LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

PROF. DR. MARK A. ZÖLLER

LEHRSTUHL FÜR DEUTSCHES, EUROPÄISCHES UND INTERNATIONALES STRAFRECHT UND STRAFPROZESSRECHT, WIRTSCHAFTSSTRAFRECHT UND DAS RECHT DER DIGITALISIERUNG

Professor-Huber-Platz 2 · 80539 München

Prof. Dr. Mark A. Zöller

Geschäftsführer des Instituts für Digitalisierung und das Recht der Inneren Sicherheit (IDRIS)

Telefon +49 (0)89 2180-3542

Mark.Zoeller@jura.uni-muenchen.de

www.jura.uni-muenchen.de

Dienstadresse
Ludwigstr. 29/IV. OG, Raum 406
80539 München

Herrn
Stellvertretenden Vorsitzenden des Ausschusses
für Inneres und Heimat
des Deutschen Bundestages
Prof. Dr. Lars Castellucci, MdB
Platz der Republik 1

11011 Berlin

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)324 E

München, 03.11.2023

Schriftliche Stellungnahme

zum Gesetzentwurf der Bundesregierung
„Entwurf eines Gesetzes zur Änderung des BND-Gesetzes" (BT-Drs. 20/8627)

sowie

zum Gesetzentwurf der Bundesregierung
„Entwurf eines Gesetzes zum ersten Teil der Reform des Nachrichtendienstrechts" (BT-Drs 20/8626)

im Rahmen der Anhörung des Ausschusses für Inneres und Heimat am 6. November 2023

Sehr geehrter Herr Vorsitzender, sehr geehrte Damen und Herren Abgeordnete,

für die Einladung zur oben genannten Anhörung und die Gelegenheit zur Stellungnahme darf ich mich herzlich bedanken. Aufgrund der Kürze der zur Verfügung stehenden Zeit, werde ich mich im Schwerpunkt auf den zweitgenannten Gesetzentwurf beziehen, der sich im Wesentlichen mit der Reform der Übermittlungsvorschriften

sowie neuen Maßnahmen zur Eigensicherung des Bundesamtes für Verfassungsschutzes (BfV) befasst. Sofern Parallelen zu den entsprechenden Befugnissen des Bundesnachrichtendienstes (BND) bestehen oder diese aus meiner Sicht geschaffen werden müssten, wird in diesem Kontext auch auf den erstgenannten Gesetzentwurf der Bundesregierung für eine Neuregelung des BNDG eingegangen.

Vor diesem Hintergrund erlaube ich mir, wie folgt Stellung zu nehmen:

A. Vorbemerkungen

Auffällig ist, dass sich beide Gesetzentwürfe inhaltlich in erheblichem Umfang von den Vorgaben des Bundesverfassungsgerichts (BVerfG) aus den primär einschlägigen Entscheidungen zum Bayerischen Verfassungsschutzgesetz (BayVSG)

> BVerfG, Urt. v. 26.04.2022, 1 BvR 1619/17

sowie den Übermittlungsbefugnissen des Bundesverfassungsschutzgesetzes

> BVerfG, Beschl. v. 28.09.2022, 1 BvR 2354/13

entfernt haben. Stattdessen werden **vor allem aktuelle Wunschvorstelllungen der Sicherheitsbehörden** kodifiziert. Dies führt gerade im Bereich der Datenübermittlungen durch das BfV anstelle der aus Karlsruhe mit Blick auf den Grundsatz der Verhältnismäßigkeit intendierten Einschränkungen im Vergleich zur geltenden Rechtslage sogar zu einer **Ausweitung der nachrichtendienstlichen Befugnisse**. Der Regelungsanlass für das Gesetzgebungsverfahrens wird auf diese Weise in sein Gegenteil verkehrt. Dabei wird von den Entwurfsverfassern übergangen, dass das BVerfG in seiner Entscheidung einen eindeutigen **„Strafmechanismus“** etabliert hat:

> dazu BVerfG, Urt. v. 26.04.2022 – 1 BvR 1619/17, Rn. 172; Zöller, StV 2022, 693 (696).

Entsprechen die Übermittlungsregelungen für die Nachrichtendienste auch in Zukunft nicht den verfassungsgerichtlich skizzierten Anforderungen, dann sollen für die Dienste überhaupt keine Maßnahmen im Vorfeld von polizeirechtlicher Gefahr und strafprozessualem Anfangsverdacht mehr möglich sein. Rechtspolitisch wird man also in dieser Situation über alle Parteigrenzen hinweg gut beraten sein, die aus Karlsruhe gezogenen Grenzen eindeutig einzuhalten, um nicht das Risiko einzugehen, am Ende ohne Vorfeldbefugnisse dazustehen. Wer sich für zu weite (Übermittlungs-)Befugnisse der deutschen Nachrichtendienste stark macht, läuft Gefahr, den Sicherheitsbehörden für ihre wichtige Tätigkeit im Rahmen unserer wehrhaften Demokratie im Endeffekt einen „Bärendienst“ zu erweisen. **Zu weite Übermittlungsbefugnisse bedeuten also den Verlust von nachrichtendienstlichen Befugnissen bei**

der Informationserhebung im Wege der Vorfeldaufklärung. Das Bundesverfassungsgericht hat insbesondere in seiner Entscheidung zum BayVSG deutlich gemacht, dass seine Geduld mit Sicherheitsgesetzgebern in Bund und Ländern erschöpft ist, die immer wieder die von ihm markierten Grenzen überschreiten. Es erscheint deshalb logisch nicht nachvollziehbar, dass beide Entwürfe, insbesondere aber der Entwurf zur Neuregelung des BVerfSchG, dieses Risiko ausblenden bzw. einzugehen bereit sind. Angesichts der in diesem Kontext ungewöhnlich klaren Vorgaben des BVerfG für eine Einhegung der Übermittlungsvorschriften sind diese Gesetzgebungsverfahren der denkbar schlechteste Zeitpunkt, um Vorschriften zu etablieren, die diese Vorgaben mehr oder minder geschickt zu umgehen versuchen, um weitestmögliche Flexibilität für die Sicherheitsbehörden zu bewahren oder sogar noch auszubauen.

Auffällig ist des Weiteren, dass gerade die **Entwurfsbegründung** zur Reform des Bundesverfassungsschutzrechts in erheblichen Teilen trotz weitschweifiger und vordergründig juristisch-fachterminologischer Formulierung letztlich erstaunlich **inhaltsleer** bleibt. So werden vermeintliche juristische Notwendigkeiten suggeriert, die in Wahrheit nicht bestehen. Und zahlreiche Zitate aus der Rechtsprechung des BVerfG decken, liest man sie einmal nach, die von den Entwurfsverfassern gezogenen Schlüsse in Wirklichkeit nicht. Der Anwendungsbereich einzelner Bestimmungen wird nicht nur für juristische Laien, sondern für auch die interessierte und mit der Materie vertraute Leserschaft häufig nicht klar erkennbar. Insofern muss man erhebliche Zweifel daran anmelden, dass derart kryptisch formulierte Befugnisse zu Eingriffen in die Grundrechte der Bürgerinnen und Bürger in der Praxis für die mit Fragen der Übermittlung an andere Stellen befassten Sachbearbeiterinnen und Sachbearbeiter des BfV Sicherheit bei der Rechtsanwendung schaffen. Wenn selbst sog. Experten derartige Normen ehrlicherweise nicht verstehen, wie will man dann den Angehörigen der Dienste solche risikobehafteten Entscheidungen aufbürden?

