Hochschule des Bundes
für öffentliche Verwaltung

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)844 F

POSTANSCHRIFT HS BUND, POSTFACH 40527, 10063 BERLIN

Deutscher Bundestag
Ausschuss für Inneres u. Heimat
Platz der Republik 1
11011 Berlin
- via E-Mail -

Prof. Dr. Jan-Hendrik Dietrich
HAUSANSCHRIFT Habersaathstr. 51, 10115 Berlin
POSTANSCHRIFT Postfach 40527, 10063 Berlin
TEL 030 – 22 00 89 – 86341
EMAIL jan-hendrik.dietrich@hsbund-nd.de

DATUM Berlin, 17.05.2021

Schriftliche Stellungnahme

zum Gesetzentwurf der Bundesregierung

„Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts“

(BT-Drucksache 19/24785, 19/24900)

Übersicht

Zusammenfassung

Der vorliegende Gesetzentwurf dient der Effektivierung der sicherheitsbehördlichen Arbeit. Insgesamt begegnet er keinen durchgreifenden Bedenken. Im Detail besteht indes Anpassungsbedarf.

Die Erweiterung des Bestrebungsbegriffs nach § 4 Abs. 1 S. 3-4 BVerfSchG-E erscheint zu weitgehend. Die Vorschrift setzt pauschal Einzelpersonen und Personenzusammenschlüsse gleich. Das kann so nicht überzeugen, da Einzelpersonen ja nicht abstrakt gleichermaßen gefährlich sind. Hier sollte besser die bestehende Regelung des § 4 Abs. 1 S. 4 BVerfSchG modifiziert werden.

Die Einbeziehung des BAMAD in diesen Informationsverbund ist mit Blick auf die vergleichsweise hohe Zahl der Extremismusverdachtsfälle in der Bundeswehr (siehe BMVg, Zweiter Bericht der Koordinierungsstelle für Extremismusverdachtsfälle, Berichtszeitraum 1. Januar bis 31. Dezember 2020, S. 7) zu begrüßen. Auch die weitgehende Identität des gesetzlichen Auftrags von BAMAD und Verfassungsschutzbehörden legen eine engere Zusammenarbeit nahe. Vor dem Hintergrund der Kooperationspflichten der Länder sollte indes die fakultative Teilnahme des BAMAD mittelfristig in eine obligatorische überführt werden.

Die Änderungen des Artikel 10-Gesetzes sind vor dem Hintergrund einer zunehmenden Verbreitung von Verschlüsselungstechniken zu sehen. Klassische Überwachungsinstrumente stoßen zunehmend an ihre Grenzen. An dieser Stelle setzt die Quellen-Telekommunikationsüberwachung an. Über die Infiltration eines informationstechnischen Systems wird die Kommunikation abgegriffen, bevor sie verschlüsselt oder nachdem sie entschlüsselt wurde. Die am Vorbild von § 100a StPO orientierten Neuregelungen halten einer verfassungsrechtlichen Prüfung stand.

Aufgrund des kurzen Vorlaufs für die sachverständige Begutachtung des Gesetzesentwurfs konzentrieren sich die nachfolgenden Überlegungen nur auf zentrale Vorschriften der Novelle.

I. Änderungen des BVerfSchG und des MADG (Artikel 1 und 2)

1. Erweiterung des Bestrebungsbegriffs (§ 4 Abs. 1 S. 3-4 BVerfSchG-E)

Dem Entwurf zufolge sollen Bestrebungen i.S.v. § 3 Abs. 1 BVerfSchG nun auch von Einzelpersonen ausgehen können, die nicht in einem oder für einen Personenzusammenschluss handeln. Nach § 4 Abs. 1 S. 4 BVerfSchG-E muss das Verhalten dieser Personen aber auf aber Ziele i.S.v. Satz 1 gerichtet sein (z.B. „einen der in Absatz 2 genannten Verfassungsgrundsätze zu beseitigen oder außer Geltung zu setzen“).

