



---

**Ausschussdrucksache 21(4)233 A**  
vom 9. Oktober 2026

---

**Schriftliche Stellungnahme**

von Prof. Dr. Markus Löffelmann, Hochschule des Bundes für  
öffentliche Verwaltung vom 8. Oktober 2026

zu dem

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



Hochschule des Bundes  
für öffentliche Verwaltung

POSTANSCHRIFT HS BUND, POSTFACH 40527, 10063 BERLIN

Herrn Vorsitzenden

des Innenausschusses des Deutschen  
Bundestags

- ausschließlich per E-Mail -

**Prof. Dr. Markus Löffelmann**

HAUSANSCHRIFT Habersaathstr. 51, 10115 Berlin

POSTANSCHRIFT Postfach 40527, 10063 Berlin

TEL 030 – 22 00 89 – 85513

E-MAIL markus.loeffelmann@hsbund-nd.de

DATUM Berlin, 08.10.2026

**BETREFF Stellungnahme zu BT-Drs. 21/7868**

Sehr geehrter Herr Vorsitzender,

anliegend übersende ich die erbetene Stellungnahme zu dem

Gesetzentwurf der Bundesregierung

**Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts**

BT-Drucksache 21/7868



## A. Vorbemerkung

Der Gesetzentwurf dient einer grundsätzlichen Neuausrichtung des Rechts der Nachrichtendienste auf Bundesebene. Ein erster Teil der Reform erfolgte bereits mit den Gesetzen vom 22.12.2023 zur Novellierung der Übermittlungsbefugnisse, ein zweiter Teil mit der Gesamtnovellierung des MADG durch das Gesetz vom 9.1.2026. Parallel wurden bereits in zahlreichen Ländern die Verfassungsschutzgesetze überarbeitet oder neugefasst.<sup>1</sup>

Die Reform des deutschen Nachrichtendienstrechts ist aus mehreren Gründen überfällig: Erstens hat das BVerfG in den letzten rund fünf Jahren in mehreren Entscheidungen zum Nachrichtendienstrecht<sup>2</sup> und anderen Bereichen des Sicherheitsrechts<sup>3</sup> grundsätzliche Weichenstellungen vorgegeben, die der Umsetzung bedürfen. Die beiden zentralen Gesichtspunkte sind insoweit die Etablierung eines gestuften Systems der nachrichtendienstlichen Beobachtungsbedürftigkeit und korrespondierender Eingriffsschwellen für nachrichtendienstliche Befugnisse sowie eines Systems der Vorabkontrolle bei eingriffsintensiven Maßnahmen. Zweitens erfordern technische Entwicklungen ein Schritthalten der Gesetzgebung auch im Tätigkeitsbereich der Nachrichtendienste. Drittens erfordern neue Bedrohungslagen, insbesondere durch Cyberangriffe und hybride Maßnahmen, neue nachrichtendienstliche Reaktionsmöglichkeiten. Und viertens behindert die vielfach uneinheitliche und unklare Rechtslage für die Nachrichtendienste auf Bundes- und Länderebene eine effektive und effiziente sicherheitsbehördliche Zusammenarbeit.

Der Gesetzentwurf wird diesen Herausforderungen weitgehend gerecht. Er geht aber vielfach auch über sie hinaus, strapaziert verfassungsrechtliche Grenzen und bewegt sich – bewusst – auf verfassungsrechtliches Neuland. Allein der schiere Umfang der Regelungen, die hohe Regelungsdichte sowie komplexe Gesetzgebungstechniken machen dabei eine Analyse des Entwurfs zu einer echten Herausforderung. Die für das parlamentarische Verfahren – auch im Vergleich zu den vorangegangenen langjährigen Arbeiten auf Ressortebene – zur Verfügung stehende Kürze der Zeit und Begrenztheit der Ressourcen steht zu der Tragweite der Änderungen in keinem angemessenen Verhältnis.

---

<sup>1</sup> Vgl. bislang BayVSG, LVSG BW, HmbVerfSchG, HVSG, LVerfSchG M-V, NVerfSchG, VSG NRW, LVerfSchG RP, SVerfSchG, SächsVSG, VerfSchG-LSA; andere Gesetzgebungsvorhaben sind derzeit im Gang.

<sup>2</sup> BVerfGE 154, 152; BVerfGE 156, 11; BVerfGE 162, 1; BVerfGE 163, 43; BVerfGE 169, 30; BVerfGE 170, 79.

<sup>3</sup> BVerfGE 158, 170; BVerfGE 165, 1; BVerfGE 165, 363; BVerfGE 169, 332; BVerfGE 170, 247; BVerfGE 172, 46; BVerfGE 172, 106.



Im Folgenden (B.) wird kursorisch auf zentrale Kritikpunkte an dem Gesetzespaket eingegangen. Abschließend (C.) erfolgt eine zusammenfassende, auch die gelungenen Regulationsaspekte in den Fokus rückende Gesamtwürdigung. Dass eine sachverständige Stellungnahme in dem verfügbaren Zeitrahmen nicht alle Probleme eines so umfangreichen Gesetzgebungsvorhabens ausloten oder auch nur identifizieren kann, versteht sich von selbst. Die Artikel 6 bis 23 wurden keiner Prüfung unterzogen.

## B. Kritische Würdigung

### I. Zu Artikel 1 – BVerfSchG-E

#### 1. Zu § 8 Abs. 1 BVerfSchG-E

Die Vorschrift erweitert die Möglichkeiten der Datenerhebung aus öffentlich zugänglichen Quellen (OSINT) auf automatisierte Anwendungen. Sie erlaubt dabei auch das systematische Zusammenführen von Daten zu einer Person (Satz 2 Nummer 1) und den Abgleich von biometrischen Merkmalen (Satz 2 Nummer 2).

Problem: Das automatisierte Erheben von Daten aus öffentlich zugänglichen Quellen ist keine Datennutzung, wie sie „jedem Dritten“<sup>4</sup> zugänglich ist.<sup>5</sup> Das Erheben der Daten besitzt deshalb Eingriffsqualität und eine sehr große Streubreite. Es handelt sich de facto um eine Form der Massendatenverarbeitung, für die das BVerfG<sup>6</sup> und europäische Gerichte<sup>7</sup> strenge Vorgaben aufgestellt haben. Weil sich auf diese Weise eine Vielzahl von personenbezogenen Daten zu einem Verhaltens- und Persönlichkeitsprofil verdichten lassen, ist auch die potenzielle Eingriffsintensität hoch. Die Regelung in einer Generalklausel wird dem nicht gerecht. Erst recht gilt das, wenn es sich um das Erheben und Abgleichen biometrischer, also besonders sensibler (Art. 9 DS-GVO, Art. 10 JI-RL) Daten handelt. Daran ändert auch das „Vorfeldprivileg“ der Nachrichtendienste, Informationen unter insgesamt niedrigeren Schwel-

---

<sup>4</sup> BVerfGE 120, 351, 361; BVerfGE 142, 234, 252.

<sup>5</sup> Das gilt ungeachtet der Tatsache, dass heute Webcrawler kommerziell leichter verfügbar sind; das BVerfG hatte bei der zitierten Rechtsprechung erkennbar manuelle Datenerhebungen im Blick.

<sup>6</sup> Vgl. BVerfGE 125, 274; BVerfGE 154, 152; auch die Maßgaben zur automatisierten Datenanalyse (BVerfGE 165, 363) dürften hier in ihrer grundsätzlichen Zielrichtung maßstabsbildend sein, zumal eine qualifizierte Auswertung nach § 37 BVerfSchG-E nach Vorstellung der Entwurfsverfasser auch im Rahmen einer Datenerhebung Anwendung finden soll (S. 287).

<sup>7</sup> EGMR, Big Brother Watch u.a. ./ Vereinigtes Königreich [GK], 25. Mai 2021, Nr. 58170/13 u.a.; EGMR, 25. Mai 2021, Centrum för Rättvisa ./ Schweden, Nr. 35252/08.



len als andere Sicherheitsbehörden erheben zu dürfen<sup>8</sup>, nichts, weil das automatisierte Erheben von Daten aus öffentlich zugänglichen Quellen gerade im Binnenvergleich nachrichtendienstlicher Mittel ein erhöhtes Eingriffsgewicht aufweist. Ähnliche Befugnisse in anderen aktuellen Gesetzentwürfen der Bundesregierung sind deutlich enger und präziser ausgestaltet und trotzdem nicht verfassungsrechtlich unbedenklich.<sup>9</sup>

Lösung: Regelung der automatisierten Datenerhebung als selbständiges nachrichtendienstliches Mittel mit qualifizierten Eingriffsschwellen.

## 2. Zu § 8 Abs. 2 BVerfSchG-E

Die Vorschrift erlaubt die Durchführung eines Abgleichs biometrischer Merkmale durch öffentliche und nicht-öffentliche Stellen in Drittstaaten außerhalb der EU.

Problem: Mit der Übermittlung besonders sensibler personenbezogener Daten in Drittstaaten erhöhen sich die datenschutzrechtlichen Risiken für betroffene Personen beträchtlich. Es ist z.B. zwanglos vorstellbar, dass allein der Umstand einer in einen Drittstaat adressierten Anfrage des BfV zu einem biometrischen Merkmal für die betroffene Person dort (etwa bei einer Einreise) mit nachteiligen Konsequenzen verbunden ist. Bei der Einbindung von privaten Stellen ist die Schwierigkeit ihrer datenschutzrechtlichen Kontrolle und die Möglichkeit des hoheitlichen Zugriffs auf deren Datenbestände zu berücksichtigen (vgl. etwa den US-amerikanischen Cloud Act). Generell berührt die Einbindung von Stellen in Drittstaaten Aspekte der digitalen Souveränität.<sup>10</sup> Das BVerfG fordert bei nachrichtendienstlichen Datenübermittlungen ins Ausland besondere Vorkehrungen zum Daten- und Menschenrechtsschutz.<sup>11</sup> Die Maßgaben der KI-VO greifen – ungeachtet der Frage, ob nachrichtendienstliches Handeln generell unter den Vorbehalt nationaler Sicherheit fällt – bei einer Datenverarbeitung in Drittstaaten nicht. Das alles begründet ein hohes verfassungsrechtliches Risiko.

Lösung: Beschränkung der Auftragsdatenverarbeitung auf Stellen innerhalb der EU.

---

<sup>8</sup> BVerfGE 162, 1, 77 m.w.N.

<sup>9</sup> Vgl. hierzu ausf. Löffelmann, Deutscher Bundestag, Innenausschuss, Ausschussdr. 21(4)214 B zu BT-Drs. 21/6131, 21/6132, 21/6511, 21/6806, 21/6913 und 21/6917.

<sup>10</sup> Vgl. BfDI, Deutscher Bundestag, Innenausschuss, Ausschussdr. 21(4)179, S. 7 f., 10; DAV, Deutscher Bundestag, Innenausschuss, Ausschussdr. 21(4)214 E, S. 18; allg. zur Problematik Digitaler Souveränität im Zusammenhang mit sicherheitsbehördlichem Handeln Kelber/Bortnikov, NJW 2023, 2000.

<sup>11</sup> BVerfGE 154, 152, 273 ff.; BVerfGE 162, 1, 121 ff.



### **3. Zu § 10 Abs. 1 S. 2 Nr. 2 BVerfSchG-E**

Die Vorschrift erlaubt das Einrichten eines automatisierten Verfahrens für den Abruf von bei inländischen öffentlichen Stellen gespeicherten personenbezogenen Daten „in geeigneten Fällen“.

Problem: Automatisierte Abrufverfahren bergen ein erhöhtes datenschutzrechtliches Risiko, weil eine Rechtmäßigkeitsprüfung für die Übermittlung durch die abgebende Stelle im Einzelfall fehlt. Dieses Defizit wird üblicherweise durch die Einrichtung besonderer organisatorisch-technischer Sicherungen abgedeckt.<sup>12</sup> Daran fehlt es hier. Die Norm lässt noch nicht einmal Kriterien erkennen, nach denen sich richtet, ob es sich um einen geeigneten Fall handelt. Hinzu kommt, dass automatisierte Abrufverfahren generell Daten in größerem Umfang auch für weitere Zwecke der automatisierten Analyse (vgl. § 37 BVerfSchG-E) verfügbar machen.

Lösung: Streichung oder präzise Regelung automatisierter Verfahren mit organisatorisch-technischen Sicherungen für bestimmte Daten und übermittelnde Stellen.

### **4. Zu § 11 Abs. 1 Nr. 2 BVerfSchG-E**

Die Vorschrift etabliert eine Befugnis zur Abfrage von Kfz-Telemetriedaten bei Kfz-Herstellern und Kfz-Werkstätten.

Problem: Kfz-Telemetriedaten können eine Vielzahl von Daten unterschiedlichster Schutzwürdigkeit umfassen, wie etwa Daten zum Fahrverhalten, zur Nutzung von Assistenz- und Infotainmentsystemen bis hin zu Innenraumdaten. Auf diese Weise ist eine engmaschige Überwachung der Fahrzeuginsassen möglich. Zugleich wird der Umfang von Telemetriedaten perspektivisch weiter zunehmen; schon heute können keine Neuwagen mehr erworben werden, die keine Daten übertragen. Vor diesem Hintergrund müsste es sich zumindest um eine qualifizierte Auskunft handeln. Die Parallelnorm in § 20 Abs. 1 S. 1 Nr. 2 MADG ist auf Standortdaten begrenzt. Außerdem sollte bei einer Beauskunftung über einen längeren Zeitraum ein Gleichlauf mit § 20 BVerfSchG-E hergestellt werden.

---

<sup>12</sup> Vgl. etwa zur automatisierten Bestandsdatenabfrage nach § 173 TKG ausf. Löffelmann in: Dietrich/Gärditz (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2. Aufl. 2026, VI § 5 Rn. 3 ff.



Lösung: Begrenzung auf Standortdaten oder Anheben der Eingriffsschwelle.

### **5. Zu § 11 Abs. 3 S. 2, Abs. 6, auch i.V.m. § 13 Abs. 1 S. 2 BVerfSchG-E**

Die Vorschriften etablieren erstmals die Verpflichtung einer Auskunft erteilenden Stelle gegenüber einem Nachrichtendienst, künftig anfallende und zu beauskunftende Daten zu speichern.

Problem: Die Speicherpflicht begründet für die verpflichteten Stellen einen zusätzlichen Eingriff in Art. 12 GG. Für die betroffenen Personen erhöht sich die Eingriffsintensität der Auskunftserteilung erheblich, denn auf diese Weise erfolgt nicht nur eine retrograde Datenerfassung, sondern wird prospektiv für die Dauer von bis zu einem Jahr (§ 11 Abs. 6 S. 1 BVerfSchG-E) eine Überwachung ermöglicht. Das kommt de facto einer langfristigen Überwachung durch das BfV selbst gleich.

Lösung: Streichung oder Herstellung eines Gleichlaufs mit langfristigen Überwachungsmaßnahmen.

### **6. Zu § 15 BVerfSchG-E**

Die Vorschrift schafft eine Befugnis zum Zugriff auf Videoüberwachungseinrichtungen privater und öffentlicher Stellen.

Problem: Die Videoüberwachung des öffentlichen Raums bedeutet einen erheblichen<sup>13</sup> oder sogar schweren<sup>14</sup> Eingriff in das Recht auf informationelle Selbstbestimmung. Rechtsgrundlage hierfür ist i.d.R. § 4 BDSG. Nach § 4 Abs. 2 BDSG sind u.a. Name und Kontaktdaten des Verantwortlichen erkennbar zu machen. Die Kenntnis der betroffenen Personen beseitigt zwar nicht die Eingriffsqualität<sup>15</sup>, mindert aber deren Intensität. Vor diesem Hintergrund müsste die Mitbenutzung solcher Einrichtungen durch das BfV kenntlich gemacht werden. Das sieht die Norm (aus Gründen der Praktikabilität zurecht) nicht vor. Parallelnormen in

---

<sup>13</sup> Eichberger in Huber/Voßkuhle, GG, 8. Aufl. 2024, Art. 2 Rn. 333.

<sup>14</sup> BVerfG NVwZ 2007, 688, 691.

<sup>15</sup> BVerfG NVwZ 2007, 688, 690.



einigen Bundesländern sehen nur eine Pflicht zum Ausleiten vor (vgl. Art. 19a Abs. 1 S. 4 BayVSG; § 14a Abs. 11 BbgVerfSchG; anders aber § 21 LVerfSchG RP).

Lösung: Begrenzung auf die Verpflichtung zum Ausleiten von Aufzeichnungen.

### **7. Zu § 16 Abs. 1 S. 1, Abs. 5 S. 1 Nr. 2, S. 3, 4 BVerfSchG-E**

Die Norm sieht – wie schon das geltende Recht – eine Befugnis zum Einsatz nachrichtendienstlicher Mittel bereits zur Quellenanbahnung vor („zur Gewinnung von Erkenntnissen über ... die zu deren Aufklärung erforderlichen verdeckten Hilfspersonen“).

Problem: Da Quellen keine Veranlassung dafür gesetzt haben, dass nachrichtendienstliche Mittel gegen sie eingesetzt werden, kann das Veranlassungsprinzip, dem das BVerfG eine zentrale legitimatorische Funktion zuschreibt<sup>16</sup>, nicht als Rechtfertigungsgrund herangezogen werden. Vor diesem Hintergrund begegnet jedenfalls der Einsatz eingriffsintensiver nachrichtendienstlicher Mittel zur Quellenanbahnung gewissen Bedenken, auch wenn der Zweck einer erfolgreichen Quellenführung solche Maßnahmen als praktisch sinnvoll erscheinen lassen mag. § 16 Abs. 5 S. 4 BVerfSchG-E sieht insoweit eine Einschränkung nur für besonders eingriffsintensive Mittel vor. Eine ausgewogene Lösung verfolgt z.B. das neue Verfassungsschutzgesetz des Landes Berlin: Nach § 23 Abs. 3 S. 1 VSG Bln dürfen nachrichtendienstliche Mittel auch zum Schutz der Nachrichtenzugänge eingesetzt werden; zu deren Anbahnung stehen im Umkehrschluss nur die allgemeinen Befugnisse gem. § 11 VSG Bln zur Verfügung.

Lösung: Erstreckung von Absatz 5 Satz 4 auf Maßnahmen die bei erheblich beobachtungsbedürftigen Bedrohungen zulässig sind.

