Gesellschaft für Freiheitsrechte

freiheitsrechte.org

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 **eingerissen**. 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

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 Bagatellstraftaten 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 Regelbeispiele[2] 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 verschleiernd 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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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 Bespiele 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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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. Auskunftsersuchen, §§ 11 ff. BVerfSchG-E

Der vorliegende Entwurf qualifiziert Auskunftsersuchen 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 Auskunftsersuchen 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 Auskunftsersuchen 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 Auskunftsersuchen erhoben wurden, gestellt werden (siehe dazu sogleich A. V.).

Aus Gründen der Verhältnismäßigkeit sind die Auskunftsersuchen **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 ist[7]. 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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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 (S. 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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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-Grundrecht[11] 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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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 Schutzpflichten[16] 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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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 Datenanalyseurteil[17] 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 Bundesverfassungsgerichts[18] 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-ermittlungsbgefugnisse, 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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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 lizensiert haben soll[27] – obwohl keine Rechtgrundlage 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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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 möglich[32], 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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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 Berufsgeheimnisträger*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 Berufsgeheimnisträger*innen, § 32 Abs. 4 BVerfSchG-E

Ebenso ist der Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger*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-erklaert/.
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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

Möglichkeiten auf **vertrauliche Rechtsberatung**, da Menschen, die bestimmten Bestrebungen nahestehen, häufig bei bestrebungs- und szenenahen Anwält*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. i 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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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 Löschungsfrist 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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

Genau diese Rechtfertigung entfiele 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 Rechtgüterund einer engen Verbindung zu den Schutzgütern

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

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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 Auskunftsersuchen 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 Auskunftsersuchen 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 Auskunftsersuchen 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 Auskunftsersuchen 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 Tatsachen[50], 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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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 (S. 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, 2UKRatG-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

Zwischenfeststellunganordnungen 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 Anwält*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 nichtrichterliche 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.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

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 (S. 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/.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS