



Ausschussdrucksache 21(4)233 D
vom 12. Oktober 2026

Schriftliche Stellungnahme

von Franziska Görlitz, Gesellschaft für Freiheitsrechte e.V., Berlin vom
10. Oktober 2026

zu dem

- a) Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts

BT-Drucksachen 21/7868, 21/8295

und

- b) Antrag der Abgeordneten Stefan Keuter, Dr. Malte Kaufmann, Kay Gottschalk, weiterer
Abgeordneter und der Fraktion der AfD

*Stärkung der nationalen Souveränität und der operativen Fähigkeiten des
Bundesnachrichtendienstes*

BT-Drucksache 21/8114

Gesellschaft für Freiheitsrechte e.V. · Boyenstraße 41 · 10115 Berlin

Deutscher Bundestag
Innenausschuss
Platz der Republik 1
11011 Berlin

Berlin, den 10. Oktober 2026

Betreff: Stellungnahme zur öffentlichen Anhörung am 12. Oktober 2026

Sehr geehrte Damen und Herren,

als Stellungnahme im Rahmen der öffentlichen Anhörung als Sachverständige im Innenausschuss zu den BT-Drucksachen 21/7868, 21/8295 und der BT-Drucksache 21/8114 übersende ich die Stellungnahme der Gesellschaft für Freiheitsrechte e.V. (GFF) zum Referentenentwurf eines Gesetzes zur Reform des Nachrichtendienstrechts im Rahmen der Verbändebeteiligung vom 3. Juli 2026. Ebenso übersende ich die Stellungnahme von Rechtsanwalt Dr. Peter Schantz, Ministerialdirektor a.D. im Rahmen der Verbändebeteiligung zum Referentenentwurf. Diese ist auf Bitte der GFF entstanden und enthält eine eigenständige wissenschaftliche Bewertung des Entwurfs zum BND-Gesetz sowie der damit zusammenhängenden Regelungen. Herr Rechtsanwalt Dr. Schantz ist mit der Übersendung einverstanden.

Auf Grund der nur geringfügigen Änderungen zwischen Referenten- und Regierungsentwurf treffen die Stellungnahmen überwiegend auch auf den vorliegenden Entwurf zu. Hingewiesen sei auf die Änderungen zur Übermittlungspflicht des BSI an den BND, § 12 Abs. 4 Nr. 2 BNDG-E, auf die Änderungen an § 32 Abs. 2 BNDG-E sowie auf die Neubezeichnung des Besonderen Feststellungsfalls, § 125 BNDG-E im Regierungsentwurf.

Mit freundlichen Grüßen

Franziska Görlitz
Juristin und Verfahrenskoordinatorin

14. Juli 2026

Stellungnahme

zum Referentenentwurf eines Gesetzes zur Reform des Nachrichtendienstrechts

im Rahmen der Verbändebeteiligung vom 3. Juli 2026

von Franziska Görlitz, Volljuristin und Verfahrenskoordinatorin bei der Gesellschaft für
Freiheitsrechte e.V.

Die Gesellschaft für Freiheitsrechte setzt sich mit juristischen Mitteln für die Grund- und Menschenrechte ein. Sie hat die Verfassungsbeschwerden initiiert und koordiniert, die zu den Entscheidungen des Bundesverfassungsgerichts zum Bayerischen Verfassungsschutzgesetz und zum Hessischen Verfassungsschutzgesetz führten. Diese Entscheidungen bilden unter anderem den Anlass für das vorliegende Gesetzgebungsverfahren.

Der vorliegende Gesetzesentwurf fasst das Nachrichtendienstrecht in Deutschland umfassend neu. Aufgrund der grundlegenden Entscheidungen des Bundesverfassungsgerichts werden das Bundesverfassungsschutzgesetz (BVerfSchG-E) und das Bundesnachrichtendienstgesetz (BNDG-E) grundlegend neu gefasst. Die bisher im G 10 geregelten Befugnisse zur Überwachung von Post und Telekommunikation unter Eingriff in Art. 10 GG werden nun jeweils in den einschlägigen Gesetzen des jeweiligen Nachrichtendienstes geregelt. Zum Zwecke der Modernisierung und Anpassung an neuartige Bedrohungen werden die **Überwachungsbefugnisse** der Nachrichtendienste erheblich erweitert, die nicht nur Bedrohungen im Cyberraum begegnen. Vor allem aber werden den Nachrichtendiensten auch **operative Befugnisse**, also **aktive Eingriffs- bzw. Abwehrrechte**, übertragen. Ebenso wird die **Kontrolle der Nachrichtendienste** neu geregelt und beim **Unabhängigen Kontrollrat (UK-Rat)** zentralisiert.

Zusammenfassende Bewertung des Entwurfs:

Die Neufassung und Anpassung des Nachrichtendienstrechts an die verfassungsgerichtliche Rechtsprechung der letzten Jahre ist im Grundsatz zu begrüßen. Die Neuregelungen führen zu mehr Übersicht. Besonders die Einbettung der früheren Überwachungsbefugnisse des G 10 ist gesetzessystematisch sinnvoll.

Jedoch sind **Maßstäbe der bundesverfassungsgerichtlichen Rechtsprechung** an vielen Stellen **nicht eingehalten**. Dies gilt insbesondere im Bereich der **Eingriffsschwellen**, bei verschiedenen **neuen Eingriffsbefugnissen** und im Bereich der Übermittlungsbefugnisse. Die Regelungen greifen unverhältnismäßig in die Grundrechte ein. Der Entwurf ist daher **in weiten Teilen verfassungswidrig**.

Der vorliegende Entwurf führt zudem zu **erheblichen Veränderungen und strukturellen Verschiebungen** nicht nur im System der Nachrichtendienste, sondern **im gesamten Gefüge der Sicherheitsbehörden** in Deutschland. Die strenge **Trennung zwischen** den nur überwachenden, aber nicht operierenden **Nachrichtendiensten** und der dann eingreifenden **Polizei** wird **eingерissen**. Zur Vermeidung von Schutzlücken soll nun **operatives Handeln** sowohl des BND als auch des BfV möglich sein. Die Regelungen brechen mit dem Charakter der reinen Nachrichtendienste und führen zu einer „**Verpolizeilichung**“. Sie wecken Begehrlichkeiten für immer neue operative Befugnisse, da sich immer neue „Lücken“ finden und vermeintliche Eingriffsbedarfe begründen lassen. Vor allem aber **entziehen** sie die **Grundlage** für die **bisherigen modifizierten Anforderungen an** nachrichtendienstliches Handeln. **Ein Geheimdienst, der operativ tätig wird, darf verfassungsrechtlich nicht wie bislang unter geringeren Voraussetzungen schon im Gefahrenvorfeld überwachen**. Operative Eingriffsbefugnisse des BND, also aktive Maßnahmen des BND im Ausland, werfen auch die Frage auf, ob hier wie bei Auslandseinsätzen der Bundeswehr der Parlamentsvorbehalt gilt. Darüber hinaus verwässert der Entwurf auch die **Trennung der Geheimdienste untereinander**, da dem **BND** durch Nacheile-Regelungen nun auch **Überwachungsbefugnisse im Inland** gegeben werden. Auch diese Regelungen brechen die bisherige Struktur der Nachrichtendienste grundlegend auf.

Zudem **zentralisiert** der Entwurf die **Kontrolle der Nachrichtendienste** im Wesentlichen **beim UK-Rat**. Dass dem*der **BfDI die datenschutzrechtliche Aufsicht** über die Dienste **weitgehend entzogen** wird, schwächt die grundrechtsschützende Kontrolle erheblich. Zudem **fehlt** dem UK-Rat die **technische Expertise** und der **personelle Unterbau**, um die Datenschutzkontrolle der neuen komplexen **technischen Befugnisse** tatsächlich gewährleisten zu können.

Inhaltsverzeichnis

A. Regelungen des Bundesverfassungsschutzgesetzes	3
I. Eingriffsschwellen, § 3 Abs. 7 f. BVerfSchG-E	3
II. Besonders gewichtige Rechtsgüter, § 3 Abs. 9 BVerfSchG-E.....	6
III. Besondere Befugnisse und nachrichtendienstliche Mittel	6
1. Auskunftersuchen, §§ 11 ff. BVerfSchG-E	6
2. Zugriff auf Einrichtungen der Videoüberwachung, § 15 BVerfSchG-E	6
3. Eingriffe in informationstechnische Geräte bzw. Systeme, §§ 23 ff. BVerfSchG-E	7
4. Qualifizierte Auswertung bzw. automatisierte Datenanalyse, § 37 BVerfSchG-E	12
5. Biometrischer Datenabgleich, § 8 Abs. 1 Satz 2 Nr. 2 BVerfSchG-E	15
6. Datenerhebung bei Dritten und zeugnisverweigerungsberechtigten Personen	17
7. KI-Training, § 36 Abs. 1 Nr. 1 lit. a, Abs. 2 Satz 1 Nr. 5 BVerfSchG-E	18
IV. Operative Befugnisse, §§ 60 ff. BVerfSchG-E	19
V. Übermittlungsvorschriften, §§ 45 ff. BVerfSchG-E	21
B. Nachrichtendienstliche Kontrolle und Transparenz.....	25

Bewertung der Regelungen im Einzelnen

Die vorliegende Stellungnahme ist aufgrund des Umfangs des vorliegenden Entwurfs und der kurzen Stellungnahmefrist auf **ausgewählte Aspekte** vor allem zum Entwurf des neuen Bundesverfassungsschutzgesetz **beschränkt**. Eine umfassende Begutachtung der 700-seitigen Neufassung des gesamten Nachrichtendienstrechts kann in der Kürze der zur Verfügung stehenden Zeit nicht erfolgen. Zur Bewertung des Entwurfs zum Bundesnachrichtendienstgesetz sei auf die **Stellungnahme von Rechtsanwalt Dr. Peter Schantz, Ministerialdirektor a.D.** im Rahmen der Verbändebeteiligung zum vorliegenden Entwurf verwiesen. Diese ist auf Bitte der GFF entstanden und enthält eine eigenständige wissenschaftliche Bewertung des Entwurfs zum BND-Gesetz sowie der damit zusammenhängenden Regelungen.

A. Regelungen des Bundesverfassungsschutzgesetzes

I. Eingriffsschwellen, § 3 Abs. 7 f. BVerfSchG-E

Die in § 3 Abs. 7 BVerfSchG-E enthaltenen Stufen der Beobachtungsbedürftigkeit genügen den verfassungsrechtlichen Anforderungen nicht. Überwachungsmaßnahmen der Geheimdienste bedürfen einer Eingriffsschwelle zur Rechtfertigung der damit einhergehenden Grundrechtseingriffe. Diese setzt nach dem Bundesverfassungsgericht hinreichende Anhalts-

punkte einerseits dafür voraus, dass eine beobachtungsbedürftige Bestrebung besteht und andererseits dafür, dass die ergriffene Maßnahme im Einzelfall zur Aufklärung geboten ist.¹

Die Beobachtungsbedürftigkeit knüpft der Entwurf nun an den Begriff der Bedrohung (nicht den der Bestrebung an) an. Bedrohungen sind sowohl verfassungsfeindliche Bestrebungen (§ 2 Abs. 1 Nr. 1, 2 BVerfSchG-E) als auch sicherheitsgefährdende (§ 2 Abs. 1 Nr. 3 lit. a), geheimdienstliche (§ 2 Abs. 1 Nr. 3 lit. b) Tätigkeiten und funktionsgefährdende (§ 2 Abs. 4) Tätigkeiten.

Für eine **erhebliche Beobachtungsbedürftigkeit** sind nach **§ 3 Abs. 7 Satz 1 BVerfSchG-E** tatsächliche Anhaltspunkte dafür erforderlich, dass die Bedrohung geeignet ist, die Schutzgüter des § 2 Abs. 1 BVerfSchG zu beeinträchtigen.

Gemäß § 3 Abs. 7 Satz 2 BVerfSchG-E ist eine solche Eignung anzunehmen und damit unwiderleglich vermutet, wenn zur Zielverfolgung Straftaten begangen werden. Da keine weiteren Erfordernisse an die Straftaten gestellt werden, begründen **auch Bagatelldelikte stets** eine erhebliche Beobachtungsbedürftigkeit, die zu intensiven Grundrechtseingriffen ermächtigt. Dieser Automatismus ist unverhältnismäßig. Nicht jede Straftat begründet zwangsläufig eine Eignung, die Schutzgüter des § 2 Abs. 1 BVerfSchG-E zu beeinträchtigen. Dies gilt insbesondere für geringfügige Taten wie das Kleben von Stickern oder das Abreißen von Plakaten, gerade im Rahmen von politischem Protest. In seiner Entscheidung zum Hessischen Verfassungsschutzgesetz hat das Bundesverfassungsgericht unwiderlegliche Vermutungen für eine erhebliche Beobachtungsbedürftigkeit beanstandet. Der Gesetzgeber schreibt hier bei der Begehung von Straftaten eine unwiderlegbare Vermutung für eine Beobachtungsbedürftigkeit fest, statt zur Einhaltung des Grundsatzes der Verhältnismäßigkeit Regelbeispiele² vorzusehen. So ist nicht sichergestellt, dass tatsächlich hinreichende Anhaltspunkte bestehen, dass Verfassungsschutzgüter auch konkret bedroht sind und dass das gegen sie gerichtete Handeln erfolgreich sein kann.³ Die Begehung von Straftaten sollte daher nur als Indiz bzw. Vermutung für eine erhebliche Beobachtungsbedürftigkeit formuliert werden.

