Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)844 C

Stellungnahme

von

Prof. Dr. Kurt Graulich, Humboldt Universität zu Berlin

Richter am Bundesverwaltungsgericht a.D.

Für die Öffentliche Anhörung des Ausschuss für Inneres und Heimat des Deutschen Bundestags am Montag, 17. Mai 2021, 12.00 Uhr zum Gesetzentwurf der Bundesregierung für ein Gesetzes zur Anpassung des Verfassungsschutzrechts (BT-Drs. 19/24785)

Gliederung

Einzelheiten:

Zusammenfassung in Thesen:

I. BVerfSchG

1. Soziale Medien ermöglichen Einzelpersonen eine zuvor nicht gekannte große Wirkungsbreite für Agitation und Hassbotschaften. Durch eine Änderung von § 4 Abs. 1 BVerfSchG sollte daher – bei Vorliegen der Voraussetzungen - auch die Beobachtung von isoliert handelnden Einzelpersonen ermöglicht werden.

2. Die beabsichtigte Änderung von § 6 Abs. 2 BVerfSchG vertieft in sinnvoller Weise die Kooperation im Verfassungsschutzverbund von BfV und MAD.

3. Der neu anzufügende § 8a Abs. 4 BVerfSchG stellt den Anwendungsbereich der Bestandsdatenauskunft in Bezug auf ausländische Unternehmen klar. Auch die inländische Leistungserbringung begründet die deutsche Jurisdiktion über den Sachverhalt. Um ausländischen Unternehmen im Kundenverhältnis eine eindeutige Legitimationsgrundlage für ihre Kooperation zu geben, wird das Marktortprinzip nunmehr ausdrücklich im Gesetz verankert (BT-Drs. 19/24785 S.1 18).

II. MADG

Nach der Begründung im Regierungsentwurf handelt es sich bei § 3 Abs. 3 MADG um die Komplementärregelung zum neuen § 6 Absatz 2 BVerfSchG (Artikel 1 Nummer 2) im MAD-Gesetz. Aufgrund der Neufassung von § 6 Abs. 2 Satz 2 BVerfSchG in diesem Gesetzesentwurf kann der MAD zur Erfüllung der Unterrichtungspflichten nach § 3 Abs. 3 Satz 1 des MADG am nachrichtendienstlichen Informationssystem teilnehmen und damit seinen Beitrag zur informationellen Zusammenarbeit erfüllen. Der vorgeschlagenen Neuregelung im MADG sollte daher zugestimmt werden.

III. G 10

1. Mit der beabsichtigten Änderung von § 2 Abs. 1 G 10 durch die Einfügung eines neuen § 2 Abs. 1a G 10 werden die bisher in § 2 Abs. 1 Satz 3 bis 5 G 10 geregelten Pflichten der Anbieter, die geschäftsmäßig Telekommunikationsdienste erbringen oder hieran mitwirken, eigenständig geregelt und an die Gegebenheiten der digitalisierten Nachrichtenübermittlung angepasst. Damit wird die Konsequenz aus der telekommunikationsrechtlichen Vorlage in § 110 Abs. 1 Nr. 5 TKG gezogen.

2. Die beabsichtigte Neuregelung des § 3a Abs. 1 Satz 12 G 10 schafft – als Aspekt des Kernbereichsschutzes - verfassungskonforme Löschungsfristen für die Löschung von Löschprotokollen (BVerfGE 141, 220 – Rn. 205).

3. § 11 Abs. 1a G 10 des Gesetzesentwurfs sieht Befugnisse für schwerwiegende Eingriffe in das Grundrecht der Telekommunikationsfreiheit – in Form einer Online-Durchsuchung - und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer – in Form einer Durchsuchung des Speichersystems im Anschluss an die Telekommunikation - durch die in § 9 G10 benannten Nachrichtendienste vor. Die Voraussetzungen für die Ausübung dieser Befugnisse werden in der Regelung nicht besonders benannt; die allgemeinen Befugnisse aus dem G 10 reichen dafür nicht aus. Das Regelungsdefizit wird dadurch verstärkt, dass auch nicht nach dem Verhältnismäßigkeitsgrundsatz differenziert wird, soweit es um die Inlandsnachrichtendienste einerseits und den Auslandsnachrichtendienst andererseits geht, denn die Erforderlichkeit von Eingriffen in Speichermedien stellt sich bei ihren Aufgaben unterschiedlich. In der vorgelegten Form ist das Gesetz nicht verfassungsgemäß.

