Dr. Peter Schantz
Rechtsanwalt
Ministerialdirektor a.D.
peter.schantz@schantz-law.de

Berlin, den 14. Juli 2026

Stellungnahme zum Entwurf des Gesetzes zur Reform der Nachrichtendienste – Reform des BND-Gesetzes –

1 Die vorliegende Stellungnahme geht auf eine Bitte der **Gesellschaft für Freiheitsrechte e.V. (GFF)** zurück, den Entwurf zur Neuregelung des BND-Gesetzes (**BNDG-E)** sowie damit zusammenhängender Regelungen wissenschaftlich zu bewerten. Der Referentenentwurf des Gesetzes der Reform der Nachrichtendienste[1] (im Folgenden: **„Referentenentwurf“** oder **„Entwurf“**) ist ausgesprochen umfangreich (707 Seiten), sehr komplex, weil die Regelungen zum Bundesnachrichtendienst (**BND**) auf eine komplett neue Grundlage stellt, und mit einer unangemessen kurzen Stellungnahmefrist (zehn Tage bzw. sieben Werktage) veröffentlicht worden. Die vorliegende Stellungnahme wird sich daher auf ausgewählte kritische Punkte konzentrieren.

[1] Abrufbar unter: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/OESI2/NDRefG.pdf?__blob=publicationFile&v=1

Inhaltsverzeichnis

Zusammenfassung

1. Die Reform weitet die Aufgaben des BND durch eine neue, aber zu unbestimmte **Bedrohungsdogmatik** erheblich aus; die vorgesehenen Rechtsgüter und Qualifikationsstufen (§§ 2 ff. BNDG-E) sind zu **unbestimmt** formuliert und lassen die **Zuständigkeit des BND bei praktisch jedem Auslandsbezug uferlos** werden. Diese ist teilweise nicht mehr von der Gesetzgebungskompetenz des Bundes für die auswärtigen Angelegenheiten gedeckt, sondern überschreitet die Grenze zur Gewährleistung der inneren Sicherheit; hier ist der Bund nur punktuell zuständig.

2. Mit der Einführung erweiterter nachrichtendienstlicher Maßnahmen (§§ 49 ff. BNDG-E) erhält der BND erstmals **operative Befugnisse**. Dieser Paradigmenwechsel wirft grundlegende Fragen der **Gesetzgebungskompetenz**, des **Trennungsgebots** und – angesichts denkbarer kinetischer Mittel – des **wehrverfassungsrechtlichen Parlamentsvorbehalts** auf.

3. Der Entwurf hält formal am Leitbild des Auslandsnachrichtendienstes fest, weitet aber **Inlandstätigkeit des BND** in mehrfacher Hinsicht aus (z.B. Cyberabwehr, ausdrückliche Inlandsbefugnisse) und überträgt dem BND immer mehr Befugnisse zur Abwehr von Gefahren und Cyberbedrohungen. Gefahrenabwehr ist aber primär eine Aufgabe der Polizei. Nicht überzeugend ist das Argument, der BND verfüge anders als die Polizei über bestimmte Fähigkeiten: **Das Können muss der Kompetenz folgen**. Auch der Verweis darauf, dass Informationen fremder Dienste nicht weitergegeben werden dürften, darf die deutsche Zuständigkeitsordnung nicht aushebeln.

4. Der **Zustimmungsfall** (§§ 125 ff. BNDG-E) führt eine „**Logik des Ausnahmezustands**“, schränkt Grundrechte erheblich ein und ist verfassungsrechtlich nicht tragfähig.

5. Der Gesetzentwurf schlägt eine Vielzahl von Befugnissen vor, die den **Zugriff auf IT-Systeme** erlauben. Die Regelungen zur Online-Durchsuchung sind mit dem IT-System-Grundrecht nicht vereinbar, soweit sie keine zumindest konkretisierte Gefahr erfordern. Zweifelhaft sind bereits im Ansatz die Überlegungen heimlich inländische Telekommunikationsanbieter zu hacken oder heimlich Spuren in den IT-Systemen der Opfer von Cyberangriffen zu erheben.

6. Die **verpflichtende Weiterleitung von IT-Schwachstellen (0-Day-Exploits) vom BSI an den BND** (§ 10 Abs. 2 BNDG-E) löst den Zielkonflikt zwischen nachrichtendienstlichem Nutzungsinteresse und IT-Sicherheit einseitig zulasten der IT-Sicherheit und gefährdet den Coordinated-Vulnerability-Disclosure-Prozess des BSI. Ein gesetzlich geregeltes **Schwachstellenmanagement fehlt weiterhin**.

7. Der Gesetzentwurf sieht erstmals aktive Cybermaßnahmen („**Hackbacks**“) vor – auch dies ein Paradigmenwechsel, der nicht ausreichend geregelt ist und ohne Einbindung des BSI stattfinden soll. Bedenklich ist die Befugnis die Entscheidung, ob ein Cyberangriff vorliegt, ob und wie auf ihn reagiert werden soll und die Ausführung der **Reaktion in die Hände einer KI zu legen**.

8. Bei der **strategischen Aufklärung** ist die vorgesehene **Volumenbegrenzung (15 % statt 30 %) faktisch wirkungslos**, weil sie an Kapazitäten statt an die tatsächlichen Kommunikationsströme anknüpft; zudem sind die **Weitergabe ungefilterter Rohdaten** an die Bundeswehr und ausländische Dienste sowie die Ausweitung der Zugriffsmöglichkeiten auf (qualifizierte) Inlandskommunikation verfassungsrechtlich zweifelhaft.

9. Der Entwurf zeigt, dass **Ankauf von Daten bei kommerziellen Anbietern (ADINT)** zum *modus operandi* des BND gehört. Es fehlt aber weiterhin eine gesetzliche Regelung. Diese muss sicherstellen, dass nicht Regelungen umgangen werden, die der BND erfüllen müsste, wenn er selbst die Daten erheben würde (hypothetischer Ersatzeingriff).

10. Die Regelungen zum Einsatz und zur Verwendung von **KI-Analysen** (§§ 52 f. BNDG-E) sind **überraschend unterkomplex** und tragen den besonderen Herausforderungen selbstlernender Systeme in keiner Hinsicht nicht Rechnung, die sogar Gefährlichkeitsanalysen erstellen sollen; z. B. fehlt eine robuste KI-Governance, eine Kontrolle durch den UKR sowie an Vorgaben zu Datenbestand, Qualität und Trainingsdaten.

11. Auch der **biometrische Abgleich im Internet** (§ 5 Abs. 3 BNDG-E) und der Zugriff auf **Videoüberwachungsanlagen** (§§ 11, 15, 16 BNDG-E) sehen zu niedrige Eingriffsschwellen und keine ausreichende Vorabkontrolle vor; Letzterer verstößt zudem gegen das datenschutzrechtliche Doppeltürmodell.

12. Der **Schutz von Berufsgeheimnisträgern** (§ 22 BNDG-E) bleibt hinter den verfassungsrechtlichen Anforderungen zurück, insbesondere weil er keine Abwägung im Einzelfall und keine gerichtsähnliche Vorabkontrolle vorsieht.

13. Es ist bedauerlich, dass die **BfDI entmachtet** worden ist und nicht mehr für die datenschutzrechtliche Kontrolle des BND zuständig ist. Hier fehlt insbesondere technischer Sachverstand.

14. Der **Unabhängige Kontrollrat** sollte stärker für Mitglieder ohne Hintergrund in der Justiz oder Verwaltung geöffnet werden. Es erschließt sich nicht, warum er nur für die Überwachung der Verarbeitung personenbezogener Daten zuständig ist und keine allgemeine Rechtskontrolle ausführen darf.

I. Grundfragen

1. Aufgaben und Bedrohungsdogmatik

2 Das BNDG erhält durch die Reform eine komplett neue Struktur und Systematik. Kern ist eine Ausweitung der Aufgaben des BND und eine neue Bedrohungsdogmatik. Sie sieht verschiedene Stufen vor und vollzieht damit eine Entwicklung nach, die bereits aus dem Verfassungsschutzrecht bekannt ist (siehe auch § 3 BVerfSchG-E). Allerdings sind die Stufen sehr weit und unklar formuliert, so dass die Zuständigkeit des BND letztlich allumfassend wird, soweit ein Bezug zum Ausland besteht.

a) Verfassungsrechtlicher Maßstab

3 Eine unklare oder zu weite Aufgabenbeschreibung des BND ist grundrechtlich und kompetenzrechtlich problematisch. Grundrechtlich ist sie problematisch, weil das BVerfG dem Gesetzgeber bei der Regelung der Auslandsaufklärung aufgrund ihrer überragenden Bedeutung einen großen Spielraum einräumt. Wird dieses Feld verlassen, verliert diese Privilegierung ihre Wirkung und es gelten grundrechtlich strengere Maßstäbe.[2] Daher muss der Gesetzgeber auch im Bereich der strategischen Überwachung eine normenklare und hinreichend bestimmte Regelung schaffen.[3]

4 Darüber hinaus kann der Gesetzgeber sich nur auf Art. 73 Abs. 1 Nr. 1 1. Alt. GG, die auswärtigen Angelegenheiten, stützen. Eine weitere Grenze ergibt sich daraus, dass dem Bund keine umfassende Gesetzgebungskompetenz zur Abwehr von Gefahren und im Bereich der inneren Sicherheit zusteht; er ist nur im Rahmen der Art. 73 Abs. 1 Nr. 9a und Nr. 10 GG sehr begrenzt zuständig.[4] Das BVerfG fasst dies so zusammen:

> „bb) Hieraus ergibt sich, dass der Bund den Bundesnachrichtendienst mit der Auslandsaufklärung **nicht allgemein zum Zweck der Gewährleistung der inneren Sicherheit** betrauen kann. Art. 73 Abs. 1 Nr. 1 GG berechtigt den Bundesgesetzgeber nicht dazu, Befugnisse einzuräumen, die auf die Verhütung, Verhinderung oder Verfolgung von Straftaten als solche gerichtet sind (vgl. BVerfGE 100, 313 <370>; 133, 277 <319 Rn. 101>). Dem Bundesnachrichtendienst können insoweit nur Aufgaben und Befugnisse übertragen werden, die **eine außen- und sicherheitspolitische Bedeutung haben und damit eine internationale Dimension** aufweisen.
>
> Dies beschränkt den Bundesgesetzgeber umgekehrt allerdings nicht darauf, den Bundesnachrichtendienst allein mit der Aufgabe zu betrauen, die

[2] BVerfGE 154, 152 Rn. 161 ff. – Strategische Ausland-Ausland-Fernmeldeaufklärung;
[3] BVerfGE 154, 152 Rn. 137 ff. – Strategische Ausland-Ausland-Fernmeldeaufklärung.
[4] BVerfGE 154, 152 Rn. 123 ff. – Strategische Ausland-Ausland-Fernmeldeaufklärung; siehe auch schon BVerfGE 100, 313 (369 f.) – G-10-Gesetz.