### **8. Zu § 16 Abs. 4 S. 2-5 BVerfSchG-E**

Die Vorschriften erlauben die Erprobung unbenannter nachrichtendienstlicher Mittel für die Dauer von vier Jahren.

---

<sup>16</sup> Vgl. nur BVerfGE 141, 220, 269.



Problem: Ob ein Mittel „vergleichbar gewichtig eingreifend“ wie die in den §§ 17 bis 27 BVerfSchG-E geregelten Mittel ist, und ob es der Verfassungsschutzbehörde zur Verfügung gestellt werden soll, ist eine originäre Bewertung und Entscheidung durch den Gesetzgeber. Gerade bei qualifiziert eingriffsintensiven Mitteln kann die Entscheidung darüber nicht auf die Exekutivbehörde verlagert werden. Das ist schon deshalb ausgeschlossen, weil der Gesetzgeber bei der Schaffung neuer Befugnisse auch das kumulative Zusammenwirken bestehender Befugnisse und die „Überwachungsgesamtbelastung“ berücksichtigen muss.<sup>17</sup> Die Regelung begrenzt die Erprobung neuer Mittel noch nicht einmal der Anzahl nach. Die wünschenswerte Technikoffenheit von Befugnissen kann in der Regel durch einen höheren Abstraktionsgrad der Formulierung oder eine phänomenologische (und nicht technische) Beschreibung der Maßnahme erreicht werden.

Lösung: Streichung.

## 9. Zu § 17 BVerfSchG-E

Die Norm schafft erstmals eine spezifische Rechtsgrundlage für den praktisch wichtigen Einsatz „virtueller Agenten“.

Problem: Eine erhöhte Eingriffsintensität ist nicht nur bei realweltlichen Treffen mit der Zielperson oder mehr als dreimaligen wirtschaftlichen Zuwendungen denkbar. Diese Tatbestände wirken zu einem gewissen Grad beliebig und sind vermutlich das Ergebnis einer praxisorientierten Betrachtungsweise. Fraglich ist zudem, warum hier die Qualifikationen und Verbote des § 18 Abs. 2 bis 6 BVerfSchG-E nicht gelten sollen. Das hat u.a. zur Folge, dass für Straftaten, die im Rahmen von Internetermittlungen begangen werden, kein spezieller gesetzlicher Rechtfertigungsgrund greift (vgl. § 18 Abs. 5 und 6 BVerfSchG-E). Evtl. wäre eine Regelung im Kontext des § 19 BVerfSchG-E (der dann thematisch weiter gefasst wäre) systematisch sinnvoller.

Lösung: Überarbeitung.

---

<sup>17</sup> BVerfGE 125, 260, 323 f.



## **10. Zu § 18 Abs. 1, 5 und 6 BVerfSchG-E**

Die Vorschriften übernehmen mit wenigen Modifizierungen die entsprechenden Regelungen des § 9b BVerfSchG.

Problem: Die Regelungen des geltenden Rechts begegnen in vielfacher Hinsicht der Kritik.<sup>18</sup> Der Entwurf versäumt es, darauf zu reagieren.

Lösung: Überarbeitung.

## **11. Zu § 22 Abs. 1 S. 4 BVerfSchG-E**

Die Vorschrift gestattet der Verfassungsschutzbehörde das Einbringen von Mitteln – auch technischen – in Brief- und Postsendungen zum Zweck der Informationsgewinnung.

Problem: Nach dem Verständnis der Entwurfsverfasser soll die Vorschrift nicht nur das Einbringen von Mitteln in Brief- und Postsendungen, also einen Eingriff in Art. 10 GG, erlauben, sondern auch das Einbringen in die in den Sendungen enthaltenen Objekte (S. 255), wodurch zusätzlich andere Grundrechte betroffen sein können und sich die Eingriffsintensität erhöht. Das sollte klargestellt werden (vgl. § 28 Abs. 3 BNDG-E).

Lösung: Einfügen der Formulierung „und in diesen enthaltenen Gütern“ nach dem Wort „Postsendungen“.

## **12. Zu § 22 Abs. 1 S. 2 Nr. 2, Abs. 2 BVerfSchG-E**

Die Reichweite der Befugnis zur Telekommunikationsüberwachung in Abgrenzung zu Maßnahmen nach §§ 23, 25 und 26 BVerfSchG-E ist schwer verständlich.

Problem: Der Schutzbereich des Art. 10 GG folgt keinem technischen Telekommunikationsbegriff.<sup>19</sup> Das BVerfG hat in seiner jüngeren Rechtsprechung jedoch angedeutet, dass auch nicht interpersonelle Datenübertragungen, wie das Surfen im Internet oder Datensynchroni-

---

<sup>18</sup> Vgl. ausf. Löffelmann/Zöller, Nachrichtendienstrecht, 2. Aufl. 2025, Rn. B.81 ff.

<sup>19</sup> Vgl. BVerfGE 124, 43, 55 f.; BVerfG NJW 2007, 351, 353; BVerfG NJW 2016, 3508 ff.



sierungen Art. 10 GG zuzuordnen sein sollen.<sup>20</sup> Die Ausklammerung der Überwachung solcher Kommunikation aus § 22 BVerfSchG-E und Zuordnung zu den Befugnissen nach §§ 23, 25 und 26 BVerfSchG-E ist vor diesem Hintergrund verwirrend. Im Ergebnis wird durch diese Weichenstellung das Überwachen „einseitiger“ Telekommunikation dem Erfassen von Verkehrsdaten gleichgestellt, was eine erhebliche Befugnisserweiterung bedeutet (vgl. auch die Ausführungen unter II.15.).

Lösung: Streichung von § 22 Abs. 2 BVerfSchG-E und Ergänzung von § 22 Abs. 1 S. 2 BVerfSchG-E um eine Ziffer 3, die andere Signale erfasst, welche keine Inhalte von Telekommunikationsdiensten sind.

### **13. Zu § 22 Abs. 5 BVerfSchG-E**

Die Regelung übernimmt den Rechtswegausschluss des geltenden Rechts aus § 13 G 10.

Problem: Der explizite Rechtswegausschluss schmälert nach den vom EGMR entwickelten Maßstäben erheblich die Legitimationsfähigkeit der Telekommunikationsüberwachung. Das grundsätzliche Offenstehen eines Rechtswegs besitzt vor diesem Hintergrund eine nicht geringe strategische Bedeutung. Die praktische Bedeutung des Rechtswegausschlusses ist demgegenüber marginal. Für andere heimliche Maßnahmen – auch solche der strategischen Telekommunikationsüberwachung – ist er im geltenden Recht nicht vorgesehen.

Lösung: Streichung.

### **14. Zu § 23 BVerfSchG-E**

Die Vorschrift regelt informationstechnische Eingriffe in nicht-private IT-Systeme.

Problem: Entgegen dem Eindruck, den die Überschrift erweckt, erfasst die Norm nicht den „klassischen“ Fall der Asservatenauswertung, also die Auswertung privater IT-Geräte. Diese soll nur nach Maßgabe der §§ 25, 26 BVerfSchG-E zulässig sein (§ 23 Abs. 5 S. 1 BVerfSchG-E). Das Auswerten von IT-Geräten unterscheidet sich aber phänomenologisch klar

---

<sup>20</sup> BVerfGE 172, 46, 83 f.



von der „Online-Durchsuchung“, da im ersten Fall keine aktiv genutzten Geräte betroffen sind und nur eine retrograde Datenerhebung möglich ist. In anderen Bereichen des Sicherheitsrechts ist die Asservatenauswertung – wenngleich nicht unumstritten – relativ niedrigschwellig zulässig.<sup>21</sup> Das spricht dafür, sie in Abgrenzung zur Online-Durchsuchung als eigenständiges nachrichtendienstliches Mittel zu regeln, wie z.B. in § 16 Abs. 2 MADG oder § 54 BNDG-E. Außerdem können auch nicht-private IT-Systeme unter Verhältnismäßigkeitsgesichtspunkten gleich schutzwürdig wie private sein, etwa wenn sich darauf wichtige Geschäftsgeheimnisse befinden. Die Differenzierung zwischen privaten und nicht-privaten IT-Systemen mag daher mit Blick auf den Schutzbereich des IT-System-Grundrechts ihre Berechtigung haben, schöpft aber die Varianz der erforderlichen Verhältnismäßigkeitserwägungen nicht aus.

Lösung: Schaffung einer eigenständigen Befugnis zur Asservatenauswertung unabhängig davon, ob private oder andere IT-Systeme betroffen sind.

## 15. Zu § 25 BVerfSchG-E

Die Vorschrift betrifft informationstechnische Eingriffe vom Zuschnitt einer „Online-Durchsuchung“.

Problem: Nach der – explizit zum Bereich nachrichtendienstlicher Tätigkeit ergangenen – verfassungsgerichtlichen Rechtsprechung ist diese hoch eingriffsintensive Maßnahme nur zur *Abwehr* von Gefahren zulässig.<sup>22</sup> Die Vorschrift enthält – anders als die beiden bereits existierenden landesrechtlichen Vorschriften (Art. 10 Abs. 1 S. 1 BayVSG; § 7a HVSG) – keine entsprechende Zweckbindung. Weil die mit dem Gefahrbegriff verknüpfte Prognose einer Rechtsgutsverletzung eine Wahrscheinlichkeit des erwarteten Schadens zugrunde legt, die umgekehrt proportional zum Gewicht der betroffenen Rechtsgüter steht<sup>23</sup>, beseitigt die Voraussetzung einer Gefahr auch nicht die Praktikabilität einer solchen Maßnahme. Denn

---

<sup>21</sup> Das gilt insbesondere für das Auswerten von Datenträgern zu Zwecken der Strafverfolgung; vgl. hierzu die Verhandlungen der strafrechtlichen Abteilung des 74. DJT 2024; dazu Krause, ZRP 2025, 17 ff.; El-Ghazi, NJW-Beilage 2024, 46 ff.; Hiéramente, ZRP 2025, 221 ff.; jew. m.w.N.

<sup>22</sup> BVerfGE 120, 274, 330: kein Anlass zu behördenbezogenen Differenzierungen; BVerfGE 162, 1, 81 f., 86 f.

<sup>23</sup> Vgl. dazu ausf. m.w.N. Löffelmann/Pfundmair/Lutsch, GSZ 2026, Heft 5 (i.E.); Löffelmann, „Wer alles weiß, soll nicht alles dürfen“ – technische Überwachungsbefugnisse von Polizei und Nachrichtendiensten im Vergleich in: Dietrich/Gärditz/Schmahl/Gusy/Warg (Hrsg.), Nachrichtendienstrecht im Wandel der Technik. 6. Symposium zum Recht der Nachrichtendienste, i.E.



Verfassungsschutzbehörden schützen besonders gewichtige Rechtsgüter, weshalb die Wahrscheinlichkeit des Schadenseintritts niedriger ausfallen kann als bei einem auf andere Rechtsgüter bezogenen gefahrenabwehrenden Handeln.

Lösung: Einfügen einer auf die Abwehr von Gefahren gerichteten Zweckbindung.

## 16. Zu § 26 BVerfSchG-E

Die Vorschrift erlaubt informationstechnische Eingriffe unterhalb eines Zugriffs auf das System, der Einblick in wesentliche Teile der Lebensgestaltung einer Person ermöglicht.

Problem: Informationstechnische Eingriffe, durch die ein Einblick in wesentliche Teile der Lebensgestaltung einer Person ermöglicht werden, nehmen in der Rechtsprechung des BVerfG aufgrund ihrer sehr hohen Eingriffsintensität grundsätzlich eine Sonderstellung ein. Das BVerfG überträgt auf solche Maßnahmen die Anforderungen, die es an eine Wohnraumüberwachung stellt.<sup>24</sup> In seiner jüngsten Rechtsprechung zur Quellen-Telekommunikationsüberwachung hat das Gericht allerdings zu erkennen gegeben, dass ein Absenken dieser Anforderungen nach Verhältnismäßigkeitsgesichtspunkten möglich ist.<sup>25</sup> Was das genau bedeutet und ob insbesondere in solchen Fällen die auf die Abwehr von Gefahren gerichtete Zweckbindung sowie die Subsidiarität gegenüber polizeilichen Maßnahmen nicht gelten, ist unklar. Die Quellen-Telekommunikationsüberwachung und die durch sie zu erlangenden Daten besitzen jedenfalls so präzise Konturen, dass diese Maßnahme klar gegenüber einer Online-Durchsuchung und den dort im Einzelfall vorzunehmenden Verhältnismäßigkeitserwägungen abgegrenzt werden kann.<sup>26</sup> Bei § 26 BVerfSchG-E ist das nicht der Fall. Die Legaldefinition der „abgegrenzten Datenerhebung“ in Absatz 1 Satz 2 ist teilweise tautologisch und viel zu unbestimmt. Insbesondere kann auch bei einer Datenerhebung aus abgegrenzten Teilen des Systems und bestimmten Daten ein Einblick in wesentliche Teile der Lebensgestaltung einer Person ermöglicht werden. Hier besteht die Gefahr einer Umgehung der hohen verfassungsrechtlichen Anforderungen an eine Online-Durchsuchung.

---

<sup>24</sup> BVerfGE 120, 274, 328 f.; BVerfGE 141, 220, 272 f.; BVerfGE 162, 1, 85, 129 f., 139 ff.

<sup>25</sup> BVerfGE 172, 46, 98.

<sup>26</sup> In der älteren Rechtsprechung des BVerfG galt die Quellen-Telekommunikationsüberwachung ohnehin als ein nur in Art. 10 GG eingreifendes aliud zur Online-Durchsuchung, vgl. BVerfGE 120, 274, 308, 309.



Lösung: Streichung oder klare gesetzliche Bezeichnung von Art und Umfang der zu erhebenden Daten.

### **17. Zu § 28 Abs. 1 BVerfSchG-E**

Die Vorschrift etabliert eine Befugnis zur Anwendung unmittelbaren Zwangs im Falle einer gegenwärtigen Gefahr für Leib, Leben und Freiheit von Bediensteten oder Hilfspersonen des BfV und dritten Personen sowie Sachen von bedeutendem Wert.

Problem: Die Entwurfsbegründung (S. 265 f.) weist zutreffend darauf hin, dass entsprechende Maßnahmen auch bislang schon auf Grundlage der allgemeinen Notwehr- und Nothilferegulungen möglich waren. Warum diese nicht ausreichen, wird nicht deutlich. Der hinter der Regelung stehende Gedanke lässt sich letzten Endes auf alle hoheitlichen Bediensteten übertragen, die besonderen Konfliktsituationen ausgesetzt sein können, ohne dass entsprechende Regelungen in anderen Gesetzen vorgesehen sind. Das gilt sogar für die Polizeigesetze, in denen die Anwendung unmittelbaren Zwangs als Mittel zur Durchsetzung polizeilicher Anordnungen geregelt ist (vgl. etwa Art. 77 BayPAG), nicht aber speziell zur Einsatzsicherung. Hierfür gelten auch dort die zivil- und strafrechtlichen Vorschriften über Notwehr und Notstand (vgl. etwa explizit Art. 77 Abs. 2 BayPAG), soweit die Ausübung des Zwangs nicht von der allgemeinen polizeilichen Befugnis zur Gefahrenabwehr getragen ist. Weil Bedienstete des BfV und deren Hilfspersonen nicht als solche erkennbar auftreten (insbesondere nicht uniformiert sind) und also von potenziellen Störern nicht als Träger von zwangsweise durchsetzbarer Hoheitsgewalt identifiziert werden können, besteht ein gesteigertes Risiko, dass es zu Eskalationen und der Anwendung unmittelbaren Zwangs kommen kann. In jedem Fall dürfte es deshalb erforderlich sein, dass sich die Bediensteten und Hilfspersonen des BfV als mit Sonderrechten ausgestattete Hoheitsträger zu erkennen geben, bevor sie unmittelbaren Zwang anwenden. Das würde der verfassungsgerichtlichen Einordnung entsprechen, wonach polizeiliche Befugnisse grundsätzlich offen ausgeübt werden<sup>27</sup> und sollte in der Norm klargestellt werden.

Lösung: Überprüfung der Erforderlichkeit der Regelung und ggf. Klarstellung.

---

<sup>27</sup> BVerfGE 133, 277, 328.



## 18. Zu § 30 Abs. 1 BVerfSchG-E

Die Vorschrift übernimmt die Regelung des § 8 Abs. 2 S. 2 BVerfSchG.

Problem: Auch durch allgemeine Befugnisse zur Datenerhebung und -verarbeitung (wie etwa § 8 Abs. 1 BVerfSchG-E) wird in „Individualrechte“ eingegriffen. Die Grenzziehung zwischen Individual- und Kollektivrechten ist außerdem keineswegs eindeutig, weshalb auf sie verzichtet werden sollte. Letzten Endes ist die Norm entbehrlich.

Lösung: Streichung.

## 19. Zu § 32 BVerfSchG-E

Die Norm enthält schützende Regelungen für Berufsgeheimnisträger i.S.d. § 53 StPO.

Problem: Der § 53 StPO zugrunde liegende Regelungsgedanke verfängt im Nachrichtendienstrecht nicht, weil es dort keine Zeugnispflicht gibt. § 53 StPO knüpft an Konfliktverhältnisse zwischen der Zeugnispflicht und der beruflichen Verschwiegenheitspflicht für bestimmte Berufsgruppen an, die eine besondere Nähe zu strafrechtlich relevantem Verhalten aufweisen. Das passt auf die Informationsgewinnung durch Nachrichtendienste nicht.<sup>28</sup> Warum hier z.B. eine besondere Schutzregelung für Apotheker, Hebammen oder Zahnärzte (vgl. § 53 Abs. 1 S. 1 Nr. 3 StPO) etabliert werden müsste, erschließt sich nicht ansatzweise. Die Bezugnahme auf § 53 StPO ist das Ergebnis einer im Sicherheitsrecht verbreiteten „Copy and paste-Kultur“. Erforderlich wäre eine nachrichtendienstspezifische gesetzgeberische Abwägung, wie sie etwa § 22 BNDG-E für bestimmte Berufsgruppen vornimmt.

Lösung: Überarbeitung.

## 20. Zu § 34 BVerfSchG-E

Die Vorschrift legt fest, welche Maßnahmen der Vorabkontrolle durch den Unabhängigen Kontrollrat bedürfen.

---

<sup>28</sup> Vgl. ausf. zu diversen Kritikpunkten Löffelmann/Zöller, Nachrichtendienstrecht, 2. Aufl. 2025, Rn. A.103 f.; Löffelmann, GSZ 2019, 119 ff.



