19. Wahlperiode

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Wortprotokoll
der 139. Sitzung

Ausschuss für Inneres und Heimat
Berlin, den 17. Mai 2021, 12:00 Uhr
10557 Berlin
Konrad-Adenauer-Str. 1
Paul-Löbe-Haus, Raum 4 900

Vorsitz: Andrea Lindholz, MdB

Tagesordnung - Öffentliche Anhörung

Tagesordnungspunkt	**Seite 6**

a) Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts

BT-Drucksache 19/24785

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss für Wirtschaft und Energie
Verteidigungsausschuss
Ausschuss Digitale Agenda

Gutachtlich:
Parlamentarischer Beirat für nachhaltige Entwicklung

Berichterstatter/in:
Abg. Michael Brand (Fulda) [CDU/CSU]
Abg. Uli Grötsch [SPD]
Abg. Dr. Christian Wirth [AfD]
Abg. Benjamin Strasser [FDP]
Abg. Dr. André Hahn [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

b) Antrag der Abgeordneten Konstantin Kuhle, Stephan Thomae, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP

Bürgerrechte und Sicherheit schützen – Für einen wirksamen Verfassungsschutz

BT-Drucksache 19/16875

Federführend:
Ausschuss für Inneres und Heimat

Berichterstatter/in:
Abg. Michael Brand (Fulda) [CDU/CSU]
Abg. Uli Grötsch [SPD]
Abg. Dr. Christian Wirth [AfD]
Abg. Benjamin Strasser [FDP]
Abg. Dr. André Hahn [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

c) Antrag der Abgeordneten Dr. André Hahn, Gökay Akbulut, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE.

Zivilgesellschaft stärken, Verfassung wirksam schützen

BT-Drucksache 19/8960

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss für Menschenrechte und humanitäre Hilfe

Berichterstatter/in:
Abg. Michael Brand (Fulda) [CDU/CSU]
Abg. Uli Grötsch [SPD]
Abg. Dr. Christian Wirth [AfD]
Abg. Benjamin Strasser [FDP]
Abg. Dr. André Hahn [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

d) Antrag der Abgeordneten Dr. Konstantin von Notz, Dr. Irene Mihalic, Luise Amtsberg, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Neustart des Verfassungsschutzes des Bundes

BT-Drucksache 19/8700

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Ausschuss für Recht und Verbraucherschutz

Berichterstatter/in:
Abg. Michael Brand (Fulda) [CDU/CSU]
Abg. Uli Grötsch [SPD]
Abg. Dr. Christian Wirth [AfD]
Abg. Benjamin Strasser [FDP]
Abg. Dr. André Hahn [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

Inhaltsverzeichnis

Mitglieder des Ausschusses

	Ordentliche Mitglieder	**Stellvertretende Mitglieder**
CDU/CSU	Brand (Fulda), Michael Lindholz, Andrea Müller, Axel Throm, Alexander	
SPD	Grötsch, Uli	
AfD	Wirth, Dr. Christian	
FDP	Kuhle, Konstantin Strasser, Benjamin	
DIE LINKE.	Renner, Martina	
BÜNDNIS 90/DIE GRÜNEN	Notz, Dr. Konstantin von	
fraktionslos		

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 17. Mai 2021, 12.00 Uhr
„Verfassungsschutzrecht“

Prof. Dr. Matthias Bäcker
Johannes Gutenberg-Universität Mainz

Prof. Dr. Jan-Hendrik Dietrich
Hochschule des Bundes für öffentliche Verwaltung, Berlin

Prof. Dr. Kurt Graulich
Richter am Bundesverwaltungsgericht a. D., Berlin

Thomas Haldenwang
Präsident - Bundesamt für Verfassungsschutz, Köln

Prof. Dr. Ralf Poscher
Geschäftsführender Direktor
Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht, Freiburg i. Br.

Dr. Benjamin Rusteberg
Georg-August-Universität Göttingen

Tagesordnungspunkt

a) Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts

BT-Drucksache 19/24785

b) Antrag der Abgeordneten Konstantin Kuhle, Stephan Thomae, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP

Bürgerrechte und Sicherheit schützen – Für einen wirksamen Verfassungsschutz

BT-Drucksache 19/16875

c) Antrag der Abgeordneten Dr. André Hahn, Gökay Akbulut, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE.