> Bundesregierung mit Entscheidungsgrundlagen zur Sicherung ihrer außen- oder verteidigungspolitischen Handlungsfähigkeit zu versorgen (vgl. BVerfGE 100, 313 <368 ff.>). Zwar liegt hierin die primäre Aufgabe der Auslandsaufklärung, von der das Gesamtprofil des auf Art. 73 Abs. 1 Nr. 1 GG gestützten Dienstes auch geprägt bleiben muss. Jedoch kann dem Bundesnachrichtendienst als eigene Aufgabe auch die Früherkennung von aus dem Ausland drohenden Gefahren anvertraut werden, wenn diese eine hinreichend internationale Dimension aufweisen. Maßgeblich ist, dass es sich um **Gefahren handelt, die sich ihrer Art und ihrem Gewicht nach auf die Stellung der Bundesrepublik in der Staatengemeinschaft auswirken können** und gerade in diesem Sinne von außen- und sicherheitspolitischer Bedeutung sind."[5]

b) Stufensystematik der §§ 2 ff. BNDG-E

aa) Rechtsgüter und Grundtatbestand (§ 2 BNDG-E)

5 Aufgabe des BND ist die Sammlung und Erhebung von Informationen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind. Ziel ist dabei die Früherkennung von Bedrohungen für besonders gewichtige Rechtsgüter (§ 2 Abs.1 S. 2 BNDG-E). Dies ist auch zugleich der **Grundtatbestand** für Eingriffe durch den BND.[6]

6 Diese besonders gewichtigen Rechtsgüter zählt § 2 Abs. 2 BNDG-E auf. Allerdings ist die Aufzählung **nicht abschließend**; dies ist bereits problematisch mit Blick auf den Grundsatz der **Normenklarheit** und **Bestimmtheit**. Welches Rechtsgut besonders gewichtig ist, ist eine entscheidende Frage, weil an die Bedrohung dieser Rechtsgüter auch die höheren Bedrohungsstufen anknüpfen (§ 3 Abs. 1 i.V.m. § 4 Abs. 1 BNDG-E), die zu tiefen Grundrechtseingriffen ermächtigen.

7 Sehr unbestimmt ist der Begriff der **außenpolitischen Handlungsfähigkeit** der Bundesrepublik Deutschland (§2 Abs. 2 Nr. 3 BNDG-E). Diese kann von unzähligen Faktoren abhängen.

8 Verfassungsrechtlich problematisch ist es zudem, dass Bedrohungen für **Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist** (§ 2 Abs. 2 Nr. 5 BNDG-E), und – durchaus gewichtige – Individualrechtsgüter wie das Leben, die körperliche Unversehrtheit, die Freiheit und die sexuelle Selbstbestimmung einer Person (§ 2 Abs. 2 Nr. 6 BNDG-E) als gewichtige Schutzgüter für die Tätigkeit des BND ausreichen sollen. Der Schutzbedarf dieser hochrangigen Rechtsgüter steht außer Frage, **überschreitet jedoch die Grenze zur Gewährleistung der inneren**

[5] BVerfGE 154, 152 Rn. 127 f. – Strategische Ausland-Ausland-Fernmeldeaufklärung;
[6] Referentenentwurf, S. 377 und S. 378.

Sicherheit, wenn ihre Gefährdung aus Sicht der Bundesrepublik Deutschland insgesamt keine internationale Dimension aufweist und sich nicht auf die Stellung der Bundesrepublik in der Staatengemeinschaft auswirken kann.[7] Allein die allgemeine Aufgabenzuweisung in § 2 Abs. 1 S. 2 BNDG-E stellt dies außen- und sicherheitspolitische Dimension nicht sicher.

bb) Qualifikationsstufen

9 Als niedrigere Qualifikationsstufe der Bedrohung sieht der Entwurf die **erhebliche Bedrohung** vor; diese ist geeignet, eines der besonders gewichtigen Rechtsgüter nach § 2 Abs. 2 BNDG-E in besonderem Maße zu beeinträchtigen (§ 3 Abs. 1 BNDG-E). Im Falle einer **Bedrohung von herausgehobener Bedeutung** muss im Einzelfall ein erhöhtes Gefährdungspotential hinzukommen, das sich entweder in einer verdichteten Bedrohungslage oder einem gesteigerten Schadenspotential zeigt (§ 4 Abs. 1 BNDG-E). Eine Regelung nach Qualifikationsstufen ist ein gangbarer Ansatz. Allerdings sind die Begriffe zur Abgrenzung („erhöhtes Gefährdungspotential", „in besonderem Maße beeinträchtigt") sehr schwammig und damit die Stufen kaum abgrenzbar. Dies ist problematisch, weil von der Frage, welche Qualifikationsstufe vorliegt, die Zulässigkeit erheblicher Grundrechtseingriffe abhängt.

10 Dies ist offenbar auch den Entwurfsverfassern bewusst. Die Feinsteuerung soll daher durch die Indizien gemäß § 3 Abs. 3 und 4 sowie § 4 Abs. 3 bis 5 BNDG-E geschehen.[8] Diese Regelungen enthalten Bedrohungsziele, Bedrohungsfelder und Bedrohungslagen. Der Blick auf diese Indizien zeigt jedoch, eine erhebliche Ausdehnung der Aufgaben des BND, die damit letztlich für jede Bedrohung mit Auslandsbezug mit einigem Gewicht zuständig wird. Dies ist problematisch, wenn die Bedrohungen keine „eine außen- und sicherheitspolitische Bedeutung" und damit keine „internationale Dimension" aufweisen.[9] Es bestehen Zweifel, ob dies bei erheblichen Beeinträchtigungen der Wirtschaft und Wissenschaft oder der Versorgung mit wesentlichen Rohstoffen und Gütern, Energien sowie kritische Technologien (§ 3 Abs. 3 Nr. 1 und 2 BNDG-E) durchgängig gewährleistet ist. Ein solcher Bezug fehlt auch im Falle von „disruptiven Technologien", worunter beispielhaft künstliche Intelligenz genannt wird (§ 3 Abs. 4 Nr. 5 BNDG-E), auch wenn dies zweifellos eine wichtige Entwicklung ist.

11 Die Grenze zur Bekämpfung der Kriminalität wird nicht gewahrt, wenn ein Bedrohungsfeld allein auf die **organisierte Kriminalität** abgestellt wird, die

---

[7] BVerfGE 154, 152 Rn. 128, 162, 176 – Strategische Ausland-Ausland-Fernmeldeaufklärung; BVerfGE 100, 313 (373) – G-10-Gesetz.
[8] Referentenentwurf, S. 384.
[9] BVerfGE 154, 152 Rn. 128 – Strategische Ausland-Ausland-Fernmeldeaufklärung.

auf die Begehung von Straftaten mit erheblicher Bedeutung gerichtet ist. Hierunter fällt bereits mittlere Kriminalität, bei der eine internationale Dimension typischerweise fehlt, zumal ein besonders gewichtiges Rechtsgut auch Individualrechtsgüter sein können (§ 2 Abs. 2 Nr. 5 und 6 BNDG-E).[10] Zum Vergleich: § 4 Abs. 5 Nr. 4 BNDG-E knüpft auch an die Begehung von Straftaten an – aber nur, „wenn dadurch außen- oder sicherheitspolitischen Interessen der Bundesrepublik Deutschland erheblich beeinträchtigt werden".

12 Besonders deutlich wird die Ausweitung des Blickwinkels des BND in § 4 Abs. 5 S. 2 BNDG-E. Ein Indiz sind danach Bedrohungslagen, die zu einer Gefährdung der wirtschaftlichen Struktur oder der grundlegenden gesellschaftlichen Strukturen der Bundesrepublik Deutschland führen können. Die Begründung nennt hier exemplarisch die „Entwicklungen im Bereich der ‚Künstlichen Intelligenz'".[11]

2. Operative Befugnisse des BND: Erweiterte nachrichtendienstliche Maßnahmen

13 Ein **bedenklicher Paradigmenwechsel** ist die Einführung erweiterter nachrichtendienstlicher Maßnahmen (§§ 49 ff. BNDG-E). Der BND erhält hier erstmals **operative Befugnisse**.

a) Regelungsinhalt

14 Unter erweiterten nachrichtendienstlichen Maßnahmen wird das „aktive Einwirken mit dem Ziel der Abwendung oder Einschränkung" einer Gefährdung verstanden (§ 49 Abs. 1 S. 1 BNDG-E). Die Maßnahme darf sich nur gegen eine fremde Macht richten und nicht gezielt gegen das Leib und Leben einer Person (§ 51 Abs. 3 BNDG-E); damit werden gezielte Tötungen – außerhalb des Verteidigungsfalles (§ 129 Abs. 3 S. 2 BNDG-E) – ausgeschlossen, aber nicht die **Tötung oder Verletzung von Personen als Kollateralschaden**.[12] Im Übrigen ist die Art der einzusetzenden Mittel nicht eingegrenzt; es muss nur erforderlich und angemessen sein (§ 51 Abs. 1 und Abs. 4 BNDG-E). In der Begründung zu § 129 BNDG-E werden explizit „**kinetische Mittel**" erwähnt; es erscheint durchaus denkbar, dass diese auch außerhalb des Zustimmungs-, Spannungs- oder Verteidigungsfalles eingesetzt werden, sofern die Ziele keine Personen sind.