Die Gesetzesbegründung hebt in diesem Zusammenhang auf die „Bedingungen der digitalen Moderne und Erkenntnisse zu Radikalisierungsverläufen“ ab. Angesichts „eruptiver Radikalisierungsverläufe von Einzelpersonen“ wie bei den Anschlägen von Halle und Hanau würden über die Erweiterung des Bestrebungsbegriffs „Extremisten bereits im Vorfeld militanter Handlungen besser in den Blick“ genommen werden können (vgl. BT-Drs. 19/24785, S. 17).

Sicherheitspolitisch ist diese Motivation nachvollziehbar. Die Vergangenheit hat gezeigt, dass Anschläge zunehmend auch von Einzelpersonen begangen werden, die sich nicht selten über das Internet radikalisiert haben. Während früher die extremistischen und gewaltverherrlichenden Botschaften durch persönliche Kontakte in einschlägige Milieus hinein wahrgenommen wurden, sind sie heute nur noch einen Mausklick entfernt (Vgl. *Pfahl-Traughber*, Der Einzeltäter im Terrorismus, https://www.bpb.de/politik/ extremismus/rechtsextremismus/304169/ der-einzeltaeter-im-terrorismus). Hier kann insbesondere das oft beschriebene Gamification-Phänomen dafür sorgen, dass in den Köpfen virtuelle und reale Welt verschmelzen (Näher dazu *Schlegel*, Jumanji Extremism? How games and gamification could facilitate radicalization processes, Journal for Deradicalization 2020, 23 ff.). Der Radikalisierungsprozess kann durch die Allgegenwart und Verfügbarkeit des Internets u.U. sogar in relativ kurzer Zeit erfolgen (zu sog. Schnellradikalisierten kürzlich BVerwG,

Beschluss v. 25.6.2019, 1 VR 1.19). Einzelpersonen können allerdings nicht nur Adressatinnen und Adressaten von extremistischen Parolen im Internet sein, sondern auch deren Urheberinnen und Urheber. Die Mechanismen der Algorithmen sozialer Netzwerke eröffnen einzelnen Posts oder Tweets vom heimischen Schreibtisch v.a. eine große Breitenwirkung, wenn sie technisch durch Social-Bots oder Filterblasen begünstigt werden (siehe *Dietrich*, Desinformation als Problem des Sicherheitsrechts, in: Dietrich/Gärditz, Sicherheitsverfassung – Sicherheitsrecht, 2019, S. 75, 78). In solchen Fällen ist nicht zu übersehen, dass Einzelpersonen ein besonderes Bedrohungspotential zukommen kann.

Der erweiterte Bestrebungsbegriff setzt an dieser Stelle an, um eine Beobachtungslücke zu schließen. Bei näherem Blick ist das indes nicht unproblematisch. Nachrichtendiensten obliegt die anlasslose Lage-, Milieu- und Strukturaufklärung im Vorfeld von konkreten Gefährdungslagen. Für den Verfassungsschutz findet dieser Auftrag seinen Ausdruck insbesondere über den Begriff der Bestrebung, die gem. § 4 Abs. 1 BVerfSchG als politisch bestimmte, ziel- und zweckgerichtete Verhaltensweise in oder für einen „Personenzusammenschluss“ definiert wird. Der Rekurs auf Personenzusammenschlüsse zeigt, dass v.a diesen ein Gefahrenpotential für die Schutzgüter des Gesetzes eingeräumt wird (*Droste*, Handbuch des Verfassungsschutzrechts, 2007, S. 168 ff.). Im Vergleich zu auf sich gestellten Einzelpersonen bietet die Gemeinschaft die Möglichkeit einer Arbeitsteilung und Identifikation als Gruppe. Gruppendynamik und Gruppendruck können den Ausstieg erschweren (siehe *Warg*, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, V § 1 Rn. 27).

