als eine anlasslose Speicherung, weil sie nur vorhandene Daten vor der Löschung bewahrt und der Abruf eigenen Voraussetzungen unterliegt. Wir empfehlen deshalb eine Befugnis, Verkehrsdaten zu bestimmten Kennungen sichern zu lassen, wenn tatsächliche Anhaltspunkte für eine Bestrebung oder Tätigkeit bestehen. Die Sicherung sollte auf höchstens drei Monate befristet und einmal verlängerbar sein. Abgerufen werden dürften die Daten nur unter den regulären Voraussetzungen der Verkehrsdatenauskunft, und mit Fristablauf wären sie zu löschen. Eine Absenkung auf das Niveau des Prüffalls trüge dagegen nicht, weil schon die Sicherung in Art. 10 GG eingreift.

#### IV. Nachrichtendienstliche Mittel (§§ 16–32)

##### 1. Systematik (§§ 16, 29)

Die Systematik der Mittel ergänzt der Entwurf um eine Erprobungsklausel (§ 16 Abs. 4 S. 2 BVerfSchG-E). Danach dürfen Mittel, die nicht gesetzlich geregelt, aber vom Eingriffsgewicht her vergleichbar gewichtig sind, zur Erprobung in eine Dienstvorschrift aufgenommen und dann im Wirkbetrieb des Inlandsdienstes eingesetzt werden. Jene Erprobung ist auf vier Jahre befristet, während derer die Weiterverarbeitung der gewonnenen Daten beschränkt ist und die Zustimmung von BMI und UKRat sowie die Unterrichtung des PKGr voraussetzt. Vor dem Hintergrund dieser Kontrollmechanismen ist die Klausel – wohl gerade noch – verfassungsrechtlich vertretbar.<sup>233</sup> In der Sache ist sie zudem jedenfalls begründet, weil durch den rasanten technischen Fortschritt und das Fehlen von Generalklauseln im allgemeinen Nachrichtendienstrecht, dem diese gegenüber der offen handelnden Polizei strukturell fremd sind, ansonsten ein ständiges Zurückbleiben hinter den Möglichkeiten anderer Dienste, aber auch der Beobachtungsobjekte selbst droht. Der Gesetzgeber muss die Regelung aber enger ziehen, indem er klarstellt, dass die Klausel keine neuen Arten von Eingriffen in Wohnungen, private informationstechnische Systeme oder das Fernmeldegeheimnis eröffnet. Folgerichtig unterwirft § 29 schließlich Einsatzformen, die den geregelten Mitteln in der Eingriffstiefe gleichkommen, derselben Schwelle und der Vorabkontrolle (§ 34 Abs. 1 Nr. 10). Aus rechtspolitischer Sicht empfehlen wir zudem eine Frist von nur zwei Jahren und einen Bericht über das Ergebnis an das PKGr. So erreicht die Frage, ob das erprobte Mittel normiert werden soll, rechtzeitig den Bundestag.

Neu ist auch die heimliche Inbesitznahme von Sachen zur Auswertung (§ 16 Abs. 1 S. 2 Nr. 4). Sie erinnert an die polizeiliche Sicherstellung, ist der Sache nach aber auf Informationsbeschaffung gerichtet. Der Dienst nimmt die Sache nämlich nicht in Besitz, um eine Gefahr abzuwehren, sondern um die in ihr verkörperten Informationen auszuwerten, und er tut das heimlich, ohne dem Betroffenen eine Duldung aufzugeben. Das lässt sich als „Sammlung von Unterlagen“ verstehen, die das Grundgesetz dem Verfassungsschutz zuweist (Art. 73 Abs. 1 Nr. 10 lit. b, Art. 87 Abs. 1 S. 2 GG), und begründet wohl noch keine operative Anschlussbefugnis. Diese Einordnung trägt aber nur, solange die Inbesitznahme der nachrichtendienstlichen Auswertung dient – in diesem Sinne stellt sie auch keine Folgemaßnahme dar, sondern umgekehrt eine der nachrichtendienstlichen Auswertung vorgelagerte Beschaffungsmethode. Nachgebessert werden sollte allerdings bei den Vorschriften zur Rückgabe der Sache, die nach dem Regierungsentwurf vorgenommen werden soll, wenn keine überwiegenden Sicherheitsinteressen entgegenstehen (Satz 3). Was bei dauerhafter Nichtrückgabe gilt, regelt der Entwurf zudem leider nicht. Behält der Dienst eine Sache, um sie dem Betroffenen dauerhaft zu entziehen (etwa eine Waffe), so wirkt die Maßnahme wie eine Sicherstellung zur Gefahrenabwehr und verliert ihren Primärbezug zur Sammlung von Unterlagen zwecks ihrer Auswertung. Wir empfehlen deshalb, die Nichtrückgabe auf Fälle zu beschränken, in denen die Rückgabe die Maßnahme oder ihre Quellen offenlegen würde. Ist dagegen eine Gefahr abzuwehren, sollte der Dienst die Sache an die zuständige Polizei übergeben, wie es § 110 BNDG-E für die Eigensicherung vorsieht (vgl. dazu unter B.X.3). Für Sachen, die dauerhaft einbehalten werden, sollte zudem eine Entschädigung nach dem Vorbild des Bundespolizeigesetzes vorgesehen werden, sofern dem nicht

---

<sup>233</sup>A.A. Löffelmann, VerfBlog v. 20.8.2026 (Fn. oben), der in den Erprobungsklauseln (§ 16 Abs. 4 BVerfSchG-E, § 19 Abs. 1 BNDG-E) eine Selbstermächtigung der Exekutive unter Umgehung des Parlaments sieht.

auf das Engste begrenzte Geheimhaltungsgründe entgegenstehen. (Zur Inbesitznahme in Wohnungen vgl. unter B.I.5.)

## 2. Adressatenkreis (§ 16 Abs. 5)

Für alle Mittel regelt der Entwurf gemeinsam, gegen wen sie sich richten dürfen: § 16 Abs. 5 BVerfSchG-E übernimmt hier die Vorgaben des Bundesverfassungsgerichts zur Überwachung Dritter.<sup>234</sup> Konsequenterweise ist, dass sich Maßnahmen der Spitzenstufe nicht gegen Kontaktpersonen richten dürfen (Satz 4). Klärungsbedürftig ist dagegen § 22 Abs. 3 S. 2, wonach schon die Teilnahme an einer Kommunikationsgruppe, die im Wesentlichen für Zwecke der Bedrohung genutzt wird, ein Anhaltspunkt für eine Beteiligung ist. In Gruppen mit Hunderten Mitgliedern ist die bloße Mitgliedschaft nicht zwingend so angereichert, dass sich daraus Beteiligungsverhältnisse konstruieren lassen. Der Gesetzgeber sollte klarstellen, dass „Teilnahme“ eine aktive Beteiligung an der Kommunikation meint.

## 3. Vertrauenspersonen und Verdeckte Bedienstete (§§ 17–19)

Vertrauenspersonen sind Privatpersonen, die dem BfV verdeckt berichten, Verdeckte Bedienstete in Abgrenzung hierzu eigene Mitarbeiter, die unter einer Legende eingesetzt werden.<sup>235</sup> Wer als Vertrauensperson nicht in Betracht kommt, regelt schon das geltende Recht. Daran knüpft der Entwurf an. Der Ausschlusskatalog des § 18 Abs. 1 S. 2 BVerfSchG-E entspricht § 9b Abs. 2 BVerfSchG.<sup>236</sup> Auch die Ausnahme vom Ausschluss Verurteilter (Nr. 5) kannte schon § 9b Abs. 2 S. 3 BVerfSchG. Neu sind dagegen zwei weitere Ausnahmen: Erstens kann die Amtsleitung Minderjährige ab 16 Jahren zulassen, wenn der Einsatz zur Aufklärung besonders erheblich beobachtungsbedürftiger Bestrebungen unerlässlich ist. Zum zweiten kann die Amtsleitung unter gleichem Maßstab für einen befristeten Einsatz das Verbot, wirtschaftlich Abhängige einzusetzen, suspendieren. Gegen die zweite Ausnahme ist wenig einzuwenden, denn der Ausschluss wirtschaftlich Abhängiger soll vor allem die Nachrichtenehrlichkeit sichern und damit die Gefahr, dass eine Quelle aus finanziellem Eigeninteresse Informationen erfindet oder ausschmückt, begrenzen. Dieses Risiko dürfte bei einem befristeten Einsatz naturgemäß geringer sein und ist angesichts der erhöhten Anordnungsschwelle auch verhältnismäßig. Auch die erste Ausnahme halten wir im Grundsatz für vertretbar, sie verlangt aber sorgfältige Sicherungen, die das Gesetz bisher vermissen lässt. Ein Sechzehn- oder Siebzehnjähriger kann die Risiken einer Zusammenarbeit noch begrenzter überblicken als ein sonstiger V-Mann, und soll (wenngleich im Sinne der Bedrohungsstufenlogik konsequent) ausgerechnet in den gefährlichsten Milieus der Beobachtungsschwellen-Spitzenstufe eingesetzt werden. Zudem bleibt unbestimmt, was es bedeutet, dass Belange der Fürsorge „besonders zu berücksichtigen“ sind (Satz 4). Hinzu kommt eine zivilrechtliche Frage: Die Zusammenarbeit wird vertraglich abgewickelt, und dafür bedarf es bei einem Minderjährigen grundsätzlich die Zustimmung seiner gesetzlichen Vertreter (§§ 107, 108 BGB).<sup>237</sup> Die Begründung nennt als Anwendungsfall einen Sechzehnjährigen, den eine terroristische Vereinigung zum Transport von Tatwaffen einsetzt.<sup>238</sup> Die Ausnahme zielt also auf Minderjährige, die bereits in die Bedrohung eingebunden sind. Gerade dann wird das Zustimmungserfordernis aber zum Problem. Gehören die Eltern selbst zum aufzuklärenden Umfeld, würde ihre

<sup>234</sup> BVerfGE 162, 1, Rn. 209 ff.

<sup>235</sup> Zur strafrechtlichen Stellung Geheimer Mitarbeiter, die sich im Rahmen ihres Auftrags in extremistischen Umfeldern bewegen, Manns, GSZ 2026, 81 (82 ff.).

<sup>236</sup> Dietrich, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, VI § 2 Rn. 57, 59.

<sup>237</sup> Zur Einordnung als privatrechtlicher Vertrag sui generis mit Zügen eines Dienst- oder Werkvertrags Dietrich, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, VI § 2 Rn. 68. Die Begründung zu § 18 Abs. 1 S. 3 BVerfSchG-E (BT-Drs. 21/7868, S. 245) spricht die Vertragsgestaltung nicht an.

<sup>238</sup> Begr. zu § 18 Abs. 1 S. 3 BVerfSchG-E, BT-Drs. 21/7868, S. 245.

Einbindung die Quelle und den Jugendlichen gefährden, und ansonsten würden sie die Tätigkeit wohl niemals genehmigen. Ob die Zusammenarbeit ohne sie wirksam begründet werden kann, beantworten weder der Normtext noch die Begründung. Diese Frage sollte der Gesetzgeber deshalb selbst regeln. Aus rechtspolitischer Sicht sollte die Ausnahme zudem im Normtext auf Minderjährige beschränkt werden, die im Sinne der durch die Gesetzesbegründung selbst gewählten Beispielkonstellation bereits in die Bedrohung eingebunden sind. Wie die Belange der Fürsorge berücksichtigt werden, sollte in der Anordnung dokumentiert und dem UKRat dargelegt werden.

Die Vorabkontrolle des Quelleneinsatzes (§ 34 Abs. 1 Nr. 3 BVerfSchG-E) bleibt derzeit unvollständig. Nach § 13 Abs. 4 UKRatG-E ist die Einholung jener Angaben, die die Identität operativ eingesetzter Personen erkennen lassen, von den Befugnissen des UKRats ausgenommen. Die Anordnung nach § 33 Abs. 2 BVerfSchG-E nennt zudem nur Aufklärungsgegenstand und Zielperson, nicht aber die Vertrauensperson. Anhand pseudonymisierter Vorgänge kann der UKRat zwar Auftrag, Führung und Berichte der Quelle nach den Angaben des Dienstes prüfen. Personenabhängige Voraussetzungen lassen sich dadurch aber nicht unabhängig überprüfen – etwa ob die Person nach § 18 Abs. 1 S. 2 ausgeschlossen ist, ob die Angaben über ihre Vorgeschichte zutreffen oder ob sie steuernden Einfluss nimmt. Gerade eine effektive, einzelfallbezogene Vorabkontrolle verlangt das Bundesverfassungsgericht aber für den Einsatz von Vertrauenspersonen.<sup>239</sup> Zwar hat es den Quellenschutz hoch gewichtet und eine Ausgestaltung verlangt, die die Vertrauensperson schützt.<sup>240</sup> Dass der Kontrolleur nicht weiß, wen er kontrolliert, hat es aber nicht verlangt. Gerade die Person der Quelle kann ein ernsthaftes, auch politisches Problem für Nachrichtendienste aufwerfen, wie die parlamentarische Aufarbeitung früherer Quelleneinsätze mehrfach gezeigt hat. Die Gesetzesbegründung stützt die Mitteilungssperre darauf, dass schon der Eindruck fehlender Vertraulichkeit Quellen abschrecken könne.<sup>241</sup> Die zitierte Entscheidung betraf aber einen parlamentarischen Untersuchungsausschuss, nicht eine zur Verschwiegenheit verpflichtete und gerichtsähnliche Kontrollinstanz wie den UKRat, der sogar im Austausch mit ausländischen Partnerdiensten nicht der Third Party Rule unterfällt. Bereits der NSU-Untersuchungsausschuss dokumentierte zudem, dass eine interne Fachprüfgruppe des BfV uneingeschränktes Einsichtsrecht in die Operativakten hat(te).<sup>242</sup> Überspitzt gesagt kann das notwendige Geheimhaltungsmaß also derart überschießend eng auch innerhalb des Dienstes nicht verstanden werden. Tatsächlich zeigt das Vorhandensein der innerdienstlichen Prüfstrukturen, dass sich Quellenschutz und ein eng begrenzter Kontrollzugang zur Identität organisatorisch vereinbaren lassen. Was einer internen Prüfinstanz zugänglich sein kann, sollte einem sicherheitsüberprüften Mitglied des gerichtsähnlichen Kontrollorgans nicht verschlossen bleiben, notfalls im Sinne des „Treptow-Verfahrens“ über eine Einsicht nur in den Räumlichkeiten des BfV. Regelfall sollte sein, dass der Dienst dem UKRat auf Verlangen eine Überprüfung der personenbezogenen Einsatzvoraussetzungen ermöglicht, etwa zu Vita, einschlägigen Straftaten und Stellung der Vertrauensperson in der beobachteten Vereinigung, ohne unmittelbar und vollständig ihre Personenidentität offenzulegen, d.h. den Namen zu nennen (vgl. dazu auch unter D.XI). Soweit identifizierende Informationen unerlässlich sind, sollte § 13 Abs. 4 UKRatG-E so ergänzt werden, dass die Identität einem vom Senat bestimmten Mitglied des gerichtsähnlichen Kontrollorgans (Quellenbeauftragter) auf Verlangen in den Räumen des Dienstes offengelegt wird, ohne dass

<sup>239</sup> BVerfGE 162, 1, Rn. 219; BVerfGE 141, 220, Rn. 174. Zur Eingriffsintensität des Einsatzes verdeckter Personen weiterführend Bergemann, NVwZ 2015, 1705; Roggan, DÖV 2019, 425; a.A. Unterreitmeier, GSZ 2019, 233; zum geltenden Recht vgl. Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 9b BVerfSchG.

<sup>240</sup> BVerfGE 162, 1, Rn. 355.

<sup>241</sup> Begr. zu § 13 Abs. 4 UKRatG-E, BT-Drs. 21/7868, S. 570, unter Hinweis auf BVerfGE 146, 1, Rn. 114.

<sup>242</sup> BT-Drs. 17/14600, S. 197 (Abschnitt „cc) Die Fachprüfgruppe“).

Rückschlüsse auf diese Einsichtnahme in die Akten des UKRats gelangen. Ablehnungen von Anträgen des UKRats auf Basis dieser Einzeleinsichtnahme müssten dann nur tenoriert, nicht aber inhaltlich begründet erfolgen, was angesichts dessen gut vertretbar ist, dass hierdurch bilaterale erläuternde Hinweise des Quellenbeauftragten an das BfV – etwa an die dortige interne Fachprüfgruppe – nicht ausgeschlossen sind und es mangels einer Rechtsmittelinstanz zu keiner Überprüfungsproblematik durch eine andere gerichtsähnliche Stelle hinsichtlich der Entscheidungsgründe kommt.

Ungeregelt bleibt der Schutz von Vertrauenspersonen in behördlichen und gerichtlichen Verfahren. Werden sie als Zeugen geladen oder müssen sie gegenüber Behörden Einkünfte angeben, geraten sie in einen Konflikt zwischen Wahrheits- und Offenbarungspflichten und ihrer Enttarnung, die sie an Leib und Leben gefährden kann. Eine Erlaubnis zur Falschaussage wäre verfassungsrechtlich nicht tragfähig, weil sie die Wahrheitsfindung und die Verfahrensrechte Dritter trafe, insbesondere das Recht auf ein faires Verfahren. Vertretbar ist dagegen ein gesetzliches Recht, Angaben über die Zusammenarbeit mit dem Dienst zu verweigern, das an eine Sperrerklärung des BMI gekoppelt ist und die Kontrollmechanismen des Prozessrechts unberührt lässt. Für Zuwendungen an Vertrauenspersonen empfehlen wir statt einer straffreien Täuschung ein abgeschirmtes Melde- und Anrechnungsverfahren, in dem das BfV die zuständigen Stellen unterrichtet, ohne die Quelle offenzulegen.

Abschließend ist es bedauerlich, dass der Entwurf die bisherige Regelung zur Beteiligung von Vertrauenspersonen an Bedrohungen unverändert fortführt. Zulässig bleibt eine solche Beteiligung nur, wenn sie nicht in Individualrechte eingreift, von den Beteiligten derart erwartet wird, dass sie zur Gewinnung und Sicherung der Informationszugänge unumgänglich ist, und nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts steht (§ 18 Abs. 5 S. 3).<sup>243</sup> Die pauschale Trennung zwischen Organisations- und Begleitdelikten einerseits und Eingriffen in Individualrechtsgüter fällt dabei extrem strikt aus. Sie schließt selbst geringe Eingriffe wie eine Sachbeschädigung aus, auch wenn diese der Aufdeckung drohender Anschläge dient und eine allgemeine Verhältnismäßigkeitsprüfung eindeutig zugunsten der Maßnahme ausfiele. Praktisch wiegt das schwer, weil manche Gruppierungen die Loyalität ihrer Mitglieder gezielt durch „Keuschheitsproben“ prüfen, bei denen Straftaten gerade dazu dienen, staatliche Einschleusungen zu enttarnen. Verweigert sich eine Vertrauensperson, folgt nahezu sicher ihr Ausschluss, mit dem der Informationszugang verloren geht und der sie im Einzelfall selbst gefährden kann. Das Argument, ein Katalog zulässiger Taten erleichtere die Enttarnung, trägt dabei wenig, weil schon heute bekannt ist, dass kein Nachrichtendienstgesetz Eingriffe in Individualrechte erlaubt. Gerade die Verweigerung einer kleinen Sachbeschädigung kann deshalb verräterisch wirken, weil sie im Vergleich zur Begehung von Leib- oder Lebensschäden von offensichtlich viel geringerem Gewicht ist. Für Straftaten gegen Leib und Leben ist der Ausschluss selbstverständlich zwingend, weil Dritte keine derart intensiven Eingriffe hinnehmen müssen, die nur der Abtarnung einer Quelle dienen. Für jedes Delikt gilt das aber nicht, zumal die Nichtentdeckung einer Quelle über ihre fortgesetzte Beobachtungsfähigkeit letztlich dem Schutz besonders gewichtiger Rechtsgüter dient, darunter gerade Leib und Leben anderer Personen. Eine Sachbeschädigung, etwa das Besprühen einer Hauswand mit verfassungsfeindlichen Symbolen, kann – wie bereits abstrakt skizziert – verhältnismäßig sein, wenn sie unumgänglich ist und der Staat den Schaden ersetzt, sobald das ohne Gefährdung der operativen Sicherheit möglich ist.<sup>244</sup> Zumindest rechtspolitisch sollte der Gesetzgeber den Ausschluss deshalb auf Eingriffe in Leib und Leben und vergleichbar gewichtige Individualrechtsgüter beschränken und geringfügige Eingriffe in andere

<sup>243</sup>Ebenso bislang § 9a Abs. 2 S. 3 i.V.m. § 9b Abs. 1 S. 1 BVerfSchG.

<sup>244</sup>So schon Manns, GSZ 2026, 81 (82, 84, 86).

Individualrechtsgüter unter den übrigen Voraussetzungen des Satzes 3 und mit einer Entschädigungspflicht nach Maßgabe der operativen Sicherheit und einer nachträglichen Prüfung durch den UKRat zulassen.

#### **4. Observation, Standortfeststellung (§§ 20, 21)**

Die Zeit- und Tagesschwellen der §§ 20 und 21 BVerfSchG-E setzen die Karlsruher Vorgaben zur längerfristigen Observation klar um. Da der Vorabkontrolle aber nur die Maßnahmen der Spitzenstufe unterliegen (§ 34 Abs. 1 Nr. 4 und 5), bleiben Observationen an sieben oder mehr Tagen innerhalb von 30 Tagen (§ 20 Abs. 1 Nr. 1 lit. b) ohne unabhängige Anordnungskontrolle. Ob das Bundesverfassungsgericht eine solche Kontrolle schon ab dieser Dauer verlangt, ist nicht eindeutig.<sup>245</sup> Zumindest rechtspolitisch empfehlen wir deshalb, auch diese Observationen der Vorabkontrolle zu unterstellen (C.V).

#### **5. Brief-, Post- und Telekommunikationsüberwachung (§ 22)**

Die Überwachung von Brief-, Post- und Telekommunikation war bislang im G 10 geregelt. An die Stelle der §§ 1, 3 G 10 tritt nun § 22 BVerfSchG-E. Das ist systematisch stimmig, weil die Überwachung damit dort geregelt ist, wo auch die übrigen Befugnisse des BfV stehen (vgl. B.III.1). Die Überwachung knüpft künftig an die besonders erhebliche Beobachtungsbedürftigkeit an (Abs. 1 S. 1). Da schon § 3 Abs. 1 S. 1 G 10 Verhaltensweisen im Vorfeld einer Rechtsgutsverletzung erfasste und das Staatsschutzrecht umfangreiche Delikte im Bereich der Aktivitäten fremder Mächte vorsieht (vgl. unter B.IV), liegt die Überwachungsschwelle in der Spionageabwehr schon nach geltendem Recht niedrig. Dass geheimdienstliche Tätigkeiten nach dem neuen Recht ohne Weiteres abhörfähig sind (§ 3 Abs. 8 Nr. 2), stellt insofern keine rechtlich erhebliche Ausweitung dar. Außerhalb der Spionage wechselt der Entwurf dagegen das System (vgl. diesbezüglich zur Bewertung unter C.I.2, die für das BfV sinngemäß gilt, soweit dort Inlandsmaßnahmen des BND angesprochen sind).

Überdenken sollte der Gesetzgeber allerdings die Abstufung in Absatz 1 Satz 2 Nr. 2. Das Fernmeldegeheimnis knüpft an die Verwundbarkeit der räumlich distanzierten Übermittlung an, nicht an die Art der Beteiligten oder den Inhalt. Es schützt deshalb neben dem fernmündlichen Gesprächsverkehr auch Datenströme, an denen auf einer oder beiden Seiten kein Mensch beteiligt ist.<sup>246</sup> Der Entwurf lässt die Überwachung der Inhalte nicht interpersoneller Dienste gleichwohl schon auf der ersten Steigerungsstufe zu und unterstellt ihnen damit ein geringeres Gewicht. Das trifft nur zum Teil zu. Welche Seiten jemand aus der Internetnutzung aufruft, was er eine Auskunftsoftware fragt oder welche Werte ein Fitnessdienst überträgt, kann ebenso viel über eine Person verraten wie ein Gespräch. Eine typisierende Abstufung ist dem Gesetzgeber nicht verwehrt. Sie muss aber beim Eingriffsgewicht ansetzen und nicht bei der Kategorie des Dienstes. Wir empfehlen deshalb, die niedrigere Schwelle nur für Inhalte zu eröffnen, die keine vergleichbar gewichtigen Einblicke in die Lebensgestaltung erlauben, mit der Formel, die § 26 Abs. 2 schon für den abgegrenzten Eingriff enthält.

Neu ist schließlich die Befugnis, in Brief- und Postsendungen technische Mittel einzubringen (Abs. 1 S. 4). Sie geht insoweit über die passive Überwachung hinaus, als sie erlaubt, Sendungen zu manipulieren. Die Gesetzesbegründung nennt exemplarisch sowohl den Einsatz von GPS-Trackern

<sup>245</sup> BVerfGE 162, 1, Rn. 219 f.: unabhängige Kontrolle längerfristiger Observationen, wobei es auf die Dauer der Maßnahme ankommt.

<sup>246</sup> BVerfG, Beschl. v. 24.6.2025, 1 BvR 2466/19, Rn. 87 ff., 91.

als auch die softwaretechnische Manipulation versandter IT-Geräte.<sup>247</sup> Absatz 1 Satz 4 gestattet dabei allerdings nur das Einbringen in die Sendung. Da die Begründung auch das Einbringen in die versandten Gegenstände selbst erfasst wissen will, sollte der Wortlaut um die in der Sendung enthaltenen Güter ergänzt werden. Die technische Maßnahme selbst, etwa die Ortung oder der Zugriff auf ein versandtes Gerät, bedarf einer eigenen gesetzlichen Befugnis. Es handelt sich insoweit – wie auch die Betretung von Wohnungen – nicht um eine auf eine nachrichtendienstliche Aufklärung folgende operative Anschlussmaßnahme, sondern im Gegenteil nur um eine Vorbereitungshandlung zur Ermöglichung des gesondert geregelten Überwachungsverfahrens, dessen Eingriffsgewicht weiterhin maßgeblich bleibt. Von daher ist die Regelung nicht in unverhältnismäßiger Weise ausgestaltet.

## **6. Eingriffe in informationstechnische Systeme (§§ 23–26)**

### **a) Auslesen informationstechnischer Geräte (§ 23)**

Die Eingriffe in informationstechnische Systeme verteilt der Entwurf nach ihrem Gewicht auf vier Befugnisse. Auf der ersten Steigerungsstufe erlaubt § 23 BVerfSchG-E das Auslesen gespeicherter Daten informationstechnischer Geräte, auch solcher, die ein ausländischer Nachrichtendienst übergeben hat (Abs. 1 S. 2 Nr. 2 lit. b). Das ist mehr als das Auslesen vorhandener Asservate. Die Norm erfasst vielmehr auch Fälle, in denen sich der Dienst erst Zugang zu dem Gerät verschafft, und die Begründung bezieht sogar den elektronischen Fernzugang ein.<sup>248</sup> Insoweit unterscheidet sich die Norm von § 54 BNDG-E, der einen Speicher im Besitz des Dienstes voraussetzt. Auch wer ein Gerät und die Zugangsdaten zu externen Speichern besitzt, darf allerdings nicht ohne Weiteres neue Daten aus einer Cloud erheben. Ein neuer Zugriff auf ein privat genutztes, auch vernetztes System muss vielmehr die Voraussetzungen der besonderen IT-Befugnisse erfüllen, wie § 23 Abs. 5 S. 1 durch den Verweis auf die §§ 25 und 26 klarstellt. Der Gesetzgeber sollte deshalb präzisieren, dass auch ein elektronischer Fernzugang nach § 23 nur zur Auswertung bereits auf dem Gerät gespeicherter Daten berechtigt. Private Systeme, die technisch auf Gerät und Cloud verteilt sind, sind dabei als Einheit zu betrachten.

Gestuft ist auch die Weiterverarbeitung. Ergeben die Daten umfassende Informationen über private Lebensbereiche, dürfen sie nur bei besonders erheblicher Beobachtungsbedürftigkeit weiterverarbeitet werden (Abs. 3). Für Verhaltens- oder Persönlichkeitsprofile verweist Absatz 5 Satz 2 sogar auf § 25, so dass auch diese Stufe nicht für jede Profilbildung genügt. Auslesen und Weiterverarbeitung in den Fällen der Absätze 2 und 3 unterliegen zudem der Vorabkontrolle durch den UKRat (§ 34 Abs. 1 Nr. 7). Die Abgrenzung zum privaten System des § 25 über Funktionalität und Datenmenge entspricht der Rechtsprechung.<sup>249</sup> Praktisch wird ihre Anwendung aber schwerfallen, weil das BfV vor dem Zugriff selten weiß, welche Kategorien von Daten mit welcher persönlichkeitsrechtlichen Intensität ein Gerät enthält. Neben der externen Kontrolle ist der richtige Ort dafür die Vorprüfung durch den Aufsichtsbediensteten (Abs. 2; bislang als G 10-Juristen bezeichnet), die allerdings nur greift, wenn „nach den Umständen des Einzelfalls“ besonders schutzwürdige Informationen zu erwarten sind. Mindestens aus rechtspolitischer Sicht sollte eine Vorprüfung oder begleitende Prüfung

<sup>247</sup> Begr. zu § 22 Abs. 1 BVerfSchG-E, BT-Drs. 21/7868, S. 255.

<sup>248</sup> BT-Drs. 21/7868, S. 28 f., 37; Begr. S. 257 f.

<sup>249</sup> BVerfGE 120, 274 (313 f.); 141, 220, Rn. 209 ff. Zur Kontrolle nachrichtendienstlicher IT-Zugriffe weiterführend Schlömer, NVwZ 2023, 1121.

durch den Aufsichtsbeamten deshalb regelmäßig vorgesehen werden, wenn ein Gerät nicht erkennbar ein reines Funktionsgerät ist.

## **b) Eingriff in private informationstechnische Systeme (§ 25)**

Am schwersten wiegt die Online-Durchsuchung, die § 25 BVerfSchG-E für das BfV einführt. Sie setzt kumulativ voraus: eine konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut durch eine besonders erheblich beobachtungsbedürftige Bedrohung, Subsidiarität auch gegenüber polizeilicher Hilfe, die Beschränkung auf Beteiligte und auf Dritte, deren System ein Beteiligter nutzt, sofern die Aufklärung durch eine Maßnahme gegen den Beteiligten nicht ebenso möglich ist (§ 25 Abs. 2 Nr. 2), die Vorabkontrolle (§ 34 Abs. 1 Nr. 9) sowie Kennzeichnung und Übermittlungssperre. Damit übernimmt der Entwurf die Vorgaben des Bundesverfassungsgerichts zu Schwelle und Anordnung, offen bleibt allein der Kernbereichsschutz (dazu sogleich).<sup>250</sup> Mit der zusätzlichen Bindung an die Spitzenstufe geht der Entwurf sogar über das erforderliche Schwellenmaß hinaus. Das ist richtig, weil es die Maßnahme an den Aufgabenbereich des Dienstes rückbindet. Für den Verfassungsschutz ist die vollständige Online-Durchsuchung ohnehin kein Instrument der Vorfeldaufklärung, sondern ein in die Gefahrenabwehr hineinragendes Mittel an der Grenze seiner Zuständigkeit.

Gegen die Befugnis werden im Wesentlichen zwei Einwände erhoben: Der erste hält sie wegen der Subsidiarität zur Polizei für überflüssig.<sup>251</sup> Dabei handelt es sich aber um ein rein rechtspolitisches Argument. Das Bundesverfassungsgericht hat die Befugnis nämlich für die Dienste hingegen gerade nicht ausgeschlossen, sondern mit der Subsidiaritätsbindung zugelassen.<sup>252</sup> Fälle, in denen allein ein Dienst die Gefahr kennt und eine Übermittlung an die Polizei ausgeschlossen ist (etwa aufgrund der Third Party Rule), sind zwar selten, aber denkbar. Gleiches gilt dafür, dass rechtzeitiges Einschreiten der Polizeien nicht mehr möglich sein kann. Der zweite Einwand trifft dagegen zu: Nach § 25 Abs. 1 S. 2 soll ein System nur dann als privat gelten, wenn es „als eigenes privat genutzt“ wird. Das Bundesverfassungsgericht schützt dagegen Systeme, die der Betroffene als eigene nutzt, ohne es darauf ankommen zu lassen, ob er sie privat nutzt.<sup>253</sup> Der Beschluss vom 24. Juni 2025 stützt diese funktionale Betrachtung.<sup>254</sup> Ein dienstlich überlassenes Gerät ist danach nicht schon wegen seiner Überlassung vom Schutz privater Systeme ausgeschlossen. Nutzt jemand ein Mobiltelefon als eigenes, aber ausschließlich dienstlich, käme nach dem Entwurf grundsätzlich nur § 23 in Betracht, weil auch § 26 ein privates System voraussetzt. Der Zugriff wäre dann schon auf der ersten Steigerungsstufe möglich. Die Begründung stellt demgegenüber zu Recht auf die Bedeutung des Systems für die persönliche Lebensführung ab.<sup>255</sup> Verfassungsrechtlich spricht deshalb viel dafür, das Wort „privat“ in Satz 2 zu streichen.

Entscheidend ist allerdings der Kernbereichsschutz. Das Bundesverfassungsgericht hat im BKAG-Urteil verlangt, dass Daten aus einer Online-Durchsuchung vor der Auswertung von einer unabhängigen Stelle gesichtet werden. Im BayVSG-Urteil hat es diese Vorgabe auf die Nachrichtendienste übertragen.<sup>256</sup> Der Entwurf setzt auf beiden Ebenen an. Bei der Erhebung ist, soweit technisch möglich, sicherzustellen, dass kernbereichsrelevante Informationen nicht erhoben werden (§ 31 Abs. 1

<sup>250</sup> BVerfGE 162, 1, Rn. 166, 175 ff., 178 (Angleichung an die polizeiliche Schwelle, Subsidiarität).

<sup>251</sup> Gesellschaft für Freiheitsrechte, Stellungnahme v. 14.7.2026 (Fn. oben).

<sup>252</sup> BVerfGE 162, 1, Rn. 178 ff.

<sup>253</sup> BVerfGE 120, 274 (315); ebenso Gesellschaft für Freiheitsrechte, Stellungnahme v. 14.7.2026 (Fn. oben).

<sup>254</sup> BVerfG, Beschl. v. 24.6.2025, 1 BvR 180/23 (Trojaner II), Rn. 173.

<sup>255</sup> Begr. zu § 25 Abs. 1 BVerfSchG-E, BT-Drs. 21/7868, S. 261, unter Hinweis auf BVerfG, Beschl. v. 24.6.2025, 1 BvR 2466/19 (Trojaner I), Rn. 104, 113, und 1 BvR 180/23 (Trojaner II), Rn. 173, 230.

<sup>256</sup> BVerfGE 141, 220, Rn. 224; 162, 1, Rn. 315.

S. 4 BVerfSchG-E). Vorzulegen sind dem UKRat aus einer Online-Durchsuchung aber nur fortgesetzte automatische Aufzeichnungen nach Absatz 3 und Informationen, bei denen Zweifel an der Kernbereichsrelevanz bestehen (§ 31 Abs. 4 S. 1 Nr. 1 und 3, Abs. 5 S. 1 Nr. 1). Diese Informationen dürfen erst nach seiner Zustimmung genutzt werden (Abs. 6). Eine vollständige Vorlage aller aus einer Online-Durchsuchung gewonnenen Daten verlangt das Gesetz damit nicht. Die Begründung stützt das auf § 100d Abs. 3 S. 2 StPO, auf Ausführungen im Trojaner II-Beschluss, die sie selbst als nicht tragend bezeichnet, und auf die Undurchführbarkeit einer Vollsichtung bei großen Datenmengen.<sup>257</sup> Zwar ist im Sinne des Regierungsentwurfs anzuerkennen, dass eine unabhängige Vollsichtung den Kernbereich besser schützt, aber bei umfangreichen Datenbeständen einen so hohen Aufwand erfordert, dass hierdurch angesichts der zugleich hohen Schwellen für die Online-Durchsuchung kaum mehr Raum besteht, um nach der Sichtung noch rechtzeitig nachrichtendienstlich zu handeln. Insofern beißen sich die Zielvorgaben aus der Rechtsprechung an dieser Stelle gegenseitig. Zudem ist es ein gewichtiges Vergleichsargument, dass § 100d Abs. 3 StPO keine allgemeine Vollsichtung verlangt. Verfassungsrechtlich bleibt aber ein Risiko, weil die Gesetzesbegründung nicht tragende Ausführungen gegen eine tragende Vorgabe des Verfassungsgerichts stellt und nicht darlegt, warum die unterschiedlichen Erhebungs- und Auswertungsbedingungen die Abweichung tragen.<sup>258</sup> Hält das Bundesverfassungsgericht an seiner Vorgabe fest, stünde mit dem Kernbereichsschutz des § 31 Abs. 4 auch die Online-Durchsuchung selbst in Frage.