I. Änderung des Bundesverfassungsschutzgesetzes

1. § 4 Abs. 1 BVerfSchG Beobachtung von Einzelpersonen

In ihrer überkommenen Fassung schränkt § 4 Abs. 1 Satz 4 BVerfSchG die Beobachtung von isoliert handelnden Einzelpersonen ein, die weder in einem noch für einen Personenzusammenschluss handeln (BVerwGE 137, 275 Rn. 66). Danach sind Verhaltensweisen von Einzelpersonen, die nicht in einem (§ 4 Abs. 1 Satz 1 BVerfSchG) oder für einen (§ 4 Abs. 1 Satz 2 BVerfSchG) Personenzusammenschluss handeln, Bestrebungen im Sinne des BVerfSchG, wenn sie auf Anwendung von Gewalt gerichtet oder aufgrund ihrer Wirkungsweise geeignet sind, eines der in § 3 Abs. 1 oder § 4 Abs. 1 BVerfSchG genannten Schutzgüter erheblich zu beschädigen (Roth in Schenke/Graulich/Ruthig, BVerfSchG, 2. Aufl., §§3/4 Rn. 37). Grund für diese Einschränkung war die Einschätzung des Gesetzgebers, dass Einzelpersonen, die unabhängig von Personenzusammenschlüssen agieren, grundsätzlich eine geringere Gefahr für die gesetzlichen Schutzgüter darstellen als Personenzusammenschlüsse und daher nur unter restriktiveren Voraussetzungen zu beobachten sind. Personenzusammenschlüsse und deren Mitglieder und Anhänger sind grundsätzlich gefährlicher, sowohl wegen ihrer Zahl als auch deshalb, weil der Gruppendruck geeignet ist, Bedenken und Kritik auszuschalten und den Ausstieg zu erschweren ((Roth in Schenke/Graulich/Ruthig, BVerfSchG, 2. Aufl., §§3/4 Rn. 38).

Der Regierungsentwurf geht demgegenüber davon aus, unter den Bedingungen der digitalen Moderne und Erkenntnissen zu Radikalisierungsverläufen könne an dieser Unterscheidung so nicht festgehalten werden. Beispielsweise eröffneten soziale Medien gleichermaßen Einzelpersonen eine enorme Wirkungsbreite für Agitation und Hassbotschaften, wobei soziale Medien ihrerseits eine hohe Alltagsverbreitung aufweisen, ihrer Nutzung an sich nichts Besonderes mehr anhaftet. Dem ist zu folgen (BT.-Drs. 19/24785 S. 17).

2. § 6 Abs. 2 Sätze 1 bis 4 BVerfSchG MAD im Verfassungsschutzverbund

§ 6 Abs. 2 BVerfSchG enthält die Regelungen zum Führen gemeinsamer Dateien innerhalb des Verfassungsschutzverbundes von Bund und Ländern (sog. Verbunddateien), passt diese jedoch an die gewachsenen Informationsbedürfnisse der Verfassungsschutzbehörden untereinander an; dies fördert angesichts der gestiegenen Herausforderungen an die Sicherheitsbehörden die erforderlichen Synergieeffekte und Kooperationsmöglichkeiten (BT-Drs. 18/4654, S. 22). Von der Führung der gemeinsamen Dateien gem. § 6 Abs. 2 BVerfSchG unberührt bleibt die Errichtung projektbezogener gemeinsamer Dateien (§ 22a BVerfSchG) und gemeinsamer Dateien mit ausländischen Nachrichtendiensten durch das BfV (§

22b BVerfSchG). Daneben kommt eine Teilnahme der Verfassungsschutzbehörden an projektbezogenen gemeinsamen Dateien des BND (§ 25 BNDG) und des BKA (§ 9a BKAG) sowie die Teilnahme des BfV an gemeinsamen Dateien mit ausländischen Nachrichtendiensten (§ 22c) in Betracht (Roth in Schenke/Graulich/Ruthig, BVerfSchG, 2. Aufl., § 6 Rn. 3).

Wesentlicher Inhalt der in § 6 Abs. 2 BVerfSchG neu eingefügten Sätze 1 bis 4 ist die in Satz 2 eröffnete Möglichkeit, den MAD vollständig in den Informationsverbund der Verfassungsschutzbehörden zu integrieren. Das nachrichtendienstliche Informationssystem dient gerade dazu, die Informationen der Verfassungsschutzbehörden zusammenzuführen und allen Behörden für ihre jeweilige Aufgabe verfügbar zu machen. Dies hat nicht nur die föderale Komponente der Gliederung des Verwaltungszweigs in Landesbehörden und das Bundesamt. Der MAD hat – mit spezieller Zuständigkeit im Geschäftsbereich des BMVg – gleichfalls Aufgaben einer Verfassungsschutzbehörde (vgl. § 3 Abs. 1 und 2 Nr. 1 und 2 BVerfSchG und § 1 Abs. 1 und 3 Nr. 1 MADG) (BT-Drs. 19/). Die beabsichtigte Neuregelung vertieft die Zusammenarbeit zwischen BfV und MAD beim Abruf der in Verbunddateien gespeicherten Informationen. Demgegenüber müssen andere Stellen für die Übermittlung von Daten weiterhin den allgemeinen Übermittlungsvorschriften folgen.