§ 4 Abs. 1 S. 3-4 BVerfSchG-E setzen nun pauschal Einzelpersonen und Personenzusammenschlüsse gleich. Das kann so nicht überzeugen, da Einzelpersonen ja nicht abstrakt gleichermaßen gefährlich sind. Einer ausufernden Einbeziehung von Einzelpersonen in die Beobachtung soll der Gesetzesbegründung durch eine besondere Würdigung des Einzelfalls begegnet werden (vgl. BT-Drs. 19/24785, S. 17). Anders als bei Personenzusammenschlüssen sei ein Entschließungsermessen auszuüben. Für diese Annahme erscheint aber eine Regelung in § 4 Abs. 1 BVerfSchG insofern nicht geeignet, als es sich bei der Vorschrift um eine Begriffsbestimmung

handelt. Den gesetzlichen Auftrag des Verfassungsschutzes drückt allein § 3 Abs. 1 BVerfSchG aus. Nach allgemeiner Auffassung kommt danach den Verfassungsschutzbehörden im Falle des Vorliegens einer Bestrebung gerade kein Entschließungsermessen zur Beobachtung („Auftrag ... ist...“) zu (vgl. *Roth*, in Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl., 2019, §§ 3, 4 BVerfSchG Rn. 131 ff.).

De lege lata ist bereits die Beobachtung von Einzelpersonen unter engen Voraussetzungen möglich. Entweder handeln diese „in oder für einen Personenzusammenschluss“ oder ihre Verhaltensweise kann ausnahmsweise selbst als Bestrebung gelten. Letzteres ist gem. § 4 Abs. 1 S. 4 BVerfSchG der Fall, soweit deren Verhalten auf Anwendung von Gewalt gerichtet oder aufgrund der Wirkungsweise geeignet ist, ein Schutzgut des BVerfSchG erheblich zu beschädigen. Die oben dargelegten Wertungswidersprüche ließen sich vermeiden, wenn anstelle einer pauschalen Erweiterung des Bestrebungsbegriffs auf Einzelpersonen § 4 Abs. 1 S. 4 BVerfSchG modifiziert werden würde.

2. Einbeziehung BAMAD in das Informationssystem NADIS

§ 6 Abs. 2 S. 1-4 BVerfSchG-E und § 3 Abs. 3 MADG-E bieten dem BAMAD die Möglichkeit, am Nachrichtendienstlichen Informationssystem Wissensnetz (NADIS WN) teilzunehmen, das im Verfassungsschutzverbund allen Behörden zur Verfügung gestellt wird (dazu ausführlich *Dietrich*, Verfassungsschutz in der föderalen Ordnung, in: Kudlich/Engelhart/Vogel, FS für Sieber, 2021 i.E.). §§ 5, 6 BVerfSchG adressieren Koordinationsrechte und Kooperationspflichten im Verbund. Über § 5 Abs. 2 BVerfSchG wird dem BfV die Informationsauswertung als Zentralstellenaufgabe zugeschrieben. Die Landesbehörden werden nach § 6 Abs. 1 BVerfSchG zur Übermittlung von Informationen („unverzüglich“) verpflichtet. Die Informationsübermittlung ist aber nicht als Einbahnstraße angelegt. Nach derselben Vorschrift muss auch das BfV der Landesebene Informationen zur Verfügung stellen.

Wie der Informationsaustausch im Einzelnen erfolgt, wird über § 6 Abs. 2 BVerfSchG zumindest im Ansatz geregelt: danach werden alle Verfassungsschutzbehörden ver-

pflichtet, sog. „gemeinsame Dateien“ zu führen, für deren Bereitstellung wiederum das BfV als Zentralstelle nach § 5 Abs. 4 Nr. 1 BVerfSchG zuständig ist. Angesprochen ist hiermit im Wesentlichen das erwähnte Nachrichtendienstliche Informationssystem (NADIS), das in strukturierter Form Einzelangaben zu Personen und Objekten enthält.