Problem: Nach verfassungsgerichtlicher Rechtsprechung bedürfen eingriffsintensive Überwachungsmaßnahmen einer präventiven Kontrolle durch eine unabhängige und neutrale Instanz.<sup>29</sup> Diese Vorgabe löst der Entwurf zwar weitgehend, aber nicht vollständig ein. Aufgrund der jeweiligen Eingriffsqualität läge auch bei inhaltsbezogenen Auskunftersuchen zu Telekommunikation und Postverkehr gem. § 13 Abs. 4 und § 14 Abs. 2 BVerfSchG-E und bei der Herausgabe einer Datenkopie gem. § 12 Abs. 3 S. 2 BVerfSchG-E eine Vorabkontrolle nahe. Außerdem kommt dieses Instrument bei den sog. Schutzmaßnahmen gem. § 59 BVerfSchG-E in Betracht. Gerade angesichts des Ausnahmecharakters solcher Maßnahmen und ihrer ggf. weitreichenden Konsequenzen, die im Rahmen einer Folgenabwägung (§ 59 Abs. 4 BVerfSchG-E) zu berücksichtigen sind, wäre eine verfahrensrechtliche Sicherung wichtig. Bedürfnissen der Reaktionsschnelligkeit könnte durch eine Regelung zu Gefahr im Verzug begegnet werden.

Lösung: Erweiterung der Vorabkontrolle.

## 21. Zu § 35 BVerfSchG-E

Die Vorschrift regelt die verfassungsrechtlich gebotene Benachrichtigung betroffener Personen bei besonders eingriffsintensiven Maßnahmen, die auch der unabhängigen Vorabkontrolle unterliegen.

Problem: Die Benachrichtigungspflicht gilt nicht bei besonders eingriffsintensiven HUMINT-Maßnahmen. Das ist mit Blick auf den Schutz von verdeckten Bediensteten und Hilfspersonen und den Methodenschutz einerseits verständlich. Andererseits dürften solche Belange kein generelles Absehen von einer Benachrichtigung rechtfertigen können. Gerade bei HUMINT-Maßnahmen und den dadurch verursachten Verletzungen zwischenmenschlichen Vertrauens kann allgemein ein großes Bedürfnis betroffener Personen an einer nachträglichen Kenntniserlangung vermutet werden. Geheimschutzbelange können dahinter zurücktreten (etwa nach dem Versterben einer Hilfsperson oder wenn diese sich selbst gegenüber der betroffenen Person erklärt hat). Die Überlegung, dass sich andernfalls keine Quellen gewinnen ließen (S. 282) dürfte jedenfalls für eigene Bedienstete nicht verfangen. Die Motive zu einer Zusammenarbeit von Hilfspersonen mit dem Verfassungsschutz können außerdem

---

<sup>29</sup> BVerfGE 112, 304, 318 f.; BVerfGE 120, 274, 331 f., 335; BVerfGE 122, 120, 143 f.; BVerfGE 125, 260, 337 f.; BVerfGE 141, 220, 284, 290, 294, 303, 306, 312; BVerfGE 154, 152, 255, 290 ff. u.ö.



vielfältig sein. In anderen Regelungskontexten erfolgt in solchen Fällen eine Benachrichtigung (vgl. etwa § 101 Abs. 4 S. 1 Nr. 9 StPO). Der generelle Ausschluss einer Benachrichtigung (und damit de facto des nachträglichen Rechtsschutzes) macht die betreffenden Maßnahmen zudem konventionsrechtlich angreifbarer.<sup>30</sup>

Lösung: Einbeziehung von HUMINT-Maßnahmen und Aufnahme einer darauf bezogenen besonderen Zurückstellungsklausel.

## 22. Zu § 37 BVerfSchG-E

Die Vorschrift im Verbund mit § 36 BVerfSchG-E schafft eine Rechtsgrundlage für die automatisierte Datenanalyse.

Problem: Die automatisierte Analyse von personenbezogenen Daten, auch unter Einbeziehung von selbstlernenden Systemen, stellt für die nachrichtendienstliche Tätigkeit eine Befähigung von herausragender Bedeutung dar.<sup>31</sup> Das BVerfG hat für das Polizeirecht die Zulässigkeit einer automatisierten Datenanalyse an anspruchsvolle Voraussetzungen geknüpft und vom Gesetzgeber eine präzise Einhegung solcher Maßnahmen, insbesondere auch nach Art und Umfang der für eine Analyse zur Verfügung stehenden Daten und den zulässigen Analysemethoden gefordert. Erforderlich sind außerdem verfahrensrechtliche Sicherungen.<sup>32</sup> Für einen Einsatz im Gefahrenvorfeld (das hier betroffen ist) hat das BVerfG einschränkende Vorgaben zur Methode der Analyse, insbesondere einen ausdrücklichen Ausschluss des Einsatzes selbstlernender Systeme gefordert.<sup>33</sup> Die aktuell für das Strafverfahrensrecht und Polizeirecht auf Bundesebene diskutierten Vorschriften sind deutlich enger gefasst als § 37 BVerfSchG-E und begegnen dennoch gewichtigen verfassungsrechtlichen Einwänden.<sup>34</sup> Erforderlich ist vor diesem Hintergrund eine Fortentwicklung der für die polizei-

---

<sup>30</sup> Der EGMR misst der Möglichkeit nachträglichen Rechtsschutzes eine wichtige Bedeutung für die Legitimationsfähigkeit von Überwachungsmaßnahmen bei, vgl. EGMR, Big Brother Watch, a.a.O., Rn. 499 ff.; EGMR, Centrum für Rättvisa, a.a.O., Rn. 354 ff. u.ö.

<sup>31</sup> Zur Bandbreite von Einsatzmöglichkeiten Hornung/Kostov, Der Einsatz von KI bei den Nachrichtendiensten: Erforderlichkeit neuer Befugnisse?, in: Dietrich/Gärditz/Schmahl/Gusy/Warg (Hrsg.), Nachrichtendienstrecht im Wandel der Technik. 6. Symposium zum Recht der Nachrichtendienste (i.E.), unter II.

<sup>32</sup> BVerfGE 165, 363, 409, 412 ff.

<sup>33</sup> BVerfGE 165, 363, 418.

<sup>34</sup> S. ausf. Löffelmann, Deutscher Bundestag, Innenausschuss, Ausschussdr. 21(4)214 B, S. 13 ff.



liche Tätigkeit entwickelten verfassungsrechtlichen Maßgaben für den nachrichtendienstlichen Bereich.

Insoweit enthält § 37 BVerfSchG-E mit der Differenzierung eines dauerhaft im „informationstechnischen Hintergrund“ ablaufenden Analyseprozesses und dem – abhängig von der Persönlichkeitsrelevanz der generierten Erkenntnisse – unterschiedlich gestuften Abruf der Analyseprodukte zwar durchaus systembildende Weichenstellungen. Die Unterscheidung der Analyse (einschließlich Speicherung) vom Abruf ihrer Ergebnisse ist allerdings schon für sich angreifbar, weil bereits die Analyse eine Datenverarbeitung darstellt, bei deren Rechtfertigung künftige Verwendungszwecke zu berücksichtigen sind.<sup>35</sup> Letzten Endes erfolgt dadurch eine Speicherung von Analyseergebnissen auf Vorrat bis zu einem etwaigen Abruf, also unabhängig von einer im Einzelfall bestehenden Beobachtungsbedürftigkeit (so ausdrücklich für die Parallelnorm im BNDG-E S. 470). Eingriffsgewicht und Eingriffsschwellen kommen dann erst – entgegen der bisherigen Linien der Verfassungsrechtsprechung – nach einer menschlichen Wahrnehmung zum Tragen.<sup>36</sup> Selbst wenn man eine solche Konstruktion als grundsätzlich rechtfertigungsfähig ansehen wollte, weil die Analyse großer Datenmengen zum Tätigkeitsprofil der Nachrichtendienste als „analytische Informationsdienstleister“ gehört, dürfte eine gesetzliche Einhegung der im Hintergrund laufenden Prozesse zur Verringerung von Datenschutzrisiken zwingend erforderlich sein.<sup>37</sup> Solche Sicherungen und Vorgaben können auch auf die untergesetzliche Ebene verlagert werden, wofür der Gesetzgeber aber die Voraussetzung schaffen muss.<sup>38</sup>

Insbesondere weist die Entwurfsbegründung zutreffend darauf hin, dass nach verfassungsgerichtlicher Rechtsprechung Vorgaben zur Verarbeitungsmethode unentbehrlich sind (S. 287 u.), wenn die Analyse nicht im Einzelfall durch einen konkreten Anlass getragen ist.<sup>39</sup> Gerade das ist hier der Fall, denn einen konkreten Anlass setzt nach § 37 Abs. 1 S. 1 BVerfSchG-E nicht die Analyse, sondern erst der Datenabruf voraus. Das liegt quer zur ständigen Verfassungsrechtsprechung, wonach bereits die Speicherung (und erst recht die Analyse)

---

<sup>35</sup> Vgl. BVerfGE 169, 332, 404 zur Notwendigkeit der Zweckbestimmung bei einer bevorratenden Speicherung.

<sup>36</sup> Vgl. zutr. Hornung/Kostov, a.a.O., unter III.3.b).

<sup>37</sup> Vgl. Hornung/Kostov, a.a.O., unter IV.2.a) cc), die im Übrigen das Normkonzept als plausibel ansehen: „Der Entwurf vergibt die Chance, durch deutlich stärker ausgeformte technikadäquate Verfahrensvorgaben eine gute Modell- und Systementwicklung normativ zu untermauern – und damit die Grundrechtsfragen zu entschärfen, die der Einsatz maschinellen Lernens zwecks Generierung konkreter personenbezogener Informationen (Musterabgleich) aufwirft.“

<sup>38</sup> BVerfGE 165, 363, 414 f.

<sup>39</sup> BVerfGE 165, 363, 407.



personenbezogener Daten einen rechtfertigungsbedürftigen Grundrechtseingriff darstellt.<sup>40</sup> Eine entsprechende Einhegung der Analyse selbst und deren Abstimmung auf entsprechende Instrumente anderer Sicherheitsbehörden ist zudem geboten, weil sonst ein Konflikt mit dem zentralen Prinzip der hypothetischen Datenneuerhebung<sup>41</sup> droht. Andernfalls könnten durch den Nachrichtendienst neu generierte Daten im Rahmen des allgemeinen Übermittlungsregimes an Behörden mit operativen Anschlussbefugnissen weitergegeben werden, die selbst über solche Analyseinstrumente nicht oder nur unter strengeren Voraussetzungen verfügen dürften. Die dort geltenden Analysebeschränkungen würden dann unterlaufen.

Auf der Ebene des Abrufs der Analyseprodukte besonders kritisch ist, dass nach § 37 Abs. 2 Nr. 1 Buchst. b) sogar individuelle Bedrohungsprofile und nach Buchst. c) personenbezogene Vorhersagen und Entscheidungen generiert werden können. Das entspricht der Qualität eines Predictive Policing, welches das BVerfG nur in engsten Grenzen als zulässig erachtet hat.<sup>42</sup> Gerade bei solchen personenbezogenen Analysen erscheinen Vorkehrungen zur Qualitätssicherung<sup>43</sup> und eine Abstimmung auf die Analyseinstrumente der Polizeibehörden unverzichtbar. Außerdem können nach Absatz 6 aktive Maßnahmen wie die Löschung von Daten durch eine qualifizierte Analyse automatisiert – also ohne Entscheidung eines menschlichen Akteurs – veranlasst werden. Die Vorgaben der KI-Verordnung (vgl. u.a. Art. 14 Abs. 5 UAbs. 1 KI-VO), die Maßnahmen mit nachteiligen Wirkungen ohne menschliche Überprüfung verhindern sollen, kommen hier wegen des Vorbehalts der nationalen Sicherheit zwar nicht unmittelbar zum Tragen, schlagen aber auf die verfassungsrechtliche Ebene durch. Allgemein ist bedenklich, dass ein Abruf schon zur Prüffallbearbeitung nach § 4 Abs. 4 S. 1 BVerfSchG-E und bei allen neu eingehenden Informationen spezifisch veranlasst und damit zulässig sein soll, wodurch zusätzlich die Zweckbindung und Löschungsfristen für Prüffalldaten entfallen (so explizit S. 288). Im Falle der „originären Verdachtsschöpfung“ (S. 289) nach § 37 Abs. 2 Nr. 1 Buchst. a) BVerfSchG-E ist der Abruf sogar vollständig entkoppelt von personenspezifischen tatsächlichen Anhaltspunkten nach Absatz 1 Satz 1, die durch die Analyse erst gewonnen werden sollen. Der Abruf wird damit zu einem von Eingriffsschwellen unabhängigen Standardinstrument der Fallbearbeitung, was dem selbständigen hohen Eingriffsgewicht der Analyse nicht gerecht wird.

<sup>40</sup> Vgl. insbes. BVerfGE 125, 274, 316 ff.

<sup>41</sup> BVerfGE 141, 220, 326 ff.; BVerfGE 169, 130, 180 f.

<sup>42</sup> BVerfGE 165, 363, 407 f.

<sup>43</sup> Vgl. z.B. die Vorschläge bei Teichmann, HRRS 2026, 13, 27 f. (prä-operativen Audit-Report über Trainingsdaten, Modellarchitektur und Validierungsmetriken, laufende halbjährliche Bias-Prüfungen, öffentliche Fehler- und Beschwerdestatistik).



All das begründet ein sehr hohes verfassungsrechtliches Risiko.

Lösung: Umfassende Überarbeitung.

### **23. Zu § 38 i.V.m. § 36 Abs. 3 BVerfSchG-E**

Die Vorschriften regeln in ihrem Zusammenspiel den Umgang mit pseudonymisierten Daten.

Problem: Die Lösungsregelungen des § 38 BVerfSchG-E beziehen sich nicht auf pseudonymisierte Daten, für die gem. § 36 Abs. 3 BVerfSchG-E bereits die Einschränkungen für eine Speicherung personenbezogener Daten nicht gelten. Das führt dazu, dass pseudonymisierte Daten unbefristet und unabhängig von einem konkreten Bedrohungszusammenhang gespeichert werden können. Pseudonymisierte Daten können de-pseudonymisiert werden, wovon auch der Gesetzentwurf ausgeht (§ 36 Abs. 3 S. 2 BVerfSchG-E). De facto wird dadurch eine „Vorratsdatenspeicherung“ von personenbezogenen Daten ermöglicht.

Lösung: Klarstellung in § 38 BVerfSchG-E, dass die Lösungsregeln auch für pseudonymisierte Daten gelten.

### **24. Zu § 42 BVerfSchG-E**

Die Vorschrift erlaubt die gemeinsame automatisierte Datenanalyse im Zusammenwirken mit anderen inländischen öffentlichen Stellen.

Problem: Die Ausführungen unter 22. gelten hier erst recht, denn auf diese Weise kann für die automatisierte Analyse ein in Art und Umfang unbegrenzter Datenvorrat zur Verfügung gestellt werden. Fraglich ist außerdem, ob die Regelungen zum Ausschluss operativer Anschlussmaßnahmen den verfassungsgerichtlichen Vorgaben genügen, denen zufolge es nicht darauf ankommt, ob die anderen Stellen solche Befugnisse nutzen, sondern ob sie darüber verfügen.<sup>44</sup>

Lösung: Überarbeitung im Verbund mit § 37 BVerfSchG-E.

---

<sup>44</sup> BVerfGE 169, 130, 229.



## 25. Zu § 55 BVerfSchG-E

Die Vorschrift nimmt aus allgemein zugänglichen Quellen erhobene Daten (OSINT) aus dem Anwendungsbereich des regulären Übermittlungsregimes aus.

Problem: Das BVerfG hat ausdrücklich offengelassen, ob die von ihm entwickelten Anforderungen auch für OSINT-Daten gelten.<sup>45</sup> Es hat andererseits die Erforderlichkeit strenger Übermittlungsvorschriften darauf zurückgeführt, dass Nachrichtendienste ihre Informationen mit einer Vielzahl von unterschiedlich eingriffsintensiven Aufklärungsmethoden gewinnen. Dazu zählt auch OSINT. Hinzu kommt, dass die Erhebung aus öffentlich zugänglichen Quellen den Charakter eines eigenständigen nachrichtendienstlichen Mittels haben kann (vgl. oben zu 1.).

Lösung: Klarstellung, dass die Ausnahme vom allgemeinen Übermittlungsregime nur für Daten gilt, die ausschließlich und nicht automatisiert aus öffentlich zugänglichen Quellen erhoben wurden.

## 26. Zu § 59 BVerfSchG-E

Die Vorschrift erlaubt ein verdecktes Einwirken auf Gegenstände und Güter zur Abwendung einer Gefährdung für ein besonders gewichtiges Rechtsgut.

Problem: Die Vorschrift verleiht dem BfV aktionelle Befugnisse, wie sie grundsätzlich nur der Polizei zur Verfügung stehen und berührt damit das sog. Trennungsgebot.<sup>46</sup> Dieses ist im Grundgesetz zwar nicht verfassungsunmittelbar verankert<sup>47</sup>, allerdings wirkt die multidimensionale Trennung von Nachrichtendienstbehörden und Polizeibehörden grundrechtsschonend und ist deshalb zentraler Aspekt einer Verhältnismäßigkeitsprüfung.<sup>48</sup> Für das BVerfG stellt der Umstand, dass Nachrichtendienste über keine „operativen Anschlussbefugnisse“

---

<sup>45</sup> BVerfGE 162, 1, 111; BVerfGE 163, 43, 90; vgl. dazu bereits Löffelmann, Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschussdr. 20(4)324 D, S. 11.

<sup>46</sup> Ausf. zu dessen verschiedenen Dimensionen Löffelmann/Zöller, Nachrichtendienstrecht, 2. Aufl. 2025, Rn. A.60 ff., B.4.

<sup>47</sup> Vgl. zu dieser „klassischen“ Streitfrage Deutscher Bundestag, Wissenschaftliche Dienste, WD 3-3000-089/25 m.w.N.