---

[10] BVerfGE 154, 152 Rn. 132 f. – Strategische Ausland-Ausland-Fernmeldeaufklärung hat offengelassen, ob als Kompetenz in diesem Fall die „internationale Verbrechensbekämpfung" (Art. 73 Abs. 1 Nr. 10 GG) in Betracht käme; hierauf berufen sich die Verfasser des Referentenentwurfs, S. 229, aber nicht.
[11] Referentenentwurf, S. 399.
[12] Referentenentwurf, S. 527.

15 Dem Einsatz nachrichtendienstlicher Mittel geht ein zweistufiges Verfahren voraus: Zuerst muss eine spezifische Gefährdungslage – tatsächliche Anhaltspunkte, dass besonders gewichtige Rechtsgüter in besonderem Maße durch das anhaltende und planvolle Handeln einer fremden Macht gefährdet sind – festgestellt werden (§ 49 Abs. 1 S.1 und Abs. 2 BNDG-E). Zudem müssen Art und Umfang der Maßnahmen in einer Grundanordnung vom Präsidenten des BND angeordnet werden (§ 50 BNDG-E).

b) Bewertung

16 Die Regelung wirft tiefgreifende verfassungsrechtliche Fragen auf verschiedenen Feldern auf, welche durch die „**Verpolizeilichung" der Nachrichtendienste** entstehen, d.h. der Betrauung mit Aufgaben der Gefahrenabwehr oder Straftatenverhütung.

17 Erstens: die **Gesetzgebungskompetenz**. Das BVerfG hat die Gesetzgebungskompetenz des Bundes für den BND, wie auch jetzt der Referentenentwurf,[13] allein auf die auswärtigen Angelegenheiten (Art. 73 Abs. 1 Nr. 1 1. Alt. GG) gestützt; hierbei hat das Gericht die Tätigkeit des BND allein auf die Früherkennung von Gefahren beschränkt[14] und betont, dass die Abwehr von Gefahren mit Ausnahme der Art. 73 Abs. 1 Nr. 9a und Nr. 10 GG bei den Ländern liege.[15] Teilweise wird erwogen, den Kompetenztitel der Verteidigung (Art. 73 Abs. 1 Nr. 1 2. Alt. GG) heranzuziehen; dies tut der Entwurf allerdings nicht.[16] Konsequenterweise würde dies Abgrenzungsfragen zur Bundeswehr aufwerfen.

18 Zweitens: Das **Trennungsgebot**. Das BVerfG hat in seiner Rechtsprechung deutlich gemacht, dass sich die weiten Spielräume des BND bei der Gefahrenfrüherkennung nur dadurch rechtfertigen lassen, dass er über keine operativen Anschlussbefugnisse verfügt.[17] Diese richten sich hier zwar gegen fremde Staaten. Eine Betroffenheit von Grundrechtsträgern ist jedoch nicht ausgeschlossen. Zu berücksichtigen ist zudem, dass der BND – wenn auch subsidiär (vgl. § 51 Abs. 2 BNDG-E) – diese Maßnahmen **im Inland** anwenden kann. Dies ist zulässig, wenn nur er über die erforderlichen Fähigkeiten verfügt, oder aber eine Informationsweitergabe aus Gründen der Geheimhaltung nicht möglich ist. Letzterer Fall dürfte die Regel sein, wenn

---

[13] Referentenentwurf, S. 229.
[14] BVerfGE 154, 152 Rn. 128 – Strategische Ausland-Ausland-Fernmeldeaufklärung.
[15] BVerfGE 154, 152 Rn. 126 – Strategische Ausland-Ausland-Fernmeldeaufklärung.
[16] Referentenentwurf, S. 229.
[17] BVerfGE 154, 152 Rn. 149, 165 f. – Strategische Ausland-Ausland-Fernmeldeaufklärung; ähnlich für den Verfassungsschutz BVerfGE 162, 1 Rn. 154 – Bayerisches Verfassungsschutzgesetz.

die Maßnahme auf Informationen aus der internationalen Zusammenarbeit der Nachrichtendienste aufbaut.[18]

19 Drittens: **der Parlamentsvorbehalt**. Es ist nicht ausgeschlossen, dass die Folgen einer solchen Maßnahme einer militärischen Maßnahme vergleichbar sind (Bsp.: Einsatz von Sprengstoff). Es kommt daher potentiell nicht nur zu einer „Verpolizeilichung", sondern auch zu einer „**Militarisierung**" der Arbeit der Nachrichtendienste. In diesen Fällen könnte das „Eskalations- und Verstrickungspotential" in einen bewaffneten Konflikt gegeben sein, welches das BVerfG als Kriterium für den wehrverfassungsrechtlichen Parlamentsvorbehalt entwickelt hat.[19]

3. Trennungsgebot und Inlandstätigkeit

20 **Formal** hält der Gesetzentwurf am Leitbild als Auslandsnachrichtendienst fest. Die Position des BND wird jedoch in drei Dimensionen erheblich gestärkt:

21 **Erweiterung des Aufgabenspektrums** nach §§ 2 bis 4 BNDG-E zu einer umfassenden Früherkennung (→ Rn. 5 ff.). Dies wirft Probleme hinsichtlich der Gesetzgebungskompetenz des Bundes auf.

22 **Gefahrenabwehr, Cyberabwehr und aktive Maßnahmen**: Der BND darf vielfach zur Abwehr einer Gefahr tätig werden, obwohl ihm selbst eigentlich die Mittel zur Gefahrenabwehr fehlen. Eine Ausnahme ist hier der Bereich der Cyberabwehr, in dem der BND zu aktiven Maßnahmen ermächtigt werden soll. Ein wiederkehrende Argumentationstopoi sind die fehlenden Fähigkeiten anderer Behörden und die Schwierigkeit Daten ausländischer Dienste mit anderen Behörden aufgrund der Third Party Rule zu teilen. Dieses Argument ist bedenklich, weil letztlich Usancen der Zusammenarbeit der Nachrichtendienste bestimmen würden, welche deutsche Behörde tätig werden darf.

23 Symbolisch für diese Hinwendung zur Gefahrenabwehr ist, dass der Entwurf **§ 2 Abs 3 BNDG nicht aufnimmt**. Dieser stellte klar, dass dem BND keine polizeilichen Befugnisse zustehen und er dafür auch die Polizei nicht zur Amtshilfe bitten darf, weil er sie nur um Maßnahmen ersuchen darf, die er selbst vornehmen dürfte. Diese Regelung sollte – schon als Auslegungshilfe für das Gesetz insgesamt – wieder aufgenommen werden.

24 Im Bereich der **Cyberabwehr** tritt die Befugnis zu aktiven Maßnahmen hinzu, also zu Vollzugshandlungen. Diese fußen auf Informationen, die der BND aufgrund seiner weiten Befugnisse als Nachrichtendienst erheben

[18] Referentenentwurf, S. 524.
[19] Vgl. BVerfGE 121, 135 Rn. 71 – Luftraumüberwachung Türkei.

durfte. Dies durfte er aber nur, weil er gerade nicht über solche operativen Befugnisse verfügte.[20] Dies ist daher ebenso wie die Befugnis zu erweiterten nachrichtendienstlichen Maßnahmen vor dem Hintergrund des Trennungsprinzips hochproblematisch.

25 **Inlandstätigkeiten**: Es fällt auf, dass dem BND häufig auch die Tätigkeit im Inland erlaubt wird. Dies beginnt bei der Erlaubnis, Maßnahmen für 72 Stunden im Inland fortzusetzen, wenn eine Person nach Deutschland reist (gewissermaßen eine „nachrichtendienstliche Nacheile"). Auch viele Befugnisse sehen ausdrücklich die Möglichkeit vor, im Inland angewendet zu werden (z.B. der Zugriff auf Videoüberwachungsanlagen (§ 16 Abs. 2 i.V.m. § 15 BNDG-E; die Wohnraumüberwachung (§ 29 Abs. 2 BNDG-E); Zugriffe auf die IT-Systeme von Telekommunikationsanbietern (§§ 31 Abs. 6, 32 Abs. 2 BNDG-E). Viele andere Befugnisse lassen diese Frage offen.

26 Eine stärkere **Tätigkeit des BND im Inland ist nicht unbedenklich**. Der BND darf nicht nur mehr als Polizeibehörden, weil er ein Nachrichtendienst ist, sondern er darf als Auslandsnachrichtendienst auch mehr als der Verfassungsschutz. Auch dies ist darin begründet, dass der BND im Ausland über keine Hoheitsbefugnisse verfügt; er kann zwar eine breite Informationsbasis beschaffen und auswerten, Folgemaßnahmen kann er aber nicht leicht ergreifen.[21] Dies ist bei einer Tätigkeit im Inland anders.

4. Logik des Ausnahmezustands

27 Zu warnen ist vor den Regelungen in den §§ 125 ff. BNDG-E. Sie führen eine **Logik des Ausnahmezustands** in das deutsche Sicherheitsrecht ein. Es handelt sich um Spezialregelungen für den Spannungs- und Verteidigungsfall (Art. 80a, Art. 115a GG), aber auch für den Zustimmungsfall. Der Zustimmungsfall ist nicht im Grundgesetz angelegt, sondern wird neu durch das BNDG-E eingeführt. Er soll dann eintreten, wenn der der Verteidigungs- oder Spannungsfall unmittelbar bevorstehen und dies aus Gründen der Verteidigung zwingend notwendig ist. Die Bundesregierung kann ihn mit Zustimmung des PKGr, d.h. mit einfacher Mehrheit, feststellen (§ 125 Abs. 3 S. 1 BNDG-E). Eine Veröffentlichung ist nicht vorgesehen. Eine öffentliche politische Diskussion findet damit auch nicht statt. Folge des Zustimmungsfalls ist es, dass wesentliche verfahrensrechtliche, datenschutzrechtliche grundrechtliche Sicherung wegfallen, z.B. der Schutz von Berufsgeheimnisträgern; ferner können z.B. Behörden und Unternehmen zu Unterstützungsleistungen herangezogen werden.

[20] BVerfGE 154, 152 Rn. 149 – Strategische Ausland-Ausland-Fernmeldeaufklärung.
[21] BVerfGE 154, 152 Rn. 149 – Strategische Ausland-Ausland-Fernmeldeaufklärung.