Tragfähiger wäre ein Sichtungsverfahren, das die unabhängige Filterung vor die operative Kenntnisnahme legt, ohne dass jede Datei unabhängig von ihrem Inhalt manuell gesichtet werden muss. Denkbar ist eine technische Vorfilterung nach Dateitypen, Speicherorten und Suchmerkmalen, deren Parameter der UKRat billigt. Daten, die danach eindeutig keinen Kernbereichsbezug haben, werden freigegeben. Zweifelhafte Daten prüft dagegen ein Bediensteter des administrativen Kontrollorgans, der dem operativen Auswertungsteam nicht angehört, aber im BfV sehr zeitnah erreichbar ist. Dieser Bedienstete gibt erhobene Daten frei und legt nur solche Informationen dem gerichtsähnlichen Organ zur abschließenden Entscheidung vor, bei denen er selbst zweifelt. Ein Beobachter, der eine laufende Auswertung erst stoppt, nachdem das operative Team Kernbereichsdaten bereits gesehen hat, genügt hingegen den Karlsruher Anforderungen nicht. Nach dem hier vorgeschlagenen Modell lägen Durchführung und Entscheidungsverantwortung hingegen „maßgeblich“ in unabhängiger Hand, ohne dass jede Datei manuell gelesen werden müsste.<sup>259</sup> Ob ein solches Verfahren den Anforderungen des Bundesverfassungsgerichts vollständig genügt, ist zwar nicht entschieden. Es verbindet aber eine praktikable technische Vorauswahl mit unabhängiger Verantwortung dort, wo der Schutz tatsächlich gefährdet ist. Wir empfehlen deshalb, ein solches Verfahren in § 31 Abs. 5 zu regeln, gegebenenfalls mit einer Übergangsfrist, bis der UKRat das Personal dafür hat. Große Datenmengen rechtfertigen organisatorische und technische Lösungen, aber keinen schwächeren Schutz des absolut geschützten Kernbereichs.

Erfassen muss die Regelung zudem die Eilfreigabe: § 31 Abs. 6 S. 2 erlaubt bei Gefahr im Verzug eine vorläufige Freigabe zur Weiterverarbeitung durch den Aufsichtsbediensteten des BfV (also den bisherigen G 10-Juristen), obwohl die Informationen dem UKRat vorzulegen sind. Ungeklärte kernbereichsverdächtige Inhalte sollten aber nicht schon aufgrund einer solchen internen Eilfreigabe

<sup>257</sup> Begr. zu § 31 Abs. 4 BVerfSchG-E, BT-Drs. 21/7868, S. 271, unter Hinweis auf BVerfG, Beschl. v. 24.6.2025, 1 BvR 180/23 (Trojaner II), Rn. 267.

<sup>258</sup> Tragend BVerfGE 141, 220, Rn. 224; 162, 1, Rn. 315. Nicht tragend BVerfG, Beschl. v. 24.6.2025, 1 BvR 180/23 (Trojaner II), Rn. 267.

<sup>259</sup> Zur Formel BVerfGE 141, 220, Rn. 224.

operativ zugänglich werden, weil die externe Entscheidung sonst zu spät kommt. Daten, die bereits als kernbereichsrelevant erkannt sind, bleiben nach Absatz 7 ohnehin auch im Eilfall unverwertbar.<sup>260</sup>

Zwischen beiden Gesetzen weicht zudem die Vorlageschwelle ab. § 31 Abs. 4 Nr. 3 BVerfSchG-E löst die Vorlage aus, „soweit Zweifel bestehen“. § 21 Abs. 5 S. 2 BNDG-E verlangt dagegen für Daten aus Eingriffen in informationstechnische Systeme „tatsächliche Anhaltspunkte“ für die Kernbereichsrelevanz. Beide erlauben statt der Vorlage die unverzügliche Löschung. Da Zweifel weniger sind als Anhaltspunkte, empfehlen wir aus rechtspolitischer Sicht die niedrigere Schwelle des BVerfSchG-E für beide Gesetze. Sie schützt den Kernbereich wirksamer, weil schon Zweifel die Vorlage auslösen, und nimmt den Diensten die Entscheidung im Grenzfall ab.

### c) Abgegrenzter Eingriff (§ 26)

Unterhalb der Online-Durchsuchung setzt der abgegrenzte Eingriff an. Nach § 26 BVerfSchG-E ist der Eingriff in private Systeme zur abgegrenzten Datenerhebung schon auf der ersten Steigerungsstufe zulässig (Abs. 1). Zielt die Erhebung auf Inhaltsdaten interpersoneller Kommunikation ohne Begrenzung auf einzelne nicht laufende Kommunikationsvorgänge oder auf vergleichbar gewichtige Einblicke, gilt dagegen die Spitzenstufe (Abs. 2), die neben laufender Kommunikation auch weitergehende Zugriffe auf gespeicherte Kommunikation erfasst. Die Konstruktion ist „rechtshandwerklich“ durchaus geschickt, weil sie die Quellen-Telekommunikationsüberwachung erfasst und einen Raum unterhalb der Online-Durchsuchung öffnet, etwa für einzelne Speicherorte. Für die Quellen-TKÜ hat das Bundesverfassungsgericht zunächst maßgeblich darauf abgestellt, dass technisch gesichert ist, dass nur die laufende Kommunikation erfasst wird.<sup>261</sup> Nach dem Beschluss vom 24. Juni 2025 greift die Quellen-TKÜ laufender Kommunikation aber zugleich in Art. 10 GG und in das IT-Grundrecht ein. Die erweiterte Quellen-TKÜ, die auch gespeicherte Kommunikation erfasst, ist sogar allein am IT-Grundrecht zu messen.<sup>262</sup> Die technische Begrenzung der ausgeleiteten Daten beseitigt den Integritätseingriff also nicht, verschiebt aber das Schutzgut. Vor diesem Hintergrund ist die hinsichtlich des erforderlichen Bedrohungsgrads im Vergleich zur vollständigen Online-Durchsuchung niedrigere Schwellenzuordnung zwar richtig. Gerade beim BfV hatten wir jedoch eingangs darauf hingewiesen (C.I.2), dass die „erhebliche Bedrohung“ bei den allermeisten Beobachtungsobjekten und geradezu regelmäßig vorliegen dürfte, sodass der abgegrenzte Eingriff ein potentiell sehr häufig einzusetzendes Mittel werden kann. Der Gesetzgeber muss prüfen, ob er dies politisch möchte und ob es verfassungsrechtlich trägt. Umgehungsverbot (Abs. 1 S. 3) und technische Beschränkung (Abs. 4) tragen außerhalb der Schwellenfrage einer benötigten Begrenzung bereits Rechnung.

Offen ist zudem die Frage einer Vorabkontrolle, weil § 34 Abs. 1 Nr. 9 nur § 26 Abs. 2 S. 1 erfasst, also die vollständige Online-Durchsuchung. Ob die vorherige unabhängige Kontrolle verfassungsrechtlich auch für den abgegrenzten Eingriff geboten ist, hat das Bundesverfassungsgericht nicht entschieden. Es knüpft die vorherige unabhängige Kontrolle an das besondere Gewicht des heimlichen Zugriffs auf informationstechnische Systeme, und dieses Gewicht folgt schon aus der Infiltration, die das System für weitere Zugriffe öffnet.<sup>263</sup> Das trifft den abgegrenzten Eingriff ebenso, weil seine technische Begrenzung erst nach dem Eindringen wirkt. Dagegen lässt sich allerdings anführen, dass der Gesetzgeber das geringere Gewicht der Erhebung gerade durch die niedrigere

<sup>260</sup> BT-Drs. 21/7868, S. 33 f.

<sup>261</sup> BVerfGE 141, 220, Rn. 228 ff.

<sup>262</sup> BVerfG, Beschl. v. 24.6.2025, 1 BvR 180/23 (Trojaner II), Leitsätze 1 und 2a.

<sup>263</sup> BVerfGE 120, 274 (331 ff.); 162, 1, Rn. 214.

Schwelle abgebildet hat. Verfassungsrechtlich spricht deshalb viel für eine Vorabkontrolle, zwingend ist sie aber wohl nicht.

#### **d) Angriffsinfrastruktur (§ 24)**

Eine Sonderstellung nimmt der Eingriff zur Aufklärung von Angriffsinfrastruktur ein. § 24 Abs. 1 BVerfSchG-E erlaubt einen solchen Eingriff in Systeme auskunftspflichtiger Anbieter (§ 12), wenn Informationen über Angriffsspuren nicht ohne Gefährdung des Zwecks durch Übermittlung zu gewinnen sind. Die Befugnis entspricht dem heimlichen Zugang des BND zu Anbietersystemen (§ 32 Abs. 2 BNDG-E) und ist operativ nachvollziehbar, weil Angreifer gerade die Infrastruktur von Anbietern nutzen, deren Mitwirkung nicht immer rechtzeitig oder ohne Warnung des Angreifers zu erlangen ist. So existieren selbst in Deutschland Anbieter, die notorisch bekannt dafür sind, illegalen Diensteanbietern Speicher zu vermieten. Da durch die Maßnahme aber das System eines formal Unbeteiligten betroffen wird, während die Vorabkontrolle nur die Ausleitung einer Kopie erfasst (§ 34 Abs. 1 Nr. 8), sollte wie beim BND (vgl. unter B.III.2) auch der Eingriff selbst in den Katalog der vorabkontrollpflichtigen Maßnahmen aufgenommen werden. Absatz 2 erlaubt zudem, Angriffswerkzeuge und erbeutete Daten im System des Anbieters zu löschen, wenn polizeiliche Hilfe nicht rechtzeitig zu erlangen ist. Das ist eine digitale Abwehrhandlung, die sich an niemanden richtet und nichts durchsetzt – und damit keine operative Anschlussmaßnahme (vgl. unter C.VIII.2). Sie entspricht vielmehr der Abwehr während laufender Erfassung, die auch dem Auslandsdienst künftig gestattet werden soll (§ 31 Abs. 6 BNDG-E), und ist wie diese eine sinnvolle Eilbefugnis. Wer im System eines Anbieters Angriffswerkzeuge oder abgeflossene Daten findet, soll sie entfernen dürfen, bevor sie weiter genutzt werden. Ein Einverständnis des Anbieters zu verlangen, wäre nicht sachgerecht, weil Unternehmen es aus Sorge vor Haftungs- und Compliance-Risiken häufig nicht sofort erteilen dürften und die rasche Abwehr dann scheiterte. Wie beim BND (vgl. unter B.III.2) empfehlen wir aber zwei Konkretisierungen: Die Löschung sollte ausdrücklich auf die Angriffswerkzeuge und erbeuteten Daten beschränkt sein, deren Entfernung zur Abwehr erforderlich ist, und tatsächliche Anhaltspunkte für einen Angriff voraussetzen. Zudem sollte sie dokumentiert und dem UKRat nachträglich zur Einzelfallkontrolle vorgelegt werden. Den Anbieter sollte das BfV unterrichten, sobald das den Zweck der Maßnahme nicht mehr gefährdet. Für Systeme Dritter, auf die der Angriff zurückführt, gilt im Übrigen § 59.

#### **7. Heimliches Betreten von Wohnungen (§ 16 Abs. 6)**

§ 16 Abs. 6 S. 2 BVerfSchG-E erlaubt das heimliche Betreten von Wohnungen zur Vorbereitung und Durchführung eines nachrichtendienstlichen Mittels. Vorausgesetzt sind eine konkretisierte Gefahr für besonders gewichtige Rechtsgüter und eine besondere Anordnung, die der Vorabkontrolle durch den UKRat unterliegt (§ 34 Abs. 1 Nr. 1). Die Befugnis ist gleich gebaut wie § 18 Abs. 2 BNDG-E. Für ihre verfassungsrechtliche Einordnung, die Grenze zur Durchsuchung, die heimliche Inbesitznahme (§ 16 Abs. 1 S. 2 Nr. 4) und die Frage, wer die Vorabkontrolle ausübt, gilt deshalb das dort Gesagte, wonach es sich keinesfalls um eine skandalöse Maßnahme handelt (vgl. ausführlich unter B.I.5). Für das BfV bringt die Regelung zusätzlich einen Gewinn an Normenklarheit, da das heimliche Betreten im Schrifttum mitunter als unselbständige Annexmaßnahme verstanden wird,<sup>264</sup> ohne dass das geltende BVerfSchG dafür eine ausdrückliche bundesgesetzliche Ermächtigung enthält.

---

<sup>264</sup> Löffelmann, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, VI § 3 Rn. 42 (Betreten als unselbständige Begleitmaßnahme im Wege der Annexkompetenz); zum heimlichen Betreten zu Observationszwecken ebd., Rn. 88.

## 8. Wohnraumüberwachung, Einsatzsicherung (§§ 27, 28)

Die Wohnraumüberwachung (§ 27 BVerfSchG-E) ist an die dringende Gefahr, eine negative Kernbereichsprognose, die Subsidiarität gegenüber polizeilicher Hilfe und die Feststellung des Bundesverwaltungsgerichts gebunden (§ 34 Abs. 4), dessen Zuständigkeit aus Art. 13 Abs. 4 GG folgt. Erfolgt die Überwachung über ein informationstechnisches System, entscheidet folgerichtig allein das Gericht (§ 34 Abs. 4 S. 2). Die Regelungen sind insoweit streng an den verfassungsrichterlichen Vorgaben ausgerichtet. Die Einsatzsicherung nach § 28 Abs. 2 unterliegt dagegen keiner Vorabkontrolle; sollen die dabei erhobenen Daten für Gefahrenabwehr oder Strafverfolgung genutzt werden, bedarf das allerdings der Feststellung des Gerichts (§ 34 Abs. 4 S. 3). Stimmig ist das, solange die Erhebung auf den Schutz der eingesetzten Person beschränkt bleibt. Der Gesetzgeber sollte deshalb das Merkmal des unmittelbaren zeitlichen Zusammenhangs mit dem Einsatz (§ 28 Abs. 2 S. 1) noch konkretisieren.

Über die Datenerhebung zur Einsatzsicherung hinaus geht § 28 Abs. 1 BVerfSchG-E. Er erlaubt besonderen Vollzugskräften unmittelbaren Zwang zur Abwehr gegenwärtiger Gefahren für eingesetzte Personen und Sachen, auch zugunsten Dritter. Damit geht er über die bisherigen Durchsetzungsmittel der Eigensicherung aus § 26c Abs. 7 BVerfSchG hinaus (vgl. unter C.IX.3). Die Befugnis berührt das informationelle Trennungsprinzip nicht. Sie setzt keine Erkenntnisse aus der Aufklärung gegen Beobachtungsobjekte durch, sondern schützt die eigenen Kräfte vor einem gegenwärtigen Angriff auf Leben, körperliche Unversehrtheit, Freiheit oder Sachen von bedeutendem Wert. Kompetenzrechtlich lässt sie sich deshalb wie die Eigensicherung an die Aufgabe anbinden (vgl. unter C.VIII.1). Begrenzt ist sie zudem, weil besonders geschulte Vollzugskräfte vorausgesetzt werden und das UZwG nur eingeschränkt gilt (§ 28 Abs. 1 S. 3 und 4). Dass auch Gefahren für Dritte erfasst sind, die die Bediensteten im Einsatz feststellen (Satz 2), ändert daran nichts, weil der Staat seine Bediensteten nicht zu bloßen Zuschauern einer gegenwärtigen Gefahr machen kann. Im Ergebnis beendet diese explizite, sehr eng gefasste reine Schutznorm die Rechtsunsicherheiten einer bislang gelebten Praxis, die etwa bei Werbeversuchen oder Treffen mit Quellen auf Notwehr und Nothilfe angewiesen waren. Wir begrüßen die Regelung daher. Zu eng ist allerdings die Bindung an den Einsatz „nach diesem Unterabschnitt“. Bedienstete, die offen auftreten, etwa bei Befragungen, sind ebenso gefährdet, und ihr Schutz sollte nicht davon abhängen, ob eine Maßnahme verdeckt erfolgt. § 28 Abs. 1 sollte deshalb jede dienstliche Tätigkeit erfassen.

Im Zuge der expliziten Ausgestaltung von bereits heute durchgeführten Eigensicherungsmaßnahmen sollte auch der Personenschutz für besonders gefährdete Bedienstete ausdrücklich normiert werden, wie er heutzutage namentlich für die Amtsleitung bereits durch spezielle Kräfte des BfV erfolgt. Auch er folgt nicht auf nachrichtendienstliche Tätigkeit und begründet somit von vornherein keine operativen Anschlussbefugnisse. Eine Subsidiarität gegenüber der Polizei ist somit nicht geboten, zumal die Kapazitäten des polizeilichen Personenschutzes überaus stark begrenzt sind und eine polizeiliche Begleitung zu vertraulichen Terminen selbst Geheimhaltungsprobleme aufwürfe. Vorzusehen sind aber eine Gefährdungsfeststellung durch die Amtsleitung (bzw. bei dieser selbst durch das BMI), eine Unterrichtung der zuständigen Polizeibehörden<sup>265</sup> über die Anordnung und eine

---

<sup>265</sup> Bislang dürfte die zuständige Polizeibehörde jene des Wohnsitzes der Schutzperson sein. Dies sollte beibehalten und ggf. ergänzt werden um die Polizeien an den großen Dienstsitzen des BfV (PP Köln und LKA Berlin), weil dort ebenfalls Unterstützung angefordert werden könnte, auf die die landespolizeilichen Kräfte vorbereitet sein müssen.

Dienstvorschrift, für die das Gesetz Rahmenvorgaben macht, etwa zum geschützten Personenkreis, zur Dauer und zur Dokumentation. (Zur Bewaffnung der Vollzugskräfte vgl. C.IX.3.)

## 9. Kernbereich und Berufsgeheimnisträger (§§ 31, 32)

§ 31 BVerfSchG-E regelt den Kernbereichsschutz erstmals einheitlich für alle nachrichtendienstlichen Mittel. Für Maßnahmen, die nicht typischerweise in den Kernbereich vordringen, genügt dabei die Prüfung durch den Aufsichtsbediensteten innerhalb des BfV (Abs. 5 S. 2; bisheriger G 10-Jurist).<sup>266</sup> Ein Gewinn ist zudem, dass § 32 den Berufsgeheimnisschutz des § 3b G 10 auf alle Mittel erstreckt. Die Abstufung bleibt dabei erhalten: Absolut geschützt sind Geistliche, Verteidiger, Rechtsanwälte, Kammerrechtsbeistände und Abgeordnete (Abs. 1), relativ die übrigen Berufsgeheimnisträger des § 53 Abs. 1 S. 1 StPO, darunter Ärzte, Psychotherapeuten und Journalisten (Abs. 2). Das entspricht § 160a StPO, den das Bundesverfassungsgericht nicht beanstandet hat.<sup>267</sup> Die Kritik, der Entwurf nehme Heilberufe aus dem absoluten Schutz heraus, trifft deshalb nicht zu, denn diesem unterfielen sie nie.<sup>268</sup> Auch das BKAG-Urteil verlangt nichts anderes, weil es zwar die Unterscheidung zwischen Strafverteidigern und sonstigen Rechtsanwälten verworfen hat, nicht aber die Abstufung zwischen Berufsgruppen an sich.<sup>269</sup>

Dennoch ist Kritik an der aktuellen Regelung zu üben: Erstens ist der relative Schutz schwächer ausgeprägt, als er klingt. § 32 Abs. 2 setzt nur eine erheblich beobachtungsbedürftige Bedrohung voraus, und diese Stufe ist wegen § 3 Abs. 7 S. 4 der Regelfall (vgl. unter C.I.2). Zwar können Gespräche über Krankheit und seelisches Befinden höchstpersönliche Inhalte haben und damit in den nach § 31 absolut geschützten Kernbereich fallen. Allein die berufliche Beziehung oder das Gesprächsthema begründen diesen Schutz aber nicht.<sup>270</sup> Zweitens knüpft der Entwurf den geschützten Personenkreis an die Zeugnisverweigerungsrechte des § 53 StPO. Im Strafverfahren erklärt sich diese Anknüpfung daraus, dass § 160a StPO verhindern soll, dass verdeckte Ermittlungsmaßnahmen ein Zeugnisverweigerungsrecht umgehen. Die Nachrichtendienste können dagegen niemanden zur Aussage verpflichten. Der Schutz von Berufsgeheimnisträgern beruht hier deshalb nicht auf dem Umgehungsgedanken, sondern unmittelbar auf dem Gewicht der jeweiligen Vertrauensbeziehung.<sup>271</sup> Die strafprozessuale Auswahl führt dazu, dass etwa Berater außerhalb anerkannter Beratungsstellen, die kein Zeugnisverweigerungsrecht haben, in keinem der beiden Gesetze geschützt sind.<sup>272</sup> Für den Verfassungsschutz ist das keine Randfrage, denn der Entwurf schützt Aussteiger (§ 18 Abs. 1 S. 2 Nr. 3), ihre Berater aber nicht.

Ein Wechsel der Heilberufe in den absoluten Schutz ist entgegen diesbezüglichen Forderungen der Berufsverbände verfassungsrechtlich nicht geboten<sup>273</sup>. Klarstellen sollte das Gesetz aber, dass

<sup>266</sup> BVerfGE 141, 220, Rn. 129; BVerfGE 165, 1, Rn. 119 (Verzichtbarkeit einer unabhängigen Sichtung bei Vertrauenspersonen und verdeckt Ermittelnden, wenn andere Überprüfungsmöglichkeiten bestehen).

<sup>267</sup> BVerfGE 129, 208 (258 ff.).

<sup>268</sup> Bundesärztekammer, Stellungnahme v. 27.7.2026 zum Referentenentwurf; Kassenärztliche Bundesvereinigung, Stellungnahme v. 13.8.2026 zum Referentenentwurf v. 5.7.2026; zur Pressefreiheit DJV u.a., gemeinsame Stellungnahme v. 14.7.2026.

<sup>269</sup> BVerfGE 141, 220, Rn. 256 f.

<sup>270</sup> BVerfGE 109, 279 (322 f.); 141, 220, Rn. 121; zu § 100d StPO, der im Einzelfall auch Vertrauensverhältnisse zu Ärzten erfasst, BT-Drs. 18/12785, S. 56, wiedergegeben in BVerfG, Beschl. v. 24.6.2025, 1 BvR 180/23 (Trojaner II), Rn. 19.

<sup>271</sup> Löffelmann, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, VI § 4 Rn. 58, dort auch zur fehlenden verfassungsrechtlichen Gebotenheit der über den Kernbereichsschutz hinausgehenden Einschränkungen.

<sup>272</sup> Zur fehlenden verfassungsrechtlichen Pflicht, Sozialarbeitern ein Zeugnisverweigerungsrecht einzuräumen, vgl. BVerfGE 33, 367.

<sup>273</sup> So etwa Bundespsychotherapeutenkammer, Stellungnahme zum Gesetzentwurf v. 31.8.2026, S. 4 f.; Bundesärztekammer, Stellungnahme zum Gesetzentwurf v. 6.10.2026, S. 3 ff.; Kassenärztliche Bundesvereinigung, Stellungnahme v.

psychotherapeutische Sitzungen und vergleichbar höchstpersönliche Behandlungsinhalte dem absoluten Kernbereichsschutz des § 31 unterfallen. Im Übrigen empfehlen wir aus rechtspolitischer Sicht zwei Änderungen. Zum einen sollten Maßnahmen nach § 32 Abs. 2 gegen Heilberufe erst zur Aufklärung besonders erheblich beobachtungsbedürftiger Bedrohungen zulässig sein, also auf der Stufe, auf der auch Online-Durchsuchung und Telekommunikationsüberwachung zulässig sind. Zum anderen sollten die Berater staatlich anerkannter oder geförderter Ausstiegs- und Distanzierungsprogramme in den relativen Schutz aufgenommen werden, weil ihr Kreis bestimmbar und für den Auftrag des BfV unmittelbar relevant ist. Zum Schutz der Heilberufe gegenüber dem BND siehe B.II.

Die Verstrickungsklausel (§ 32 Abs. 4 BVerfSchG-E) gilt künftig für alle nachrichtendienstlichen Mittel. Der Schutz entfällt, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Person an der Bedrohung beteiligt ist. Beteiligter ist nach § 3 Abs. 5 Nr. 2 dabei auch, wer eine Bestrebung nachdrücklich unterstützt. Nach der Gesetzesbegründung soll die objektive Förderung genügen, während es auf Wissen und Wollen des Unterstützers grundsätzlich nicht ankomme. Zwar heißt es, Absatz 4 entspreche der bisherigen Verstrickungsregelung.<sup>274</sup> Das trifft nur teilweise zu. § 3b Abs. 4 G 10 hob den Schutz auf, wenn die zeugnisverweigerungsberechtigte Person selbst Verdächtige einer Katalogtat war oder tatsächliche Anhaltspunkte dafür bestanden, dass sie die Bestrebungen durch Entgegennahme oder Weitergabe von Mitteilungen bewusst unterstützte.<sup>275</sup> Beide Alternativen setzten vorsätzliches Verhalten voraus. Neu ist insofern nicht der Begriff der nachdrücklichen Unterstützung – das geltende Recht verwendet ihn für das Handeln für einen Personenzusammenschluss (§ 4 Abs. 1 S. 2 BVerfSchG) bereits heute –, sondern seine Verwendung in der Verstrickungsklausel, durch die künftig eine objektive Förderung genügt. Zumindest für bestimmte Berufe wie diejenigen von Journalisten geht der Wegfall des subjektiven Elements zu weit, weil schon ihre Berichterstattung eine Bestrebung objektiv fördern kann. Das Gesetz sollte deshalb klarstellen, dass ordnungsgemäße berufstypische Tätigkeiten wie Beratung, Vertretung, Beurkundung, Behandlung oder journalistische Recherche für sich allein keine Verstrickung begründen. Für den Wegfall des besonderen Berufsgeheimnisschutzes sollte zudem eine objektiv wesentliche und konkret gefahrenerhebliche Förderung erforderlich sein. Keine Absenkung liegt dagegen in der Wortwahl zur Gefahrenvorfeldschwelle: Nach überwiegender Auffassung entspricht der sprachlichen Differenzierung zwischen „tatsächlichen Anhaltspunkten“ und „Tatsachen, die die Annahme rechtfertigen“ keine inhaltliche Differenzierung der Eingriffsschwellen, sodass beide Formulierungen die im Ergebnis gleichartige Schwelle bezeichnen.<sup>276</sup>

## V. Anordnung, Vorabkontrolle, Mitteilung (§§ 33–35)

Wer ein Mittel anordnen darf, entscheidet sich nach dem Regierungsentwurf künftig gemäß der avisierten Eingriffsstufe. § 33 BVerfSchG-E verteilt die Zuständigkeit dabei praxistauglich zwischen Amts- und Abteilungsleitung. Abteilungsleiter im BfV sind hinreichend erfahren und auch mit den politischen Implikationen ihrer Anordnungen vertraut, um für das gesamte Haus Handlungen vorzunehmen. Der Katalog der Vorabkontrolle (§ 34 Abs. 1) ist umfangreich, aber nicht lückenlos.<sup>277</sup>

---

13.8.2026 zum Referentenentwurf v. 5.7.2026; DGPPN/DGKJP/DGPM, Stellungnahme zum Regierungsentwurf v. 9.9.2026.

<sup>274</sup> Begr. zu § 32 Abs. 4 BVerfSchG-E, BT-Drs. 21/7868, S. 272, dort mit Verweis auf „§ 3 Absatz 4 G 10“; gemeint ist § 3b Abs. 4 G 10.

<sup>275</sup> § 3b Abs. 4 G 10 (geltende Fassung).

<sup>276</sup> Vgl. Tabbara, GSZ 2022, 215.

<sup>277</sup> Ebenso Höning, VerfBlog v. 14.8.2026 (Fn. oben). Kritisch zur Zuweisung von Vorabkontrollen an das Bundesverwaltungsgericht (§ 34 Abs. 4 und 5 BVerfSchG-E) Kraft, VerfBlog v. 2.9.2026 (Fn. oben).

Neben dem abgegrenzten Eingriff nach § 26 Abs. 1 (C.IV.6) sollte der Gesetzgeber zumindest rechtspolitisch auch die Observationen der ersten Steigerungsstufe (§ 20 Abs. 1), die Standortfeststellung (§ 21 Abs. 1 Nr. 1) und den Eingriff in Anbietersysteme (§ 24 Abs. 1) der Vorabkontrolle unterstellen, auch wenn die Rechtsprechung hier weniger eindeutig ist. Jede Erweiterung verlangt allerdings Personal und ist nur mit einer angepassten Ausstattung des UKRats sinnvoll (vgl. unter D.XVII).

Neu ist zudem, dass vorbereitende technische Eingriffe in die Integrität eines Systems schon vor der Anordnung zulässig sind, wenn sonst der Erfolg gefährdet wäre (§ 33 Abs. 1 S. 2). Daten dürfen dabei zwar nicht erhoben werden. Der Sache nach erlaubt die Norm aber, ein System zu infiltrieren, bevor die Maßnahme genehmigt ist. Das mag technisch geboten sein, und der Ausschluss der Datenerhebung begrenzt den Eingriff. Aus rechtspolitischer Sicht sollte sie aber dokumentiert und dem UKRat mit der Anordnung vorgelegt werden. Spät setzt zudem die Kontrolle von Erstreckungen ein. Erstreckt das BfV eine Maßnahme auf Grundlage eines Zusatzes nach § 33 Abs. 3 auf weitere Personen oder Anschlüsse, muss es diese Vorgänge dem UKRat nach § 34 Abs. 2 erst mit Ablauf der Anordnung zur Entscheidung über die Rechtmäßigkeit vorlegen. Für mehrere Maßnahmen lässt § 33 Abs. 4 dafür bis zu ein Jahr zu. Das BNDG-E verlangt dagegen die unverzügliche Vorlage (§ 97 Abs. 3 BNDG-E, B.IX.1). Die vorherige Genehmigung des Erstreckungsvorbehalts ist nicht dasselbe wie die Kontrolle seines Einsatzes gegen weitere Personen oder Anschlüsse. Wir empfehlen die unverzügliche Vorlage der einzelnen Erstreckungsvorgänge und klare Folgen einer unzulässigen Erstreckung, nicht aber eine erneute Vorabgenehmigung jeder Erstreckung.<sup>278</sup>

Für den Eilvollzug (§ 34 Abs. 3 BVerfSchG-E i.V.m. § 31 UKRatG-E) gilt das unter D.IX Gesagte. Die Frist von drei Werktagen läuft danach erst ab der Vorlage, und der UKRat kann einen Fortgeltungsbeschluss fassen. Großzügiger ist die Übergangsregelung des § 79 Abs. 2 BVerfSchG-E. Sie erlaubt für ein Jahr ab der Verkündung Anordnungen nach altem Recht ohne Vorabkontrolle. Ausgenommen sind nur Eingriffe in das Brief-, Post- und Telekommunikationsgeheimnis einschließlich qualifizierter Auskünfte, Eingriffe in private informationstechnische Systeme und die Wohnraumüberwachung. Für Observationen und Vertrauenspersonen verlängert dies zwar jenen Zustand, den das Bundesverfassungsgericht bereits im Jahr 2022 andernorts beanstandet hatte. Die Begründung verweist allerdings zutreffend darauf, dass sich auch der UKRat auf die neue Rechtslage einstellen muss.<sup>279</sup> Vor allem in Ansehung seiner derzeit noch zu knappen Ausstattung (vgl. unter D.XVII) wäre mit einer sofortigen Unterwerfung aller Maßnahmen unter die Vorabkontrolle wenig gewonnen; jedenfalls aus rechtspolitischer Sicht sollte allerdings die Frist für Vertrauenspersonen verkürzt werden, deren Einsatz besonders häufig über Jahre läuft und in der Vergangenheit bei fehlerhafter Personenauswahl oder -führung den Verfassungsschutzverbund schwer in der Öffentlichkeit belastet hat.

Die Mitteilung an Betroffene regelt § 35 BVerfSchG-E neu. Die Grundstruktur folgt § 12 G 10: Mitteilung nach Einstellung der Maßnahme, Zurückstellung bei Gefährdung ihres Zwecks oder bei Nachteilen für das Staatswohl und Zustimmung des UKRats zu einer Zurückstellung über zwölf Monate hinaus (Abs. 3, Abs. 5 Nr. 2). Als Neuerung trifft indes das Entfallen der Mitteilungspflicht von vornherein hinzu, wenn bei der Spionageabwehr nicht nachträglich ausgeschlossen werden kann, dass eine Tätigkeit für eine fremde Macht vorlag, oder wenn eine verdeckt eingesetzte Person beteiligt war und ihre Enttarnung nicht ausgeschlossen werden kann (Abs. 2 Nr. 2 und 3). Das entspricht in

<sup>278</sup> BT-Drs. 21/7868, S. 36 f., 134 f.

<sup>279</sup> Begr. zu § 79 BVerfSchG-E, BT-Drs. 21/7868, S. 319.

der Sache § 100 Abs. 4 S. 1 Nr. 1 und 2 BNDG-E (vgl. unter B.III.6). Anders als dort bedarf die Nichtmitteilung im Fall der verdeckt eingesetzten Person allerdings der Zustimmung des UKRats (Abs. 5 Nr. 1), was erfreulich ist. Darüber hinaus soll das endgültige Absehen von der Mitteilung erleichtert werden. Nach § 12 Abs. 1 S. 5 G 10 musste die G 10-Kommission einstimmig feststellen, dass der Zurückstellungsgrund fünf Jahre nach Beendigung der Maßnahme noch vorliegt und mit an Sicherheit grenzender Wahrscheinlichkeit auch künftig vorliegen wird.<sup>280</sup> Künftig genügt dagegen, dass die Gründe der Zurückstellung auf absehbare Zeit erwartbar fortbestehen. Zudem ist die Zustimmung des UKRats nicht an Einstimmigkeit gebunden (Abs. 4 Nr. 2, Abs. 5 Nr. 1). Die Mitteilung ist aber Voraussetzung nachträglichen Rechtsschutzes, und bei der Telekommunikationsüberwachung bleibt der Rechtsweg bis zur Mitteilung sogar ganz ausgeschlossen (§ 22 Abs. 5). Angesichts der Eingriffsschwere wäre eine Beibehaltung des Prognosemaßstab aus dem G 10 rechtssicherer.

## VI. Weiterverarbeitung (§§ 36–44)

Gleichermaßen neu wie für die Arbeit des Inlandsdienstes von sehr hoher Relevanz ist die qualifizierte Auswertung nach § 37 BVerfSchG-E – gewissermaßen die Antwort auf das Urteil zur automatisierten Datenanalyse.<sup>281</sup> Nach Absatz 2 ordnet sie die Suche nach Anhaltspunkten gegen bislang Unverdächtige, das Erstellen von Persönlichkeitsprofilen und den Einsatz anpassungsfähiger, auf autonomen Betrieb angelegter Systeme der ersten Steigerungsstufe (erhebliche Bedrohungen) zu. Die Gewinnung besonders privater Erkenntnisse ist auf besonders erhebliche Bedrohungen als Spitzenstufe beschränkt. Die Stufung nach Eingriffsgewicht ist im Ansatz richtig. Zweifel begründet aber die Zuordnung der ersten Gruppe. Für polizeiliche Analysen, die den Kreis der Betroffenen über Verdächtige hinaus erweitern oder komplexe Verfahren einsetzen, hat das Bundesverfassungsgericht nämlich sogar eine konkretisierte Gefahr verlangt.<sup>282</sup> Ob das auf das nachrichtendienstliche Vorfeld übertragbar ist, hat das Gericht zwar nicht entschieden und es spricht im Hinblick auf die deutlich geringeren Folgeeinwirkungsmöglichkeiten des BfV auf den Betroffenen auch einiges gegen eine jedenfalls unangepasste Übertragung. Für die niedrigeren Schwelle lässt sich zudem die Aufgabe der Früherkennung ins Felde führen. Solange die erste Steigerungsstufe nach § 3 Abs. 7 S. 4 aber faktisch der Regelfall ist (vgl. unter C.I.2), wäre es sehr zu empfehlen, die Verdachtsgewinnung gegen Unverdächtige und selbstlernende Systeme der Spitzenstufe zuzuordnen.