<sup>48</sup> Sie ist daher mehr als nur ein „rechtspolitischer Reflex“, so Arts/Jipp, GSZ 2026, 147, 148.



verfügen ein wichtiges Kriterium dafür dar, dass ihnen weitreichende Aufklärungsbefugnisse schon weit im Vorfeld einer konkretisierten Gefahr zugestanden werden können.<sup>49</sup> Bei einer Übermittlung von nachrichtendienstlichen Erkenntnissen an Behörden mit operativen Anschlussbefugnissen muss das durch hohe Übermittlungsschwellen kompensiert werden.<sup>50</sup> Diese Logik verfängt nicht mehr uneingeschränkt, wenn Nachrichtendiensten ebenfalls aktionelle Befugnisse zur Verfügung gestellt werden. Die Vorschrift besitzt deshalb einen systemverändernden Charakter. Außerdem stellt das Verwenden von durch informationelles Handeln erlangten personenbezogenen Daten für aktionelle Maßnahmen eine Zweckänderung dar<sup>51</sup>, die der Rechtfertigung bedarf. Das verfassungsrechtliche Prinzip der hypothetischen Datenneuerhebung lässt sich auf diese Konstellation nicht unmittelbar anwenden, weil es hier um einen aktionellen und nicht informationellen Folgeeingriff geht; das verdeckte Einwirken ist kein „vergleichbares Mittel“ wie der Primäreingriff. Die zentralen Fragen lauten daher, ob und unter welchen Voraussetzungen Verfassungsschutzbehörden nach verfassungsrechtlichen Maßstäben aktionelle Befugnisse zuerkannt werden dürfen, und ob dies ggf. dazu führen muss, dass ihnen weniger informationelle Befugnisse zustehen dürfen. Hierzu gibt es noch keine spezifische verfassungsgerichtliche Rechtsprechung. Läge die Schwelle – wie in § 59 BVerfSchG-E vorgesehen – unterhalb derer einer Datenübermittlung an Behörden mit operativen Anschlussbefugnissen (konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut), stellte dies jedenfalls einen klaren Wertungswiderspruch zur bisherigen Verfassungsrechtsprechung dar.<sup>52</sup>

Fraglich ist darüber hinaus, ob solche aktionellen Maßnahmen überhaupt auf die Gesetzgebungskompetenz des Art. 73 Abs. 1 Nr. 10 Buchst. b) und c) GG gestützt werden können. Herkömmlich werden diesem Titel nur die informationellen Befugnisse des Verfassungs-

---

<sup>49</sup> BVerfGE 133, 277, 325 ff.; BVerfGE 162, 1, 74 ff.; BVerfGE 163, 43, 86 ff.

<sup>50</sup> BVerfGE 162, 1, 106 ff.; BVerfGE 163, 43, 88 ff.; BVerfGE 169, 130, 216 ff., 226 ff.

<sup>51</sup> Zu zutr. Witte, Kausaloperationen des Bundesnachrichtendienstes im Entwurf zur Reform des Nachrichtendienstrechts, 2026, S. 44 f. zum BNDG-E, der insoweit eine Regelungslücke identifiziert; abrufbar unter: <https://zenodo.org/records/23015252>.

<sup>52</sup> Damit soll nicht gesagt sein, dass die Schwelle für eine Weiterverarbeitung der Daten für aktionelle Maßnahmen die reguläre Eingriffsschwelle für polizeiliches Handeln sein muss [so aber wohl Arts, NVwZ 2026, 455, 460: „Konsequenterweise könnte eine (einheitliche) Behörde unter (nachrichtendienstlichen) Schwellen personenbezogene Daten erheben und sodann unter (polizeilichen) Schwellen verwenden.“; ähnl. Deutscher Bundestag, Wissenschaftliche Dienste, WD 3-3000-089/25, S. 13 f. unter Bezugnahme auf Bäcker]. Nach der Logik der Verfassungsrechtsprechung müssten die Schwellen vielleicht auch höher liegen, gerade weil die Nachrichtendienste über Aufklärungsmittel verfügen, die Polizeibehörden nach verfassungsrechtlichen Maßstäben nicht zur Verfügung gestellt werden dürfen.



schutzes zugeordnet.<sup>53</sup> Hierfür spricht auch, dass als ergänzende Kompetenzgrundlage für das BfV Art. 87 Abs. 1 S. 2 GG herangezogen wird („Sammlung von Unterlagen“).

Erachtet man es als grundsätzlich zulässig, Verfassungsschutzbehörden aktionelle Befugnisse einzuräumen, müssen diese entsprechend den Anforderungen des verfassungsrechtlichen Grundsatzes der Bestimmtheit und Normenklarheit ausreichend präzise geregelt sein, wobei umso höhere Anforderungen an die gesetzlichen Vorgaben zu stellen sind, je eingriffsintensiver die Maßnahmen sind. Hier ist problematisch, dass Voraussetzungen und Umfang der Schutzmaßnahmen nach § 59 BVerfSchG-E unklar sind. Absatz 1 knüpft ihre Zulässigkeit an den Begriff der „Gefährdung“. Damit wird erkennbar vom klassischen polizeirechtlichen Gefahrbegriff abgewichen, ohne dass deutlich würde, was eine Gefährdung kennzeichnet und wie sie sich von einer Bedrohung (§ 3 Abs. 4 BVerfSchG-E) unterscheidet. Absatz 2 erlaubt das verdeckte Einwirken auf Gegenstände und Güter und stellt klar, dass eine Einwirkung nicht durch unmittelbaren Zwang gegen Personen erfolgen darf (Satz 2). Nicht ausgeschlossen ist damit das mittelbare Einwirken auf Personen. So ist z.B. zwanglos denkbar, dass durch das Einwirken auf IT-Systeme oder Versorgungseinrichtungen mittelbar Personen betroffen sein können, bis hin zu letalen Auswirkungen großen Umfangs.

All das begründet ein hohes verfassungsrechtliches Risiko.

Bei alledem ist die Schaffung von Befugnissen des BfV zu aktionellen Maßnahmen in spezifischen Gefahrensituationen unter dem Blickwinkel einer effektiven Sicherheitsgewährleistung durchaus diskutabel. Es stellt sich dabei aber auch die umgekehrte Frage, warum solche polizeilichen Befugnisse nur auf besondere Bedrohungen im Sinne des Absatzes 3 beschränkt sein sollen. Denn auch im Falle weniger gewichtiger Bedrohungen können Situationen eintreten, die zur Abwendung eines großen Personen- oder Sachschadens ein umgehendes Einwirken erfordern können. Anstelle des unscharfen Begriffs der Gefährdung könnte vor diesem Hintergrund alternativ an den etablierten und engen Begriff der gegenwärtigen Gefahr für ein besonders gewichtiges Rechtsgut angeknüpft werden (vgl. in diese Richtung § 31 Abs. 6 BNDG-E). Hier besteht ersichtlich noch Diskussionsbedarf.

Lösung: Vertiefende Erörterung.

---

<sup>53</sup> Ähnl. Arts/Jipp, GSZ 2026, 147, 148 Fn. 24; vgl. auch Timu, VerfBlog v. 27.8.2026, der zutr. darauf hinweist, dass Art. 73 Abs. 1 Nr. 9a GG die Abwehr terroristischer Gefahren ausdrücklich dem BKA zuweist, abrufbar unter: <https://verfassungsblog.de/nachrichtendienste-reform-operativ-bka/>.



## 27. Zu § 65 BVerfSchG-E

Die Vorschrift erweitert den bisherigen § 26b Abs. 7 BVerfSchG dahin, dass auch Drohnen abgewehrt werden dürfen, die sich Bediensteten und Hilfspersonen auf 100 Metern annähern. Außerdem dürfen künftig konventionelle Schusswaffen zur Drohnenabwehr eingesetzt werden.

Problem: Anders als in der Variante des Eindringens in einen geschützten Luftraum, bei der das Eindringen selbst eine Rechtsgutsverletzung begründet, fehlt es bei der Annäherung an eine Person an einer Gefahr. Das Annähern mit Drohnen an Personen ist weder einfachgesetzlich verboten noch begründet es per se eine Gefahr. Demnach wäre eine Attribution der Drohne als „gefährlich“ erforderlich. Betroffene Personen können zudem nicht erkennen, ob sie sich mit ihrer Drohne einem Bediensteten oder einer Hilfsperson des BfV annähern, da solche Personen regelmäßig verdeckt operieren. Mit dem Gebot der Normenklarheit ist das nicht zu vereinbaren.

Lösung: Streichung der auf Bedienstete und Hilfspersonen bezogenen Variante.

## 28. Zu § 75 BVerfSchG-E

Die Vorschrift sieht Modifikationen für bestimmte Befugnisse des BfV im Spannungs- und Verteidigungsfall vor und etabliert erweiterte Unterstützungspflichten für Unternehmen.

Problem: Art. 10 Abs. 2 S. 2, Art. 11 Abs. 2, Art. 12a Abs. 3 bis 6, Art. 17a Abs. 2 und Art. 115c Abs. 2 GG sehen für den Verteidigungsfall Modifikationen der Schutzwirkung von bestimmten Grundrechten vor. Aus dieser Entscheidung des verfassungsgebenden Gesetzgebers lässt sich entnehmen, dass eine Verengung des Schutzbereichs außerhalb dieser Normen nicht möglich ist.<sup>54</sup> Eine Berücksichtigung des Spannungs- und Verteidigungsfalls als Abwägungskriterium auf der Ebene der Rechtfertigung schließt das nicht aus. Verfassungsgerichtliche Rechtsprechung existiert insoweit allerdings nicht, woraus ein gewisses verfassungsrechtliches Risiko resultiert. Das betrifft konkret § 75 Abs. 3 Nr. 2 BVerfSchG-E, der im Verteidigungsfall den Polizeivorbehalt bei der Online-Durchsuchung und der Wohnraum-

---

<sup>54</sup> Vgl. Epping in: Dürig/Herzog/Scholz, GG, Stand: 107. EL März 2025, Art. 115c Rn. 22 f.



überwachung suspendiert. Insbesondere bei der Wohnraumüberwachung wird die Subsidiarität gegenüber polizeilichen Maßnahmen unmittelbar aus Art. 13 Abs. 4 GG („Abwehr“) hergeleitet. Problematisch erscheint auch § 75 Abs. 4 BVerfSchG-E, der unter anderem festlegt, dass im Spannungs- und Verteidigungsfall eine Benachrichtigung betroffener Personen nicht erfolgt bzw. zurückgestellt wird. Das berührt das Recht auf effektiven Rechtsschutz (Art. 19 Abs. 4 GG), das nach herrschender Meinung notstandsfest ist.<sup>55</sup> Der Vergleich mit Art. 10 Abs. 2 S. 2 GG und der dazu ergangenen Verfassungsrechtsprechung<sup>56</sup> zeigt, dass der Rechtsschutz auch im Notstandsfall nicht vollständig abgedungen werden kann. Aus demselben Grund problematisch erscheint das vollständige Entfallen der Vorabkontrolle im Spannungs- und Verteidigungsfall durch eine Entscheidung der Bundesregierung mit Zustimmung des PKGr gem. § 75 Abs. 8 S. 2 BVerfSchG-E. Gerade die Erweiterung materieller Befugnisse im Spannungs- und Verteidigungsfall erfordert prozedurale Sicherungen. Die von den Entwurfsverfassern geltend gemachten Gründe der Ressourcenschonung überzeugen insoweit nicht, denn die Mitglieder und Mitarbeitenden des Unabhängigen Kontrollrats werden kaum operative nachrichtendienstliche Tätigkeiten ausüben. Sinnvoll wäre es hingegen zweifellos, die behördeninternen Antrags- und Verwaltungsverfahren bei den Nachrichtendiensten selbst ressourcenschonender auszugestalten. Diese aufwändigen Verfahren sind ganz überwiegend nicht gesetzlich vorgegeben, sondern beruhen auf internen Weisungen und Dienstvorschriften.

Lösung: Verzicht auf eine Einschränkung der Vorabkontrolle; bloße Zurückstellung von Benachrichtigungen.

## **II. Zu Artikel 2 – BNDG-E**

### **1. Zu § 2 Abs. 1 S. 4 BNG-E**

Die Norm ist missverständlich, denn Bedrohungen können im Umkehrschluss auch als nur einfache Bedrohungen zu qualifizieren sein. Satz 4 ist entbehrlich und könnte gestrichen werden.

---

<sup>55</sup> Vgl. Epping in: Dürig/Herzog/Scholz, GG, Stand: 107. EL März 2025, Art. 115c Rn. 24.

<sup>56</sup> BVerfGE 30, 1.



## **2. Zu § 5 Abs. 2 BNDG-E**

Die Vorschrift regelt das Erheben von personenbezogenen Daten zum Zweck ihrer systematischen Zusammenführung.

Problem: Die Entwurfsbegründung geht offenbar davon aus, dass damit auch eine Rechtsgrundlage für Formen der automatisierten Datenerhebung geschaffen werde (S. 360 f.). Das kommt im Wortlaut nicht zum Ausdruck und hiergegen spricht auch eine systematische Auslegung mit Blick auf § 8 Abs. 1 S. 2 BVerfSchG-E und § 4 Abs. 3 MADG. Eine automatisierte Datenerhebung aus öffentlich zugänglichen Quellen stellt ein Instrument der Massendatenverarbeitung dar, das höhere Schwellen erfordert. Auf die Ausführungen unter I.1. wird Bezug genommen.

Lösung: Selbständige Regelung der automatisierten Datenerhebung.

## **3. Zu § 5 Abs. 3 BNDG-E**

Die Vorschrift erlaubt den Abgleich mit öffentlich zugänglichen biometrischen Daten, auch in Drittstaaten.

Problem: Der Abgleich biometrischer Daten stellt einen schweren Grundrechtseingriff dar. Durch die Datenübermittlung in einen Drittstaat erhöht sich die belastende Wirkung beträchtlich. Auf die Ausführungen unter I.1. und 2. wird Bezug genommen. Die Vorschrift sieht hierfür keine angemessenen Schwellen vor.

Lösung: Ausgestaltung des biometrischen Abgleichs als eigenständiges nachrichtendienstliches Mittel; Streichung der Datenverarbeitung in einem Drittstaat.

## **4. Zu § 6 Abs. 1 S. 2 BNDG-E**

Die Norm übernimmt die Regelung des § 8 Abs. 2 S. 2 BVerfSchG, auf die § 5 S. 2 BNDG verweist. Sie ist widersprüchlich, entbehrlich und sollte gestrichen werden. Auf die Ausführungen unter I.18. wird Bezug genommen.



## 5. Zu § 6 Abs. 3 BNDG-E

Die Norm sieht für Maßnahmen, die sich gegen Hoheitsträger fremder Staaten richten, einen Verzicht auf qualifizierte Schwellen vor, wenn die betroffene Person sich im Bundesgebiet aufhält oder die deutsche Staatsangehörigkeit besitzt.

Problem: Hoheitsträger anderer Staaten sind, wenn sie ausschließlich in dieser Funktion betroffen sind, keine Grundrechtsträger.<sup>57</sup> Eingriffsbefugnisse sind folglich nicht erforderlich. Das sollte im Kontext der Norm klargestellt werden. Der Regelungsgehalt beträfe dann nur solche Konstellationen, in denen auch eine persönliche Betroffenheit vorliegt oder nicht mit hinreichender Sicherheit auszuschließen ist, bzw. Privatpersonen im Auftrag eines fremden Staates tätig werden.

Lösung: Klarstellung.

## 6. Zu § 7 Abs. 1 und § 9 Abs. 1 S. 1 BNDG-E

Die Normen bilden die Rechtsgrundlage für Übermittlungersuchen des BND im Sinne des „Doppeltürmodells“.

Problem: Die Normen dürften zugleich die Rechtsgrundlage für den kommerziellen Erwerb von personenbezogenen Daten durch den BND darstellen<sup>58</sup>, lassen dies aber nicht erkennen. Deutlich wird außerdem nicht, dass die ersuchten Stellen nicht zur Übermittlung verpflichtet sind, soweit dies nicht anderweitig (§§ 11 ff. BNDG-E) geregelt ist. Vor diesem Hintergrund sollte § 9 Abs. 1 S. 1 BNDG-E von „Auskunft“ und nicht „Auskunftspflicht“ sprechen.

Lösung: Klarstellung.

## 7. Zu § 7 Abs. 2 und § 10 Abs. 1 BNDG-E

Die Vorschriften sollen eine Übermittlungsbefugnis für die Auskunft erteilenden Stellen begründen.

---

<sup>57</sup> BVerfG, 2 BvR 483/17 v. 8.3.2017, juris, Rn. 3.

<sup>58</sup> Vgl. zu sog. ADINT-Daten S. 501 zu § 88 Abs. 2 BNDG-E und zuvor bereits BT-Drs. 20/8627, S. 43 zu § 41 MADG; Vines/Roesner/Kohn, WPES 2017; <https://netzpolitik.org/tag/adint/>.



Problem: Soweit es sich bei dem Recht der Auskunft erteilenden Stellen um Landesrecht handelt, fehlt dem Bund die Gesetzgebungskompetenz hierfür. Das BVerfG hat ausdrücklich darauf hingewiesen, dass das Zusammenführen von Abruf- und Übermittlungsbefugnis in einer Norm nur zulässig ist, wenn der betreffende Gesetzgeber die Kompetenz zur Regelung beider Bereiche besitzt.<sup>59</sup>

Lösung: Überprüfung.

### **8. Zu § 9 Abs. 1 S. 2, Abs. 2 BNDG-E**

Die Vorschriften begründen eine Speicherpflicht für die zur Auskunft verpflichteten Stellen.

Problem: Absatz 1 Satz 2 ist zunächst insoweit missverständlich, als dem Wortlaut und der systematischen Stellung nach auch für Auskunftersuchen nach § 7 Abs. 1 BNDG-E, bei denen keine Auskunftsverpflichtung besteht, eine Speicherpflicht angeordnet werden kann. Das wäre widersprüchlich. Eine Speicherverpflichtung stellt außerdem im Zusammenhang mit Auskunftspflichten ein Novum im Nachrichtendienstrecht dar. Auf diese Weise können nicht nur Daten erhoben werden, die die verpflichtete Stelle aus eigenem Interesse speichert, und erfolgt die Erhebung nicht nur retrograd, sondern auch in die Zukunft gerichtet für bis zu zwölf Monate. Das erhöht die Eingriffsintensität für die betroffenen Auskunftsstellen und für die betroffenen Zielpersonen beträchtlich, weshalb höhere Eingriffsschwellen und verfahrensrechtliche Sicherungen erforderlich sind. Auf die Ausführungen unter I.5. wird Bezug genommen. Dass nur solche Daten betroffen sind, die „von dem Anbieter vernünftigerweise gespeichert werden würden“ (S. 367) ergibt sich aus der Norm nicht.