28 Die Unterscheidung zwischen einer „normalen Lage“ und einer Art „Notstandslage“ oder „Ausnahmezustand“ gibt es in Deutschland – anders als etwa in Frankreich – nicht. Dies hat historische Gründe, beruht aber auch auf Erkenntnis, dass grundrechtliche Gewährleistungen gerade in Krisenfällen den Einzelnen schützen sollten. Zudem trägt ein solcher Ausnahmezustand die Tendenz in sich, immer weiter verlängert zu werden. Gerade in Zeiten von hybriden Bedrohungen könnte eine Phase vor dem Spannungsfall lange andauern. Ein Zustimmungsfall könnte zudem von der Regierung und der sie tragenden Parlamentsmehrheit beschlossen werden – anders als der Spannungs- und der Verteidigungsfall, die nur mit einer Zweidrittelmehrheit im Bundestag beschlossen werden können. Verfassungsrechtlich schließlich bestehen gravierende Zweifel: Der Zustimmungsfall hat keine verfassungsrechtliche Grundlage. Derart weite und unbestimmte Befugnisse und Grundrechtseinschränkungen sind daher nicht mit dem Grundgesetz vereinbar.

II. Einzelne Befugnisse

1. Zugriff auf informationstechnische Systeme

29 Der Entwurf enthält eine Vielzahl von neuen Befugnissen, welche den Zugriff auf informationstechnische Systeme erlauben oder gar aktive Cybermaßnahmen. Eine Regelung zu einem verantwortungsvollen Umgang mit Schwachstellen fehlt demgegenüber weiterhin.

a) Online-Durchsuchung

30 Die Regelungen zur Online-Durchsuchung nach § 37, 38 BNDG-E sind **verfassungsrechtlich sehr problematisch**. Der Gesetzentwurf versucht, verschiedene Differenzierungen einzuführen, um neben einer Online-Durchsuchungen heimliche Zugriffe auf informationstechnische Systeme zu erlauben, die aus seiner Sicht nicht die hohen Hürden einer Online-Durchsuchung erfüllen müssen. Nach der Rechtsprechung des BVerfG handelt es sich bei einer Online-Durchsuchung um eine Maßnahme mit dem – neben einer heimlichen Wohnraumüberwachung – höchsten Eingriffstiefe. Im präventiven Bereich setzt eine Online-Durchsuchung daher zumindest eine konkretisierte Gefahr für ein höchstes Rechtsgut voraus – auch eine Online-Durchsuchung durch Nachrichtendienste.[22] Hintergrund ist die zentrale Bedeutung eigengenutzter IT-Systeme für die Lebensgestaltung des heutigen Menschen und die damit verbundene Aussagekraft der darauf verarbeiteten

[22] BVerfGE 162, 1 Rn. 176 – Bayerisches Verfassungsschutzgesetz.

Daten. Es handelt sich gewissermaßen um das „ausgelagerte Gehirn“ (Burkhard Hirsch) des modernen Menschen.

31 Zunächst unterscheidet der Entwurf nach dem **Umfang des Eingriffs** zwischen einem Zugriff, der Einblicke in wesentliche Teile der Lebensgestaltung einer Person erlaubt oder ein aussagekräftiges Bild seiner Persönlichkeit ergibt (§ 37 BNDG-E), einerseits und einem begrenzteren Zugriff (§ 38 BNDG-E) andererseits. Diese Differenzierung übersieht den Kern des IT-System-Grundrechts: den Integritätsschutz von IT-Systemen.[23] Entscheidend ist, welche Aussagekraft die darauf potentiell gespeicherten Daten haben. Denn ist erst einmal die Integrität des Systems verletzt, lässt sich der Umfang des Zugriffs kaum noch nachvollziehen. Dies hat das BVerfG in seinen beiden Entscheidungen zum Trojaner im Jahr 2025 klargestellt und die bisherige Privilegierung der Quellen-TKÜ nicht mehr weitergeführt. Das Gericht hat zwar in den Raum gestellt, dass begrenzte Zugriffe geringeren Schwellen unterliegen könnten,[24] hat dies im Falle einer Quellen-TKÜ aber gerade nicht angenommen.[25] Dementsprechend wäre ein Zugriff auf Kommunikationsinhalte oder vergleichbare Daten auf dem IT-System eines deutschen Staatsangehörigen – anders als § 38 Abs. 2 BNDG-E vorschlägt – nur bei Vorliegen einer konkretisierten Gefahr zulässig. Im Übrigen lädt die vorgeschlagene Differenzierung zu Umgehungen ein und setzt die Diskussion über die Abgrenzung zwischen Online-Durchsuchung und Quellen-TKÜ, die das BVerfG gerade erst beigelegt hatte, auf einer anderen Ebene fort. Auch hier wird dann eine entscheidende Rolle spielen, ob die Software nur den Zugriff auf diesen begrenzten Datenbestand erlaubt (§ 38 Abs. 3 S. 1 BNDG-E); dies hat sich bisher als praktisch unmöglich erwiesen.

32 Im Rahmen des § 37 BNDG-E unterscheidet der Entwurf zwischen **„eigenen privaten“ und anderen IT-Systemen**. Nach der Rechtsprechung des BVerfG kommt es nur darauf an, ob es ein „eigengenutztes“ System ist, nicht welchem Zweck es dient. Die betroffene Person muss davon ausgehen können, dass sie allein oder zusammen anderen Personen selbstbestimmt über die Nutzung bestimmt.[26] Dies ist auch nachvollziehbar, weil erstens viele Menschen ihre beruflichen IT-Systeme auch für private Zwecke nutzen[27] und zweitens auch der berufliche Kontext einen wesentlichen Teil der Lebensgestaltung und Persönlichkeit ist. Soweit sich eine Online-Durchsuchung gegen eine Person

---

[23] Hierzu BVerfG MMR 2026, 44 Rn. 99 f., 103, 117 – Trojaner I; BVerfG MMR 2026, 52 Rn. 221, 228, 237.
[24] BVerfG MMR 2026, 52 Rn. 199 – Trojaner II; BVerfG MMR 2026, 44 Rn. 124 – Trojaner I; darauf stützend Referentenentwurf, S. 498.
[25] BVerfG MMR 2026, 52 Rn. 200, 201 ff. – Trojaner II,
[26] BVerfGE 120, 274 (315) – Online-Durchsuchung; ähnlich BVerfG MMR 2026, 44 Rn. 115 – Trojaner I.
[27] So aber Referentenentwurf, S. 500 f.

deutscher Staatsangehörigkeit oder mit Aufenthalt im Inland richtet ist daher **immer eine konkretisierte Gefahr erforderlich** und nicht nur bei eigenen privaten IT-Systemen, ebenso eine Vorabkontrolle durch den UKR (bisher nur für § 38 Abs. 2 BNDG-E, vgl. § 97 Abs. 1 Nr. 15 BNDG-E).

33 Eine Online-Durchsuchung zur Abwehr einer konkretisierten oder konkreten Gefahr ist eine **Maßnahme der Gefahrenabwehr**. Nachrichtendienste wie der BND oder das Bundesamt für Verfassungsschutz verfügen zur Abwehr einer Gefahr, d.h. den Maßnahmen, die auf die Online-Durchsuchung folgen, über keine Befugnisse. Sie dürfen diese Maßnahmen daher nur durchführen, wenn polizeiliche Hilfe nicht rechtzeitig käme.[28] Das Gericht zielt also auf die zeitliche Dimension, während der Entwurf auf das Können abstellt. Dies ist aber nicht überzeugend, denn das **Können muss der Kompetenz folgen**. Diese liegt für die Gefahrenabwehr bei den Ländern und nur in engen Grenzen (Art. 73 Abs. 1 Nr. 9a GG) beim Bund. Anderenfalls würde die Zuständigkeit letztlich von der Ausstattung bestimmt werden und nicht die Ausstattung von den Aufgaben. Fallen beide auseinander, muss ggf. um Amtshilfe gebeten werden. Problematisch ist es, dass auch hier der Entwurf davon ausgeht, dass der BND zuständig werden könne, weil er Informationen von ausländischen Diensten nicht weitergeben dürfe (Third Party Rule).[29]

b) Weiterleitung von IT-Schwachstellen an den BND

34 Verfassungsrechtlich und politisch **alarmierend** ist die Verpflichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) Informationen an den BND weiterzugeben (§ 10 Abs. 2 S. 1 Nr. 2 BNDG-E) – und zwar nicht auf Nachfrage im Einzelfall, sondern „proaktiv“[30]. Die Begründung führt deutlich aus, dass damit die Meldung von Schwachstellen (0-Day-Exploits) gemeint ist, die den Herstellern noch unbekannt sind. Die Zeit zwischen Kenntnis des BSI und Schließung der Lücke durch den Hersteller möchte der BND nutzen, „um die Schwachstellen in Wert bringen zu können“.[31] Hintergrund sei, dass die Beschaffung (wohl auf dem Schwarzmarkt) und die Suche nach Schwachstellen teuer und personalintensiv sei.[32]

35 Wenn der Staat sich entschließt, Schwachstellen für eigene Zwecke zu nutzen, entsteht ein **Zielkonflikt mit der IT-Sicherheit**. Schwachstellen sind eine Gefahr für Bürgerinnen und Bürger, Unternehmen und andere Organisationen, aber auch für das Gemeinwesen und seine Einrichtungen, denn sie können durch die Ausnutzung dieser Sicherheitslücken geschädigt werden. Kurzum:

---

[28] BVerfGE 162, 1 Rn. 178 ff. – Bayerisches Verfassungsschutzgesetz.
[29] Referentenentwurf, S. 503.
[30] Referentenentwurf, S. 412.
[31] Referentenentwurf, S. 411 f.
[32] Referentenentwurf, S. 411.

IT-Sicherheit ist die **Achillesferse der Informationsgesellschaft**. Das Risiko wächst, weil KI-Systeme heute in der Lage sind, Schwachstellen aufzufinden und zu nutzen – in einer früher kaum denkbaren Geschwindigkeit.