Zudem **konterkarieren intransparente Befugnisnormen das Ziel, die Tätigkeit der Dienste insgesamt transparenter und bürgerfreundlicher auszugestalten**, um das nötige Vertrauen und den Rückhalt in der Bevölkerung zu schaffen. Allerdings steht zu befürchten, dass dieser Mangel an Transparenz und Normenklarheit zu einem gewissen Grad gewollt sein könnte. Auf diese Weise werden „Platzhalter" für möglicherweise erst in der Zukunft erkennbar werdende Fallkonstellationen geschaffen. Dieses mit Blick auf die praktische Arbeit der Dienste durchaus nachvollziehbare Anliegen verkennt allerdings die Tatsache, dass Grundrechtseingriffe wie auch die Übermittlung von personenbezogenen Daten zu unbestimmten oder noch nicht hinreichend bestimmbaren Zwecken nach ständiger Rechtsprechung des BVerfG strikt untersagt sind:

BVerfGE 65, 1 (46); 100, 313 (360); 115, 320 (350); 125, 260 (321).

Durch zahlreiche Zitate aus der Verfassungsrechtsprechung wird zudem in der Entwurfsbegründung an vielen Stellen der Eindruck eines Umsetzungsbedarfs erweckt, der sich aus den zitierten Fundstellen jedenfalls so häufig gar nicht ergibt. **Stellungnahmen aus der Rechtswissenschaft** werden gerade im Kontext der Neuregelungen des BVerfSchG nur sehr **einseitig ausgewertet**. Insofern erhalten die Abgeordneten zumindest aus dem Entwurf selbst naturgemäß kein ausgewogenes Bild des gesamten Meinungsspektrums und der Rechtslage.

Schließlich ist darauf hinzuweisen, dass für zwei vergleichbare Materien – Rechtsgrundlagen für die Arbeit von BfV und BND – von der Bundesregierung **zwei unabhängige Gesetzesvorschläge vorgelegt** wurden**, die sich in Stil, Umfang und Regelungsdichte teilweise erheblich unterscheiden**. Das ist faktisch ohne Zweifel der Tatsache geschuldet, dass die Federführung für die Entwurfserstellung mit dem Bundesministerium des Innern und für Heimat (für das BVerfSchG) sowie dem Bundeskanzleramt (für das BNDG) in zwei verschiedenen Häusern lag. Aber auch wenn die unterschiedlichen Aufgabenstellungen für Inlands- und Auslandsnachrichtendienste gewisse Abweichungen im Detail rechtfertigen mögen, nehmen sich die beiden Entwürfe doch gegenseitig ein gewisses Maß an Überzeugungskraft, weil sie zum Ausdruck bringen, dass man in zwei parallelen Regierungsentwürfen nicht einmal zu grundlegenden Fragestellungen, wie z.B. Übermittlungskatalogen zu Gefahrenabwehr- und Strafverfolgungszwecken, Minderjährigen- oder Kernbereichsschutz oder dem Schutz von Berufsgeheimnisträgern, Konsens herstellen konnte. Schon diese nicht nachvollziehbaren Unterschiede in grundlegenden Fragen machen deutlich, dass die vorgeschlagenen Regelungen jeweils nicht alternativlos sind.

Dass diese beiden Entwürfe, sollten sie in dieser oder ähnlicher Gestalt tatsächlich Gesetzeswirklichkeit werden, jedenfalls in Gänze **keinen Bestand vor den Schranken des Bundesverfassungsgerichts** haben dürften, soll anhand der nachfolgend skizzierte Kritikpunkte an einzelnen Reglungen beispielhaft, d.h. ohne Anspruch auf Vollständigkeit, verdeutlich werden.

B. Einzelkritik

I. § 6 Absatz 3 Satz 5 BVerfSchG-E (Verlängerung der Speicherungsfrist für Protokolldaten)

Mit dieser Regelung soll die **Speicherungspflicht für Protokolldaten** im NADIS-System **auf fünf Jahre** und damit in erheblichem Maße **verlängert** werden. Dabei bleibt der Sinn und Zweck einer solchen massiven Ausweitung der Speicherungsdauer (bislang: Löschung zum Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, d.h. ohnehin schon mit einer faktischen Speicherungsdauer zwischen ein und zwei Jahren) auch unter Berücksichtigung der Entwurfsbegründung unklar: diese Daten dürfen nach geltendem Recht (§ 6 Absatz 3 Satz 4 BVerfSchG) nur „für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage verwendet werden". Es geht also erkennbar um die technische Absicherung datenschutzrechtlicher Vorgaben. Nach der Entwurfsbegründung (BT-Drs. 20/8626, S. 17) sollen aber angesichts aktueller Vorkommnisse („Fall Carsten L.") vor allem Spione in den eigenen Reihen enttarnt werden. Wie das genau mit länger verfügbaren Protokolldaten anstelle besserer Sicherheitsmaßnahmen erreicht werden soll, wird nicht erläutert. Hier scheint **unter dem Deckmantel der Eigensicherung der Wunsch nach längeren Speicherfristen** in Bezug auf Daten **bedient** zu werden, die hierzu praktisch möglicherweise gar nichts beitragen können.

Es wird daher empfohlen, § 6 Absatz 3 Satz 5 BVerfSchG-E zu streichen oder ein klares gesetzlichen Konzept dafür zu schaffen, wie mit verlängerten Speicherungspflichten für Protokolldaten wirksam Eigensicherung für das BfV verwirklicht werden kann.

II. § 19 BVerfSchG-E (Übermittlung an inländische öffentliche Stellen zur Gefahrenabwehr)

1. § 19 Absatz 1 Nr. 1 BVerfSchG-E

Diese Bestimmung soll offensichtlich (auch) die Datenübermittlung an Polizeibehörden in Bundesländern ermöglichen, die in ihrem Polizeirecht bereits ein Einschreiten **zur Abwehr lediglich drohender Gefahren** erlauben. Sie ist damit in erster Linie eine „Lex Bavaria" (vgl. Art. 11a des Bayerischen Polizeiaufgabengesetzes [BayPAG]). Die im Freistaat Bayern seit dem Jahr 2017 beständig ausgeweitete Absenkung der präventivpolizeilichen Eingriffsschwelle auf lediglich drohende Gefahren ist Gegenstand zahlreicher, derzeit noch vor dem BVerfG und dem Bayerischen Verfassungsgerichtshof (BayVerfGH) anhängiger Verfassungsklagen von Vertreterin-

nen und Vertretern von SPD, Bündnis 90/Die Grünen und FDP gegen die entsprechenden Regelungen im BayPAG, in denen die Unbestimmtheit und Unverhältnismäßigkeit entsprechender Bestimmungen gerügt wird. Mit der Umsetzung der in § 19 Abs. 1 Nr. 1 BVerfSchG-E vorgeschlagenen Übermittlungsregelung würde man somit „durch die Hinter- bzw. Übermittlungstür" die Verfassungskonformität der drohenden Gefahr als polizeiliche Eingriffsschwelle anerkennen und den entsprechenden Verfassungsklagen den rechtlichen Boden entziehen:

Zöller, StV 2022, 693 (700).