Lösung: Streichung der Speicherpflicht oder selbständige Regelung.

### **9. Zu § 10 Abs. 2 S. 3 BNDG-E**

Die Vorschrift ermöglicht „in geeigneten“ Fällen den automatisierten Abruf von Daten bei den übermittelnden Stellen.

---

<sup>59</sup> BVerfGE 130, 151, 203.



Problem: Formen der automatisierten Datenübermittlung sind wegen der fehlenden Einzelfallprüfung besonders risikoanfällig. Erforderlich sind deshalb organisatorisch-technische Vorkehrungen für automatisierte Abrufverfahren, wie sie in Absatz 3 nur für das BAMF vorgesehen sind. Auf die Ausführungen unter I.3. wird Bezug genommen.

Lösung: Etablierung jeweils selbständiger automatisierter Abrufverfahren.

## **10. Zu § 11 Abs. 4 und § 15 BNDG-E**

Die Vorschriften erlauben dem BND die Mitbenutzung öffentlicher und privater Einrichtungen zur Videoüberwachung.

Problem: Durch die Mitbenutzung solcher Einrichtungen dürfte der BND „Verantwortlicher“ i.S.d. § 4 Abs. 2 BDSG werden und unterliegt dann einer Publikationspflicht. Die Eingriffsintensität solcher Maßnahmen erhöht sich durch die behördliche Mitbenutzung beträchtlich, weshalb höhere Eingriffsschwellen geboten sind. Auf die Ausführungen unter I.6. wird Bezug genommen.

Lösung: Verzicht auf die Befugnis zur Mitbenutzung.

## **11. Zu § 13 BNDG-E**

Die Vorschrift regelt qualifizierte Auskunftersuchen gegenüber nicht öffentlichen Stellen.

Problem: Die unterschiedlichen Zielrichtungen der Auskunftersuchen zu Verkehrs-, Nutzungs-, Inhaltsdaten und anderen Daten lassen sich nur mit großer Mühe erschließen. § 13 Abs. 1 BNDG-E erfasst alle Auskunftersuchen, die sich nicht auf Bestandsdaten oder reine Sachinformationen beziehen. Darunter fallen also Verkehrs-, Nutzungs- und Inhaltsdaten, ggf. auch andere Datenarten, wie bei Auskunftersuchen gem. § 12 Abs. 2 Nr. 2 BNDG-E etwa Telemetriedaten (vgl. § 11 Abs. 1 Nr. 2 BVerfSchG-E). Diese Gleichsetzung ist nicht tragfähig, auch wenn sie regelungstechnisch aus Gründen der Vereinfachung wünschenswert sein mag. Es ist letzten Endes nicht erkennbar, welche Daten beauskunftet werden müssen. Auch sind unterschiedliche Schwellen geboten. So sollte sich die Beauskunftung von Telekommunikations-Inhaltsdaten an § 35 BNDG-E orientieren. Nutzungsdaten von Digi-



talen Diensten kommen solchen Inhaltsdaten jedenfalls nahe. Hinsichtlich Kfz-Telemetriedaten wird auf die Ausführungen unter I.4. Bezug genommen. Die Mitwirkungspflichten nach § 13 Abs. 4 und 5 BNDG-E wären als vorbereitende Maßnahmen im Regelungskontext der „Hauptmaßnahmen“ besser verortet.

Lösung: Überarbeitung der Regelung unter Bezugnahme auf die zu übermittelnden Datenarten.

## 12. Zu § 19 Abs. 1 BNDG-E

Die Vorschrift erlaubt die Erprobung gesetzlich unbenannter eingriffsintensiver nachrichtendienstlicher Mittel für bis zu vier Jahre.

Problem: Die Zulassung eingriffsintensiver nachrichtendienstlicher Mittel stellt eine originäre gesetzgeberische Aufgabe dar, die nicht der Exekutive überantwortet werden kann. Auf die Ausführungen unter I.8. wird Bezug genommen. Erschwerend kommt hier hinzu, dass die unbenannten Mittel noch nicht einmal in der Dienstvorschrift nach § 95 Abs. 1 BNDG-E enthalten sein müssen.

Das Bedürfnis nach einer flexiblen und zugleich rechtssicheren Lösung für den Einsatz neuer Technologien ist dabei gerade im Tätigkeitsbereich des BND, der in „Konkurrenz“ mit den Geheimdiensten anderer, nicht rechtsstaatlich verfasster Staaten steht, nachvollziehbar. Zugleich wirkt hier – anders als für das BfV – zugunsten einer solchen Lösung die im Ausland abgesenkte Schutzwirkung der Grundrechte bei einem Handeln gegenüber Ausländern<sup>60</sup> und das Fehlen einer Konflikts mit dem Tätigkeitsbereich der Gefahrenabwehrbehörden. Dennoch darf das Schaffen neuer Befugnisse – auch zur Erprobung – nicht einfach in die Hand der Exekutive gelegt werden. Das würde nicht nur Grundsätze der Gewaltenteilung in Frage stellen, sondern hätte auch eine präjudizielle Wirkung für andere Bereiche des Sicherheitsrechts, in denen seit jeher Forderungen nach flexiblen Befugnissen bestehen, die das Durchlaufen eines aufwändigen parlamentarischen Entscheidungsprozesses entbehrlich machen sollen.

---

<sup>60</sup> BVerfGE 154, 152, 224.



Einen gangbaren Weg könnte hier das Etablieren eines originären parlamentarischen Entscheidungsvorbehalts unter Beteiligung des Parlamentarischen Kontrollgremiums darstellen. Bei diesem Verfahren könnte die Bundesregierung einen Antrag auf Erprobung eines neuen nachrichtendienstlichen Mittels stellen. Dieser Antrag bedürfte der Zustimmung des Unabhängigen Kontrollrats, wodurch eine sorgfältige und unabhängige Prüfung der Gleichwertigkeit der neuen Maßnahme mit bereits bestehenden Befugnissen gewährleistet wäre. Dieser Schritt würde zugleich zu einem gewissen Grad das Fehlen eines parlamentarischen Anhörungsprozesses kompensieren. Die Letztentscheidung über den Einsatz des neuen Mittels würde beim Parlamentarischen Kontrollgremium liegen und damit im parlamentarischen Raum verbleiben. Zugleich könnte hierdurch erreicht werden, dass dieses Verfahren nicht zum Vorbild für das Schaffen neuer Befugnisse in anderen Bereichen des Sicherheitsrechts genommen wird. Flankierend würde es sich anbieten, diese neue Funktion des Parlamentarischen Kontrollgremiums im PKGrG zu verankern

Lösung: Parlamentarischer Entscheidungsvorbehalt.

### **13. Zu § 27 Abs. 3 und § 97 Abs. 1 Nr. 8 BNDG-E**

Die Vorschriften bilden die Rechtsgrundlage für die Überwachung des gesprochenen Worts sowie für Bild- und Videoaufzeichnungen außerhalb von Wohnungen.

Problem: Solche Maßnahmen entsprechen in ihrer Eingriffsintensität einer Telekommunikationsüberwachung (vgl. auch § 9 Abs. 3 BVerfSchG)<sup>61</sup> und bedürfen deshalb entsprechender Eingriffsschwellen und verfahrensrechtlicher Sicherungen. Insbesondere wäre hier auch eine Anordnung durch den Unabhängigen Kontrollrat angezeigt, also eine Erweiterung von § 97 Abs. 1 Nr. 8 um Maßnahmen nach § 27 Abs. 3 BNDG-E. Zumindest muss dies für Maßnahmen mit nochmals erhöhter Eingriffsintensität nach Satz 2 dieser Vorschrift gelten.

Lösung: Anpassung der Schwellen und Vorabkontrolle.

---

<sup>61</sup> Vgl. BVerfGE 141, 220, 287; BT-Drs. 12/989, S. 39.



#### 14. Zu § 29 BNDG-E

Die Vorschrift ist die Rechtsgrundlage für die Wohnraumüberwachung.

Problem: Die in Absatz 2 statuierten Voraussetzungen für eine Wohnraumüberwachung im Inland oder gegen deutsche Staatsangehörige setzen die Vorgaben des Art. 13 Abs. 4 GG um. Diese verfassungsunmittelbaren Maßgaben gelten grundsätzlich auch und unabhängig von Verhältnismäßigkeitserwägungen, deren Varianz das BVerfG betont<sup>62</sup>, bei einem Handeln im Ausland. Der Verzicht darauf – auch wenn er sinnvoll erscheinen mag (S. 415) – begründet deshalb ein hohes verfassungsrechtliches Risiko.

Lösung: Verzicht auf die Binnendifferenzierung.

#### 15. Zu § 30 Nr. 3, 4 und 7 BNDG-E

Die Vorschriften definieren den Begriff der „Kommunikation“.

Problem: Die Normen folgen einem engen Begriff von (Tele-)Kommunikation, der nur den Austausch zwischen zwei und mehr Teilnehmern erfasst. Nicht unter den Begriff fallen danach einseitige Kommunikationen wie Anrufversuche, Mensch-zu-Maschine-Kommunikation (so S. 431) oder das „Surfen“ im Internet. Diese Art von Kommunikation unterfällt gleichwohl Art. 10 GG<sup>63</sup>, wovon auch der Gesetzentwurf ausgeht (S. 425). Nach bislang geltendem Recht wurde nur zwischen einem Informationsaustausch „ohne unmittelbaren Bezug zu einem konkreten menschlichen Kommunikationsvorgang“ (§ 26 Abs. 3 S. 1 Nr. 1 BNDG) und anderen (von Art. 10 GG geschützten) Kommunikationsvorgängen unterschieden. Die genannten Formen „einseitiger“ Kommunikation unterfielen demnach dem Regelungsregime der §§ 19 ff. BNDG. Das wirkte sich insbesondere auf die verfassungsgerichtliche Vorgabe aus, dass „reine Inlandskommunikation“ (Ziffer 7) und Kommunikation mit „qualifiziertem Inlandsbezug“ (Ziffer 6) bei der Ausland-Ausland-Fernmeldeaufklärung herausgefiltert werden musste (nun § 32 Abs. 3 BNDG-E). Aufgrund des engeren Kommunikationsbegriffs soll das künftig nicht mehr für „einseitige“ Kommunikation gelten. Ruft also z.B. ein deutscher Staatsangehöriger vom Inland aus eine Webseite im Internet auf, kann das mit Mitteln der strategi-

---

<sup>62</sup> BVerfGE 154, 152, 224.

<sup>63</sup> BVerfG NJW 2002, 3619, 3620 f.; BVerfG NJOZ 2011, 1492, 1493; BVerfG NJW 2016, 3508, 3509; BVerfGE 172, 46, 83 f.; ausf. zum „Surfen“ Heinrich, ZIS 2020, 421 ff.



schen Aufklärung uneingeschränkt erfasst und können die erlangten Informationen weiterverarbeitet werden. Das stellt eine beträchtliche Ausweitung der Möglichkeiten der strategischen Fernmeldeaufklärung dar. Die dogmatische Herleitung dieser Ausweitung ist – ungeachtet von Verhältnismäßigkeitserwägungen – angreifbar. Ihr liegt ein in der jüngeren verfassungsgerichtlichen Rechtsprechung in einem obiter dictum angedeutetes erweitertes Verständnis zum Schutzbereich von Art. 10 GG zugrunde.<sup>64</sup> Anliegen des Gerichts ist erkennbar eine möglichst breite Anwendung des durch Art. 10 GG vermittelten Schutzes. Der Entwurf nutzt diese Ausweitung auf der Schutzbereichsebene, um auf der Rechtfertigungsebene eine Binnendifferenzierung zwischen verschiedenen schutzwürdigen Kommunikationen zu etablieren (Maschine-zu-Maschine-Kommunikation, Mensch-zu-Maschine-Kommunikation, Mensch-zu-Mensch-Kommunikation), was im Ergebnis jedoch zu einem Absenken des Schutzniveaus führt. Darin liegt ein verfassungsrechtliches Risiko.

Lösung: Zuordnung von Mensch-zu-Maschine-Kommunikation zur Mensch-zu-Mensch-Kommunikation.

## **16. Zu § 32 Abs. 3 S. 5 Nr. 3 und § 33 Abs. 2 Nr. 3 BNDG-E**

Die Vorschriften erlauben das Erheben von bzw. die Einsichtnahme in Daten durch strategische Aufklärungsmaßnahmen zum Zweck der Gefahrenabwehr.

Problem: Die Vorschrift geht über das geltende Recht (§ 19 Abs. 7 S. 6, § 26 Abs. 4 S. 3 und 4 BNDG) hinaus, indem sie von vornherein ein Erheben von reiner Inlandskommunikation zum Zweck der Gefahrenabwehr zulässt. Im geltenden Recht werden unter ähnlichen Voraussetzungen lediglich die Löschungspflichten suspendiert. Hieraus entsteht ein Konflikt mit der Aussage des BVerfG, dass eine so eingriffsintensive Befugnis wie die zur strategischen Fernmeldeaufklärung Behörden mit operativen Anschlussbefugnissen nicht eingeräumt werden dürfe.<sup>65</sup> Denn die Maßnahme erfolgt hier zwar durch den BND, aber mit einem breiten Anwendungsspektrum von vornherein zur Gefahrenabwehr und mit dem Ziel und der Möglichkeit der Datenübermittlung an Gefahrenabwehrbehörden (§ 82 BNDG-E) oder der Gefahrenabwehr durch den BND selbst (§ 31 Abs. 6, § 51 BNDG-E). Die Befugnis bezieht sich

---

<sup>64</sup> BVerfGE 172, 46, 83 f.

<sup>65</sup> BVerfGE 154, 152, 242, 244 f., 249 f.; ähnl. für den Verfassungsschutz BVerfGE 162, 1, 106 ff.; BVerfGE 163, 43, 92, 94, 95.



folglich nicht mehr nur auf Beifang. Der limitierende Begriff der „erheblichen Gefahr“ wird zudem im Polizeirecht dahin verstanden, dass das gefährdete Rechtsgut von gesteigerter Bedeutung sein muss<sup>66</sup>, womit ihm gegenüber dem Kanon der besonders gewichtigen Rechtsgüter keine eigenständige Bedeutung zukommt. Dennoch erscheint die Befugnis aus einer sicherheitlichen Perspektive sinnvoll, weil das wirkmächtige Instrument der strategischen Fernmeldeaufklärung damit für Zwecke der Gefahrenabwehr zur Verfügung gestellt wird. Um das verfassungsrechtliche Risiko zu reduzieren, bietet es sich an, einen anderen qualifizierten Gefahrbegriff zu verwenden, etwa den der dringenden<sup>67</sup> oder (besser) unmittelbar bevorstehenden (gegenwärtigen) Gefahr.

Lösung: Schärfung des Gefahrgrads.

## 17. Zu § 34 BNDG-E

Die Vorschrift integriert die bisher in § 5 G 10 geregelte strategische Inland-Ausland-Fernmeldeaufklärung in das neue harmonisierte Regelungssystem.

Problem: Die Eingriffsschwellen liegen nun niedriger als die nach § 5 G 10. Zugleich bricht die Gleichbehandlung von Metadaten (Absatz 1) und Inhaltsdaten (Absatz 2) mit der neuen Binnenlogik der Regelungen, die für die Ausland-Ausland-Fernmeldeaufklärung insoweit eine Differenzierung treffen (§ 33 Abs. 1 und 2 BNDG-E). Konsequenter wäre es, die Erhebung von Inhaltsdaten nach Absatz 2 unter die Voraussetzung einer herausgehobenen Bedrohung zu stellen. Damit würde die Schwelle mit der einer inlandsbezogenen Individualüberwachung (§ 35 Abs. 2 BNDG-E) gleichgezogen. Weil im geltenden Recht die Schwelle von Maßnahmen nach § 5 G 10 gegenüber derjenigen von Maßnahmen nach § 3 G 10 etwas abgesenkt ist, vermeidet der Entwurf diese Lösung, die zu einer leichten Einschränkung bei der Inlands-Auslands-Fernmeldeaufklärung führen würde. Andererseits ist zu berücksichtigen, dass der Entwurf ohnehin einen engeren Kommunikationsbegriff zugrunde legt (vgl. oben 15.) und einer Binnendifferenzierung von Maßnahmen der inhaltsbezogenen Kommunikationsüberwachung in dem dreistufigen System der Eingriffsschwellen Grenzen gezogen sind.

Lösung: Erörterung im Kontext mit dem neuen Kommunikationsbegriff.

---

<sup>66</sup> Pewestorf in: Pewestorf/Söllner/Tölle, Polizei- und Ordnungsrecht, 3. Aufl. 2022, § 1 Rn. 31.

<sup>67</sup> Die Auslegung dieses Begriffs ist uneinheitlich und umfasst sowohl zeitliche als auch auf das Gewicht des Rechtsguts bezogene Aspekte, vgl. a.a.O. Rn. 33 m.w.N.



## 18. Zu §§ 37 und 38 BNDG-E

Die Vorschriften regeln informationstechnische Eingriffe in IT-Systeme (CNE-Maßnahmen).

Problem: Hinsichtlich der verfassungsrechtlichen Problematik bei solchen Maßnahmen wird zunächst auf die Ausführungen unter I.14. bis 16. Bezug genommen. Die hier und im BVerfSchG-E verfolgten Ansätze unterscheiden sich allerdings voneinander. § 37 BNDG-E enthält zunächst – anders als § 25 Abs. 1 S. 2 BVerfSchG-E – keine Legaldefinition eines privaten IT-Systems. Aus dem systematischen Verhältnis von Absatz 1 und Absatz 2 ergibt sich zudem, dass die Merkmale „Einblick in wesentliche Teile der Lebensgestaltung einer Person oder ein aussagekräftiges Bild der Persönlichkeit“ (Absatz 1) und „als eigenes privat genutzt“ (Absatz 2) – anders als im BVerfSchG-E – nicht deckungsgleich sind. Diese Konstruktion ist missverständlich, denn sie kann so verstanden werden, dass unter Absatz 1 auch Systeme Dritter fallen, die die betroffene Person mit einer berechtigten Vertraulichkeitserwartung mitbenutzt. Die Nutzung von Cloud-Computing soll nach der Entwurfsbegründung hingegen unter Absatz 2 fallen (S. 443 u.). Absatz 1 soll demgegenüber etwa auf „Server oder auch Netzwerkelemente einer militärischen Einrichtung eines anderen Staates, aber auch sonstige dienstliche bzw. geschäftliche informationstechnische Systeme, die Mitarbeitenden zur Nutzung im beruflichen Kontext übertragen werden“ (S. 442) abzielen. Diese Zielrichtung wird aus dem Normtext nicht deutlich, insbesondere, wie durch das Infiltrieren solcher Systeme „Einblick in wesentliche Teile der Lebensgestaltung einer Person“ gewonnen werden können. Denkbar wäre ein solcher Einblick allerdings, wenn die militärischen oder anderen Systeme in einem anderen Staat bereits entsprechende Sammlungen personenbezogener Daten enthalten (etwa staatliche Datenbanken zu Social Crediting, Datenbanken von Sicherheitsbehörden). Insoweit lässt sich durchaus vertreten, dass eine Infiltration solcher Systeme nicht an den hohen Anforderungen des IT-System-Grundrechts zu messen ist. Auf Systeme, die Dritten von Unternehmen (etwa Cloud-Providern) zur Nutzung überlassen werden, lässt sich das nicht übertragen.<sup>68</sup> Insbesondere geht es bei einer Infiltration von deren Systemen nicht um den grundrechtlichen Status der Unternehmen, sondern den der Nutzer. Vor diesem Hintergrund sollte der Wortlaut der Norm nachgeschärft werden.