Zivilgesellschaft stärken, Verfassung wirksam schützen

BT-Drucksache 19/8960

d) Antrag der Abgeordneten Dr. Konstantin von Notz, Dr. Irene Mihalic, Luise Amtsberg, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Neustart des Verfassungsschutzes des Bundes

BT-Drucksache 19/8700

Vors. **Andrea Lindholz** (CDU/CSU): Erstmal begrüße ich alle Kolleginnen und Kollegen, die Herren Sachverständigen, die ich gleich noch einzeln vorstellen werde, sowie Herrn Marscholleck vom BMI.

Als Sachverständige zugeschaltet sind uns Herr Prof. Bäcker, Herr Prof. Graulich, Herr Prof. Poscher und Herr Dr. Rusteberg, herzlich Willkommen. Für die Union ist außerdem zugeschaltet der Abgeordnete Michael Brand, für die AfD Herr Dr. Wirth – der ist noch nicht da. Für die Fraktion DIE LINKE. ist Frau Renner zugeschaltet. Im Raum anwesend ist als Sachverständiger der Präsident des Bundesamtes für Verfassungsschutz Herr Haldenwang sowie Herr Prof. Dietrich. Ferner vertreten ist die Union mit Herrn Throm, die FDP mit Herrn Kuhle und Herrn Strasser, Herr Dr. von Notz von der Fraktion BÜNDNIS 90/DIE GRÜNEN und Herr Grötsch von der SPD.

Die Anhörung zur Anpassung des Verfassungsschutzrechtes ist vorgesehen für das Zeitfenster 12:00 bis 14:00 Uhr. Unsere Anhörung wird wie üblich live im Parlamentsfernsehen des Deutschen Bundestages oder per Stream auf der Homepage übertragen und später dann auch über die Mediathek der Öffentlichkeit zur Verfügung gestellt. Ich bedanke mich ganz herzlich bei allen Sachverständigen, dass Sie uns mit Ihrer Expertise zur Verfügung stehen und auch für Ihre schriftlichen Stellungnahmen, die bereits bei uns eingegangen sind. Diese werden zusammen mit dem Protokoll als Gesamtdrucksache veröffentlicht. Sie erhalten das Protokoll vorher noch zur Durchsicht und Ihnen wird mitgeteilt, wie Sie Korrekturen vornehmen können.

Bei der Anhörung halten wir es so, dass ich zunächst jedem Sachverständigen die Möglichkeit gebe, ein kurzes Eingangsstatement zu halten, das ein fünfminütiges Zeitfenster möglichst nicht überschreiten sollte. Danach werden die Kolleginnen und Kollegen der Fraktionen ihre Fragen stellen und Sie erhalten dann wiederum nach Abschluss der Fragerunde die Möglichkeit, gesammelt auf die Fragen zu antworten. In der ersten Fragerunde gilt, dass jeder Fragesteller entweder zwei Fragen an einen Sachverständigen stellen kann, eine gleiche Frage an zwei Sachverständige oder an zwei Sachverständige jeweils eine unterschiedliche Frage. Wir schauen dann nach der ersten Runde, wieviel Zeit wir noch für die zweite Runde haben und mit welchem Fragemodus wir dann weitermachen. Wenn dazu keiner eine Frage hat, dann würden wir beginnen mit der Einführung durch die Sachverständigen und hier dem Alphabet nach mit Herrn Professor Bäcker, bitte.

SV **Prof. Dr. Matthias Bäcker** (Johannes Gutenberg-Universität, Mainz): Vielen Dank, Frau Vorsitzende. Und ich bedanke mich herzlich für die Gelegenheit, zu dem Gesetzesentwurf Stellung zu nehmen.

Ich möchte in meiner mündlichen einleitenden Stellungnahme auf zwei Punkte eingehen: Zum einen die Ausweitung des Begriffs der „verfassungsschutzrelevanten Bestrebung“ auch auf Einzelpersonen und dann die Ermächtigung zur Durchführung von sogenannten Quellentelekommunikationsüberwachungen.