Ungeachtet solcher verfassungsprozesstaktischer Erwägungen ist jedoch entscheidend, dass die Vorschrift die Vorgaben des Bundesverfassungsgerichts klar missachtet, wonach Datenübermittlungen an Gefahrenabwehrbehörden lediglich zur Abwehr „wenigstens hinreichend konkretisierter Gefahren" zulässig sein sollen:

BVerfG, Urt. v. 26.04.2022, 1 BvR 1619/17, Leitsatz 3a).

Diese konkretisierte Gefahr, die bislang noch kein expliziter Bestandteil der deutschen Polizei- und Ordnungsbehördengesetze ist, wurde allerdings als Begriff in der jüngeren Rechtsprechung des BVerfG näher ausgeformt:

BVerfGE 141, 220 (272 f.); BVerfG, Beschl. v. 28.09.2022, 1 BvR 2354/13, Rn. 134; Beschl. v. 9.12.2022, 1 BvR 1345/21, Rn. 91.

Sie beschreibt Entscheidungssituationen, die rechtsdogmatisch mit Blick auf die Strenge der Eingriffsvoraussetzungen in einem Bereich zwischen einer lediglich drohenden und einer konkreten Gefahr anzusiedeln sind. Aus dem Zusatz „wenigstens" folgt, dass dies nach Einschätzung des BVerfG die absolute **Mindestgrenze für Übermittlungen zu Gefahrenabwehrzwecken** darstellen soll. Übermittlungen nachrichtendienstlich erhobener Daten mit Personenbezug zur Abwehr lediglich drohenden Gefahren sind somit von vornherein unzulässig. Dies alles wird im vorgeschlagenen Gesetzeswortlaut nicht abgebildet.

Hinzu kommt, dass auch eine spezielle Regelung für die Übermittlung solcher personenbezogenen Daten fehlt, die das BfV durch **Maßnahmen der Wohnraumüberwachung** erhoben hat. Die Übermittlung solcher Daten an Gefahrenabwehrbehörden ist vor dem Hintergrund von Art. 13 Abs. 4 GG nur zur Abwehr dringender Gefahren für besonders gewichtige Rechtsgüter verfassungsrechtlich zulässig:

BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 248.

Es wird daher empfohlen, § 19 BVerfSchG-E dergestalt abzuändern, dass Übermittlungen an Gefahrenabwehrbehörden lediglich zur Abwehr zumindest konkretisierter Gefahren für klar und abschließend zu definierende, besonders gewichtige Rechtsgü-

ter zugelassen werden. Zudem empfiehlt es sich schon zugunsten der Rechtsanwender im BfV, eine Legaldefinition der konkretisierten Gefahr in den Gesetzestext aufzunehmen. Eine solche Legaldefinition könnte in Anlehnung an die Vorgaben des BVerfG wie folgt lauten: „Eine konkretisierte Gefahr liegt vor, wenn sich der zum Schaden führende Kausalverlauf zwar noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, aber bereits bestimmte Tatsachen im Einzelfall auf die Entstehung einer konkreten Gefahr für ein besonders gewichtiges Rechtsgut hinweisen." Im Übrigen ist die Übermittlung von Daten, die das BfV durch Maßnahmen der Wohnraumüberwachung erhoben hat, auf die Abwehr dringender Gefahren zu beschränken.

2. § 19 Absatz 1 Nr. 2 BVerfSchG-E

Diese Bestimmung enthält entgegen der Rechtsprechung des BVerfG **weder eine Beschränkung auf den Schutz besonders gewichtiger Rechtsgüter noch eine Bindung an die** verfassungsrechtlich unverzichtbare **Schwelle der zumindest konkretisierten Gefahr.** Auch eine inhaltliche Eingrenzung der zu verhindernden Straftaten fehlt, sofern es nur bei einem Höchststrafmaß von mindestens zehn Jahren Freiheitsstrafe bleibt. Dies ist bereits bei zahlreichen Straftatbeständen aus dem Bereich der mittleren Kriminalität der Fall (z.B. § 89a oder § 244 StGB). Im Übrigen erscheint die Regelung aus dogmatisch Sicht überflüssig, da die Verhinderung („Verhütung") von Straftaten ohnehin zu den Aufgaben der polizeilichen Gefahrenabwehr zählt. Die diesbezügliche Entwurfsbegründung (BT-Drs 20/8626, S. 19 f.), die auf die Notwendigkeit eines Gleichklangs mit Übermittlungen zur Strafverfolgung abstellt, ist rechtsdogmatisch unzutreffend.

Insofern wird empfohlen, diese evident verfassungswidrige Vorschrift ersatzlos zu streichen.

3. § 19 Absatz 2 BVerfSchG-E

Die **Definition der Schutzgüter** in § 19 Absatz 2 BVerfSchG-E ist **zu weit** geraten. Das BVerfG erlaubt Datenübermittlungen nur zum „Schutz besonders wichtiger Rechtsgüter". Unbestimmte Begriffe wie „sonstige Güter der Allgemeinheit" (Nr. 2) oder „vergleichbar besonders gewichtige Rechtsgüter" (Nr. 3) ermöglichen jenseits dieser Grenzen unvertretbaren Spielraum für den Rechtsanwender im Einzelfall. Auch ausdrücklich genannte Rechtsgüter wie Leib oder Freiheit sind nicht per se besonders wichtig, könnten dies aber natürlich im Einzelfall häufig sein. Mit ihrer einschränkungslosen Einbeziehung würde man die Datenübermittlung durch das

Bundesamt für Verfassungsschutz z.B. auch zur Abwehr von Gefahren durch leichte Körperverletzungen (z.B. Ohrfeigen) oder leichte Freiheitsbeeinträchtigungen (z.B. Bedrohungen oder kurzfristiges Festhalten) zulassen.

Insofern wird empfohlen, den Katalog besonders wichtiger Rechtsgüter deutlich enger zu fassen und insbesondere auf vage formulierte Auffang- bzw. Generalklauseln zu verzichten.

4. § 19 Absatz 3 Nr. 1 BVerfSchG-E

Bei den hier genannten Fällen, in denen nicht nur eine Übermittlungsbefugnis, sondern eine **Übermittlungspflicht** bestehen soll, handelt es sich auf Seiten der datenempfangenden Stelle nicht vorrangig um die Erfüllung von Gefahrenabwehraufgaben, sodass die Regelung schon systematisch falsch verankert sein dürfte und im Entwurfskontext der Sache nach eher unter das Dach des § 20 BVerfSchG-E gehört. Die in der Entwurfsbegründung zur Legitimierung angeführte, angeblich bereits eingetretene „Störung der Verfassungsschutzgüter" (BT-Drs. 20/8626, S. 21) hat im Gesetzeswortlaut keinen Niederschlag gefunden.

Insofern wird empfohlen, den sachlichen Regelungsgehalt des § 19 Absatz 3 Nr. 1 BVerfSchG verfassungskonform in den Anwendungsbereich von § 20 BVerfSchG zu überführen.

5. § 19 Absatz 3 Nr. 2 BVerfSchG-E

Der Anwendungsbereich dieser Vorschrift bleibt sowohl nach dem Wortlaut des Gesetzes als auch mit Blick auf die Begründung vollkommen im Dunkeln.