36 Der Entwurf löst diesen Zielkonflikt **einseitig zulasten der IT-Sicherheit**. Es fehlt zunächst an einem **Schwachstellenmanagement**. Das BVerfG hat aus dem IT-System-Grundrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) eine Schutzpflicht des Staates abgeleitet, wenn er Schwachstellen kennt, aber der Hersteller nicht.[33] Dies ist nicht nur der Fall, wenn das BSI den BND über Schwachstellen informiert, sondern auch, wenn der BND Schwachstellen ankauft oder kommerzielle Spähsoftware (z.B. Pegasus) nutzt. Verfassungsrechtlich

> „verlangt die grundrechtliche Schutzpflicht eine Regelung darüber, wie die Behörde bei der Entscheidung über ein Offenhalten unerkannter Sicherheitslücken den Zielkonflikt zwischen dem notwendigen Schutz vor Infiltration durch Dritte einerseits und der Ermöglichung von Quellen-Telekommunikationsüberwachungen andererseits aufzulösen hat. Der Behörde muss eine Abwägung der gegenläufigen Belange für den Fall aufgegeben werden, dass ihr eine Zero-Day-Schutzlücke bekannt wird. Es ist sicherzustellen, dass die Behörde bei jeder Entscheidung über ein Offenhalten einer unerkannten Sicherheitslücke einerseits die Gefahr einer weiteren Verbreitung der Kenntnis von dieser Sicherheitslücke ermittelt und andererseits den Nutzen möglicher behördlicher Infiltrationen mittels dieser Lücke quantitativ und qualitativ bestimmt, beides zueinander ins Verhältnis setzt und die Sicherheitslücke an den Hersteller meldet, wenn nicht das Interesse an der Offenhaltung der Lücke überwiegt.“[34]

37 Der Gesetzgeber hat bisher noch nicht einmal ansatzweise einen derartigen *Vulnerabilities Equities Process* (VEP) geschaffen, obwohl er die Befugnisse immer mehr ausweitet, die Schwachstellen ausnutzen. Es stellt sich allerdings auch die Frage, ob ein solcher Prozess angesichts der Geschwindigkeit in der KI Schwachstellen aufspürt und ausnutzt noch trägt oder ob an die Stelle das **Primat der Schließung von Sicherheitslücken** treten sollte.

38 Zudem **kompromittiert der Vorschlag** den Coordinated Vulnerability Disclosure (CVD)-Prozess des BSI, in dem BSI vertraulich Sicherheitslücken gemeldet werden können. Sicherheitsforscher oder White Hacker melden in diesem Verfahren eine Sicherheitslücke, damit sie schnell geschlossen, nicht damit sie ausgenutzt wird. Die vorgeschlagene Regelung unterminiert das Vertrauen in das BSI, ohne das der CVD-Prozess nicht funktioniert. Der Vorschlag zeigt, dass die Bundesregierung dem Ziel der **IT-Sicherheit weiterhin nicht die erforderliche Priorität** einräumt, sondern es zu leicht anderen Interessen unterordnet.

---

[33] BVerfGE 158, 170 Rn. 40, 41f. – IT-Schwachstellen.
[34] BVerfGE 158, 170 Rn. 43 – IT-Schwachstellen.

c) Aktive Cybermaßnahmen („Hackbacks“)

39 § 39 Abs. 4 S. 1 BNDG-E erlaubt dem BND die Veränderung und Löschung von Daten, die Umleitung und Unterbindung von Datenverkehren und die Einschränkung oder Unterbindung des IT-Systems von dem eine Gefahr ausgeht, zur Abwehr einer unmittelbar bevorstehenden Gefahr für ein besonders gewichtiges Rechtsgut. Die Begründung nennt dies eine „Annex-Kompetenz“.[35] Hierfür spricht, dass die Gefahr beim Zugriff auf ein IT-System nach §§ 36 ff. BNDG-E erkannt worden sein muss. In der Praxis wird das Aufspüren der Quelle des Angriffs aber wahrscheinlich Zweck des Zugriffs auf das IT-System sein, so dass die aktive Folgemaßnahme bereits von vornherein als möglich eingeplant sein dürfte. Damit ist auch hier aber die Kompetenz des Bundesgesetzgebers zweifelhaft, denn es handelt sich eindeutig um eine Maßnahme der Gefahrenabwehr.

40 Die Regelung ist nicht normenklar und enthält auch **keine ausreichend differenzierten Regelungen**, etwa zur Attribution und möglichen Folgen des Einwirkens durch „Hackbacks“ auf ein IT-System in einem fremden Staat. Denkbar ist es z.B., dass der Cyberangriff über einen fremdgesteuerten Rechner eines unbeteiligten Dritten läuft. Diese können erhebliche Schäden erleiden (z.B. wenn das IT-System eines Krankenhauses gezielt als Proxy genutzt wird, möglicherweise in der Absicht einen „virtuellen Gegenschlag“ zu provozieren, der ein Krankenhaus trifft). Bemerkenswert ist auch, dass der Entwurf nicht vorsieht, dass der BND andere Behörden, insbesondere das BSI einbeziehen muss, sondern im Alleingang tätig werden darf.

41 Eine weitere aktive Cybermaßnahme enthält § 36 Abs. 2 BNDG-E. Danach darf der BND Daten löschen, die bei einem Cyberangriff „erbeutet“ worden sind. Dies kann auch **ohne Sicherungskopie** erfolgen, was zum kompletten Verlust der Daten führen kann. Dies erscheint ohne Rücksprache mit dem Opfer des Cyberangriffs problematisch. Auch hier handelt es sich nicht um eine Maßnahme der Früherkennung, sondern der **Gefahrenabwehr**.

42 Hinzuweisen ist in diesem Zusammenhang auch auf die bedenkliche Regelung in § 53 Abs. 7 S. 2 BNDG-E. Danach erscheint es möglich, dass aktive **Gegenmaßnahmen auf der Basis einer KI-Analyse von einer KI autonom ausgelöst** werden. Der Gesetzentwurf will dem autonomen System auch die Entscheidung überlassen**, ob ein Cyberangriff vorliegt und eine aktive Gegenmaßnahme notwendig ist,**:

> „In Satz 2 findet sich eine Ausnahme von dem soeben dargestellten Grundsatz, welche das Themenfeld der „Cyber-Angriffe“ betrifft. Hier ist (schon aufgrund technischer Notwendigkeiten) erforderlich, dass zur Abwehr solcher Angriffe durch Datenlöschung oder Umleitung von

[35] Referentenentwurf, S. 509.

> Datenströmen in Fällen, in denen eine anderweitige Abwehr nicht zielführend wäre, auch ein autonomes Handeln der automatisierten Systeme zulässig sein muss. Dabei ist denknotwendigerweise auch die Entscheidung, ob ein solcher Angriff vorliegt, welche Maßnahme am geeignetsten ist und ob (nur) eine automatische Veranlassung erfolgsversprechend ist, dem autonomen System vorbehalten."[36]

Dies könnte bedeuten: **Eine KI-Anwendung entscheidet, ob ein Angriff vorliegt und ob und auf wen sie virtuell „zurückschießt" und welche Folgen sie dabei in Kauf nimmt**. Dies erscheint angesichts der Implikationen von Hackbacks unverantwortlich. Gerade die schwierige Frage der Attribution ist entscheidend und kann nicht delegiert werden.

d) Zugriff auf Passwörter

43 § 12 Abs. 5 BNDG-E verpflichtet Telekommunikationsunternehmen und digitale Diensteanbieter, Daten herauszugeben, die den Zugriff auf Endgeräte und Speichereinrichtungen in Endgeräten oder räumlichen hiervon getrennt ermöglichen. Diese Daten dürften etwa **Passwörter** sein. Sie erlauben damit zumindest in vielen Fällen einen Eingriff in das IT-System-Grundrecht, denn dieses schützt nicht nur das informationstechnische System, sondern auch damit vernetzte Geräte, z.B. Cloud-Speicher.[37] Die Einblicke in das Leben einer Person können damit ähnlich weit gehen wie bei einer Online-Durchsuchung. Der Gesetzentwurf regelt dies aber nicht normenklar und präzise, sondern verweist auf die „gesetzlichen Voraussetzungen für die Nutzung der Daten"; damit liegt die Entscheidung der Nutzungsvoraussetzungen beim BND, obwohl der Gesetzgeber sie festlegen müsste. Ungeregelt bleibt zudem der Zugriff selbst, der bereits die Integrität des IT-Systems verletzt und damit das IT-System-Grundrecht[38] (ähnlich wie der Einbruch in eine Wohnung, unabhängig davon, ob etwas gestohlen wird).

e) Heimlicher Zugriff auf IT-Systeme von Telekommunikationsanbietern

44 Neu ist, dass der BND sich heimlich in die informationstechnischen Systeme von inländischen Telekommunikationsanbietern **„hacken"** darf, auch wenn sich diese **im Inland** befinden (§ 32 Abs. 2 BNDG-E). Dies ist bereits dann erlaubt, wenn – wie bei den meisten deutschen Telekommunikationsanbietern – ein **ausländisches Unternehmen einen beherrschenden Einfluss** ausübt (z.B. Telefónica/O2 oder Vodafone, § 32 Abs. 2 S. 2 Nr. 1 BNDG-E); hier wird typisiert angenommen, ausländische Muttergesellschaften würden ihre

[36] Referentenentwurf, S. 525.
[37] BVerfGE 141, 220 Rn. 209 f. – BKA-Gesetz.
[38] BVerfG MMR 2026, 44 Rn. 100, 103 – Trojaner I.

Tochtergesellschaften anweisen, nicht mit dem BND zu kooperieren. Zumindest in Bezug auf Unternehmen aus anderen Mitgliedstaaten der EU wäre zu prüfen, ob der Anwendungsbereich des Unionsrechts trotz Art. 4 Abs. 2 S. 3 EUV nicht eröffnet ist und eine unzulässige Diskriminierung vorliegt. Zudem ist es sehr zweifelhaft, ob bereits aufgrund einer so grob typisierten Betrachtung ein Auslandsnachrichtendienst im Inland zu einer **heimlichen Selbstvornahme** ermächtigt werden sollte, statt den üblichen Weg mit Verwaltungszwang und Bußgeld zu gehen. Diese prinzipiellen Bedenken bestehen auch gegenüber dem heimlichen Zugriff auf die informationstechnischen Systeme von TK-Anbietern, die einer **Anordnung nach § 13 Abs. 5 BNDG-E nicht nachgekommen** sind (§ 32 Abs. 2 S. 2 Nr. 2 BNDG-E). Denkbar wäre auch, dass der TK-Anbieter die Anordnung für rechtswidrig hielt; dies dürfte ihm bis zu einer finalen Klärung nicht zur Last gelegt werden.