Ebenso wenig genügt die Regelung des § 3 Abs. 7 Satz 3 Nr. 1 lit. d, Satz 4 BVerfSchG-E den Anforderungen an eine verfassungsschutzspezifische Eingriffsschwelle. Als Regelbeispiel wird herangezogen, wenn die Vorgehensweise bei der Zielverfolgung planmäßig verschleiern ist. Das Bundesverfassungsgericht hat zwar entschieden, dass die Beobachtungsbedürftigkeit auch vom

¹ BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17, BVerfGE 162, 1, Rn. 182 ff.

² Zur Zulässigkeit eines solchen Regelbeispiels: Vgl. BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22, BVerfGE 169, 130, Rn. 154.

³ Vgl. BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22, BVerfGE 169, 130, Rn. 151 f.

Maß der Abschottung abhängen kann.⁴ Es hat jedoch zugleich auf kritische Stimmen verwiesen,⁵ die darauf hinweisen, dass Maßnahmen zur IT-Sicherheit oder zum Datenschutz als Abschottung betrachtet werden können. Eine Verschleierung kann zudem dem legitimen Ziel dienen, sich vor Angriffen des politischen Gegners oder vor ausländischen Geheimdiensten zu schützen. Gerade besonders schutzbedürftige Personen, wie Aktivist*innen oder Journalist*innen, die Bedrohungen ausgesetzt sind, ergreifen derartige Maßnahmen. Dieses Verhalten ist in diesen Fällen als grundrechtlich geschützter Eigenschutz anzusehen und darf nicht als Indiz für eine Beobachtungsbedürftigkeit herangezogen werden. Die vorgesehene Regelvermutung, wie sie der Gesetzentwurf aufstellt, sollte daher gestrichen, jedenfalls präzisiert werden.

Auch die Beispiele des § 3 Abs. 7 Satz 3 Nr. 2, 3 BVerfSchG-E sollten konkretisiert und begrenzt werden. Nach der Rechtsprechung des Bundesverfassungsgerichts genügt als Anhaltspunkt für eine erhebliche Beobachtungsbedürftigkeit nicht schon, dass eine Bestrebung „im erheblichen Umfang gesellschaftlichen Einfluss auszuüben sucht“.⁶ Daher bedarf es zum einen einer Beschränkung bzw. Präzisierung des „Umfangs“ der gesellschaftlichen Einflussnahme in § 3 Abs. 7 Satz 3 Nr. 3 BVerfSchG-E. In § 3 Abs. 7 Satz 3 Nr. 2 BVerfSchG-E kann allein das „Aktionspotenzial“ und damit die Fähigkeiten und -möglichkeiten zu konkreten Handlungen einer Bedrohung eine Potenzialität nicht ohne weiteres begründen. Es bedarf einer Konkretisierung der „Aktionen“ unmittelbar zur Beeinträchtigung der Schutzgüter nach § 2 Abs. 1 BVerfSchG-E.

§ 3 Abs. 8 BVerfSchG-E definiert die Eingriffsschwelle der **besonders erheblich beobachtungsbedürftigen Bedrohung**. Positiv zu bewerten ist hier, dass legalistische Bestrebungen nicht zu den besonders erheblich beobachtungsbedürftigen Bedrohungen zählen und daher nicht mit besonders eingriffsintensiven Mitteln überwacht werden sollen.

Zu weitgehend ist jedoch § 3 Abs. 8 Nr. 1 lit. b BVerfSchG-E, der pauschal Ersatzorganisationen von verbotenen Vereinen erfasst. Solche Ersatzorganisationen haben nicht zwingend eine gesteigerte Potentialität. Der Verstoß gegen ein Vereinsverbot erschüttert entgegen der Gesetzesbegründung nicht automatisch das "Vertrauen der Bevölkerung in die Funktionsfähigkeit der Herrschaft des Rechts" (S. 246 des Entwurfs). Unzulässig ist es auch, pauschal von einem solchen Vertrauensverlust darauf zu schließen, dass die Sicherheit des Bundes qualifiziert gefährdet wäre. Verstöße gegen behördliche und gesetzliche Verbote, wie sie in Deutschland tagtäglich vorkommen, gefährden nicht automatisch das "Vertrauen in die Funktionsfähigkeit der Herrschaft des Rechts" und die "Sicherheit des Bundes".

4 BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17, BVerfGE 162, 1, Rn. 196.

5 BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17, BVerfGE 162, 1, Rn. 196.

6 BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17, BVerfGE 162, 1, Rn. 155 f.

Die Einwände gegen die vorgesehen Eingriffsschwellen wirken sich auch auf die Verfassungsgemäßheit der Spezialbefugnisse aus, die an diese Eingriffsschwellen anknüpfen.

II. Besonders gewichtige Rechtsgüter, § 3 Abs. 9 BVerfSchG-E

In § 3 Abs. 9 Nr. 4 BVerfSchG-E sollte die Öffnung der besonders gewichtigen Rechtsgüter auf „vergleichbare besonders gewichtige Rechtsgüter“ gestrichen werden. Die generelle Öffnung auf vergleichbare Rechtsgüter geht zu weit, gerade weil in der Gesetzesbegründung (S. 248) auch „komplexere Rechtsgüter wie das Kindeswohl“ umfasst gesehen werden. Die Aufnahme vergleichbarer Fälle entgrenzt die Befugnis und stellt ihre Bestimmtheit und Normenklarheit in Frage.

III. Besondere Befugnisse und nachrichtendienstliche Mittel

1. Auskunftersuchen, §§ 11 ff. BVerfSchG-E

Der vorliegende Entwurf qualifiziert Auskunftersuchen des BfV **nicht als nachrichtendienstliche Mittel**, sondern reguliert diese abgetrennt in einem eigenen Unterabschnitt. Dies erfolgt abweichend von anderen Verfassungsschutzgesetzen, beispielsweise dem Bayerischen Verfassungsschutzgesetz.

Dies hat zur Folge, dass für Auskunftersuchen wesentliche Schutzvorschriften zum Einsatz nachrichtendienstlicher Mittel keine Anwendung finden. Konkret sind sowohl allgemeine Schranken (§ 30 BVerfSchG-E) als auch Vorgaben zum Kernbereichsschutz und zum Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger*innen nur im Abschnitt der nachrichtendienstlichen Mittel enthalten. Dabei kommen auch Auskunftersuchen als Maßnahmen der heimlichen Informationsbeschaffung teils ein hohes Eingriffsgewicht zu.

Zudem folgt aus der Systematik, dass auch weniger strenge Voraussetzungen an die Übermittlung von Daten, die mit Auskunftersuchen erhoben wurden, gestellt werden (siehe dazu sogleich A. V.).

Aus Gründen der Verhältnismäßigkeit sind die Auskunftersuchen **daher in den Unterabschnitt 2 als nachrichtendienstliche Mittel** aufzunehmen.

2. Zugriff auf Einrichtungen der Videoüberwachung, § 15 BVerfSchG-E

Als unverhältnismäßig und daher **verfassungswidrig** anzusehen ist die Befugnis des § 15 Abs. 1 BVerfSchG-E, die Verfügungsberechtigte **privater und öffentlicher Videoüberwachungseinrichtungen** verpflichtet, die **Mitbenutzung ihrer Videoüberwachung** zu ermöglichen, **Daten in Echtzeit** an das BfV **auszuleiten** und gespeicherte **Bild- und Tonaufzeichnungen** zu **übermitteln**. Das **Eingriffsgewicht** der nicht einmal als nachrichtendienstliches Mittel kategorisierten Maßnahme ist **enorm**. Die Befugnis erstreckt sich auf die Überwachung des

gesamten öffentlichen Raums. Dadurch weist die Maßnahme eine extrem hohe Streubreite aus. Faktisch alle Menschen, die sich in Deutschland aufhalten, werden von solchen Videoüberwachungen erfasst. Betroffen sind daher nicht nur gezielt observierte Personen, sondern auch alle Menschen, die als Unbeteiligte zufällig von der Überwachung aufgenommen werden. Auch sind die Grundrechte privater Betreiber*innen der Videoüberwachungseinrichtungen betroffen. Dem BfV wird so eine **weitgehend durchgängige Überwachung des öffentlichen Raums** ermöglicht. Dies ist auch unter Berücksichtigung der vorgesehenen Eingriffsschwelle der erheblich beobachtungsbedürftigen Bedrohung **unverhältnismäßig**.

3. Eingriffe in informationstechnische Geräte bzw. Systeme, §§ 23 ff. BVerfSchG-E

§§ 23 ff. BVerfSchG-E ermächtigen das BfV zum „nachrichtendienstlichen Eingreifen“ in informationstechnische Geräte bzw. Systeme. Dabei soll die Differenzierung zwischen den Normen danach erfolgen, ob in ein „privates System“ im Sinne des § 25 Abs.1 Satz 2 BVerfSchG-E eingegriffen wird.

a. Zu unbestimmte Ermächtigung zu Auslesen und Trojaner-Einsatz

Das von §§ 23 ff. BVerfSchG-E gestattete „nachrichtendienstliche Eingreifen“ ermöglicht dem BfV Zugang zu IT-Systemen auf unterschiedlichen technischen Wegen. Die Normen regeln die zulässigen Eingriffsgrundlagen jedoch **unsystematisch** und **nicht ausreichend normenklar**. Sie ermächtigen mangels ausreichender Einschränkungen jeweils sowohl zum Zugriff mit technischen Mitteln auf Geräte bzw. Systeme, die das BfV in seinem Gewahrsam hat (Auslesen) als auch zum Fernzugriff mittels Staatstrojaner.

§ 23 BVerfSchG-E ist zwar mit „Auslesen informationstechnischer Geräte“ überschrieben, während die §§ 25 f. den Titel „(Abgegrenzter) Eingriff in die Integrität privater informationstechnischer Systeme“ tragen. Sowohl in §§ 23 Abs.1 Satz 1, 24 Abs.1 BVerfSchG-E als auch in §§ 25 Abs.1, 26 Abs.1 BVerfSchG-E wird die gestattete Maßnahme als **„nachrichtendienstlich eingreifen“** beschrieben. In § 23 Abs.1 Satz 1 Nr. 1, 2 BVerfSchG-E wird das nachrichtendienstliche Eingreifen legaldefiniert, wobei die „Zugangsverschaffung mit nachrichtendienstlichen Mitteln zum Auslesen gespeicherter personenbezogener Daten“ und das „Auslesen gespeicherter personenbezogener Daten nach a) Zugangsverschaffung nach Nummer 1 oder b) Erhalt des informationstechnischen Geräts von einem ausländischen Nachrichtendienst“ umfasst ist. Unter „Zugangsverschaffung mit nachrichtendienstlichen Mitteln“ in § 23 Abs.1 Satz 1 Nr. 1 BVerfSchG-E ist nach der Begründung (S. 295 des Entwurfs) auch der „elektronische Fernzugang“ umfasst, also auch der Einsatz von **Staatstrojanern**. Daten aus Maßnahmen nach § 25 BVerfSchG-E werden als Informationen aus einer „Online-Überwachung“ bezeichnet (S. 299 des Entwurfs). Jedenfalls ist ein Ausschluss des Einsatzes von Staatstrojanern dem Gesetz nicht zu entnehmen.

Der Gesetzesentwurf enthält eine erstmalige Befugnis des BfV zur Online-Durchsuchung und weitet damit die Befugnisse des BfV erheblich aus. Gleichzeitig stellen die §§ 23 ff. BVerfSchG-E eine Rechtsgrundlage auch für das technische Aufbrechen und Auslesen von Geräten bzw. Systemen dar, die sich bereits im Gewahrsam des BfV befinden. Diese Gleichbehandlung ist zu begrüßen, da der Schutz des IT-System-Grundrechts nicht auf heimliche Zugriffe beschränkt ist⁷. Zudem ist das Eingriffsgewicht des heimlichen Trojaner-Einsatzes mit dem heimlichen Erlangen und Auslesen eines Geräts/Systems durch nachrichtendienstliche Mittel vergleichbar.

Die verschiedenen Eingriffsmöglichkeiten sollten im Wortlaut der Norm mit **Blick auf den Bestimmtheitsgrundsatz jedoch klarer erkennbar gemacht** werden. Ohne die Gesetzesbegründung ist den Normen nicht ohne weiteres zu entnehmen, welche technischen Handlungen „nachrichtendienstliches Eingreifen“ im Sinne des § 23 Abs.1 Nr.1 BVerfSchG-E umfassen, insbesondere, dass auch ein Trojaner-Einsatz möglich ist. Dies gilt insbesondere, da § 23 Abs.1 BVerfSchG-E auf „Geräte“ beschränkt ist, während §§ 24 ff. BVerfSchG-E den Eingriff in „Systeme“ erlauben. Ebenso sollte klargestellt werden, dass den §§ 23 ff. BVerfSchG-E ein **einheitlicher Begriff des „nachrichtendienstlich Eingreifens“** zugrunde liegt.

b. Unzutreffende Abgrenzung anhand „privater“ Nutzung

Die Abgrenzung, ob für einen Trojaner-Einsatz die höheren Hürden der §§ 25 f. BVerfSchG-E greifen, erfolgt daran, ob auf ein **privates informationstechnisches System** im Sinne des § 25 Abs.1 Satz 2 BVerfSchG-E zugegriffen wird. Danach ist ein informationstechnisches System dann privat, wenn „es als eigenes privat genutzt wird und aufgrund seiner technischen Funktionalität allein oder durch technische Vernetzung Daten derart vorhalten kann, dass Umfang und Vielfalt der Daten einen Einblick in wesentliche Teile der Lebensgestaltung der Person oder ein aussagekräftiges Bild der Persönlichkeit ermöglichen.“

Nach der Rechtsprechung des Bundesverfassungsgerichts besteht der Schutz des IT-System-Grundrechts jedoch, „soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt“.⁸ Durch die **zusätzliche Einschränkung** auf eine „private“ Nutzung ist die Definition der privaten informationstechnischen Systeme **enger als der Anwendungsbereich des IT-System-Grundrechts**. Der **Nutzungszweck** ist für den Schutz des IT-System-Grundrechts **nicht entscheidend**. Das Bundesverfassungsgericht hat vielmehr bekräftigt, dass sich nicht nur bei einer

⁷ BVerfG, Beschluss vom 24. Juni 2025 - 1 BvR 2466/19, Rn. 96.