Die Vorschrift sollte ersatzlos gestrichen werden.

III. § 20 BVerfSchG-E (Übermittlung an inländische Stellen zum administrativen Rechtsgüterschutz)

Diese Vorschrift ist in der im Regierungsentwurf vorgeschlagenen Fassung in nahezu jeder Hinsicht als **verfassungswidrig** einzustufen. Durch die **Verwendung und Kumulation einer Vielzahl von unbestimmten Begriffen**, bleibt bereits der der Anwendungsbereich der Norm in erheblichen Teilen unklar. Formulierungen wie „besondere Gelegenheiten durch besondere Sachverhalte oder Rechtsverhältnisse für Handlungen, die die Bestrebungen oder Tätigkeiten besonders fördern" (Absatz 1 Nr. 3) bieten eher Stoff für juristische Kuriositätensammlungen, aber keine prakti-

kable Rechtsgrundlage für schwierige Entscheidungen in grundrechtssensiblen Bereichen. Wer so oft in einem Satz das Wort „besonders“ verwendet, hat seine Sache offensichtlich nicht besonders gut gemacht.

Im Übrigen liegt dem Regelungsvorschlag erkennbar der Leitgedanke zugrunde, die Möglichkeiten zur Übermittlung von personenbezogenen Daten für das BfV dadurch zu erweitern, dass die „operative Anwendung unmittelbaren Zwangs“ für den Datenempfänger ausgeschlossen wird, auch wenn diesem nach dem für ihn geltenden Recht von dem für ihn zuständigen Gesetzgeber solche Befugnisse eingeräumt worden sind. Ein solcher Ausschluss von operativen Anschlussbefugnissen im Recht der datenübermittelnden Stelle ist aber jedenfalls im Verhältnis zu solchen Empfängerstellen, die der Landesgesetzgebung unterfallen, **kompetenzwidrig**. Der Bund kann etwa den der Gesetzgebungskompetenz der Länder unterfallenden Landesverfassungsschutzbehörden und Landespolizeibehörden nicht die Nutzung von Zwangsbefugnissen im Einzelfall untersagen, die diese zuvor bereits abstrakt-generell von dem für sie zuständigen Landesgesetzgeber erhalten haben. Das Regelungskonzept des § 20 BVerfSchG-E geht aber auch sachlich in die falsche Richtung. Das BVerfG stellt lediglich darauf ab, ob der Datenempfänger nach den für ihn geltenden gesetzlichen Bestimmungen generell über operative Zwangsbefugnisse verfügt, und nicht darauf, ob diese im jeweiligen Einzelfall zur Anwendung kommen (sollen) oder nicht:

> BVerfG, Urt. vom 26.04.2022, 1 BvR 1619/17, Leitsatz 1.

Zudem lässt sich die Nutzung faktisch bestehender Zwangsbefugnisse bzw. der Verzicht hierauf auf Empfängerseite durch die übermittelnde Stelle praktisch **kaum wirksam kontrollieren**. Sind die Daten einmal herausgegeben, sind sie auch auf Empfängerseite in der Welt und können als Ermittlungsansätze genutzt werden. Von einem Rückgriff auf Zweckbindungsregelungen steht auch in den einschlägigen Judikaten des BVerfG nichts. Der Regelungsvorschlag ist daher ein teilweise verfassungsrechtlich unzulässiger „Kniff“ zur vermeintlichen **Legitimierung von weiteren Übermittlungsbefugnissen „am BVerfG vorbei“**.

Hinzu kommt, dass weite Teile der in § 20 Absatz 1 Satz 1 BVerfSchG katalogartig aufgezählten Übermittlungszwecke in ihrem tatsächlichen Anwendungsbereich unklar bleiben. Jedenfalls unter Verhältnismäßigkeitsgesichtspunkten verfassungsrechtlich unzulässig ist die Ausgestaltung der generalklauselartig formulierten **Auffangvorschrift in § 20 Absatz 1 Satz 1 Nr. 5 BVerfSchG-E**. Danach soll die Übermittlung auch zulässig sein, um „auf vergleichbare Weise das Gefährdungspotenzial der Bestrebungen oder Tätigkeiten zu reduzieren“. Eine solche **Vergleichbarkeitsbeurteilung** lässt sich schon aufgrund der Inhomogenität der in Nummern 1 bis 4 vorgeschlagenen Übermittlungszwecke faktisch kaum durchführen.

Und schließlich vereint § 20 BVerfSchG-E **ohne jegliche Differenzierung** (und insoweit abweichend von den §§ 11c, 11d BNDG-E) unter einem Dach sowohl **Übermittlungen an öffentliche wie an private Stellen**. Dies erscheint schon deshalb als unverhältnismäßig, weil Private von vornherein nicht über operative Zwangsbefugnisse verfügen und im Zweifel auch im Umgang mit nachrichtendienstlichen Informationen und Kontakten ungeübt sind. Man denke nur an das Beispiel des Vermieters, der kurz vor Abschluss eines Mietvertrages Besuch von Miterbeitern des BfV mit Informationen über die Aktivitäten des zukünftigen Mieters im Reichsbürgermilieu erhält. Zudem sind Private nicht wie staatliche Stellen unmittelbar an Recht und Gesetz gebunden. Und schließlich ist es schlicht nicht Aufgabe des Verfassungsschutzes, vom Beobachtungsauftrag umfasste Personen, bei denen noch keine zu gefahrenabwehrrechtlich oder strafverfolgungsrechtlich relevanten Eingriffsschwellen verdichteten Erkenntnisse vorliegen, durch Einwirkungen auf private Vermieter, Dienstebetreiber, Veranstalter oder Kreditinstitute von der legalen Teilnahme am gesellschaftlichen Leben abzuschneiden.

> Hierzu *Ronen Steinke*, Innere Sicherheit: Lizenz zum Anschwärzen, Süddeutsche Zeitung v. 26.10.2023.

Es müssen **auch für unliebsame Personen** in einem liberalen Rechtsstaat **Freiräume** im gesellschaftlichen Leben **jenseits staatlicher Kontrolle** verbleiben, auch wenn deren Nutzung von der Mehrheit missbilligt wird und Anlass zur Sorge gibt. Gerade bei privaten Empfängern nachrichtendienstlich erlangter Informationen ist daher in besonderer Weise Augenmaß zu wahren.

Vor diesem Hintergrund wird empfohlen, in § 20 BVerfSchG lediglich einen abschließenden Katalog von Übermittlungszwecken zum administrativen Rechtsgüterschutz durch inländische öffentliche Stellen zu belassen, bei dem sich Übermittlungen über die Fälle des § 19 BVerfSchG hinaus (in den meisten praxisrelevanten Fällen wird ohnehin schon eine zumindest konkretisiere Gefahr vorliegen und dann diese Vorschrift als Grundnorm für die Datenübermittlung einschlägig sein) ausnahmsweise aufgrund verfassungsrechtlicher Wertungen auch unterhalb der Schwelle konkretisierter Gefahren rechtfertigen lassen (z.B. im öffentlichen Dienstrecht infolge der dort geltenden Treuepflicht oder bei EU-Vorgaben infolge der Loyalitätspflicht der Mitgliedstaaten nach Art. 4 Abs. 3 EUV). In diesen Fällen könnte man dann auch auf problematische Zweckbindungsvorgaben für die Empfängerseite verzichten, also die dort gesetzlich vorgesehenen operativen Zwangsbefugnisse unangetastet lassen, die im jeweiligen Kontext behördlichen Handelns ohnehin meist eine untergeordnete Rolle spielen. Für Übermittlungen an Private sollte eine eigenständige, noch deutlich restriktivere Regelung geschaffen werden. Ungeachtet dessen sollte sich der Gesetz-

geber aber der Tatsache bewusst sein, dass man auch bei einer solchen – gegenüber § 20 BVerfSchG-E eingeschränkten – Regelung den bislang gesicherten Boden der Verfassungsrechtsprechung verlässt. Ein gewisses Restrisiko, erneut vor den Schranken des BVerfG in Karlsruhe zu scheitern, bliebe somit bestehen.