Die Einbeziehung des BAMAD in diesen Verbund ist nicht nur mit Blick auf die vergleichsweise hohe Zahl der Extremismusverdachtsfälle in der Bundeswehr (siehe *BMVg*, Zweiter Bericht der Koordinierungsstelle für Extremismusverdachtsfälle, Berichtszeitraum 1. Januar bis 31. Dezember 2020, S. 7) zu begrüßen. Vor allem die weitgehende Identität des gesetzlichen Auftrags von BAMAD und Verfassungsschutzbehörden legen eine engere Zusammenarbeit nahe. Vor dem Hintergrund der Kooperationspflichten der Länder sollte indes die fakultative Teilnahme des BAMAD mittelfristig in eine obligatorische überführt werden, sobald dafür die technischen Voraussetzungen geschaffen worden sind. Das will wohl die Gesetzesbegründung andeuten (vgl. BT-Drs. 19/24785, S. 17).

II. Änderungen des Artikel 10-Gesetzes (Artikel 5)

Mit den Neuregelungen der §§ 2, 11 G10-E soll die sog. Quellen-Telekommunikationsüberwachung in das BVerfSchG eingeführt werden. Zugleich wird durch die Neufassung des § 15 G10-E die Kontrolle der Überwachungsmaßnahmen durch die G10-Kommission gestärkt.

1. Quellen-Telekommunikationsüberwachung und Verschlüsselungstechnik

Die genannten Änderungen sind vor dem Hintergrund einer zunehmenden Verbreitung von Verschlüsselungstechniken zu sehen (näher *Dietrich*, GSZ 2021, 1 ff.). Klassische Überwachungsinstrumente stoßen zunehmend an ihre Grenzen. Die deutschen Sicherheitsbehörden warnen bereits seit einiger Zeit vor einem sog. „Going Dark-Problem“: die verbreitete Nutzung von Verschlüsselungstechnik führe dazu, dass bewährte Telekommunikations-Überwachungsinstrumente nur noch we-

nig ertragreich seien (So z.B. *Haldenwang/Postberg*, in: Sauerland/Leppek (Hrsg.), FS für Bönders, 2019, S. 51 ff. Näher dazu auch *Unterreitmeier*, in: Deutscher Verwaltungsgerichtstag (Hrsg.), Dokumentation 19. Verwaltungsgerichtstag, 2020, S. 199 ff.). Neu sind solche Überlegungen keineswegs. Die Anfänge der „Kryptokontroverse“ reichen bis in die 1990er Jahre zurück (Siehe ausführlich *Bizer*, in: Hammer (Hrsg.), Sicherungsinfrastrukturen – Gestaltungsvorschläge für Technik, Organisation und Recht, S. 179 (179 ff.); *Kuner*, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, Teil 17 Rn. 62 ff.). Seitdem hat sich die Lage aber weiter verschärft. In seinen „Internet Organised Crime Threat Assessments“ der Jahre 2019 und 2020 warnte zuletzt EUROPOL erneut eindringlich vor versiegenden Informationsquellen:

> „Encryption, while recognised as an essential element of our digitised society, also facilitates significant opportunities for criminals. Investigative techniques, such as lawful interception, are becoming increasingly ineffective (or even impossible) as criminals exploit encrypted communication services, applications and devices. Similarly, criminals can deny forensic investigators access to critical evidence by encrypting their data. The criminal abuse of encryption technologies, whether it be anonymisation via VPNs or Tor, encrypted communications or the obfuscation of digital evidence (especially in cases of CSEM), was a significant threat highlighted by respondents to this year’s IOCTA survey” (EUROPOL, Internet Organised Crime Threat Assessment 2019 (IOCTA 2019), S. 56 f.).