---

<sup>68</sup> Vgl. BVerfGE 120, 274, 315; BVerfGE 172, 46, 86.



Im Übrigen ist darauf hinzuweisen, dass die Maßnahmen nach der Rechtsprechung des BVerfG nur zum Zweck der Abwehr von Gefahren und zu Zwecken der Strafverfolgung zulässig sind.<sup>69</sup> Ein Verzicht darauf erscheint bei einem Handeln im Ausland diskutabel, aber durchaus angreifbar. Bei einem Handeln im Inland dürfte die Einschränkung unverzichtbar sein (vgl. bereits oben I.15.).

Hinsichtlich § 38 BNDG-E wird auf die Ausführungen unter I.16. Bezug genommen, die entsprechend gelten.

Lösung: Nachschärfung.

#### **19. Zu § 41 Abs. 1 und §§ 43, 44, 45 Abs. 2 BNDG-E**

§ 41 Abs. 1 BNDG-E erlaubt das automatisierte Übermitteln von durch Maßnahmen der Technischen Aufklärung erhobenen Daten an ausländische Kooperationspartner.

Problem: Die Befugnis geht über das geltende Recht (§ 31 Abs. 3 BNDG) hinaus, weil auch eine automatisierte Datenübermittlung generell zulässig sein soll. Bislang ist eine automatisierte Übermittlung nur für selektierte Daten (§ 32 Abs. 4 BNDG) und für unselektierte Verkehrsdaten (§ 33 Abs. 1 BNDG) unter nach verfassungsgerichtlichen Vorgaben<sup>70</sup> erhöhten Schwellen und Sicherungen zulässig, die der besonderen Risikoanfälligkeit automatisierter Übermittlungen (vgl. dazu oben I.3.) Rechnung tragen sollen. Diese beiden Konstellationen werden nun – inhaltlich weitgehend unverändert – in §§ 43, 44 BNDG-E geregelt. Hinzu tritt mit § 45 Abs. 2 BNDG-E eine neue Vorschrift zur automatisierten Übermittlung von Daten der Technischen Aufklärung, die nicht aus strategischen Aufklärungsmaßnahmen stammen. Die Sicherungen der §§ 32 und 33 BNDG fehlen weitgehend bei § 41 Abs. 1 und § 45 Abs. 2 BNDG-E. Die dem zugrunde liegende Interpretation der verfassungsgerichtlichen Rechtsprechung (S. 454 o.) vermag nicht uneingeschränkt zu überzeugen, denn Gegenstand des Judikats waren nur Maßnahmen der strategischen Aufklärung. Daraus lässt sich nicht folgern, dass bei der automatisierten Übermittlung von aus anderen Maßnahmen herrührenden Daten keinerlei Sicherungen erforderlich wären. Auch das Argument, Instrumente der Massendatenerhebung seien mit Blick auf die (ungewollte) Verletzung schutzwürdige Belange be-

---

<sup>69</sup> BVerfGE 120, 274, 329 f.; BVerfGE 162, 1, 80 f., 86 f.

<sup>70</sup> BVerfGE 154, 152, 284 f.



troffener Personen risikoanfälliger als individuelle Maßnahmen (S. 454 m.) trägt nur eingeschränkt. Denn auch bei individuellen Maßnahmen entstehen unstrukturierte Datenbestände, welche Daten enthalten können, die dem Kernbereich privater Lebensgestaltung oder einer besonders schutzbedürftigen Person zuzuordnen sind (vgl. § 43 Abs. 3 Nr. 2 und 3 BNDG-E). Zugleich wird durch das Nebeneinander der vier Normen das Regelungsregime für automatisierte Übermittlungen unnötig kompliziert. Transparenter wäre es, allgemein Anforderungen für automatisierte Übermittlungen an ausländische Partner zu definieren und für wenig schutzwürdige Daten (nach der neuen Systematik solche, die nicht „Kommunikation“ betreffen, vgl. S. 453) Erleichterungen vorzusehen.

Lösung: Entweder Ausgliederung der automatisierten Übermittlung aus dem allgemeinen Kooperationsregime und Regelung eines allgemeinen automatisierten Verfahrens oder Streichung des Worts „automatisiert“ aus § 41 Abs. 1 BNDG-E und des § 45 BNDG-E.

## **20. Zu § 47 Abs. 3 BNDG-E**

Die Vorschrift legt die maximale (verlängerbare) Anordnungsdauer für Maßnahmen der strategischen Aufklärung nach Absatz 1 (nicht: „Satz 1“) fest.

Problem: Das geltende Recht (§ 23 BNDG) enthält keine expliziten Vorgaben zur Anordnungsdauer (anders § 37 Abs. 3 S. 1 BNDG zu CNE-Maßnahmen: zwölf Monate), allerdings ist die zulässige Dauer gem. § 23 Abs. 2 S. 1 Nr. 4 BNDG im Einzelfall festzulegen. Mit der Festlegung einer – sehr langen – Höchstfrist von 36 Monaten in Absatz 3 und der Bezugnahme darauf in Absatz 2 Satz 1 Nummer 3 besteht die Gefahr einer Automatisierung der Befristung entsprechend dieser Dauer zulasten einer Einzelfallprüfung.

Lösung: Reduzierung oder Streichung der Höchstdauer.

## **21. Zu §§ 49 bis 51 BNDG-E**

Die Vorschriften etablieren aktionelle („erweiterte“) Befugnisse des BND für den Fall einer spezifischen Gefährdungslage.



Problem: Zunächst wird auf die Ausführungen unter I.26. zu den Verschiebungen in der Sicherheitsarchitektur durch das Schaffen von aktionellen Befugnissen für deutsche Nachrichtendienste und das insoweit bestehende verfassungsrechtliche Risiko Bezug genommen.<sup>71</sup> Im Gegensatz zum BfV besteht für den BND insoweit allerdings eine besondere Situation<sup>72</sup>: Erstens gerät der BND bei einem Handeln im Ausland nicht in einen Konflikt mit dem Trennungsgebot, weil deutsche Sicherheitsbehörden mit operativen Anschlussbefugnissen dort keine Hoheitsbefugnisse besitzen. Und zweitens hat der deutsche Staat wegen des Fehlens solcher Befugnisse dort nur stark eingeschränkte Möglichkeiten zur Wahrnehmung seiner Interessen. Dieses Defizit kann nicht durch ein Zusammenwirken mit den Sicherheitsbehörden des anderen Staates kompensiert werden. Vor diesem Hintergrund besteht für das Schaffen von aktionellen Befugnissen für den BND bei einem Handeln im Ausland ein berechtigtes Interesse. Der Spielraum für solche Befugnisse ist dabei zugleich weiter als der für das BfV, weil bei einem Handeln gegenüber Ausländern im Ausland der durch die Grundrechte vermittelte Schutz abgesenkt sein kann.<sup>73</sup>

Dennoch müssen solche Befugnisse in rechtsstaatskonformer Weise ausgestaltet, insbesondere durch den Gesetzgeber hinreichend präzise eingehegt werden. Hier liegt bei den durch den Entwurf vorgeschlagenen Regelungen das zentrale Problem. Denn die §§ 50 und 51 BNDG-E definieren nicht, welche Befugnisse dem BND konkret zustehen sollen. Diese sollen vielmehr in einer Grundanordnung gem. § 50 BNDG-E eine „gewisse abstrakte Eingrenzung“ (S. 463) – wenngleich noch keine konkrete Benennung – erfahren. Die Befugnis nach § 51 BNDG-E soll „alle denkbaren Durchführungsformen“ umfassen (S. 464). Diese Konstruktion verlagert die Entscheidung über Art und Umfang der Maßnahmen vollständig auf die Exekutive. Es handelt sich eben nicht nur um eine „punktueller“<sup>74</sup>, „situativ eng begrenzte“<sup>75</sup>, sondern globale Einräumung aktioneller Befugnisse. Mit dem Grundgedanken parlamentarischer Legitimation von Grundrechtseingriffen ist das nicht zu vereinbaren. Zugleich ist gut nachvollziehbar, dass ein großes praktisches Bedürfnis für Interventionsmög-

---

<sup>71</sup> Vgl. auch ausf. zur Veränderung der Rechtfertigungszusammenhänge Witte, Kausaloperationen des Bundesnachrichtendienstes im Entwurf zur Reform des Nachrichtendienstrechts, 2026, S. 46 ff., abrufbar unter: <https://zenodo.org/records/23015252>.

<sup>72</sup> Näher dazu Arts/Jipp, GSZ 2026, 7, 8, 10; dies., GSZ 2026, 147, 149 Fn. 28, 150 f.; Arts, NVwZ 2026, 455, 457 f.

<sup>73</sup> BVerfGE 154, 152, 224.

<sup>74</sup> Vgl. Thiel, KriPoZ 2026, 208, 2016, der eine „punktueller Einräumung“ für ggf. zu rechtfertigen hält.

<sup>75</sup> Arts/Jipp, GSZ 2026, 147, 151 zur Abwehr von Gefahren im nachrichtendienstlichen Regelbetrieb.



lichkeiten besteht, die nicht von der vorangehenden Durchführung eines parlamentarischen Verfahrens abhängig gemacht werden können.<sup>76</sup>

Eine Lösung könnte darin bestehen, das bereits im Zusammenhang mit der Erprobung unbenannter nachrichtendienstlicher Mittel vorgeschlagene Verfahren eines parlamentarischen Entscheidungsvorbehalts (s. oben 12.) nutzbar zu machen. Die konkret benötigten erweiterten Befugnisse würden bei diesem Verfahren auf Antrag der Bundesregierung, der vom Unabhängigen Kontrollrat auf Rechtmäßigkeit (insbesondere Vorliegen einer spezifischen Gefährdungslage und Verhältnismäßigkeit) zu prüfen wäre, durch das Parlamentarische Kontrollgremium beschlossen. Auf diese Weise könnte die Letztentscheidung über erweiterte Befugnisse im parlamentarischen Raum verbleiben. Hinzu müsste eine wirksame nachträgliche Kontrolle treten.<sup>77</sup> Für Maßnahmen, die sich ausschließlich gegen hoheitliche Stellen eines anderen Staates richten (vgl. § 51 Abs. 3 S. 1 BNDG-E), ohne dass dadurch ausländische Grundrechtsträger in ihren Grundrechten verletzt werden, könnte eine Ausnahme von diesem Verfahren vorgesehen werden. In diesem Fall müssen sich die Maßnahmen nur im Rahmen der behördlichen Aufgabenzuschreibung halten und ist einer gesonderte Befugnis nicht erforderlich. In diesem Zusammenhang ist darauf hinzuweisen, dass das aktive Einwirken auch in der Aufgabenbeschreibung des § 2 Abs. 1 BNDG-E berücksichtigt werden sollte.<sup>78</sup>

Lösung: Etablierung eines parlamentarischen Entscheidungsvorbehalts, ggf. Beschränkung erweiterter Befugnisse auf ein Handeln im Ausland.

## 22. Zu § 52 Abs. 2 Nr. 1 BNDG-E

Die Vorschrift erlaubt die Weiterverarbeitung von Daten aus allgemein zugänglichen Quellen unabhängig vom Prinzip der hypothetischen Datenneuerhebung.

Problem: Auch das Erheben von Daten aus allgemein zugänglichen Quellen kann in Funktion und Belastung dem Einsatz eines eingriffsintensiven nachrichtendienstlichen Mittels

---

<sup>76</sup> Ausf. plädiert hierfür Arts, NVwZ 2026, 455 ff.

<sup>77</sup> Hierfür auch Arts/Jipp, GSZ 2026, 147, 149.

<sup>78</sup> A.A. Arts/Jipp, GSZ 2026, 147, 149, die hier die Möglichkeit einer „Annex-Aufgabe“ sehen, was angesichts des paradigmenerändernden Charakters aktioneller Befugnisse aber nicht so recht überzeugt; weniger ablehnend Arts, NVwZ 2026, 455, 461.



gleichkommen (vgl. näher oben I.1.). Für solche Konstellationen müsste Absatz 1 gelten. Außerdem soll Absatz 2 nach der Entwurfsbegründung (S. 468) auch für kommerziell erworbene Daten gelten. Dass solche Daten (etwa mittels Werbe-IDs erhobene Daten) den vom BND in allgemein zugänglichen Quellen selbst erhobenen Daten gleichgesetzt werden können, ist fraglich. Denn die Einwilligung der betroffenen Person zur Weiterverarbeitung ihrer Daten gegenüber dem jeweiligen Diensteanbieter dürfte sich in aller Regel nicht (wirksam) auf die Nutzung durch einen Nachrichtendienst erstrecken. Auch solche Formen des Datenerwerbs besitzen mithin die Eingriffsqualität eines nachrichtendienstlichen Mittels und sollten entsprechend geregelt werden.

Lösung: Regelung entsprechender Formen der Datenerhebung als nachrichtendienstliche Mittel und Herausnahme aus Absatz 2 Nummer 1.

### **23. Zu § 52 Abs. 4, § 53 Abs. 2 Nr. 1 und § 63 BNDG-E**

Die Vorschriften regeln die automatisierte Datenanalyse beim BND, nach § 63 BNDG-E im Verbund mit anderen inländischen öffentlichen Stellen.

Problem: Die Normen genügen nicht den anspruchsvollen materiellen und prozeduralen verfassungsrechtlichen Anforderungen an automatisierte Datenanalysen. Auf die Ausführungen unter I.22. wird Bezug genommen. Die Normen verzichten bewusst auf eine „normative Differenzierung zwischen den für die automatisierte Auswertung herangezogenen Datenarten, -mengen, -typen, -herkunft etc.“, weil eine Einbeziehung aller Daten zwingend erforderlich sei (S. 471). Das dürfte mit den verfassungsgerichtlichen Vorgaben zu einer präzisen gesetzlichen Einhegung hinsichtlich Art und Umfang der einzubeziehenden Daten und der zulässigen Analysemethoden nicht zu vereinbaren sein. Gerade im Falle einer normativen Differenzierung zwischen einer dauerhaft im „informationstechnischen Hintergrund“ ablaufenden Analyse und dem an Eingriffsschwellen gebundenen Datenabruf sind verfahrensrechtliche Sicherungen für den Analyseprozess erforderlich. Besonders schwer wiegt auch hier [wie bei § 37 Abs. 2 Nr. 1 Buchst. b) und c) BVerfSchG-E] die Nutzung solcher Systeme zu Analysen vergleichbar dem Predictive Policing (so ausdrücklich S. 472 u.), zur Erstellung individueller Verhaltens- und Persönlichkeitsprofile, für personenbezogene Vorhersagen und Empfehlungen und für aktionelle Maßnahmen (§ 53 Abs. 4 Nr. 2, 3 und 4, Abs. 7 S. 2 BNDG-E). Für



behördenübergreifende Datenanalysen gelten diese Überlegungen erst recht (näher oben I.24.). Hier besteht insgesamt ersichtlich noch erheblicher Diskussionsbedarf.

Lösung: Schaffung eines differenzierten Regelungsregimes für automatisierte Datenanalysen.

#### **24. Zu § 56 Abs. 2 BNDG-E**

Die Vorschrift regelt die Pflicht zur regelmäßigen Überprüfung der Erforderlichkeit der gespeicherten Daten.

Problem: Die Anhebung des Regelprüfturnus von 5 auf 15 Jahre erscheint auch vor dem Hintergrund der in der Begründung (S. 476 f.) genannten Gesichtspunkte sehr weitreichend. Diesen lässt sich entgegenhalten, dass auch die Volatilität sicherheitsbedrohender Ereignisse größer geworden ist und deshalb aus einer grundrechtsschützenden Perspektive eine Überprüfung in kürzeren Abständen erforderlich wäre. Den genannten Belangen dürfte im Regelfall durch die in Absatz 6 geregelte Ausnahme von „Produkten“ des BND von der Löschungspflicht begegnet werden können. Grundsätzlich sollte nach datenschutzrechtlichen Grundsätzen eine Löschung erfolgen, wenn ein konkreter Datenerhebungsvorgang abgeschlossen ist und die Daten für Zwecke der erhebenden Stelle und des Rechtsschutzes nicht mehr erforderlich sind. Dass dies in der Regel erst nach 15 Jahren der Fall sei, überzeugt nicht. Ferner erschließt sich nicht, warum Daten aus allgemein zugänglichen Quellen [Absatz 1 Nummer 2 Buchstabe b), Absatz 2 Nummer 1 Buchstabe a)] dem Prüfturnus nicht unterfallen sollen; auf oben I.1. wird insoweit Bezug genommen. Diese Differenzierung macht außerdem eine Kennzeichnung solcher Daten erforderlich, was mit zusätzlichem Aufwand einhergeht.

Lösung: Überprüfung.

#### **25. Zu §§ 65, 66 BNDG-E**

Die Vorschriften regeln besondere Prüf- und Löschungspflichten für Daten aus der Technischen Aufklärung.