IV. § 21 BVerfSchG-E (Übermittlung an Strafverfolgungsbehörden zur Strafverfolgung)

Mit dieser Regelung wird die **Intention des BVerfG**, wonach die Datenübermittlung zu Zwecken der Strafverfolgung auf die Verfolgung besonders schwerer Straftaten zu beschränken ist,

> BVerfG, Urt. vom 26. April 2022, 1 BvR 1619/17, Leitsatz 3b),

in ihr Gegenteil verkehrt. Die Vorschrift ist in der zur Begutachtung vorgelegten Fassung nichts anderes als eine weitgehende Kodifikation sicherheitsbehördlicher Wunschlisten. Erkennbar wollen die Entwurfsverfasser hier trotz der klaren Botschaft aus Karlsruhe nicht von dem bisherigen status quo der Übermittlungsmöglichkeiten abweichen. Ein solcher Ansatz ist mit Blick auf die Praxis wiederum durchaus nachvollziehbar, aber verfassungsrechtlich von vornherein zum Scheitern verurteilt. Die in Absatz 2 im Wege eines Straftatenkataloges erfolgende, **verfassungsschutzspezifische Definition der besonders schweren Straftaten**, die von bereits existierenden Katalogen im Strafprozessrecht (§§ 100b Absatz 2, 100g Absatz 2 StPO) abweicht, **verlässt bereits ab Nr. 2 den sicheren Boden des durch die Verfassungsrechtsprechung Abgesegneten**. Straftaten, die im Höchstmaß mit Freiheitsstrafe von fünf Jahren bedroht sind, machen im Übrigen einen großen Teil der im deutschen Strafrecht kodifizierten Straftatbestände aus und erfassen Deliktsbereiche, die von Bagatellkriminalität bis zu mittlerer Kriminalität reichen, etwa auch einfache Diebstähle (§ 242 Absatz 1 StGB) und Betrugstaten (§ 263 Absatz 1 StGB). Damit bieten sie per se kaum Begrenzungspotenzial. Für den im Wortlaut des § 21 Absatz 2 Nr. 2 geforderten **Staatsschutzbezug** werden über den Deliktscharakter der im dortigen Katalog aufgeführten Straftatbestände hinaus keine materiellen Kriterien verlangt, die diesen Begriff mit Leben füllen würden. Insofern handelt es sich um eine bloße Leerformel. Formulierungen wie „zu Tätigkeiten bzw. Bestrebungen begangen" in § 21 Absatz 2 Nr. 3 und 4 BVerfSchG-E sind nicht nur sprachlich misslungen, sondern öffnen Tür und Tor zur für eine Übermittlung zur Verfolgung von Bagatelldelikten, sofern sie nur im Zusammenhang mit nachrichtendienstlichen Beobachtungsobjekten verwirklicht werden.

Schließlich müsste vor dem Hintergrund des Prinzips der hypothetischen Datenneuerhebung im Gesetzestext festgehalten werden dass eine Übermittlung von personenbezogenen Daten, die das Bundesamt für Verfassungsschutz durch eine **Maßnahme zur optischen Wohnraumüberwachung** nach § 9 Absatz 2 Satz 2 BVerfSchG erhoben hat, zum Zweck der Strafverfolgung von vornherein ausgeschlossen ist, weil strafprozessual nur die akustische Wohnraumüberwachung zulässig ist.

Um nicht jegliche Formen von Begleit- und Beschaffungskriminalität im Zusammenhang mit Beobachtungsobjekten des BfV mit einzubeziehen, ist dringend zu empfehlen, § 21 Absatz 2 Nr. 2 BVerfSchG-E durch eine Regelung zu ersetzen, die zwar dem Grunde nach an die Mindesthöchststrafe von fünf Jahren Freiheitsstrafe anknüpfen kann, dann aber einen deutlich klareren und engeren Staatsschutzbezug formuliert. Alternativ könnte man auch darüber nachdenken, anstelle einer solchen Generalklausel einen mit einem echten Staatsschutzbezug versehenen, überschaubaren Katalog von Delikten zu schaffen, die in diesem Deliktsschwerebereich liegen und nach den Erfahrungen des BfV schon bislang in besonderem Maße Gegenstand von Übermittlungen an die Strafverfolgungsbehörden sind, etwa tätliche Angriffe auf Vollstreckungsbeamte (§ 114 StGB), öffentliche Aufforderungen zu Straftaten (§ 111 StGB) oder Geldwäschetaten (§ 261). In jedem Fall ist eine Übermittlung von Daten an die Strafverfolgungsbehörden, die das BfV durch Maßnahmen der optischen Wohnraumüberwachung erlangt hat, gesetzlich auszuschließen.

Nach diesen Grundsätzen wäre dann auch § 11a BNDG-E anzupassen.

V. § 22 BVerfSchG-E (Übermittlung an inländische Stellen ohne belastende Maßnahmen mit Außenwirkung)

Diese Regelung übersieht in den Absätzen 1 und 3, dass es für die Bejahung eines Grundrechtseingriffs nicht auf die Außenwirkung, sondern auf den **Übermittlungsvorgang** selbst ankommt, der als **eigenständiger Grundrechtseingriff** zu qualifizieren ist:

> BVerfGE 113, 348 (375 ff.); 154, 152 (237 f.); 156, 11 (44 ff.); BVerfG, Beschl. v. 28.9.2022, 1 BvR 2354/13, Rn. 108.

Zudem soll nach dem vorgeschlagenen Gesetzeswortlaut entscheidend sein, ob bzw. dass die Datenübermittlung von Seiten des BfV subjektiv auf Maßnahmen mit Außenwirkung „zielt". Solche **subjektiven Zielsetzungen** lassen sich nur schwer überprüfen. Zudem kann sich die tatsächliche Situation und deren Einschätzung jederzeit ändern. Wenn der Empfänger die Sachlage nach Erhalt der Daten später anders be-

urteilt und nun doch Maßnahmen mit Außenwirkung ergreifen möchte, wäre das nach dieser Konzeption letztlich zulässig. Im Ergebnis würde damit der Gefahr von Schutzbehauptungen bei Übermittlungsvorgängen Tür und Tor geöffnet.

Die Vorschrift sollte ersatzlos gestrichen werden.