Der erste Punkt betrifft eine Änderung des Bundesverfassungsschutzgesetzes, wonach jetzt auch Einzelpersonen verfassungsschutzrelevante Bestrebungen darstellen können, wenn, so das Gesetz, ihre Verhaltensweise darauf gerichtet ist, die verfassungsfeindlichen Ziele nach § 3 des Gesetzes zu verwirklichen. Diese Regelung geht potentiell außerordentlich weit, weil sie letztlich den Verfassungsschutzbehörden praktisch generell ermöglicht, Einzelpersonen aufgrund von Anhaltspunkten oder auch Vermutungen zu ihrer subjektiven Motivation zu überwachen. Dafür sehe ich keinen Grund und ich glaube auch, dass insbesondere die Überwachungsermächtigungen – die Ermächtigungen zum Einsatz nachrichtendienstlicher Mittel – im Zusammenhang mit diesem Begriff der „verfassungsschutzrelevanten Bestrebungen“ sehr problematisch werden. Die Gesetzesbegründung nennt im Wesentlichen zwei Fallkonstellationen, in denen eine solche Überwachung von Einzelpersonen oder Beobachtung von Einzelpersonen erforderlich sein soll. Einmal nennt sie rasche – „eruptive“ – Radikalisierungsverläufe, die zu Gewalt und zu schweren Schäden führen können. Zum anderen nennt sie den Themenkomplex Hetze im Internet. Das sind meiner Ansicht nach beides legitime Ziele, die auch rechtfertigen können, Einzelpersonen unter den Bestrebungsbegriff zu fassen, allerdings müsste das dann auch besonders geregelt werden. Gewaltbereite Einzelpersonen sind sowieso jetzt schon vom Bestrebungsbegriff erfasst – da sehe ich nicht wirklich, warum der ausgeweitet werden muss. Sachverhalte, in denen Einzelpersonen im Internet zahlreiche verfassungsfeindliche Inhalte posten, ohne selbst gewaltbereit zu sein, aber so eine Atmosphäre von Aggression und Rechtsbruch schaffen, könnte man besonders in das Gesetz aufnehmen – das ist auch vielleicht rechtspolitisch eine gute Idee – aber die Regelung so, wie sie im Gesetzentwurf steht, geht weit darüber hinaus. Ich glaube im Übrigen auch nicht, dass die Beobachtungspraxis des Verfassungsschutzes diese Regelung auch nur annähernd ausschöpft derzeit. Man muss aber bei der Bewertung eines solchen Gesetzes gerade auch darauf achten, was möglich wäre, ohne gegen den Buchstaben des Gesetzes zu verstoßen. Und das ist einfach zu viel.

Dann die Quellentelekommunikationsüberwachung – auch hier gilt wieder: Es ist grundsätzlich möglich, den Nachrichtendiensten eine Ermächtigung zur Quellentelekommunikationsüberwachung zu geben – das ist auch in der Rechtsprechung schon geklärt. Die geplante Regelung weist aber zwei Defizite und Probleme auf. Das erste Problem, das meiner Ansicht nach das am schwersten wiegende ist, betrifft den Zugriffsweg. Quellentelekommunikationsüberwachungen setzen die Infiltration eines informationstechnischen Systems voraus. Diese Infiltration kann auf verschiedenen Wegen geschehen. Gegen viele dieser Wege bestehen keine generellen Bedenken – einer geht gar nicht, und das ist die Ausnutzung von Sicherheitslücken, die bisher nicht erkannt worden sind, sogenannter Zero Days. Die Ausnutzung von Zero Days verursacht Gefahren für die informationstechnische Infrastruktur der Bundesrepublik, die so groß sind, dass es kein relevantes Anliegen des Verfassungsschutzes geben kann, das es rechtfertigen würde, solche Gefahren hinzunehmen. Darum muss die Ausnutzung solcher Sicherheitslücken zwingend verboten werden. Das muss auch im Gesetz ausdrücklich klargestellt werden, sonst wird meiner Ansicht nach das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme in seiner Ausprägung als Pflicht zum Schutz der informationstechnischen Infrastruktur in der Bundesrepublik verletzt.

Das zweite Problem betrifft die Erstreckung der Quellentelekommunikationsüberwachung auch auf gespeicherte Inhalte, sofern diese seit Anordnung der Maßnahme Gegenstand eines Kommunikationsvorganges waren. Das ermöglicht – wenn man es geschafft hat, die Infiltrationssoftware aufzubringen – rückwirkend das System zu durchsuchen und zu gucken, was seit der Anordnung – die ja deutlich davor liegen kann – alles auf dem System an Kommunikation gemacht worden ist. Und das kann dann ausgeleitet werden. Das ist keine Quellentelekommunikationsüberwachung mehr, denn Quellentelekommunikationsüberwachungen beziehen sich auf laufende Kommunikation – hier geht es um vergangene Kommunikation. Das ist auch von der Funktionsweise her keine Quellenkommunikationsüberwachung, sondern eine beschränkte Onlinedurchsuchung, an die aber höhere Anforderungen bestehen.