Problem: Das differenzierte Zusammenspiel von §§ 56, 65 und 66 BNDG-E ist aus dem Gesetz heraus kaum zu erschließen, was bereits erhebliche Bedenken mit Blick auf das verfassungsrechtliche Gebot der Normenklarheit aufwirft. Im Ergebnis schafft § 66 Abs. 1 BNDG-E die Befugnis zu einer sechsmonatigen Vorratsspeicherung von Inhaltsdaten aus einer strategischen Aufklärungsmaßnahme. Bislang war das nur für Verkehrsdaten zulässig (§ 26 Abs. 5 S. 1 BNDG) und begegnete bereits bei der Schaffung des geltenden Rechts der Kritik.<sup>79</sup> Anders als nach bisherigem Recht (§ 27 Abs. 1 S. 1 BNDG) und anders als künftig bei Daten aus einer Individualüberwachung (§ 65 Abs. 2 BNDG-E) ist bei Daten aus einer strategischen Maßnahme also keine (erstmalige) unverzügliche Überprüfung erforderlich, sondern hat der BND hierfür sechs Monate Zeit. Für Verkehrsdaten gilt insoweit gemäß § 66 Abs. 4 S. 1 Nr. 1 BNDG-E nunmehr eine Frist von mindestens (Satz 2) zwölf Monaten. Für Daten aus informationstechnischen Eingriffen gilt eine Prüffrist von mindestens (Satz 2) 36 Monaten (§ 66 Abs. 4 S. 1 Nr. 2 BNDG-E). Eine Prüffrist von 15 Jahren gilt für sämtliche (auch inhaltsbezogene) nicht lesbaren oder nicht trennbaren Daten aus einer strategischen Aufklärungsmaßnahme gem. § 66 Abs. 2 BNDG-E. Im Ergebnis führt das für große Teile des Erhebungsaufkommens zu einer mindestens (vgl. Absatz 2 Satz 2) 15-jährigen Vorratsdatenspeicherung.<sup>80</sup> Das und die erweiterten Prüffristen für (lesbare) Inhalts- und Verkehrsdaten verändern das Gepräge der strategischen Aufklärung fundamental. Der Erhebung des Rohdatenstroms kommt damit eine bedeutend größere Eingriffsintensität zu als bisher angenommen. Ein lediglich niederschwelliger Eingriff für diese erste Stufe der Datenverarbeitung<sup>81</sup> oder sogar das Fehlen einer Eingriffsqualität<sup>82</sup> lässt sich dann nicht mehr vertreten, was Auswirkungen auf die verfassungsrechtliche Einordnung der Maßnahme insgesamt hat.

Lösung: Beibehaltung des bisherigen Regelungsregimes.

---

<sup>79</sup> Dietrich, Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschussdr. 19(4)731 G, S. 16 f.; Löffelmann, Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschussdr. 19(4)731 C, S. 15.

<sup>80</sup> Vgl. zu – im internationalen Vergleich durchaus nachvollziehbaren – Argumenten für eine gebotene Ausweitung der Speicherfristen Arts, NVwZ 2026, 455, 462.

<sup>81</sup> Vgl. zu der vom EGMR entwickelten Differenzierung von vier Stufen der Datenverarbeitung bei Maßnahmen der Massendatenüberwachung (1. initiales Erheben des Rohdatenstroms, 2. Anwendung von Selektoren, 3. Relevanzprüfung durch Datenanalysten, 4. Weiterverarbeitung der erlangten Daten) EGMR, Big Brother Watch u.a. ./ Vereinigtes Königreich [GK], 25. Mai 2021, Nr. 58170/13 u.a., Rn. 325.

<sup>82</sup> Näher zur entsprechenden Rechtsprechungslinie des BVerfG m.w.N. Löffelmann, JR 2024, 458, 459.



## 26. Zu § 78 BNDG-E

Die Vorschrift erlaubt „in geeigneten Fällen“ das Einrichten automatisierter Verfahren für die Datenübermittlung an inländische öffentliche Stellen. Auf die Ausführungen unter I.3. wird Bezug genommen.

## 27. Zu § 88 BNDG-E

Die Vorschrift nimmt Daten, die nicht durch nachrichtendienstliche Mittel, Auskunftersuchen oder einen Abgleich biometrischer Daten erhoben wurden, vom regulären Übermittlungsregime aus. Auf die Ausführungen unter I.25. wird Bezug genommen.

## 28. Zu § 97 BNDG-E

Die Vorschrift legt fest, welche Maßnahmen der Vorabkontrolle oder Einzelfallkontrolle durch den Unabhängigen Kontrollrat unterliegen.

Problem: Eingriffsintensive Überwachungsmaßnahmen bedürfen einer Vorabkontrolle durch eine unabhängige und neutrale Instanz zur präventiven Sicherung des Grundrechtsschutzes (vgl. bereits oben I.20.). Diese Vorgabe löst der Entwurf weitgehend, aber nicht vollständig ein. Nicht der Vorabkontrolle – obwohl die Eingriffsqualität das nahelegen würde – unterliegen die längerfristige Videoüberwachung gem. § 15 Abs. 3 BNDG-E, die optische und akustische Überwachung besonders privater Informationen gem. § 27 Abs. 3 S. 2 BNDG-E (näher oben 13.) und die Asservatenauswertung gem. § 54 Abs. 2 BNDG-E. Wertungsmäßig inkonsistent erscheint weiter, dass bei den erweiterten Befugnissen lediglich die Grundanordnung gem. § 50 BNDG-E (§ 97 Abs. 2 BNDG-E), nicht aber die einzelnen Maßnahmen einer Kontrolle unterliegen. Das ist in anderen Bereichen des Sicherheitsrechts anders, wo auch eingriffsintensive aktionelle Maßnahmen grundsätzlich einem Richtervorbehalt unterliegen (vgl. nur den Katalog in Art. 94 BayPAG). Erfordernissen der Reaktionsschnelligkeit des Handelns wird dort durch Regelungen zu Gefahr im Verzug Rechnung getragen.<sup>83</sup> Gerade angesichts der Unbestimmtheit der gesetzlichen Regelung wäre eine Vorabkontrolle solcher

---

<sup>83</sup> Vgl. näher zu alledem Löffelmann in: Möstl/Schwabenbauer (Hrsg.), Polizei- und Sicherheitsrecht Bayern, 2. Aufl. 2025, Art. 94 und 95.



Maßnahmen angezeigt. Alternativ müssten sie zumindest einer Einzelfallkontrolle i.S.d. § 97 Abs. 3 BNDG-E unterliegen.

Lösung: Erweiterung der Vorab- und Einzelfallkontrolle.

### **29. Zu § 103 BNDG-E**

Die Vorschrift etabliert erstmals einen ausdrücklichen Rechtswegausschluss auch für Maßnahmen der strategischen Aufklärung und bestimmte Auskunftersuchen. Auf die Ausführungen unter I.13. wird Bezug genommen.

### **30. Zu § 112 BNDG-E**

Die Vorschrift erweitert die Möglichkeiten zur Abwehr von Drohnen unter anderem auf den Fall einer Annäherung auf 100 Meter zu den vom BND eingesetzten Personen oder seinen Dienststellen. Auf die Ausführungen unter I.27. wird Bezug genommen.

### **31. Zu § 113 Abs. 1 BNDG-E**

Die Vorschrift etabliert eine Befugnis für die Durchführung „erforderlicher Maßnahmen“ zur Abwehr gegenwärtiger Gefahren für Bedienstete des BND und andere Personen, die für ihn tätig sind, sowie eingesetzte Sachen von bedeutendem Wert.

Problem: Zunächst wird umfassend auf die Ausführungen unter I.17. Bezug genommen. Erschwerend kommt hier hinzu, dass die Art der „erforderlichen Maßnahmen“ vollkommen unbestimmt bleibt. Mit dem verfassungsrechtlichen Bestimmtheitsgebot dürfte das nicht zu vereinbaren sein.

Lösung: Nachschärfung und Überprüfung der Erforderlichkeit der Regelung.



### 32. Zu § 125 Abs. 3 BNDG-E

Die Vorschrift etabliert den „Besonderen Feststellungsfall“ unterhalb der Schwelle eines Spannungsfalls.

Problem: Die Feststellung eines Spannungsfalls (Art. 80a GG) und eines Verteidigungsfalls (Art. 115a GG) ist von der Verfassung an die hohe Schwelle einer parlamentarischen Zweidrittelmehrheit geknüpft. Der Verteidigungsfall bedarf zusätzlich einer entsprechenden Feststellung durch den Bundesrat. Der besondere Zustimmungsfall (Art. 80a GG) bedarf in jedem Fall einer parlamentarischen Mehrheitsentscheidung. Daneben stellt der Gesetzgeber nun auf der Ebene des einfachen Rechts den Besonderen Feststellungsfall, der von der Bundesregierung mit Zustimmung des Parlamentarischen Kontrollgremiums festgestellt werden kann. Diese niedrige verfahrensrechtliche Schwelle löst sich bewusst von den verfassungsrechtlichen Vorgaben für den Spannungs- und Verteidigungsfall, erzeugt damit aber einen Wertungswiderspruch.

Die Konsequenzen eines Besonderen Feststellungsfalls sind dabei weitreichend und werden denen in einem Spannungs- und Verteidigungsfall weitgehend gleichgestellt. So gilt für den Einsatz nachrichtendienstlicher Mittel generell die niedrigste Eingriffsschwelle (§ 128 Abs. 2, § 133 Abs. 1 BNDG-E), der Schutz von Vertraulichkeitsbeziehungen wird suspendiert (§ 128 Abs. 3 Nr. 1 Alt. 2 BNDG-E), erweiterte nachrichtendienstliche Maßnahmen sind allgemein zulässig (§ 129 Abs. 2 BNDG-E). Außerdem werden Betroffene nicht mehr benachrichtigt und erhalten keine Auskunft (§ 132 Abs. 5 BNDG-E), die administrative Kontrolle durch den Unabhängigen Kontrollrat wird ausgeschaltet (§ 132 Abs. 1 BNDG-E) und es gibt keine Prüf-, Lösch- und Protokollierungspflichten (§ 130 Abs. 3, 4, § 133 Abs. 2 BNDG-E), was insgesamt die Frage aufwirft, ob die verbleibende Konstruktion den verfassungsrechtlichen Anforderungen an eine wirksame Kontrolle noch genügt.<sup>84</sup> Einige dieser Folgen begegnen schon für den Spannungs- und Verteidigungsfall verfassungsrechtlichen Bedenken (vgl. dazu oben I.28.). Erst recht gilt dies für den Besonderen Feststellungsfall. Hinzu kommt, dass § 125 Abs. 5 BNDG-E den BND ermächtigt, die zur Durchführung der für den Besonderen Feststellungsfall geltenden Regelungen erforderlichen „Vorbereitungen“ zu treffen. Diese völlig unbestimmte Generalermächtigung bedeutet im Ergebnis nochmals eine Vorverlagerung des Besonderen Feststellungsfalls. Und eine weitere Verschärfung der Problematik zeigt sich mit

---

<sup>84</sup> So auch Witte, Kausaloperationen des Bundesnachrichtendienstes im Entwurf zur Reform des Nachrichtendienstrechts, 2026, S. 54, abrufbar unter: <https://zenodo.org/records/23015252>.



Blick auf die ohnehin kritischen aktionellen Befugnisse (oben 21.). Weil im Verteidigungsfall § 51 Abs. 3 S. 2 BNDG-E suspendiert wird (§ 129 Abs. 4 BNDG-E), sind dann – sogar ohne Grundanordnung (§ 129 Abs. 3 BNDG-E) – zum Zweck der Abwendung oder Einschränkung der Bedrohungslage gezielte Maßnahmen gegen Leib und Leben – also auch gezielte Tötungen von Personen, sogar unter Einsatz von Kriegswaffen<sup>85</sup> – durch den BND zulässig. Das gilt grundsätzlich auch gegenüber deutschen Staatsangehörigen und im Inland (vgl. § 51 Abs. 2 und 3 BNDG-E). Die Schieflage zu einem entsprechenden polizeilichen Handeln („finaler Rettungsschuss“), die vor allem aus der Vagheit des Handlungszwecks resultiert („zur Abwendung oder Einschränkung der Bedrohungslage“), ist hier mit Händen zu greifen.

Verfassungsrechtsprechung zu solchen Konstellationen existiert bislang nicht, weshalb es an belastbaren Orientierungslinien fehlt. Daraus resultiert ein sehr hohes verfassungsrechtliches Risiko. Klar ist, dass jenseits der Modifikationen, die der Verteidigungsfall für den Schutzbereich bestimmter Grundrechte zulässt (Art. 10 Abs. 2 S. 2, Art. 11 Abs. 2, Art. 12a Abs. 3 bis 6, Art. 14, Art. 17a Abs. 2, Art. 104 GG), auch „tektonische Verschiebungen“ unter Verhältnismäßigkeitsaspekten zulässig sind. Dann läge es aber in der Logik solcher Verschiebungen, dass sich Abstufungen zwischen Verteidigungsfall, Spannungsfall und Besonderem Feststellungsfall ergeben müssten. Fruchtbar machen ließe sich möglicherweise auch der Gedanke von Schutzbereichsausnahmen oder -begrenzungen, mit denen das BVerfG vereinzelt (allerdings im Kontext nur mittelbarer Grundrechtsbeeinträchtigungen) argumentiert hat.<sup>86</sup> Klar dürfte auch sein, dass eine Absenkung des Grundrechtsschutzes nach Verhältnismäßigkeitsaspekten nicht zu seinem vollständigen Wegfall führen darf. Nach diesem Gedanken begegnet vor allem die Suspendierung der administrativen Kontrolle, von Auskunft- und Benachrichtigungspflichten sowie der den individuellen Rechtsschutz und die aufsichtliche Kontrolle absichernden Prüf-, Lösch- und Protokollierungspflichten erheblichen verfassungsrechtlichen Bedenken. Der Gedanke der Verhältnismäßigkeit verbietet es zudem, eine „Abwägung der jeweiligen Eingriffsintensität pauschaliert und zugunsten der öffentlichen Sicherheit“ vorzunehmen (so S. 540). Legislative Abwägungen müssen in Ansehung der konkreten Abwägungsgegenstände erfolgen und zeichnen den Rahmen für die Einzelfallanwen-

---

<sup>85</sup> Vgl. Artikel 6 des Gesetzes zur Reform des Nachrichtendienstrechts mit der Einfügung von § 15 Abs. 1a KrWaffKontrG, wonach die Einschränkungen nach §§ 2 bis 4a und 12 KrWaffKontrG auf den BND keine Anwendung finden.

<sup>86</sup> Vgl. Dietrich in: v. Kielmansegg/Terhechte/Weingärtner, Handbuch Recht der Streitkräfte, 2025, § 21 Rn. 192 ff. unter Fortentwicklung des in BVerfGE 77, 170, 221 (C-Waffen-Beschluss) angelegten Gedankens; dazu auch Salomon, a.a.O., § 4 Rn. 44; Starski, a.a.O., § 20 Rn. 255 f.; Link, Grundrechtsbindung der Bundeswehr im Ausland, 2020, S. 49.



derung vor. Ein pauschaler Vorrang von Sicherheitsinteressen ist eine Abschaffung des Verhältnismäßigkeitsprinzips. Klar dürfte schließlich auch sein, dass verfahrensrechtliche Sicherungen, wie sie die Verfassung für den Spannungs- und Verteidigungsfall vorsieht, wertungsmäßig auf der Ebene des einfachen Rechts für vergleichbare Konstellationen Berücksichtigung finden müssen. Das ist hier für den Besonderen Feststellungsfall nicht erkennbar.

Bei alledem ist durchaus nachvollziehbar, dass es für den Besonderen Feststellungsfall ein praktisches Bedürfnis geben mag. Eine größere Annäherung an die verfassungsrechtliche Einordnung des Spannungs- und Verteidigungsfalls – wenngleich keine Behebung aller skizzierten Bedenken – ließe sich erreichen, indem man die Feststellung des Besonderen Feststellungsfalls ebenfalls in den parlamentarischen Raum hinein verlagerte. Hierfür könnte sich zum Beispiel ein „parlamentarischer Entscheidungsvorbehalt“ anbieten, wie er bereits in anderem Zusammenhang vorgeschlagen wurde (oben 12., 21.). Die Feststellung des Besonderen Feststellungsfalls würde dann auf Antrag der Bundesregierung durch das Parlamentarische Kontrollgremium (ggf. mit Zweidrittel-Mehrheit) erfolgen. Eine solche Konstruktion unterscheidet sich nicht in ihrer Praktikabilität von der im Entwurf vorgesehenen Zustimmungslösung, wohl aber in ihrer Legitimationskraft und Außenwahrnehmung. Diese Entscheidung könnte außerdem befristet werden, um eine parlamentarische Auseinandersetzung und Entscheidung (wie sie in § 125 Abs. 4 Nr. 3 BNDG-E nur für den Spannungs- und Verteidigungsfall vorgezeichnet ist) herbeizuführen und einen dauerhaften Status quo in Gestalt eines Ausnahmezustands zu vermeiden. Und schließlich müsste darüber nachgedacht werden, ob es ausreicht, Betroffenenrechte und Kontrollfunktionen lediglich einzuschränken oder vorübergehend auszusetzen, statt sie vollständig zu suspendieren. Entsprechende Absenkungen des Grundrechtsschutzes müssten substantiell begründet werden. Der Entwurf lässt zum Beispiel nicht erkennen, inwiefern sich die besondere Rolle der Bundesrepublik Deutschland als Gast-, Aufmarsch- und Transitzone für Bündnispartner (S. 537) konkret auf die Notwendigkeit einer Einschränkung von Betroffenenrechten auswirkt. Die hier geltend gemachten und als alternativlos dargestellten Ressourcenerwägungen überzeugen nicht. Eine wie vorgesehen weit gefasste Befugnis des BND zum gezielten Töten von Personen dürfte sich auch für den Verteidigungsfall nur schwer verfassungsrechtlich legitimieren lassen und kollidiert sogar mit für militärisches Handeln geltenden völkerrechtlichen Grundsätzen („Unterscheidungsgebot“, „Kombattantenstatus“).

Lösung: Erörterung und Überarbeitung.



### III. Zu Artikel 3 – UKRatG-E

#### 1. Zu § 14 Abs. 2 UKRatG-E

Die Vorschrift regelt, wer Mitglied des gerichtsähnlichen Kontrollorgans des Unabhängigen Kontrollrats werden kann.