⁸ BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, Rn. 206.

Nutzung für private Zwecke, sondern auch bei einer geschäftlichen Nutzung aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen lässt.⁹

Der Begriff der privaten Nutzung ist zudem **zu unbestimmt**. Die Definition eines privaten informationstechnischen Systems mit einer Nutzung als privates System ist **schon nicht aussagekräftig**. Die Gesetzesbegründung benennt zur Abgrenzung u.a. Fälle, in welchen Systeme nur zur Durchführung der Bedrohung oder für Zwecke oder Tätigkeiten einer Vereinigung betrieben werden (§. 299 des Entwurfs). Dies sei der Fall, wenn Agent*innen für geheimdienstliche Tätigkeiten spezielle Hardware erhielten oder bei der Hardwarenutzung in „professionellen“ extremistischen und terroristischen Zusammenhängen. Die Begrenzung auf eine private Nutzung begründet aber **zahlreiche weitere Grenzfälle**. Dies gilt für gemeinschaftlich genutzte Geräte (z.B. im partnerschaftlichen, familiären oder freundschaftlichen Kontext), für beruflich genutzte bzw. dienstlich zur Verfügung gestellte Geräte sowie Leihgeräte. Sowohl bei gemischter Nutzung von Systemen als auch bei gemeinschaftlicher Mitnutzung können ebenso je nach Umfang und Art der Daten auch schon die Gefahren eintreten, vor denen das IT-System-Grundrecht gerade schützen soll. So können **auch in Fällen**, in denen der Schutz des **IT-System-Grundrechts** besteht, Maßnahmen aufgrund der geringeren Voraussetzungen des § 23 BVerfSchG-E angeordnet werden, weil eine „private Nutzung“ verneint wird.

c. Staatstrojaner-Einsatz bei privaten IT-Systemen, §§ 25 f. BVerfSchG-E

§ 25 BVerfSchG-E ermächtigt zu einer **unbegrenzten Online-Durchsuchung** privater IT-Geräte. Dieser Staatstrojaner-Einsatz ermöglicht tiefgreifende Eingriffe in die Privatsphäre, da insbesondere Smartphones heute einen umfassenden Einblick in die Persönlichkeit bis in intimste Details ermöglichen. Diese Befugnis ist jedoch als überflüssig anzusehen. Das Bundesverfassungsgericht hat entschieden, dass der Verfassungsschutz nur subsidiär tätig werden darf, also nur, wenn die Durchführung der Überwachungsmaßnahme durch die Gefahrenabwehrbehörde selbst nicht geeignet ist oder nicht rechtzeitig käme.¹⁰ Dieses Erfordernis setzt § 25 Abs. i Satz 3 BVerfSchG-E um. Solche Konstellationen sind jedoch nur schwer vorstellbar. Die Befugnis sollte daher gestrichen werden.

Zum Eingriff in die Integrität privater informationstechnischer Systeme führt der Entwurf zudem eine neue Struktur ein, in der **neben der unbegrenzten Online-Durchsuchung weitere Eingriffsstufungen** eingeführt werden. § 26 Abs.1 BVerfSchG-E beinhaltet nunmehr (als niedrigste Stufe) eine allgemeine Befugnis zu „abgegrenzten Eingriffen“ in IT-Systeme. Diese unterliegt geringeren Eingriffsvoraussetzungen. Höhere, aber gegenüber § 25 BVerfSchG-E abgesenkte Voraussetzungen bestehen bei gezielter Erhebung von Inhaltsdaten interpersoneller

⁹ BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, Rn. 203.

¹⁰ BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17, BVerfGE 162, 1, Rn. 178 ff.

Kommunikation sowie von Daten, die gewichtige Einblicke in die Lebensführung ermöglichen (§ 26 Abs. 2 BVerfSchG-E). Die bisherigen Fälle der einfachen und erweiterten Quellen-Telekommunikationsüberwachung sollen Unterfälle dieser Eingriffskategorie sein.

Gerade die neue Kategorie des „abgegrenzten Eingriffs“ wirft erhebliche Fragen auf:

Die Stufen des Eingriffs in IT-Systeme sind **juristisch nicht klar** voneinander **abgrenzbar**. Insbesondere bestehen erhebliche Unsicherheiten, welche Informationen den erhöhten Anforderungen des § 26 Abs. 2 BVerfSchG-E unterliegen. Erfasst sind namentlich Inhaltsdaten personeller Kommunikation sowie umfassende bildliche Dokumentationen. Darüber hinaus ist vollkommen unklar und vermutlich je nach Zielperson unterschiedlich, welche Daten gewichtige Einblicke in die Lebensführung ermöglichen. Das birgt die Gefahr, dass insbesondere Daten gesucht werden, die weder Bild- noch Kommunikationsinhalte enthalten und doch weitgehende Einblicke ermöglichen. Denkbar sind Notizen-Apps und Kalender, aber auch gesundheitsbezogene Tracking-Apps.

Die Abgrenzung der verschiedenen Maßnahmen ist zudem schon technisch nicht sicher gewährleistet. Wird ein Mobiltelefon oder Computer mit einem Staatstrojaner gehackt, hat das BfV technisch **Zugriff auf das gesamte Gerät und alle verfügbaren Daten**. Die von § 26 BVerfSchG-E suggerierte leichte Abtrennbarkeit einzelner Daten oder Datenverarbeitungen ist nach dem **derzeitigen Stand der Technik nicht gegeben**. Dies stellt die abgestuften Eingriffsschwellen schon grundsätzlich in Frage.

Mit dem in § 26 Abs. 1 Satz 3 BVerfSchG-E geregelten Umgehungsverbot soll zwar verhindert werden, dass das BfV durch mehrere Einzelmaßnahmen im Ergebnis die gleichen Erkenntnisse wie durch § 25 BVerfSchG-E erlangen kann. Wie dies **in der Praxis verhindert** werden soll, wenn **wiederholt** einzelne Datenteile unter den geringeren Anforderungen des § 26 BVerfSchG-E erfasst werden, ist unklar. Somit drohen erhebliche Eingriffe in das IT-System-Grundrecht¹¹ unter zu geringen Voraussetzungen.

Die Absenkung der Eingriffsschwelle für die abgegrenzte Online-Durchsuchung ist zudem **unangemessen**. Auch hier findet bereits ein Eingriff in das IT-System der Betroffenen von erheblichem Gewicht statt.¹² Zwar hat das BVerfG in seiner Trojaner II-Entscheidung einen Unterschied der Eingriffsintensität einer Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung festgestellt.¹³ Die Begründung war jedoch auf wesentliche Unterschiede einer Überwachung von laufenden Kommunikation gegenüber allen gespeicherten Daten begründet.

¹¹ Zur Reichweite zuletzt BVerfG, Beschluss vom 24. Juni 2025 - 1 BvR 2466/19, Rn. 95 ff.

¹² BVerfG, Beschluss vom 24. Juni 2025 - 1 BvR 180/23, Rn. 186 ff.

¹³ BVerfG, Beschluss vom 24. Juni 2025 - 1 BvR 180/23, Rn. 199.

Hieraus kann nicht ohne weiteres gefolgert werden, dass jegliche Eingrenzung derart eingriffsmildernd wirkt, dass andere abgesenkte Voraussetzungen gelten. Dies gilt umso mehr, weil das Bundesverfassungsgericht auch die Quellen-Telekommunikationsüberwachung als sehr schwerwiegenden Eingriff in das IT-Systemgrundrecht angesehen hat.¹⁴

d. Nachrichtendienstliches Eingreifen in sonstige Geräte/Systeme, §§ 23 f. BVerfSchG-E

Auch die Eingriffe in **nicht privat genutzte Geräte** bzw. **IT-Systeme** greifen **tief** in die **Grundrechte** ihrer Nutzer*innen ein. Zum einen umfasst § 23 BVerfSchG-E aufgrund der zu engen und zu unbestimmten Definition des privaten IT-Systems auch Systeme, die vom IT-System-Grundrecht geschützt sind (siehe soeben a.). Selbst wenn in diesen Fällen kein Eingriff ins IT-Grundrecht erfolgt, ermächtigen die §§ 23 f. BVerfSchG-E zu Eingriffen in das Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, das Fernmeldegeheimnis, Art. 10 Abs. 1 GG, und die Berufsfreiheit, Art. 12 Abs. 1, 2 GG.

Die vorgesehene **Eingriffsschwelle** der „erheblich beobachtungsbedürftigen Bedrohung“ **genügt nicht**, um auch die intensiveren ermöglichten Grundrechtseingriffe zu rechtfertigen. Die in § 23 Abs. 3 BVerfSchG-E vorgesehene höhere Eingriffsschwelle muss auf andere besonders eingriffsintensive Informationserlangung ausgeweitet werden. Insbesondere darf sie nicht auf „systematisch gesammelte höchstprivate Informationen“ beschränkt sein, sondern muss auch dann greifen, wenn ohne System höchstprivate Informationen erlangt werden. Auch wenn einzelne Informationen über Lebensbereiche wie sensible berufliche oder wirtschaftliche Inhalte nicht „umfassend“ sind, ist die höhere Eingriffsschwelle geboten.

e. Fehlendes staatliches Schwachstellenmanagement

Schließlich sei darauf hingewiesen, dass die Nutzung von Staatstrojanern durch §§ 23 ff. BVerfSchG-E nun erheblich ausgeweitet wird, ohne dass das vom **Bundesverfassungsgericht geforderte Schwachstellenmanagement**¹⁵ besteht. Der vorliegende Entwurf lässt ein solches nicht einmal in Ansätzen erkennen. Stattdessen wird in § 10 Abs. 2, 1 BNDG-E zusätzlich eine Verpflichtung für das BfV und das Bundesamt für Sicherheit in der Informationstechnik geregelt, Schwachstellen an den BND zu übermitteln. Es ist daher zu befürchten, dass die Ausnutzung unbekannter Sicherheitslücken (zero-days) auch durch den BND weiter ansteigen wird. Vorgaben zu einem strukturierten, nachvollziehbaren Abwägungsprozess im Umgang mit entdeckten Sicherheitslücken – etwa durch Regeln zum Melden und Schließen solcher Schwachstellen – enthält der Entwurf nicht. Die Bundesrepublik Deutschland wird ihren konkreten grundrechtlichen Schutzpflichten¹⁶ nicht gerecht.

¹⁴ BVerfG, Beschluss vom 24. Juni 2025 - 1 BvR 180/23, Rn. 200 ff.

¹⁵ BVerfG, Beschluss vom 8. Juni 2021 – 1 BvR 2771/18, BVerfGE 158, 170.

¹⁶ BVerfG, Beschluss vom 8. Juni 2021 – 1 BvR 2771/18, BVerfGE 158, 170, Rn. 35 ff., 41 ff.

4. Qualifizierte Auswertung bzw. automatisierte Datenanalyse, § 37 BVerfSchG-E

Mit § 37 BVerfSchG-E soll auch für den Verfassungsschutz eine Befugnis zur **automatisierten Datenanalyse** geschaffen werden. Die Befugnis wird systematisch bei den Vorgaben zur Datenweiterverarbeitung normiert, ermächtigt aber zu einer Ermittlungsmaßnahme, der ein eigenständiges Eingriffsgewicht zukommt. Die Datenanalyse bzw. qualifizierte Auswertung dient dazu, vorhandene, unverbundene Datenbestände mit Analysesoftware zu verarbeiten, um so **neues Wissen** zu erlangen. Genau zu einer solchen Maßnahme ermächtigt § 37 Abs.1 Satz 2 BVerfSchG-E.

Mit seinem Datenanalyseurteil¹⁷ hat das Bundesverfassungsgericht zur verfassungsrechtlichen Rechtfertigung automatisierter Datenanalysen durch die Polizei entschieden. Diese Maßstäbe sind auf die Nachrichtendienste im Wesentlichen übertragbar.

Der vorliegend geplanten automatisierten Datenanalyse kommt nach den Maßstäben des Bundesverfassungsgerichts¹⁸ ein hohes Eingriffsgewicht zu. Sie stellt einen **schwerwiegenden Grundrechtseingriff** dar. Einbezogen werden können nach § 37 Abs.1 Satz 2 BVerfSchG-E sämtliche „in Datensystemen des Bundesamts für Verfassungsschutz gespeicherte personenbezogene Daten“. Weder ist die Datenanalyse auf rechtmäßig erhobene Daten beschränkt,¹⁹ noch werden besonders sensible Daten aus der Datenanalyse ausgenommen. Daher fließen erstens ihrer Art nach besonders sensible Daten wie biometrische Daten, Fotos, Videos oder Telekommunikationsdaten in die Analyse ein. Zum anderen wird die Analyse auch auf Daten aus besonders gewichtigen Grundrechtseingriffen mit nachrichtendienstlichen Mitteln erstreckt. Auch Daten aus Wohnraumüberwachungen oder Online-Durchsuchungen können in die Analyse einfließen, obwohl dazu verfassungsrechtlich zwingend eine dringende Gefahr oder zumindest eine im Einzelfall konkretisierte Gefahr erforderlich wäre.²⁰

Auch die **Analysemethoden** zur Gewinnung neuen Wissens sind **kaum beschränkt** und ermöglichen damit auch weitreichende Analysemethoden wie die Erstellung von Personenprofilen („**Profiling**“) oder **komplexe Personen- und Sachverhaltsbewertungen**. Diese Methoden weisen ein hohes Eingriffsgewicht auf. In § 37 Abs.7 BVerfSchG-E wird dem Bundesamt für

17 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 2634/20, BVerfGE 165, 363.