Mindestens ebenso wichtig wie die Einführung passender rechtlichen Schwellen ist die Sicherung der eingesetzten Technik. Setzt das BfV Analyseplattformen externer, insbesondere EU-ausländischer Anbieter ein, steigt das abstrakte Risiko von Informationsabflüssen durch Hersteller und die hinter ihnen stehenden Herkunftsstaaten. Dies stellt, wenn ein erforderliches, hohes Maß an operativer Sicherheit technisch unerreicht bleibt, nicht nur ein erhebliches politischer Problem dar, sondern wirft auch verfassungsrechtliche Fragen auf. Bislang sehen die Nachrichtendienstgesetze kaum, und wenn überhaupt nur maximal abstrakte, Vorgaben zur operativen Informationssicherheit vor. Dadurch ist es für Bürger jedoch nicht möglich, das Schutzniveau der durch den Dienst mittels Drittsoftware verarbeiteter Daten zu erblicken, weil diesbezügliche Dienstvorschriften nichtöffentlich sind. Spätestens durch die jetzige Novelle mit ihrer teils enormen Ausweitung digitaler Eingriffs- und Abfragebefugnisse tut es not, Mindestvorgaben im Gesetz zu statuieren. Dies ist im Wesentlichen auf drei Arten möglich: Erstens kann der Anbieter einer Software die Einsicht in ihren Quellcode zum Zwecke einer verfassungsschutzseitigen Sicherheitsprüfung gewähren, was wohl vor allem bei

<sup>280</sup> § 12 Abs. 1 S. 5 G 10 (geltende Fassung).

<sup>281</sup> Vgl. BVerfGE 165, 363.

<sup>282</sup> BVerfGE 165, 363, Rn. 105 ff.

Anbietern im EU-Raum mitunter ermöglicht wird, um einen Mehrwert zu technisch überlegenen US-Produkten zu generieren. Zweitens kann das System, wenn eine solche tiefgehende technische Untersuchung anbieterseitig nicht gestattet wird, „air gapped“ betrieben werden, also nur innerhalb eines vom Internet oder anderen ausgehenden Verbindungen streng isolierten Binnennetzes.<sup>283</sup> Es kann aber Systeme geben, bei denen eine Anbindung an das Internet nicht ausgeschlossen werden kann, weil gerade darin ihr Zweck liegt, so etwa bei Tools wie PimEyes, die (in diesem Fall: biometrische) Massenabgleiche aus offenen Quellen vornehmen; bekannt geworden durch das Aufspüren der früheren RAF-Terroristin Daniela Klette durch Journalisten. Was in diesem dritten Fall an Schutzvorkehrungen bleibt, ist eher eine Notlösung: Gesuchte Kennungen werden mit unzähligen erfundenen oder belanglosen Daten eingespeist, damit der Anbieter nicht erkennt, für wen sich der Dienst interessiert. Solche Randomisierungen sollte das Gesetz jedoch nur für Maßnahmen von einfachem und allenfalls mittlerem Eingriffsgewicht vorsehen, wohingegen etwa die Verarbeitung heimlich gewonnener Telekommunikationsüberwachungsdaten über Internet-verknüpfte Tools selbst bei Randomisierung durch Vermischung mit anderen Datensätzen unverhältnismäßig würde. All das sollte das Gesetz im Grundsatz aufgreifen und dann nur die nähere Ausgestaltung dienstinterner Vorschriften überlassen.

Für Anwendungen, die anpassungsfähig auf einen autonomen Betrieb angelegt sind, enthält § 37 Abs. 7 bereits Anforderungen unter anderem an Genauigkeit, Robustheit, Cybersicherheit, Nichtdiskriminierung und stichprobenartige Funktionsprüfungen sowie an die Beschaffung aus Drittstaaten.<sup>284</sup> Ergänzend sollten für Anwendungen nach Absatz 2 eine prüffähige technische Dokumentation und eine wirksame Prüfung des konkreten Einsatzes durch den UKRat vorgesehen werden. Den Überblick für seine strukturbezogene Kontrolle gäbe dem UKRat ein Anwendungsregister, in dem jede Anwendung vor ihrem ersten Einsatz mit Zweck, Datenbasis und Betriebsform angemeldet wird. Für § 53 BNDG-E sollte dasselbe gelten. Er würde sofern weniger die gerichtsähnliche Aufgabe als diejenige allgemeine Datenschutzaufsicht, die er von der BfDI übernimmt, stärken. § 37 Abs. 6 erlaubt zudem, Schutzmaßnahmen nach § 59 Abs. 2 S. 1 Nr. 1 lit. b und d zur Abwehr eines informationstechnischen Angriffs automatisiert zu veranlassen, deren zusätzliche Voraussetzungen maßgeblich bleiben. Für sie gilt das zu § 53 Abs. 7 BNDG-E und zur Grenze zwischen Erzeugung und Verwendung Gesagte entsprechend (vgl. dazu unter B.VII).

Eine weitere Neuerung der Weiterverarbeitung betrifft die Speicherdauer. Nach § 38 Abs. 3 S. 1 Nr. 3 BVerfSchG-E sind Daten über verfassungsfeindliche Bestrebungen spätestens nach 15 Jahren zu löschen, gerechnet ab der letzten Information, die die Speicherung begründet (Abs. 4). Das geltende Recht setzt diese Grenze bei zehn Jahren und lässt Ausnahmen nur auf Entscheidung der Abteilungsleitung im Einzelfall zu.<sup>285</sup> Die Begründung stützt die Verlängerung darauf, dass der Verfassungsschutz längerfristige Phänomene aufklärt und länger zurückliegende Vorgänge wiederholt bedeutsam geworden sind. Als Beispiele nennt sie den NSU-Komplex, das Oktoberfestattentat, den Anschlag auf Henriette Reker und den Mordfall Lübcke.<sup>286</sup> Dieser Befund ist ernst zu nehmen, denn gerade im gewaltorientierten Extremismus können Personen über Jahre unauffällig bleiben und später wieder in Erscheinung treten. Die Verlängerung der Regelfrist tragen die Beispiele aber nur

<sup>283</sup> So hat es das BfV in der Vergangenheit etwa mit der NSA-Applikation „xKeyscore“ gehalten, weil der US-amerikanische Signalerfassungsdienst als Entwickler den deutschen Partnerbehörden naheliegenderweise keinen vollständigen IT-Einblick zugestehen wollte, vgl. Aussagen der Zeugin Monika Genkova (BfV) gemäß Stenografischem Protokoll der 89. Sitzung des 1. PUA der 18. WP des BT v. 25.2.2016, S. 97 ff.

<sup>284</sup> BT-Drs. 21/7868, S. 40 f.

<sup>285</sup> § 12 Abs. 3 S. 2 BVerfSchG (geltende Fassung).

<sup>286</sup> Begr. zu § 38 Abs. 3 BVerfSchG-E, BT-Drs. 21/7868, S. 291 f.

bedingt. So stützte sich die Aufarbeitung des NSU-Komplexes nach der Begründung selbst auf Sachakten, für die § 38 nach seinem Absatz 5 nicht gilt. Im Fall des Anschlags auf Henriette Reker wiederum lagen die älteren Informationen über den Täter bei einer zivilgesellschaftlichen Organisation und nicht im Verfassungsschutzverbund. Für den Einzelfall, in dem ältere Erkenntnisse erkennbar bedeutsam bleiben, genügt zudem die Ausnahme durch die Abteilungsleitung, die schon das geltende Recht kennt und die der Entwurf beibehält (§ 38 Abs. 3 S. 3). Im Ergebnis kehrt die Verlängerung damit vor allem das Verhältnis von Regel und Ausnahme um. Das ist nicht unerheblich, weil das Gewicht einer Speicherung mit ihrer Dauer wächst.<sup>287</sup> Aus rechtspolitischer Sicht sollte es deshalb bei der Regelfrist von zehn Jahren bleiben. Jedenfalls aber sollte nach zehn Jahren eine dokumentierte Einzelfallprüfung vorgeschrieben werden, die die weitere Erforderlichkeit begründet. Klarzustellen ist zudem, dass die Löschpflichten des § 38 auch pseudonymisierte Daten erfassen. § 36 Abs. 3 nimmt sie nur von den Speichervoraussetzungen des Absatzes 2 aus, und ihr Personenbezug lässt sich unter den Voraussetzungen des § 36 Abs. 2 S. 1 Nr. 1 wiederherstellen. Unbefristet und ohne Bedrohungsbezug dürfen sie deshalb nicht vorgehalten werden.

## VII. Übermittlung (§§ 45–58)

Das Übermittlungsregime der §§ 46–58 BVerfSchG-E übernimmt vielfach das geltende Recht, weicht aber in zwei Punkten ab. Zum einen ordnet § 47 Übermittlungen für Aufgaben nach den Versammlungsgesetzen (Abs. 1 Nr. 3 lit. c) und zur Untersagung der Ausreise (Nr. 5) neu dem administrativen Rechtsgüterschutz zu. Für die Neuregelung spricht der Präventionsbedarf der entsprechenden Behörden. Die Begründung stützt sie zudem darauf, dass die Schwellen des Bundesverfassungsgerichts auch bei personen- oder gruppenbezogener Risikoprävention erfüllt sein können.<sup>288</sup> Diesen nachvollziehbaren Wertungen steht allerdings der Maßstab des HVSG-Beschlusses entgegen, nach dem unterhalb der konkretisierten Gefahr nur übermittelt werden darf, wenn die Empfängerentscheidung keine operative Anschlussmaßnahme ist.<sup>289</sup> Das Gericht stellt dabei zwar grundsätzlich auf die Ausstattung der empfangenden Stelle ab und nicht nur auf die konkret drohende Folgemaßnahme innerhalb der empfangenden Stelle (vgl. unter C.VIII.2). Dass sie diesen Maßstab selbst nicht durchhalten, beweisen die Karlsruher Richter allerdings an anderer Stelle selbst, wenn sie Übermittlungen zur personen- oder gruppenbezogenen Risikoprävention schon bei tatsächlichen Anhaltspunkten für Zuverlässigkeitsprüfungen im Waffenrecht zulassen, obwohl die Waffenbehörden im Übrigen über Zwangsbefugnisse verfügen.<sup>290</sup> Zumindest die Untersagung der Ausreise ist dagegen ein unmittelbar freiheitsbeschränkender Eingriff in Art. 8 GG und Art. 2 Abs. 1 GG und keine bloße Risikoprävention. Ihre Zuordnung zum administrativen Rechtsgüterschutz ist deshalb verfassungsrechtlich nicht gesichert. Ob dies auch auf ein Versammlungsverbot oder eine beschränkende Verfügung zutrifft, scheint weniger sicher, weil hier exekutive Folgemaßnahmen erst mittelbar als eigenständige Folge auf eine Verweigerung des Beschränkten anzuordnen sind. Zumindest für die Ausreiseversagungen sollten Übermittlungen weiterhin eine konkretisierte Gefahr voraussetzen. Einen anderen Mangel weisen die Nummern 8 und 9 auf. Das geltende Recht beschränkt die Übermittlung an die Finanzdienstleistungsaufsicht auf den Schutz vor Terrorismusfinanzierung, der Entwurf öffnet sie für die gesamte Aufsicht und stellt die Gewerbeaufsicht daneben.<sup>291</sup> Die enge Verbindung zu den Schutzgütern des Verfassungsschutzes, die das

<sup>287</sup> Vgl. BVerfGE 125, 260, Rn. 215 zur Bedeutung der Speicherdauer.

<sup>288</sup> BVerfGE 169, 130, Rn. 106 ff., 113.

<sup>289</sup> BVerfGE 169, 130, Rn. 106 f.

<sup>290</sup> BVerfGE 169, 130, Rn. 112 f.

<sup>291</sup> § 20 Abs. 1 S. 1 Nr. 7 BVerfSchG (geltende Fassung).

Bundesverfassungsgericht für Übermittlungen unterhalb der konkretisierten Gefahr verlangt, muss im Normtext erhalten bleiben, etwa durch die Beschränkung auf die Terrorismusfinanzierung und auf das Sicherheitsgewerbe.

Zum anderen ändert die Novelle die Pflicht des BfV, Anfragen zu beantworten. Nach geltendem Recht *muss* es in gesetzlich besonders geregelten Anfrageverfahren seine Erkenntnisse übermitteln, etwa bei der waffenrechtlichen Regelanfrage (§ 20 Abs. 1 S. 2 BVerfSchG). Dasselbe gilt für jedes Ersuchen einer Stelle, die eine begünstigende Maßnahme vorbereitet, durchführt oder überprüft, etwa eine Förderentscheidung (§ 20 Abs. 2 S. 2 BVerfSchG). Der Entwurf übernimmt nur die erste Pflicht und erstreckt sie auf besonders geregelte Anfrageverfahren bei begünstigenden Maßnahmen (§ 47 Abs. 3). Auf gewöhnliche Ersuchen zu begünstigenden Maßnahmen *darf* das BfV dagegen künftig nur noch übermitteln (§ 47 Abs. 2), und die Begründung stellt ausdrücklich klar, dass ihn keine Übermittlungspflicht mehr trifft. Das überzeugt nicht. Über begünstigende Leistungen entscheidet nicht der Inlandsdienst, sondern die zuständige Stelle. Sie trägt nach der Begründung auch die Verantwortung für die Veranlassung ihres Ersuchens, während das BfV nur prüft, ob es einem gesetzlichen Zweck dient und ob ein Übermittlungsverbot entgegensteht (Doppeltürprinzip).<sup>292</sup> Die übermittelten Erkenntnisse muss sie selbst würdigen, mit den übrigen Gesichtspunkten abwägen und den Betroffenen, soweit der Geheimschutz es zulässt, Gelegenheit zur Stellungnahme geben. Ein Ermessen des BfV, ob es auf ein solches Ersuchen antwortet, passt in diese Verteilung der Verantwortung nicht hinein. Es wiese dem BfV eine Bewertung zu, die ihm nicht zusteht, nämlich darüber, wer „wirklich“ überprüft werden soll, und macht den Inlandsdienst zugleich zum eigenständigen Akteur in den Förderverfahren, was ihm (auch medial) nicht gut zu Gesicht stände. Der Gesetzgeber sollte die Pflicht des geltenden § 20 Abs. 2 S. 2 BVerfSchG deshalb in § 47 Abs. 3 aufnehmen.<sup>293</sup>

## VIII. Schutzmaßnahmen (§§ 59–62)

### 1. Tatbestand, Maßnahmenkatalog

Die Schutzmaßnahmen stehen im Mittelpunkt der öffentlichen Debatte, in der teils von einer Geheimpolizei die Rede ist. In ihrem Umfang fallen sie aber tatsächlich moderat aus. Nach § 59 soll das BfV verdeckt auf Gegenstände einwirken können, die für eine Bedrohung eingesetzt werden, wenn das im Sinne der Subsidiarität zur Polizei erforderlich ist, um eine von einer besonderen Bedrohung ausgehende Gefährdung eines besonders gewichtigen Rechtsguts abzuwenden (Abs. 1 S. 1). Als besondere Bedrohungen gelten terroristische Bestrebungen mit Unruhepotenzial und systematische sicherheitsgefährdende oder geheimdienstliche Tätigkeiten fremder Mächte, die besonders schwere Schäden befürchten lassen (Abs. 3). Der Katalog der Maßnahmen sieht neben der Beeinträchtigung von Tatmitteln in der Realwelt auch cybergestützte Schritte wie die Umleitung und Veränderung von Verkehren und das Platzieren von falschen Informationen vor (Abs. 2). Die Amtsleitung stuft die Bedrohung für höchstens ein Jahr ein. Wirksam wird die Einstufung erst, wenn der UKRat ihre Rechtmäßigkeit festgestellt hat (§ 60 Abs. 2).

<sup>292</sup>Begr. zu § 47 BVerfSchG-E, BT-Drs. 21/7868, S. 296.

<sup>293</sup> § 20 Abs. 1 S. 2, Abs. 2 S. 2 BVerfSchG; BT-Drs. 21/7868, S. 47 und 299 (Begr. zu § 47 Abs. 3 BVerfSchG-E).

Der Bedarf ist im Ansatz nachvollziehbar, wenn auch deutlich weniger als beim BND für im Ausland erfolgende erweiterte Maßnahmen nach § 51 BNDG-E, die zur Behauptung Deutschlands im „Schattenkrieg“ insbesondere gegen die Russische Föderation schlagend sein können. Der Bedarf des BfV liegt demgegenüber eher in Randbereichen und Sonderkonstellationen seiner Arbeit. Stoßen Verfassungsschützer beispielsweise auf Tatmittel einer fremden Macht wie ein Waffenlager, dürfen sie es bislang nicht unschädlich machen, sondern müssen die Polizei hinzuziehen. Gleiches gilt für Server, von denen aus fremde Geheimdienste Angriffe auf Kritische Infrastrukturen in der Bundesrepublik durchführen. Dies wird als misslich empfunden, weil entweder eine rechtzeitige Entschaltung der Polizeibehörden nicht mehr gewährleistet werden kann oder weil aus anderem Grunde eine Herbeirufung nicht möglich ist – als Beispiel werden unter der Third Party Rule übermittelte Informationen genannt. Klärungsbedürftig ist im Tatbestand die „Bereitstellung falscher Informationen für Beteiligte“ (Abs. 2 S. 1 Nr. 1 lit. c). Systematisch ist sie ein Regelbeispiel des Einwirkens auf Gegenstände, ihrem Wortlaut nach erfasst sie aber jede Täuschung von Beteiligten. Die Begründung versteht sie enger als Fehlleitung von Angreifern in unschädliche Handlungen.<sup>294</sup> Weil Beteiligte an Bestrebungen auch Parteien oder deren Umfeld sein können, würde der weite Wortlaut Fragen nach Art. 21 GG und dem staatlichen Neutralitätsgebot auf. Aus „rechtshandwerklicher“ Sicht sollte das Verständnis der Begründung deshalb in den Normtext übernommen werden.

## 2. Verhältnismäßigkeit auf Schwellenebene

Mit den Schutzmaßnahmen entfallen zugleich die Trennungsklauseln des § 8 Abs. 3 des geltenden BVerfSchG und des § 2 Abs. 3 des geltenden BNDG. Sie schlossen polizeiliche Befugnisse aus und untersagten Amtshilfeersuchen an die Polizei für Maßnahmen, zu denen der Dienst selbst nicht befugt ist.<sup>295</sup> Es bleibt nur das Angliederungsverbot (§ 1 Abs. 2 S. 3 BVerfSchG-E). Gegen den Wegfall spricht die Signalwirkung einer Klausel, die so alt ist wie das Gesetz.<sup>296</sup> Der Hinweis, ein Ausschluss polizeilicher Befugnisse wäre angesichts der §§ 28 und 59 BVerfSchG-E unrichtig geworden, beschreibt nur die Änderung, rechtfertigt sie aber nicht.<sup>297</sup> Tragen muss die Streichung eine sachliche und kompetenzrechtliche Begründung für die konkret vorgesehenen Befugnisse. Für die Schutzmaßnahmen sehen wir sie nur teilweise (vgl. unter C.VIII.3), für die Löschung von Angriffswerkzeugen nach § 24 Abs. 2 nur unter engen Voraussetzungen (vgl. unter C.IV.6.d). Die Befugnisse zur Einsatzsicherung (§ 28 Abs. 1) und zur Drohnenabwehr (§ 65) dienen dagegen vorrangig dem Schutz der eingesetzten Kräfte und lassen sich insoweit an die Aufgabe anbinden (vgl. unter C.IV.8, C.IX.1, C.IX.3).

Maßstab für die Schwelle der Schutzmaßnahmen ist gleichwohl nicht das Trennungsgebot als solches. Es ist im Grundgesetz nicht ausdrücklich verankert, und das Bundesverfassungsgericht hat ihm bislang keinen selbständigen Prüfungsmaßstab entnommen.<sup>298</sup> Insoweit teilen wir die Skepsis der Gesetzesbegründung, die die Trennung als organisatorische Sicherung der Erkenntnisqualität versteht und auf Mischbehörden in Österreich, Schweden oder den Vereinigten Staaten verweist.<sup>299</sup>

<sup>294</sup>Begr. zu § 59 Abs. 2 S. 1 Nr. 1 lit. c BVerfSchG-E, BT-Drs. 21/7868, S. 307.

<sup>295</sup>§ 8 Abs. 3 BVerfSchG, § 2 Abs. 3 BNDG (jeweils geltende Fassung).

<sup>296</sup>Dietrich, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, III § 3 Rn. 61.

<sup>297</sup>Ebenso Timu, VerfBlog v. 27.8.2026 (Fn. oben), der zwischen organisatorischer, funktioneller, befugnisrechtlicher und informationeller Trennung unterscheidet; zum Verhältnis von Trennungsgebot und Kooperationsgebot Friehe/Wallrath, NVwZ 2025, 201 (201). Zur einfachgesetzlichen Natur des Trennungsgebots Manns, ZRP 2026, 63 (63 f.).

<sup>298</sup>BVerfGE 133, 277, Rn. 113 (Aufgliederung der Sicherheitsbehörden), 123 (informationelles Trennungsprinzip). Zum Polizeibrief und zum umstrittenen verfassungsrechtlichen Rang Dietrich, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, III § 3 Rn. 35, 59.

<sup>299</sup>Begr. zu § 2 Abs. 2 BVerfSchG-E, BT-Drs. 21/7868, S. 209 ff.

Der Rechtsvergleich trägt allerdings als solches nicht die geplanten Schutzmaßnahmen, weil die genannten Behörden ihre gefahrenabwehrenden Aufgaben unter polizeirechtlichen Schwellen und mit polizeirechtlichem Rechtsschutz wahrnehmen. Gerade diese Kombination einer „Intelligence Division“ mit niedrigen Schwellen und einer „Criminal Division“ mit hohen Schwellen unter einem Behördendach will der Entwurf vermeiden. Maßgeblich ist vielmehr das informationelle Trennungsprinzip, nach dem Daten aus der Vorfeldaufklärung nicht ohne eigene Schwelle in eingriffsintensive Folgemaßnahmen überführt werden, und das nichts anderes als eine Verkörperung des Verhältnismäßigkeitsprinzips darstellt. Seit dem HVSG-Beschluss verlangt die Übermittlung an Stellen mit operativen Anschlussbefugnissen eine konkretisierte Gefahr oder einen entsprechenden Straftatverdacht.<sup>300</sup> Der Einwand der Begründung, das Prinzip stehe Einwirkungsbefugnissen nicht entgegen, deren Anlass keine Datenerhebung sei,<sup>301</sup> trägt jedenfalls für die realweltliche Einwirkungen des § 59 nicht. Denn die Schutzmaßnahme setzt gerade Erkenntnisse operativ um, die unter den niedrigeren nachrichtendienstlichen Schwellen gewonnen wurden.

Der Entwurf lässt die Schutzmaßnahme trotz dessen unterhalb der konkretisierten Gefahr zu. Verlangt wird nämlich nur eine „Gefährdung“, die von einer besonderen Bedrohung ausgeht. Die Begründung sieht die erhebliche Unruhe im terroristischen Vorgehen „regelmäßig angelegt“ und die besondere Schadensintensität in der Wirkungsmacht staatlicher Angreifer.<sup>302</sup> Damit ist das Einwirken schon unterhalb der Schwelle eröffnet, ab der das BfV seine Erkenntnisse nach § 46 an die Polizei geben dürfte. Nach unserer Auffassung begegnet das mit Blick auf die Schutzfunktion des informationellen Trennungsprinzips erheblichen verfassungsrechtlichen Bedenken, die sich aber durch eine höhere Schwelle ausräumen ließen. Zwar hat die Rechtsprechung bisher nur über die Übermittlung an operative Stellen entschieden, nicht über eine solche Eigenvornahme. Wer ein Tatmittel unbrauchbar macht, nimmt aber vorweg, was die Polizei erst bei konkreter Gefahr darf. Für die Anforderungen an die Gefahrenabwehr kommt es auf die Wirkung der Maßnahme an und nicht auf die handelnde Behörde.<sup>303</sup> Andernfalls ließen sich die Anforderungen an die Polizei durch Verlagerung auf einen Dienst umgehen. Wir empfehlen deshalb, zumindest für das realweltliche Einwirken auf körperliche Gegenstände die konkretisierte Gefahr in § 59 Abs. 1 aufzunehmen und damit die Übermittlungsschwelle nachzuzeichnen, die § 46 Abs. 1 bereits enthält. Die Schwelle gilt dabei nur für diese Maßnahme. Beobachtung, Quellenführung und Analyse behalten ihre Vorfeldschwellen, und eine einzelne Einwirkungsbefugnis verändert den Charakter des Dienstes nicht.

Für digitalen Gegenmaßnahmen einschließlich der Verbreitung von Desinformation ist differenzierter zu urteilen. Die Umleitung eines Datenverkehrs oder die Löschung einer Schadsoftware auf einem fremden Server richtet sich an niemanden, verlangt keine Duldung und lässt sich nicht mit Zwang durchsetzen. Sie wirkt also rein technisch, ohne einen hoheitlichen Gehorsamsanspruch zu erheben, und der Angreifer muss den Gegenschlag rechtlich nicht hinnehmen. Nach unserer Auffassung ist eine solche Maßnahme deshalb keine operative Anschlussmaßnahme im Sinne der Rechtsprechung, sofern durch sie nicht ausnahmsweise direkte realweltliche Schäden eintreten (z.B.

---

<sup>300</sup> BVerfGE 169, 130, Rn. 106 f.

<sup>301</sup> Begr. zu § 28 BNDG-E, BT-Drs. 21/7868, S. 413 f.

<sup>302</sup> Begr. zu § 59 Abs. 3 und Abs. 3 Nr. 1 BVerfSchG-E, BT-Drs. 21/7868, S. 307.

<sup>303</sup> BVerfGE 162, 1, Rn. 153 ff.; BVerfGE 163, 43 (Beschl. v. 28.9.2022, 1 BvR 2354/13), Rn. 120, 123; zur Reichweite des Begriffs auch BVerfGE 169, 130, Rn. 89. Weiterführend zum Begriff Warg, ZD 2024, 434, und zu operativen Befugnissen der Dienste Thiel, KriPoZ 2026, 208.

Hackback, der zur Explosion eines Kraftwerks führt), sodass das informationelle Trennungsprinzip für sie keine polizeigleiche Schwelle verlangt (zur Parallelfrage beim BND B.VI.4.a).<sup>304</sup>

Dem lässt sich nach hiesiger Auffassung auch nicht entgegenhalten, das Bundesverfassungsgericht verzichte auf das Merkmal des Zwangs in seiner einschlägigen Spruchpraxis. Tatsächlich hat es lediglich klargestellt, dass die strengerer Übermittlungsanforderungen nicht erst greifen, wenn die Übermittlung gerade unmittelbaren Zwang ermöglichen soll. Eingriffsverstärkend wirke bereits die Übermittlung an Stellen, die über operative Anschlussbefugnisse als solche verfügen, weil diese die den Diensten verschlossenen eingriffsintensiven Folgemaßnahmen gegenüber Bürgerinnen und Bürgern ergreifen könnten.<sup>305</sup> Das Gericht verlagert die Prüfung damit vom Zweck der einzelnen Übermittlung auf die Ausstattung des Empfängers. Den Begriff selbst hält es aber fest. Operativ ist die Möglichkeit, gegenüber Einzelnen Maßnahmen erforderlichenfalls auch mit Zwang durchzusetzen, und operative Befugnisse und operative Zwangsbefugnisse sind gleichbedeutend.<sup>306</sup> Entscheidend ist danach, ob eine Befugnis den Dienst in die Lage versetzt, gegenüber Bürgern Pflichten zu begründen und durchzusetzen. Eine digitale Gegenmaßnahme leistet das aus den genannten Gründen nicht. Dass das Gericht den Begriff bei näherer Betrachtung dann doch nicht so mechanisch an der Ausstattung einer Behörde festmacht, wie es dies selbst abstrakt formuliert hatte, zeigt zudem die bereits angesprochene Anwendung der eigenen Kriterien auf Waffen- und Luftsicherheitsbehörden mit einem gegenläufigen Ergebnis. Zu Prüfzwecken hält es sie schon auf Grundlage tatsächlicher Anhaltspunkte für grundsätzlich möglich, obwohl diese Behörden durchsuchen und sicherstellen dürfen, weil die Übermittlung dort der Risikoprävention dient.<sup>307</sup>

Verfassungsrechtlich spricht nach alledem viel dafür, dass digitale Gegenmaßnahmen den Dienst nicht zu einer operativ ausgestatteten Stelle machen. Ein Restrisiko bleibt, weil das Bundesverfassungsgericht erkennbar zu einem weiten, an der Ausstattung orientierten Verständnis neigt. Rechtspolitisch sollte der Gesetzgeber die Hackbacks daher möglichst begrenzt halten: Digitale Maßnahmen sollten sich nur gegen Systeme und Daten richten dürfen, die für die Bedrohung eingesetzt werden. Sie sollten keine Pflichten für Personen begründen und keine Wegnahme von Geräten bei Personen erlauben. Wo der Dienst Daten nutzt, um gezielt in Rechtsgüter bestimmter Personen einzugreifen, sollte die Schwelle der konkretisierten Gefahr, die für Übermittlungen an operative Stellen gilt, auch intern gelten. Und sie sollten keine direkten realweltlichen Folgen auslösen dürfen, die über die mit der Ausschaltung der gegnerischen IT-Komponenten zwangsweise verbundenen hinausgehen.

Grundrechtlich bleibt die digitale Gegenmaßnahme gleichwohl ein Eingriff, der erheblich wiegen kann, etwa wenn sie Systeme nachhaltig unbrauchbar macht, Daten vernichtet oder unbeteiligte Nutzer trifft. Wir unterscheiden deshalb nach dem Eingriffsgewicht: Für die Abwehr eines laufenden Angriffs durch Umleiten oder Unterbinden des Datenverkehrs und das Entfernen von Schadsoftware halten wir eine Schwelle unterhalb der konkretisierten Gefahr für vertretbar, weil der Angriff bereits wirkt, die Maßnahme eng auf ihn bezogen ist und Rechte Dritter nur gering berührt. Für vorgelagerte Maßnahmen, die keinen laufenden Angriff abwehren, müssen dagegen die Nähe zur konkreten nachrichtendienstlichen Tätigkeit, die Tatsachengrundlage, die Erforderlichkeit und das Eingriffsgewicht gesondert begründet werden. Aus Gründen der Verhältnismäßigkeit sollte für gravierende

<sup>304</sup>Manns, ZRP 2026, 63 (65); a.A. Timu, VerfBlog v. 27.8.2026 (Fn. oben), der jede eigene Verwendung der Erkenntnisse zur Einwirkung auf den Geschehensablauf als operativ einordnet.

<sup>305</sup>BVerfGE 169, 130, Rn. 231; BVerfGE 162, 1, Rn. 234.

<sup>306</sup>BVerfGE 169, 130, Rn. 231; BVerfGE 162, 1, Rn. 154.

<sup>307</sup>BVerfGE 169, 130, Rn. 112 f.

Eingriffe wie die nachhaltige Unbrauchbarmachung von Systemen, die Vernichtung von Daten oder Maßnahmen mit erheblichen Folgen für unbeteiligte Dritte aber die konkretisierte Gefahr gelten. Das gilt nach unserer Auffassung jedenfalls dort, wo die Maßnahme in ihrer Wirkung einer polizeilichen Sicherstellung oder Vernichtung entspricht.

### 3. Kompetenz, Regelungsvorschlag

Das eigentliche Problem der Schutzmaßnahmen wurzelt indes nicht in der Verhältnismäßigkeit, sondern in der grundgesetzlichen Kompetenzzuweisung. Die Gesetzesbegründung hält die Schutzmaßnahmen irritierend schmallippig für „generisch in der auf Wirksamkeit angelegten Gesetzgebungskompetenz zum bundesbehördlichen Verfassungsschutz eingeschlossen“.<sup>308</sup> Das trifft nicht zu, jedenfalls nicht für körperliche Einwirkungen. Art. 87 stellt jene Tätigkeit in die Verwaltung des Bundes und beschreibt damit die Funktion des BfV, die sich auf die „Sammlung von Unterlagen für Zwecke des Verfassungsschutzes und des Schutzes gegen Bestrebungen im Bundesgebiet, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden“, richtet. Man mag gut und gerne argumentieren, dass „Sammlung“ im Zeichen der Zeit zu verstehen ist und daher nicht nur, wie die Mütter und Väter des Grundgesetzes es sich vorgestellt haben mögen, das Zusammentragen von Papieren umfasst, sondern auch Abhören, Hacken oder gar in Wohnungen eindringen, soweit auch dies wiederum letztlich dem Zusammentragen von Informationen dient. Geradezu klassische Gefahrenabwehr aber, wie es das Unschädlichmachen einer Waffe oder von Sprengstoffen (also das Beseitigen einer Gefahr für die Öffentliche Sicherheit und Ordnung) darstellt, hat nichts mehr mit der nachrichtendienstlichen Informationsaufgabe zu tun, sondern stellt bei allem Wohlwollen und vorhandenem praktischem Verständnis für die Belange des BfV eine den Polizeien nach dem Grundgesetz übertragene Aufgabe dar. Hinzu kommt, dass diese Gefahrenabwehr im Grundsatz Ländersache ist, soweit das Grundgesetz nichts anderes bestimmt (Art. 30, 70, 83 GG).<sup>309</sup> Dass diese Grenze ernst gemeint ist, zeigt die Föderalismusreform von 2006: Für die Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt musste das Grundgesetz eigens geändert werden (Schaffung von Art. 73 Abs. 1 Nr. 9a GG).<sup>310</sup> Was selbst für eine Polizeibehörde des Bundes einer Verfassungsänderung bedurfte, lässt sich für eine nach der Verfassung als nachrichtendienstliche Zentralstelle angelegte Behörde kaum aus der Natur der Sache herleiten.<sup>311</sup> Vermutlich dürfte der Versuch des Regierungsentwurfs, an einer Anpassung des Grundgesetzes vorbeizukommen, schlicht den politischen Mehrheiten geschuldet sein, die ein entsprechendes Vorhaben nicht mittragen würden.

Obwohl im Grundsatz bei uns viel Verständnis dafür herrscht, dass der Gesetzgeber auch an die Grenzen der Rechtsprechung gehen oder dem Bundesverfassungsgericht Gelegenheit zu neuen Wertungen geben will, kann nach hiesiger Auffassung nicht einmal im Ansatz damit gerechnet werden, dass § 59 vor dem Bundesverfassungsgericht Bestand haben könnte. Falls der Gesetzgeber die Norm dennoch unbedingt vorsehen möchte – was sich vor allem im Cyberbereich sehr lohnen könnte, denn hier liegt der praktische Schwerpunkt der Erweiterungen mit einer wichtigen Stärkung

<sup>308</sup> Begr. zu § 59 BVerfSchG-E, BT-Drs. 21/7868, S. 305 ff.

<sup>309</sup> Im Ergebnis ebenso Timu, VerfBlog v. 27.8.2026 (Fn. oben), der für Bestrebungen des internationalen Terrorismus zudem auf die Zuweisung an das Bundeskriminalamt in Art. 73 Abs. 1 Nr. 9a GG verweist; ferner Höning, VerfBlog v. 14.8.2026 (Fn. oben), unter Hinweis darauf, dass kein Polizeigesetz vergleichbare Befugnisse kennt.

<sup>310</sup> Gesetz zur Änderung des Grundgesetzes v. 28.8.2006, BGBl. I S. 2034.

<sup>311</sup> Bestätigt wird das durch die Wissenschaftlichen Dienste des Bundestages, die für das parallele Cybersicherheitsgesetz zu dem Ergebnis kommen, dass eine Zuständigkeit des Bundeskriminalamts für die Abwehr von Cyberangriffen unterhalb der Schwelle des internationalen Terrorismus ausscheiden dürfte, vgl. Wissenschaftliche Dienste des Deutschen Bundestages, WD 3 - 3000 - 056/26 v. 6.7.2026, S. 12.

der Cyber- und Spionageabwehr des BfV, so bedarf es dringlich dreier Änderungen, die möglicherweise dazu führen könnten, dass die Schutzmaßnahmen jedenfalls nicht mehr evident verfassungswidrig wäre, auch wenn ein erhebliches Risiko bliebe:

Erstens sollte § 59 in eine Norm für realweltliche Einwirkungen körperliche Gegenstände und in eine für Datenverkehre und informationstechnische Systeme einschließlich der Platzierung von Falschinformationen geteilt werden, damit durchgreifende Zweifel an der einen Variante nicht ohne Weiteres auch die andere erfassen. Zwar lässt sich dies auch durch eine Absatzlogik innerhalb eines Paragraphen lösen, die Trennung sollte aber möglichst sichtbar vollzogen werden.