Da muss man nun allerdings sagen, dass die Ermächtigung zur Quellentelekommunikationsüberwachung nicht die Anforderungen an Onlinedurchsuchungen erfüllt – letztlich aber auch nicht den Anforderungen an Telekommunikationsüberwachungen genügt, weil sie in das G10-G eigepflegt wird, das schlicht von vorn bis hinten unzureichend ist. Es gibt gegen das G10-G eine große Zahl von verfassungsrechtlichen Einwänden: Die Eingriffsschwellen des § 3 G10-G sind unzureichend und auch völlig systemwidrig im Verfassungsschutzrecht, weil sie auf Straftaten abstellen; die Regelungen über die Weiterverarbeitung und Übermittlung von Daten gehen viel zu weit, die Vorschriften über die Benachrichtigung der betroffenen Person sind viel zu schwammig und haben viel zu weitgehende Ausnahmen. Das G10-G bedarf generell einer Überarbeitung. Die Einpflegung dieser Vorschrift zur Quellentelekommunikationsüberwachung vertieft den Überarbeitungsbedarf noch einmal. Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann kommen wir als nächstes zu Herrn Professor Dietrich.

SV **Prof. Dr. Jan-Hendrik Dietrich** (HS Bund, Berlin): Vielen Dank Frau Vorsitzende. Meine Damen und Herren Abgeordnete, ich bedanke mich zunächst auch einmal für die Möglichkeit, hier heute meine Expertise einbringen zu dürfen. Den vorliegenden Gesetzesentwurf der Bundesregierung habe ich ebenfalls in einer ausführlichen schriftlichen Stellungnahme gewürdigt.

Die vorgeschlagenen Änderungen reagieren auf technische und tatsächliche Entwicklungen der letzten Zeit. Mit Blick auf lange unvorstellbare Ereignisse, wie etwa die Angriffe auf das Reichstagsgebäude durch gewalttätige Corona-Leugner oder gerade zuletzt antisemitische Kundgebungen vor Synagogen, erscheint ein längeres Zuwarten auf eine große Reform des Verfassungsschutzrechts, auf die wir ja alle noch warten, zur Zeit nicht angezeigt. Zusammengefasst kann man sagen, dass der Gesetzesentwurf im Wesentlichen einer rechtlichen Überprüfung standhält. Im Detail besteht gleichwohl Änderungsbedarf, der meiner Stellungnahme entnommen werden kann.

Herzstück der beabsichtigten Regelungen – der Kollege Bäcker hat das eben ausgeführt – ist die Einführung der sogenannten Quellentelekommunikationsüberwachung. Ich möchte meine Ausführungen vor dem Ausschuss daher darauf beschränken. Die genannten Änderungen sind vor dem Hintergrund einer zunehmenden und auch gewünschten Verbreitung von Verschlüsselungstechniken zu sehen. Klassische Überwachungsinstrumente stoßen zunehmend an ihre Grenzen und die Lage verschärft sich, je besser die Ende-zu-Ende-Verschlüsselung wird, die wir uns alle wünschen. In seinen Internet Organised Crime Threat Assessments aus den Jahren 2019 und 2020 hat EUROPOL erneut eindringlich vor versiegenden Informationsquellen gewarnt. Was für kriminelle Machenschaften gilt, gilt auch für extremistische Bestrebungen und terroristische Aktivitäten. Die Verschlüsselungen verhindern den Zugriff der Verfassungsschutzbehörden auf Kommunikationsinhalte über bekannte G10-Maßnahmen. Gesetzliche Beschränkungen von Verschlüsselungen erweisen sich bei näherer Betrachtung als verfassungsrechtlich unzulässig oder kaum durchsetzbar. An dieser Stelle setzt nun die Quellentelekommunikationsüberwachung an. Über die Infiltration eines informationstechnischen Systems wird in die Kommunikation eingegriffen, bevor sie verschlüsselt oder nachdem sie entschlüsselt wird. Die Sicherheitsbehörden werden dadurch erst in die Lage versetzt, ihrem gesetzlichen Auftrag trotz des verbreiteten Einsatzes von Verschlüsselungstechnik nachzukommen.

Der Gesetzesentwurf folgt nun dem Vorbild von § 100a StPO, der kürzlich eingeführt worden ist: Über § 2 Absatz 1a wird den Nachrichtendiensten ausdrücklich die Möglichkeit eröffnet, Datenströme mithilfe der beteiligten Telekommunikationsunternehmen auszuleiten und zu manipulieren. Das ist einer der Wege, die der Kollege Bäcker eben gerade benannt hat. Dagegen bestehen grundsätzlich keine rechtlichen Bedenken, die betroffenen Unternehmen werden wie bei einer klassischen Telekommunikationsüberwachung lediglich verpflichtet, einen Datenstrom physisch umzuleiten und zur Nutzung dieses Datenstroms bestimmte Informationen zur Verfügung zu stellen. Die Unternehmen müssen also weder Überwachungsprogramme selbst aufspielen, noch müssen sie konkrete Kommunikationsinhalte ausleiten.