Problem: Das BVerfG hatte in seiner der Errichtung des Unabhängigen Kontrollrats zugrundeliegenden Rechtsprechung einen gerichtsähnlichen Zuschnitt des Kontrollorgans und seine „maßgebliche“ Besetzung mit Personen, die über eine langjährige richterliche Erfahrung verfügen, gefordert. Die Möglichkeit der Einbeziehung von Personen, die Erfahrung in anderen juristischen Berufen besitzen, hatte es ausdrücklich eröffnet.<sup>87</sup> Der Gesetzgeber hatte die Vorgaben dahin umgesetzt, dass er nur Bundesrichtern mit langjähriger Erfahrung in dieser Tätigkeit den Zugang zum Unabhängigen Kontrollrat eröffnet hatte (§ 43 Abs. 1 BNDG). Hiervon weicht § 14 Abs. 2 UKRatG-E nun ab und schließt in den Kandidatenkreis Bundesanwälte, Beamte einer obersten Bundesbehörde in einem Amt der Besoldungsgruppe B 6 oder höher sowie Mitglieder der G 10-Kommission des Bundes ein. Die beiden zuletzt genannten Weiterungen begegnen dabei Bedenken mit Blick auf Art. 12 GG (Berufszugangsregelung) und Art. 33 Abs. 2 GG (Prinzip der Bestenauslese). Denn es ist nicht erkennbar, warum die Tätigkeit für eine oberste Bundesbehörde oder die G 10-Kommission des Bundes ein sachlich gebotenes Differenzierungskriterium darstellt, das es erlaubte, Beamte der Länder im selben Statusamt und Mitglieder der G 10-Kommissionen der Länder von dieser Tätigkeit auszuschließen. Am Rande ist darauf hinzuweisen, dass eine Unterscheidung zwischen richterlichen und nicht-richterlichen Mitgliedern, sowie die Wahl von Präsident oder Präsidentin und Vizepräsident oder -präsidentin lediglich aus dem Kreis der richterlichen Mitglieder (§ 17 Abs. 3 UKRatG-E) nicht zu einer homogenen Behördenkultur beitragen dürfte. Verfassungsrechtlich vorgegeben ist das – wie im Übrigen auch die Festlegung auf mindestens sieben richterliche Mitglieder (Absatz 3) – nicht, sondern nur ein „maßgebliches Gewicht“ der richterlichen Perspektive bei der Entscheidungsfindung.

Lösung: Streichung von Nummer 1 Buchstabe a) Doppelbuchstabe cc) und Nummer 1 Buchstabe b) oder Erweiterung der Vorschriften auf die Länder.

---

<sup>87</sup> BVerfGE 154, 152, 295.



## **2. Zu § 17 UKRatG-E**

Die Vorschrift regelt die Wahl der Mitglieder des gerichtsähnlichen Kontrollorgans.

Problem: Der Entwurf übernimmt hier die Vorschrift des geltenden Rechts (§ 43 Abs. 4 S. 2 BNDG). Allerdings ist zu berücksichtigen, dass dem Unabhängigen Kontrollrat zukünftig eine wichtige Rolle bei der Überprüfung von Entscheidungen zukommen soll, die der Sache nach den Wirkungskreis des Parlaments berühren (Zustimmung zu unbenannten eingriffsintensiven nachrichtendienstlichen Mitteln, Grundanordnung für erweiterte Befugnisse). Vor diesem Hintergrund und angesichts der generell erweiterten Machtfülle des Unabhängigen Kontrollrats könnte (wie bei Bundesrichtern) die Wahl der Mitglieder des gerichtsähnlichen Kontrollorgans durch das Plenum angezeigt sein.

Lösung: Erörterung.

## **IV. Zu Artikel 5 – MADG-E**

### **1. Zu § 18 Abs. 1 S. 2 Nr. 2 MADG-E**

Die Vorschrift erlaubt das Überwachen von Inhalten nicht interpersoneller Telekommunikationsdienste unter abgesenkten Voraussetzungen. Auf die Ausführungen unter I.18. und II.15. wird Bezug genommen.

### **2. Zu § 18a MADG-E**

Die Vorschrift übernimmt mit leichten Modifikationen die Regelungen des § 2 G 10. Fraglich ist, warum sich der Entwurf hier nicht an die neue Systematik des BVerfSchG-E anlehnt (vgl. dort § 14 Abs. 2 S. 2).



### **3. Zu § 22 Abs. 1a, § 23 Abs. 4 S. 2 und § 46 Abs. 1 S. 2 MADG-E**

Die Vorschriften regeln die Zuständigkeit des Unabhängigen Kontrollrats für die Vorabkontrolle von Maßnahmen der Telekommunikationsüberwachung, deren administrative Kontrolle und das Zurückstellen der Benachrichtigung von Betroffenen. Hierdurch wird die Systematik des § 22 MADG (gerichtliche Anordnung) ohne erkennbaren sachlichen Grund durchbrochen.

## **C. Schlussbemerkung**

Der Gesetzentwurf bildet insgesamt eine tragfähige Grundlage für die Reform des Nachrichtendienstrechts auf Bundesebene. Er bildet den vorläufigen Schlusspunkt langjähriger hochkomplexer Reformarbeiten, die eine Vielzahl von verfassungsgerichtlichen Vorgaben zu berücksichtigen hatten. Für die Rechtssicherheit des nachrichtendienstlichen Handelns ist das Reformpaket von großer Bedeutung.

Wesentliche Gesichtspunkte, die mit der Reform in grundsätzlich gelungener Weise umgesetzt werden, sind

- die Schaffung eines integrierten, fachspezifischen BNDG unter Abkoppelung vom BVerfSchG und dadurch die Auflösung von vielfach kritisierten „Verweisungskaskaden“;
- die Auflösung des G 10 und Integration seiner Regelungsgehalte in die Fachgesetze und damit der Abbau von dysfunktionalen Doppelstrukturen<sup>88</sup>;
- die im Wesentlichen (auch im Vergleich von BVerfSchG-E und BNDG-E) schlüssige und kohärente Umsetzung des vom BVerfG eingeforderten Stufenmodells von Eingriffsgewichten und Aufklärungsbedarfen (vgl. Anlage 1);
- die Zusammenführung und Verschlinkung der Vorschriften zur strategischen Fernmeldeaufklärung des BND;

---

<sup>88</sup> Vgl. zur bislang gegebenen „defizitären Überkomplexität“ prägnant Arts, NVwZ 2026, 455, 459 f.



- die Auflösung der in der verfassungsgerichtlichen Judikatur angelegten dysfunktionalen Differenzierung zwischen politischer Unterrichtung und Gefahrenfrüherkennung durch den BND;
- die durchgängige Schaffung von Auslandsbefugnissen für den BND und damit folgerichtige Fortentwicklung der Vorgaben des BVerfG aus seiner Entscheidung vom 19.5.2020<sup>89</sup>;
- die Schaffung von Befugnissen zur wirksamen Abwehr von Cyberangriffen;
- die Neuordnung, Verschlinkung und Stärkung der Kontrollarchitektur mit dem Unabhängigen Kontrollrat als zentralem, für die Kontrolle der operativen Tätigkeit der Nachrichtendienste zuständigen Akteur in einem neuen UKRatG.<sup>90</sup>

Allerdings bedarf der Entwurf an zahlreichen Stellen noch der Nachjustierung. Außerdem geht der Entwurf an mehreren Stellen bewusst ein hohes verfassungsrechtliches Risiko ein. Hervorzuheben sind insofern

- die Regelungen zur automatisierten Datenerhebung einschließlich des Abgleichs biometrischer Daten (I.1.,2. und II.2.,3.);
- die neuen Auskunftersuchen zu Kfz-Telemetriedaten (I.4. und II.11.);
- die deutlich erweiterten und zugleich in wesentlichen Teilen zu unbestimmten Befugnisse zu informationstechnischen Eingriffen (I.14.-16. und II.18.);
- die neuen Befugnisse zur automatisierten Datenanalyse („qualifizierte Auswertung“; I.22. und II.23.);
- die Regelungen zur Erprobung gesetzlich nicht benannter eingriffsintensiver nachrichtendienstlicher Mittel (I.8. und II.12.);
- die Ausweitung der bevorratenden Speicherung von Rohdaten durch den BND (II.25.);

---

<sup>89</sup> Zu der insoweit gebotenen „pauschalisierenden“ Absenkung des Schutzniveaus zutr. Arts, NVwZ 2026, 455, 459.

<sup>90</sup> Vgl. hierzu bereits Löffelmann, VerfBlog v. 20.8.2026, <https://verfassungsblog.de/nachrichtendienstreform-kontrolle-unabhaengerigerkontrollrat/>.



- die neuen Befugnisse des BfV zu „Schutzmaßnahmen“ (I.26.);
- die neuen „erweiterten“ Befugnisse des BND in „besonderen Gefährdungslagen“ (II.21.);
- die Absenkung des grundrechtlichen Schutzniveaus im „Besonderen Feststellungsfall“ und dessen verfahrensrechtliche Voraussetzungen (II.33.).

Ob der parlamentarische Gesetzgeber bereit ist, diese Risiken einzugehen, ist letzten Endes eine politische Frage. Dabei wird zu berücksichtigen sein, dass durch zivilgesellschaftliche Initiativen mit hoher Wahrscheinlichkeit eine erneute verfassungsgerichtliche Überprüfung angestoßen wird. Soweit Befugnisse zur Massendatenverarbeitung in Rede stehen, muss, wie schon bei der „Vorratsdatenspeicherung“, mit dem Erlass einer einstweiligen Anordnung durch das BVerfG gerechnet werden.

Abschließend ist darauf hinzuweisen, dass mit dem Entwurf die Regelungsfülle und -dichte im Nachrichtendienstrecht auf Bundesebene massiv zunehmen wird (vgl. Anlage 2). Das hat nicht nur Vorteile, sondern kann das operative Handeln und die Sicherheit der Rechtsanwendung auch beeinträchtigen. Eine insgesamt schlankere Regelung mit einem höheren Abstraktionsgrad wäre möglich gewesen. Vor allem aber verändert sich mit einer Vielzahl neuer und weit reichender Aufklärungsbefugnisse der Kontext für sicherheitsbehördliches Handeln (nicht nur der Nachrichtendienste) in Deutschland. Die „Überwachungsgesamtbelastung“ wird mit den Reformgesetzen ein neues Niveau erreichen und den Gesetzgeber künftig noch weiter als bisher bei der Schaffung neuer Überwachungsbefugnisse einschränken.<sup>91</sup> Das muss bereits bei anderen aktuellen Vorhaben im Bereich der Sicherheitsgesetzgebung Berücksichtigung finden. Die Datenschutzbeauftragten von Bund und Ländern haben vor diesem Hintergrund vor Kurzem – zurecht – einen sorgfältigen parlamentarischen Umgang mit der Balance von Freiheit und Sicherheit angemahnt.<sup>92</sup>

*gez. Prof. Dr. Markus Löffelmann*

---

<sup>91</sup> Vgl. BVerfGE 125, 260, 323 f.; ausf. zur Thematik Löffelmann, Überwachungsgesamtrechnung und Verhältnismäßigkeitsgrundsatz, 2022; ders., GSZ 2024, 18.

<sup>92</sup> Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 23. September 2026, [https://www.datenschutzkonferenz-online.de/media/en/26-09-23\\_Entschliessung\\_Freiheit\\_schuetzen-Sicherheitsgesetze\\_angemessen\\_gestalten.pdf](https://www.datenschutzkonferenz-online.de/media/en/26-09-23_Entschliessung_Freiheit_schuetzen-Sicherheitsgesetze_angemessen_gestalten.pdf).



| Maßnahme                                     | Norm                  | Stufe 1 | Stufe 2 | Stufe 3 | UKR |
|----------------------------------------------|-----------------------|---------|---------|---------|-----|
| Generalklausel nd-Mittel                     | § 16 I BVerfSchG      | x       |         |         |     |
|                                              | § 18 I BNDG           | x       |         |         |     |
| Auskunftersuchen Diensteanbieter             | § 11, 13, 14          | x       |         |         |     |
|                                              | § 12                  | A/I     |         |         |     |
| qualifizierte Auskunftersuchen               | § 11 III 1, V, 13 III |         | x       |         | x   |
|                                              | § 13 I 1, 2           | A       | I       |         |     |
| Auskunftersuchen Inhalt TK u. Post           | § 13 IV, § 14 II      |         |         | x       |     |
|                                              | § 13 I 1, 2           | A       | I       |         | I   |
| Auskunftersuchen Cyberangriff                | § 12 III 1 2.         |         | x       |         |     |
|                                              | § 14 I                | A/I     |         |         |     |
| Auskunftersuchen Cyber Kopie                 | § 12 III 2            |         |         | x       |     |
|                                              | § 14 II               | A/I     |         |         | A/I |
| Ersuchen zur Videoüberwachung                | § 15 I, II 1          |         | x       |         |     |
|                                              | § 15 II               |         | A/I     |         |     |
| Ersuchen VideoÜ. längerfristig               | § 15 II 2             |         |         | x       | x   |
|                                              | § 15 III              |         |         | A/I     |     |
| VP/NDV länger 6 Mo.                          | § 18 II 1 1.          |         | x       |         | x   |
|                                              | § 24 I 1., II 1.      | A       | I       |         | I   |
| VP/NDV gegen Kontaktpersonen                 | § 18 II 1 2.          |         | x       |         | x   |
|                                              | n.g.                  |         |         |         |     |
| VP/NDV bes. Vertraulichkeitsbez.             | § 18 II 2             |         |         | x       | x   |
|                                              | § 24 I 2., II 2.      |         | A       | I       | I   |
| Legende vertiefte Vertrauensbasis (Internet) | § 17                  |         | x       |         | x   |
|                                              | § 25 I, II            | A       | I       |         | I   |
| VB/NDV Vertrauensbeziehung                   | § 19 I 2              |         | x       |         | x   |
|                                              | n.g.                  |         |         |         |     |
| Observation länger 48 St. o. an 7 Tg.        | § 20 I 1.             |         | x       |         |     |
|                                              | § 27 I 1., II 1.      | A       | I       |         |     |
| Observation länger 7 Tg.                     | § 20 II 1.            |         |         | x       | x   |
|                                              | § 27 I 2., II 2.      |         | A       | I       | I   |
| opt./akust. Überwachung                      | § 20 I 2.             |         | x       |         |     |
|                                              | § 27 III 1 1., 2.     | A       | I       |         |     |
| opt./akust. Ü. bes. priv. Information        | § 20 II 2.            |         |         | x       | x   |
|                                              | § 27 III 2            |         | A       | I       |     |
| StandortÜ. länger 7 o. 14/30 Tg.             | § 21 I 1.             |         | x       |         |     |
|                                              | § 26 I 1., II 1.      | A       | I       |         |     |
| StandortÜ. 30 Tg. o. 5 Wo./60 Tg.            | § 21 I 2.             |         |         | x       | x   |
|                                              | § 26 I 2., II 2.      |         | A       | I       | I   |
| Brief-/Postüberwachung Inhalt                | § 22 I 1              |         |         | x       | x   |
|                                              | § 28 I 1, II 1        |         | A       | I       | I   |
| Brief-/Postüberwachung Umstände              | § 22 I 2              |         | x       |         | x   |



|                                        |                              |      |      |          |          |
|----------------------------------------|------------------------------|------|------|----------|----------|
|                                        | § 28 I 2, II 2               | A    | I    |          |          |
| TelekommunikationsÜ. Inhalt            | § 22 I 1                     |      |      | x        | x        |
|                                        | § 35 I 2, II 2               |      | A    | I        | I        |
| TelekommunikationsÜ. Umstände          | § 22 I 2                     |      | x    |          | x        |
|                                        | § 35 I 1, II 1               | A    | I    |          | I        |
| Wohnraumüberwachung                    | § 27 I                       |      |      | x (dG)   | BVerwG   |
|                                        | § 29 I                       |      |      | A/I (dG) | BVerwG I |
| WohnraumÜ. Eigensicherung              | § 28 II                      |      |      | x (G)    |          |
|                                        | § 113 II                     |      |      | I (G)    |          |
| Betreten von Wohnraum                  | § 16 VI 2                    |      |      | x (G)    | x        |
|                                        | § 18 II                      |      | A/I  | A/I (G)  | I        |
| Asservatenauswertung                   | § 23 I 1                     |      | x    |          | x        |
|                                        | § 54 II                      |      | A    | I        |          |
| Asservatenauswertung bes. priv.        | § 23 II, III 1               |      |      | x        | x        |
|                                        | n.g.                         |      |      |          |          |
| Asservatenauswertung nicht-priv.       | § 54 I                       | A/I  |      |          |          |
| IT-Eingriff bei Auskunftsverpfl. Cyber | § 24                         | x    |      |          | x        |
|                                        | § 36                         | A/I  |      |          |          |
| Online-Durchsuchung priv.              | § 25                         |      |      | x (G)    | x        |
|                                        | § 37 II, III                 |      |      | A/I (G)  | A/I      |
| Online-Durchsuchung nicht-priv.        | § 37 I                       |      | A/I  |          |          |
| abgegrenzte Online-Ds. priv.           | § 26 I                       |      | x    |          |          |
|                                        | § 38 I, II 1 1.              |      | A    | I        | I        |
| erweiterte abgegrenzte Online-Ds.      | § 26 II                      |      |      | x        | x        |
|                                        | § 38 II 1 2.                 |      |      | A/I      | x        |
| unbenannte Mittel                      | § 16 IV 2, § 29              |      | x    | x        | x        |
|                                        | § 19 I, II                   |      | A/I  | A/I      | A/I      |
| Maßnahmen gg. Berufsgeh.tr.            | § 32 II 1., III              |      | x    |          | x        |
|                                        | § 22 II 1., 2.               |      | A/I  | A/I      | (x)      |
|                                        |                              |      |      |          |          |
| strategische Aufklärung Umstände       | § 32 I, 33 I, 34 I           | A    | I*   |          | A/I      |
| strategische Aufklärung Inhalte        | § 32 I, 33 II, 34 II         |      | A/I* |          | A/I      |
| IT-Eingriff TK-Anbieter Umstände       | § 32 II, § 34 I              | A/I* |      |          | A/I      |
| IT-Eingriff TK-Anbieter Inhalte        | § 32 II, § 33 II 1., § 34 II |      | A/I* |          | A/I      |
| Eignungsprüfung Umstände + Inhalte     | § 33 IV                      | A/I* |      |          |          |

\* Erhebung *reiner* Inlandskommunikation bei strategischen Aufklärungsmaßnahmen generell nur ausnahmsweise zulässig (§ 32 III 2).

A = reiner Auslandssachverhalt; I = Sachverhalt mit Inlandsbezug; G = Gefahr; dG = dringende Gefahr; n.g. = nicht geregelt



### Regelungsdichte im Nachrichtendienstrecht des Bundes im zeitlichen Verlauf