3. § 8a Abs. 4 BVerSchG Bestandsdatenauskunft bei Telediensten u.a.

Die zur Anfügung vorgesehene Regelung des § 8a Abs. 4 BVerfSchG bedarf der Vergewisserung des bereits vorhandenen Normierungsbestandes insbesondere in § 8a Abs. 1und Abs. 2 BVerfSchG. Die im Jahr 2007 eingefügte Vorschrift des § 8a BVerfSchG regelt die offene Datenerhebung im Wege besonderer Auskunftsverlangen des BfV. Die mit dem – im Anschluss an die Anschläge vom 11.9.2001 erlassenen – Terrorismusbekämpfungsgesetz vom 9.1.2002 erweiterten Befugnisse des BfV, die namentlich auf die Aufklärung internationaler Finanz- und Kommunikationsstrukturen extremistischer bzw. terroristischer Netzwerke zielen, wurden mit dem Terrorismusergänzungsgesetz vom 5.1.2007 modifiziert und in § 8a BVerfSchG übernommen. Es folgte das Gesetz vom 7.12.2011, das darauf abzielte, die rechtsstaatliche Kontrolle und den Grundrechtsschutz „durch eine systematisch stimmig ausgestaltete Regelung der Verfahren und Mitteilungspflichten“ zu verbessern (vgl. BT-Drs. 17/6925, S. 1, 10 ff.). § 8a räumt dem BfV Befugnisse zur Auskunftseinholung (Abs. 1 und 2) ein. Es steht im Ermessen des BfV, ob es von diesen Befugnissen Gebrauch macht. Mit der in § 8a BVerfSchG geregelten Erhebungsbefugnis des BfV korrespondiert nach § 8 b Abs. 6 BVerfSchG eine Auskunftspflicht der ersuchten nicht-öffentlichen Stellen (Mallmann in Schenke/Graulich/Ruthig, BVerfSchG, 2. Aufl., § 8a Rn. 1 ff.).

§ 8a Abs. 1 BVerfSchG regelt die Befugnis des BfV zur Einholung von Auskunft über Bestandsdaten von Telediensten im Einzelfall (also nicht rastermäßig; ebenso § 8a Abs. 2 BVerfSchG) und definiert zugleich den Begriff Bestandsdaten. Es handelt sich hierbei um Daten, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Teledienste gespeichert worden sind. Erforderlich sind weiter tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die in § 3 Abs. 1 BVerfSchG genannten Schutzgüter (Mallmann in Schenke/Graulich/Ruthig, BVerfSchG, 2. Aufl., § 8a Rn. 4). § 8a Abs. 2 BVerfSchG fasst die bisherigen Luftfahrt-, Banken- und Verkehrsdatenauskunftsregelungen zusammen und erweitert sie hinsichtlich der Kontostammdaten. Nach Abs. 2 Satz 1 Nr. 4 darf das BfV bei denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, Auskunft zu bestimmten Verkehrsdaten i.S.v. § 96 TKG einholen. Nach § 3 Nr. 24 TKG sind „Telekommunikationsdienste“ in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen (Mallmann a.a.O. Rn. 14). Darüber hinaus erstreckt sich die Befugnis des BfV zur Einholung von Auskünften nach Abs. 2 Nr. 4 auf sonstige zum Aufbau und zur Aufrechthaltung der Telekommunikation notwendige Verkehrsdaten i. S. v. § 3 Nr. 30 TKG (hierzu und zum Folgenden Löffelmann in Dietrich/Eiffler, Handbuch VI § 5 Rn. 75 ff. mwN; s. auch oben Rn. 12 und § 96 Abs. 1 Nr. 5 TKG; vgl. zur Vorratsdatenspeicherung BVerfGE 125, 260). Hierdurch erfasst sind Standortdaten für den Fall der „Stand-by-Daten“, weil einem Mobilfunknetz zum Zweck des Aufbaus einer Telekommunikation zu einem Mobiltelefon dessen Standort – zumindest grob – bekannt sein muss. Die Angabe zu einem aktiv geschalteten Mobiltelefon kann also unabhängig vom Verbindungsaufbau erfolgen (vgl. BT-Drs. 16/ 2921, S. 15).