Was für kriminelle Machenschaften gilt, gilt auch für extremistische Bestrebungen und terroristische Aktivitäten. Sog. Ende-zu-Ende-Verschlüsselungen verhindern zunehmend den Zugriff der Verfassungsschutzbehörden auf Kommunikationsinhalte über bekannte G10-Maßnahmen. Gesetzliche Beschränkungen von Verschlüsselungen erweisen bei näherer Betrachtung als unzulässig oder kaum durchsetzbar (siehe *Dietrich*, GSZ 2021, 1 ff.).

An dieser Stelle setzt die Quellen-Telekommunikationsüberwachung an. Über die Infiltration eines informationstechnischen Systems wird die Kommunikation abgegriffen, bevor sie verschlüsselt oder nachdem sie entschlüsselt wurde (ausführlich *Löffelmann*, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, VI §

4 Rn. 106 ff.). Die Sicherheitsbehörden werden dadurch in die Lage versetzt, ihrem gesetzlichen Auftrag trotz des verbreiteten Einsatzes von Verschlüsselungstechnik nachzukommen. Gegenüber gesetzlichen Beschränkungen von Verschlüsselungen erweist sich die Quellen-Telekommunikationsüberwachung als Grundrechtseingriff von deutlich geringer Intensität (Vgl. *Martini/Fröhlingsdorf*, NVwZ 2020, 1803, 1805).

2. Gesetzliche Ausgestaltung der Quellen-Telekommunikationsüberwachung

Der Gesetzesentwurf folgt dem Regelungsvorbild von § 100a StPO. § 11 Abs. 1a G10-E orientiert sich maßgeblich an § 100a Abs. 1 S. 2 und 3 sowie Abs. 5 und 6 StPO. Auch vor Inkrafttreten der Neuregelung in der Strafprozessordnung wurde die Zulässigkeit der Quellen-Telekommunikationsüberwachung nicht bestritten. Vielmehr ging die wohl herrschende Ansicht davon aus, die Quellen-Telekommunikationsüberwachung sei eine mögliche Form der technischen Überwachung einer angeordneten Überwachungsmaßnahme (zur alten Regelung in §§ 100a, 100b StPO siehe z.B. *Bär*, in KMR/StPO, § 100a Rn. 31a). Die nun gefundene Regelung wirft in zweierlei Hinsicht Fragen auf.

Zum einen geht es um sog. Begleitmaßnahmen der einzelnen Überwachungsmaßnahme. Gemeint ist damit, auf dem Zielgerät der zu überwachenden Person ein Programm zu platzieren, welches den Zugriff auf die laufende Kommunikation ermöglicht (ausführlich *Derin/Golla*, NJW 2019, 1111 ff.). Operativ ist das für Sicherheitsbehörden sehr anspruchsvoll, denn die Zielperson darf Manipulation und Zugriff ja nicht bemerken. Der Gesetzesentwurf hält sich an dieser Stelle grundsätzlich verschiedene Infektionswege offen (zur Ausnutzung von Sicherheitslücken siehe *Dietrich*, GSZ 2021, 1, 5 f.). Über § 2 Abs. 1a G10-E wird den Nachrichtendiensten ausdrücklich die Möglichkeit eröffnet, Datenströme mit Hilfe der beteiligten Telekommunikationsunternehmen auszuleiten und zu manipulieren. Dagegen bestehen grundsätzlich keine rechtlichen Bedenken. Die betroffenen Unternehmen werden wie bei einer klassischen Telekommunikationsüberwachung lediglich verpflichtet, den Datenstrom physisch umzuleiten und zur Nutzung des Datenstroms notwendige Informationen zu beauskunften (durch die sog. Over-the-Top-Dienste). Die Unternehmen müssen we-

der die Überwachungsprogramme selbst aufspielen, noch konkrete Kommunikationsinhalte ausleiten. Damit ist der Grundrechtseingriff in Art. 12 GG auf Seiten der Unternehmen deutlich geringer als bei der klassischen Telekommunikationsüberwachung.