VI. § 24 BVerfSchG-E (Minderjährigenschutz)

Durch § 24 Satz 2 BVerfSchG-E wird der Schutz von Minderjährigen gegenüber der bisherigen Rechtslage in § 11 Absatz 1 BVerfSchG ohne nachvollziehbare Begründung eingeschränkt. Sie weicht zudem von der parallelen Regelung in § 9f BNDG-E ab. Damit können auch die Löschungspflichten nach § 11 Absatz 2 BVerfSchG ausgehebelt werden, weil für die Löschung der übermittelten Informationen dann (auch) der Empfänger nach dem für ihn geltenden Regelungsregime verantwortlich ist. Bei Minderjährigen, die ins Visier des BfV geraten (z.B. bei Botengängen für oder auffälligem Kontakt zu Extremisten), kann es sich häufig um eine Art Jugendverfehlung aufgrund von entwicklungsbedingter Unreife handeln. Insofern ist schon nach geltendem Recht die sog. „Mitziehregelung" des § 11 Absatz 2 Satz 2 BVerfSchG problematisch.

Vor diesem Hintergrund könnte eine praxistaugliche und zugleich dem Schutz personenbezogener Daten Minderjähriger Rechnung tragende Vorschrift sowohl im BVerfSchG als auch im BNDG alternativ wie folgt lauten:

„Das Bundesamt für Verfassungsschutz darf personenbezogene Daten über das Verhalten Minderjähriger vor Vollendung des 14 Lebensjahres nach den §§ 19 und 20 nur übermitteln, solange die Voraussetzungen der Speicherung nach § 11 Absatz 1 Satz 1 erfüllt sind. Liegen diese Voraussetzungen nicht mehr vor, bleibt eine Übermittlung nur zulässig

1. zur Abwehr dringender Gefahren zum Schutz besonders gewichtiger Rechtsgüter nach § 19 Absatz [...] oder

2. zur Verfolgung von Straftaten nach § 20 Abs. 2 Satz 1 Nummer 1."

VII. § 25 BVerfSchG-E (Weiterverarbeitung durch den Empfänger)

Diese Norm beruht insbesondere in Absatz 2 auf der verfehlten Überlegung, dass man durch **Zweckbindung von Daten bzw. Zweckvorgaben für die datenempfangende Stelle** die **Übermittlungsmöglichkeiten für das BfV ausweiten** kann. Insofern gilt die bereits zu § 20 BVerfSchG-E vorgetragene Kritik diesbezüglich erst recht. Eine Gesetzgebungskompetenz für die Weiterverarbeitung und Zweckbindung

der Daten bei der Nutzung durch den Empfänger besteht für den Bund nicht, soweit es sich bei den Empfängern um Stellen handelt, deren Aufgaben und Befugnisse durch den Landesgesetzgeber zu regeln sind (z.B. Polizeibehörden der Länder, Landesverfassungsschutzbehörden etc.). Nach dem vom BVerfG für Datenübermittlungen zwischen den deutschen Sicherheitsbehörden entwickelten sog. Zwei-Türen-Modell kann der Bund nur die „Tür aus dem Kontext des Bundesamtes für Verfassungsschutz heraus" mehr oder minder weit öffnen. Die Nutzung der so übermittelten Daten, also die zweite „Tür zu den Empfängerstellen", müssen diese selbst regeln, sofern der Bund hierfür keine Regelungskompetenz besitzt.

Jedenfalls die Regelung in § 25 Absatz 2 BVerfSchG-E sollte daher ersatzlos gestrichen werden. Parallel hierzu ist dann auch § 9a BNDG-E entsprechend anzupassen.

XIII. § 25a BVerfSchG (Übermittlung an ausländische sowie über- und zwischenstaatliche Stellen)

Die Regelung ist insgesamt **zu unbestimmt, zu wenig transparent und** in dieser Form **kaum praktikabel**. Zudem trägt sie wiederum Elemente einer **Zweckbindungslösung**, die sich im Ausland noch weniger als im Inland kontrollieren lassen. In Anlehnung an die Regelung im neuen Art. 26 BayVSG könnte man, unter Streichung der problematischen Zweckbindungsregelung, wie folgt formulieren:

„(1) Für die Übermittlung personenbezogener Daten an ausländische öffentliche und private Stellen sowie an über- und zwischenstaatliche Stellen gelten die §§ 19 bis [...] entsprechend.

(2) Die Übermittlung unterbleibt, unbeschadet der Regelung in § 23, wenn im Einzelfall

1. auswärtige Belange der Bundesrepublik Deutschland entgegenstehen,

2. ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist oder

3. der Empfänger nicht zusichert, dass die Daten nur mit Zustimmung des Bundesamtes für Verfassungsschutz an Dritte übermittelt werden, wenn das Bundesamt für Verfassungsschutz dies im Zuge der Übermittlung verlangt oder sich vorbehält.

IX. § 25b BVerfSchG-E (Übermittlungen zum Schutz der betroffenen Person)

Ob die Übermittlung personenbezogener Daten im Interesse der betroffenen Person liegt, entscheidet nach der in § 25b S. 1 BVerfSchG-E vorgeschlagenen Regelung allein das BfV im Wege einer **Prognose**. Diese kann sich im Nachhinein schlicht als unzutreffend erweisen, der mit der Übermittlung verbundene Grundrechtseingriff aber anschließend nicht mehr geheilt werden. Zudem scheint das praktische Bedürfnis nach einer solchen Übermittlungsregelung nicht gesichert. Schließlich müssen die Verfassungsschutzbehörden beispielsweise die Gefahrenabwehr- oder Strafverfolgungsbehörden nach den hierfür einschlägigen Übermittlungsvorschriften ohnehin umfassend informieren und dabei **auch entlastende Umstände** weitergeben. Zudem sollte die Regelung zur Übermittlung an die **Jugendhilfe** (§ 25b S. 2 BVerfSchG-E) auf ihre Sinnhaftigkeit und Praxistauglichkeit überprüft werden. Sowohl die Jugendämter als auch private Träger der Kinder- und Jugendhilfe werden mit solchen Informationen von Seiten des BfV (z.B. über einen vorherigen Aufenthalt des Kindes in einem ausländischen Terrorcamp oder Kontakte zu radikalen Predigern und Gleichaltrigen) häufig schlicht überfordert sein. Zudem besteht die Gefahr der Stigmatisierung solcher Kinder, gerade bei nicht ausreichend geschultem Personal. Mit der Jugendhilfe sollen aber gerade positive Lebensbedingungen geschaffen und Benachteiligungen vermieden werden.

Insoweit ist zu empfehlen, die Regelung in § 25b Satz 1 BVerfSchG ebenso wie die parallele Regelung in § 9h Absatz 1 BNDG-E ersatzlos zu streichen. Die Regelung in § 25b Satz 2 BVerfSchG sollte unter Einbeziehung von einschlägigem Sachverstand aus dem Bereich der Kinder- und Jugendhilfe auf ihre Sinnhaftigkeit überprüft werden und könnte dann ggf. in die Übermittlungsvorschriften an inländische öffentliche und private Stellen integriert werden.