45 Es **fehlt eine spezielle Vorabkontrolle** durch den UKR, welche die Besonderheiten dieses Zugriffs berücksichtigt. Es handelt sich nicht nur um einen Unterfall einer strategischen Aufklärungsmaßnahme (§ 97 Abs. 1 Nr. 11 BNDG-E). Selbst wenn man der Gesetzesbegründung folgen würde und keinen Eingriff in das IT-System-Grundrecht annehmen würde,[39] würde es sich um einen **schwerwiegenden Eingriff** in die Grundrechte eines Grundrechtsträgers im Inland handeln (Art. 12 Abs. 1, Art. 10 Abs. 1 GG). Die Maßnahme greift in die **Integrität einer kritischen Infrastruktur,** auf deren Vertraulichkeit eine Vielzahl von Bürgerinnen und Bürgern sowie Unternehmen bei ihrer Nutzung für ihre Kommunikation vertrauen. Dieses Vertrauen wird so erschüttert und die Nutzerinnen und Nutzer weiteren Risiken ausgesetzt. Denn § 32 Abs. 2 BNDG-E **eröffnet eine Zugriffsmöglichkeit**, über die potentiell auch kriminelle oder ausländische Mächte auf die – ungefilterten und damit auch inländischen – Kommunikationsströme zugreifen könnten.

46 Höchst bedenklich ist, dass der BND aktive Cybermaßnahmen auch gegen IT-Systeme von Telekommunikationsanbietern ergreifen darf, wenn er eine unmittelbar bevorstehende Gefahr erkennt (§ 31 Abs. 6 Nr. 3 BNDG-E). Letztlich könnte er so möglicherweise ein Telekommunikationsnetz abschalten.

f) Heimliche Spurenerhebung in IT-Systemen

47 § 36 Abs. 1 BNDG-E erlaubt – verkürzt gesagt – eine heimliche digitale Spurensicherung eines Cyberangriffs, indem sich der BND selbst in das betroffene System hackt und Teile des IT-Systems kopieren darf. Zu dieser

[39] Referentenentwurf, S. 485.

Maßnahme darf der BND greifen, wenn seine Auskunft des Anbieters nach § 14 Abs. 1 BNDG-E die Untersuchung vereitelt würde. Zur Auskunft verpflichtet sind Anbieter, die Dritten informationstechnische Systeme öffentlich zur Verfügung stellen. Neben Anbietern von Telekommunikationsanbietern fallen darunter Hostinganbieter,[40] z.B. Cloud-Anbieter.

48 Die vorgeschlagene Maßnahme erscheint fragwürdig und unverhältnismäßig. Es erschließt sich nicht, warum – ohne sein Einverständnis **heimlich** – **in das IT-System des Opfers eines Cyberangriffs eingegriffen** wird und damit eine weitere Integritätsverletzung vorgenommen wird, statt das IT-System abzusichern. Damit wird in die Grundrechte des Anbieters eingegriffen, der typischerweise dafür selbst keinen Anlass gegeben hat. Bereits ein heimlicher Eingriff in ein IT-System einer Person, die selbst Ursache einer Gefahr ist, setzt – anders als § 36 Abs. 1 BNDG-E – zumindest eine konkretisierte Gefahr voraus. Dies muss hier im Falle eines Nichtstörers erst recht gelten. Auch dies zeigt, dass es sich um keine Maßnahme handelt, die in das Aufgabenprofil des BND als Auslandsnachrichtendienst mit dem Ziel der Früherkennung passt.

49 Durch eine Teilkopie des IT-Systems kann zudem in die Grundrechte einer Vielzahl von Personen eingegriffen werden; spezielle Regeln zum Umgang mit diesen Daten, die der besonderen Eingriffssituation Rechnung tragen, fehlen. Ein Eingriff dieser Tiefe würde schließlich eine Vorabkontrolle durch den UKR erfordern; diese sollte vorgesehen werden.

2. Strategische Aufklärung

50 Die Regelungen zur strategischen Aufklärung führen die Regelungen aus dem G-10-Gesetz und BNDG zur strategischen Fernmeldeüberwachung zusammen. Dies ist grundsätzlich zu begrüßen, zumal punktuell aus grundrechtlicher Sicht auch Verbesserungen festzustellen sind (z.B. hinsichtlich der Volumenbegrenzung oder dem Verbot der Wirtschaftsspionage). Der einheitliche Ansatz trägt auch der Realität der Kommunikationsströme Rechnung, denn auch bei einer reinen Inlandskommunikation werden Datenpakete teilweise über das Ausland geleitet.

a) Begrenzung des Umfangs

51 Der **Umfang der überwachten Kommunikation ist nicht ausreichend begrenzt**. Das BVerfG verlangt, dass eine letztlich anlasslose Überwachung des Kommunikationsverkehrs nicht den gesamten

[40] Referentenentwurf, S. 424.

Telekommunikationsverkehr umfassen darf. Der Anteil der überwachten Kommunikationsströme muss daher begrenzt werden, einmal dem Volumen nach und zum anderen durch Auswahl der Übertragungswege. Dem wird § 31 Abs. 3 S. 2 Nr. 2 BNDG-E nicht gerecht. Zu begrüßen ist zwar, dass statt 30 Prozent nur noch 15 Prozent des Datenvolumens überwacht werden dürfen. Allerdings beziehen sich diese 15 Prozent auf alle Telekommunikationsnetze und nicht nur auf die ausgewählten Kommunikationsnetze. Zum anderen läuft die Begrenzung praktisch leer, weil sie nicht auf die tatsächlichen Kommunikationsströme abstellt, sondern auf die Kapazitäten. Selbst am größten deutschen Internetknotenpunkt werden in der Regel nicht mehr als 15 Prozent der Kapazitäten genutzt.[41]

b) Weitergabe von Rohdaten ohne Filterung und Einsichtnahme

52 Die anlasslose und unterschiedslose Erhebung der Kommunikationsdaten setzt grundrechtlich zwingend eine Filterung und Sichtung voraus, weil der BND reine Inlandskommunikation nicht überwachen darf und auch für die Inland-Ausland-Kommunikation („qualifizierte Inlandskommunikation“) strengere Maßstäbe gelten als für Auslandskommunikation.[42] Es ist daher verfassungsrechtlich zweifelhaft, wenn § 31 Abs. 2 die Weitergabe ungefilterter Kommunikation (einschließlich reiner Inlandskommunikation) an die Bundeswehr erlaubt oder an ausländische Dienste im Rahmen von Kooperationen nach §§ 43, 44 BNDG-E. Es bleibt unklar, ob und wie die Limitierungen der §§ 43, 44 BNDG-E ohne eine Sichtung angewendet werden können.[43]

c) Zugriff auf reine Inlandskommunikation

53 Die Erhebung **reiner Inlandskommunikation** ist unzulässig (§ 32 Abs. 3 S. 1 BNDG-E).[44] Gleichwohl sieht § 32 Abs. 3 S. 2 eine Reihe von Ausnahmen vor, z.B. zur Abwehr von **Cyberangriffen**, zum Schutz der betroffenen Person oder zur **Gefahrenabwehr**. Diese Ausnahmen sind in der Rechtsprechung des **BVerfG bisher nicht vorgesehen**. Sie verschieben auch die Aufgabe des BND immer weiter von der Auslandsaufklärung weg zur Cyberabwehr und Gefahrenabwehr. Problematisch ist auch die Weiterverwendung von „unkenntlich“ gemachten Daten, wenn diese gerade

---

[41] *Biselli/Leisegang/Reuter*, Geheimdienstreform Zeitenwende für Spione, netzpolitik.org vom 10. Juli 2026, abrufbar unter https://netzpolitik.org/2026/geheimdienstreform-zeitenwende-fuer-spione/.

[42] Vgl. BVerfGE 154, 152 Rn. 155 f., 171 f. – Strategische Ausland-Ausland-Fernmeldeaufklärung.

[43] BVerfGE 154, 152 Rn. 263 f. – Strategische Ausland-Ausland-Fernmeldeaufklärung.

[44] So auch sehr strikt BVerfGE 154, 152 Rn. 171, 253, 304 – Strategische Ausland-Ausland-Fernmeldeaufklärung.

dem Aufspüren von Kommunikationsnetzten dienen sollen;[45] dann besteht ein erhebliches **Risiko der Re-Identifikation**.

d) Auslandskommunikation

54 § 33 Abs. 1 BNDG-E erlaubt den Zugriff auf Metadaten der Auslandskommunikation bereits dann, wenn dies nur zur Auslandsaufklärung erforderlich ist. Dies wird der **besonderen Sensibilität von Metadaten** nicht gerecht. Diese geben erhebliche Aufschlüsse über das Leben, die Persönlichkeit und das Umfeld der betroffenen Personen und eignen sich besonders zu einer automatisierten Auswertung.

e) Qualifizierte Inlandskommunikation

55 § 34 BNDG-E lässt den Zugriff auf Metadaten und Inhaltsdaten der qualifizierten Inlandskommunikation zu, wenn eine erhebliche Bedrohung vorliegt. Hier macht sich die Unbestimmtheit der Bedrohungsstufen nach §§ 3, 4 BNDG-E bemerkbar; aufgrund der Vielzahl an Indizien umfassen sie nahezu alles. Anders als anhand der Gefahrenquellen des G-10-Gesetzes ist es kaum noch möglich, anhand dieser Regelungen die Gebiete einzugrenzen, auf die sich die Überwachung der qualifizierten Inlandskommunikation beziehen kann.