Zweitens sollten beide Varianten, unbedingt aber zumindest die realweltliche, auf die Spionageabwehr beschränkt werden, also auf eine Abwehrtätigkeit des BfV gegen fremde Mächte (§ 2 Abs. 1 Nr. 3). Für sie lässt sich die Bundeskompetenz analog zum BNDG-E auf Art. 73 Abs. 1 Nr. 1 GG stützen. Denn die Abwehr hoheitlicher Tätigkeit fremder Mächte auf deutschem Boden ist als Kehrseite der Gegenspionage des BND eine Wahrnehmung der Gebietshoheit gegenüber einem anderen Völkerrechtssubjekt und berührt damit auswärtige Angelegenheiten. Dieses Ergebnis trägt auch die enge Vernetzung mit dem Auswärtigen Amt, wenn es beispielsweise um die Ausweisung enttarnter Legalresidenten geht. Anders als im US-amerikanischen Modell besteht zwischen BND und BfV keine starre Trennung derart, dass der Auslandsdienst analog etwa zur US-amerikanischen CIA grundsätzlich nicht auf dem eigenen Hoheitsgebiet tätig werden darf. Vielmehr muss nur sein Blick auf auswärtige Angelegenheiten gerichtet sein, wozu auch Handlungen im Inland beitragen können. Andersherum macht der Verfassungsschutz nicht an den Staatsgrenzen halt, was auch die faktische Tätigkeit des BfV belegt (man denke nur an die Befragung von Personen in Flüchtlingseinrichtungen auf Drittstaatsgebiet, die in die Bundesrepublik einzureisen wünschen.) Wo Aktivitäten fremder Mächte Sabotage gegen die Verteidigungsfähigkeit abgewehrt werden, was immer häufiger anfallen dürfte, berührt die Aufgabenerfüllung des BfV zugleich, wenngleich am Rande den Kompetenztitel der Verteidigung. Insoweit gilt dasselbe wie für die erweiterten Maßnahmen des BND (vgl. unter B.VI). Man mag darin mit einigem, aber vertretbarem guten Willen auch eine spezielle Zuweisung sehen, die der allgemeinen Gefahrenabwehrkompetenz der Länder vorgeht. Auf denselben Titel stützt die Bundesregierung die neuen Abwehrbefugnisse des Bundeskriminalamts im parallelen Cybersicherheitsgesetz,<sup>312</sup> sodass zumindest eine einheitliche Linie der Regierungskoalition feststünde, die es dann in Karlsruhe zu verteidigen gilt. Die Beschränkung vermiede zudem eine Überschneidung mit der Abwehrkompetenz, die Art. 73 Abs. 1 Nr. 9a GG für den internationalen Terrorismus dem Bundeskriminalamt zuweist. Ein darauf gestütztes Gesetz bedürfte überdies nach Art. 73 Abs. 2 GG der Zustimmung des Bundesrates.<sup>313</sup> Im Terrorismusbereich bliebe das Einwirken auf Gegenstände dann den Polizeien vorbehalten, denen die Erkenntnisse nach § 46 zu übermitteln sind. Falls es hier durch die von BMI und BfV ins Feld geführten Beispiele einer Übermittlungsproblematik durch die Third Party Rule zu Rechtsverlusten kommt, wären diese im Interesse der ansonsten wohl vollständig verfassungswidrigen Schutzmaßnahmen hinzunehmen.

Drittens sollte die Begründung, die der Bundestag im Bericht des federführenden Ausschusses ergänzen kann, beide Varianten unterschiedlich und vor allem überhaupt inhaltlich vernünftig begründen. Für die realweltlichen Eingriffe sollte sie allein auf die auswärtigen Angelegenheiten abstellen

<sup>312</sup>BT-Drs. 21/6585, Begr. A.IV (Gesetzgebungskompetenz), zu Artikel 3 (Änderung des Bundeskriminalamtgesetzes), wo neben Art. 73 Abs. 1 Nr. 9a und 10 GG auch Art. 73 Abs. 1 Nr. 1 GG genannt ist.

<sup>313</sup>Timu, VerBlog v. 27.8.2026 (Fn. oben), der Art. 73 Abs. 1 Nr. 9a GG darüber hinaus als ausschließliche Zuweisung an das Bundeskriminalamt versteht.

und diese Zuordnung einer solchen unter die allgemeine Gefahrenabwehr als Auffangrecht vorgeht. Die Gesetzesbegründung hebt selbst hervor, dass das Eingriffsgewicht dort besonders gering ist, wo auf Einsatzmittel eines anderen Staates eingewirkt wird.<sup>314</sup> Für die digitale Variante sollte sie dagegen ausführlich darlegen, warum es sich nicht um Gefahrenabwehr im klassischen Sinne handelt. Dafür kann sie auf die Gründe zurückgreifen, aus denen die digitale Gegenmaßnahme keine operative Anschlussmaßnahme ist (vgl. unter C.VIII.2).<sup>315</sup> So verstanden ergänzt sie die Aufklärung einer konkreten, vom BfV erkannten Tätigkeit und lässt sich als Annex der Kompetenz aus Art. 73 Abs. 1 Nr. 10 lit. b und c GG verstehen. Bloße Nützlichkeit oder Sachnähe genügen dafür allerdings nicht, und die Reichweite des Ansatzes ist umstritten, wie die Wissenschaftlichen Dienste dokumentiert haben.<sup>316</sup> Der Einwand, das BfV erhalte Befugnisse, die nicht einmal die Polizei habe,<sup>317</sup> verliert zudem an Gewicht, seit das Cybersicherheitsgesetz dem Bundeskriminalamt und der Bundespolizei vergleichbare digitale Befugnisse geben will. Eine allgemeine Zuständigkeit des BfV für die Cybersicherheit folgt aus dem vorliegenden Regelungsentwurf ebenfalls nicht. Wir empfehlen deshalb, den Anwendungsbereich der digitalen Befugnis im Normtext auf Einwirkungen gegen konkrete, vom BfV aufgeklärte Tätigkeiten zu begrenzen.

#### 4. Subsidiarität, Kontrolle

Die Subsidiarität des § 59 Abs. 1 S. 2 ist alternativ gefasst: Das BfV darf selbst einwirken, wenn eine andere Stelle den Zweck nicht erreichen kann oder wenn eine Übermittlung an den Übermittlungsverbieten des § 51 BVerfSchG-E scheitert, namentlich am Quellenschutz bzw. der bereits angesprochenen Third Party Rule. Die erste Alternative betrifft Fälle, in denen keine andere Stelle rechtzeitig und gleich wirksam handeln kann, die zweite Fälle, in denen eine andere Stelle zwar handeln könnte, die erforderlichen Informationen aber wegen eines gesetzlichen Übermittlungsverbots nicht erhalten darf. Wir halten die Alternativität im Grundsatz für richtig, allerdings mit zwei einzufordernden Nachbesserungen: Zum einen ist ein konkret belegtes gesetzliches Übermittlungsverbot erforderlich, nicht bloß ein Geheimhaltungswunsch, institutionelle Bequemlichkeit oder die allgemeine Berufung auf Quellenschutz. Zum anderen muss die Maßnahme des BfV unabhängig davon alle ihre eigenen Voraussetzungen erfüllen. Insbesondere gilt: Dass eine Übermittlung an die Polizei ausscheidet, nur weil entsprechende Schwellen nicht erreicht sind, macht eine sonst unzulässige Maßnahme keinesfalls zulässig, denn damit würde gerade eine Umgehung der für die Eingriffsverwaltung geschaffenen höheren Hürden erfolgen, ganz gleich im Gewand welcher Behörde der Eingriff erfolgt. Hinzu kommt, dass die im Regierungsentwurf vorgesehene Vorabkontrolle nur bestätigen soll, dass eine besondere Bedrohungslage besteht (§ 60 Abs. 2), sie die einzelne Operation aber nicht erfasst. Für das Einwirken auf körperliche Gegenstände sollte deshalb auch die Einzelanordnung der Vorabkontrolle unterliegen, wie es § 60 Abs. 4 S. 2 für Eingriffe in informationstechnische Systeme und Wohnungen vorsieht, soweit kein Eilfall gegeben ist, der besonders zu regeln wäre.

Aus rechtspolitischer Sicht sollten digitale Einwirkungen zudem dokumentiert und dem UKRat zur nachträglichen Prüfung zugänglich gemacht werden. Eingriffsintensive Einwirkungen sollte er im Einzelfall prüfen, technische Routineschritte innerhalb einer bereits geprüften Maßnahme über Protokolle und Stichproben. Die Abstufung selbst ließe sich in einer Dienstvorschrift konkretisieren, die der Zustimmung des BMI und des UKRats bedarf. Das Gesetz sollte dafür den Rahmen vorgeben,

<sup>314</sup> Begr. zu § 59 BVerfSchG-E, BT-Drs. 21/7868, S. 305.

<sup>315</sup> Manns, ZRP 2026, 63 (65); a.A. Timu, VerfBlog v. 27.8.2026 (Fn. oben).

<sup>316</sup> Wissenschaftliche Dienste des Deutschen Bundestages, WD 3 - 3000 - 056/26 v. 6.7.2026, S. 16 f.

<sup>317</sup> Höning, VerfBlog v. 14.8.2026 (Fn. oben), unter Berufung auf Bäcker.

nämlich die zulässigen Kategorien der Einwirkung, die Schwelle je Kategorie, den Schutz unbeteiligter Nutzer und die Dokumentation. Hinzu kommt ein Punkt, den der Entwurf übergeht. Die Mitteilungspflicht des § 35 erfasst Schutzmaßnahmen nicht, sodass Personen, in deren Rechte eine Maßnahme eingreift, davon nie erfahren. Für Eingriffe in Verhaltensfreiheit und Eigentum ist das nicht hinnehmbar. Die Rechtsprechung zur eingeschränkten Mitteilung heimlicher Überwachung trägt hier nicht, weil Schutzmaßnahmen nicht auf Erkenntnis, sondern auf Einwirkung gerichtet sind und Art. 19 Abs. 4 GG dem Betroffenen die eigene Rechtsverteidigung sichert, die eine objektive Kontrolle durch den UKRat nicht ersetzt. Wir empfehlen deshalb, § 35 auf Schutzmaßnahmen zu erstrecken, die in Rechte bestimmbarer Personen eingreifen. Die Mitteilung darf zurückgestellt werden, solange sie den Zweck der Maßnahme oder nachrichtendienstliche Quellen und Methoden gefährdet, und sie entfällt nur, wenn der Betroffene nicht mit vertretbarem Aufwand zu ermitteln ist.

Einwand: wohl kaum, weil sollte gleichwohl dürfen.

Mit der Subsidiarität hängt das Amtshilfeverbot zusammen, das mit den Trennungsklauseln entfällt. Es hinderte den Dienst bislang, die Polizei um Maßnahmen zu ersuchen, die er selbst nicht vornehmen durfte. Diese Frage beantworten die Übermittlungsschwellen der §§ 46 ff. BVerfSchG-E nicht. Sie regeln nur, welche Daten die Polizei erhält, nicht aber, ob sie auf Ersuchen des BfV einen Eingriff vornehmen darf, zu dem das BfV selbst nicht befugt wäre. Für den BND erklärt die Begründung die Streichung für folgenlos,<sup>318</sup> für das BfV fehlt eine entsprechende Erklärung.

## **IX. Eigensicherung (§§ 28, 63–67)**

### **1. Aufgabe, Kompetenz**

Eigensicherungsbefugnisse kennt schon das geltende Recht. Neu ist aber, dass § 2 Abs. 4 BVerfSchG-E die Eigensicherung als Fachaufgabe regelt. Die Begründung ordnet sie zutreffend als Gefahrenabwehr für die Rechtsgüter des Verfassungsschutzes ein, weil die Funktionsfähigkeit des BfV Element der Sicherheit des Bundes ist.<sup>319</sup> Der Schutz der eigenen Funktionsfähigkeit folgt aus der Aufgabe, so dass ihn bei Bundesbehörden dieselbe Kompetenz trägt wie die Aufgabe selbst. Anders als bei den Schutzmaßnahmen schützt das BfV hier nämlich sich selbst und nicht Dritte, sodass der kompetenzielle Rückgriff stark überzeugt. Die Befugnisse der §§ 63 und 64 übernehmen im Kern die §§ 26b und 26c des geltenden Rechts. Sie rechtfertigen sich dadurch, dass sich Personen freiwillig und in Kenntnis des geltenden Rechts in den Bereich einer Sicherheitsbehörde begeben. Diese Rechtfertigung verliert aber an Kraft, wo der Entwurf den Anknüpfungspunkt der Befugnisse erweitert: Durchsuchung, Sicherstellung und unmittelbarer Zwang knüpfen künftig nämlich an „funktionsgefährdende Tätigkeiten“ an, nach § 2 Abs. 4 also an alle Tätigkeiten, die geeignet sind, die ordnungsgemäße Aufgabenwahrnehmung zu beeinträchtigen. Das geltende Recht verlangte dagegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten.<sup>320</sup> Der neue Begriff kann somit auch nicht strafbare Störungen innerhalb des Eigensicherungsbereichs erfassen. Außerhalb davon bleibt die Reichweite allerdings begrenzt. § 63 Abs. 2 betrifft Personen, die diesen Bereich betreten oder sich darin aufhalten. Für Personen in unmittelbarer Nähe gilt die Befugnis nach Absatz 6 Nummer 1 nur in Nacheile-Situationen, also wenn sie sich einer Maßnahme innerhalb des Bereichs entziehen. Eine allgemeine Durchsuchungsbefugnis vor den Toren des BfV folgt daraus nicht, und ein Demonstrant vor dem Tor wird nicht schon wegen einer möglichen Funktionsbeeinträchtigung erfasst (anders

<sup>318</sup>Begr. zu § 5 BNDG-E, BT-Drs. 21/7868, S. 360.

<sup>319</sup>Begr. zu § 2 Abs. 4 BVerfSchG-E, BT-Drs. 21/7868, S. 212.

<sup>320</sup>Begr. zu § 63 BVerfSchG-E, BT-Drs. 21/7868, S. 309.

liegt es beim BND, dessen Befugnisse § 108 Nr. 4 BNDG-E auf das unmittelbare Umfeld der Dienststellen erstreckt; vgl. unter B.X.2). Da für das BfV keine nebenstrafrechtlichen Tatbestände wie im BNDG-E geschaffen werden, die dann als „qualifiziert funktionsgefährdende Tätigkeiten“ gelten können, verzichtet der Gesetzgeber hier auf eine wirkungsvolle Absicherung von Ausspähungen über die zusätzliche repressive Komponente. Warum die Dienste unterschiedlich behandelt werden, erklärt die Begründung nicht.<sup>321</sup> Aus rechtspolitischer Sicht vorzugswürdig wäre es, die nebenstrafrechtlichen Tatbestände des BNDG-E zu übernehmen und dann maßgeblich hierauf im BVerfSchG-E abzustellen. Außerdem sollte der unzulässigen Drohnenbetrieb nach § 21h Abs. 3 Nr. 4 LuftVO ergänzt werden, wie er sich für den BND in § 104 Nr. 2 lit. d BNDG-E wiederfindet.

## 2. Befugnisse im Eigensicherungsbereich (§§ 63, 64)

Neu im Befugniskatalog sind die Identitätsfeststellung (§ 63 Abs. 2 S. 2), die verdachtsunabhängige Durchsuchung von Räumen (Abs. 4 S. 1), die Sicherstellung und Untersuchung vorschriftswidrig eingebrachter Gegenstände (Abs. 5 S. 1 Nr. 2) und die Sicherstellung nicht zuzuordnender Gegenstände im Nahumfeld (Abs. 6 Nr. 2).<sup>322</sup> Hervorzuheben sind drei Punkte. Erstens umfasst die Untersuchung vorschriftswidrig eingebrachter Geräte den Eingriff mit technischen Mitteln und die Verarbeitung der gespeicherten Daten (Abs. 5 S. 2). Ausgelöst wird sie nicht erst durch (zusätzliche) Anhaltspunkte für eine funktionsgefährdende Tätigkeit, sondern schon durch das verbotene Einbringen. Laut der Gesetzesbegründung soll damit die leidige Streitfrage entschieden werden, ob bereits das Einbringen des Geräts als solches einen Anhaltspunkt darstellt.<sup>323</sup> Der Zugriff auf ein privates informationstechnisches System erfolgt nach der vorliegenden Norm zwar ohne die Voraussetzungen des § 25, ist aber dennoch verhältnismäßig. Die Befugnis stellt ein Sonderrecht für Personen dar, die sich freiwillig in den Dienst und seine Sicherheitsbereiche begeben. Wer sein privates Gerät trotz Hinweis und Belehrung vor der Schleuse heimlich mitführt, begründet die naheliegende Besorgnis, dass er damit Ton- oder Bildaufnahmen gefertigt oder Daten abgeleitet hat. Das Spiegeln des Geräts und sein Einbehalten für die Dauer der Untersuchung sind dann besonders in Abwägung mit den durch Innentätern verbundenen erheblichen Abflussmöglichkeiten und daraus resultierenden Rechtsgutsbeeinträchtigungen gerechtfertigt. Müsste das BfV zusätzlich Anhaltspunkte für eine funktionsgefährdende Tätigkeit darlegen, liefe die Kontrolle in aller Regel leer. Klarstellen sollte das Gesetz aber, dass die Befugnis nur greift, wenn auf das Einbringungsverbot zuvor erkennbar hingewiesen und über mögliche Kontrollen belehrt wurde, und dass Daten ohne Bezug zur Eigensicherung unverzüglich zu löschen sind. Dieselbe Regelung empfehlen wir für den BND (vgl. unter B.X.4).

Zweitens kann das BfV die Herausgabe eines Telekommunikationsendgeräts künftig davon abhängig machen, dass der Betroffene an einem unverschlüsselten Abbild mitwirkt (§ 64 Abs. 5 S. 6). Das kommt einer erzwungenen Entschlüsselung gleich, weil der Betroffene sein Gerät sonst nicht zurückerhält. Gegenüber Bediensteten folgt eine solche Mitwirkungspflicht aus dem Dienstverhältnis. Besucher trifft dagegen keine Pflicht, eigene Daten zu entschlüsseln. Aus rechtspolitischer Sicht sollte die Regelung deshalb auf Bedienstete und sicherheitsüberprüfte Personen beschränkt werden; im Übrigen müssen die Personen den temporären Verlust des Endgeräts hinnehmen. Drittens schließt § 67 die Mitbestimmung des Personalrats bei Maßnahmen der Eigensicherung aus, auch bei technischen Einrichtungen, die das Verhalten der Beschäftigten erfassen. Eine gesetzliche

<sup>321</sup> Weder die Begründung zu § 63 BVerfSchG-E noch die zu § 104 BNDG-E geht auf die Divergenz ein (BT-Drs. 21/7868, S. 309 ff., 522 ff.).

<sup>322</sup> Begr. zu § 63 Abs. 2 und 4–6 BVerfSchG-E, BT-Drs. 21/7868, S. 310.

<sup>323</sup> Begr. zu § 63 Abs. 5 BVerfSchG-E, BT-Drs. 21/7868, S. 310.

Eingrenzung hält die Begründung für untunlich.<sup>324</sup> Dann sollten aus rechtspolitischer Sicht wenigstens die Grenzen der Videoüberwachung (§ 63 Abs. 4 S. 2), insbesondere Speicherdauer und Auswertungsanlässe, direkt im Gesetz geregelt werden. (Zur Rechtmäßigkeit von Umfeldbefugnissen, falls das BfV diese im Sinne des BNDG-E ebenfalls noch anstreben sollte, siehe B.X.2.).

### 3. Einsatzsicherung, Waffen, Drohnenabwehr (§§ 28, 63 Abs. 7, 65)

Am weitesten reicht die Einsatzsicherung. Schon § 26c Abs. 7 BVerfSchG kennt begrenzte Mittel zur Durchsetzung von Eigensicherungsmaßnahmen. § 63 Abs. 7 S. 1 Nr. 3 BVerfSchG-E übernimmt diese Regelung nach der Begründung im Ergebnis unverändert.<sup>325</sup> Darüber hinaus erweitert der Entwurf die bestehenden Eigensicherungsbefugnisse um besondere Abwehrfälle (§ 28 Abs. 1, § 63 Abs. 7 S. 1 Nr. 1 und 2). Für diese Fälle eröffnet er unter den gesetzlichen Voraussetzungen auch den Waffengebrauch. Zur Durchsetzung von Kontrollen bleiben Waffen dagegen ausgeschlossen (§ 63 Abs. 7 S. 3). Sachgerecht ist die Verweisung auf das UZwG, weil sie den Schusswaffengebrauch gegen Personen nur in den Fällen des § 10 Abs. 1 Nr. 1 und 2 UZwG eröffnet. Ob die Nummer 2, die den Schusswaffengebrauch zum Anhalten flüchtender Personen unter den dort qualifizierten Voraussetzungen erlaubt, für die Eigensicherung erforderlich ist, sollte der Gesetzgeber allerdings prüfen und die Nummer andernfalls streichen.<sup>326</sup> Im Übrigen schließt die Regelung eine Lücke. Das Führen von Waffen ist den Bediensteten des BfV zwar mangels Verbot<sup>327</sup> erlaubt, eine besondere hoheitliche Befugnis zum Waffengebrauch fehlte bislang aber, so dass sie auf die allgemeinen Notwehr- und Nothilferechte angewiesen waren. Ein solcher Rückgriff ist für Personen, die staatliche Gewalt ausüben, in der Tat unglücklich und für die Bürger weniger vorhersehbar. Wenig glücklich ist, dass die für den Schusswaffengebrauch erforderliche Ausbildung gänzlich in das Ermessen der Amtsleitung gestellt wird („besondere Schulung“). Für Beamte, die Schusswaffen gegen Menschen einsetzen dürfen, wäre aus rechtspolitischer Sicht ein gesetzlicher Standard vorzugswürdig, etwa die Ausbildung nach den für die Bundespolizei geltenden Vorschriften oder Teilen hiervon.

Auch die Drohnenabwehr wird ausgebaut. § 65 BVerfSchG-E erstreckt sie auf den Schutz eingesetzter Personen und erlaubt die Abwehr bei Annäherung auf 100 Meter oder beim Eindringen in das Gebiet der Liegenschaften. Damit reicht die Regelung weniger weit als § 112 BNDG-E, der die Abwehr auch bei tatsächlichen Anhaltspunkten für eine qualifiziert funktionsgefährdende Nutzung erlaubt und Maßnahmen gegen den Steuernden zulässt (Abs. 1 S. 2, Abs. 2 Nr. 3). Beides fehlt im BVerfSchG-E. Da eine Drohne, die aus 150 Metern filmt, nicht weniger gefährlich ist als eine, die sich auf 100 Meter nähert, wäre aus rechtspolitischer Sicht die Angleichung an § 112 BNDG-E sinnvoll. In diesem Zuge sollte § 65 Abs. 2 S. 2 zur Durchsetzung einer Sicherstellung auch Hilfsmittel der körperlichen Gewalt und Waffen (ohne Schusswaffengebrauch) zulassen – wer ein abgewehrtes Fluggerät nicht herausgibt, lässt sich nämlich mit bloßer Einwirkung oft nicht dazu bewegen, und die Beschränkung auf besondere Vollzugskräfte (Satz 3) bleibt als Sicherung erhalten.

### 4. Vergleich mit dem BNDG-E, Regelungslücken

Das BNDG-E regelt die Eigensicherung deutlich weiter (§§ 104–124 BNDG-E). Es kennt vorübergehende besondere Sicherheitsbereiche mit grundsätzlich vorheriger Zustimmung des BKAmT, Entschädigung und Kennzeichnung (§§ 106, 107), den Platzverweis (§ 111 Abs. 1), das kurzzeitige

<sup>324</sup> Begr. zu § 67 BVerfSchG-E, BT-Drs. 21/7868, S. 312.

<sup>325</sup> § 26c Abs. 7 BVerfSchG; BT-Drs. 21/7868, S. 55 f.; Begr. S. 310 f.

<sup>326</sup> § 10 Abs. 1 Nr. 1 und 2 UZwG.

<sup>327</sup> § 55 Abs. 5 WaffG i.V.m. § 1 Nr. 1 lit. b, § 2 Nr. 1 lit. a und b WaffGBundFreistV v. 30.11.2020 (BGBl. I S. 2610).

Festhalten bis zur Überstellung an die Polizei (§ 109 Abs. 3, § 111 Abs. 2) und einen eigenen Unterabschnitt zur Sicherung von Verschlusssachen (§§ 115–119, dazu B.X.4). Das BVerfSchG-E sieht dagegen mangels entsprechender Tatbestände weder die Straftatanknüpfung noch die Kennzeichnung besonderer Sicherheitsbereiche vor, die sichtbar macht, wo besondere Befugnisse gelten, noch die Belehrung der Personen in den Dienststellen über mögliche Kontrollen (§ 115 Abs. 3 BNDG-E), obwohl das BfV Verschlusssachen in vergleichbarem Umfang verwahrt und denselben Innentäterrissen ausgesetzt ist. Ob die Asymmetrie gewollt ist, lässt die Begründung nicht erkennen, in der Sache liegt sie aufgrund der ähnlichen Bedrohungen für beide Dienste aber fern.

Aus rechtspolitischer Sicht sollten deshalb die Vorschriften zur Kennzeichnung besonderer Sicherheitsbereiche und zur Sicherung von Verschlusssachen (§§ 106 f., 115–118, 120 BNDG-E) angepasst übernommen werden, die für das BfV schärfer gestellte Handyauswerteregelung allerdings umgekehrt in das BNDG-E übernommen werden. Zudem sollte der Gesetzgeber erwägen, dem Verfassungsschutz eine eng begrenzte Befugnis zum Festhalten nach dem Vorbild des § 111 Abs. 2 BNDG-E einzuräumen, einschließlich der richterlichen Sicherung über die §§ 40–42 BPolG (vgl. unter B.X.3). Dass kurzfristiges Festhalten nicht begrifflich der Polizei vorbehalten ist, zeigt § 127 Abs. 1 StPO. Das Festnahmerecht knüpft aber an eine frische Tat an, während die Eigensicherung vorbeugend wirkt, sodass Anlass, Adressaten, Dauer und Sicherungen eigens zu regeln sind. Problematisch ist dabei nicht die Befugnis, sondern ihre Erstreckung auf das Umfeld der Dienststellen über Nacheilesituationen hinaus, wie sie § 108 Nr. 4 BNDG-E vorsieht (vgl. unter B.X.2).

Ein einheitliches Eigensicherungsgesetz für alle drei Dienste halten wir nicht für geboten, weil parallele Regelungen in den Fachgesetzen der Normalfall sind. Abweichungen zwischen ihnen brauchen aber einen Grund, und an diesem mangelt es.

## **X. Kontrolle, Auskunft, Übergang (§§ 69, 70, 79)**

Neu ist die Aufteilung der Rechts- und Datenschutzkontrolle nach § 69 BVerfSchG-E: Der UKRat ist für die Aufgaben nach § 2 Abs. 1–4 und die Schutzmaßnahmen zuständig, wohingegen dem BfDI nur noch die Aufsicht für die allgemeine Verwaltung und für die Mitwirkungsaufgaben obliegt. Diese Grenzlinie ist nachvollziehbar, wird aber Abgrenzungsfragen aufwerfen, etwa bei der Eigensicherung, die zugleich die Personalverwaltung berührt. Aus rechtspolitischer Sicht sollten UKRat und BfDI deshalb zum Austausch befugt sein (vgl. auch unter D.II.1). Beim Auskunftsrecht übernimmt § 70 BVerfSchG-E vom BND-Modell bereits die Beschwerde beim UKRat (Abs. 4) und die Entscheidung durch die Amtsleitung (Abs. 2 S. 2). Den Gegenstand fasst er eigenständig. Erfasst sind strukturiert gespeicherte Daten und sonstige Daten, soweit der Aufwand nicht außer Verhältnis zum Auskunftsinteresse steht (Abs. 1 S. 2). Bei den gesetzlichen Ausschlüssen bleibt er dagegen beim alten Modell. § 70 Abs. 3 schließt nur Herkunft und Übermittlungsempfänger aus, die zusätzlichen Ausschlussgründe des § 102 Abs. 2 Nr. 2 und 3 BNDG-E kennt er nicht. Gefährdungen verdeckt eingesetzter Personen oder der Arbeitsweise behandelt § 70 Abs. 2 Nr. 2 vielmehr als Versagungsgründe, die eine Abwägung im Einzelfall verlangen.<sup>328</sup> Verfassungsrechtlich ist eine Angleichung weder geboten noch ausgeschlossen, weil der Anspruch auf ermessensfehlerfreie Entscheidung auch gegenüber gesetzlichen Ausschlüssen fortbesteht (B.IX.2). Rechtspolitisch empfehlen wir, § 70 Abs. 3 so anzupassen, dass er § 102 Abs. 2 Nr. 2 und 3 BNDG-E entspricht.<sup>329</sup> Auch das BfV erhält Erkenntnisse von Partnerdiensten unter der Third Party Rule und ist Ziel fremder Ausforschung. Zudem

<sup>328</sup> BT-Drs. 21/7868, S. 58 f., 138; Begr. S. 314.

<sup>329</sup> Vgl. bereits Ogorek/Manns, VerfBlog v. 24.9.2026.

muss es jede Verweigerung nach Absatz 2 im Einzelfall abwägen und gegebenenfalls in Sperrerklärungs- und In-camera-Verfahren begründen. Entsprechend § 102 Abs. 2 Nr. 2 BNDG-E sollte der Ausschluss dabei auf die drohende Enttarnung verdeckt eingesetzter Personen beschränkt werden. Die Funktionsfähigkeit sollte, wie unter B.IX.2 vorgeschlagen, auf die Zusammenarbeit mit anderen Stellen bezogen werden. Der übrige Schutz nach Absatz 2 Nr. 2 bliebe dann in der Abwägung. Die Übergangsregelungen des § 79 haben wir unter C.V und eingangs von C bewertet.

## **D. Art. 3 – UKRatG-E**

Die Neufassungen des BNDG und des BVerfSchG betreffen in erster Linie die Voraussetzungen nachrichtendienstlicher Tätigkeit und das Instrumentarium der Dienste. Weil diese Befugnisse typischerweise verdeckt ausgeübt werden, bleibt ihre verfassungsrechtliche Beurteilung unvollständig, solange nicht geklärt ist, welche Kontrollmechanismen die mit der Heimlichkeit verbundenen Rechtsschutzdefizite ausgleichen. Ein zentrales Element des Entwurfs ist deshalb die Neuordnung der Kontrollarchitektur. Sie ist heute defizitär zersplittert, weil neben der Rechts- und Fachaufsicht des zuständigen Ressorts und der politischen Kontrolle durch das PKGr und das Vertrauensgremium des Haushaltsausschusses eine Kontrolle auch erfolgt durch: die G 10-Kommission (G 10-Maßnahmen), den UKRat (Ausland-Ausland-Fermeldeaufklärung) und die BfDI (allgemeiner Datenschutz). Am Rande ist schließlich der Bundesrechnungshof involviert. Die Präsidentin und die Präsidenten der Nachrichtendienste des Bundes haben vor dem PKGr wiederholt und berechtigt darauf hingewiesen, dass dieses Nebeneinander erhebliche personelle Ressourcen bindet, ohne die Notwendigkeit externer Kontrolle in Frage zu stellen.<sup>330</sup>

Art. 3 des Regierungsentwurfs löst die Vorschriften über den UKRat aus den §§ 40 bis 58 BNDG heraus und überführt sie in ein eigenes Gesetz. Aus 19 Paragraphen werden 42 (BT-Drs. 21/7868, S. 159 ff.). Zugleich tritt das G 10 außer Kraft (Art. 23 Nr. 3), und von der G 10-Kommission gehen deren Kontrollaufgaben auf den UKRat über.<sup>331</sup> Der UKRat erhält damit erstmals Zuständigkeiten für das BfV. Er tritt dort wie auch im BND an die Stelle der G 10-Kommission und kontrolliert in beiden Häusern zusätzlich all jene Maßnahmen, die bislang keiner unabhängigen Vorabkontrolle unterlagen, es aber nach der Karlsruher Spruchpraxis bedürfen. Dies betrifft etwa den längerfristigen Einsatz von Vertrauenspersonen und Verdeckten Bediensteten sowie eingriffsintensive Formen der optischen, akustischen und technischen Bewegungsüberwachung (§ 34 Abs. 1 Nr. 3 bis 5 BVerfSchG-E). Auch die Datenschutzkontrolle der Dienste übernimmt weitgehend der UKRat (§ 2 UKRatG-E), wohingegen dem BfDI im Wesentlichen die Datenverarbeitung außerhalb der nachrichtendienstlichen Aufgabenerfüllung verbleibt, also insbesondere in der allgemeinen Verwaltung sowie in der Aus- und Fortbildung (§ 69 Abs. 2 Nr. 2 BVerfSchG-E, § 98 Abs. 2 BNDG-E).

## **I. Verfassungsrechtlicher Rahmen**

### **1. Gerichtsäquivalente Ersatzkontrolle bei Eingriffen in Art. 10 GG**

Soweit Eingriffe in das Brief-, Post- und Fernmeldegeheimnis in Rede stehen, sind die Kontrollmechanismen an Art. 10 Abs. 2 S. 2 GG zu messen. Danach kann gesetzlich bestimmt werden, dass

<sup>330</sup>Vgl. die Selbstdarstellungen des BfV, [https://verfassungsschutz.de/DE/verfassungsschutz/auftrag-und-arbeitsweise/aufsicht-und-kontrolle/aufsicht-und-kontrolle\\_artikel.html](https://verfassungsschutz.de/DE/verfassungsschutz/auftrag-und-arbeitsweise/aufsicht-und-kontrolle/aufsicht-und-kontrolle_artikel.html), und des BND, [https://bnd.bund.de/DE/Die\\_Arbeit/Aufsicht\\_Kontrolle/aufsicht\\_kontrolle\\_node.html](https://bnd.bund.de/DE/Die_Arbeit/Aufsicht_Kontrolle/aufsicht_kontrolle_node.html).

<sup>331</sup>Zugleich sehen § 79 Abs. 1 und 2 BVerfSchG-E sowie § 140 Abs. 1 und 2 BNDG-E Fortgeltungs- und Überleitungsvorschriften für laufende und bereits angeordnete Maßnahmen vor und gestatten für bestimmte Maßnahmen die befristete Anwendung des bisherigen Rechts.

heimliche Beschränkungen zum Schutz der freiheitlichen demokratischen Grundordnung den Betroffenen nicht mitgeteilt werden und dass an die Stelle des Rechtswegs die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.<sup>332</sup> Diese Nachprüfung muss der gerichtlichen Kontrolle in materieller und verfahrensmäßiger Hinsicht gleichwertig sein.<sup>333</sup> Das Kontrollorgan darf keinen Weisungen unterliegen, seine Mitglieder sind jedenfalls für eine bestimmte Zeit fest zu berufen, und es muss personell und sachlich so ausgestattet sein, dass es seine Aufgabe ordnungsgemäß wahrnehmen kann.<sup>334</sup> Für die strategische Ausland-Ausland-Fernmeldeaufklärung hat das Bundesverfassungsgericht 2020 zwei sich ergänzende Kontrollformen verlangt. Die eine ist gerichtsähnlich ausgestaltet und entscheidet in unabhängigen Spruchkörpern förmlich und verbindlich, die andere kontrolliert eigeninitiativ und stichprobenartig den gesamten Überwachungsprozess.<sup>335</sup> Der Gesetzgeber hat diese Vorgaben mit den §§ 40 ff. BNDG schon im geltenden Recht umgesetzt und den UKRat in ein gerichtsähnliches und ein administratives Kontrollorgan gegliedert.