Zu beachten ist, dass der Schutzbereich des Telekommunikationsgeheimnisses (Fernmeldegeheimnisses) nach Art. 10 GG (dazu H.A.Wolff in Hömig/Wolff Grundgesetz 11. Aufl. 2016 Art. 10 Rn. 2 ff. mwN zur Rechtsprechung; s. auch Schantz in Schantz/Wolff, Das neue Datenschutzrecht 2017 Rn. 178 ff.; vgl. weiter § 8c) über die Inhalte der Kommunikation hinausgeht. Geschützt ist vielmehr auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs, zu denen insbesondere gehört, ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist. In der Erfassung von Telekommunikationsdaten, ihrer Speicherung, ihrem Abgleich mit anderen Daten, ihrer Auswertung, ihrer Selektierung zur weiteren Verwendung oder ihrer Übermittlung an Dritte liegen je eigene Eingriffe in das Telekommunikationsgeheimnis (vgl. BVerfGE 100, 313 [366 f.]). Folglich liegt in der Anordnung gegenüber Kommunikationsunternehmen,

Telekommunikationsdaten zu erheben, zu speichern und an staatliche Stellen zu übermitteln, jeweils ein Eingriff in Art. 10 Abs. 1 GG (vgl. BVerfGE 107, 299 [313]; vgl. zum Ganzen die Kommentierung des § 1 G 10 Rn. 2 ff.). (Mallmann a.a.O. Rn. 14a).

Nach der Begründung im Regierungsentwurf trifft der neu anzufügende § 8a Abs. 4 BVerfSchG eine Klarstellung zum Anwendungsbereich in Bezug auf ausländische Unternehmen. Bereits die geltende Auskunftsregelung enthält keine Beschränkung auf Unternehmen mit einer (Zweig-)Niederlassung im Inland. Auch die inländische Leistungserbringung begründet die deutsche Jurisdiktion über den Sachverhalt. Um ausländischen Unternehmen im Kundenverhältnis eine eindeutige Legitimationsgrundlage für ihre Kooperation zu geben, wird das Marktortprinzip nunmehr ausdrücklich im Gesetz verankert (BT-Drs. 19/24785 S.1 18). Dieses Verständnis deckt sich mit der Anwendung des unionalen Wirtschaftsrechts im Allgemeinen. Nach dem Marktortprinzip setzt beispielsweise die Anwendung deutschen Wettbewerbsrechts voraus, dass die wettbewerblichen Interessen der Mitbewerber im Inland aufeinander treffen (BGH, GRUR 2006, 513 TZ 25 - Arzneimittelwerbung im Internet; KG Berlin, Urteil vom 29. September 2015 – 5 U 16/14 –, Rn. 49 - 50).

II. Artikel 2 Änderung des MAD-Gesetzes

1. § 3 Abs. 3 MADG Gegenseitige Unterrichtung und Datenabruf

§ 3 MADG betrifft die Zusammenarbeit des MAD im Bereich des Verfassungsschutzes. Dazu gehört die Zulässigkeit eines Abrufs aus Verbunddateien des BfV durch den MAD. In § 3 Abs. 3 MADG ist die informationelle Zusammenarbeit zwischen MAD und den Verfassungsschutzbehörden – BfV und LfV – als spezieller Fall der Zusammenarbeit geregelt (Siems in Schenke/Graulich/Ruthig, MADG, 2. Aufl., § 3 Rn. 1). Die auf Gegenseitigkeit beruhende Unterrichtung des MAD und des BfV über relevante Sachverhalte im Zuständigkeitsbereich der jeweils anderen Behörde nach § 3 Abs. 3 MADG stellt die wichtigste Form der Zusammenarbeit dar. Das Gesetz verzichtet anders als zwischen den Verfassungsschutzbehörden untereinander in § 1 Abs. 2 und § 6 Satz 1 BVerfSchG auf die ausdrückliche Formulierung als Pflicht, räumt aber mit seinem Wortlaut ebenfalls keinen Ermessensspielraum ein. Die Pflicht begründet sich in dem für das Zusammenwirken der mit Verfassungsschutzaufgaben betrauten Behörden zwingend notwendigen Ausgleich der organisatorischen Trennung. Die Regelung geht daher den Übermittlungsvorschriften des §§ 10, 11 MADG i. V. m. §§ 17 ff. BVerfSchG vor (Siems in Schenke/Graulich/Ruthig, MADG, 2. Aufl., § 3 Rn. 9 ff.). Nach der Neufassung von § 6 Abs. 2 Satz 2 BVerfSchG in diesem Gesetz kann der MAD zur Erfüllung der Unterrichtungspflichten nach § 3 Abs.