18 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 2634/20, BVerfGE 165, 363, Rn. 72 ff.

19 So aktuell die Entwürfe des BMI und BMJV zu Datenanalysebefugnissen für Bundeskriminalamt, Bundespolizei und Strafverfolgungsbehörden. Zu den geplanten Befugnissen für BKA und BPol umfassend: <https://freiheitsrechte.org/publikationen#2026-stellungnahme-zu-referententwuerfen-des-bundesministeriums-des-innern-zur-staerkung-digitaler-ermittlungsbefugnisse>, S. 12 ff. Zur geplanten Befugnis für die Strafverfolgungsbehörden umfassend: <https://freiheitsrechte.org/publikationen#2026-stellungnahme-zum-referentenentwurf-des-bundesministeriums-der-justiz-zur-Aenderung-der-strafprozessordnung-im-bereich-digitaler-ermittlungsmassnahmen>, S. 8 ff.

20 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 2634/20, BVerfGE 165, 363, Rn. 59.

Verfassungsschutz auch der Einsatz künstlicher Intelligenz ermöglicht. Dem Einsatz **selbstlernender Systeme** und vergleichbar komplexer Algorithmen kommt nach dem Datenanalyseurteil ein besonders Eingriffsgewicht zu.²¹

Da die vorliegend ermöglichten Datenanalysen **schwere Grundrechtseingriffe** darstellen, sind diese nur unter den Anforderungen zu rechtfertigen, die allgemein für eingriffsintensive Überwachungsmaßnahmen gelten.²² Das Bundesverfassungsgericht fordert für solche **polizeiliche Datenanalysen die Eingriffsschwelle einer konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut**.²³ Es stellt sich daher die Frage, ob so weitreichende Datenanalysen im Gefahrenvorfeld durch Verfassungsschutzbehörden **überhaupt zulässig** sein können. Die ist besonders fraglich für den Einsatz künstlicher Intelligenz, den das Bundesverfassungsgericht im Gefahrenvorfeld explizit ausschließt.²⁴ Bei Übertragung der Forderung einer besonders hohen Eingriffsschwelle ist für die Datenanalysen im BVerfSchG-E jedenfalls die Schwelle der „**besonders erheblichen Beobachtungsbedürftigkeit**“ (§ 3 Abs. 8 BVerfSchG-E) und nicht nur die „erhebliche Beobachtungsbedürftigkeit“ (§ 3 Abs. 7 BVerfSchG-E) notwendig.

Im Entwurf fehlen die **notwendigen flankierenden Schutzmaßnahmen**, die bei komplexen Datenanalysen zur Vermeidung von Fehlern und Diskriminierung und zur Sicherung der Nachvollziehbarkeit der Analyseergebnisse erforderlich sind. Diesen Vorkehrungen bedarf es insbesondere, da komplexe Analysesoftware wie selbstlernende Systeme zum Einsatz kommen können.²⁵ Die bloß abstrakten Ge- bzw. Verbote der § 37 Abs. 7 Nr. 2, 3 BVerfSchG genügen nicht, da **keine konkreten Maßnahmen** zum Schutz vor Diskriminierung und zur Wahrung der Sicherheitsstandards vorgegeben werden.

Abzulehnen ist die Regelung des § 37 Abs. 6 BVerfSchG-E. Dass Schutzmaßnahmen vollständig automatisiert durch qualifizierte Auswertungen, also automatisiert durch Software ohne menschliche Mitwirkung, angeordnet werden, muss **in jedem Falle ausgeschlossen sein**.

Positiv ist anzumerken, dass der Entwurf eine regelmäßige **Kontrolle** der Datenanalysen durch den UK-Rat (§ 37 Abs. 5 Satz 2 BVerfSchG-E) und stichprobenartige Kontrollen durch das Bundesamt selbst (§ 37 Abs. 7 Nr. 4 BVerfSchG-E) vorsieht. Gerade zu Beginn der Nutzung von Analysetools ist jedoch eine häufigere externe Kontrolle als alle zwei Jahre notwendig. Zudem ist der Umfang der vorzunehmenden Kontrolle nicht geregelt. Es bleibt fraglich, wie der UK-Rat eine

21 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 2634/20, BVerfGE 165, 363, Rn. 100.

22 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 2634/20, BVerfGE 165, 363, Rn. 104.

23 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 2634/20, BVerfGE 165, 363, Rn. 105 f.

24 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 2634/20, BVerfGE 165, 363, Rn. 120 f.

25 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 2634/20, BVerfGE 165, 363, Rn. 100.

technische Kontrolle von Softwaretools tatsächlich sicherstellen soll. Hierzu bedarf es spezialisierter technischer Expertise, gerade, wenn der Quellcode der genutzten Software nicht offengelegt ist. Die internen Kontrollen gemäß § 37 Abs. 7 Nr. 4 BVerfSchG-E sind zudem auf die Kontrolle „**auf ordnungsgemäßes Funktionieren**“ **beschränkt**. Dieser Begriff ist offen und enthält jedenfalls keine ausreichende gesetzliche Anleitung zur Kontrolle von komplexen KI-Analysesystemen. Erforderlich ist eine **tatsächliche Kontrolle**, ob die Software zu fehlerhaften Ergebnissen führt oder Inhalte halluziniert. Ebenso muss darauf kontrolliert werden, dass sich aufgrund der ggf. einseitigen Datengrundlage diskriminierende Algorithmen herausbilden. Die interne Kontrolle umfasst zudem keine Kontrolle auf möglichen **Missbrauch** der Software. Eine solche Kontrolle ist auch intern unbedingt erforderlich. Vorgaben zur Kontrolle der in die Künstliche Intelligenz eingespeicherten Daten und ihrer Qualität fehlen ebenfalls.

Ebenso ist grundsätzlich positiv anzumerken, dass der Schutz zur **digitalen Souveränität** im Entwurf mitbedacht wurde. § 37 Abs. 7 Nr. 1 BVerfSchG -E ist zum Schutz der digitalen Souveränität jedoch **ungeeignet**. Es stellt sich schon die Frage, ob die Regelung nicht durch europäische Niederlassungen bzw. Tochtergesellschaften „umgangen“ werden kann. Auch Risiken, dass europäische Unternehmen in Drittstaaten verziehen, begegnet die Norm nicht. Zudem müssen auch die diskriminierenden Wirkungen einer Bevorzugung europäischer Anbieter*innen Berücksichtigung finden.

Ohnehin **stellt** ein **europäischer Sitz eines Unternehmens nicht** ohne Weiteres **sicher**, dass **rechtsstaatliche Grundsätze gewahrt** bleiben. Auch bei europäischen privaten Anbietern bestehen Risiken, insbesondere bezüglich der Nachvollziehbarkeit bei komplexen Algorithmen und KI.²⁶ Fehler, Diskriminierungen, aber auch Datenlecks, Manipulation und unbefugte Zugriffe können kaum ausgeschlossen werden. Dies gilt auch für den Anbieter **Chapsvision** und seine Software ArgonOS, welche das BfV im Jahr 2026 bereits lizenziert haben soll²⁷ – obwohl keine Rechtsgrundlage zum Betrieb oder Test eines solchen Tools gesetzlich vorgesehen ist. Der BfV soll den Berichten zur Folge somit zwar nicht die Software Gotham des US-Anbieters Palantir nutzen. Eine Gefahr für die Grundrechte sind Datenanalysen aber **unabhängig vom Anbieter**.

Vorgaben allein an die Herkunft der Anbieter*innen eines Analyseprogramms gewähren keinen wirksamen Schutz. Zur Sicherstellung der digitalen Souveränität und des Datenschutzes bedarf es vielmehr **Vorgaben an den Code bzw. an das Tool selbst**, nicht nur an die anbietenden Unternehmen. Die offene Formulierung des § 37 Abs. 7 Nr. 2 BVerfSchG-E enthält keine konkreten Maßstäbe und technischen Anforderungen. Notwendig sind verpflichtende **Kontrollen** des

²⁶ BVerfG, Urteil vom 16. Februar 2023, 1 BvR 2634/20, BVerfGE 165, 363, Rn. 100.

²⁷ *Diehl/Flade*, Verfassungsschutz setzt auf Palantir-Alternative, SZ.de vom 13. Mai 2026, abrufbar unter <https://www.sueddeutsche.de/politik/verfassungsschutz-cybersicherheit-palantir-alternative-li.3482432>.

Quellcodes bzw. der Funktionsweise und Sicherheit der Software vor Inbetriebnahme und **auch bei Updates**.

Bei jeder Software eines privaten Anbieters stellen sich Probleme um die digitale Souveränität und entstehende Abhängigkeiten von Softwaretools privater Anbieter*innen. Private Unternehmen erhalten Einblicke in die Arbeit der Nachrichtendienste, vor allem können sie deren Arbeit aber beeinflussen und im schlimmsten Falle technisch behindern. Diesen Risiken begegnet der Gesetzesentwurf nicht.

5. Biometrischer Datenabgleich, § 8 Abs. 1 Satz 2 Nr. 2 BVerfSchG-E

Auch die Ermächtigung zum biometrischen Datenabgleich ist verfassungswidrig. § 8 Abs. 1 Satz 2 Nr. 2 BVerfSchG-E ermöglicht es dem BfV, **umfassend biometrische Abgleiche** vorzunehmen, ohne dass die Befugnis angesichts ihres schwerwiegenden Eingriffsgewichts an eine ausreichende Eingriffsschwelle geknüpft wird.

Die Vorschrift ermächtigt das BfV, **öffentlich zugängliche Quellen**, damit auch Daten aus dem Internet, mit allen Daten, auf die das BfV „zur Erfüllung seiner Aufgaben zugreifen darf“ biometrisch abzugleichen.

Indem die Befugnis in die Datenerhebungs-Generalklausel integriert ist, entsteht fälschlicherweise der Eindruck, es handele sich um eine Befugnis mit geringem Eingriffsgewicht. Biometrische Abgleiche mit internetbasierten Diensten ermöglichen allerdings **schwerwiegende Grundrechtseingriffe**. Die Streubreite der Maßnahme ist enorm. Heimlich abgeglichen werden biometrische Daten auch von massenhaft völlig unbeteiligten Menschen. Denn auch ein Abgleich als Nicht-Treffer stellt insoweit einen Grundrechtseingriff dar.²⁸ Insbesondere Bilder, aber auch andere biometrische Inhalte von Menschen, landen oft **ohne deren Wissen oder sogar gegen ihren Willen** im Netz. Eine Löschung ist oft schwer oder gar nicht möglich, sodass sich einzelne Personen nicht vor dieser Maßnahme schützen können. Automatisierte biometrische Abgleiche greifen gerade auch auf solche Inhalte zu. Hinzu kommt, dass durch den biometrischen Abgleich Rückschlüsse auch auf besonders **sensible und grundrechtsgeschützte Lebensbereiche** möglich sind. Erfasst sind beispielsweise Daten aus Dating-Plattformen oder sexualisierte Deep Fakes, aber auch Aufnahmen von Versammlungen. Die Schutzregelungen für nachrichtendienstliche Mittel, gerade der Kernbereichsschutz, finden jedoch (ebenso wie bei §§ 11 ff. BVerfSchG-E, siehe dazu oben A. III. 1) keine Anwendung. Auch der Adressat*innenkreis des Abgleichs ist nicht auf Anlasspersonen beschränkt.

Diesem hohen Eingriffsgewicht wird die Eingriffsschwelle des § 8 Abs. 1 Satz 2 Nr. 2 BVerfSchG („tatsächliche Anhaltspunkte im Einzelfall“) nicht gerecht. Als schwerwiegender

²⁸ BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, BVerfGE 150, 244, Rn. 51.

Grundrechtseingriff wäre ein Anknüpfen an eine **besonders erheblich beobachtungsbedürftige Bedrohung** sowie die **Einstufung als nachrichtendienstliches Mittel**, die bestimmte Schutzvorkehrungen auslöst, erforderlich. In der vorgesehenen Fassung ist die Norm **unverhältnismäßig und verfassungswidrig**.

Zudem dürfen **nicht sämtliche im Internet allgemein öffentlich verfügbaren Daten** für den Abgleich verarbeitet werden, sondern nur solche, bei welchen eine gesteigerte Wahrscheinlichkeit für Treffer besteht. Das wäre beispielsweise der Fall bei Daten aus einschlägigen öffentlichen Chat-Gruppen. Beachtet werden muss in diesem Zusammenhang das vom Bundesverfassungsgericht für die Kennzeichenerfassung geforderte **Flächendeckungsverbot**.²⁹ Kontrollen dürfen „nur an einzelnen erfolgversprechenden Stellen, das heißt punktuell örtlich begrenzt durchgeführt werden [...], nicht aber zu dem Zweck, kontrollfreie Bewegungen möglichst weiträumig oder gar im gesamten Zuständigkeitsbereich der Behörde auszuschließen“.³⁰ Das Flächendeckungsverbot soll verhindern, dass der Staat ohne hinreichenden Anlass den gesamten öffentlichen Raum nach potenziellen Treffern durchsucht. Auch für den biometrischen Datenabgleich ist ein solcher Schutz im digitalen Raum erforderlich, da die Maßnahme sensiblere Daten betrifft und die Streubreite sehr hoch ist.