Zum anderen wirft der Gesetzesentwurf Fragen auf, soweit es um den Zugriff auf gespeicherte Kommunikationsinhalte geht. § 11 Abs. 1a G10-E sieht vor, dass „auf dem informationstechnischen System des Betroffenen ab dem Zeitpunkt der Anordnung gespeicherte Inhalte und Umstände der Kommunikation“ überwacht und aufgezeichnet werden dürfen, „wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können“.

Auf diese Weise soll ein technisches Problem gelöst werden: bei Messenger-Diensten wie z.B. „whatsapp“ ist anders als bei der Sprach- und Videotelefonie in Echtzeit der Übertragungsvorgang mit dem Zugang der Nachricht am Endgerät abgeschlossen. Das bedeutet, dass keine „laufende Kommunikation“ mehr vorliegt, die allein nach Ansicht der BVerfG zulässiger Gegenstand der Quellen-Telekommunikationsüberwachung sein darf (BVerfGE 120, 274, 309). Damit ist die Nachricht nicht mehr vom Schutz des Fernmeldegeheimnisses nach Art. 10 GG erfasst. Soll sie dennoch ausgelesen werden, muss sich dieser Eingriff am Maßstab des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme i.S.v. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG messen lassen.

Nach der Rechtsprechung des BVerfG sind jedoch an solche Grundrechtseingriffe erhöhte Anforderungen zu stellen. Für den präventiven Bereich hat das Gericht festgelegt, dass Eingriffe nur in Betracht kommen, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut (z.B. Leib oder Leben) bestehen (BVerfGE 120, 274, 328 ff.). Vom Intensitätsgrad und Gewicht wird der Eingriff in das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme mit einem Eingriff in die Unverletzlichkeit der Wohnung i.S.v. Art. 13 GG verglichen.

Das BVerfG hat in seiner bisherigen Rechtsprechung allerdings nicht den Fall vor Augen gehabt, dass sich die Überwachung auf neu ankommende und abgesendete Messenger-Nachrichten auf einem Endgerät beschränkt. Vielmehr ging es um das Auslesen eines gesamten IT-Systems. Im Fall von § 11 Abs. 1a G10-E wird die Reichweite des Eingriffs ausdrücklich auf die Kommunikationsdaten beschränkt, die auch im Wege einer klassischen Telekommunikationsüberwachung hätten erhoben werden dürfen. Dadurch soll die Anwendung von Art. 10 GG gewissermaßen fingiert werden. Rechtsdogmatisch muss das nicht jeden überzeugen. Ein Schutzbereich eines Grundrechts ist eröffnet oder ist es nicht. Es verwundert deshalb auch nicht, dass die verwandte Regelung in § 100a StPO mitunter in der Literatur kritisch gesehen wird (vgl. z.B. *Martini/Fröhlingsdorf*, NVwZ 2020, 1803 ff.; *Mansdörfer*, GSZ 2018, 45, 46 f.) Entscheidend dürften allerdings grundrechtsspezifische Wertungen sein. Das sog. IT-Grundrecht schützt die informationstechnische Privatheit vor staatlichen Übergriffen. Es soll verhindert werden, dass über die Ausspähung höchstpersönlicher Informationen wie gespeicherten Bildern oder Briefen Persönlichkeitsprofile des Grundrechtsträgers zusammengestellt werden können. Im Fall der Quellen-Telekommunikationsüberwachung ist dies jedoch nicht zu besorgen. In Bezug auf die gespeicherten Messenger-Daten erreicht der Eingriff unter keinen Umständen die Intensität einer Wohnraumüberwachung. Stattdessen gleicht er der klassischen Telekommunikationsüberwachung. Infolgedessen ist es wertungsmäßig nicht zu beanstanden, wenn an die Rechtfertigung des Eingriffs in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG niedrigere Anforderungen gestellt werden.

(Prof. Dr. Jan-Hendrik Dietrich)