3. Ankauf von Daten (ADINT)

56 An mehreren Stellen erwähnt die Begründung den Ankauf von Daten durch den BND. Hintergrund ist die zunehmende Praxis von Sicherheitsbehörden, Daten anzukaufen, die vor allem zu Werbezwecken (daher die Kurzbezeichnung „ADINT“)[46] gesammelt worden sind.[47] Damit wird deutlich, dass es sich um einen üblichen *modus operandi* des BND handelt. Offenbar werden die Daten als wenig sensibel eingestuft, weil fälschlich angenommen wird, sie seien allgemein zugänglich. Dies ist erstens nicht zutreffend, weil sie zwar käuflich sind, aber nicht frei abrufbar; zweitens sind auch allgemein zugängliche Daten nicht schutzlos. Es stellt sich zudem die Frage, ob die Daten durch die Datenverkäufer (Data Broker) rechtmäßig verarbeitet worden sind. Im Entwurf **fehlt eine gesetzliche Regelung**.[48]

---

[45] Referentenentwurf, S. 488.

[46] Umfassend *Wetzling/Ruckerbauer*, Nachrichtendienstliche Datenkäufe – Ein Minusgeschäft für Deutschland und Taiwan? (2026); *dies.*, Data bought, rights ignored: European intelligence services' use of commercially sourced data (2026).

[47] Referentenentwurf, S. 392 (zu § 5 Abs. 4 BNDG-E zur Nutzung einer Legende), S. 512 (zur Weiterverwendung allgemeinzugänglicher Daten nach § 52 Abs. 2 BNDG-E), S. 557 (automatische Übermittlung nach § 88 Abs. 2 BNDG-E) und S. 640 (zu § 37 UKRG-E).

[48] So zur bisherigen Rechtslage schon *Wissenschaftliche Dienste des Deutschen Bundestages*, Rechtliche Voraussetzungen und Grenzen des behördlichen Ankaufs von

57 Diese wäre jedoch notwendig, weil sich der Ankauf auch auf sensible Daten beziehen kann (z.B. Standortdaten, Vorlieben, Nutzungsverhalten im Internet). Dabei muss der **Gedanke des hypothetischen Ersatzeingriffs** berücksichtigt werden: Hätte der Staat diese Daten auch selbst erheben dürfen? Dabei wird zu berücksichtigten sein, ob der Verkäufer die Daten rechtmäßig verarbeitet und wie er sie gewonnen hat, welcher Personenkreis betroffen ist – häufig handelt es sich um Massedaten – und wie Kontrolle und Rechtsschutz gewährleistet werden können. Anderenfalls **droht die Umgehung der gesetzlichen und verfassungsrechtlichen Eingriffsvoraussetzungen**, die an die staatliche Datenerhebung zu stellen wären.

4. KI-Analyse

a) Einsatz von KI-Anwendungen

58 Zentrale Regelung für den Einsatz von KI-Anwendungen ist § 52 Abs. 4 S. 2 BNDG-E. Die Regelung trägt den besonderen Herausforderungen des Einsatzes von KI-Anwendungen nicht annähernd Rechnung und ist **überraschend unterkomplex**. Sie erlaubt den Einsatz von KI-Anwendungen im größtmöglichen Umfang, insbesondere durch selbstlernende Systeme. Solche Systeme bergen in besonderem Maße das Risiko, dass sich die Anwendungen im Verlauf des Lernprozesses immer mehr von der ursprünglichen menschlichen Programmierungen lösen und ihre Ergebnisse so immer schwerer nachzuvollziehen sind.[49] Die Nachvollziehbarkeit wird aber umso wichtiger, wenn auf Basis einer solchen Analyse neue Erkenntnisse über Unbeteiligte gewonnen werden, Verhaltens-, oder Persönlichkeitsprofile oder gar Bedrohungsanalysen automatisiert erstellt werden (§ 53 Abs. 2 Nr. 3, Abs. 4 Nr. 2 bis Nr. 4 BNDG-E).[50] Dies wiegt umso schwerer als bis auf „Stichproben“ keine Maßnahmen zur Sicherung der Qualität, Nachvollziehbarkeit und Vermeidung von Diskriminierung vorgesehen sind.[51] KI-Anwendungen müssen bereits vor ihrer Anwendung ausreichend getestet werden – und zwar mit technischem Sachverstand und nicht nur juristischem, wie es § 52 Abs. 4 S. 5 BNDG-E vorschlägt (vgl. Art. 12 und 16 der KI-Konvention des Europarates). Eine spezielle Kontrolle durch den UKR ist nicht vorgesehen; hier zeigt sich exemplarisch, dass die technische Expertise

---

personenbezogenen Daten aus Werbedatenbanken, WD 3 - 3000 - 065/25, 27. November 2025.

[49] BVerfGE 165, 363 Rn. 100 – Automatisierte Datenanalyse; schon für weniger komplexe Algorithmen BVerfGE 154, 152 Rn. 192 – Nachrichtendienstliche Ausland-Ausland-Fernmeldeüberwachung.

[50] Vgl. BVerfGE 165, 363 Rn. 96 ff., 121 – Automatisierte Datenanalyse.

[51] Zum besonderen Eingriffsgewicht

der BfDI fehlt. Kurzum: Es **fehlt eine robuste KI-Governance**, um auf die Herausforderungen durch den Einsatz zu reagieren.

59 Es ist zudem vollkommen **unklar, welcher Datenbestand**[52] jeweils in die Analyse einbezogen werden darf, ob diese Daten dauerhaft zusammengeführt werden dürfen (dies legen die Abrufregelungen für Auswerteprodukte nach § 53 BNDG-E nahe) und welche **Trainingsdaten** dem KI-Modell zugrunde liegen.[53] Lediglich § 60 Abs. 3 BNDG-E enthält hierzu nur eine unklare Regelung zu Forschungsdaten. Bedenklich ist in diesem Zusammenhang § 52 Abs. 2 Nr. 1 BNDG-E, der eine Weiterverarbeitung von allgemeinzugänglichen Daten ohne Schranken erlaubt; eine flächendeckende Auswertung des Internets – quasi eine **„Online-Rasterfahndung"** – mittels KI ist damit nicht ausgeschlossen. Es sind auch keine Vorkehrungen getroffen, wie das besondere Gewicht der Erhebung von **Daten durch nachrichtendienstliche Mittel** bei der Verarbeitung durch die KI-Anwendung erhalten bleibt.[54]

60 Bereits diese Punkte zeigen, dass es sich beim Einsatz von KI-Anwendungen, wie sie § 52 Abs. 4 BNDG-E ermöglicht, es sich um einen **besonders gewichtigen Eingriff** handelt. Das BVerfG hat einen so gewichtigen Einsatz von künstlicher Intelligenz durch die Polizei nur zugelassen, wenn zumindest eine konkretisierte Gefahr vorliegt. Es lassen sich in der Rechtsprechung des Bundesverfassungsgerichts zwar Ansatzpunkte finden, dass es für Nachrichtendiensttätigkeiten eine andere Eingriffsschwelle akzeptieren würde. Bereits für einen weit weniger grundrechtsintensiven Einsatz von KI hat es jedoch „ein wenigstens der Art nach konkretisiertes und absehbares Geschehen verlangt."[55] Diesen Anforderungen wird der Entwurf nicht annähernd gerecht. Die Verfasser ignorieren sogar das besondere Eingriffsgewicht einer automatisierten Weiterverarbeitung und eines Einsatzes von KI-Anwendungen; so dürften keine höheren Anforderungen an die Weiterverarbeitung als an die Erhebung zu stellen sein, sonst die Erhebungsbefugnis ins Leere liefe. Dies sieht das BVerfG in seiner Rechtsprechung anders.

b) Verwendung von KI-Analysen

61 Der Entwurf wählt einen neuen Ansatz, in dem er zwischen der Verarbeitung von Daten durch KI-Anwendungen einerseits und dem Abruf von

---

[52] BVerfGE 165, 363 Rn. 78, 116 – Automatisierte Datenanalyse
[53] BVerfGE 165, 363 Rn. 109 – Automatisierte Datenanalyse.
[54] Zum besonderen Gewicht der Verarbeitung dieser Daten in diesem Zusammenhang BVerfGE 165, 363 Rn. 118 – Automatisierte Datenanalyse; BVerfGE 156, 11 Rn. 113 – Antiterrordateigesetz II.
[55] BVerfGE 156, 11 Rn. 119 – Antiterrordateigesetz II.

Auswertungsprodukten andererseits unterscheidet. Positiv an diesem Ansatz ist, dass dies erlaubt nach den unterschiedlichen grundrechtlichen Auswirkungen zu differenzieren. Es besteht allerdings die Gefahr, dass durch diese Zweiteilung dem grundrechtlichen Gewicht der Verarbeitung durch die KI zu wenig Beachtung geschenkt wird.

62 Auch in seiner konkreten Ausgestaltung wird die Regelung nicht den verfassungsrechtlichen Anforderungen gerecht. Der Entwurf unterscheidet hier – in Anlehnung an die Stufensystematik der §§ 2 ff. BNDG-E – zwischen verschiedenen Eingriffsintensitäten. Wenn eine KI-Analyse bereits auf der niedrigsten Stufe zulässig ist (§ 53 Abs. 2 und Abs. 3 BNDG-E), ist dies nicht verhältnismäßig. Gleiches gilt für Analysen zu unbescholtenen Personen, die dadurch in den Fokus des BND rücken sowie Verhaltens- und Persönlichkeitsprofilen und personenbezogenen Vorhersagen und Empfehlungen (§ 53 Abs. 4 Nr. 2 bis 4 BNDG-E). Hierbei handelt es sich um eine Form des *predictive policing* und damit um einen sehr schweren Grundrechtseingriff,[56] der allenfalls auf der höchsten Stufe zulässig sein könnte.