Besonders problematisch ist es, dass der Entwurf zudem den Abgleich **durch öffentliche Stellen sowie private Dritte im Nicht-EU-Ausland ermöglicht** (§ 8 Abs. 2 BVerfSchG-E). Damit kann das BfV auf Anbieter*innen wie PimEyes und Clearview zurückgreifen. Diese verstoßen allerdings gegen Unionsrecht.³¹ Zwar dürfen diese Anbieter*innen nur subsidiär an Anspruch genommen werden. Eine massenhafte Auswertung des Internets ist praktisch allerdings nur durch vorgehaltene Biometrie-Datenbanken möglich³², deren Erstellung aber in der Regel verfassungswidrig wäre. Insofern sieht § 8 Abs. 2 Satz 2 BVerfSchG-E auch eine Löschverpflichtung vor. Da ein Abgleich (ohne Referenzdatenbank) dann aber regelmäßig „nicht gleichermaßen“ durch das BfV, eine andere inländische Stelle oder eine Stelle eines EU-Mitgliedsstaates erfolgen kann, steht zu befürchten, dass die Subsidiaritätsregelung leerläuft und Abgleiche unter **Umgehung wesentlicher verfassungsrechtlicher und europarechtlicher Standards erfolgen**, indem regelmäßig auf **Anbieter wie PimEyes zurückgegriffen** wird. Vorgaben an die privaten Dritten zur Sicherung der digitalen Souveränität fehlen hier vollständig.

29 BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, BVerfGE 150, 244, Rn. 100.

30 BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, BVerfGE 150, 244, Rn. 115.

31 Gegen PimEyes wurde daher durch den LfDI Baden-Württembergs ein Bußgeldverfahren eingeleitet, vgl. die Pressemitteilung des LfDI BW vom 21. Dezember 2022, abrufbar unter <https://www.baden-wuerttemberg.datenschutz.de/pimeyes-lfdi-eroeffnet-bussgeldverfahren/>.

32 Lewandowski, Braucht die Polizei eine Datenbank zum biometrischen Abgleich? Das Durchsuchen von Internetbildern zur Gesichtserkennung, September 2025, abrufbar unter <https://algorithmwatch.org/de/wp-content/uploads/2025/10/2025-AW-Gutachten-V9.pdf>.

Der Entwurf sieht zudem ebenso wenig wie für Tools zur automatisierten Datenanalyse (siehe dazu soeben A. III. 4.) Vorgaben an die eingesetzte Software vor. Damit ist weder die **Einhaltung des Datenschutzes gesichert**, noch wird vor **Fehlern und Diskriminierung** geschützt. Dies ist besonders bedeutsam, da Systeme zum biometrischen Abgleich fehlerbehaftet sind und bestimmte Bevölkerungsgruppen (Frauen*, PoC) deutlich schlechter erkennen.³³ **Bei Fehlidentifikationen drohen weitere Grundrechtseingriffe.** Gerade ohnehin marginalisierte Gruppen müssen mit ungerechtfertigten Überwachungsmaßnahmen auf Basis rechtswidriger und fehlerhafter biometrischer Abgleiche rechnen.

6. Datenerhebung bei Dritten und zeugnisverweigerungsberechtigten Personen

Der vorliegende Entwurf gestattet zu weitreichende Überwachungsmaßnahmen gegenüber Dritten und schützt Berufsheimnisträger*innen unzureichend.

a. Datenerhebung bei Dritten, § 16 Abs. 5 BVerfSchG-E

§ 16 Abs. 5 Nr. 2 BVerfSchG-E gestattet zu weitreichend und daher **verfassungswidrig** nachrichtendienstliche Mittel bereits dann gegen Dritte, wenn diese „im Zusammenhang mit einer Bedrohung stehen, der Grund zur Annahme gibt, dass durch die Maßnahme Erkenntnisse über die Bedrohung gewonnen werden können [...]“. Die gesetzliche Neuregelung knüpft dabei an den Begriff des Zusammenhangs an, obwohl allein „lose Zusammenhänge“ laut Bundesverfassungsgericht **gerade nicht** für eine Anordnung heimlicher Überwachungsmaßnahmen **genügen**.³⁴ Die weiteren verfassungsrechtlich gebotenen Einschränkungen, dass zusätzliche Anhaltspunkte für einen Bezug zum Ermittlungsziel vorliegen und eine nicht unerhebliche Wahrscheinlichkeit für die Dienlichkeit der Überwachungsmaßnahme zur Aufklärung der Bestrebung besteht, sind in § 16 Abs. 5 Nr. 2 BVerfSchG-E nicht vorgesehen.

b. Unzureichender Schutz von Berufsheimnisträger*innen, § 32 Abs. 4 BVerfSchG-E

Ebenso ist der Schutz zeugnisverweigerungsberechtigter Berufsheimnisträger*innen durch die Verstrickungsregelung des § 32 Abs. 4 BVerfSchG unangemessen beschränkt. Gegen eine vergleichbare Regelung im nordrhein-westfälischen Verfassungsschutzgesetz ist bereits eine Verfassungsbeschwerde anhängig.³⁵ Dass für die **Beteiligung** (§ 3 Abs. 5 BVerfSchG-E) bereits jede objektive und mittelbare Unterstützung genügen soll (so auch S. 312 f. des Entwurfs), weitet die Verstrickungsregelung zu weitgehend aus. Im Bereich der Rechtsanwält*innen **beschränkt** sie die

33 Dazu Grother u.a., Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 2019; siehe auch die aktuellen Zahlen auf https://pages.nist.gov/frvt/html/frvt_demographics.html; ALGORITHMWATCH, Explainer: Biometrische Erkennungssysteme Zeige dein Gesicht und KI sagt dir, wer du bist, 24. September 2024, abrufbar unter <https://algorithmwatch.org/de/biometrische-erkennung-erklart/>.

34 Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 212.

35 Vgl. Verfassungsbeschwerde zu § 9 Abs. 8 VSG NRW, Rn. 78, abrufbar unter <https://fdp.fraktion.nrw/initiative/verfassungsbeschwerde-gegen-das-verfassungsschutzgesetz-nordrhein-westfalen>.

Möglichkeiten auf **vertrauliche Rechtsberatung**, da Menschen, die bestimmten Bestrebungen nahestehen, häufig bei bestrebungs- und szenenahen Anwalt*innen Rechtsbeistand suchen (müssen). Bei nachrichtendienstlicher Überwachung im Vorfeld konkretisierter Gefahren und ohne strafrechtlichen Anfangsverdacht sind Einschränkungen des Vertraulichkeitsschutzes bereits bei objektiven Förderungshandlungen ohne subjektive Tatseite als unverhältnismäßig anzusehen. Die Norm erfasst darüber hinaus zu weitgehend auch Fälle mittelbarer Unterstützung z.B. durch Nachrichtenmittlung (S. 313 des Entwurfs). Das Bundesverfassungsgericht hat zu Fällen der Ausland-Ausland-Überwachung entschieden, dass die Überwachung von Journalist*innen und Rechtsanwält*innen als Nachrichtenmittler*innen an qualifizierte Eingriffsschwellen zu binden ist.³⁶ Dieses Erfordernis ist aufgrund gleicher Schutzbedürftigkeit auf die nachrichtendienstliche Inlandsüberwachung zu übertragen.

7. KI-Training, § 36 Abs. 1 Nr. 1 lit. a, Abs. 2 Satz 1 Nr. 5 BVerfSchG-E

Die allgemeine Befugnis zur zweckändernden Weiterverarbeitung von Daten kann, anders als in der Gesetzesbegründung angenommen (S. 327 des Entwurfs), offensichtlich **keine verfassungskonforme Rechtsgrundlage** für ein **KI-Training mit den beim BfV vorhandenen Daten** darstellen.

Die Norm ist bereits **so unbestimmt**, dass sie als Befugnis für ein KI-Training **nicht ohne die Erläuterung in der Begründung erkennbar** ist.

Auch sichert die Norm die Einhaltung der Zweckbindungsgrundsätze insbesondere bei Daten aus schwerwiegenden Grundrechtseingriffen nicht. Art, Umfang und Herkunft der einbezogenen Daten werden nicht differenziert, das Eingriffsgewicht der Datenerhebung findet keine Berücksichtigung. Die Ausschlüsse der § 36 Abs. 1 Nr. 2 BVerfSchG-E genügen nicht. Es bedarf einer differenzierten Regelung, die sowohl dem **Eingriffsgewicht der Datenerhebung der jeweiligen Daten** als auch dem **Eigengewicht** des Trainingsvorgang ausreichend Rechnung trägt. Mangels Ausschlusses von **besonders sensiblen Daten** oder Daten von **unbeteiligten Dritten** greift dieses heimliche KI-Training **tief** in die Grundrechte ein. Der Verwendungszweck ist bis auf die Aufgaben des BfV nach § 2 BVerfSchG-E nicht beschränkt. Eine Beschränkung auf bestimmte Produkte oder Modelle ist nicht enthalten. Auch besonders eingriffsintensive Systeme wie biometrische Identifizierungssysteme sind möglich. Auch hier kommt dem möglichen Einsatz **selbstlernender Systeme** ein besonders hohes Eingriffsgewicht zu.³⁷ Die Norm lässt **keine** dafür erforderliche **Eingriffsschwelle** erkennen. Sie ist daher **unverhältnismäßig**.

³⁶ Vgl. BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17, Rn. 194.

³⁷ BVerfG, Urteil vom 16. Februar 2023, 1 BvR 2634/20, BVerfGE 165, 363, Rn. 100 zu automatisierten Datenanalysen.

Zudem fehlt es vollständig an **flankierenden Schutzmaßnahmen** zu den spezifischen Risiken für Trainingsdaten einer komplexen, ggf. selbstlernenden Software. Weder Risiken zur Entwicklung fehlerhafter oder diskriminierender Algorithmen noch zum Verbleib von Daten auch nach Lösungsfrist und zu unzulässigen Zwecken wird mit konkreten Schutzmaßnahmen begegnet. Auch eine Nachvollziehbarkeit der Trainingsvorgänge wird nicht sichergestellt.

IV. Operative Befugnisse, §§ 60 ff. BVerfSchG-E

In §§ 60 ff. BVerfSchG-E sieht der Gesetzgeber operative Befugnisse für das BfV vor. Diese sollen die Übermittlungsvorschriften ergänzen und Schutzlücken schließen. Neben der originären Aufgabe der Weitergabe von Erkenntnissen soll ergänzend gegen Bedrohungen eingeschritten werden können.

Die vorgesehenen Regelungen enthalten erhebliche Eingriffsbefugnisse, die die systematische Aufgabentrennung von Polizei und Geheimdiensten unterlaufen. Bei Einführung stellen sie das gesamte verfassungsrechtliche Gefüge der Sicherheitsbehörden in Frage. Mit operativen Eingriffsbefugnissen für das BfV stellen sich **verfassungsrechtlich neuartige Maßstäbe für die Rechtfertigung**. Viel bedeutsamer ist jedoch, dass die Eingriffsbefugnisse mit hoher Wahrscheinlichkeit die **Rechtfertigungsanforderungen für nachrichtendienstliches Handeln insgesamt erhöhen**. Bei Einführung der Befugnisse sind daher **für sämtliche Aufklärungsbefugnisse** des BfV die **verfassungsrechtlichen Rechtfertigungsanforderungen neu zu beurteilen**.

Entscheidet sich der Gesetzgeber, einen operativ handelnden Geheimdienst zu schaffen, der neuartigen Bedrohungen mit eigenen Gefahrenabwehrmaßnahmen begegnet, **kann dieser nachrichtendienstliche Mittel nicht unter erleichterten Rechtfertigungsanforderungen bereits im Gefahrenvorfeld vornehmen**. Die herabgesetzten Eingriffsschwellen der Nachrichtendienste hängen nach dem Bundesverfassungsgericht gerade eng damit zusammen, dass den Nachrichtendiensten **keine operativen Befugnisse zukommen**.³⁸ Das Gericht führt dazu aus:

*„Dass eine **Verfassungsschutzbehörde nicht über eigene operative Anschlussbefugnisse verfügt**, rechtfertigt es im Grundsatz, die ihr zur Wahrnehmung ihrer Beobachtungsaufgaben eingeräumten Datenerhebungsbefugnisse im Vergleich zu den Befugnissen einer Polizeibehörde wegen des geringeren Eingriffsgewichts **an modifizierte Eingriffsschwellen** zu knüpfen, die zugleich dem speziellen Charakter der Aufgaben des Verfassungsschutzes entsprechen.“³⁹*

38 BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17, BVerfGE 162, 1, Rn. 154.

39 BVerfG, Urteil vom 26. April 2022 - 1 BvR 1619/17, BVerfGE 162, 1, Rn. 156.

Genau diese Rechtfertigung entfielen mit den neuen Befugnissen. §§ 60 ff. BVerfSchG sind gerade kein Annex oder eine Ergänzung der Informationsübermittlung. Sie enthalten **eigenständige operative Befugnisse**.

§ 60 BVerfSchG-E ermächtigt, anders als in der Gesetzesbegründung angenommen, nicht nur zu geringfügigen Ergänzungsmaßnahmen. Dem Wortlaut nach ermöglicht die Norm **weitläufig „Einwirkung auf Gegenstände, die für die Bedrohung gegenwärtig oder künftig eingesetzt werden“** sowie „Güter, die im Rahmen einer Bedrohung ausgeführt werden sollen“. Der Anwendungsbereich erschöpft sich daher gerade nicht in Sonderfällen. Ausgeschlossen ist zwar gemäß § 60 Abs. 2 Satz 2 BVerfSchG-E die Anwendung von Zwang und damit auch von Gewalt gegen Personen. Dies ändert jedoch nichts daran, dass auch Einwirkungen auf Gegenstände weitreichende und unter Umständen grundrechtsintensive Maßnahmen darstellen, die nach außen den operativen Befugnissen der Polizei in vielen Fällen gleichkommen. Der Annahme, die Befugnis verbleibe „im nachrichtendienstlichen Gepräge“, muss daher deutlich widersprochen werden. Die Befugnis ist dafür in ihrer sachlichen Anwendbarkeit durch Nutzung zahlloser offener Rechtsbegriffe deutlich zu weit geraten.