Das Gericht hat auch die institutionelle und personelle Ausgestaltung der gerichtsähnlichen Kontrolle näher bestimmt.<sup>336</sup> Sie ist durch Spruchkörper auszuüben, die mit Personen in gleichsam richterlicher Unabhängigkeit besetzt sind und in formalisierten Verfahren schriftlich und abschließend mit Wirkung für Bundesregierung und Nachrichtendienst entscheiden. Der richterlichen Perspektive muss maßgebliches Gewicht zukommen, während andere juristische Berufserfahrung und technischer Sachverstand einbezogen werden dürfen (es aber ausdrücklich nicht müssen, d.h. Karlsruhe fordert kein Schöffenmodell).<sup>337</sup> Die Kontrolle muss fachlich kompetent, professionalisiert und grundsätzlich hauptamtlich sein und über die erforderlichen Mittel verfügen.<sup>338</sup> Diese Maßstäbe hat das Gericht im Oktober 2024 auf die strategische Inland-Ausland-Fernmeldeaufklärung übertragen.<sup>339</sup> Die G 10-Kommission genügt ihnen danach jedenfalls insoweit nicht, als ihre Mitglieder ehrenamtlich tätig sind und eine durch richterliche Erfahrung geprägte Perspektive gesetzlich nicht gesichert ist.<sup>340</sup> Beanstandet hat das Gericht zudem, dass Änderungen von Beschränkungsanordnungen durch das anordnende BMI keiner hinreichenden Begründungspflicht unterliegen.<sup>341</sup>

## 2. Unabhängige Vorabkontrolle bei sonstigen eingriffsintensiven Maßnahmen

Das Erfordernis einer unabhängigen Vorabkontrolle ist nicht auf Art. 10 GG beschränkt.<sup>342</sup> Für die Wohnraumüberwachung verlangt Art. 13 Abs. 4 GG eine richterliche Anordnung – wobei die Norm hier aufgrund der Verankerung des Richterbegriffs im Wortlaut wohl keine Ersatzkontrolle zulässt. Aber auch andere heimliche Überwachungsmaßnahmen können so schwer wiegen, dass ihre Durchführung einer vorherigen unabhängigen Kontrolle bedarf.<sup>343</sup> Das Bundesverfassungsgericht hat dieses Erfordernis in der Entscheidung zum Bayerischen Verfassungsschutzgesetz aus dem Verhältnismäßigkeitsgrundsatz hergeleitet, namentlich für Online-Durchsuchungen sowie, abhängig von Ausgestaltung und Eingriffsintensität, für den längerfristigen Einsatz Verdeckter Mitarbeiter und Vertrauensleute, längerfristige Observationen und eine länger andauernde Ortung von

<sup>332</sup>Ogorek, in: Epping/Hillgruber, BeckOK GG, 66. Ed. 15.8.2026, Art. 10 Rn. 82.

<sup>333</sup>BVerfGE 30, 1 (23); 100, 313 (361 f.); Ogorek, in: Epping/Hillgruber, BeckOK GG (Fn. oben), Art. 10 Rn. 82.

<sup>334</sup>Ogorek, in: Epping/Hillgruber, BeckOK GG (Fn. oben), Art. 10 Rn. 82.

<sup>335</sup>BVerfGE 154, 152, Rn. 275 f.

<sup>336</sup>BVerfGE 154, 152, Rn. 275, 281 ff.

<sup>337</sup>BVerfGE 154, 152, Rn. 286.

<sup>338</sup>BVerfGE 154, 152, Rn. 287 f.

<sup>339</sup>BVerfGE 170, 79, Rn. 172, 208.

<sup>340</sup>BVerfGE 170, 79, Rn. 207 ff.

<sup>341</sup>BVerfGE 170, 79, Rn. 207 ff.; näher Friedrich, JZ 2025, 403 (409 f.).

<sup>342</sup>Vgl. BVerfGE 162, 1, Rn. 213 f.; Höning, Externe Rechtskontrolle der Nachrichtendienste, 2024, S. 103 ff.

<sup>343</sup>BVerfGE 162, 1, Rn. 214; Höning, Externe Rechtskontrolle (Fn. oben), S. 71 ff., 103 ff.

Mobilfunkendgeräten.<sup>344</sup> Dagegen ist eingewandt worden, aus Angemessenheitserwägungen ließen sich keine zwingenden Vorgaben für die verfahrensrechtliche Ausgestaltung eines Eingriffs ableiten. Das Grundgesetz sehe Richtervorbehalte nur punktuell vor, und ungeschriebene Vorbehalte griffen in das Zuordnungsgefüge der Gewaltenteilung ein.<sup>345</sup> Diese Einwände greifen zu kurz. Die Vorabkontrolle ist eine verfahrensrechtliche Sicherung des Grundrechtsschutzes bei besonders eingriffsintensiven und heimlichen Maßnahmen. Weil Betroffene von dem Eingriff regelmäßig nichts erfahren, ist nachträglicher Rechtsschutz erheblich eingeschränkt. Dieses Defizit begründet ein gesteigertes Kontrollbedürfnis, das eine von der eingreifenden Behörde unabhängige Kontrolle kompensieren kann.<sup>346</sup> Dass der Verhältnismäßigkeitsgrundsatz die Ausgestaltung nicht in allen Einzelheiten festlegt, schließt Mindestanforderungen an eine wirksame Kontrolle nicht aus. Dem Gesetzgeber bleibt ein erheblicher Spielraum. Vorgegeben ist nicht notwendig eine gerichtliche, wohl aber eine dem Gewicht des Eingriffs angemessene, unabhängige und effektive Überprüfung.

Daraus folgt nicht, dass für jede Form unabhängiger Kontrolle dieselben Anforderungen gelten. Die für die strategische Fernmeldeaufklärung entwickelten Maßstäbe lassen sich nicht ohne Weiteres auf jede aus Verhältnismäßigkeitsgründen gebotene Vorabkontrolle übertragen. Die strategische Aufklärung erhält ihr Gewicht vor allem durch ihre Streubreite, weil sie Kommunikationsdaten einer Vielzahl von Personen erfasst, die keinen Anlass gegeben haben. Gezielte Überwachungsmaßnahmen haben eine geringere Streubreite, können für die betroffene Person aber wegen ihrer Zielgerichtetheit und der möglichen Verdichtung personenbezogener Erkenntnisse ebenso schwer wiegen. Der Gesetzgeber darf unterschiedliche Fallgruppen aus Gründen der Typisierung einem einheitlichen Kontrollverfahren unterwerfen. Die organisatorischen Anforderungen, die das Gericht speziell für die strategische Aufklärung entwickelt hat, muss er dabei nicht in allen Einzelheiten übernehmen, darf dies aber selbstverständlich tun.

### **3. Bedeutung des Wegfalls nachträglichen Rechtsschutzes**

Für die erforderliche Kontrolldichte ist außerdem von Bedeutung, ob die betroffene Person die Maßnahme später gerichtlich überprüfen lassen kann. Bei bestimmten Maßnahmen des BND schließt § 103 BNDG-E wie auch bislang das G 10 den Rechtsweg aus, solange die Mitteilung nicht erfolgt ist. Die Mitteilung selbst beschränkt § 100 BNDG-E auf Personen mit hinreichendem Inlandsbezug und lässt weitere Ausnahmen zu, etwa zum Schutz nachrichtendienstlicher Verbindungen. Auch das BVerfSchG-E kennt Mitteilungspflichten, von denen abgesehen oder deren Erfüllung aufgeschoben werden kann (vgl. unter C.V). Wo eine spätere individuelle gerichtliche Kontrolle nicht oder erst sehr spät stattfindet, gewinnt die unabhängige objektivrechtliche Kontrolle zusätzlich an Gewicht. Sie übernimmt dort einen Teil der Kontrolle, die sonst auf Initiative der betroffenen Person ein Gericht leisten könnte. Parlamentarische Kontrolle und behördeninterne Aufsicht erfüllen andere Funktionen und können diesen Ausfall nicht ersetzen.

---

<sup>344</sup>BVerfGE 162, 1, Rn. 218, 332, 348, 354, 361; Schlömer, ZRP 2024, 143 (144); Höning, Externe Rechtskontrolle (Fn. oben), S. 112 ff.

<sup>345</sup>Vgl. Unterreitmeier, GSZ 2019, 233 (237 f.).

<sup>346</sup>Vgl. Höning, Externe Rechtskontrolle (Fn. oben), S. 66 ff.; Alt, Kompensatorische Kontrolle heimlicher Grundrechtseingriffe, 2024, S. 369 f.

## II. Bündelung der Kontrollzuständigkeiten

### 1. Zentralisierung und Gesamtüberblick

Die Forderung, die Zuständigkeiten der G 10-Kommission auf den UKRat zu übertragen, wird in der Literatur seit geraumer Zeit erhoben.<sup>347</sup> Wir halten die Grundentscheidung des Entwurfs für richtig, weil die Alternativen schlechter wären und das Gremium hinsichtlich seines gerichtsähnlichen Kontrollorgans – zumindest bislang! – sehr professionell aufgestellt ist. So sind beispielsweise die Amtsgerichte, auf die einzelne Länder zurückgreifen, für nachrichtendienstliche Prüfungen institutionell nicht spezialisiert, und ihre Ermittlungsrichter nehmen diese Aufgabe neben vielen anderen wahr. Die G 10-Kommission verfügt zwar über eine Geschäftsstelle, ihre Mitglieder arbeiten aber ehrenamtlich und weisen zumindest teilweise politiknahe Hintergründe auf.<sup>348</sup> Für die Bündelung sprechen deshalb die hauptamtliche und fachlich gebündelte Struktur des UKRats und die Vermeidung von Zuständigkeitskonflikten.<sup>349</sup> Der UKRat ist eine oberste Bundesbehörde mit hauptamtlichen, überwiegend richterlichen Mitgliedern, die für ihre Amtszeit Beamte auf Zeit werden und deren Richteramts ruht (§§ 18, 19 UKRatG-E); ergänzt um ein administratives Kontrollorgan, das den Vollzug prüft. Einem ausdrücklichen Richtervorbehalt wie dem des Art. 13 Abs. 2 GG genügt diese Stellung allerdings wohl nicht, jedenfalls aber einer ungeschriebenen Pflicht zur unabhängigen Vorabkontrolle auf gerichtsgleichem Niveau (vgl. schon unter B.I.5).

Eine Kontrolle aus einer Hand erweist sich zudem im Hinblick auf additive Grundrechtseingriffe als sinnvoll.<sup>350</sup> Der Begriff bezeichnet Fälle, in denen mehrere Maßnahmen oder Datenverarbeitungen in ihrem Zusammenhang eine eigenständige oder gesteigerte Belastung entfalten, die über die isolierte Betrachtung der einzelnen Eingriffe hinausgeht.<sup>351</sup> Wird eine Person außerhalb der Wohnung observiert und innerhalb der Wohnung akustisch überwacht, verfügt nur eine Stelle, die beide Maßnahmen kontrolliert, über den Gesamtüberblick, den die Verhältnismäßigkeitsprüfung verlangt.<sup>352</sup> Der UKRat kann die Überwachungsgesamtrechnung, die das Bundesverfassungsgericht verlangt, so auf die Ebene des Einzelfalls holen.<sup>353</sup> Als Alternative wird ein klassischer Richtervorbehalt erörtert, wie ihn Bayern und Hessen über Art. 13 Abs. 4 GG hinaus für verdeckte Zugriffe auf informationstechnische Systeme, qualifizierte Observationen und bestimmte Einsätze Verdeckter Mitarbeiter und Vertrauensleute vorsehen und wie ihn die §§ 22 Abs. 1, 45 MADG für den Militärischen Abschirmdienst kennen.<sup>354</sup> Der spezifische Vorteil des UKRats liegt aber darin, dass die gebündelte Vorabkontrolle mit einer eigenen administrativen Vollzugskontrolle verbunden werden kann, die das Bundesverfassungsgericht für die strategische Fernmeldeaufklärung sogar als Verfassungspostulat identifiziert hat.<sup>355</sup> Diese Kontrolldimension kann ein Richtervorbehalt nicht abbilden, und die Gerichte würde sie angesichts ihres Umfangs an funktionale Leistungsgrenzen führen.

<sup>347</sup>Vgl. Höning, Externe Rechtskontrolle (Fn. oben), S. 321 ff., 329 f.; Friedrich, JZ 2025, 403 (411 ff.); Schlömer, ZRP 2024, 143 (143, 145).

<sup>348</sup>Gerade das hat das Bundesverfassungsgericht beanstandet, BVerfGE 170, 79, Rn. 208 ff.

<sup>349</sup>Vgl. BVerfGE 154, 152, Rn. 286 ff.; zur ehrenamtlichen Besetzung weiterführend Bartodziej, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, VII § 2.

<sup>350</sup>Vgl. Friedrich, JZ 2025, 403 (412); Höning, Externe Rechtskontrolle (Fn. oben), S. 321 ff.

<sup>351</sup>Vgl. BVerfGE 112, 304 (319 f.); 141, 220, Rn. 130; 162, 1, Rn. 287 f.; grundlegend Brade, Additive Grundrechtseingriffe, 2020, S. 33 ff.; ferner Benz, Additive Überwachungsmaßnahmen, 2024, S. 1 ff.

<sup>352</sup>BVerfGE 141, 220, Rn. 130; 162, 1, Rn. 287 ff.; Friedrich, JZ 2025, 403 (412).

<sup>353</sup>BVerfGE 141, 220, Rn. 130; BVerfGE 125, 260, Rn. 218.

<sup>354</sup>Löffelmann/Zöller, Nachrichtendienstrecht (Fn. oben), F. Rn. 49, 67; Schlömer, ZRP 2024, 143 (144).

<sup>355</sup>BVerfGE 154, 152, Rn. 272, 276.

Mit der Verlagerung entfällt allerdings eine Kontrollperspektive. So kontrolliert der BfDI im Rahmen seiner datenschutzrechtlichen Aufsicht neben den Diensten auch das Bundeskriminalamt, die Bundespolizei und den Zoll – sowie die Aufsichtsressorts der Dienste. Wirken nachrichtendienstliche und polizeiliche Überwachung gegenüber derselben Person zusammen, sieht diese sich addierenden Eingriffe künftig niemand mehr aus einer Hand. Der Entwurf begegnet dem mit § 37 Abs. 3 UKRatG-E bislang unvollständig, der beiden Stellen erlaubt, sich über Angelegenheiten ihrer Kontrolltätigkeit auszutauschen, aber dies „insbesondere“ auf grundsätzliche Fragen der Auslegung bezieht. Ob das den Austausch über Maßnahmen gegen bestimmte Personen deckt, ist daher mindestens als offen zu bezeichnen, weil jede Stelle nur „im Rahmen ihrer jeweiligen Kontrollzuständigkeit“ handeln darf. Als Kann-Vorschrift begründet die Norm zudem keine Pflicht zur Auskunft. Wir empfehlen deshalb, § 37 Abs. 3 um eine Befugnis des UKRats zu ergänzen, vom BfDI Auskunft darüber zu verlangen, ob gegen eine bestimmte Person polizeiliche Überwachungsmaßnahmen des Bundes laufen. Klarzustellen ist ferner, dass beide Stellen dabei eingestufte Informationen austauschen dürfen. Die Begründung schließt das zunächst aus und lässt es wenig später doch zu.<sup>356</sup> Die Auskunft sollte auf die Tatsache und den Umfang der Maßnahme beschränkt sein. Eine umgekehrte Mitteilungspflicht des UKRats empfehlen wir nicht, weil die Erkenntnisse eines gerichtsähnlichen Kontrollorgans, das auch Informationen außerhalb der Third Party Rule sieht, besonders schutzbedürftig sind. Schnittstellen zur Polizei und zum bislang in die Reform bedauerlicherweise nur teilweise einbezogenen, überwiegend derzeit zum Amtsgericht Köln verwiesenen Militärischen Abschirmdienst bleiben damit bestehen (vgl. unter F.I). Für den Grundrechtsschutz zählt der gestärkte Blick des UKRats im Einzelfall gleichwohl mehr als der Gesamtblick des BfDI auf den Regierungsbetrieb.<sup>357</sup>

Gegen die Verlagerung werden drei weitere Einwände erhoben. Der erste betrifft die unangekündigte Prüfung und greift nicht, weil § 13 Abs. 2 UKRatG-E jederzeit Zutritt zu den Dienststellen sowie Zugang zu den informationstechnischen Systemen gewährt und § 26 Abs. 1 S. 5 unangekündigte Kontrollen ausdrücklich vorsieht. Das betrifft allerdings nur den Zeitpunkt der Prüfung, nicht ihren Gegenstand (vgl. dazu unter D.X). Der zweite Einwand stellt die Wirksamkeit der neuen gegenüber der bisherigen Aufsicht in Frage. Er lässt sich nur durch einen Vergleich beantworten, der Prüfungsgegenstand, Eigeninitiative, Informationszugang und Durchsetzung getrennt bewertet – und maßgeblich vom tatsächlichen Engagement des administrativen Kontrollorgans des UKRats abhängt, welches naturgemäß vor der Aufgabenzuweisung noch nicht absehbar ist. Wichtig ist jedoch, dass das Bundesverwaltungsgericht erst vor wenigen Monaten entschieden hatte, dass dem BfDI gegenüber den Diensten und ihren Aufsichtsbehörden keine gerichtlich durchsetzbare Rechtsposition zukomme, die der UKRat nun jedoch zumindest bei gewichtigeren Beanstandungen erhält (§ 34, dazu D.XII).<sup>358</sup> Berechtigt ist damit nach hiesiger Wertung allein der dritte wesentliche Einwand, der gegen den UKRat erhoben wird den Zeitpunkt seines ersten öffentlichen Berichts betrifft (vgl. dazu D.XIV).

## 2. Verlagerung der Anordnungszuständigkeit auf die Dienste

Auf den ersten Blick wie eine Verschlechterung der Kontrolle zu bewerten sind die Veränderungen bei der Anordnung der bisherigen Beschränkungsmaßnahmen nach dem G 10. Das G 10 ordnete auf Bundesebene das Innenressort auf Antrag des jeweiligen Dienstes an, also auch etwa für den BND (§ 10 Abs. 1 G 10). Nun könnte man argumentieren, die Ministerialbeteiligung stelle zwar keine

<sup>356</sup>Begr. zu § 37 UKRatG-E, BT-Drs. 21/7868, S. 586 einerseits, S. 587 andererseits; darauf weist Sosna, ZD 2026, 657 (658 f.), hin.

<sup>357</sup>Kritisch der BfDI, 34. Tätigkeitsbericht, BT-Drs. 21/5950, S. 19 f.

<sup>358</sup>BVerwG, Urt. v. 4.3.2026, 6 A 2.24.

unabhängige Kontrolle im verfassungsrechtlichen Sinne dar,<sup>359</sup> schaffe aber eine von der operativ handelnden Behörde getrennte exekutive Prüfungsstufe. Das Ministerium könne das Aufklärungsbegehren mit größerer Distanz prüfen, in sicherheitspolitische Zusammenhänge einordnen und Anträge ändern oder ablehnen.<sup>360</sup> Sähe man dies so, würde die künftig direkt durch die Dienste erfolgende Anordnung als Minus zu werten sein. Tatsächlich handelt es sich aber nur um eine Verschlangung des Antragsprozesses, der kaum mit Rechtsverlusten einhergeht, weil das BMI (was diese Bewertung nachsehen möge) ohnehin im Wesentlichen den Antragstext nur in die Anordnungsvorlage kopierte. Grund hierfür war nicht, dass das Ministerium seinen Pflichten nicht nachkommen wollte, sondern eine Kombination aus vorgeschalteten Prüfungen bis zum Erreichen des Ministeriums innerhalb der Dienste, der niedrigen Anordnungsschwellen und – bezogen auf Folgeanordnungen – einer personell faktisch unmöglich leistbaren Nachkontrolle der bisherigen (vermeintlichen) Überwachungserfolge. Die Anordnung beim BfV je nach Eingriffsgewicht durch Amts- oder Abteilungsleitung (§ 33 BVerfSchG-E) bzw. beim BND durch die Behördenleitung oder eine von ihr bestimmte Vertretung, wobei es sich faktisch um Abteilungs- oder Direktorsleitungen handeln dürfte, sind sachgerecht (§§ 46 bis 48 BNDG-E). Da der Ansatz mit einem Gewinn an operativer Reaktionsfähigkeit einhergeht, und die erheblich ausgeweitete unabhängige Vorabkontrolle einzustellen ist, ist die Anpassung begrüßenswert.

### 3. Prüfungsmaßstab

Mit der Überführung verändert sich möglicherweise der Prüfungsmaßstab. Die G 10-Kommission kontrolliert Zulässigkeit und Notwendigkeit von Beschränkungsmaßnahmen (§ 15 Abs. 5 S. 1, Abs. 6 S. 2 G 10), der UKRat die Rechtmäßigkeit einschließlich der Verhältnismäßigkeit (§ 2 Abs. 1, 2 und 4 UKRatG-E, § 34 BVerfSchG-E, § 97 Abs. 1 BNDG-E). In der Literatur wird der bisherige Maßstab teilweise so verstanden, dass er Opportunitätserwägungen einschließt.<sup>361</sup> Träfe das zu, hätte die Überführung eine gewisse Reduzierung der Kontrolldichte zur Folge. Diese eventuelle Einbuße darf indes nicht überbewertet werden: Die Gerichte haben die Kontrolle der G 10-Kommission ungeachtet des Wortlauts seit jeher als Rechtskontrolle gedeutet,<sup>362</sup> und die Annahme einer Opportunitätskontrolle ist in der Literatur nicht unwidersprochen geblieben.<sup>363</sup> Was mit ihr dogmatisch gemeint sein soll, bleibt ohnehin offen. Soll weder ein behördlicher Ermessensspielraum noch eine politische Zweckmäßigkeitskontrolle bezeichnet werden, ist ein von der Rechtmäßigkeitsprüfung abgrenzbarer Maßstab kaum erkennbar. Die Prüfung der Notwendigkeit lässt sich ohne Weiteres als Bestandteil der Erforderlichkeitsprüfung verstehen.<sup>364</sup> Steht der G 10-Kommission weder ein politischer Beurteilungsspielraum noch ein Ermessen auf der Rechtsfolgenseite zu,<sup>365</sup> ist der Wechsel zur Feststellung der Rechtmäßigkeit überhaupt keine Einbuße, sondern allein eine terminologische Präzisierung.

<sup>359</sup>Vgl. §§ 9 Abs. 2, 10 Abs. 1, 15 Abs. 6 G 10; Friedrich, JZ 2025, 403 (405 f.); Löffelmann/Zöller, Nachrichtendienstrecht (Fn. oben), F. Rn. 56.

<sup>360</sup>Vgl. §§ 9 Abs. 1 und 2, 10 Abs. 1 G 10; Friedrich, JZ 2025, 403 (404 f.).

<sup>361</sup>Friedrich, JZ 2025, 403 (405, 408).

<sup>362</sup>BVerfGE 100, 313 (361 f.); 143, 1, Rn. 54, 57; BVerwGE 130, 180, Rn. 44 ff.; vgl. auch BVerwGE 149, 359, Rn. 40.

<sup>363</sup>Bantlin, Die G 10-Kommission, 2021, S. 157.

<sup>364</sup>Bantlin, Die G 10-Kommission (Fn. oben), S. 157.

<sup>365</sup>Löffelmann/Zöller, Nachrichtendienstrecht (Fn. oben), F. Rn. 52, unter Verweis auf Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, § 15 G 10 Rn. 42; ebenso Bantlin, Die G 10-Kommission (Fn. oben), S. 157.

### III. Besetzung (§ 14 UKRatG-E)

#### 1. Erweiterung des Kreises richterlicher Mitglieder

Erheblichen Einwände bestehen hier gegen die Umgestaltung des gerichtsähnlichen Kontrollorgan. Dass dieses von sechs (§ 43 Abs. 1 S. 1 BNDG) auf neun Mitglieder (§ 14 Abs. 1 UKRatG-E) wachsen soll, ist angesichts des immensen Aufgabenzuwachses nur mehr als verständlich.

Unglücklich ist aber die personelle Ausdehnung bei der Gerichtsherkunft der Kontrolleure: Während das geltende Recht verlangt, dass alle Mitglieder zuvor mit langjähriger Erfahrung am Bundesgerichtshof oder am Bundesverwaltungsgericht tätig waren, können die richterlichen Mitglieder künftig aus allen fünf obersten Gerichtshöfen des Bundes kommen (§ 14 Abs. 2 Nr. 1 lit. a Doppelbuchst. aa). Die Gesetzesbegründung verweist dafür auf einen vermeintlichen Gewinn an zusätzlicher Fach Erfahrung. Streng verfassungsrechtlich ist dagegen zwar nichts zu erinnern, rechtspolitisch halten wir die Öffnung aber für unglücklich und nicht vertrauensbildend. Gegen Richter des Bundessozialgerichts oder des Bundesfinanzhofs spricht nicht ihre Qualifikation, sondern die fehlende Nähe ihrer Vorerfahrungen zum Gegenstand der dem UKRat obliegenden Aufsicht: Wer über Vertrauenspersonen, Online-Durchsuchung oder strategische Aufklärung entscheidet, sollte bestenfalls vorher im Staatsschutzbereich strafrichterlich tätig gewesen sein oder Vorerfahrungen bei der verwaltungsrichterlichen Aufsicht von (Sicherheits-)Behörden vorweisen können haben. Unterschiedliche Arbeitskulturen sind dagegen kein Argument, denn sie bestehen auch zwischen Bundesgerichtshof und Bundesverwaltungsgericht.<sup>366</sup> Soweit die Öffnung Besetzungsschwierigkeiten begegnen soll, worauf die in der Literatur beschriebene begrenzte Auswahl bei der ersten Besetzungsrunde im UKRat hindeutet,<sup>367</sup> muss die Antwort darauf ein verstärktes Werben an Bundesgerichtshof und Bundesverwaltungsgericht sein.

#### 2. Öffnung für nichtrichterliche Mitglieder

Entgegengetreten werden muss aber vor allem und vehement der avisierten Öffnungsklausel hinsichtlich der beruflichen Vorprägung der gerichtsähnlichen Kontrolleure. Nach dem Regierungsentwurf sollen nicht mehr alle (dann: neun) Mitglieder des gerichtsähnlichen Kontrollorgans eine richterliche Vorprägung aufweisen, sondern nur noch sieben von ihnen (§ 14 Abs. 3). Für die übrigen zwei Plätze eröffnet § 14 Abs. 2 UKRatG-E die Mitgliedschaft für Bundesanwälte, für Beamte oberster Bundesbehörden ab der Besoldungsgruppe B 6 mit Befähigung zum Richteramt und mindestens dreijährigem fachlichem Bezug zu Sicherheitsbehörden (Nr. 1 lit. a Doppelbuchst. cc, Nr. 3 und 4) sowie für ehemalige Mitglieder eines von einer Volksvertretung bestellten Organs zur Nachprüfung von Eingriffen in Art. 10 GG, also trotz des verunglückten Wortlauts der in Kürze aufgrund ihrer Auflösung ausscheidenden Mitglieder der G 10-Kommission (lit. b), jeweils mit langjähriger Erfahrung in dieser Tätigkeit (Nr. 2).<sup>368</sup> Verfassungsrechtlich ist keine dieser Gruppen ausgeschlossen. Die Gesetzesbegründung beruft sich zur Rechtfertigung dieses irritierenden Schrittes darauf, dass das Bundesverfassungsgericht der richterlichen Perspektive zwar ein maßgebliches Gewicht zuweist, die Kontrolle aber für andere Erfahrung nicht verschlossen hat.<sup>369</sup> Das ist im Ansatz richtig gelesen und mag bei isolierter Betrachtung aufgrund der im Entwurf angelegten Sicherungen

<sup>366</sup>BVerfGE 154, 152, Rn. 286 f.

<sup>367</sup>Begr. zu § 14 Abs. 2 und 3 UKRatG-E, BT-Drs. 21/7868, S. 571; zur begrenzten Auswahl bei der ersten Besetzung Hoch/Schmidt-Räntsch/Brunst, NVwZ 2023, 712 (713); Löffelmann/Zöller, Nachrichtendienstrecht (Fn. oben), F. Rn. 67.

<sup>368</sup>BT-Drs. 21/7868, S. 166 ff.

<sup>369</sup>Begr. zu § 14 UKRatG-E, BT-Drs. 21/7868, S. 571, unter Hinweis auf BVerfGE 154, 152, Rn. 286.

rechtmäßig sein, wozu die gesetzliche Unabhängigkeit aller Mitglieder (§ 15 UKRatG-E), die Mehrheit von sieben richterlichen Mitgliedern (§ 14 Abs. 3), die richterliche Mehrheit in jeder Kammer (§ 23 Abs. 3) und die einmalige zwölfjährige Amtszeit, während der das bisherige Amt ruht (§ 19 Abs. 1 und 3), zählt. Durch die Vielzahl der dem UKRat künftig zufallenden Aufgaben muss dieser aber vermehrt auf einzelrichterliche Entscheidungen zurückgreifen, die sogar für sehr eingriffsintensive Anordnungen wie jene zur vollständigen Online-Durchsuchung vorgesehen sind (§ 97 Abs. 1 Nr. 14 i.V.m. § 37 Abs. 2 und 3 BNDG-E, § 28 Abs. 1 UKRatG-E). Hinzu tritt deutliche rechtspolitische Kritik: Ein Organ, das künftig ein Vielfaches an Anordnungen prüft, braucht aber personelle Stabilität und langjährige Kontrollerfahrung, die nicht jede der vorgesehenen neuen Berufsgruppen strukturell in dem erforderlichen, sehr hohen Maße leisten kann:

#### **a) Bundesanwälte**

Die Öffnung für Bundesanwälte halten wir für fachlich vertretbar. Ihre langjährige justizielle Erfahrung in Staatsschutzsachen ergänzt die richterliche Perspektive sachgerecht, und sie gehörten bereits dem Unabhängigen Gremium beim Bundesgerichtshof an.<sup>370</sup> Maßgeblich ist ihre unabhängige Amtsstellung im UKRat und nicht, ob ihre bisherige Stellung richterlicher Unabhängigkeit gleichkam. Die frühere Weisungsgebundenheit ist von der Rechtsstellung im Kontrollamt zu unterscheiden, für die die Garantien der §§ 15 und 22 Abs. 1 UKRatG-E auch für nichtrichterliche Mitglieder gelten. Zudem sind die Bundesanwälte an die Arbeitsweise der auf absehbare Zeit durch den Bundesgerichtshof geprägten richterlichen Mitgliedschaft gewöhnt, was im Hinblick auf die erforderlichen schnellen Startfähigkeiten des neu zusammengesetzten Senats bei der Erfüllung seiner zahlreichen Kontrollaufgaben begrüßenswert ist.

#### **b) Beamte oberster Bundesbehörden**

Im Ergebnis ablehnend beurteilen wir die Öffnung für höhere Beamte der obersten Bundesbehörden, gegen die auch in der Literatur Vorbehalte artikuliert worden sind.<sup>371</sup> Ihre Erfahrung in Organisation, Leitung und Sicherheitsverwaltung wäre zwar eine ergänzende Perspektive. Gegen ihre Einbeziehung spricht aber, dass sie aus der Exekutive stammen, deren Steuerung sie bislang selbst wahrgenommen haben, und dass ihre Erfahrung langjähriger justizieller Kontrolle nicht gleichwertig ist. Das Bundesverfassungsgericht verlangt gerade, personell wie strukturell auf eine hinreichende Distanz zum kontrollierten Dienst Bedacht zu nehmen und auf eine ausgewogene Zusammensetzung der Kontrollinstanz zu achten.<sup>372</sup> Aus einer früheren Tätigkeit in der Exekutive folgt zwar keine fortbestehende Weisungsabhängigkeit im rechtlichen Sinne. Davon zu trennen ist aber die konkrete Vorbefassung, etwa wenn ein Mitglied als Ministerialbeamter jahrelang an der möglichst intensiven Vorbereitung, Anordnung und Durchsetzung gerade jener Maßnahme beteiligt war, die er nun kontrollieren soll. Zwar trägt § 9 VerfO-UKRat konkreten Interessenkonflikten Rechnung, indem er die §§ 20, 21 VwVfG entsprechend anwendet und die Entscheidung dem Senat zuweist.<sup>373</sup> Die faktisch häufig zu starke Prägung durch die Behördenbelange, denen der UKRat als natürlicher Gegenspieler gegenübersteht, beseitigt das aber nicht, auch wenn er sie nicht verhindern, sondern „nur“ einhegen soll.

<sup>370</sup>Löffelmann/Zöller, Nachrichtendienstrecht (Fn. oben), F. Rn. 57.

<sup>371</sup>Vgl. Gärditz, Ausschuss-Drs. 19(4)731 A, S. 22 f.

<sup>372</sup>BVerfGE 154, 152, Rn. 287.

<sup>373</sup>§ 9 VerfO-UKRat v. 22.6.2026, BAnz AT 5.8.2026 B4, i.V.m. §§ 20, 21 VwVfG.

### c) Künftig ehemalige Mitglieder der G 10-Kommission

Ebenfalls abzulehnen ist die Öffnung für ehemalige Mitglieder der G 10-Kommission.<sup>374</sup> Die Kritik des Bundesverfassungsgerichts an der Kommission betraf zwar nur die ehrenamtliche Amtsausübung und die fehlende Sicherung einer richterlich geprägten Perspektive hinsichtlich ihrer heutigen defizitären Ausgestaltung,<sup>375</sup> woraus kein verfassungsrechtlicher Ausschluss früherer Kommissionsmitglieder von einer zukünftig hauptamtlichen Kontrolltätigkeit folgt. Auch eine frühere Rolle als Bundestagsabgeordneter, wie es bei einigen Mitgliedern der G 10-Kommission der Fall ist, rechtfertigt für sich genommen nicht den Schluss, dass die betreffende Person im Kontrollamt nicht unabhängig entscheiden werde. Wer einem ehrenamtlichen Kontrollorgan angehört hat, bringt damit aber noch nicht mit, was eine hauptamtliche und hochkomplexe gerichtsähnliche Rechtskontrolle verlangt. Auch die Befähigung zum Richteramt und G 10-Erfahrung gewährleisten das für sich genommen nicht. Dass § 14 Abs. 2 Nr. 2 hier langjährige Erfahrung verlangt, hilft, heilt aber nicht den strukturellen Einwand, dass ebendiese Erfahrung unter Bedingungen erworben wurde, die das Bundesverfassungsgericht beanstandet hat. Zusammen mit der Öffnung für Beamte oberster Bundesbehörden empfehlen wir deshalb sehr stark, § 14 Abs. 2 Nr. 1 lit. a Doppelbuchst. cc und lit. b zu streichen. Dafür sprechen fachliche Eignung, professionelle Kontrollerfahrung und institutionelle Distanz.

### IV. Altersgrenze (§ 20 Abs. 1 S. 1 UKRatG-E)

Die Mitglieder des gerichtsähnlichen Kontrollorgans treten mit Ablauf der Amtszeit, spätestens mit Vollendung des 70. Lebensjahres in den Ruhestand (§ 20 Abs. 1 S. 1 UKRatG-E, bisher § 45 Abs. 4 S. 1 BNDG). Bundesrichter erreichen die Regelaltersgrenze dagegen mit 67 Jahren (§ 48 Abs. 1 DRiG). Vereinzelt ist diese Abweichung als „sehr misslich“ bezeichnet worden,<sup>376</sup> wir halten sie jedoch für nachvollziehbar. Bundesrichter wechseln regelmäßig erst gegen Ende ihrer Laufbahn in den UKRat, und die Tätigkeit dort verlangt trotz großer Vorerfahrung eine erhebliche Einarbeitung in die operativen Besonderheiten nachrichtendienstlicher Tätigkeit. Hinzu kommt ein struktureller Unterschied: Richterliche Entscheidungen würdigen typischerweise einen abgeschlossenen Sachverhalt, die Vorabkontrolle ist dagegen prognostisch geprägt. Die im Kontrollorgan erworbene Erfahrung sollte deshalb nicht durch eine (zu) niedrige Altersgrenze vorschnell verloren gehen.

### V. Wahl (§§ 16, 17 UKRatG-E)

Die Mitglieder des gerichtsähnlichen Kontrollorgans wählt das PKGr mit einfacher Mehrheit (§ 17 UKRatG-E). Das Vorschlagsrecht der Präsidenten des Bundesgerichtshofs und des Bundesverwaltungsgerichts (§ 43 Abs. 3 BNDG) entfällt. An seine Stelle treten eine Ausschreibung (§ 16), die Vorstellung der Bewerber vor dem Gremium, die Anhörung der Bundesregierung sowie Stellungnahmen des zuständigen Gerichtspräsidenten, des Generalbundesanwalts oder des Dienstvorgesetzten (§ 17 Abs. 2 S. 2 Nr. 1 bis 3). Die Anhörung der Bundesregierung gibt den Aufsichtsbehörden der kontrollierten Dienste eine Möglichkeit der Einflussnahme, ohne ihnen ein Veto zuzubilligen. Verfassungsrechtlich ist diese Bestellung tragfähig. Art. 10 Abs. 2 S. 2 GG verlangt für den Rechtswegausschluss (§ 22 Abs. 5 BVerfSchG-E, § 103 BNDG-E) die Nachprüfung durch von der Volksvertretung bestellte Organe. Das PKGr ist ein Organ des Bundestages, es wählt schon heute die

<sup>374</sup>Kritisch zur Öffnung auch Löffelmann, VerfBlog v. 20.8.2026 (Fn. oben).