Fragen wirft der Gesetzentwurf auf, soweit es um den Zugriff auf gespeicherte Informationsinhalte geht. § 11 Absatz 1a des G10-Entwurfs 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 Übertragungsvorganges im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können“. Auf diese Weise soll jetzt ein technisches Problem gelöst werden: Bei Messenger-Diensten wie zum Beispiel WhatsApp ist, anders als bei der Sprach- und Videotelefonie in Echtzeit, der Übertragungsvorgang mit dem Zugang der Nachricht am Endgerät abgeschlossen. Das bedeutet – Herr Bäcker hat es gerade gesagt – dass keine laufende Kommunikation mehr vorliegt, die dem Schutz des Fernmeldegeheimnisses unterfallen würde. Soll die Nachricht dennoch ausgelesen werden, muss sie am Maßstab des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme gemessen werden. Nach Maßgabe des Bundesverfassungsgerichts kommen in diesem Fall Eingriffe aber nur in Betracht, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Das ist eine sehr, sehr hohe Eingriffsschwelle. Das Bundesverfassungsgericht hat aber in seiner Rechtsprechung bisher nicht den Fall vor Augen gehabt, das sich die Überwachung auf neu ankommende oder abgesetzte Messenger-Nachrichten auf einem Endgerät beschränkt – viel mehr ging es um das Auslesen eines gesamten IT-Systems. Im Fall der Telekommunikationsüberwachung, so wie sie hier geregelt ist, ist das nicht zu besorgen. In Bezug auf die gespeicherten Messenger-Daten erreicht der Eingriff nur die Intensität der klassischen Telekommunikationsüberwachung. Infolgedessen ist es wertungsmäßig zu vertreten, wenn an die Rechtfertigung des Eingriffs in dieses Grundrecht niedrigere Anforderungen gestellt werden. Näheres kann meiner Stellungnahme entnommen werden. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann Herr Professor Graulich.

SV **Prof. Dr. Kurt Graulich** (Richter a. D. am BVerwG, Berlin): Frau Vorsitzende, vielen Dank für die Gelegenheit, meine Stellungnahme mündlich zu erläutern.

Ich konzentriere mich wie die beiden Vorredner ebenfalls auf zwei Stellen des Entwurfs. Einmal den § 4 des Bundesverfassungsschutzgesetzes: Die Ausdehnung der Beobachtung auf Einzelpersonen ist ein fundamentaler Schritt. Ich habe auch lange gezögert, wie ich diesen Schritt vom Eingriffsgewicht her werten sollte, schließe mich aber dem Entwurf an. Die amerikanischen Verhältnisse – die ich hier nicht inhaltlich werte, weil das die Sache der amerikanischen Innenpolitik ist – aber die haben uns jedenfalls von der Dynamik her gezeigt, welche Wucht eine Einzelperson bei entsprechender Organisation mithilfe von Telemedien erzielen kann. Ich denke da gar nicht einmal an die Extremismusbestrebungen hier in Deutschland, sondern das ist eigentlich für mich das Beispiel – sodass man, glaube ich, nicht dabei stehenbleiben kann zu sagen, dass es immer kopfstarke Bewegungen sein müssen, die beträchtliche politische Auswirkungen haben können. Von daher meine ich, wenn man nicht im Telemedienrecht selbst Grenzen einzieht, bleibt einem eigentlich unter Verfassungsschutzgesichtspunkten nur das Bundesverfassungsschutzgesetz übrig. Und da halte ich den Weg, der jetzt im Entwurf vorgeschlagen wird, für gangbar.