Die zulässigen Maßnahmen sind zudem kaum konkretisiert. Gerade § 60 Abs. 2 Nr. 1 BVerfSchG-E ist fast uferlos weit. Das Objekt des Gegenstands ist nicht auf körperliche Gegenstände beschränkt, sondern umfasst gerade auch nichtkörperliche Objekte wie Informationen. Umfassende digitale Maßnahmen im Rahmen von **Hackbacks** werden daher möglich. Notwendig ist nur, dass der Gegenstand für die Bedrohung gegenwärtig oder absehbar eingesetzt wird. Die sodann erfolgende Aufzählung in den Buchstaben a) -d) ist nicht abschließend. Letztlich kann **also auf sämtliche körperliche und nicht körperliche Gegenstände, also auch auf digitale Bestände wie Daten, Software und digitale Infrastruktur wie Plattformen** eingewirkt werden, wenn diese für eine Bedrohung eingesetzt wird. Der Einsatz ist dabei gerade bei neutraler, zweckoffener Infrastruktur schnell gegeben. Die Befugnis ist gerade **nicht auf** die in der Begründung (S. 355 des Entwurfs) genannten **Fälle staatlicher Angriffe** und die Einwirkung auf Einsatzmittel fremder Staaten **beschränkt**. Es ist nach dem Wortlaut des Gesetzes nicht erforderlich, dass die Gegenstände den gefahrverursachenden Personen gehören oder irgendwie zugeordnet sein müssen. Dass die Maßnahmen laut Gesetzesbegründung (S. 355 des Entwurfs) auf die Verantwortlichen der Bedrohungssituation beschränkt sein sollen, ist dem Gesetz selbst nicht zu entnehmen, gerade weil der Maßnahmenkatalog, der dies implizieren soll, mit nicht abschließenden Beispielen ausgestattet ist. Die Einwirkung kann dann gerade Infrastruktur **völlig unbeteiligter Dritter** betreffen. Die Definition der Schutzmaßnahme genügt den Anforderungen an die **verfassungsrechtliche Bestimmtheit und Normenklarheit** nicht. Weder für anwendende Mitarbeiter*innen des BfV

noch für Bürger*innen als Betroffene ist die Vornahme von Schutzmaßnahmen so begrenzt, dass eine klare Grenze der zulässigen Maßnahmen erkennbar ist.

Daran vermag auch das Erfordernis einer besonderen Bedrohung im Sinne des Absatzes 3 und der grundsätzliche Vorrang operativer Maßnahmen anderer Stellen (§ 60 Abs. 1 Satz 2 BVerfSchG-E) nichts zu ändern. Zudem verkehrt § 60 Abs. 1 Satz 2 den jedenfalls teilweise als Schutzvorschrift ausgestalteten § 52 BVerfSchG-E vollständig ins Gegenteil. Dessen Anwendbarkeit ermöglicht nun gerade Grundrechtseingriffe durch operative Maßnahmen des BfV.

Ebenso irritiert die ausschließliche Kontrolle der Maßnahmen durch den UK-Rat, § 63 Abs. 2 BVerfSchG-E. Gerade wegen der technisch faktisch unbegrenzten Möglichkeiten der „Einwirkung auf Gegenstände“ in Form von Hacks und digitalen Angriffen ist eine **Kontrolle in technischer und datenschutzrechtlicher Hinsicht** auch durch **Expert*innen im IT-Bereich unerlässlich**.

Die geplanten Befugnisse ermöglichen operatives Handeln zur Gefahrenabwehr. Es ist zu erwarten, dass mit Gebrauch der Befugnis immer **weitere zu schließende Schutzlücken** festgestellt werden. §§ 60 BVerfSchG **öffnen** dem BfV die **Tür zur operativen Gefahrenabwehr**. Dies führt zu einer **Verwischung** der klaren **Trennung von Polizei und Geheimdiensten** und stellt die verfassungsrechtlichen Grundsätze der nachrichtendienstlichen Befugnisse in Frage. Dies gilt umso mehr, da auch dem BND zu unbestimmt gefasste operative Eingriffsbefugnisse gewährt werden, die im Widerspruch zur bisherigen Funktion als reiner Nachrichtendienst stehen.

Neben den verfassungsrechtlichen Einschränkungen bestehen bezüglich der Vornahme von operativen Eingriffshandlungen im Ausland, z.B. im Falle von Hackbacks, auch erhebliche **völkerrechtliche Bedenken**.

Daher sind die §§ 60 ff. ersatzlos zu streichen.

V. Übermittlungsvorschriften, §§ 45 ff. BVerfSchG-E

Auch die im Entwurf des BVerfSchG enthaltenen Übermittlungsbefugnisse genügen nicht in allen Fällen den verfassungsrechtlichen Anforderungen.

Dies gilt insbesondere für **§ 47 BVerfSchG-E**, der in unverhältnismäßiger Weise Datenübermittlungen an weite Aufgabenbereiche der Verwaltung gestattet. Es fehlt an der verfassungsrechtlich erforderlichen erhöhten Übermittlungsschwelle einer konkretisierten Gefahr.⁴⁰ Diese ist laut Bundesverfassungsgericht nur in engen Ausnahmen und im Einzelfall zulässig. Erforderlich ist ein gesetzlich geregelter Zusammenhang mit einem besonders hohen Gefahrenpotenzial für hochrangige Rechtsgüter und einer engen Verbindung zu den Schutzgütern

⁴⁰ BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22, BVerfGE 169, 130, Rn. 222.

des Verfassungsschutzes. Als mögliche Fälle nennt das Bundesverfassungsgericht dabei Prüfzwecke im Waffen- oder Luftsicherheitsrecht, personenbezogene Eignungs- und Sicherheitsüberprüfungen im öffentlichen Dienst oder in Fällen, in denen einer nur potenziellen Gefährdung der freiheitlich demokratischen Grundordnung, z.B. durch Vorbereitung von Vereinsverboten, begegnet werden soll.⁴¹

Dieses Gefährdungspotenzial liegt nicht hinsichtlich aller in § 47 Abs. 1 BVerfSchG-E aufgeführten Fälle vor und wird auch nicht durch die Bezugnahme auf den Bedrohungsbegriff des § 3 Abs. 4 BVerfSchG-E gewährleistet. Insbesondere § 47 Abs. 1 Nr. 8 BVerfSchG-E (Gewerbeaufsicht) genügt nicht den verfassungsrechtlichen Anforderungen. Bereits in der Vorgängervorschrift war nicht normenklar geregelt, welche konkreten verwaltungsbehördlichen Überprüfungen erfasst werden sollten.⁴² Die Neufassung verzichtet nun gänzlich auf die Einschränkung auf Zuverlässigkeits- und Eignungsüberprüfungen und lässt die Übermittlung für den gesamten Bereich der Gewerbeaufsicht zu. Eine Beschränkung auf bestimmte Überprüfungen, die mit besonders schadenträchtigem Verhalten verbunden sind, findet nicht statt. Aber auch § 47 Abs. 1 Nr. 7 und 9 enthalten keine weitergehenden Einschränkungen auf besonders gefahrenintensive Bereiche und Überprüfungen.

So beinhaltet § 47 Abs. 1 BVerfSchG-E nun klassische Aufgabenbereiche der Gefahrenabwehr. Das betrifft vor allem § 47 Abs. 1 Nr. 3 lit. c BVerfSchG-E, der die Übermittlung für Aufgaben nach den Versammlungsgesetzen beinhaltet. Es ist nicht nachvollziehbar, warum dieser Aspekt nun in den Katalog zum administrativen Rechtsgüterschutz aufgenommen wurde, da diese Aufgaben bisher als Fall der Abwehr einer konkretisierten Gefahr verstanden wurden (S. 343 f. des Entwurfs). Gleiches gilt für die neue Ausreiseuntersagung in § 47 Abs. 1 Nr. 5 BVerfSchG-E, die ebenfalls bislang zu Recht als reiner Fall der Abwehr einer konkretisierten Gefahr verstanden wurde (S. 344 des Entwurfs). Hier fehlt eine trennscharfe Eingrenzung auf rein administrative Zwecke, zumal die Maßnahmen erhebliche Grundrechtsrelevanz haben. Laut Bundesverfassungsgericht ist die Schwelle zur Übermittlung selbst bei öffentlichen Stellen ohne operative Befugnisse abhängig von dem Gewicht des Grundrechtseingriffs.⁴³ Gerade im eingriffserheblichen Bereich des Versammlungsrechts darf insofern nicht auf das Erfordernis einer konkretisierten Gefahr verzichtet werden.

Ebenso sollte aufgrund der hohen Grundrechtsrelevanz auch für die Fälle § 47 Abs. 1 Nr. 4 lit. b, Nr. 11 BVerfSchG-E die Übermittlungsschwelle nicht abgesenkt werden. Dies gilt für Nr. 4 lit. b gerade,

41 BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22, BVerfGE 169, 130, Rn. 113.

42 Vgl. Verfassungsbeschwerde der Gesellschaft für Freiheitsrechte e.V. zu § 20 Abs. 1 Satz 1 Nr. 5 BVerfSchG, S. 48; abrufbar unter <https://freiheitsrechte.org/themen/freiheit-im-digitalen-zeitalter/bverfSchg>.

43 Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, BVerfGE 162, 1, Rn. 259.

weil die Norm keine Tatsachengrundlage für den Verdacht strafbarer Handlungen fordert. Ferner bleiben die verfassungsrechtlichen Bedenken hinsichtlich der Bezugnahme auf das Aufenthalts- und Staatsangehörigkeitsrecht (§ 47 Abs. 1 Nr. 5 BVerfSchG-E) bestehen.⁴⁴

Verfassungsrechtlich zu beanstanden ist auch **§ 48 BVerfSchG**, die die Übermittlung an die Strafverfolgungsbehörden regelt. Dieser knüpft entgegen der Rechtsprechung des Bundesverfassungsgerichts **nicht nur an die Verfolgung besonders schwerer Straftaten**⁴⁵ an. Neben Straftaten, die im Höchstmaß mit einer Freiheitsstrafe von mehr als fünf Jahren bedroht sind, können auch Straftaten mit einer Höchstfreiheitsstrafe von mindestens fünf Jahren als besonders schwer einzustufen sein. Voraussetzung hierfür ist aber, dass sich eine bestimmte Begehungsform im Tatbestand selbst niederschlägt und zugleich das besonders schwere Unrecht der Tat begründet.⁴⁶ Anlage 1 zu § 48 Abs. 2 Nr. 2 BVerfSchG-E führt eine breite Menge an Tatbeständen auf, die nicht in allen Fällen diesem Maßstab genügen. Für die unzureichende Eingrenzung auf besonders schwere Straftatbestände spricht indiziell, dass der Katalog in Anlage 1 beinahe alle sog. Staatsschutzdelikte (vgl. §§ 74a, 120 GVG) aufführt, die im Höchstmaß mit fünf Jahren Freiheitsstrafe bedroht sind. Das Bundesverfassungsgericht hat indes ausdrücklich festgestellt, dass nicht alle Staatsschutzdelikte auch besonders schwere Straftaten darstellen.⁴⁷ Hier wird der Eindruck erweckt, dass die Tatbestände nicht ausreichend differenziert gewichtet wurden. In diesem Sinne ist bei einigen aufgeführten Delikten zweifelhaft, dass ihre Begehung oder ihre Folgen nicht die Schwelle einer besonders schweren Tat erreichen. Dies gilt besonders für die §§ 90 bis 90b StGB (Nr. 8 bis 10 der Anlage 1), zumindest so weit auch die Grundtatbestände erfasst werden, sowie für § 106 StGB (Nr. 17 der Anlage), der nicht einmal eine qualifizierte Nötigungshandlung voraussetzt, und § 109d StGB (Nr. 21 der Anlage).

Ebenso ist die in **§ 51 BVerfSchG-E** geregelte Neufassung der Übermittlungsbefugnisse an Private als zu weitgehend und unverhältnismäßig anzusehen. Ebenso wie die Übermittlung von Daten an öffentliche Stellen muss die Übermittlung an Private dem Schutz besonders gewichtiger Rechtsgüter dienen.⁴⁸ Private sind nicht unmittelbar an Grundrechte gebunden und unterliegen nicht denselben Transparenzpflichten und rechtsstaatlichen Standards, sodass der Übermittlung ein hohes Eingriffsgewicht zukommt. Der vorliegende Entwurf nimmt erstens nicht auf besonders gewichtige Rechtsgüter Bezug und umfasst in seinem Katalog auch breite Gebiete, bei welchen eine Gefährdung weniger gewichtiger Rechtsgüter denkbar ist. Dies betrifft etwa die Bereiche der

44 Vgl. Verfassungsbeschwerde der Gesellschaft für Freiheitsrechte e.V. zu § 20 Abs. 1 Satz 1 Nr. 5 BVerfSchG, S. 47; abrufbar unter <https://freiheitsrechte.org/themen/freiheit-im-digitalen-zeitalter/bverfschg>.

45 Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, BVerfGE 162, 1, Rn. 251.