3 Satz 1 des MADG am nachrichtendienstlichen Informationssystem teilnehmen und damit seinen Beitrag zur informationellen Zusammenarbeit erfüllen. Nach der Begründung im Regierungsentwurf handelt es sich bei § 3 Abs. 3 MADG um die Komplementärregelung zum neuen § 6 Absatz 2 BVerfSchG (Artikel 1 Nummer 2) im MAD-Gesetz. Die Regelung ist gleichermaßen nicht auf einen obligatorischen Volleinbezug des MAD im NADIS beschränkt, sondern eröffnet auch flexiblere (Übergangs-)Lösungen gemeinsamer Datenhaltung für technisch und wirtschaftlich optimierte (Zwischen-)Gestaltungen, die auch in der gegenseitigen Einräumung (lesender oder schreibender) Zugriffsrechte bestehen können. Einwände gegen die vorgesehen Neuregelung bestehen nicht.

III. Zu Artikel 5 (Änderung des Artikel 10-Gesetzes)

1. Zu § 2 G 10 Pflichten der Anbieter von Post- und TK-Diensten; Verordnungsermächtigung

a) Aufhebung von § 2 Abs. 1 S. 3 bis 5 G10

Mit der Aufhebung der bisher in § 2 Abs. 1 Satz 3 bis 5 G 10 geregelten Pflichten der TK-Anbieter und deren eigenständige Regelung in § 2 Abs. 1a G 10 sollen ihre Obliegenheiten an die Gegebenheiten der digitalisierten Nachrichtenübermittlung angepasst werden. Zugleich wird mit der Aufhebung Platz für eine Umstellung der VO-Ermächtigung zu einer eigenen Regelung in § 2 Abs. 1 b G 10 geschaffen (BT-Drs.19 /24785 S. 21).

b) Anfügung von § 2 Abs. 1a G 10 Pflichten von TK-Dienstleistern

Die ursprünglich in § 2 Abs. 1 S. 3 bis 5 G 10 enthaltenen und nunmehr nach Abs. 1 a verschobenen Regelungen betreffen Pflichten für TK-Anbieter. Da es um „geschäftsmäßiges Erbringen“ von Dienstleistungen geht, gelten die Regelungen nicht für rein firmen- oder behördenintern betriebene Kommunikationsnetze wie z.B. das Intranet oder andere Corporate Networks (Huber in Schenke/Graulich/Ruthig, G 10, 2. Aufl., § 2 Rn. 10). Die Umstellung auf die Gewährung von „Zugang zu seinen Einrichtungen“ ist der Umstellung der Regelung auf die digitale Technizität geschuldet. Die „Verpflichtung zur Ausleitung“ beinhaltet die Übermittlung von Inhalten der Telekommunikation in der Regel in digitaler Form. Genauso wird mit § 2 Abs. 1a Satz 1 Nr. 4 G 10 eine Verpflichtung zur Mitwirkung bei der Einbringung technischer Mittel nach § 11 Abs. 1a G 10 neu eingeführt (BT-Drs.19 /24785 S. 21).

Das G 10 zieht die Konsequenz aus der telekommunikationsrechtlichen Vorlage in § 110 Abs. 1 Nr. 5 TKG. Wer eine Telekommunikationsanlage betreibt, mit der öffentlich zugängliche Telekommunikationsdienste erbracht werden, hat danach die Aufstellung und den Betrieb von Geräten für die Durchführung von

Maßnahmen nach den §§ 5 und 8 G 10 oder nach den §§ 6, 12 und 14 des BNDG a.F. in seinen Räumen zu dulden und Bediensteten der für diese Maßnahmen zuständigen Stelle sowie bei Maßnahmen nach den §§ 5 und 8 G 10 den Mitgliedern und Mitarbeitern der G 10-Kommission (§ 1 Abs. 2 G 10) Zugang zu diesen Geräten zur Erfüllung ihrer gesetzlichen Aufgaben zu gewähren. Im Rahmen der sog. strategischen Kontrolle haben die Anlagebetreiber nach §110 Abs.1 Nr.5 TKG den Mitarbeitern des BND und der G 10-Kommission Zugang zu ihren Räumlichkeiten zu gewähren und zu dulden, dass die zur Durchführung der Überwachung erforderlichen Geräte in ihren Räumlichkeiten abgestellt werden. Das Nähere regelt § 27 Abs. 2–4 TKÜV. Es lässt sich aufgrund dessen erkennen, dass der Verpflichtete nach § 2 Abs. 1 Satz 3 G 10 die Überwachung und Aufzeichnung ermöglichen und dem Bundesnachrichtendienst gemäß § 2 Abs. 1 Satz 5 G 10 i.V.m. § 110 Abs. 1 Satz 1 Nr.1 TKG, § 27 Abs.2 TKÜV eine vollständige Kopie der auf den angeordneten Übertragungswegen abgewickelten Telekommunikationen an dem jeweiligen Subknotenpunkt der Klägerin als Übergabepunkt im Inland bereitzustellen muss (Graulich in Fetzer/Scherer/Graulich, TKG 3. Aufl, § 110 Rn. 15).