<sup>375</sup>BVerfGE 170, 79, Rn. 207 ff.; BVerfGE 154, 152, Rn. 286 f.

<sup>376</sup>Friedrich, JZ 2025, 403 (408) Fn. 61.

Mitglieder des UKRats (§ 43 Abs. 4 BNDG) und bestellt seit Jahrzehnten die Mitglieder der G 10-Kommission (§ 15 Abs. 1 G 10).<sup>377</sup>

Rechtspolitisch ist die Regelung aber noch teilweise unausgegoren. So sollte das Vorschlagsrecht der Gerichtspräsidenten erhalten bleiben – nach hiesigem Vorschlag, der die Erweiterung der Richterriege ablehnt, in bisheriger Konstellation. Die Präsidenten kennen ihre Häuser und wissen, wer für ein Amt geeignet ist, das Staatsschutzkenntnis, Belastbarkeit und Verschwiegenheit verlangt. Das Vorschlagsrecht fördert personelle Kontinuität und fachliche Passung, während die Wahlentscheidung beim Deutschen Bundestag verbleibt (zur dort entscheidenden Stelle sogleich). Für den Fall, dass die Präsidien ihr Vorschlagsrecht nicht ausüben können, sollte das Gremium ausnahmsweise ohne Vorschlag wählen dürfen. Stellungnahmen sieht § 17 Abs. 2 zudem nur für Richter, Bundesanwälte und Beamte vor, nicht aber für Mitglieder der G 10-Kommission. Mit der empfohlenen Streichung erledigt sich diese Ungleichbehandlung, hilfsweise wäre eine gleichwertige Qualifikationsprüfung vorzusehen. Richtig ist, dass Präsident und Vizepräsident richterliche Mitglieder bleiben (§ 17 Abs. 3), wobei das Auswahlverfahren auch Führungs- und Verwaltungskompetenz berücksichtigen sollte.

Offen diskutiert werden sollte, ob das PKGr für die Rechte des Bundestages verantwortlich bleibt. Die dortige Wahl mit einfacher Mehrheit ist zumindest demokratietheoretisch nicht unproblematisch. Der Bundestag hat die Mitgliederzahl des PKGr für die 21. Wahlperiode auf neun festgelegt.<sup>378</sup> Tatsächlich gehören ihm derzeit sechs gewählte Mitglieder an, drei der CDU/CSU, zwei der SPD und eines von Bündnis 90/Die Grünen. Die für die AfD und Die Linke vorgesehenen Sitze sind unbesetzt, weil die vorgeschlagenen Kandidaten die erforderliche Mehrheit im Plenum nicht erreicht haben. Die Opposition ist damit nur durch ein Mitglied vertreten, und die regierungstragenden Fraktionen können ihre Kandidaten ohne Kompromiss durchsetzen. Theoretisch wäre es wohl sogar möglich, überhaupt keinen Oppositionellen in das Gremium zu wählen – eine Entscheidung, die bei anderen Machtverhältnissen im Parlament zum Beispiel eine Fraktion veranlassen könnte, deren hinter ihr stehende Partei bis dato selbst als verfassungsfeindlich eingestuft wurde. Für die einfache Mehrheit spricht aber, dass sie (auch wenn es hier derzeit zu Verzögerungen kommt) theoretisch Wahlen zuverlässig ermöglicht und Vakanzen vermeidet. Solche kann sich ein Organ, das über jeden schweren Eingriff des Inlands- und Auslandsnachrichtendienstes entscheidet, nicht leisten. Eine Zweidrittelmehrheit nach dem Vorbild des § 6 Abs. 1 BVerfGG würde zudem selbst bei der gegenwärtigen Zusammensetzung wenig ändern. Qualifizierte Mehrheiten erhöhen zugleich das Risiko verzögerter Nachbesetzungen und können Sperrminoritäten schaffen.<sup>379</sup> Gerade diese Gefahr hat den Gesetzgeber 2024 veranlasst, für die Wahl der Verfassungsrichter einen Ersatzwahlmechanismus zu schaffen (Art. 93 Abs. 2 S. 3 GG, § 7a Abs. 5 BVerfGG).<sup>380</sup> Wir halten deshalb an der einfachen Mehrheit im Gremium fest, solange das Vorschlagsrecht der Gerichtspräsidenten die fachliche Auswahl sichert. Sollte der Gesetzgeber am Wegfall des Vorschlagsrechts festhalten, sollte er die Wahlentscheidung mit einfacher Mehrheit jedenfalls aus dem PKGr herausholen und dem Plenum des Bundestages übertragen, in dem die Opposition vollständig vertreten ist.

<sup>377</sup> § 15 Abs. 1 S. 4 G 10; weiterführend Bartodziej, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, VII § 2.

<sup>378</sup> Plenarbeschluss v. 26.6.2025 auf Antrag der Fraktionen der CDU/CSU und SPD, BT-Drs. 21/563.

<sup>379</sup> Vgl. BT-Drs. 20/12978, S. 5.

<sup>380</sup> Gesetz zur Änderung des Grundgesetzes (Art. 93 und 94) v. 20.12.2024, BGBl. 2024 I Nr. 439.

## VI. Verfahren der Vorabkontrolle und Einzelentscheidung (§§ 23, 27, 28, 30 UKRatG-E)

Das Verfahren der Vorabkontrolle ist im Regierungsentwurf gut konstruiert. Der UKRat kann demnach Maßgaben und Einschränkungen anordnen (§ 27 Abs. 1 S. 2). Das entspricht auch seiner bisherigen Praxis, Anordnungen nicht pauschal abzulehnen, sondern mit Auflagen zu versehen. Dass der UKRat nur selten Anordnungen zurückweist, belegt deshalb übrigens kein Kontrolldefizit. Die Anträge der Dienste müssen allerdings so substantiiert ausfallen, dass eine Prüfung möglich ist. Eine allgemeine Pflicht, alle entscheidungserheblichen Umstände offenzulegen, wie sie das Bundesverfassungsgericht verlangt, fehlt im UKRatG-E bislang.<sup>381</sup> Sie sollte in § 27 Abs. 2 aufgenommen werden, wofür der Entwurf selbst ein Vorbild enthält: Für Vorlagen des Militärischen Abschirmdienstes gilt über § 22 Abs. 1a MADG-E bereits § 22 Abs. 1 S. 3 und 4 MADG entsprechend. (Zur Kenntnis der Quellenidentität vgl. unter D.XI und C.IV.3.)

Das gerichtsähnliche Kontrollorgan entscheidet grundsätzlich in Kollegialspruchkörpern: dem Senat und den Kammern (§ 23 Abs. 1). § 28 Abs. 1 erlaubt dem zuständigen Spruchkörper aber, einem seiner Mitglieder einen Vorgang der Vorabkontrolle zur alleinigen Entscheidung zu übertragen. Ausgenommen sind Ersuchen des Dienstes um eine Kollegialentscheidung, die erstmalige Vorlage einer strategischen Aufklärungsmaßnahme nach § 47 Abs. 1 BNDG-E sowie Anordnungen mit tatsächlichen oder rechtlichen Schwierigkeiten oder grundsätzlicher Bedeutung (§ 28 Abs. 1 S. 2). Über die Grundanordnungen für erweiterte Maßnahmen des BND entscheidet stets der Senat (§ 27 Abs. 3 Nr. 2 lit. b). Die Begründung rechtfertigt die Einzelentscheidung damit, dass das Bundesverfassungsgericht das Erfordernis eines Spruchkörpers nur für die strategische Fernmeldeaufklärung aufgestellt habe, und hält sie für die neu hinzukommenden Maßnahmen für „ausreichend und verfahrensökonomisch geboten“.<sup>382</sup> Der Rechtsprechung lässt sich tatsächlich nicht entnehmen, dass die Vorabkontrolle stets kollegial erfolgen müsste,<sup>383</sup> das sonstige Prozessrecht kennt die Übertragung auf den Einzelrichter seit jeher (§§ 348, 348a, 526 ZPO, § 6 VwGO, § 6 FGO), und der strafgerichtliche Ermittlungsrichter entscheidet allein über besonders eingriffsintensive Maßnahmen (§§ 162, 169 StPO). Bei der erwarteten Fallzahl ist die Einzelentscheidung zudem unvermeidlich, und die Ausnahmen sind richtig gesetzt. Rechtsstaatlich unproblematisch ist die Übertragung gleichwohl nicht. Die Maßnahmen werden heimlich durchgeführt, und die Dienste sind nicht in allen Fällen zur Mitteilung verpflichtet (§§ 100, 101 BNDG-E, § 35 Abs. 2 bis 4 BVerfSchG-E). Weil eine nachträgliche gerichtliche Korrektur häufig entfällt, kommt der personellen Absicherung der vorgelagerten Kontrolle besonderes Gewicht zu. Nach dem Entwurf steht die Übertragung im Ermessen des Spruchkörpers, und außerhalb der strategischen Aufklärung ist sie nicht auf Verlängerungen oder Erweiterungen beschränkt. Auch eine erstmalige Anordnung kann einem einzelnen Mitglied übertragen werden. Die Sperre des § 28 Abs. 2, nach der den Mitgliedern des Senats im ersten Jahr nach ihrer Ernennung keine Einzelentscheidungen übertragen werden dürfen, ermöglicht eine Einarbeitung, sichert aber nicht die richterliche Prägung der Einzelentscheidung.<sup>384</sup> Die im Kollegium vorhandene richterliche Erfahrung wirkt bei der alleinigen Entscheidung eines nichtrichterlichen Mitglieds nicht oder nur bedingt fort. Rechtspolitisch empfehlen wir deshalb zwei Ergänzungen. Erstmalige Anordnungen besonders eingriffsintensiver Maßnahmen, namentlich Online-Durchsuchungen und der längerfristige Einsatz von Vertrauenspersonen, sollten dem Kollegium vorbehalten bleiben. Nichtrichterlichen Mitgliedern sollten Einzelentscheidungen nur bei Verlängerungen übertragen werden

<sup>381</sup>BVerfGE 162, 1, Rn. 215; vgl. auch BVerfGE 141, 220, Rn. 118.

<sup>382</sup>Begr. zu § 28 UKRatG-E, BT-Drs. 21/7868, S. 579, unter Bezugnahme auf BVerfGE 154, 152, Rn. 275.

<sup>383</sup>Vgl. BVerfGE 154, 152, Rn. 275; demgegenüber BVerfGE 162, 1, Rn. 213 ff., 217 ff.

<sup>384</sup>Ausgenommen sind nur Präsident und Vizepräsident, Begr. zu § 28 Abs. 2 UKRatG-E, BT-Drs. 21/7868, S. 579.

dürfen. Beide Sicherungen verlören an ihrer Dringlichkeit, wenn auch künftig – wie von hieraus unter D.III.1 sehr stark angeraten – ausschließlich richterliche Mitglieder dem gerichtsähnlichen Organ angehören und diese allein aus dem Bundesgerichtshof und dem Bundesverwaltungsgericht gewonnen werden.

Schließlich wird von einigen Stimmen gefordert, nach dem Vorbild der Amici im amerikanischen FISA-Verfahren in allen Fällen eine Vertretung des Bürgerinteresses zu beteiligen. Verfassungsrechtlich ist das nicht zwingend erforderlich, und der Gesetzgeber kann mit guten Gründen beim bestehenden Modell bleiben. Will er der Forderung entgegenkommen, wäre ein Kompromiss denkbar, der eine solche Vertretung auf Grundsatzverfahren vor dem Senat beschränkt. Sie bräuchte fachliche Unabhängigkeit, Zugang zu den Unterlagen und Freiheit von Weisungen des Spruchkörpers. Ein Bediensteter des administrativen Kontrollorgans könnte jene Rolle deshalb nur übernehmen, wenn ihm eine entsprechende Stellung gesetzlich zugesichert ist.

## **VII. Begründungspflicht (§ 23 Abs. 6 UKRatG-E)**

Beschlüsse des gerichtsähnlichen Kontrollorgans sind schriftlich zu begründen, wenn die Rechtswidrigkeit einer Maßnahme festgestellt wird, die Feststellung der Rechtmäßigkeit mit Maßgaben oder Einschränkungen verbunden ist oder die Vorlage Besonderheiten aufweist oder grundsätzliche Bedeutung hat (§ 23 Abs. 6 UKRatG-E). Die Begründung hebt hervor, dass die Schriftlichkeit der Handlungssicherheit der Dienste diene und die Rolle des UKRats bei der Auslegung des Nachrichtendienstrechts stärke.<sup>385</sup> Das Bundesverfassungsgericht hat 2024 wie dargestellt beanstandet, dass das BMI Änderungen der beantragten G 10-Anordnung nicht begründen müsse.<sup>386</sup> Diese Kritik kann für externe Kontrolle naturgemäß nicht weniger gelten als für innerexekutive. Auch Bayern und Hessen, die für die richterlichen Kontrollentscheidungen über Zugriffe auf informationstechnische Systeme (Art. 10 BayVSG), längerfristige Observationen (§ 11 Abs. 2, 4 HVSG) und den Einsatz Verdeckter Mitarbeiter und Vertrauensleute (§§ 12 Abs. 3, 13 Abs. 1 HVSG) eine Begründungspflicht vorsehen, haben dies aufgegriffen, wenngleich die hessische Regelung den Umfang ausdrücklich auf die „wesentlichen Gründe“ begrenzt (§ 5a Abs. 4 S. 3 Nr. 4 HVSG).

## **VIII. Verfahrensstellung der Mitglieder (§ 23 Abs. 5, § 28 Abs. 3, § 30 UKRatG-E)**

### **1. Begrenzte individuelle Verfahrensrechte**

Die verfahrensrechtliche Stellung der einzelnen Mitglieder des gerichtsähnlichen Kontrollorgans ist schwach ausgestaltet. Ein Kammermitglied kann einen Vorgang dem Senat nur vorlegen, wenn es die Sache für grundsätzlich bedeutsam hält (§ 28 Abs. 3). Beim Bundesverfassungsgericht führt dagegen jedes Kammermitglied die Befassung des Senats herbei, indem es einer Kammerentscheidung nicht zustimmt, weil diese nur einstimmig ergehen dürfen (§ 93d Abs. 3 S. 1 BVerfGG, § 40 Abs. 2 GOBVerfG). In der Literatur ist zudem gefordert worden, im UKRat ebenfalls „eigenständige ergänzende Aufklärungs- und Informationsbeschaffungsrechte“ einzuräumen.<sup>387</sup>

<sup>385</sup>Begr. zu § 23 Abs. 6 UKRatG-E, BT-Drs. 21/7868, S. 575.

<sup>386</sup>BVerfGE 170, 79, Rn. 207 ff.; näher Friedrich, JZ 2025, 403 (409 f.).

<sup>387</sup>Fahrner, GSZ 2023, 223 (226).

## 2. Grenzen der Gerichtsähnlichkeit

Im gerichtsähnlichen Verfahren des UKRats sind keine Individualrechte der Betroffenen vorgesehen. Dies ist insoweit konsequent, als der UKRat nun einmal kein Gericht ist, sondern eine gerichtsähnliche Vorabkontrolle bietende unabhängige oberste Bundesbehörde (§ 41 Abs. 1 und 3 BNDG, § 1 UKRatG-E). § 22 Abs. 1 erklärt zwar die Vorschriften über Unabhängigkeit und Disziplinarmaßnahmen der Bundesrichter für entsprechend anwendbar – diese Annäherung betrifft aber Unabhängigkeit und Qualität der Kontrolle, nicht die Übertragung der gerichtlichen Verfahrensordnungen.<sup>388</sup> Maßgeblich ist die soeben angesprochene Funktion der gerichtsähnlichen Kontrolle. Sie muss der gerichtlichen Kontrolle gleichwertig und mindestens ebenso wirkungsvoll sein, Gleichwertigkeit bedeutet aber nicht Identität. Welche Verfahrensrechte den einzelnen Mitgliedern zukommen müssen, hat das Bundesverfassungsgericht nicht vorgegeben.<sup>389</sup> Mit dem Modell des In-Camera-Senats ist zudem auch ein „echtes“ gerichtliches Verfahren bekannt, in dem der Betroffene nicht mitwirken kann; hier wie da liegt es in der Natur des Verfahrensstoffes. Die soeben vorgeschlagenen Individualrechte sind daher ausschließlich eine zusätzliche Absicherung der Binnenkontrolle, nicht eine notwendige Folge der Gerichtsähnlichkeit.<sup>390</sup>

## 3. Ergebnis: Minderheitsvotum, Stimmengleichheit, Besetzung der Kammern

Rechtspolitisch ist die Stellung der Mitglieder dennoch zu überprüfen. Erwägenswert ist ein Recht überstimmter Mitglieder, nicht nur ihr Abstimmungsverhalten, sondern auch die Gründe ihrer abweichenden Rechtsauffassung oder Tatsachenwürdigung zu den Akten zu geben. Ein solches begründetes Minderheitsvotum sieht der Entwurf nicht vor. Eine weitere Stärkung ließe sich bei der Stimmengleichheit erreichen. Nach § 23 Abs. 5 S. 4 UKRatG-E gibt wie bisher (§ 49 Abs. 3 S. 4 BNDG) die Stimme des Vorsitzenden den Ausschlag. Bei einer nur mit zwei Mitgliedern beschlussfähigen Dreierkammer entscheidet der Vorsitzende dann „quasi alleine“, was im Schrifttum zu Recht als wenig überzeugend bezeichnet wird.<sup>391</sup> Der Entwurf entschärft das Problem, weil § 23 Abs. 3 Zahl und Größe der Kammern nicht mehr festlegt, sondern der autonomen Ausgestaltung überlässt.<sup>392</sup> Wir empfehlen deshalb, gesetzlich abzusichern, dass Kammerentscheidungen in voller Besetzung ergehen, oder bei einer zweiköpfig besetzten Kammer auf den Stichentscheid zu verzichten und stattdessen die vollständige Besetzung oder die Befassung des Senats vorzusehen. Das Bundesverfassungsgericht bietet dafür ein Vorbild, dessen Dreierkammern nur einstimmig entscheiden (§ 15a Abs. 1 S. 2, § 93d Abs. 3 S. 1 BVerfGG).

## IX. Gefahr im Verzug (§ 31 UKRatG-E)

Bei Gefahr im Verzug darf der Dienst eine kontrollbedürftige Maßnahme selbst in Gang setzen, wenn sonst ihr Zweck gefährdet wäre.<sup>393</sup> Die sofort vollziehbare Anordnung ist unverzüglich vorzulegen (§ 31 Abs. 2 S. 1) und tritt außer Kraft, wenn der UKRat sie nicht binnen drei Werktagen bestätigt (Abs. 3 S. 1). Ist eine Entscheidung in dieser Frist wegen des Umfangs oder wegen tatsächlicher oder rechtlicher Schwierigkeiten nicht möglich, soll der Spruchkörper die Fortgeltung beschließen, sofern

<sup>388</sup>Vgl. § 22 Abs. 1 UKRatG-E; BVerfGE 154, 152, Rn. 285 f.; Hoch/Schmidt-Räntsch/Brunst, NVwZ 2023, 712 (712 f.), die hervorheben, dass die gerichtsähnliche Kontrolle gerade kein Gericht sein durfte.

<sup>389</sup>BVerfGE 154, 152, Rn. 275 f.; vgl. auch Tombrink, GSZ 2024, 28 (29).

<sup>390</sup>Vgl. Fahrner, GSZ 2023, 223 (226 f.); kritisch zu dessen Ausführungen über Minderheitenrechte Schmidt-Räntsch, GSZ 2025, 165 (167 Fn. 17).

<sup>391</sup>Hoch/Schmidt-Räntsch/Brunst, NVwZ 2023, 712 (713 f.).

<sup>392</sup>Begr. zu § 23 Abs. 3 UKRatG-E, BT-Drs. 21/7868, S. 574 f.

<sup>393</sup>Zur bisherigen Praxis des Eilverfahrens beim UKRat Schmidt-Räntsch, GSZ 2025, 213 (213 f.).

keine ernstlichen Zweifel an der Rechtmäßigkeit bestehen (Abs. 4 S. 1). Die Bestätigung muss dann unverzüglich folgen (Abs. 4 S. 2).<sup>394</sup> Der Mechanismus ist im Grundsatz tragfähig. Für die Ausgestaltung bieten die zu Richtervorbehalten entwickelten Grundsätze Orientierung: Die Eilkompetenz muss Ausnahme bleiben, und organisatorische Vorkehrungen müssen eine rechtzeitige Entscheidung ermöglichen.<sup>395</sup> Dem trägt § 31 Abs. 1 Rechnung, weil die Eilkompetenz nur greift, wenn der Zweck andernfalls vereitelt oder wesentlich erschwert würde.

(Reiner) Klarstellungsbedarf besteht bei der Fortgeltungsentscheidung, die keine ernstlichen Zweifel an der Rechtmäßigkeit verlangt. Nicht jede ungeklärte Frage begründet solche Zweifel,<sup>396</sup> umgekehrt darf aus dem Umstand, dass die Prüfung noch nicht geleistet werden konnte, nicht auf das Fehlen ernstlicher Zweifel geschlossen werden. Die im verwaltungsgerichtlichen Eilrechtsschutz anerkannte Folgenabwägung bietet keinen übertragbaren Auffangmaßstab, zumal dort die Prüfungsintensität mit dem Gewicht der drohenden Rechtsverletzung steigt.<sup>397</sup> Ihre Einführung würde den Maßstab verändern, nicht klarstellen. Präzisierungsbedürftig sind deshalb die tatsächliche Grundlage und die Prüfungstiefe der Fortgeltungsentscheidung sowie der Umgang mit verbleibenden Ungewissheiten. Die Soll-Vorgabe in § 31 Abs. 4 S. 1 sollte zugleich in eine Kann-Regelung überführt werden, weil eine gerichtsähnliche Kontrolle keine gesetzlich vorgezeichnete Regelentscheidung über die Fortgeltung eines Eingriffs kennt. Nach dem Wortlaut können die Gründe für eine nicht fristgerechte Entscheidung zudem im Organisationsbereich des UKRats liegen.<sup>398</sup> Eine nur ausnahmsweise ohne vorherige Kontrolle begonnene Maßnahme darf aber nicht deshalb fortgeführt werden, weil die Kontrollinstanz nicht rechtzeitig entscheiden kann. Der UKRat muss personell und organisatorisch so ausgestattet sein, dass Eilfälle kurzfristig entschieden werden. Der bestehende Eildienst zeigt, dass das möglich ist.<sup>399</sup>

Eine absolute Höchstfrist ab Vollzugsbeginn enthält die Norm nicht. Die Dreitagesfrist bezeichnet nur die äußerste Grenze der ersten Bestätigungsphase und darf nicht als reguläre Bearbeitungsfrist verstanden werden. Rechtspolitisch empfehlen wir zudem drei Ergänzungen: eine lückenlose Dokumentation der Zeitpunkte, eine begründete Entscheidung über die Fortgeltung und eine eng begrenzte Höchstdauer der Fortgeltung ohne Bestätigung. Dazu wäre § 31 Abs. 4 S. 3 dahin zu ergänzen, dass die Anordnung spätestens mit Ablauf dieser Höchstfrist außer Kraft tritt, wenn sie bis dahin nicht bestätigt ist, und dass die Pflicht zur unverzüglichen Entscheidung unberührt bleibt. Diese Sicherungen würden zugleich verhindern, dass ein Dienst die Frist faktisch verlängert, indem er die Akten verzögert übermittelt.

## **X. Administrative Kontrolle und Prüfaufträge (§§ 25, 26, 32 UKRatG-E)**

Das administrative Kontrollorgan ist dem gerichtsähnlichen Organ nachgeordnet (§ 25 Abs. 3), seine Leitung ist an Weisungen der Behördenleitung gebunden (§ 25 Abs. 2). Es prüft anlassunabhängig und strukturbezogen im Rahmen eines Prüfprogramms, das der Senat für bis zu 24 Monate beschließt und den Diensten, der Aufsicht und dem PKGr mitteilt (§ 26 Abs. 1 und 2, § 32 Abs. 2).<sup>400</sup> Einen konkreten Prüfauftrag können Senat oder Kammer nur für die Durchführung der strategischen

<sup>394</sup>BT-Drs. 21/7868, S. 172 f.

<sup>395</sup>BVerfGE 103, 142 (155 f.); Löffelmann/Zöller, Nachrichtendienstrecht (Fn. oben), F. Rn. 48.

<sup>396</sup>Vgl. BVerwG, Beschl. v. 16.2.2017, 9 VR 3.16, Rn. 7, 29.

<sup>397</sup>BVerwG, Beschl. v. 16.2.2017, 9 VR 3.16, Rn. 6.

<sup>398</sup>Begr. zu § 31 UKRatG-E, BT-Drs. 21/7868, S. 581.

<sup>399</sup>Hoch/Schmidt-Räntsch/Brunst, NVwZ 2023, 712 (715 f.).

<sup>400</sup>Zur bisherigen Praxis der administrativen Kontrolle, insbesondere zu Prüfplan, Stichproben und Beanstandungsverfahren, Fritze/Kaiser/Schmidt-Räntsch/Zahner, NVwZ 2025, 1563 (1567 f.).

Aufklärung nach § 32 BNDG-E erteilen (§ 26 Abs. 3). Andere einzelfallbezogene Kontrollen kennt der Entwurf nur als Einzelfallkontrolle durch das gerichtsähnliche Organ selbst, soweit ihm bestimmte Kontrollgegenstände vorzulegen sind (§ 97 Abs. 3 BNDG-E, § 34 Abs. 2 BVerfSchG-E). Die Begründung stellt klar, dass die administrative Kontrolle auf Datenverarbeitungsprozesse und -strukturen gerichtet ist. Einzelvorgänge werden stichprobenartig einbezogen, eine einzelfallbezogene Verlaufskontrolle findet dagegen grundsätzlich nicht statt.<sup>401</sup> Damit weicht der Entwurf erheblich von § 51 Abs. 2 S. 2 BNDG ab, der einzelfallbezogene Prüfaufträge bislang nicht auf die strategische Aufklärung beschränkt, sondern auch für Eingriffe in informationstechnische Systeme von Ausländern im Ausland zulässt (§ 34 BNDG). Die Beschränkung begründet der Entwurf mit dem besonderen Kontrollbedarf der strategischen Aufklärung, die wegen ihrer Streubreite einer besonders engen Verschränkung beider Kontrollformen bedürfe.<sup>402</sup>

Diese Begründung überzeugt nur teilweise. Die Streubreite rechtfertigt zwar eine besonders enge Verzahnung,<sup>403</sup> aber nicht den Umkehrschluss, dass konkrete Prüfaufträge bei gezielten, ihrerseits hoch eingriffsintensiven Maßnahmen entbehrlich wären. Auch dort zeigt sich häufig erst im Vollzug, ob die Maßnahme im gebilligten Rahmen geblieben ist, etwa bei Eingriffen in informationstechnische Systeme, längerfristigen Observationen oder dem länger dauernden Einsatz von Vertrauenspersonen. Weshalb ein Prüfauftrag für Eingriffe in Systeme von Ausländern im Ausland künftig entfallen soll, legt die Begründung nicht dar.<sup>404</sup> Die administrative Kontrolle soll zudem Fehler und Vollzugsprobleme erkennen, die bei der Vorabkontrolle übersehen wurden. Sie darf sich deshalb nicht darauf beschränken, Vorentscheidungen des gerichtsähnlichen Organs zu bestätigen. Daran ändert das Recht auf unangekündigte Kontrollen (§ 26 Abs. 1 S. 5) nichts, weil es den Zeitpunkt betrifft, nicht Gegenstand oder Anlass. Verfassungsrechtlich zwingend ist eine weitergehende Befugnis nicht, weil die Maßnahmen der Strukturkontrolle zugänglich bleiben und stichprobenartig geprüft werden können.<sup>405</sup> Angesichts der erheblichen Erweiterung der Befugnisse spricht aber viel dafür, konkrete Prüfaufträge nicht auf die strategische Aufklärung zu beschränken. Wir empfehlen deshalb, dass ein Spruchkörper die administrative Kontrolle jedenfalls bei besonders eingriffsintensiven Maßnahmen gezielt auf die Umsetzung einer gebilligten Maßnahme richten kann, und zusätzlich ein eigenes Initiativrecht des administrativen Organs bei Anhaltspunkten für Verstöße. Das Prüfprogramm kann der Senat zwar jederzeit ändern, bislang aber nur nach Anhörung des Dienstes (§ 26 Abs. 1 S. 3 und 4). Für dringende Kontrollen sollte er es auch ohne vorherige Stellungnahme ergänzen können. Fachliche Feststellungen und Beanstandungen dürfen durch Weisungen nicht inhaltlich unterdrückt werden. Die Behördenleitung darf die Arbeit koordinieren, die Kontrollbewertung selbst muss unabhängig bleiben. Eine eigene Behörde verlangt die Verfassung dafür nicht. Schließlich sollte der Austausch technischer Erkenntnisse zwischen beiden Organen gesichert werden, ohne die Unabhängigkeit der Spruchkörper zu unterlaufen, und Ersuchen nach § 38 müssen zu wirksamen konkreten Prüfungen führen können (D.XIII).

## **XI. Befugnisse (§ 13 UKRatG-E)**

§ 13 UKRatG-E fächert die Befugnisse des UKRats gegenüber den Diensten auf. Er kann verlangen, dass ihm Akten, Schriftstücke und in Dateien gespeicherte Daten zur Verfügung gestellt werden (Abs. 1), ihm ist jederzeit Zutritt zu den Dienststellen und Zugang zu den informationstechnischen

<sup>401</sup>Begr. zu § 26 und § 32 UKRatG-E, BT-Drs. 21/7868, S. 577, 582 f.

<sup>402</sup>Begr. zu § 32 UKRatG-E, BT-Drs. 21/7868, S. 577, 582 f., unter Verweis auf BVerfGE 154, 152, Rn. 279.

<sup>403</sup>BVerfGE 154, 152, Rn. 272, 279.

<sup>404</sup>Vgl. § 51 Abs. 2 S. 2 BNDG.

<sup>405</sup>Begr. zu § 32 UKRatG-E, BT-Drs. 21/7868, S. 582 f.

Systemen zu gewähren (Abs. 2), und die Dienste müssen seine Fragen beantworten, soweit dies für die Kontrolle erforderlich ist (Abs. 3). Das explizite Recht, Bedienstete persönlich zu befragen (§ 56 Abs. 4 S. 1 BNDG), und die ausdrückliche Pflicht zur unverzüglichen Entsprechung werden nicht übernommen. Die Begründung hält Letztere für selbstverständlich und die Befragung durch die Auskunftspflicht der Behörde für ersetzt.<sup>406</sup> Der Zugang zu Unterlagen in einer Dienststelle gewährleistet allerdings noch nicht, dass die Kontrolleure dort praktisch ebenso gut arbeiten können wie mit eigenen Unterlagen. Wir empfehlen deshalb, die erforderlichen Arbeitsunterlagen unter Wahrung des Geheimschutzes sicher verfügbar zu machen oder kontrolliert zu übermitteln, sofern der UKRat dies für erforderlich hält.

Tatsächlich inhaltlich eingeschränkt werden die Befugnisse durch § 13 Abs. 4. Ausgenommen sind Informationen über operativ eingesetzte Personen, die deren Identität oder anderweitig eine Enttarnung ermöglichen. Nach der Begründung sind damit auch Angaben geschützt, die erst in Kombination mit weiteren Informationen eine Enttarnung ermöglichen. Für die Prüfung seien vor allem die Umstände des Einsatzes und die Art des Einsatzmittels von Bedeutung, nicht seine Individualisierung.<sup>407</sup> Eine vergleichbare Beschränkung ist schon im Gesetzgebungsverfahren zum Hessischen Verfassungsschutzgesetz durch uns sehr kritisch bewertet worden.<sup>408</sup> Vorabkontrolle droht leerzulaufen, wenn der Kontrollinstanz die personen- und einsatzbezogenen Umstände vorenthalten werden, auf die es für den konkreten Einsatz auch nach den gesetzlichen Vorgaben maßgeblich ankommt. Für die Verhältnismäßigkeit des Einsatzes einer Vertrauensperson können ihre Vita, einschlägige Straftaten und ihre Stellung in der beobachteten Vereinigung erheblich sein. Die Balance zwischen Quellenschutz und wirksamer Kontrolle ist deshalb nicht dadurch herzustellen, dass die Kontrollinstanz von relevanten Informationen abgeschnitten wird. Der Geheimschutz ist vielmehr bei der Kontrollinstanz sicherzustellen. § 13 Abs. 4 sollte daher um eine Regelung ergänzt werden, nach der der Dienst auf Verlangen eine Überprüfung der personenbezogenen Einsatzvoraussetzungen ermöglicht. Soweit dafür ausnahmsweise identifizierende Informationen unerlässlich sind, sollte ein Mitglied des UKRats die Identität unter besonderen Geheimschutzvorkehrungen erfahren können (zu den diesbezüglich genaueren Empfehlungen vgl. unter C.IV.3).

## **XII. Rechtsfolgen festgestellter Verstöße (§§ 33, 34 UKRatG-E)**

Die Rechtsfolgen festgestellter Verstöße sind zweistufig geregelt. Stellt das administrative Kontrollorgan einen Verstoß fest, dem der Dienst nicht abhilft, kann der UKRat ihn gegenüber der Aufsichtsbehörde beanstanden und diese zur Stellungnahme auffordern (§ 33 Abs. 1 und 2). Bei einem qualifizierten Verstoß, also einem Verstoß gegen das Erfordernis einer Vorab- oder Einzelfallkontrolle, gegen Maßgaben des gerichtsähnlichen Organs oder gegen besondere Regeln zur Weiterverarbeitung von Daten aus vorabkontrollierten Maßnahmen, soll das administrative Organ den Sachverhalt dem Senat vorlegen (§ 34 Abs. 1). Stellt der Senat den Verstoß fest, kann er eine Anweisung zur Abhilfe treffen, die der Dienst in der gesetzten Frist oder unverzüglich umzusetzen hat (§ 34 Abs. 2 S. 2 bis 4). Befolgt der Dienst sie nicht, wird das PKGr unterrichtet (§ 34 Abs. 2 S. 5). Eine weitergehende Durchsetzung sieht der Entwurf nicht vor. Gegenüber der Datenschutzaufsicht des BfDI ist die verbindliche Anweisung gleichwohl ein Fortschritt. Das Bundesverwaltungsgericht hat ihm ein einklagbares Recht auf Einsicht in Anordnungen individueller Aufklärungsmaßnahmen des BND

<sup>406</sup>Begr. zu § 13 UKRatG-E, BT-Drs. 21/7868, S. 570.

<sup>407</sup>Begr. zu § 13 Abs. 4 UKRatG-E, BT-Drs. 21/7868, S. 570.

<sup>408</sup>Ogorek/Manns, Stellungnahme zum Entwurf eines Gesetzes zur Änderung verfassungsschutzrechtlicher Vorschriften (LT-Drs. 21/2376), Hessischer Landtag, Ausschussvorlage INA 21/18, Teil 1, S. 58 f.

abgesprochen, sodass er bei verweigerter Einsicht auf die Beanstandung beim BKAmt verwiesen bleibt.<sup>409</sup> Eine Aufsicht, die nicht mehr als die Beanstandung kennt, wird in der Literatur für verfassungsrechtlich unzureichend gehalten.<sup>410</sup> Gegenüber dem geltenden Recht fällt der Entwurf dagegen zurück. Nach § 52 BNDG kann das administrative Organ jede Beanstandung, an der es nach der Stellungnahme des BKAmt festhält, dem gerichtsähnlichen Organ vorlegen, das bei Bestätigung die Abhilfe anordnen muss (§ 52 Abs. 3 und 4 BNDG). Der Entwurf beschränkt diesen Weg auf die qualifizierten Verstöße, und selbst dort steht die Anweisung im Ermessen des Senats. Bei allen übrigen Verstößen bleibt es bei Beanstandung und Stellungnahme. Verstöße gegen Löschfristen, Kennzeichnungs- oder Übermittlungsregeln erfasst § 34 Abs. 1 Nr. 3 nur, soweit sie Daten aus vorabkontrollierten Maßnahmen betreffen. Für sonstige Datenschutzverstöße kann der UKRat seine Aufsicht deshalb nicht durchsetzen.