46 Vgl. BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22, BVerfGE 169, 130, Rn. 207.

47 Vgl. BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22, BVerfGE 169, 130, Rn. 208.

48 Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, BVerfGE 162, 1, Rn. 255.

Wirtschaftsunternehmen (lit. c), rechtlich gewährleisteter Geheimnisse (lit. d), Erziehungs- und Bildungsziele der Schulen und Einrichtungen der Kindertagesbetreuung (lit. h) sowie der Verwendung öffentlicher Fördermittel (lit. i). Zweitens ist auch eine Datenübermittlung in besonders grundrechtssensiblen Bereichen möglich, insbesondere im Falle von § 51 Abs. 1 Nr. 4 lit. b und c und Nr. 5 lit. c und d BVerfSchG-E.

Zuletzt ist auch die Übermittlungsvorschrift des **§ 56 BVerfSchG-E** zu weit geraten und unverhältnismäßig. § 56 Abs. 3 BVerfSchG-E gestattet die Übermittlung von Daten, die das Bundesamt für Verfassungsschutz ohne Ausübung besonderer Befugnisse (§ 3 Abs. 11 BVerfSchG-E) erlangt hat, zum Schutz von besonders gewichtigen Rechtsgütern. Nicht als besondere Befugnisse stuft der Entwurf des Bundesverfassungsschutzgesetzes jedoch u.a. die Auskunftersuchen der §§ 11 ff. BVerfSchG-E und biometrische Datenabgleiche, § 8 Abs. 1 Satz 2 Nr. 2 BVerfSchG-E, ein, da diese nicht als nachrichtendienstliche Mittel systematisiert sind (siehe dazu bereits A. III. 1.) und nicht in allen Fällen eine erheblich beobachtungsbedürftige Bedrohung voraussetzen. Daher können Daten aus Auskunftersuchen und biometrische Abgleich-erkenntnisse unter den geringen Voraussetzungen des § 56 Abs. 3 BVerfSchG übermittelt werden. Die Norm fordert jedoch keinerlei Übermittlungsschwelle, weder eine konkretisierte Gefahr noch sonst eine Tatsachengrundlage für eine Übermittlung. Dabei gelten die Erfordernisse einer Übermittlungsschwelle nach bundesverfassungsgerichtlicher Rechtsprechung auch für Daten, die mit weniger eingriffsintensiveren nachrichtendienstlichen Mitteln erhoben wurden.⁴⁹ Sofern die Gesetzesbegründung (S. 353 des Entwurfs) darauf abstellt, dass die unter § 56 Abs. 3 BVerfSchG-E fallenden Daten nicht qualifiziert eingreifend gewonnen wurden, kann dies den Verzicht auf eine Übermittlungsschwelle daher nicht rechtfertigen. Die letztlich anlasslose Übermittlungsbefugnis wird der hohen Sensibilität der Daten und der Eingriffsintensität der Datenerhebungen (vor allem der Auskunftersuchen und biometrischen Abgleiche, die als nachrichtendienstliche Mittel zu qualifizieren wären, siehe dazu bereits A. III. 1. und 5.) nicht gerecht und ist als verfassungswidrig anzusehen.

Aus diesem Grund ist auch § 56 Abs. 4 BVerfSchG-E verfassungswidrig, der die Übermittlung von Daten aus Auskunftersuchen auch an Strafverfolgungsbehörden zulässt. Hier ist zwar das Erfordernis tatsächlicher Anhaltspunkte normiert. Das Bundesverfassungsgericht verlangt für die Übermittlung von Daten an Strafverfolgungsbehörden aber einen Verdacht begründende Tatsachen⁵⁰, so wie es in § 48 Abs. 1 BVerfSchG auch ausdrücklich vorgesehen ist. Dem wird die Übermittlungsschwelle des § 56 Abs. 4 BVerfSchG nicht gerecht.

⁴⁹ Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, BVerfGE 162, 1, Rn. 242.

⁵⁰ Vgl. BVerfG, Beschluss vom 17. Juli 2024 – 1 BvR 2133/22, BVerfGE 169, 130, Rn. 110.

B. Nachrichtendienstliche Kontrolle und Transparenz

Mit der Neufassung der gesetzlichen Grundlagen für BND und BfV wird auch die Kontrolle der Geheimdienste neu strukturiert. Dabei wird mit dem vorliegenden Entwurf die Kontrolle von BND und BfV im Wesentlichen dem **UK-Rat** übertragen. Dieser soll nun nicht mehr nur Überwachungstätigkeiten des BND, sondern **umfassend die Rechtmäßigkeit der Aufgabenwahrnehmung von BfV und BND** kontrollieren. Damit soll der „Zersplitterung“ der Kontrolle begegnet werden (§ 625 des Entwurfs). Die einheitliche Struktur soll dabei einen effektiveren Grundrechtsschutz bewirken, Doppelstrukturen beenden und die Ressourcen des Bundes schonen.

Als Rechtsgrundlage wird ein zentrales Gesetz über die Rechtskontrolle durch den Unabhängigen Kontrollrat geschaffen. Die Arbeitsstruktur des UK-Rats mit einem gerichtsähnlichen und einem administrativen Kontrollgremium bleibt dabei erhalten. Unter- oder Spezialabteilungen werden nicht geschaffen. Dem UK-Rat werden dabei insbesondere die früheren Aufgaben der G10-Kommission übertragen.

Zentrale Aufgabe ist die Vorabkontrolle gemäß § 27 Abs. 1, 3 Nr. 1, 2 UKRatG-E in Verbindung mit § 34 BVerfSchG-E und § 98 Abs. 1, 2 BNDG-E. Dabei ist gemäß § 3 Abs. 1 UKRatG-E bei **Rechtskontrolle durch den UK-Rat keine Zuständigkeit des*der BfDI** mehr gegeben. Die **Kontrollzuständigkeit des UK-Rats ist vorrangig**. Damit beschränkt sich für das BfV die Kontrollbefugnis des*der BfDI nun gemäß § 70 Abs. 2 Nr. 2 BVerfSchG-E auf die datenschutzrechtliche Kontrolle auf nicht anlassbezogene Verarbeitungen im Rahmen von allgemeiner Verwaltung, Aus- und Fortbildung und Mitwirkung nach § 2 Abs. 5 BVerfSchG-E. **Die datenschutzrechtliche Kontrolle** im Rahmen der **Aufgabenwahrnehmung** des BfV und bei Schutzmaßnahmen liegt nun **vollständig in der Zuständigkeit des UK-Rats**. Dies gilt nicht nur für die Vorabkontrolle, sondern auch im Falle von nachträglicher Kontrolle und bei Ersuchen von Einzelpersonen, § 70 Abs. 1 BVerfSchG-E bzw. § 38 UKRatG-E. Selbiges gilt für den BND, § 98 Abs. 1, 2 BNDG-E. Die **Aufgabenwahrnehmung der Geheimdienste selbst** wird nun **nicht mehr von dem*der BfDI beaufsichtigt**.

Kritisch zu bewerten sind in diesem Zusammenhang **die Vereinfachungen** und **Lockerungen** der Kontrollverfahren. Nicht nur werden die Möglichkeiten zur Entscheidung durch einzelne Mitglieder des UK-Rats erheblich erweitert, § 28 UKRatG-E. Erstmals wird den Geheimdienstbehörden auch ermöglicht, Maßnahmen, die grundsätzlich der Vorabkontrolle unterliegen, bei Gefahr im Verzug sofort vollziehbar zu erklären und bereits vor der Vorabkontrolle zu vollziehen, § 31 UKRatG-E. Bisher war auch in solchen Fällen eine Vorabkontrolle notwendig. Der Eilbedürftigkeit wurde mit

Zwischenfeststellungsanordnungen begegnet, in der individuelle Aufklärungsmaßnahmen für eine fest umrissene Gruppe von Cyber-Angriffen vorab als rechtmäßig bestätigt wurde.⁵¹ Der vorliegende Entwurf lockert damit die Kontrollmechanismen, während er gleichzeitig die Befugnisse der Nachrichtendienste erheblich und strukturell erweitert. In diesem Zuge die Kontrolle nicht nur zu zentralisieren, sondern auch zu vereinfachen, steht im **Widerspruch** zum **nun höheren Erfordernis umfassender Kontrolle**. Dies gilt sowohl für die neugeschaffenen operativen Maßnahmen für die Nachrichtendienste als auch für neue technische Möglichkeiten der Überwachung.

Die neuen Kontrollstrukturen **entziehen** den Bereich der nachrichtendienstlichen Aufgabenwahrnehmung, also die nachrichtendienstlichen Ermittlungsaufgaben sowie die neu ermöglichten Eingriffsbefugnisse, der **Kontrolle durch den*die BfDI**. Dies verkürzt den **Grundrechtsschutz**, dem durch eine verteilte Kontrolle entsprechend der fachlichen Spezialisierungen besser Rechnung getragen ist. **Die unabhängige Aufsicht über die Nachrichtendienste wird nachhaltig geschwächt**, wenn **der*die BfDI** mit eigener **spezieller rechtlicher Expertise und technischen Spezialerkenntnissen** sowie **eigenem Erfahrungswissen gerade** im Umgang mit **technischen Fragen keine Kontrollzuständigkeiten mehr innehat**. Dies gilt insbesondere für die **Kontrolle technischer Datenverarbeitungen und Schutzmaßnahmen im digitalen Bereich**. Hier kann der*die BfDI eine weitreichendere nicht nur juristische Datenschutzkontrolle vornehmen und so die Datensicherheit tatsächlich verifizieren. Ebenso gilt dies für die Bearbeitung von **Individualbeschwerden**. Eine Öffnung des bisher streng geheim arbeitenden UK-Rats für Betroffene und Anwalt*innen ist ebenso wenig ersichtlich wie die Regelung von Verfahrensrechten.

Der UK-Rat selbst bleibt **strukturell im Wesentlichen unverändert**. Lediglich das gerichtsähnliche Kontrollorgan soll um zwei nichttrichterliche Mitglieder erweitert werden. Eine weitere personelle und strukturelle Ausweitung entsprechend der immensen neuen Kontrollaufgaben erfolgt nicht. Das administrative Kontrollorgan bleibt gänzlich unverändert. Es ist zu befürchten, dass schon **aus Kapazitätsgründen keine angemessene Kontrolle** in allen Anwendungsfällen gewährleistet werden kann. Dies gilt insbesondere mit Blick darauf, dass der UK-Rat nun auch Kontrollen aufgrund von Ersuchen von Einzelpersonen bearbeiten soll. Der UK-Rat ist **bislang nicht als Beschwerdestelle** ausgestattet. Für den Umgang mit Bürgerbeschwerden und Individualverfahren bedürfte es vollständig neuer Arbeitsstrukturen. In der Verwaltung des UK-Rats sollen zwar neue Planstellen geschaffen werden (S. 231 des Entwurfs), es erscheint aber zweifelhaft, ob diese Zuwachse genügen.

51 Unabhängiger Normenkontrollrat, Diskussionsentwurf eines Gesetzes über den unabhängigen Kontrollrat und zur Änderung des BND-Gesetzes, S. 40.

Erforderlich wäre jedenfalls, dass der UK-Rat **tatsächlich befähigt** wird, eine umfassende Rechtmäßigkeitskontrolle der nachrichtendienstlichen Handlungen auch vorzunehmen. Die Aufnahme zweier nichtrichterlicher Mitglieder in das gerichtsähnliche Gremium genügt hierbei keinesfalls. Auch diese Mitglieder müssen Volljurist*innen sein (§ 14 Abs. 2 Nr. 3 UKRatG-E) und sind auf eine enge Auswahl juristischer Berufe beschränkt. Auch die übrigen Personalerweiterungen genügen nicht. Es ist nicht ersichtlich, dass für eine **Kontrolle digitaler Maßnahmen** wie **KI-basierte Datenanalysen, Trojaner-Einsätzen oder digitalen „Schutzmaßnahmen“** wie **Hackbacks angemessene Kontrollstrukturen** geschaffen werden. Für eine Aufsicht über solche Maßnahmen bedarf es neben ausreichender technischer Infrastruktur vor allem einer Kontrolle **durch Spezialist*innen aus dem IT-Bereich**. Eine datenschutzrechtliche Kontrolle allein an juristischen Maßstäben kann bei den neu geschaffenen Befugnissen zum Schutz der Grundrechte keinesfalls genügen. Vielmehr bedarf es unbedingt einer auch **technischen Kontrolle von genutzter Software und Hardware im Einsatz**. Dies gilt insbesondere für den Einsatz komplexer technischer Systeme und Künstlicher Intelligenz. Nur durch eine intensive technische Überprüfung können Fehler und algorithmische Diskriminierung erkannt werden. Auch technische Manipulationen, Hintertüren und unbefugte Datenzugriffe von außen sind nur bei spezialisierter technischer Prüfung erkennbar. Dem UK-Rat fehlt hierfür – in seiner aktuellen und nun geplanten Form – schon der notwendige personelle Unterbau.

Abschließend werden die Nachrichtendienste durch Änderungen des Informationsfreiheitsgesetzes noch intransparenter als bisher.⁵² Die Gesetzesbegründung (§ 659 des Entwurfs) führt an: „Alle Tätigkeiten der Nachrichtendienste sollen nach dem Willen des Gesetzgebers vom Anspruch auf Informationszugang ausgeschlossen sein“. **Parallel zur gravierenden Befugnisausweitung und zur geschwächten Kontrolle der Nachrichtendienste wird auch deren öffentliche Einsehbarkeit nochmals verengt.**

⁵² So auch *Biselli/Leisegang/Reuter*, Geheimdienstreform Zeitenwende für Spione, netzpolitik.org vom 10. Juli 2026, abrufbar unter <https://netzpolitik.org/2026/geheimdienstreform-zeitenwende-fuer-spione/>.