Der zweite wichtige Punkt, da bin ich allerdings nicht auf der Seite des Entwurfes, betrifft die Quellen-TKÜ. Ich habe in meiner Stellungnahme der Kerze die Schelle umgehängt und habe gesagt: Wir reden hier gar nicht über Quellen-TKÜ, sondern das geht einen Schritt weiter, im Grunde genommen ist das eine Onlinerecherche kombiniert mit einer Festplattendurchsicht. Ich zitiere aus dem Entwurf in dem Satz zu § 11 Absatz 1a Satz 2: „Auf dem informationstechnischen System des Betroffenen ab dem Zeitpunkt der Anordnung gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden.“ – Der Kollege Bäcker hat das in derselben Weise gewertet und ich kann es auch nicht anders verstehen. Also wir haben es hier mit abgeschlossenen Sachverhalten zu tun, die Kommunikation läuft nicht mehr und die auf der Festplatte vorhandenen Informationen dürfen ausgelesen und übermittelt werden, also ausgeleitet werden. Das ist ein äußerst schwerer Eingriff. Ich vermisse sowohl, dass die dafür allenfalls erforderlichen Tatbestandsvoraussetzungen beschrieben werden – ich kann die Gefährlichkeitsgrade und dergleichen hier nicht sehen. Und zum anderen bin ich auch sehr verwundert: Dieses Mittel soll ja allen

deutschen Nachrichtendiensten zur Verfügung gestellt werden – ich vermisse unter Erforderlichkeitsgesichtspunkten, dass hier differenziert wird – also diese Nachrichtendienste befinden sich in einer jeweils unterschiedlichen Position, was ihre Aufgaben angeht und die jetzt aber undifferenziert mit demselben Mittel auszustatten, kann ich nicht nachvollziehen. Also diese Befugnis, die in das Gesetz aufgenommen werden soll, genügt den Verhältnismäßigkeitsanforderungen auf alle Fälle nicht! Dabei belasse ich es jetzt. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann Herr Haldenwang, bitte.

SV Präs. **Thomas Haldenwang** (BfV): Vielen Dank Frau Vorsitzende. Auch danke dafür, dass ich sozusagen als Bedarfsträger für diese Novelle hier das Wort ergreifen darf.

Vielleicht ein paar einordnende Worte zur Lage, in der wir uns gerade befinden in diesem laufenden Gesetzgebungsverfahren: Der Verfassungsschutzbericht 2020, den Minister Seehofer in Kürze vorstellen wird – und da verrate ich kein Geheimnis – einmal mehr aufzeigen, dass die Anhängerschaften in allen Extremismusbereichen weiter zunehmen. Wir sehen insbesondere einen deutlichen Anstieg im gewaltorientierten Extremismus, ebenfalls in allen Phänomenbereichen. Und besonders beunruhigend und bedrohlich ist, dass die Anzahl der Straf- und insbesondere Gewalttaten deutlich steigt, deutlich steigt. Sowohl insbesondere im Rechtsextremismus – die fürchterlichen Beispiele aus dem Jahre 2020 brauche ich Ihnen allen hier nicht noch einmal ins Gedächtnis rufen: Hanau, Halle nur als Stichworte. Wir sehen aber eben auch die sehr stark steigende Gewaltorientierung im Bereich des Linksextremismus mit Gewalttaten gegen den politischen Gegner, Gewalttaten gegen politisch nicht gewünschte Personen, Immobilienmakler beispielhaft, oder insbesondere natürlich ausufernde Gewalt gegen Polizeikräfte, wo man eben teilweise auch die Tötung von Personen billigend in Kauf nimmt. Und ganz aktuell sehen wir auch im Bereich des auslandsbezogenen Extremismus in Deutschland Gewaltaktivitäten auf Deutschlands Straßen – auch in einer Dimension, wie wir es eigentlich bisher selten hatten.

Gut, da kann man sagen, das ist eine Entwicklung, das geht mal rauf, das geht mal runter. Wir haben allerdings jetzt seit einigen Jahren eine kontinuierlich aufsteigende Kurve, aber es gibt so ein paar neue Elemente in diesem Lagebild, auf die dieses Gesetz letztlich auch reagiert. Was meine ich damit? Zunächst einmal sehen wir – ich bleibe einmal im Bereich des Rechtsextremismus, der aus meiner Sicht nach wie vor die größte Gefahr für unsere Sicherheit aber auch für unsere Demokratie darstellt. Wir sehen im Rechtsextremismus, dass wir es nicht mehr zu tun haben mit den bekannten Organisationen, wie Kameradschaften, Vereine, Parteien. Wir sehen eben zunehmend, dass sich Einzelpersonen radikalisieren. Da denke ich an die Täter von Hanau und Halle – Einzelpersonen, aber im Netz radikalisiert. Einzeltäter im strafrechtlichen Sinne, aber im Netz irgendwie mit anderen verbunden, aber keiner Organisation angehörig. Einzelne Personen sind das, die dann auf einmal – und das geht sehr schnell, sehr schnelle Radikalisierung – eben von ihrer gewaltorientierten Idee auch zur Tat schreiten und dann tätig werden, ohne dass da irgendeine Organisation dahintersteht. Das ist ein Phänomen.