c) Anfügung von § 2 Abs. 1b G 10 Verordnungsermächtigung

§ 2 Abs. 1b G 10 enthält in der neuen Fassung die Ermächtigung, durch Verordnung das Nähere zur technischen und organisatorischen Umsetzung der Mitwirkungspflichten nach § 2 Abs. 1 Satz 1 Nr. 4 G 10 zu regeln. Der Ermächtigungsadressat entspricht der Regelung des § 8b Abs. 8 Satz 1 BVerfSchG, wobei hier jedoch die Zustimmung des Bundesrates vorgesehen ist, da das G 10 auch von Ländern vollzogen wird. Dies entspricht Art. 80 Abs. 2 GG.

2. Zu § 3a G 10 Schutz des Kernbereichs privater Lebensgestaltung

a) zu § 3a Abs. 1 Satz 12 G 10 Löschungspflicht

§ 3a Abs. 1 G 10 dient dem Schutz des Kernbereichs der privaten Lebensgestaltung bei Beschränkungen nach § 1 Abs. 1 Nr. 1 G 10. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Beschränkung nach § 1 Abs. 1 Nr. 1 G 10 erlangt worden sind, dürfen nicht verwertet werden (§ 3a Abs. 1 S. 8 G 10 a.F.). Aufzeichnungen hierüber sind unverzüglich zu löschen (§ 3a Abs. 1 S. 9 G 10 a.F.). Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren (§ 3a Abs. 1 S. 10 G 10 a.F.). Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden (§ 3a Abs. 1 S. 11 G 10 a.F.). Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt (§ 3a Abs. 1 S. 12 a.F. G 10 a.F.). Nach dem neuen § 3a Abs. 1 S. 12 G 10 ist die Dokumentation sechs

Monate nach der Mitteilung nach § 12 Absatz 1 Satz 1 G 10 oder der Feststellung nach § 12 Absatz 1 Satz 5 G 10 zu löschen. Dies wird mit dem Hinweis auf BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 205 begründet. Danach habe der Gesetzgeber ein Verwertungsverbot sowie die sofortige Löschung, einschließlich deren Protokollierung, für dennoch erfasste höchstpersönliche Daten zu regeln. Verfassungswidrig sei jedoch eine zu kurze Frist innerhalb derer die Löschungsprotokolle zu löschen sind. Diese war in dem der Entscheidung zugrunde liegenden Fall des alten BKAG so kurz bemessen, dass während der Aufbewahrungszeit der Löschungsprotokolle typischerweise weder mit einer Kontrolle durch den Datenschutzbeauftragten noch durch die Betroffenen gerechnet werden kann und die Protokollierung der Löschung damit ihren Sinn verliert (vgl. Bäcker, a.a.O., S. 88; vgl. hierzu auch BVerfGE 100, 313 <400>; 109, 279 <332 f.>). Weil die Löschungsprotokolle selbst keine die Betroffenen belastenden Daten enthalten, konnte diese kurze Frist insbesondere nicht mit deren Schutz gerechtfertigt werden. Dieses Defizit gleicht die Neuregelung des § 3a Abs. 1 Satz 12 G 10 aus.

b) zu § 3a Abs. 2 G 10 Sichtung von Aufzeichnungen

§ 3a Abs. G 10 ergänzt – in Anlehnung an § 51 Abs. 8 BKAG – eine Eilfallregelung, um den Behörden für Ausnahmefälle bei Gefahr im Verzug auch kurzfristig erste Handlungsmöglichkeiten einzuräumen (BVerfGE 141, 220 – Rn. 129). Dem ist zuzustimmen.

3. Durchführung von Beschränkungsmaßnahmen

a) § 11 Abs. 1a G 10 Eingriff in ein informationstechnisches System

Die Reichweite des Grundrechts auf Telekommunikationsfreiheit erstreckt sich auf jede Übermittlung von Informationen mit Hilfe der verfügbaren Telekommunikationstechniken. Auf die konkrete Übermittlungsart (Kabel oder Funk, analoge oder digitale Vermittlung) und Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) kommt es nicht an. Dementsprechend werden neben den „klassischen“ Verbindungen über Festnetz und Mobilfunknetz auch online-Verbindungen, z.B. E-Mail-Nachrichten oder Telefonie in Form von Voice over IP, vom Fernmeldegeheimnis umfasst. Das Fernmeldegeheimnis umfasst beispielsweise grundsätzlich auch die Nachrichtenübermittlung via Kurznachricht (SMS), Multimedia Messaging Service (MMS) oder Telefax (Graulich in Fetzer/Scherer/Graulich, TKG, 3. Aufl., § 88 Rn. 22 m.w.N.).