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 zur Reform der Nachrichtendienste¹ (im Folgenden: „**Referentenentwurf**“ oder „**Entwurf**“) ist ausgesprochen umfangreich (707 Seiten), sehr komplex, weil er 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.

* Redaktionell durchgesehene Version der Stellungnahme vom 14. Juli 2026.

¹ Abrufbar unter:

https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referententwuerfe/OESI2/NDRRefG.pdf?__blob=publicationFile&v=1

Inhaltsverzeichnis

Zusammenfassung	4
I. Grundfragen	7
1. Aufgaben und Bedrohungsdogmatik	7
a) Verfassungsrechtlicher Maßstab.....	7
b) Stufensystematik der §§ 2 ff. BNDG-E.....	8
aa) Rechtsgüter und Grundtatbestand (§ 2 BNDG-E)	8
bb) Qualifikationsstufen	9
2. Operative Befugnisse des BND: Erweiterte nachrichtendienstliche Maßnahmen	10
a) Regelungsinhalt	10
b) Bewertung	11
3. Trennungsgebot und Inlandstätigkeit	12
4. Logik des Ausnahmezustands	13
II. Einzelne Befugnisse	14
1. Zugriff auf informationstechnische Systeme.....	14
a) Online-Durchsuchung.....	14
b) Weiterleitung von IT-Schwachstellen an den BND	16
c) Aktive Cybermaßnahmen („Hackbacks“)	18
d) Zugriff auf Passwörter	19
e) Heimlicher Zugriff auf IT-Systeme von Telekommunikationsanbietern	20
f) Heimliche Spurenerhebung in IT-Systemen	21
2. Strategische Aufklärung.....	21
a) Begrenzung des Umfangs	22
b) Weitergabe von Rohdaten ohne Filterung und Einsichtnahme.....	22
c) Zugriff auf reine Inlandskommunikation	23
d) Auslandskommunikation	23

e)	Qualifizierte Inlandskommunikation.....	23
3.	Ankauf von Daten (ADINT)	23
4.	KI-Analyse	24
a)	Einsatz von KI-Anwendungen	24
b)	Verwendung von KI-Analysen	26
c)	Digitale Souveränität.....	27
5.	Biometrischer Abgleich	27
6.	Zugriff auf Videoüberwachungsanlagen.....	28
7.	Allgemeine Regelungen zu nachrichtendienstlichen Mitteln.....	29
a)	Erprobungsklausel	29
b)	Schutz von Berufsgeheimnisträgern.....	29
III.	Aufsicht und Kontrolle.....	30
1.	Entmachtung der BfDI.....	30
2.	Reform des UKR	30

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 die **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**“ ein, 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 die 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 der **Ankauf von Daten bei kommerziellen Anbietern (ADINT)** zum *modus operandi* des BND gehört. Es fehlt aber weiterhin eine gesetzliche Regelung. Diese muss sicherstellen, dass keine 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 Rechnung, die sogar Gefährlichkeitsanalysen erstellen sollen; z. B. fehlt eine robuste KI-Governance, eine Kontrolle durch den UKR sowie 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 entmacht**et 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 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 Sicherheit**, wenn ihre Gefährdung aus Sicht der Bundesrepublik Deutschland

⁵ BVerfGE 154, 152 Rn. 127 f. – Strategische Ausland-Ausland-Fernmeldeaufklärung;

⁶ Referentenentwurf, S. 377 und S. 378.

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 diese 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, der damit letztlich für jede Bedrohung mit Auslandsbezug von einigem Gewicht zuständig wird. Dies ist problematisch, wenn die Bedrohungen keine „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 kritischen 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 für ein Bedrohungsfeld allein auf die **organisierte Kriminalität** abgestellt wird, die auf die Begehung von Straftaten mit erheblicher Bedeutung gerichtet ist.

⁷ BVerfGE 154, 152 Rn. 128, 162, 176 – Strategische Ausland-Ausland-Fermeldeaufklärung; BVerfGE 100, 313 (373) – G-10-Gesetz.

⁸ Referentenentwurf, S. 384.

⁹ BVerfGE 154, 152 Rn. 128 – Strategische Ausland-Ausland-Fermeldeaufklärung.

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 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; die Maßnahme 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.
- 15 Dem Einsatz nachrichtendienstlicher Mittel geht ein zweistufiges Verfahren voraus: Zuerst muss eine spezifische Gefährdungslage – tatsächliche

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.

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 in verschiedenen Bereichen auf, die durch die „**Verpolizeilichung**“ der **Nachrichtendienste** entstehen, d.h. durch die 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 beschränkt¹⁴ 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 In der Folge 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 die Maßnahme auf Informationen aus der internationalen Zusammenarbeit der Nachrichtendienste aufbaut.¹⁸

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.

¹⁸ Referentenentwurf, S. 524.

- 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 des Auslandsnachrichtendienstes 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. Wiederkehrende Argumentationstopoi sind die fehlenden Fähigkeiten anderer Behörden und die Schwierigkeit, Daten ausländischer Dienste mit anderen Behörden aufgrund der Third Party Rule zu teilen. Letzteres 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 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

¹⁹ Vgl. BVerfGE 121, 135 Rn. 71 – Luftraumüberwachung Türkei.

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

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“. Dieser in § 125 Abs. 3 BNDG-E geregelte Zustimmungsfall ist in dieser Form nicht im Grundgesetz angelegt, sondern wird durch das BNDG-E neu eingeführt. Er soll dann eintreten, wenn der Verteidigungs- oder Spannungsfall unmittelbar bevorsteht 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 und grundrechtliche Sicherungen wegfallen, z.B. der Schutz von Berufsgeheimnisträgern; ferner können z.B. Behörden und Unternehmen zu Unterstützungsleistungen herangezogen werden.
- 28 Eine allgemeine Unterscheidung zwischen einer „normalen Lage“ und einer Art „Notstandslage“ oder „Ausnahmezustand“, in der Grundrechtssicherungen pauschal abgesenkt werden, kennt das Grundgesetz

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

– anders als etwa das französische Recht – nicht. Dies hat historische Gründe, beruht aber auch auf der 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 somit von der Bundesregierung mit Zustimmung der regierungstragenden Mehrheit im PKGr festgestellt werden – anders als der Spannungs- und der Verteidigungsfall, deren Feststellung jeweils eine Zweidrittelmehrheit der abgegebenen Stimmen im Bundestag voraussetzt; beim Verteidigungsfall muss diese Mehrheit zugleich mindestens der Mehrheit der Mitglieder des Bundestages entsprechen, zudem ist die Zustimmung des Bundesrates erforderlich. Verfassungsrechtlich schließlich bestehen gravierende Zweifel: Der in § 125 Abs. 3 BNDG-E geregelte Zustimmungsfall hat in dieser Ausgestaltung 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 vorsehen. 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-Durchsuchung 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 der – 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

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

Menschen und die damit verbundene Aussagekraft der darauf verarbeiteten 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 mit anderen Personen selbstbestimmt über die Nutzung des Systems verfügt.²⁶ Dies ist auch nachvollziehbar, weil erstens viele Menschen ihre beruflichen IT-Systeme auch für private Zwecke nutzen²⁷ und zweitens auch der berufliche Kontext ein wesentlicher Teil der

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.

Lebensgestaltung und Persönlichkeit ist. Soweit sich eine Online-Durchsuchung gegen eine Person 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. für die 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 seien.³²
- 35 Wenn der Staat sich entschließt, Schwachstellen für eigene Zwecke zu nutzen, entsteht ein **Zielkonflikt mit der IT-Sicherheit**. Schwachstellen sind eine

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.

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: 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 auszunutzen. Es stellt sich allerdings auch die Frage, ob ein solcher Prozess angesichts der Geschwindigkeit, mit 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 dem BSI vertraulich Sicherheitslücken gemeldet werden können. Sicherheitsforscher oder White-Hat-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 dass der CVD-Prozess

³³ BVerfGE 158, 170 Rn. 40, 41 f. – IT-Schwachstellen.

³⁴ BVerfGE 158, 170 Rn. 43 – IT-Schwachstellen.

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.

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. Solche Rechner 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

³⁵ Referentenentwurf, S. 509.

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 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, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird. 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 über die Nutzungsvoraussetzungen beim BND, obwohl der Gesetzgeber sie festlegen müsste. Ungeregt bleibt zudem der Zugriff selbst, der bereits die Integrität des IT-Systems und damit das IT-System-Grundrecht verletzt³⁸ (ähnlich wie der Einbruch in eine Wohnung, unabhängig davon, ob etwas gestohlen wird).

³⁶ Referentenentwurf, S. 525.

³⁷ BVerfGE 141, 220 Rn. 209 f. – BKA-Gesetz.

³⁸ BVerfG MMR 2026, 44 Rn. 100, 103 – Trojaner I.

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 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 werden 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.

³⁹ Referentenentwurf, S. 485.

- 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 Maßnahme darf der BND greifen, wenn eine 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 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** und damit eine weitere Integritätsverletzung vorgenommen werden soll, 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 dem 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 des Verbots der

⁴⁰ Referentenentwurf, S. 424.

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 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 oder an ausländische Dienste im Rahmen von Kooperationen nach §§ 43, 44 BNDG-E erlaubt. Es bleibt unklar, ob und wie die Limitierungen der §§ 43, 44 BNDG-E ohne eine Sichtung angewendet werden können.⁴³

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.

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 zudem die Weiterverwendung von „unkenntlich“ gemachten Daten, wenn diese gerade dem Aufspüren von Kommunikationsnetzen 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 auf Basis 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

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

⁴⁵ Referentenentwurf, S. 488.

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

- 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 berücksichtigen sein, ob der Verkäufer die Daten rechtmäßig verarbeitet und wie er sie gewonnen hat, welcher Personenkreis betroffen ist – häufig handelt es sich um Massendaten – 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 Programmierung lösen und ihre Ergebnisse so

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

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 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 eine unklare Regelung zu Forschungsdaten. Bedenklich ist in diesem Zusammenhang § 52 Abs. 2 Nr. 1 BNDG-E, der eine Weiterverarbeitung von allgemein zugänglichen 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, 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

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 aufgrund des Risikos von Diskriminierung BVerfGE 165, 363 Rn. 77, 90, 95, 100 – Automatisierte Datenanalyse.

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.

Nachrichtendiensttätigkeiten eine andere Eingriffsschwelle akzeptieren würde. Bereits für eine weit weniger grundrechtsintensive Datenanalyse 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, weil 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, indem er zwischen der Verarbeitung von Daten durch KI-Anwendungen einerseits und dem Abruf von Auswertungsprodukten andererseits unterscheidet. Positiv an diesem Ansatz ist, dass er es 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 für Verhaltens- und Persönlichkeitsprofile und personenbezogene 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 in die KI-Analyse („automation bias“), dem durch Verfahrensregelungen (z.B. dokumentierte Plausibilitätsprüfung) entgegengewirkt werden muss.

⁵⁵ BVerfGE 156, 11 Rn. 119 – Antiterrordateigesetz II.

⁵⁶ BVerfGE 165, 363 Rn. 96 ff., 100, 121 – Automatisierte Datenanalyse.

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 statuiert eine „Anschaffungssubsidarität“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 aus Drittstaaten nicht ausgeschlossen. Für diesen Fall sind keine gesetzlichen Vorgaben vorgesehen, um die Qualität und Vertrauenswürdigkeit des Anbieters und vor allem der Software sicherzustellen (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 ausländischen Muttergesellschaft, könnten ausländische Stellen Herausgabeverlangen an diese richten 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 Demonstrationen, 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**.

⁵⁷ Referentenentwurf, S. 532.

⁵⁸ Siehe aber BVerfGE 165, 363 Rn. 100 – Automatisierte Datenanalyse zu den Gefahren.

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 Bundesministerium des Innern und für Heimat); *Schantz*, CR 2026, 91 Rn. 33 jeweils m.w.N.

- 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).
- 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 werden 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 für andere Zwecke nur zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erlaubt, § 15 BNDG-E den Zugriff aber allgemein für Zwecke der Auslandsaufklärung eröffnet.⁶⁰

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

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 so weit 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 für besonders geschützte Vertraulichkeitsbeziehungen strengere Maßstäbe gelten und teilweise – etwa im Falle von Rechtsanwälten – ein absoluter Schutz gilt. Da die Befugnisse des **BND, im Inland** tätig zu werden, erheblich erweitert werden sollen, muss sichergestellt werden, dass Vertraulichkeitsbeziehungen im Inland oder mit Inlandsbezug, weil sie 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 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 Vertraulichkeitsbeziehung zwischen Anwalt und Mandant entfallen zu lassen, nur weil die Rechtsanwaltsfachangestellte oder der IT-Dienstleister eine solche Verstrickung aufweist. 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 vorgesehen (§ 97 Abs. 3 S. 1 Nr. 1 i.V.m. § 22 Abs. 3 BNDG-E).

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

⁶² BVerfGE 154, 152 Rn. 194 – Strategische Ausland-Ausland-Fernmeldeaufklärung.

III. Aufsicht und Kontrolle

- 73 Hinsichtlich der nachrichtendienstlichen 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 die 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 einen Amicus Curiae (*tech amicus*).

2. Reform des UKR

- 75 Es ist zu begrüßen, dass auch Personen ohne Hintergrund in der Justiz oder einer Sicherheitsbehörde 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 G-10-Kommission fehlt ein Aufsichtsgremium mit einem politisch-juristischen Hintergrund.
- 76 Zu überprüfen wäre, warum sich nach § 2 Abs. 1 UKRG-E die Kontrolle 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.