Das andere Phänomen, dass wir zunehmend eben auch im Internet Chatgruppen wahrnehmen, die sich auch verabreden, Gewalt zu begehen, die sich auch verabreden, möglicherweise an einem Tag X hier die Macht in diesem Staate – so stellen sie sich das jedenfalls vor – zu übernehmen. Und da müssen wir leider auch feststellen, dass solchen Chatgruppen auch immer wieder Bundeswehrangehörige oder Polizeibeamte angehören. Oft sind das sogar Gruppen, die haben ihren Ursprung in bestimmten Kreisen, auch der Bundeswehr – das Ganze wird ja aktuell sehr stark diskutiert. Und wenn wir uns dann anschauen, wie läuft so etwas, diese Radikalisierung, diese Chatgruppenbildung, dann sieht man eben auch die besondere Bedeutung des Internets und die besonderen neuen Formen der Kommunikation. Das alles spielt sich natürlich auch noch irgendwo in der realen Welt ab, aber das Internet und die neuen Kommunikationsformen spielen eine ganz wesentliche Rolle. Man radikalisiert sich, man tauscht die Ideen aus, man kommt dann aber auch über die verschiedensten Plattformen zueinander, trifft sich und dann werden eben auch aus ersten Überlegungen auch Vorbereitungshandlungen für spätere Gewalttaten. Das alles spielt sich im Netz ab und zwar nicht mithilfe analoger Kommunikation, sondern wir haben es immer häufiger mit der

Nutzung von Telemediendiensten zu tun, internetbasiert, OTT-Services, die inzwischen von 90% der Bundesbürger, genutzt werden. Und dabei handelt es sich um Kommunikation, die verschlüsselt ist und eben jeder Telekommunikationsüberwachung durch Verfassungsschutzbehörden nach dem gegenwärtigen Zustand eben nicht zur Verfügung steht. Das sind Entwicklungen, auf die wir reagieren müssen.

Und insofern bin ich froh, dass jetzt mit dem Gesetz auf einige dieser Punkte eingegangen wird. Ich nehme nur drei Dinge raus. Erstens: Der personenbezogene Aufklärungsansatz wird gestärkt, um die Radikalisierungsverläufe von Einzelpersonen noch vor der Hinwendung zur Gewalt erkennen zu können. Möglicherweise hätte es gelingen können, Täter wie in Hanau und Halle schon frühzeitiger zu entdecken, wenn man die Möglichkeit gehabt hätte, ihr Kommunikationsverhalten wahrzunehmen. Insofern müssen wir einfach in einem frühen Stadium angreifen, die Personen identifizieren, die unsere demokratische Grundordnung bedrohen, auch wenn die Gewaltbezüge noch nicht unmittelbar zutage treten. Insofern halte ich das für einen wichtigen Punkt.

Ein weiterer wichtiger Punkt in dem Gesetz: Die Anbindung des Bundesamtes für den Militärischen Abschirmdienst (BAMAD) an unser Nachrichtendienstliches Informationssystem (NADIS). Es ist bisher nicht der Fall, dass sich das BAMAD auch schreibend einbringen kann. Gerade die Situation, dass wir im Rechtsextremismus immer wieder Personen aus dem Bereich der Bundeswehr wahrnehmen und Polizisten, zeigt, dass der Austausch zwischen BAMAD und den Verfassungsschutzbehörden mit ihren verschiedenen Zuständigkeiten eng verzahnt werden muss. Das geschieht schon in diversen Arbeitsgruppen, aber dazu bedarf es auch eines technischen Instrumentariums. Und das ist eben die Anbindung an NADIS, sodass auch beim Übergang – Soldat geht ins Zivilleben – Zivilist wird Soldat – keine Informationen verloren gehen. Insofern wichtiger zweiter Aspekt.

Und der dritte Aspekt ist hier angesprochen worden und auch kritisch, das ist das Thema Quellen-TKÜ: Ich habe es angesprochen, 90% der Bundesbürger kommunizieren über diese Telemediendienste, über WhatsApp, Telegram, Instagram und Facebook. Und all das ist eben für die Dienste nicht einsehbar. Uns geht es also hier nicht um eine Erweiterung der Befugnisse, eine Erneuerung von Befugnissen, sondern wir wollen mit den Möglichkeiten, die wir haben, in der heutigen Welt ankommen und die Kommunikationsformen, die heute gebräuchlich sind, auch erreichen können. Und dazu soll der Weg gegangen werden, dass ein Endgerät vor oder dann eben nach Verschlüsselung technisch so ausgestattet wird, dass man die nicht verschlüsselte Kommunikation nachvollziehen kann. Das ist der einzige Weg, wie wir an die Daten kommen. Ich möchte an der Stelle schon direkt sagen: Dabei spielt die Ausnutzung von irgendwelchen Zero Day Exploits überhaupt keine Rolle – die Technik funktioniert anders. Die Technik kann ich Ihnen hier nicht darstellen, weil dann wüsste unser Gegner genau Bescheid, was zu tun ist. Aber es geht jedenfalls nicht um die Ausnutzung von Lücken, die bereits bisher in Internetsystemen vorhanden sind.