Wir empfehlen deshalb drei Änderungen. Erstens sollte § 33 Abs. 1 als Soll-Vorschrift gefasst werden. Zweitens sollte der Senat bei einem fortbestehenden qualifizierten Verstoß die erforderliche Abhilfe anordnen müssen, wie es § 52 Abs. 4 BNDG schon heute vorsieht. Das Auswahlermessen über die gebotene Maßnahme bliebe unberührt, weil sie vom Rechtsverstoß und vom Schutzzweck der verletzten Vorschrift abhängt. Drittens sollte der Senat die Anweisungsbefugnis für alle Verstöße gegen Vorschriften über die Verarbeitung personenbezogener Daten erhalten, wenn der Dienst einer Beanstandung nicht binnen angemessener Frist abhilft. Die Unterrichtung des PKGr bliebe als letzte Stufe erhalten. Ein Durchsetzungsdefizit verbleibt gleichwohl, weil eine nicht befolgte Anweisung keine weitere Folge hat.

### **XIII. Individuelles Ersuchen (§ 38 UKRatG-E)**

Das individuelle Ersuchen eröffnet einen vom Einzelnen ausgehenden Zugang zur objektivrechtlichen Kontrolle, den das geltende Recht nicht kennt und der die Anrufung des BfDI durch (vermeintlich oder tatsächlich) Betroffene ersetzt. Es ist mehr als nur eine unverbindliche Anregung. Wer anhand eines konkreten Sachverhalts ein substantiiertes Interesse an der Prüfung einer möglichen Verletzung eigener Rechte darlegt, löst nach § 38 S. 3 eine Prüfpflicht aus.<sup>411</sup> Die Regelung knüpft an die Überlegung des Bundesverfassungsgerichts an, Personen mit plausibler Betroffenheit eine eigene Initiative zur objektivrechtlichen Kontrolle zu eröffnen, die das Gericht von der Rechtsschutzgarantie unterschieden hat.<sup>412</sup> Das Ersuchen ergänzt die institutionelle Kontrolle, ersetzt sie aber nicht, weil die Wahrung der rechtlichen Grenzen gerade bei heimlichen Maßnahmen nicht davon abhängen kann, dass eine betroffene Person den Kontrollanlass erkennt.

Für die Darlegungsanforderungen ist diese kompensatorische Funktion maßgeblich. Erforderlich ist ein anhand konkreter Umstände nachvollziehbarer Bezug zur möglichen Verletzung eigener Rechte. Die allgemeine Befürchtung, betroffen sein zu können, genügt demnach nicht. Umgekehrt darf der Zugang nicht davon abhängen, dass die ersuchende Person die Durchführung oder gar die Rechtswidrigkeit einer geheimen Maßnahme nachweist. Andernfalls setzte die Kontrolle gerade die Kenntnisse voraus, deren Fehlen sie ausgleichen soll. Die Begründung verlangt neben dem Sachverhalt ein „besonderes Interesse“ und hält das Ersuchen ohne diese Darlegung für unstatthaft.<sup>413</sup> Das ist im Lichte des gesetzlichen Merkmals zu verstehen: Zu konkretisieren ist das Interesse an der

<sup>409</sup>BVerwG, Urt. v. 4.3.2026, 6 A 2.24, ECLI:DE:BVerwG:2026:040326U6A2.24.0, Leitsatz.

<sup>410</sup>Höning, Externe Rechtskontrolle (Fn. oben), S. 299 (zu den Datenschutzbeauftragten).

<sup>411</sup>§ 38 S. 1 bis 3 UKRatG-E; Begr. zu § 38, BT-Drs. 21/7868, S. 587.

<sup>412</sup>BVerfGE 154, 152, Rn. 280.

<sup>413</sup>Begr. zu § 38 UKRatG-E, BT-Drs. 21/7868, S. 587.

Prüfung einer möglichen eigenen Rechtsverletzung, nicht mehr. Weil Betroffene über die Maßnahmen naturgemäß wenig wissen, sollte der Gesetzgeber das ausdrücklich klarstellen. Wir empfehlen dabei, die Darlegung eines konkreten Sachverhalts genügen zu lassen und den UKRat im Gegenzug zu ermächtigen, offensichtlich unbegründete Ersuchen ohne Prüfung zurückzuweisen. Von der Prüfpflicht zu unterscheiden ist die Unterrichtung über das Ergebnis. Nach der Gesetzesbegründung teilt der UKRat unter Berücksichtigung des Geheimschutzes mit, ob eine Rechtsverletzung festgestellt wurde – das Gesetz selbst schweigt sich hierzu indes aus.<sup>414</sup> Eine gesetzliche Regelung der Mitteilung, dass geprüft wurde, und, soweit Geheimschutz und operative Belange es erlauben, ob Verstöße festgestellt wurden, würde den Wert des Ersuchens erheblich steigern.

Die Übergangsregel des § 42 Abs. 3 bestimmt für Ersuchen nur, wann die Prüfung spätestens beginnt, nämlich am ersten Tag des sechsten Kalendermonats nach der Verkündung bei Inlandsbezug und sonst am ersten Tag des achtzehnten. Ein Verbot, Ersuchen früher einzureichen, folgt daraus nicht. Wir empfehlen, die Prüfung so früh wie möglich aufzunehmen, eilbedürftige Fälle vorrangig zu behandeln und die Übergangsfristen nach Möglichkeit zu verkürzen.<sup>415</sup>

#### **XIV. Berichte und Parlament (§§ 35, 36 UKRatG-E)**

Der UKRat berichtet dem PKGr in Abständen von höchstens zwölf Monaten (§ 35 Abs. 1), bisher höchstens sechs (§ 55 Abs. 1 BNDG). Die Begründung erläutert die Verdoppelung nicht.<sup>416</sup> Sie ist vertretbar, weil § 35 Abs. 1 nur eine Höchstfrist vorgibt und der UKRat bei Anlass früher berichten kann. Auch ist einzustellen, dass die Berichterstattung erhebliche Ressourcen angesichts des deutlich erweiterten Aufgabenportfolios des UKRats kostet. Bemerkenswert ist dagegen § 35 Abs. 3, der der Aufsichtsbehörde des kontrollierten Dienstes erlaubt, die Übermittlung des Berichts oder einzelner Teile an das PKGr zu untersagen. Die Begründung versteht das als Fortführung des § 55 Abs. 2 BNDG und nennt zwingende Gründe des Staatswohls, insbesondere des Nachrichtenzugangs und des Schutzes Dritter, sowie den Kernbereich exekutiver Eigenverantwortung.<sup>417</sup> Dahinter können die Third Party Rule und der Quellenschutz stehen, und das Bundesverfassungsgericht hat anerkannt, dass der Informationsfluss zum PKGr aus Geheimhaltungsgründen begrenzt werden kann.<sup>418</sup> Die Regelung ist gleichwohl eng auszulegen: Das Staatswohl ist Bundestag und Bundesregierung gemeinsam anvertraut, und der Bundestag hat mit dem PKGr extra einen besonders geschützten Raum geschaffen.<sup>419</sup> Eine abstrahierte oder teilweise Unterrichtung sollte deshalb Vorrang haben. Die Untersagung ist nach § 35 Abs. 3 S. 2 gegenüber dem UKRat zu begründen. Das Begründungserfordernis sollte auf das PKGr erstreckt werden, weil auch das Gremium ein eigenes Interesse daran hat, die Gründe für die Beschränkung seiner Information zu kennen, wobei hier eine abstraktere Darstellung gewählt werden könnte.

Den öffentlichen Bericht erstellt der UKRat erstmals für die Jahre 2027 bis 2029 (welcher somit erst im Anschluss vorzulegen ist) und danach für jeweils zwei Jahre. Seine Verschriftlichung erfolgt unter Beachtung des Geheimschutzes, in abstrakter Weise und nach Anhörung der Aufsichtsbehörden (§ 36 Abs. 1 S. 1). Er darf rechtliche Bewertungen enthalten (§ 36 Abs. 1 S. 3). Die Bedeutung eines öffentlichen und wissenschaftlichen Austauschs ist aus der Praxis des UKRats früh hervorgehoben

<sup>414</sup>Begr. zu § 38 UKRatG-E, BT-Drs. 21/7868, S. 587.

<sup>415</sup>BT-Drs. 21/7868, S. 165 f., 174 f., 179. Ebenso kritisch zu einer „rechtsschutzlosen Zeit“ Sosna, ZD 2026, 657 (658).

<sup>416</sup>Vgl. Begr. zu § 35 UKRatG-E, BT-Drs. 21/7868, S. 585.

<sup>417</sup>Begr. zu § 35 Abs. 3 UKRatG-E, BT-Drs. 21/7868, S. 585 f.

<sup>418</sup>BVerfGE 154, 152, Rn. 292 ff., 298.

<sup>419</sup>Vgl. BVerfG, Urt. v. 14.12.2022, 2 BvE 8/21, Rn. 69, 99 ff.

worden.<sup>420</sup> Für eine Behörde, deren Aufgaben sich vervielfachen, wäre ein erster Bericht auch vor diesem Hintergrund sowie angesichts der politischen Erwartungen schon über das Jahr 2027 oder spätestens das angemessene Signal an Parlament und Öffentlichkeit. Dieser Bericht dürfte besonders knapp ausfallen, Grundsatzfragen und verallgemeinerte Entscheidungslinien sollten darin bis 2029 noch nicht verpflichtend verlangt werden, damit sich der UKRat einarbeiten kann. Nach der Anlaufphase sollte der Bericht sie dagegen regelmäßig darstellen (vgl. unter D.XV).

Auch das PKGr erhält neue Informationsrechte. Der BND unterrichtet es regelmäßig über Maßnahmen gegen Systeme Deutscher nach § 37 Abs. 3, unverzüglich über Grundanordnungen nach § 50 und über seine Dienstvorschriften (§ 96 BNDG-E). Über die Schutzmaßnahmen des BfV berichten das BMI jährlich und der UKRat in seinem Tätigkeitsbericht (§ 62 BVerfSchG-E). Hinzu treten die Wahl der Mitglieder des UKRats (§ 17 UKRatG-E) und die Zustimmung zum Besonderen Feststellungsfall (§ 125 Abs. 3 BNDG-E). Zwei Punkte passen jedoch nicht zueinander: Über die Grundanordnung für erweiterte Maßnahmen des BND wird das Gremium unverzüglich unterrichtet, von der Einstufung einer besonderen Bedrohung als Voraussetzung der Schutzmaßnahmen des BfV (§ 60 BVerfSchG-E) erfährt es hingegen nur im jährlichen Überblick. Zudem lässt „regelmäßig“ (§ 96 Nr. 1 BNDG-E) offen, in welchen Abständen berichtet wird. Rechtspolitisch sollten auch Einstufungen nach § 60 BVerfSchG-E unverzüglich mitgeteilt und für § 96 Nr. 1 BNDG-E ein Turnus festgelegt werden, etwa halbjährlich. In die umgekehrte Richtung weist § 8 Abs. 3 Nr. 2 UKRatG-E, nach dem der UKRat seine Geschäftsordnung nur im Einvernehmen mit dem PKGr beschließen kann. Das Gremium spiegelt politische Mehrheiten, und das Bundesverfassungsgericht verlangt, die Kontrollinstanzen in ihrer Arbeit von Einflussnahmen wirksam abzuschirmen.<sup>421</sup> Eine Mitentscheidung über die Kontrollverfassung passt dazu nicht. Es sollte genügen, dem Gremium die Geschäftsordnung zur Kenntnis zu geben.

## **XV. Veröffentlichung von Entscheidungen**

Der UKRat hatte 2025 insgesamt 58 Beschlüsse und Bescheide in einer als geheim eingestuften Entscheidungssammlung zusammengestellt.<sup>422</sup> Angesichts der nach dem Regierungsentwurf erheblich vergrößerten Reichweite seiner Tätigkeit und des Bedürfnisses nach einer nachvollziehbaren Rechtsentwicklung ist im Schrifttum die Veröffentlichung von Leitsätzen oder Entscheidungen vorgeschlagen worden.<sup>423</sup> Zumindest die Veröffentlichung von Entscheidungen steht in einem deutlichen Spannungsverhältnis zu ihrer Einstufung. Auch stark geschwärzte Fassungen erlauben noch Rückschlüsse auf Kontext oder Entscheidungszeitpunkt. Aus diesem Grund hat der UKRat bislang von Veröffentlichungen abgesehen.<sup>424</sup> Ob allerdings auch die Veröffentlichung abstrahierter Leitsätze oder rechtlicher Kernaussagen ohne operative Sachverhaltsdetails kategorisch ausgeschlossen scheint, darf kritisch hinterfragt werden. Die Gesetzesbegründung erkennt sogar an, dass die in einem geheimen Vorlagefall aufgeworfene abstrakte Rechtsfrage für den öffentlichen Diskurs relevant sein kann, und stellt die Aufnahme von Leitsätzen in den öffentlichen Bericht in Aussicht.<sup>425</sup> Wir empfehlen, den Regierungsentwurf um die Verpflichtung zu ergänzen, Entscheidungen von

<sup>420</sup>Hoch/Schmidt-Räntsch/Brunst, NVwZ 2023, 712 (716).

<sup>421</sup>BVerfGE 154, 152, Rn. 281.

<sup>422</sup>Schmidt-Räntsch/Tombrink, NVwZ 2025, 1041 (1041).

<sup>423</sup>Löffelmann/Zöller, Nachrichtendienstrecht (Fn. oben), F. Rn. 67.

<sup>424</sup>Hoch/Schmidt-Räntsch/Brunst, NVwZ 2023, 712 (716).

<sup>425</sup>Begr. zu § 23 Abs. 6 und § 36 UKRatG-E, BT-Drs. 21/7868, S. 575, 586.

grundsätzlicher Bedeutung in Form von Leitsätzen zu veröffentlichen, soweit Geheimhaltungsbelange nicht entgegenstehen. Ob sich abstrakte Leitsätze herstellen lassen, wäre jeweils eigens zu prüfen.

## **XVI. Öffnungsklauseln und Parlamentsvorbehalt**

Schon das geltende Recht beschränkt die Dienste nicht auf einen abschließenden Katalog nachrichtendienstlicher Mittel. Der Entwurf hält daran fest und führt die Mittel in § 16 Abs. 1 BVerfSchG-E und § 18 Abs. 1 BNDG-E nur beispielhaft auf. Unbenannte Mittel unterliegen nach ihrem Eingriffsgewicht den Anforderungen für vergleichbar eingriffsintensive Mittel (§ 16 Abs. 4 S. 2, § 29 BVerfSchG-E, § 19 Abs. 1 und 2 BNDG-E). Beim BfV sind die Mittel in einer Dienstvorschrift abschließend zu benennen, deren Zustimmung durch das BMI und hinsichtlich der Vorgaben des § 16 Abs. 4 S. 2 zusätzlich durch den UKRat vorgesehen ist (§ 16 Abs. 4 S. 1 und 4). Beim BND bedarf die Dienstvorschrift der Zustimmung des BKAm ( § 95 Abs. 4 BNDG-E) und ist, soweit sie den Katalog betrifft, dem UKRat zur Einzelfallkontrolle vorzulegen (§ 97 Abs. 3 S. 1 Nr. 6 lit. a). Die Erprobung noch nicht enthaltener Mittel begrenzt § 19 Abs. 1 BNDG-E auf vier Jahre und unterwirft sie der Vorabkontrolle (§ 97 Abs. 1 Nr. 4).

Im Schrifttum ist moniert worden, das Freischalten neuer Maßnahmen durch den UKRat oder das BKAm sei eine Umgehung des Parlaments und laufe auf eine Selbstermächtigung der Exekutive hinaus.<sup>426</sup> Dem ist entgegenzuhalten, dass der Entwurf den Katalog von vornherein nicht abschließend ausgestaltet.<sup>427</sup> Beschließt der Bundestag den Entwurf, liegt darin eine bewusste Entscheidung für eine entwicklungsoffene Auffangermächtigung (vgl. bereits die Argumentation unter C.IV.1). Sie unterliegt den Grenzen des Bestimmtheitsgebots und des Vorbehalts des Gesetzes. Umso wichtiger ist daher die Einbindung des UKRats in beiden Gesetzen, beim BfV durch seine Zustimmung zur Dienstvorschrift, beim BND durch deren Vorlage zur Einzelfallkontrolle (§ 97 Abs. 3 S. 1 Nr. 6 lit. a BNDG-E). Sie ist keine Mitgestaltung des Befugnis-katalogs im Sinne eigenständiger Befugnis-schöpfung, sondern eine anlässlich der Dienstvorschrift in generell-abstrakter Weise vorzunehmende Kontrolle, ob die Auffangermächtigung für das neue Mittel belastbare Basis ist.<sup>428</sup>

## **XVII. Ausstattung und Kontrolldichte**

Der UKRat übernimmt die Vorabkontrolle des gesamten BfV, die Kontrolle der Telekommunikationsüberwachung beider Dienste, die Datenschutzkontrolle, die bisher der BfDI ausübte, und die Kontrolle der Schutzmaßnahmen und erweiterten Maßnahmen. Für diese Aufgaben sieht der Entwurf 37 neue Stellen vor, zehn in der Verwaltung und 27 in der Kontrolle, bei jährlichen Mehrausgaben von 8,86 Millionen Euro.<sup>429</sup> Zum Vergleich nennt der Entwurf für das BfV 269 Millionen Euro jährlich zuzüglich noch nicht bezifferter Personalmittel. Eine nach Kontrollaufgaben aufgeschlüsselte Berechnung des Personal- und Sachbedarfs legt der Entwurf nicht vor.<sup>430</sup> Der Nationale Normenkontrollrat hat die Darstellung der Kostenfolgen als weder methodengerecht noch nachvollziehbar bezeichnet, wegen der besonderen Prognose- und Geheimhaltungsschwierigkeiten aber keine

<sup>426</sup>Löffelmann, VerfBlog v. 20.8.2026 (Fn. oben).

<sup>427</sup>Vgl. Höning, Externe Rechtskontrolle (Fn. oben), S. 44 f.

<sup>428</sup>Begr. zu § 16 Abs. 4 BVerfSchG-E, BT-Drs. 21/7868, S. 241 f. Zur Funktion des gerichtsähnlichen Vorabkontrolleure bei der Konkretisierung weiter Normen Höning, Externe Rechtskontrolle (Fn. oben), S. 152 f., die von einer „quasi-gesetzgeberischen Funktion“ spricht.

<sup>429</sup>Vorblatt, Abschnitt D, BT-Drs. 21/7868, S. 2 f.

<sup>430</sup>Zu den Startschwierigkeiten beim Personalaufbau des UKRats vgl. Höning, VerfBlog v. 14.8.2026 (Fn. oben); zum Aufwand des bisherigen Kontrollverfahrens Löffelmann, VerfBlog v. 20.8.2026 (Fn. oben).

Einwände erhoben.<sup>431</sup> Aus der Zahl der Stellen allein lässt sich die künftige Kontrolldichte nicht ableiten. Ausschlaggebend sind die tatsächliche Besetzung, die Dauer der Sicherheitsüberprüfungen, geeignete Räume und gegebenenfalls personelle Nachsteuerungen anhand der realen Fallzahlen nach Inkrafttreten.

Die Personalgewinnung kann der Gesetzgeber der Verwaltung überlassen, weshalb nur in aller Kürze auf eine mögliche Erleichterung hingewiesen sei: Das BfV kann die erweiterten Sicherheitsüberprüfungen für das Personal des UKRats vorrangig bearbeiten, weil das Sicherheitsüberprüfungsgesetz keine Bearbeitung in der Reihenfolge des Eingangs vorschreibt, und weitere Abordnungen aus den Diensten sowie vom Generalbundesanwalt können die Anlaufzeit verkürzen, weil deren Bedienstete bereits überprüft sind. Zudem ist auffällig, dass der Regierungsentwurf mit Einsparungen durch den Wegfall der Zuständigkeiten des BfDi und der G 10-Kommission rechnet, ohne zu regeln, ob deren Bedienstete mit ihrer Erfahrung zum UKRat wechseln können (und sollen).<sup>432</sup>

Die Selbstevaluation nach § 41 UKRatG-E setzt das Modell des § 61 BNDG fort. Für eine Behörde, deren Aufgaben sich vervielfachen, könnte der Gesetzgeber mittelfristig eine externe Evaluation im Auftrag des Bundestages vorsehen, unter Wahrung des Geheimschutzes etwa nach dem Vorbild der Ermittlungsbeauftragten parlamentarischer Untersuchungsausschüsse. Dies stellt eine rein rechtspolitische und ergebnisoffene Anregung dar. Die Stellungnahme schlägt außerdem an mehreren Stellen zusätzliche Vorlagen und Kontrollen vor, die den UKRat zusammengenommen überfordern würden, wenn jede als Einzelkontrolle ausgestaltet würde.

## **E. Spannungs-, Verteidigungs- und Besonderer Feststellungsfall**

### **I. Auslösetatbestände (§ 75 Abs. 1 BVerfSchG-E, § 125 BNDG-E)**

Beide Fachgesetze enthalten Sonderregeln für den Fall, dass die Bundesrepublik in einen bewaffneten Konflikt gerät. Sie bilden den weitestgehenden Eingriff in die Kontrollarchitektur, den der Regierungsentwurf kennt. Für das BfV gelten die Sonderregeln im Spannungsfall (Art. 80a GG) und im Verteidigungsfall (Art. 115a GG) unmittelbar (§ 75 Abs. 1 BVerfSchG-E). Für den BND greifen sie dagegen nur im Verteidigungsfall unmittelbar, im Spannungsfall hingegen erst nach einer Feststellung der Bundesregierung, die sie auf einzelne Regelungen beschränken kann (§ 125 Abs. 1 und 2 BNDG-E). Hinzu tritt der Besondere Feststellungsfall: Steht der Spannungs- oder Verteidigungsfall unmittelbar bevor, kann die Bundesregierung mit Zustimmung des PKGr die Anwendung der Sonderregeln beschließen (§ 125 Abs. 3). Aufzuheben ist die Feststellung, wenn ihre Voraussetzungen entfallen, wenn zwei Drittel des PKGr es verlangen oder, im Spannungsfall, wenn der Bundestag es verlangt (§ 125 Abs. 4).

Im Grundsatz ist das nachvollziehbar (zu den Details gleich). Nicht erklärt ist allerdings die Asymmetrie zwischen den Diensten. Warum das BfV im Spannungsfall ohne Feststellung der Bundesregierung in den Sondermodus wechselt, der BND aber nicht, erschließt sich kaum. Wir empfehlen deshalb nachdrücklich, den Sondermodus des BfV im Spannungsfall ebenfalls erst nach einer Feststellung der Bundesregierung zu aktivieren, dass seine Anwendung aus Gründen der Verteidigung zwingend notwendig ist, wie es § 125 Abs. 2 BNDG-E für den BND vorsieht. Das vermeidet automatische Rechtsfolgen, verbessert die administrative Handhabbarkeit und schafft eine einheitliche

<sup>431</sup>Stellungnahme des NKR, BT-Drs. 21/7868, S. 605.

<sup>432</sup>Begr. A.VII, BT-Drs. 21/7868, S. 206.

Ausnahmerechtsarchitektur mit angeglichenen Auslösetatbeständen. Nicht erfasst ist dagegen der Bündnisfall (Art. 80a Abs. 3 GG), obwohl die Begründung die erhöhte Handlungsbereitschaft des BND ausdrücklich auch mit den Bündnisverpflichtungen der Bundesrepublik begründet.<sup>433</sup> Wir empfehlen, § 125 BNDG-E um ihn zu ergänzen.

## II. BND (§§ 126–133 BNDG-E)

Der Abschnitt zur Landes- und Bündnisverteidigung geht weiter als § 75 BVerfSchG-E (vgl. unter E.III) und verändert das Recht des BND in mehrfacher Hinsicht, wenngleich er auch heute operativ und taktisch bereits auf den Verteidigungsfall durch eigene Aktenpläne usw. vorbereitet ist. Nach der Neuregelung werden zunächst alle inländischen öffentlichen und privaten Stellen zur Unterstützung verpflichtet, einschließlich der Schaffung digitaler Zugänge zu Systemen und Personen. Öffentliche Stellen können die Unterstützung ablehnen, wenn sie ihre eigene Aufgabenwahrnehmung ernsthaft gefährden und dem Bund dadurch ein erheblicher Nachteil drohen würde. Bei nichtöffentlichen Stellen steht ein solches Ablehnungsrecht dagegen nur Betreibern Kritischer Infrastrukturen zu (§ 126). Soweit dabei Anbieter elektronischer Kommunikationsdienste verpflichtet werden, bleibt die Datenschutzrichtlinie für elektronische Kommunikation anwendbar (vgl. unter B.I.4). Die Hilfe sonstiger nichtöffentlicher Stellen nach § 126 Abs. 2 fällt dagegen nicht schon deshalb unter die Richtlinie. Sodann richten sich die Datenerhebung unter Mitwirkung anderer Stellen und der Einsatz nachrichtendienstlicher Mittel allein nach der Erforderlichkeit für die Aufklärung der Bedrohungslage, die zur Feststellung des Falls geführt hat (§§ 127, 128). Die Personenbeschränkungen des § 20, der Schutz von Vertraulichkeitsbeziehungen nach § 22 und die Regel, dass Daten der strategischen Aufklärung erst nach einer Einsichtnahme weiterverarbeitet werden dürfen (§ 31 Abs. 2), sind außer Anwendung gesetzt (§ 128 Abs. 3). Anordnungen können als Rahmenanordnungen ergehen (§ 128 Abs. 4). Nur im Verteidigungsfall bestimmt der Dienst ihre Höchstdauer mit Zustimmung des BKAm abweichend von den gesetzlichen Fristen (§ 128 Abs. 5 S. 2). Davon zu unterscheiden ist die besondere Befristungsregel des § 127 Abs. 4 für die Datenerhebung unter Mitwirkung anderer Stellen. Bestimmte Prüf-, Lösch- und Dokumentationspflichten werden nach Maßgabe des § 128 Abs. 6 und des § 130 Abs. 3 und 4 ausgesetzt oder eingeschränkt. Sämtliche Datenpflichten entfallen damit aber nicht, und insbesondere bleibt der Kernbereichsschutz des § 21 im Grundsatz bestehen.

Für die erweiterten Maßnahmen gelten alle Anwendungsfälle als spezifische Gefährdungslage (§ 129 Abs. 2). Im Verteidigungsfall sind sie auch ohne Grundanordnung zulässig, dann mit vorheriger Zustimmung des BKAm zu Art und Umfang (§ 129 Abs. 3). Zudem entfallen das Verbot des gezielten Einwirkens auf Leib und Leben und die Subsidiarität gegenüber der Tätigkeit anderer Stellen nach § 49 Abs. 1 S. 2 (§ 129 Abs. 4). Unberührt bleibt nur die Regel des § 51 Abs. 2, nach der Maßnahmen vorrangig im Ausland durchzuführen sind. Weiterverarbeitung und Übermittlung richten sich nach der Bedrohungslage, und gemeinsame Dateien können ohne Errichtungsanordnung geführt werden (§§ 130, 131). Schließlich entfällt die administrative Kontrolle. Im Verteidigungsfall entfällt nach § 132 Abs. 3 S. 3 zudem die Vorabkontrolle des UKRats, während die gerichtliche Kontrolle der Wohnraumüberwachung nach § 97 Abs. 6 und 7 bestehen bleibt. Der gerichtliche Rechtsschutz wird dagegen nicht ausgeschlossen, weil § 132 Abs. 5 den Unterabschnitt über Mitteilung, Auskunft und Rechtsweg einschließlich des Rechtswegausschlusses nach § 103 außer Anwendung setzt.

---

<sup>433</sup>Begr. zu § 125 BNDG-E, BT-Drs. 21/7868, S. 537 ff.; ebenso Frau/Näther, Nicht genug und doch zu viel, VerBlog v. 21.9.2026, <https://verfassungsblog.de/nachrichtendienstreform-wehrverfassung>.

Der Abschnitt, die vorstehenden deskriptiven Darstellungen über seinen Umfang zugrunde gelegt, ist als Notstandsrecht für den Verteidigungsfall geschrieben, den in der Regel der Bundestag mit Zustimmung des Bundesrates und mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen, mindestens der Mehrheit seiner Mitglieder, feststellt (Art. 115a Abs. 1 GG). Stehen dem unüberwindliche Hindernisse entgegen, trifft der Gemeinsame Ausschuss die Feststellung (Abs. 2), und bei einem bereits begonnenen Angriff gilt sie unter den Voraussetzungen des Absatzes 4 als getroffen. Das reguläre Verfahren verleiht der Entscheidung eine besondere parlamentarische Legitimation. Für diesen Fall lässt sich der Abschnitt rechtfertigen, weil der BND auch militärischer Nachrichtendienst ist und die Aufklärung eines Angreifers keine Fristen oder Bürokratie duldet, sondern im Krieg ohnehin weitgehende Aufhebung der für das bürgerliche Leben geltenden Bestimmungen eintritt. Drei Festlegungen bedürfen gleichwohl der Nachsteuerung: Erstens trifft der Wegfall des Schutzes von Vertraulichkeitsbeziehungen (§ 128 Abs. 3 Nr. 1) Geistliche, Rechtsanwälte, Journalisten und Abgeordnete. Für die übrigen Berufsgruppen halten wir das im Verteidigungsfall für hinnehmbar, nicht aber für Abgeordnete. Gerade im Verteidigungsfall gefährdet der gezielte Zugriff des Auslandsnachrichtendienstes auf die Kommunikation eines Bundestagsabgeordneten die vertrauliche Wahrnehmung des Mandats und die parlamentarische Kontrolle. Das Parlament, das den Verteidigungsfall feststellt und beendet, muss vor dem Dienst geschützt bleiben, den es kontrolliert. Wir empfehlen deshalb, den Schutz der Mandatsträger nach § 22 Abs. 1 S. 2 Nr. 4 zu erhalten. Maßnahmen gegen verstrickte Abgeordnete bleiben trotzdem nach § 22 Abs. 2 zulässig, insbesondere wenn Tatsachen die Annahme rechtfertigen, dass ein Parlamentarier geheimdienstlich für die gegnerische Macht tätig ist und damit eine zumindest erhebliche Bedrohung unterstützt (§ 22 Abs. 2 Nr. 1 lit. a).

Zweitens entfällt im Verteidigungsfall das Verbot gezielter Einwirkung auf Leib und Leben (§ 129 Abs. 4). Das ist die schwerste Absenkung des Abschnitts. Der Entwurf beschränkt sie zu Recht auf den Verteidigungsfall, im Spannungsfall und im Besonderen Feststellungsfall gilt sie nicht. Im Grundsatz befürworten wir trotz der damit einhergehenden Dramatik den Wegfall, weil ein militärischer Auslandsnachrichtendienst, der einen Angreifer aufklären und dessen Operationen stören soll, im Verteidigungsfall auf solche Mittel angewiesen sein kann. Der Vergleich mit den Streitkräften trägt dabei als funktionales Argument, nicht als Übertragung ihrer Befugnisse oder des Kombattantenstatus auf Bedienstete des BND. Ob das humanitäre Völkerrecht anwendbar ist, hängt zudem vom tatsächlichen Vorliegen eines bewaffneten Konflikts ab, nicht von der innerstaatlichen Feststellung des Verteidigungsfalls. Diese erfasst nach Art. 115a Abs. 1 GG sogar schon einen unmittelbar drohenden Angriff. Begrenzt werden sollte der Einsatz durch eine politisch verantwortete Rahmenentscheidung. Der Entwurf verlangt die vorherige Zustimmung des BKAm zu Art und Umfang aber nur für Maßnahmen ohne Grundanordnung (§ 129 Abs. 3). Wir empfehlen deshalb, dass das BKAm den Einsatzrahmen für Maßnahmen gegen Leib und Leben auch dann nach Art und Umfang billigt, wenn bereits eine Grundanordnung besteht und kein Eilfall vorliegt. Einer erneuten Befassung des Bundestages bedarf es dafür nicht, weil er mit der Feststellung des Verteidigungsfalls bereits eine außerordentlich weitreichende Entscheidung getroffen hat. Innerhalb dieses Rahmens bliebe die operative Durchführung beim Dienst, während wesentliche Erweiterungen einer erneuten Entscheidung bedürften. Das PKGr sollte über den Einsatz und seine Entwicklung unterrichtet werden, nicht aber über jeden einzelnen Vollzugsakt.

Drittens entfällt im Verteidigungsfall die Vorabkontrolle (§ 132 Abs. 3 S. 3 Nr. 1), auch für die strategische Aufklärung und die Telekommunikationsüberwachung mit Inlandsbezug. Verfassungsrechtlich ist das nicht ohne Weiteres hinnehmbar. Das Grundgesetz enthält keine allgemeine Ermächtigung, Grundrechte und ihre verfahrensrechtlichen Sicherungen im Verteidigungsfall außer Kraft zu

setzen, soweit dies nicht militärische Gegner betrifft. Art. 115c Abs. 2 Nr. 2 GG erlaubt für Freiheitsentziehungen nur eine Verlängerung der richterlichen Frist auf vier Tage, nicht den Verzicht auf die richterliche Entscheidung. Angesichts der enormen Auswirkungen des Verteidigungsfalls dürfte der Wegfall der regulären Vorabkontrolle aber vertretbar sein, wenn für unaufschiebbare Maßnahmen ein Eilverfahren an ihre Stelle tritt, das den sofortigen Vollzug erlaubt und eine unverzügliche nachträgliche Bestätigung durch das gerichtsähnliche Kontrollorgan verlangt, und wenn die Mitteilung der Maßnahmen und ihre Überprüfung nach Ende des Falls gesichert sind. Der Einwand, der Regierungsentwurf beseitige die Ersatzkontrolle bei fortbestehendem Rechtswegausschluss, trifft dabei nicht zu, weil § 132 Abs. 5 auch den Rechtswegausschluss des § 103 außer Anwendung setzt. Gesichert ist die Mitteilung nach Ende des Verteidigungsfalls aber nicht, weil § 132 Abs. 5 S. 1 Nr. 3 den Unterabschnitt über Mitteilung und Auskunft im Verteidigungsfall ebenfalls außer Anwendung setzt. Ohne Mitteilung aber wird der gerichtliche Rechtsschutz praktisch kaum wirksam. Nach unserer Auffassung sollte der Gesetzgeber deshalb für unaufschiebbare Maßnahmen ein Eilverfahren mit unverzüglicher nachträglicher Bestätigung ebenso vorsehen wie eine Prüfung der Mitteilung nach Ende des Falls und eine nachträgliche Überprüfung durch den UKRat (vgl. unter E.V). Aus rechtspolitischer Sicht bleiben Rahmenfeststellungen des UKRats, wie sie § 75 Abs. 8 S. 1 BVerfSchG-E vorsieht (vgl. unter E.III), gleichwohl der bessere Weg.

### **III. BfV (§ 75 BVerfSchG-E)**

§ 75 BVerfSchG-E verändert das Recht des BfV in verschiedener Hinsicht. So werden Unternehmen über die §§ 11–15 hinaus zu Auskunft und technischer Unterstützung verpflichtet, einschließlich der Überlassung betrieblicher Mittel (Abs. 2). Zudem entfallen die Ausschlussgründe für Vertrauenspersonen mit Ausnahme des Abgeordnetenausschlusses (Abs. 3 Nr. 1), so dass Minderjährige, wirtschaftlich Abhängige, Aussteiger und Verurteilte angeworben werden dürfen. Die Löschung von Angriffswerkzeugen (§ 24 Abs. 2) und im Verteidigungsfall auch Online-Durchsuchung und Wohnraumüberwachung sind ferner ohne Rücksicht darauf zulässig, ob die Polizei rechtzeitig handeln könnte (Abs. 3 Nr. 2). Nur im Verteidigungsfall entfallen außerdem die sonst geltenden Höchstfristen der Anordnungen (Abs. 3 Nr. 3). Hinzu tritt der Wegfall von Mitteilungen und Auskünften an Betroffene nach Maßgabe des Absatzes 4. Nur bei einem Spannungsfall von höchstens drei Monaten werden die Mitteilungen zu Maßnahmen nach § 22 Abs. 1 S. 1 sowie den §§ 25 und 27 lediglich zurückgestellt und später nachgeholt. Die übrigen Mitteilungen und die Auskunft entfallen auch dann. Darüber hinaus kann die Datenpflege nach § 38 bis auf die Pflicht zur Berichtigung unterbleiben. Dokumentation und Protokollierung können zudem entfallen, soweit sie zusätzlichen Verwaltungsaufwand verursachen (Abs. 5). Schließlich wird die externe Aufsicht eingeschränkt: Die Unterstützung der unabhängigen Kontrolle ist nur noch auf Entscheidung des PKGr geschuldet. Kernbereichsrelevante Informationen werden nicht mehr dem UKRat, sondern einheitlich dem Aufsichtsbediensteten (Abs. 7; bisheriger G 10-Jurist) vorgelegt. Der UKRat kann die Vorabkontrolle durch Rahmenfeststellungen ersetzen, die Bundesregierung kann sie mit Zustimmung des PKGr sogar ganz entfallen lassen (Abs. 8).