Nach § 11 Abs. 1a S. 1 und 2 G 10 n.F. sollen Eingriffe in elektronische Speichermedien vorgesehen werden, und zwar auch während der laufenden

Telekommunikation: „Die Überwachung und Aufzeichnung der laufenden Telekommunikation, die nach dem Zeitpunkt der Anordnung übertragen worden ist, darf auch in der Art und Weise erfolgen, dass in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. Auf dem informationstechnischen System des Betroffenen ab dem Zeitpunkt der Anordnung gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können." Dies ist eine Kombination von telekommunikationsrechtlicher Online-Recherche (aa)) und Eingriffen in die Vertraulichkeit und Integrität informationstechnischer System (bb)). Dabei handelt es sich um zwei Gruppen der schwersten Grundrechtseingriffe, deren Beantragung (§ 9 G 10), Anordnung (§ 10 G 10) und Durchführung (§ 11 G 10) darüber hinaus dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz unterliegt (cc)).

aa) Telekommunikationsgrundrecht und Online-Durchsuchung

Der Quellen-TKÜ technisch eng verwandt ist die sog. Online-Durchsuchung, bei der es ebenfalls erforderlich ist, auf dem Rechner des Betroffenen heimlich eine Spionagesoftware zu installieren. Dies führt zu einem komplexen Zusammenspiel von zwei verschiedenen Grundrechten. Diese Software überwacht dann nämlich nicht – zumindest nicht vorrangig – den Inhalt der durch Art. 10 GG geschützten IP-Telefonie, sondern durchsucht die durch Art. 1 Abs- 1 i.V.m. Art. 2 Abs. 1 GG („Computer-Grundrecht") geschützte Festplatte des Betroffenen. Der durch das Telekommunikationsgeheimnis bewirkte Schutz besteht dann nicht, wenn eine staatliche Stelle die Nutzung eines informationstechnischen Systems als solche überwacht oder die Speichermedien des Systems durchsucht. Hinsichtlich der Erfassung der Inhalte oder Umstände außerhalb der laufenden Telekommunikation liegt ein Eingriff in Art.10 Abs.1 GG selbst dann nicht vor, wenn zur Übermittlung der erhobenen Daten an die auswertende Behörde eine Telekommunikationsverbindung genutzt wird, wie dies etwa bei einem Online-Zugriff auf gespeicherte Daten der Fall ist. Vor diesem Hintergrund hat das BVerfG in seiner Entscheidung zur Online-Durchsuchung (BVerfG, v. 27.02.2008, Az: 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274–350) das IT-Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sog. „Computer-Grundrecht") geschaffen und klargestellt, dass eine Online-Durchsuchung nur in eng begrenzten Ausnahmefällen zulässig ist. Der Schutz des Fernmeldegeheimnisses ist dadurch – der Idee nach – nicht betroffen (Graulich in Fetzer/Scherer/Graulich, TKG, 3. Aufl., § 88 Rn. 54 m.w.N.).

Wird ein komplexes informationstechnisches System zum Zweck der Telekommunikationsüberwachung technisch infiltriert („Quellen-Telekommunikationsüberwachung“), so ist mit der Infiltration die entscheidende Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist. Insbesondere können auch die auf dem Personalcomputer abgelegten Daten zur Kenntnis genommen werden, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen. Soweit der heimliche Zugriff auf ein informationstechnisches System dazu dient, Daten auch insoweit zu erheben, als Art.10 Abs.1 GG nicht vor einem Zugriff schützt, bleibt eine Schutzlücke, die durch das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Schutz der Vertraulichkeit und Integrität von informationstechnischen Systemen zu schließen ist (Graulich in Fetzer/Scherer/Graulich, TKG, 3. Aufl., § 88 Rn. 22 m.w.N.).

bb) Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (GGVliS)