63 Der Entwurf sieht keine Regelungen zur Überprüfung der Auswerteprodukte durch einen Menschen vor. Eine automatisierte Veranlassung von Maßnahmen ist zwar auf die Fälle des § 53 Abs. 7 BNDG-E begrenzt. Nicht ausgeschlossen ist aber ein zu großes Vertrauen auf die KI-Analyse („automation bias“), dem durch Verfahrensregelungen (z.B. dokumentierte Plausibilitätsprüfung) entgegen gewirkt werden muss.

c) Digitale Souveränität

64 Es ist zu begrüßen, dass der Entwurf das Ziel der digitalen Souveränität bei der Auswahl der Software zumindest sieht und damit auf die kritische Diskussion um Anbieter wie Palantir Technologies reagiert. § 52 Abs. 5 BNDG-E sieht eine „Anschaffungssubsidiarität“[57]; danach ist eine Beschaffung von einer privaten oder staatlichen Stelle in einem Drittstaat nicht ausgeschlossen, wenn es in der EU keine ebenso geeigneten Angebote gibt und eine Eigenentwicklung ausgeschlossen ist. Damit ist eine Nutzung von Software in Drittstaaten nicht ausgeschlossen. Für diesen Fall sind keine gesetzlichen Vorgaben vorgesehen, um die Qualität und Vertrauenswürdigkeit des Anbieters und vor allem der Software sicher zu stellen (z.B. durch Prüfung des Quellcodes).[58] Auch dürfte allein das Abstellen auf den Sitz des Anbieters nicht ausreichen. Handelt es sich z.B. um ein Tochterunternehmen einer

[56] BVerfGE 165, 363 Rn. 96 ff., 100, 121 – Automatisierte Datenanalyse
[57] Referentenentwurf, S. 532.
[58] Siehe aber BVerfGE 165, 363 Rn. 100 – Automatisierte Datenanalyse zu den Gefahren.

ausländischen Muttergesellschaft, könnten ausländische Stellen an diese Herausgabeverlangen stellen und so Zugriff auf Daten des BND erhalten.[59]

5. Biometrischer Abgleich

65 § 5 Abs. 3 BNDG-E erlaubt den Abgleich mit biometrischen Daten im Internet. Hierbei handelt es sich um eine neuartige Befugnis mit **erheblicher Streubreite**. Ausreichend ist nach dem Entwurf bereits die Erforderlichkeit für die Auslandsaufklärung; dies ist die niedrigste Zugriffshürde und damit eine zu niedrige Eingriffshürde. Sie geht offenbar von der Fehlannahme aus, dass Daten im Internet nicht schützenswert sind. Es ist auch nicht sichergestellt, dass grundrechtssensible Erhebungssituationen berücksichtigt werden, z.B. Aufnahmen von der Demonstration oder sexualisierte Darstellungen oder Deepfakes.

66 Bedenklich ist die ausdrückliche Möglichkeit, auf ausländische private oder staatliche Stellen zurückzugreifen. Es besteht so die Gefahr, dass hierfür kommerzielle Anbieter genutzt werden, deren Tätigkeit nicht im Einklang mit dem deutschen oder europäischen Recht steht. Eine staatliche Stelle wie der BND darf jedoch die **gesetzlichen Vorgaben nicht durch „Outsourcing" umgehen**.

67 Soweit beim Abgleich nach § 5 Abs. 3 BNDG-E **künstliche Intelligenz** zum Einsatz kommt, sind die Vorgaben an deren Einsatz auch hier zu beachten, etwa zur Vermeidung von Bias. Angesichts der technischen Entwicklung und der Schwere dieses noch neuartigen Instruments ist eine **Prüfung durch den UKR alle zwei Jahre nicht häufig genug**. Sie kann auch nur erfolgen, wenn der Einsatz dieses Instruments ausreichend dokumentiert ist; dies ist bisher nicht vorgesehen.

6. Zugriff auf Videoüberwachungsanlagen

68 § 11 Abs. 4 und § 15 BNDG-E ermächtigen den BND zum Zugriff auf staatliche und private Videoüberwachungsanlagen des öffentlichen Raumes – durch Zugang zu Anlagen, Aushändigung der Aufnahmen oder durch Zugriff in Echtzeit. Die Regelung gilt nur für Betreiber von solchen Anlagen im Inland (§ 16 Abs. 2 BNDG-E). Vergleichbare Regelungen haben auch Eingang in Landesverfassungsschutzgesetze gefunden (z.B. § 20 VSG NRW).

---

[59] Vgl. 31. Bericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, S. 40 (zum PolG NRW); zum rechtlichen Hintergrund ausführlich *Anheier/Nau,* ZD 2025, 557 (auf Basis eines Gutachtens für das Bundesministeriums des Innern und für Heimat); *Schantz*, CR 2026, 91 Rn. 33 jeweils m.w.N.

69 Im Vergleich zu den landesrechtlichen Regelungen (z.B. § 20 VerfSchG NRW) sind die Eingriffsvoraussetzungen für den BND ausgesprochen niedrig. Es handelt sich in der Systematik des Entwurfs noch nicht einmal um eine nachrichtendienstliche Maßnahme, was etwa den Kreis der Zielpersonen etwas eingrenzen würde; ausreichend sind tatsächliche Anhaltspunkte, dass der Zugriff für die Auslandsaufklärung erforderlich ist. Das sind – abgesehen von der Generalklausel zur Informationserhebung nach § 5 Abs. 1 BNDG-E – die niedrigsten Anforderungen, die das Gesetz an Informationserhebungen stellt. Dies wird dem Gewicht des Eingriffs nicht gerecht. Er erlaubt potentiell den Zugriff auf jede Kamera im öffentlichen Raum (auch private Kameras in Autos, Drohnen oder Handys) und erfasst damit zwangsläufig eine Vielzahl unbeteiligter Personen in verschiedensten Situationen, z.B. Versammlungen. Es **fehlt auch an einer Vorabkontrolle** durch den UKR. Der Entwurf lässt schließlich viele Fragen unbeantwortet, etwa wie der Zugriff in Echtzeit sicher gewährleistet soll. Er verstößt zudem gegen das Doppeltürmodell, weil § 4 Abs. 3 S. 3 BDSG Betreibern von Videoüberwachungsanlagen die Übermittlung der personenbezogenen Daten bzw. die Zugangsgewährung nicht erlaubt.[60]

7. Allgemeine Regelungen zu nachrichtendienstlichen Mitteln

a) Erprobungsklausel

70 § 19 Abs. 1 BNDG-E erlaubt für vier Jahre die Erprobung neuer nachrichtendienstlicher Mittel, die von der Eingriffstiefe soweit reichen können wie eine Online-Durchsuchung oder eine Telekommunikationsüberwachung. Dies ist mit dem Gesetzesvorbehalt und der Wesentlichkeitstheorie nicht vereinbar, denn über solche Maßnahmen muss der Gesetzgeber entscheiden.

b) Schutz von Berufsgeheimnisträgern

71 Unzureichend ausgestaltet ist der Schutz der Berufsgeheimnisträger nach § 22 BNDG-E, auch wenn das BVerfG dem Gesetzgeber hier größere Spielräume gibt als im Inland, wo – mit Ausnahme von Journalisten – ein absoluter Schutz der Vertraulichkeitsbeziehung gilt. Da die Befugnisse des **BND, im Inland** tätig zu werden erheblich erweitert werden sollen, muss sichergestellt werden, dass Vertraulichkeitsbeziehungen im Inland oder die Deutsche bzw. Inländer betreffen, den üblichen strengen Maßstäben unterliegen.

72 Der Schutz der Vertraulichkeitsbeziehungen wird zudem zu stark eingeschränkt. So knüpft § 22 Abs. 2 S. 1 Nr. 1 BNDG-E an verschiedene

[60] Vgl. BVerfGE 155, 119 Rn. 201 – Bestandsdatenauskunft II.

Formen der Verstrickung und Verantwortung für Bedrohungen an. Ausreichend ist es aber bereits, wenn dieser Verdacht in Bezug auf Hilfspersonen nach § 22 Abs. 1 S. 3 BNDG-E besteht. Es ist nicht gerechtfertigt, den Schutz einer Vertraulichkeitsbeziehungen zwischen Anwalt und Mandant entfallen zu lassen, nur weil die Rechtsanwaltsfachangestellte oder der IT-Dienstleister eine solche Verstrickung aufweisen. Hier fehlt die vom BVerfG zwingend vorgesehene **Abwägung im Einzelfall**.[61] Dies ist auch der Fall, soweit der Entwurf die Vertraulichkeitsbeziehungen unter einen Generalvorbehalt des Vorliegens einer erheblichen Gefahr für ein besonders gewichtiges Rechtsgut stellt. Es **fehlt zudem eine gerichtsähnliche Vorabkontrolle** für die Erhebung von Daten aus einer Vertraulichkeitsbeziehung;[62] diese ist bisher nur für die Weiterverarbeitung vorsehen (§ 97 Abs. 3 S. 1 Nr. 1 i.V.m. § 22 Abs. 3 BNDG-E).

III. Aufsicht und Kontrolle

73 Hinsichtlich der nachrichtlichen Kontrolle durch den UKR wird auf die Stellungnahme der Gesellschaft für Freiheitsrechte e.V. (GFF) verwiesen. Ich möchte nur auf wenige Punkte eingehen.

1. Entmachtung der BfDI

74 Es ist bedauerlich, dass der BfDI die operative Tätigkeit des BND nicht mehr beaufsichtigen wird. Sie hatte in diesem Bereich große juristische und technische Expertise aufgebaut. Gerade die technische Expertise wird angesichts der komplexen technischen Befugnisse des BND fehlen. Der UKR gleicht dies nicht aus, z.B. durch technische Sachverständige oder als Amicus Curiae (*tech amicus)*.

2. Reform des UKR

75 Es ist zu begrüßen, dass auch Personen ohne Hintergrund in der Justiz oder einer Sicherbehörde in das gerichtliche Kontrollorgan gewählt werden können. Die Ausnahmen sind zu sehr auf die Mitglieder der G-10-Kommission gemünzt. Dem Gremium könnte eine größere Pluralität an beruflichen Hintergründen helfen, seine Aufgabe zu erfüllen. Es wäre auch denkbar, dass nicht alle Mitglieder in Vollzeit tätig sein müssten; dies würde die Mitgliedschaft im UKR auch attraktiver machen. Nach dem Wegfall der

[61] BVerfGE 154, 152 Rn. 194, 195 – Strategische Ausland-Ausland-Fernmeldeaufklärung.
[62] BVerfGE 154, 152 Rn. 194 – Strategische Ausland-Ausland-Fernmeldeaufklärung.

G-10-Kommission fehlt ein Aufsichtsgremium mit einem politisch-juristischen Hintergrund.

76 Zu überprüfen wäre, warum nach § 2 Abs. 1 UKRG-E die Kontrolle sich allein auf die Verarbeitung personenbezogener Daten erstreckt. Es ist wenig plausibel, dass der UKR keine allgemeine Rechtskontrolle durchführen darf, sondern sich auf einen Aspekt beschränken muss.

****