Vieles davon ist nachvollziehbar. Ein Dienst, der im Verteidigungsfall Sabotagetrupps aufklären soll, braucht Zugang zu Personen, die er in Friedenszeiten nicht führen dürfte. Auf polizeiliche Hilfe kann er zudem nicht verwiesen werden, wenn die Polizei anderweitig gebunden ist. Einige Regelungen bedürfen trotzdem weitergehender Sicherungen: Erstens geht der Wegfall des Ausschlusses Minderjähriger (§ 75 Abs. 3 Nr. 1) weiter als nötig. Er lässt auch die Altersgrenze und die Sicherungen des § 18 Abs. 1 S. 3 und 4 entfallen, so dass Minderjährige jeden Alters angeworben werden dürften.

Ein absoluter Ausschluss Minderjähriger ist dabei nicht die einzig vertretbare Lösung. Der vollständige Wegfall der regulären Alters- und Fürsorgegrenzen geht aber zu weit. Aus rechtspolitischer Sicht sollten auch im Spannungs- und Verteidigungsfall jedenfalls eine besondere Unerlässlichkeit im Einzelfall, eine (allerdings nicht zu dokumentierende) Fürsorge- und Gefährdungsabwägung, der Schutz vor einer beliebigen Anwerbung sehr junger Minderjähriger erhalten bleiben. Zweitens können nach Absatz 5 Dokumentation und Protokollierung unterbleiben, wenn sie zusätzlichen Verwaltungsaufwand auslösen. Das erschwert die spätere Nachprüfung erheblich, auch wenn andere Aufzeichnungen sie nicht stets unmöglich machen. Der Verzicht sollte deshalb durch eine Pflicht ersetzt werden, Dokumentation und Protokollierung nach Ende des Verteidigungsfalls binnen einer Frist nachzuholen, soweit dies dann noch möglich ist.

Drittens kann die Bundesregierung die Vorabkontrolle mit Zustimmung des PKGr ganz entfallen lassen (Abs. 8 S. 2), auch soweit sie die Telekommunikationsüberwachung erfasst. Die Feststellung zwingender Notwendigkeit und die parlamentarische Zustimmung sind Anwendungsschranken, ersetzen aber keine unabhängige Kontrolle der Eingriffe. Verfassungsrechtlich dürfte der vollständige Wegfall deshalb nur vertretbar sein, wenn ein beschleunigtes oder generalisiertes Verfahren an die Stelle der Vorabkontrolle tritt, das bei eilbedürftigen Einzelmaßnahmen eine unverzügliche nachträgliche Bestätigung durch den UKRat sichert, und wenn die Mitteilung der Maßnahmen und ihre Überprüfung nach Ende des Falls gesichert sind. An beidem fehlt es bislang. Der Rechtsweg ist nach § 22 Abs. 5 bis zur Mitteilung ausgeschlossen und bleibt es dauerhaft, wenn die Mitteilung nach § 75 Abs. 4 unterbleibt, wie es im Verteidigungsfall und in einem länger als drei Monate dauernden Spannungsfall vorgesehen ist. Anders als § 132 Abs. 5 BNDG-E setzt § 75 BVerfSchG-E den Rechtswegausschluss nicht außer Anwendung. Entfällt zugleich die Vorabkontrolle, fehlt jede Nachprüfung durch ein von der Volksvertretung bestelltes Organ, die Art. 10 Abs. 2 S. 2 GG als Bedingung des Rechtswegausschlusses verlangt. Hinzu kommt, dass Art. 19 Abs. 4 GG anders als Art. 10 Abs. 2 S. 2 GG keine Modifikation für den Verteidigungsfall kennt und deshalb als notstandsfest gilt. Nach unserer Auffassung sollte der Gesetzgeber deshalb ein solches beschleunigtes Verfahren vorsehen, die Mitteilung nach Ende des Verteidigungsfalls prüfen lassen und dem UKRat die nachträgliche Überprüfung der Maßnahmen ermöglichen.

Im Spannungs- und Verteidigungsfall entfällt zudem die pauschale Vorlage von Aufzeichnungen aus der Wohnraumüberwachung (§ 31 Abs. 4 S. 1 Nr. 2). Vorlagen gehen dann einheitlich an den Aufsichtsbediensteten statt an den UKRat (§ 75 Abs. 7 S. 2 BVerfSchG-E). Die Begründung versteht das als Entlastung von „lagebedingt nachrangigen Verwaltungsaufwänden“.<sup>434</sup> Für die Regelung spricht, dass der Aufsichtsbedienstete die Befähigung zum Richteramt hat und in dieser Funktion weisungsfrei ist (§ 31 Abs. 5 S. 2 i.V.m. § 6 Abs. 3 BDSG). Für Maßnahmen außerhalb der §§ 25–27 existiert diese Zuständigkeit ohnehin schon im Normalfall. Ein verfassungsrechtliches Restrisiko bleibt aber dennoch aufgrund des Charakters der Wohnraumüberwachung, für die das Bundesverfassungsgericht bislang undifferenziert nach einem Verteidigungsfall die vollständige Vorlage an eine unabhängige Stelle verlangt.<sup>435</sup> Eine behördeninterne Stelle ist nicht in diesem Sinne unabhängig. Angesichts des lagebedingt erheblichen Aufwands externer Sichtung halten wir dieses Risiko im Ausnahmefall aber für vertretbar, zumal der materielle Kernbereichsschutz nach § 31 Abs. 7 gemäß der gesetzlichen Vorgaben bestehen bleibt. Für die Online-Durchsuchung gilt nach unserer Bewertung Entsprechendes, weil wir schon im Normalfall eine unabhängige Kernbereichssichtung

<sup>434</sup> Begr. zu § 75 Abs. 7 BVerfSchG-E, BT-Drs. 21/7868, S. 317.

<sup>435</sup> Hierauf verweist auch die Begr. zu § 31 Abs. 4 BVerfSchG-E, BT-Drs. 21/7868, S. 271, unter Hinweis auf BVerfGE 162, 1, Rn. 282.

vor der operativen Kenntnisnahme für geboten halten (vgl. unter C.IV.6.b). Bei der Quellen-Telekommunikationsüberwachung ist dagegen nach Maßnahme und Datenart zu unterscheiden, wobei der Zugriff auf gespeicherte Kommunikation der Online-Durchsuchung nahekommt (vgl. unter B.IV). Zumindest sollte der UKRat nachträglich Stichproben aus gesichteten Daten ziehen.

#### IV. Besonderer Feststellungsfall

Die meiste Aufmerksamkeit verdient der Besondere Feststellungsfall (§ 125 Abs. 3 BNDG-E). Er erlaubt der Bundesregierung, mit Zustimmung des PKGr das Recht des Abschnitts 9 bereits in Kraft zu setzen, wenn der Spannungs- oder Verteidigungsfall „unmittelbar bevorsteht“. Dabei handelt es sich nicht um den Zustimmungsfall, in dem der Bundestag der Anwendung einzelner Verteidigungsvorschriften besonders zustimmt (Art. 80a Abs. 1 S. 1 Alt. 2 GG), außerhalb der Fälle des Art. 12a GG mit einfacher Mehrheit (Art. 80a Abs. 1 S. 2 GG). An diesen Zustimmungsfall lehnt sich der Besondere Feststellungsfall allerdings der Begründung an.<sup>436</sup> Er übernimmt sein Vorbild, tauscht aber das entscheidende Organ aus: An die Stelle des Bundestages treten die Bundesregierung und das PKGr.

Der Grund für die Vorstufe ist verständlich: Der Spannungsfall ist seit 1968 nie festgestellt worden, die dafür praktisch erforderliche Mehrheit von zwei Dritteln der abgegebenen Stimmen (Art. 80a Abs. 1 S. 2 GG) ist hoch. Ein Dienst, der erst nach dieser Feststellung in den Lagebetrieb wechseln darf, wechselt deshalb zu spät. Zudem ist die Heimlichkeit seiner Maßnahmen nach einer Beschlussfassung im Plenum naturgemäß nicht mehr gegeben. Der Preis damit einhergehende Preis ist allerdings hoch, denn die Runde aller Abgeordneten nach den tatsächlichen Mehrheitsverhältnissen wird durch die Bundesregierung und ein kleines, geheim tagendes parlamentarisches Gremium, ersetzt obwohl mit der Ausrufung des Besonderen Feststellungsfalls das gesetzliche Schutz- und Kontrollvorkehrungen erheblich abgesenkt wird.<sup>437</sup>

Vermittelnd könnte hier eine Lösung sein, die die nachrichtendienstlichen Bedarfe ernst nimmt und den Parlamentsvorbehalt wahrt, indem sie den Feststellungsfall in zwei Stufen teilt. Auf der ersten Stufe kann die Bundesregierung mit Zustimmung des PKGr bereits die Unterstützungs- und Mitwirkungspflichten (§§ 126, 127), die Befugnis zum Einsatz nachrichtendienstlicher Mittel für die Aufklärung der Bedrohungslage (§ 128 Abs. 2) und Rahmenanordnungen (§ 128 Abs. 4) in Kraft setzen; die Heimlichkeit bleibt hier – hoffentlich – gewahrt. Die erste Stufe darf dennoch nicht pauschal freigeschaltet werden, weil es sich um Eingriffsermächtigungen mit veritabler Wirkung handelt: § 126 Abs. 2 kann etwa Private zur Bereitstellung technischer Mittel und zur Schaffung digitaler Zugänge verpflichten, § 127 Abs. 2 und 5 erweitert Auskunfts- und Mitwirkungspflichten aller inländischen Stellen, und auch § 128 Abs. 2 erleichtert Maßnahmen gegenüber Betroffenen. Die Bundesregierung sollte daher in ihrer Feststellung benennen, welche dieser Befugnisse sie aktiviert. Wir halten diese frühe Phase mit einer Befristung und zusätzlichen Sicherungen für vertretbar. Zudem sollte der UKRat unverzüglich die Unterlagen für eine nachträgliche Einzelfallprüfung erhalten. Auf der zweiten Stufe bedürfen die weitergehenden Absenkungen der Schutzvorkehrungen sodann eines Beschlusses des Bundestagsplenums mit einfacher Mehrheit. Dies betrifft der Wegfall der Personenschwellen (§ 128 Abs. 3), die Aussetzung der Prüf-, Lösch- und Protokollierungspflichten (§ 128 Abs. 6, § 130), die Erleichterungen für erweiterte Maßnahmen (§ 129) und die Einschränkungen der Kontrolle (§

<sup>436</sup> Begr. zu § 125 Abs. 3 BNDG-E, BT-Drs. 21/7868, S. 538.

<sup>437</sup> Ebenso Frau/Näther, VerfBlog v. 21.9.2026 (Fn. oben), die zudem bezweifeln, dass Art. 80a Abs. 1 GG i.V.m. Art. 73 Abs. 1 Nr. 1 Var. 2 GG das Nachrichtendienstrecht erfasst, und eine Regelung für den Bündnisfall vermissen.

132). Den Vertraulichkeitsschutz für Mandatsträger und Presse, den § 128 Abs. 3 ebenfalls entfallen lässt, sollte der Gesetzgeber anders als der Entwurf auch auf dieser Stufe erhalten (vgl. unter E.II). Im Rahmen einer so erheblichen Rechtsveränderung wäre mit einer dauerhaften Geheimhaltung ohnehin nicht zu rechnen, sodass das Heimlichkeitsargument gegenüber gegnerischen Mächten an Wirkung verliert. Unberührt bleibt auf beiden Stufen das Verbot des gezielten Einwirkens auf Leib und Leben (§ 51 Abs. 3 S. 2), weil der Entwurf es nur im Verteidigungsfall entfallen lässt (§ 129 Abs. 4), und die regulären Befugnisse der §§ 49–51 bestünde nach ihren eigenen Voraussetzungen unabhängig von diesem Stufenmodell fort.

## **V. Kontrolle und Rechtsschutz im Ausnahmezustand**

Der Entwurf nimmt die unabhängige Kontrolle im Ausnahmefall weitgehend zurück. Die Kontrollunterstützung des BfV steht unter dem Vorbehalt einer Entscheidung des PKGr (§ 75 Abs. 7 BVerfSchG-E). Die administrative Kontrolle des BND entfällt vollständig (§ 132 Abs. 1 BNDG-E). Die Einzelfallkontrolle des UKRats wird nach Maßgabe des § 132 Abs. 3 durch Berichte ersetzt, deren Abstände er bestimmt, und im Verteidigungsfall entfallen die Vorabkontrollen ebenso wie die Kontrolle der Grundanordnungen und die Einzelfallkontrolle samt der an ihre Stelle tretenden Berichte (§ 132 Abs. 3 S. 3). Bestehen bleibt allein die gerichtliche Wohnraumkontrolle nach § 97 Abs. 6 und 7. Mitteilung und Auskunft entfallen nach § 132 Abs. 5. Zugleich wird aber auch der Rechtswegausschluss des § 103 außer Anwendung gesetzt. Gerichtlicher Rechtsschutz bleibt damit grundsätzlich eröffnet, wird durch das Fehlen von Mitteilungen aber praktisch erschwert. Das PKGr wird lediglich „in regelmäßigen Abständen“ unterrichtet (§ 132 Abs. 4). All dies sind sehr weitgehende Limitationen. Wir verkennen dabei nicht, dass – überspitzt gesagt – ein UKRat im Verteidigungsfall keine Einzelanordnungen im Dreitagesrhythmus prüfen kann. Verfassungsrechtlich dürfte der Wegfall der regulären Vorabkontrolle im Verteidigungsfall deshalb vertretbar sein, wenn ein Eilverfahren mit unverzüglicher nachträglicher Bestätigung an ihre Stelle tritt und Mitteilung und Überprüfung nach Ende des Falls gesichert sind (vgl. unter E.II und E.III). Nicht vollständig entfallen sollte aber zumindest die administrative Kontrolle (§ 132 Abs. 1 BNDG-E), mit der der UKRat in die Dienste hineinhört und -fühlt, die im Verteidigungsfall sogar Killing Operations durchführen dürften und wohl auch würden. Der UKRat sollte darüber hinaus in allen Fällen des Abschnitts 9 für Lagen typische Maßnahmen generell billigen, Berichte in kurzen Abständen erhalten und die Befugnis behalten, einzelne Maßnahmen an sich zu ziehen.

## **F. Änderung des MAD-Gesetzes und Folgeänderungen**

### **I. Art. 5 – MAD-Gesetz**

Das MAD-Gesetz ist erst durch das Gesetz vom 9. Januar 2026 mit Wirkung vom 16. Januar 2026 neu, wenngleich in seinem Umfang gegenüber der nun vorliegenden Novelle voreilig, neugeregelt worden und wird durch Art. 5 deshalb nur punktuell angepasst. Individualüberwachung von Brief-, Post- und Telekommunikationsverkehren wird aus dem G 10 in die §§ 18, 18a MADG-E überführt, der Mittelkatalog des § 8 ergänzt und der Militärische Abschirmdienst teilweise in die Kontrolle des UKRats eingebunden. So unterliegen Maßnahmen nach § 18 MADG-E nach § 22 Abs. 1a MADG-E dessen Vorabkontrolle, bei Telekommunikation beschränkt auf interpersonelle Kommunikation. Die Kontrolle der Verarbeitung der nach § 18 erhobenen Daten weist der Entwurf dem UKRat zu, der insoweit die Aufgabe der G 10-Kommission übernimmt (Art. 5 Nr. 5 lit. b und Nr. 7).<sup>438</sup> Davon zu

<sup>438</sup> BT-Drs. 21/7868, S. 182 f.; Begr. S. 591 ff.

unterscheiden sind die übrigen gerichtlichen Kontrollzuständigkeiten, und gerade daraus ergeben sich drei Kohärenzfragen. Erstens bleibt die Vorabkontrolle des Militärischen Abschirmdienstes im Übrigen beim Amtsgericht Köln (§§ 22, 45 MADG).<sup>439</sup> Dieser, bereits zur Einführung fragwürdigen und auf Druck des Bundesverteidigungsministeriums hin ergangenen Entscheidung sollte der Bundestag nun ein Ende setzen und die gesamte Vorabkontrolle des MAD auf den UKRat überführen. Wir empfehlen dies nachdrücklich! Einen tragfähigen Grund für die Zuständigkeit des Amtsgerichts Köln sehen wir allein bei der Wohnraumüberwachung, für die Art. 13 GG eine richterliche Anordnung verlangt. Der UKRat kontrolliert hauptamtlich, verfügt über eigenes Personal und ist in das Nachrichtendienstrecht eingearbeitet. Hinzu kommt, dass sich die Tätigkeit des MAD mit der des BfV und des BND überschneidet, so zum Beispiel bei Reservisten mit der des BfV und im militärischen Auslandsbereich mit der des BND. Werden die Maßnahmen getrennt vorgelegt, kann keine Stelle die Überwachungsgesamtrechnung vornehmen. Die geteilte Zuständigkeit widerspricht damit dem Konzept, das der Entwurf selbst verfolgt. Im Übrigen gilt das bereits über Ermittlungsrichter gesagte, die nachrichtendienstliche Maßnahmen neben ihren sonstigen Aufgaben und ohne Spezialisierung in einem gegenüber dem UKRat strukturell unterlegenen Maße kontrollieren.

Zweitens verweist § 18 MADG-E auf die „zusätzlichen Voraussetzungen mindestens des § 8 Absatz 3“ und meint damit § 8 Abs. 3 MADG, nicht das BVerfSchG-E. Diese Stufe verlangt tatsächliche Anhaltspunkte für Tätigkeiten für eine fremde Macht oder für Straftaten mit einer Höchststrafe von mindestens fünf Jahren und entspricht damit in der Sache der Spitzenstufe des § 3 Abs. 8 Nr. 1 lit. a und Nr. 2 BVerfSchG-E. Unterhalb dieser Stufe weichen die Systeme dagegen ab, weil das MAD-Gesetz erheblich eingriffsintensive Mittel an Gruppen knüpft, etwa gewaltorientierte Personen oder solche mit eigenständigem Zugang zu dienstlichen Waffen (§ 8 Abs. 2 Nr. 1 und 4 MADG), das BVerfSchG-E hingegen an die Beobachtungsbedürftigkeit der Bestrebung (§ 3 Abs. 7 BVerfSchG-E). Diese Abweichung kann der Gesetzgeber bewusst beibehalten oder begründet angleichen.<sup>440</sup>

Drittens enthält das MAD-Gesetz 2026 bereits eine eigene Regelung für den Spannungs- und Verteidigungsfall (§ 52 MADG). Danach kann die Bundesregierung mit Zustimmung des PKGr feststellen, dass eine gerichtliche Anordnung nur noch für die Wohnraumüberwachung erforderlich ist und die Datenschutzkontrolle des BfDI entfällt. Das gilt auch dann, wenn der Spannungs- oder Verteidigungsfall erst unmittelbar bevorsteht (§ 52 Abs. 2 und 3 MADG).<sup>441</sup> Diese Verweise schreibt Art. 5 nicht fort, was in zwei Richtungen Folgen hat. Weil § 52 Abs. 2 Nr. 1 MADG den § 22 Abs. 1 modifiziert, während die neue Vorabkontrolle des UKRats in § 22 Abs. 1a steht, folgt aus dem bisherigen Wegfall gerichtlicher Anordnungen kein automatischer Wegfall dieser Vorabkontrolle. Umgekehrt verweist § 52 Abs. 2 Nr. 2 auf § 46 Abs. 1 und 2, in dessen Absatz 1 der Entwurf die Datenschutzkontrolle des UKRats einfügt. Die Ausnahme betreffe damit künftig nicht mehr allein den BfDI, sondern auch den UKRat. Der Gesetzgeber sollte deshalb die Reichweite dieser Verweise klären und das Verhältnis von Vorabkontrolle, administrativer Kontrolle und Sonderlagen ausdrücklich festlegen. Eine Ausdehnung des Kontrollwegfalls muss daraus nicht folgen. Im Ergebnis bestehen künftig drei Notstandsregime für drei Dienste, die der Gesetzgeber aufeinander abstimmen sollte. Die unter E. vorgeschlagenen Grenzen, namentlich die besonderen Sicherungen beim Einsatz Minderjähriger als Vertrauenspersonen und den Ersatz der Vorabkontrolle durch Rahmenfeststellungen, sollten dabei für alle drei Dienste gleich gefasst werden.

---

<sup>439</sup> Vgl. Sosna, GSZ 2026, 69.

<sup>440</sup> § 8 Abs. 2–4 MADG; § 3 Abs. 7 und 8 BVerfSchG-E.

<sup>441</sup> Vgl. Sosna, GSZ 2026, 69.

## II. Folgeänderungen mit Eigengewicht

Von den Folgeänderungen hat vor allem Art. 15 eigenes Gewicht. Er weist dem Bundesverwaltungsgericht erstinstanzlich drei Gruppen von Verfahren zu (§ 50 Abs. 1 Nr. 2a und 2b VwGO-E). Das sind die Feststellungsanträge zur Wohnraumüberwachung (§ 34 Abs. 4 BVerfSchG-E, § 97 Abs. 7 BNDG-E), die Klagen gegen die Einstufung von Beobachtungsobjekten und gegen die Information der Öffentlichkeit über die Einstufung (dazu C.II.3) sowie Klagen gegen Maßnahmen des UKRats in seinem Eigensicherungsbereich (§ 39 UKRatG-E). Die übrigen hier zu nennenden Folgeänderungen passen das bisherige Recht an: Die Art. 20 und 21 stimmen das Telekommunikationsgesetz und die Telekommunikations-Überwachungsverordnung auf die neuen Befugnisnormen ab. Art. 23 hebt das bisherige Recht mit Inkrafttreten des Gesetzes am Tag nach der Verkündung auf (Art. 24 Abs. 1; zur Übergangsfrist für Altanordnungen siehe C.V.). Art. 4 streicht schließlich die Übergangsvorschrift des § 79 BVerfSchG-E zum 1. Januar 2033 (Art. 24 Abs. 2), also zu dem Zeitpunkt, zu dem das G 10 auch für die Landesbehörden endgültig außer Anwendung tritt (weitergehende Kritik unter C).

## G. Querschnittsfragen

### I. Befristung und Evaluierung

Der Regierungsentwurf verzichtet auf eine Befristung und kündigt für die Fachbefugnisse eine gesetzesbegleitende Evaluierung an, ohne hierfür Ziele, Kriterien oder Zeitpunkte gesetzlich festzulegen.<sup>442</sup> Für die Effektivität der Kontrolle enthält § 41 UKRatG-E zwar bereits einen Evaluationsauftrag mit einem Bericht bis zum 1. Januar 2030 (vgl. unter D.XVII). Dieser ersetzt aber keine umfassende Evaluation der neuen Fachbefugnisse, was auch der Nationale Normenkontrollrat beanstandet hat.<sup>443</sup> Gegen eine Befristung sprechen indes nachvollziehbare Gründe: Befugnisse, die den Diensten auf Dauer zugedacht sind, sollten nicht unter dem Vorbehalt stehen, dass eine künftige Mehrheit sie durch bloße Untätigkeit auslaufen lässt. Zudem brauchen die Dienste Planungssicherheit für Personal, Technik und Kooperationen. Eine Evaluationspflicht halten wir aus rechtspolitischer Sicht dagegen für unverzichtbar. Ein Gesetz, das zwei Dienste neu aufstellt, diverse Interventionsbefugnisse schafft und die Kontrolllandschaft begründet, beruht auf Prognosen und Hoffnungen, die der Gesetzgeber überprüfen muss. Bei unsicheren Prognosen trifft ihn nach der Rechtsprechung des Bundesverfassungsgerichts zudem eine Beobachtungs- und gegebenenfalls Nachbesserungspflicht.<sup>444</sup> Wir schlagen deshalb eine Klausel vor, die die Bundesregierung verpflichtet, dem Bundestag fünf Jahre nach Inkrafttreten einen Bericht vorzulegen. Er sollte die Anwendung der Schutzmaßnahmen (§§ 59–62 BVerfSchG-E), der erweiterten nachrichtendienstlichen Maßnahmen (§§ 49–51 BNDG-E), der Eingriffe in informationstechnische Systeme (§§ 23–26 BVerfSchG-E, §§ 36–39 BNDG-E) und der Speicherfristen der strategischen Aufklärung (§ 66 BNDG-E) sowie die Arbeitsfähigkeit des UKRats behandeln. Der Bericht sollte unter Beteiligung des UKRats und eines externen Sachverständigen entstehen und sich an Kriterien orientieren, die das Gesetz benennt – namentlich Zahl und Art der Maßnahmen, Zahl der Beanstandungen und Anweisungen, Zahl der Mitteilungen an Betroffene und Dauer der Vorabkontrollverfahren. Zusätzlich empfehlen wir aus rechtspolitischer, nicht verfassungsrechtlicher Sicht eine jährliche öffentliche Statistik über die Zahl der Schutzmaßnahmen, der erweiterten nachrichtendienstlichen Maßnahmen und der Eingriffe in informationstechnische Systeme nach dem Vorbild der Übersichten des Bundesamts für Justiz zu strafprozessualen

<sup>442</sup> Begr. A.VIII, BT-Drs. 21/7868, S. 207.

<sup>443</sup> Stellungnahme des NKR, BT-Drs. 21/7868, S. 604.

<sup>444</sup> Zur Beobachtungs- und Nachbesserungspflicht des Gesetzgebers bei unsicherer Prognose vgl. BVerfGE 88, 203 u.a.

Maßnahmen (§ 101b StPO). Sie ersetzt keine Befristung, schafft aber die Grundlage politischer Befassungen. Zugleich kann sie der Sorge begegnen, der Staat überwache künftig grenzenlos.

## II. Haushaltsausgaben

Der Entwurf nennt für das BfV jährliche Mehrausgaben von 269 Millionen Euro und einmalige von 97 Millionen Euro, für den BND jeweils mindestens 35 und 40 Millionen Euro, für den UKRat 8,86 und 1,6 Millionen Euro.<sup>445</sup> Die veranschlagten jährlichen Mehrkosten des UKRats entsprechen rechnerisch knapp drei Prozent der für beide Dienste bezifferten jährlichen Mehrkosten von zusammen mindestens 304 Millionen Euro. Beim BfV sind weitere Personalkosten dabei noch nicht einmal konkret beziffert. Für sich belegt dieser Quotient weder eine Unterausstattung noch eine angemessene Ausstattung, weil Aufgaben, Ausgangsbestände und Personalkosten verschieden sind. Er gibt aber Anlass, nach einer gesonderten Bedarfskalkulation für die zusätzlichen Kontrollen zu fragen. Der Nationale Normenkontrollrat hat die Kostenschätzung als nicht methodengerecht und nicht nachvollziehbar bezeichnet und darauf hingewiesen, dass der Nutzen des Vorhabens nicht dargestellt ist. Wegen der besonderen Prognose- und Geheimhaltungsschwierigkeiten hat er gleichwohl keine Einwände erhoben.<sup>446</sup> Geheimhaltung kann die öffentliche Darstellung einzelner Bedarfe begrenzen, entbindet aber nicht von einer überprüfbaren (nötigenfalls vertraulichen) Bedarfskalkulation.

## III. Redaktionelles

Die Vorabfassung des Regierungsentwurfs enthält kleinere Verweisungsfehler und Unstimmigkeiten, die vor der Beschlussfassung zu bereinigen sind. Fehler, die uns bei der Durchsicht aufgefallen sind:

1. § 97 Abs. 3 S. 1 Nr. 4 BNDG-E: In der Wendung „auf Grundlage eines Zusatzes nach , § 46 Absatz 5“ fehlt vor dem Komma die Verweisung auf § 17 Absatz 4. Sie ist zu ergänzen, weil das bloße Entfernen des Kommas eine sachliche Kontrolllücke stehen ließe (S. 134).
2. § 31 Abs. 4 Nr. 3 BVerfSchG-E und § 21 Abs. 5 S. 2 BNDG-E: Die Vorlagepflicht bei kernbereichsrelevanten Informationen knüpft einmal an „Zweifel“, einmal an „tatsächliche Anhaltspunkte“ an. Die beabsichtigte Abweichung sollte erläutert oder der Wortlaut angeglichen werden (S. 33 und 87 f.). Es handelt sich nicht um eine bloß redaktionelle, sondern um eine materielle Schutzfrage (C.IV.6.b).
3. § 3 Abs. 8 BVerfSchG-E und § 4 Abs. 4 und 5 BNDG-E: Die höchsten Stufen tragen unterschiedliche Bezeichnungen, was nicht automatisch ein Redaktionsversehen ist. Eine einheitliche Terminologie empfehlen wir deshalb allenfalls als rechtspolitische Systematisierung, ohne unterschiedliche materielle Maßstäbe einzuebnen (S. 13 und 75).
4. Überschrift des § 32 BVerfSchG-E: „zeugnisverweigerungsberechtigten“ statt „zeugnisverweigerungsberechtigten“ (S. 8 und 34).
5. Begründung zu § 31 BVerfSchG-E: Aktenzeichen „I1 BvR 180/23“ statt „1 BvR 180/23“ (S. 271).
6. Begründung zu § 32 Abs. 4 BVerfSchG-E: Die Verweisung auf „§ 3 Absatz 4 G 10“ meint § 3b Abs. 4 G 10 (S. 272).

<sup>445</sup> Vorblatt, Abschnitt D, BT-Drs. 21/7868, S. 2 f.

<sup>446</sup> Stellungnahme des NKR, BT-Drs. 21/7868, S. 604 f. Der Bundesrat bittet zudem, den Erfüllungsaufwand der Länder unter ihrer Beteiligung zu ermitteln, BT-Drs. 21/8295, S. 1, 12.

## H. Zusammenfassung und wesentliche Thesen

1. **Die Reform ist richtig.** Sie entflechtet das BNDG, kodifiziert auch das BVerfSchG umfassend neu und integriert das G 10. Vor dem 1.1.2027 muss die Novelle in Kraft treten, damit die strategische Inland-Ausland-Aufklärung (mindestens von Cybergefahren) nicht entfällt.
2. **Die gestufte Schwellendogmatik beider Gesetze setzt die Vorgaben des Bundesverfassungsgerichts im Grundsatz um.** Nachzuschärfen sind die Öffnung des Rechtsgüterkatalogs, die Untergrenze der Spitzenstufe und die Regelvermutung für verschleiern des Vorgehen.
3. **Aufgaben und Beobachtungsobjekt-Regime des BfV sind tragfähig.** Die Fortführung eines Verdachtsfalls über fünf Jahre hinaus sollte der UKRat feststellen, der Prüffall eine Zweckbindung erhalten.
4. **Maßstab der neuen Interventionsbefugnisse ist die Wirkung der Maßnahme, nicht ein institutionelles Trennungsgebot.** Polizeiähnlich wirkende Maßnahmen verlangen mindestens eine konkretisierte Gefahr, digitale Gegenmaßnahmen ohne Anschlussbefugnisse können niedriger ansetzen.
5. **Die Zusammenführung der strategischen Aufklärung ist richtig, ihre Speicherfristen sind mit dem Grundgesetz wohl (noch) vereinbar.** Von Verfassungs wegen sind vor allem die Ausnahmen für reine Inlandskommunikation enger zu fassen und die Löschung von Protokolldaten an die Mitteilung zu koppeln. Gezielte Suchbegriffe gegen Personen im Inland sollten vorab kontrolliert, übrige personenbezogene Suchbegriffe intern freigegeben werden.
6. **Die erweiterten Maßnahmen des BND werden benötigt und sind verfassungsrechtlich tragfähig.** Ihr Anlass ist aber noch zu präzisieren, realweltliche Maßnahmen gegen bestimmte Personen und im Inland sollten eine konkretisierte Gefahr voraussetzen, und Freiheitsentziehungen im Ausland muss der Gesetzgeber entweder regulieren oder ausschließen.
7. **Die Schutzmaßnahmen des BfV sind in der Sache zwar vertretbar, zumindest kompetenzrechtlich aber sehr riskant. Wenn sie fortbestehen sollen, müssen körperliche und digitale Einwirkung für bessere Chancen in Karlsruhe getrennt werden.** Jedenfalls die realweltliche Einwirkung sollte auf eine Zielrichtung gegen fremde Mächte beschränken und an eine konkretisierte Gefahr gebunden sein. Betroffene sind nach Wegfall der Zweckgefährdung zu unterrichten.
8. **Die Systematisierung der IT-Befugnisse einschließlich der Online-Durchsuchung ist zu begrüßen.** Der Verzicht auf die Vollsichtung der Kernbereichsdaten ist jedoch verfassungsrechtlich nicht gesichert und sollte zumindest durch ein Sichtungsverfahren abgesichert werden.
9. **Die Regelungen zu menschlichen Quellen sind im Grundsatz verfassungskonform.** Der UKRat sollte die personenbezogenen Einsatzvoraussetzungen überprüfen können. Geringfügige Eingriffe in Individualrechte sollten in engem Rahmen und mit Entschädigung erlaubt, ein Weigerungsrecht in Verfahren vorgesehen werden.
10. **Das heimliche Betreten von Wohnungen ist ein Eingriff nach Art. 13 Abs. 7 GG und verfassungsrechtlich vertretbar, zumal es nur der Vorbereitung einer nachrichtendienstlichen**

**Überwachung dient.** Das Gesetz sollte jedoch u.a. klarstellen, dass die Norm nicht zur Durchsuchung im landläufigen Sinne ermächtigt.

**11. Die Abstufung des Schutzes von Berufsgeheimnisträgern ist verfassungsrechtlich vertretbar.** Die weitreichende Ausnahme im BNDG-E ist einzugrenzen, Heilberufe gehören rechtspolitisch in den Schutz, und die Verstrickung sollte eine objektiv wesentliche Förderung verlangen.

**12. Die Telekommunikationsüberwachung sollte an das Eingriffsgewicht anknüpfen, nicht an die Kategorie des Dienstes.** Inhalte der Mensch-Maschine- und Maschinenkommunikation unterfallen Art. 10 GG und können so aussagekräftig sein wie Telekommunikationsakte.

**13. Die Befugnisse zur Datenerhebung unter Mitwirkung Dritter sind im Grundsatz tragfähig.** Für gespeicherte Kommunikationsinhalte, langfristige Standortdaten und künftig anfallende Daten liegen die Schwellen eine Stufe zu niedrig. Eine befristete Sicherungsanordnung für Verkehrsdaten sollte hinzukommen.

**14. Die Übermittlungsregeln beider Gesetze sind im Ansatz tragfähig.** Die Rohdatenübermittlung an die Bundeswehr verlangt indes Sicherungen beim Empfänger, der Straftatenkatalog des BND sollte leichte Delikte verlieren, und das BfV sollte auf Ersuchen zu begünstigenden Maßnahmen weiterhin ohne eigenes Ermessen übermitteln müssen.

**15. Bei den Datenpflichten bleibt das BVerfSchG-E hinter dem geltenden Recht zurück.** Regelspeicherfrist, Speicherverbot für Kinder, Prüfintervalle und Mitteilungsmaßstab sollten eher auf dem heutigen Stand bleiben.

**16. Das Auskunftsrecht des BND überzeugt und sollte in das BVerfSchG-E übernommen werden.** Der Anspruch auf ermessensfehlerfreie Entscheidung muss dabei gegenüber den erweiterten Ausschlussgründen fortbestehen.

**17. Die Eigensicherung beider Dienste ist als Schutz der eigenen Kräfte verfassungsrechtlich tragfähig.** Straftatanknüpfung, Kennzeichnung und Belehrung sollten vom BND auf das BfV übertragen werden, die Auswertung vorschriftswidrig eingebrachter Geräte vom BfV auf den BND. Die räumliche Ausweitung im BNDG-E außerhalb der Grenzen der Dienststellen und über die Nachteile hinaus ist nicht unkritisch.

**18. Der UKRat als Gesamtkontrolleur ist eine konsequente Entscheidung.** Er braucht durchsetzbare Anweisungen, Prüfaufträge über die strategische Aufklärung hinaus, eine belegte Ausstattung und eine vollständige Besetzung nur aus Richtern des Bundesgerichtshofs und des Bundesverwaltungsgerichts (sowie gegebenenfalls noch Bundesanwälten bei Personalmangel).

**19. Sonderregeln für Spannungs- und Verteidigungsfall sind notwendig, müssen aber gestuft, befristet und parlamentarisch rückgebunden sein.** Die Vorabkontrolle darf nur durch ein Eilverfahren mit nachträglicher Bestätigung ersetzt werden, die administrative Kontrolle nicht vollständig entfallen.

**20. Auf eine Befristung des Gesetzes kann der Gesetzgeber verzichten, nicht aber auf eine Evaluationsklausel mit gesetzlichen Kriterien.**



Im Original gezeichnet

Im Original gezeichnet

(Ogorek)

(Manns)