X. § 25d BVerfSchG-E (Nicht nachrichtendienstlich erhobene personenbezogene Daten)

Diese Regelung scheint auf einem fundamentalen **Missverständnis bzw. einer Fehlinterpretation der Vorgaben des BVerfG** in seiner Entscheidung zum BayVSG vom 26.4.2022 zu beruhen. Das Karlsruher Gericht hat dort gerade nicht ausgeführt, dass die Übermittlung von nicht mit nachrichtendienstlichen Mitteln erhobenen personenbezogenen Informationen generell an geringere Voraussetzungen gebunden werden kann. Es hat vielmehr umgekehrt bei der Übermittlung von Informationen, die mit nachrichtendienstlichen Mitteln gewonnen wurden, das zusätzliche Erfordernis der **hypothetischen Datenneuerhebung** aufgestellt:

BVerfG, Urt. vom 26. April 2022, 1 BvR 1619/17, Leitsatz 3.

Dieses Kriterium spielt aber in den §§ 19 ff. BVerfSchG-E bislang allenfalls als grundlegendes verfassungsrechtliches Prinzip, nicht aber auch formal verankert im Gesetzeswortlaut eine Rolle. Infolgedessen macht auch die Differenzierung gegenüber Maßnahmen nach § 25d BVerfSchG-E nach dem bisherigen Regelungskonzept nur bedingt Sinn und weitet die Übermittlungsmöglichkeiten unter Umgehung der verfassungsgerichtlichen Vorgaben zu stark aus.

Die Übermittlungsregelungen der §§ 19 ff. BVerfSchG-E sind somit grundlegend vor dem Hintergrund des Prinzips der hypothetischen Datenneuerhebung zu überprüfen und ggf. anzupassen.

XI. §§ 26b, 26c BVerfSchG-E (Eigensicherung)

Zunächst ist zu konstatieren, dass der „Eigensicherungsbereich" als Bezugspunkt der Normen weder im Gesetzeswortlaut noch in der Entwurfsbegründung näher beschrieben bzw. konkretisiert wird. Vor allem aber lässt sich eine **aktive Mitwirkungspflicht** der sich im Eigensicherungsbereich aufhaltenden Personen nach § 26b Absatz 5 BVerfSchG-E **verfassungsrechtlich nicht begründen** und ist somit zwingend zu streichen. Ansonsten würde man gegen das auf der Achtung der Menschenwürdegarantie in Art. 1 GG beruhende **Selbstbelastungsverbot** (nemo tenetur se ipsum accusare) verstoßen. So müssten beispielsweise Personen, die der geheimdienstlichen Agententätigkeit nach § 99 StGB verdächtigt werden, im Eigensicherungsbereich aktiv an ihrer eigenen Überführung mitwirken (z.B. durch Herausgabe von potenziellen Beweismitteln, Preisgabe von Passwörtern und Codes für Smartphones und Laptops etc.). Vertretbar erscheint stattdessen in Entsprechung zur Rechtslage im Strafverfahren lediglich die Annahme einer **Duldungspflicht** gegenüber Eigensicherungsmaßnahmen des BfV. Insofern ist auch die Regelung in § 26c Abs. 7 BVerfSchG-E als unzulässig anzusehen.

Zu unbestimmt und damit auch als unverhältnismäßig erscheint der Entwurf auch in § 26b Abs. 5 S. 2 BVerfSchG-E. Da schon der Eigensicherungsbereich als solcher nicht definiert wird, bleibt erst recht unklar, was dessen **„unmittelbare Nähe"** ausmachen soll. Zudem wird außerhalb des Eigensicherungsbereichs häufig auch gar keine Gefahr für die Eigensicherung des BfV bestehen (wenn der potenzielle Störer gar nicht ins Gebäude gelangt). Vom jetzigen Wortlaut der Regelung wäre auch der Besucher von Liegenschaften des BfV erfasst, der sich den Kontrollmaßnahmen am Eingang zum Gelände (z.B. der Abgabe und Überprüfung seines Mobiltelefons) nicht

unterziehen möchte und schnell wieder nach draußen läuft, weil er unter diesen Bedingungen von einem Besuch beim Verfassungsschutz absehen möchte.

Nicht ausreichen dürfte es schließlich mit Blick auf das Erfordernis bereichsspezifischer und normenklarer Datenschutzregelungen sowie den Grundsatz vom Vorbehalt des Gesetzes, den **Einsatz von Videokameras** (Absatz 6) auf eine bloße **Dienstvorschrift** zu stützen. Zudem bedarf es bei fehlender freiwilliger Herausgabe mangels aktiver Mitwirkungspflicht dann konsequenterweise einer Regelung zur **Beschlagnahme**. Und schließlich bedarf insbesondere der **Schutz des Kernbereichs privater Lebensgestaltung** nach § 26c BVerfSchG-E einer Präzisierung durch Anpassung an die Vorgaben des BVerfG in seiner Entscheidung zum Gesetz über die Öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern:

BVerfG, Beschl. v. 09.12.2022, 1 BvR 1345/21.

Vor diesem Hintergrund könnten die Vorschriften zur Eigensicherung verfassungskonform wie folgt gefasst werden:

„§ 26b [Besondere Eigensicherungsbefugnisse]

(1) Die Eigensicherung dient dem Schutz der Beschäftigten, Einrichtungen, Gegenstände, Quellen und amtlichen Informationen des Bundesamts für Verfassungsschutz gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten. Das Bundesamt für Verfassungsschutz hat hierzu besondere Befugnisse nach Maßgabe der folgenden Absätze.

(2) Das Bundesamt für Verfassungsschutz darf bei Personen, die seine Dienststellen, Grundstücke und sonstigen Einrichtungen (Eigensicherungsbereich) betreten oder sich dort aufhalten, und von diesen Personen mitgeführte Taschen und sonstige Gegenstände sowie von diesen Personen genutzte Fahrzeuge

1. verdachtsunabhängig kontrollieren,

2. durchsuchen, wenn tatsächliche Anhaltspunkte für sicherheitsgefährdende oder geheimdienstliche Tätigkeiten vorliegen.

(3) Eine Kontrolle nach Absatz 2 Nummer 1 ist die oberflächliche Suche nach Gegenständen an Personen, an oder in Taschen, mitgeführten Gegenständen und Fahrzeugen auch unter Einsatz technischer Mittel, ohne dass ein Körperkontakt mit der betroffenen Person stattfindet. Eine Durchsuchung nach Absatz 2 Nummer 2 ist die zielgerichtete und planmäßige Suche, auch unter Einsatz technischer Mittel,

1. am äußeren Körper der betroffenen Person,

2. in Kleidung und Taschen der betroffenen Person,

3. an und in Fahrzeugen einschließlich der dort befindlichen Gegenstände der betroffenen Person sowie

4. in sonstigen Gegenständen der betroffenen Person, die zur unbefugten Verbringung von amtlichen Informationen geeignet sind.

(4) Gegenstände, die sich im Eigensicherungsbereich befinden, darf das Bundesamt für Verfassungsschutz in Verwahrung nehmen, wenn

1. tatsächliche Anhaltspunkte dafür vorliegen, dass sie für eine sicherheitsgefährdende oder geheimdienstliche Tätigkeit verwendet werden oder mit solchen Tätigkeiten gewonnen worden sind, oder

2. diese keiner bestimmten Person zuzuordnen sind und die Sicherstellung und Untersuchung zum Schutz vor einer sicherheitsgefährdenden oder geheimdienstlichen Tätigkeit erforderlich ist.

Bei Geräten der Informations- und Kommunikationstechnik umfasst das Untersuchen auch das Eingreifen mit technischen Mitteln sowie das Verarbeiten der auf dem Gerät gespeicherten Informationen einschließlich personenbezogener Daten.

Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der Beschlagnahme.

(5) Das Bundesamt für Verfassungsschutz darf optisch-elektronische Einrichtungen zur offenen Überwachung des Eigensicherungsbereichs einsetzen, soweit nicht schutzwürdige Interessen der betroffenen Personen überwiegen. Auf die Überwachung ist in geeigneter Form hinzuweisen. Einzelheiten zu Voraussetzungen, Verfahren und Grenzen der Maßnahme sind in einer Dienstvorschrift zu regeln. Eine Überwachung höchstpersönlich genutzter Räume ist unzulässig.

(6) Das Bundesamt für Verfassungsschutz kann eine nach § 21h Absatz 3 Nummer 4 der Luftverkehrs-Ordnung unzulässige Benutzung des Luftraums seines Eigensicherungsbereichs durch unbemannte Fluggeräte durch geeignete technische Mittel gegen das unbemannte Fluggerät, dessen Steuerungseinheit oder Steuerungsverbindung aufklären und abwehren.

(7) Das Bundesamt für Verfassungsschutz darf die besonderen Mittel nach den §§ 8a, 8d und 9 Absatz 1 und 4 sowie den §§ 9a und 9b unter den dort genannten Voraussetzungen auch einsetzen, soweit dies auf Grund tatsächlicher Anhaltspunkte im Einzelfall erforderlich ist zur Aufklärung von sicherheitsgefährdenden Tätigkeiten

1. seiner Beschäftigten oder

2. von Personen, die vom Bundesamt für Verfassungsschutz beauftragt sind

a) im Eigensicherungsbereich tätig zu sein oder

b) sonstige sicherheitsempfindliche Tätigkeiten wahrzunehmen.

(8) Bei der Durchführung von Maßnahmen nach Absatz 2 sowie den Absätzen 4 bis 7 hat das Bundesamt für Verfassungsschutz unter mehreren möglichen und geeigneten Maßnahmen diejenigen zu treffen, die den Einzelnen am wenigsten beinträchtigen. Eine Maßnahme darf nicht zu einem Nachteil führen, der zu dem erstrebten Erfolg erkennbar außer Verhältnis steht.

§ 26c [Verfahren; Kernbereichsschutz]

(1) Maßnahmen nach § 26b Absatz 2 Nummer 2 und Absatz 4 bedürfen der Anordnung der für die Eigensicherung zuständigen Abteilungsleitung oder einer von ihr bestimmten Vertretung. In den Fällen des § 26b Absatz 4 Satz 3 hat der Beamte, der eine Sache beschlagnahmt hat, binnen drei Tagen eine gerichtliche Bestätigung zu beantragen. Für die gerichtliche Entscheidung ist das Amtsgericht am Sitz des Landgerichts zuständig, in dessen Bezirk der Eigensicherungsbereich belegen ist. Maßnahmen nach § 26b Absatz 5 bedürfen der Anordnung der Amtsleitung.

(2) Ist eine Anordnung nach Absatz 1 Satz 1 aufgrund besonderer Eilbedürftigkeit nicht rechtzeitig zu erlangen, kann die Maßnahme auch ohne vorherige Anordnung durchgeführt werden, wenn ansonsten der Zweck der Maßnahme vereitelt oder wesentlich erschwert würde. Bei Geräten der Informations- und Kommunikationstechnik darf in diesem Fall lediglich das Gerät sichergestellt werden. Die Anordnung ist unverzüglich nachzuholen. Wird die Anordnung nach Absatz 1 Satz 1 nicht nachgeholt, so hat das Bundesamt für Verfassungsschutz unverzüglich bereits erhobene Daten zu löschen und sichergestellte Gegenstände an die betroffene Person herauszugeben.

(3) Sichergestellte oder beschlagnahmte Gegenstände sind unverzüglich an die betroffene Person herauszugeben, sobald der Zweck der Eigensicherung entfällt. Satz 1 gilt nicht, wenn die Gegenstände zur Einleitung oder Durchführung eines strafrechtlichen Ermittlungsverfahrens nach § 21 an die Strafverfolgungsbehörden weitergegeben werden dürfen.

(4) Bei Maßnahmen nach § 26b Absatz 2 Nummer 2 hat die betroffene Person das Recht, anwesend zu sein. Über eine Durchsuchung nach § 26b Absatz 2 Nummer 2, eine Sicherstellung nach § 26b Absatz 4 Satz 1 oder eine Beschlag-nahme nach § 26b Absatz 4 Satz 3 ist auf Verlangen eine Bescheinigung über die Maßnahme und den Grund der Maßnahme zu erteilen. Maßnahmen nach § 26b Absatz 4, die in Abwesenheit der betroffenen Person durchgeführt worden sind, sind ihr schriftlich mitzuteilen, wenn hierdurch nicht der Zweck der Maßnahme gefährdet wird.

(5) Bei der Untersuchung von Geräten der Informations- und Kommunikationstechnik, die nicht ausschließlich zur dienstlichen Nutzung überlassen wurden, ist sicherzustellen, dass an dem Gerät nur Veränderungen vorgenommen werden, die für die Datenverarbeitung unerlässlich sind. Vorgenommene Veränderungen sind bei Beendigung der Maßnahme, soweit technisch möglich, rückgängig zu machen. Sichergestellte Telekommunikationsend-geräte sind abweichend von Absatz 3 Satz 1 unabhängig von dem Abschluss der Maßnahmen nach § 26a Absatz 4 an die betroffene Person spätestens nach zwei Wochen herauszugeben. Macht die betroffene Person in den Fällen des Satzes 3 Gründe glaubhaft, nach denen für sie eine Aufrechterhaltung der Sicherstellung oder Beschlagnahme nicht zumutbar ist, so ist das mobile Endgerät innerhalb von 48 Stunden nach Darlegung der Gründe an die betroffene Person zurückzugeben. Das Bundesamt für Verfassungsschutz darf vor der Rückgabe ein Abbild der auf dem Gerät gespeicherten Informationen ein-schließlich personenbezogener Daten zur Datensicherung erzeugen.

(6) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme zur Eigensicherung nach diesem Gesetz allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist die Maßnahme unzulässig. Eine bereits laufende Datenerhebung ist unverzüglich abzubrechen. Von einem unverzüglichen Abbruch der Maßnahme kann so lange abgesehen werden, wie eine konkrete Gefahr für Leib oder Leben der zur Informationserhebung eingesetzten Personen besteht. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme zur Eigensicherung nach diesem Gesetz erlangt wurden, dürfen durch das Bundesamt für Verfassungsschutz nicht weiter verarbeitet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist nach Ablauf von sechs Monaten zu löschen. Über die Frage, ob Erkenntnisse in den Kernbereich privater Lebensgestaltung fallen oder ihre weitere Verarbeitung zulässig ist, entscheidet nach einer ersten Sichtung durch die zur Informationserhebung eingesetzten Personen das in Absatz 1 Satz 3 bezeichnete Gericht.

(7) Widerspruch und Anfechtungsklage gegen Maßnahmen nach § 26a haben keine aufschiebende Wirkung."

An diesen Maßstäben sollte sich dann auch die Ausgestaltung der parallelen §§ 65a ff. BNDG-E orientieren.

München, den 3. November 2023

PROF. DR. MARK A. ZÖLLER