Der Schutz des Fernmeldegeheimnisses endet in dem Moment, in dem die Nachricht bei dem Empfänger angekommen und der Übertragungsvorgang beendet ist. Die spezifischen Gefahren der räumlich distanzierten Kommunikation bestehen im Herrschaftsbereich des Empfängers, der eigene Schutzvorkehrungen treffen kann, nicht. Die Nachricht ist mit Zugang beim Empfänger nicht mehr den erleichterten Zugriffsmöglichkeiten Dritter ausgesetzt, die sich aus der fehlenden Beherrschbarkeit und Überwachungsmöglichkeit des Übertragungsvorgangs durch die Kommunikationsteilnehmer ergeben. Die – auf einem elektronischen Medium - gespeicherten Inhalte und Verbindungsdaten unterscheiden sich dann nicht mehr von Datenbeständen, die der Nutzer selbst angelegt hat. Dort beginnt der Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (GGVliS). Im Verhältnis zur Telekommunikation erlangt es angesichts seines auf Schutzlücken bezogenen Charakters praktisch zwar nur bei der Infiltration informationstechnischer Systeme Bedeutung. Der Schutz des Art.10 Abs. 1 GG endet dort, wo Daten öffentlich zugänglich sind oder wenn geschützte Daten nicht durch Teilnahme an der Telekommunikation erlangt werden (Graulich in Fetzer/Scherer/Graulich, TKG, 3. Aufl., § 88 Rn. 10 m.w.N.). Von diesem Punkt an beginnt für Daten auf einem elektronischen Speichermedium aber der Schutz durch das GGVliS.

cc) Verhältnismäßigkeitsgrundsatz

Durch die mit § 11 Abs. 1a G 10 n.F. verbundene Online-Durchsuchung und den Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (GGVliS) wird eine neue Gewichtsklasse von Beschränkungen der Telekommunikation und ihrer komplementären Bezirke im G 10 erreicht. Dafür bedarf es der Formulierung klarer und bestimmter Eingriffstatbestände. Daran fehlt es. Das neu geschaffene Eingriffsinstrumentarium legt nicht einmal hinreichend deutlich die tatbestandlichen Voraussetzungen fest, zur Aufklärung oder Abwehr welcher Szenarien von Rechtsgüterbedrohungen es geschaffen ist. Und überhaupt fehlt es an einer verhältnismäßigen Moderierung des Einsatzes der Eingriffsmittel.

Für tief in die Privatsphäre eingreifende Ermittlungs- und Überwachungsbefugnisse hat das Bundesverfassungsgericht aus dem Verhältnismäßigkeitsgrundsatz im engeren Sinne übergreifende Anforderungen abgeleitet. Diese betreffen spezifisch breitenwirksame Grundrechtsgefährdungspotenziale, insbesondere solche der elektronischen Datenverarbeitung (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 103).

Bei der näheren Ausgestaltung der Einzelbefugnisse kommt es für deren Angemessenheit wie für die zu fordernde Bestimmtheit maßgeblich auf das Gewicht des jeweils normierten Eingriffs an. Je tiefer Überwachungsmaßnahmen in das Privatleben hineinreichen und berechtigte Vertraulichkeitserwartungen überwinden, desto strenger sind die Anforderungen. Besonders tief in die Privatsphäre dringen die Wohnraumüberwachung sowie der Zugriff auf informationstechnische Systeme (BVerfG a.a.O. Rn. 105). Die Maßnahmen aus § 11 Abs. 1a G 10 stehen nach § 9 G10 ungeteilt den Nachrichtendiensten des Bundes zur Verfügung. Dies ist unter dem Gesichtspunkt der Erforderlichkeit nicht nachvollziehbar. Ein Auslandsnachrichtendienst befindet sich bei der Informationsbeschaffung in einer voraussetzungsvolleren Situation – die eher Maßnahmen nach § 11 Abs. 1a G 10 erfordern können - als ein Inlandsnachrichtendienst. Danach wir aber nicht unterschieden.

b) § 11 Abs. 1b G 10 Erstreckung der Beschränkungsmaßnahmen

Werden nach der Anordnung der Beschränkungsmaßnahme weitere Kennungen von Telekommunikationsanschlüssen der adressierten Person bekannt, darf die Durchführung der Beschränkungsmaßnahme nach einer Neuregelung in § 11 Abs. 1b G 10 auch auf diese Kennungen erstreckt werden. Der neue § 11 Abs. 1b G 10 regelt den speziellen Fall einer technischen Erweiterung der gegen eine Person laufenden Maßnahme aufgrund eindeutiger Erkenntnisse über weitere Kennungen von Telekommunikationsanschlüssen dieser von der Maßnahme betroffenen Person (BT-Drs. 19/24785 S. 22).

Funktional ist die vorgeschlagene Änderung eine Variante der Eilanordnung nach § 15a G10. Dementsprechend sollte sie mit einem Genehmigungsvorbehalt der G10 Kommission und einer Löschungsanordnung für den Fall versehen werden, dass die G10 Kommission der technischen Erweiterung nicht zustimmt.1

Prof. Dr. Kurt Graulich Berlin, d. 15.05.2021