Vielleicht noch ein Wort: Mir ist bewusst, dass man natürlich mit so einem Eingriff in die Telemediendienste mit der Quellen-TKÜ auch sehr tief in die Freiheitsrechte der Bürger eingreift – auf jeden Fall. Und deshalb halte ich es auch für sehr sachgerecht, notwendig und richtig, dass im gleichen Atemzug die Kontrolle entsprechend ausgeweitet wird. Und ich begrüße auch die Stärkung der G10-Kommission sehr, die im Gesetz vorgesehen ist. Keine dieser Maßnahmen kann durchgeführt werden – insofern reden wir hier auch nicht von Massenüberwachung, wie es gelegentlich suggeriert wird – keine dieser Maßnahmen kann ergriffen werden, ohne dass nicht der jeweilige Einzelfall durch die Kommission durchgeleitet worden ist und dort unter allen Gesichtspunkten geprüft worden ist. Und insofern ist es richtig, die Kommission zu stärken, sodass sie diese Aufgabe noch besser wahrnehmen kann. Das stärkt dann aber auch das Vertrauen der Bürgerinnen und Bürger in die ordnungsgemäße Durchführung der Maßnahmen.

Insgesamt kann ich nur sagen, das Gesetz ist ein wichtiger Schritt zur Stärkung des Bundesamtes für Verfassungsschutz, der deutschen Nachrichtendienste und zwar einzig und allein, um den Schutz der Bürgerinnen und Bürger, um den Schutz der freiheitlich-demokratischen Grundordnung in unserem Land eben auch weiter effektiv durchführen zu können. Ich danke Ihnen.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Haldenwang, vielen Dank. Dann Herr Professor Poscher.

SV **Prof. Dr. Ralf Poscher** (Max-Planck-Institut, Freiburg): Sehr geehrte Frau Vorsitzende Lindholz, sehr geehrte Damen und Herren, auch ich möchte mich erst einmal bedanken, dass ich meine schriftliche Stellungnahme hier erläutern kann.

Ich möchte die Erläuterung für drei Punkte nutzen, die alle die Neuregelung der Quellen-TKÜ betreffen. Da scheint mir zunächst ganz unpassend, dass eine qualitativ neue Überwachungsbefugnis in eine Norm implantiert wird, die ausweislich der amtlichen Überschrift des Abschnittes und auch des sonstigen Inhaltes der Vorschrift ausschließlich dem Verfahren gilt. Der Gesetzesentwurf tut also so, als handele es sich bei der Einführung der erweiterten Quellen-TKÜ lediglich um eine Verfahrensregelung, obwohl es sich um einen besonders intensiven, nicht nur das Fernmeldegeheimnis betreffenden und für das G10-Gesetz neuen und neuartigen Grundrechtseingriff handelt. Gerade, soweit die erweiterte Quellen-TKÜ nicht nur Artikel 10 betrifft, handelt es sich bei der neuen Befugnis im gewissen Sinne sogar um einen Fremdkörper in dem Gesetz, das bereits seinem Namen nach lediglich der Beschränkung des Brief-, Post- und Fernmeldegeheimnisses dienen soll. Nun hindert den Gesetzgeber nichts daran, neuartige Maßnahmen auch in das G10-Gesetz einzuführen. Doch sollte auch in der Abfassung des Gesetzes nicht der falsche Eindruck erweckt werden, es handele sich bei der Gesetzesänderung lediglich um eine Verfahrensvorschrift. Vielmehr sollte die neue und neuartige Befugnis dem Gesetzgeber schon eine eigenständige, materiell-rechtliche Befugnisnorm wert sein.

Das leitet dann auch zu dem zweiten Punkt über: Dass die neuartige Befugnis nicht in ihrer Eigenständigkeit ernst genommen wird, rächt sich dann auch – das haben ja auch die vorherigen Äußerungen schon gezeigt – in der Ausgestaltung der Regelung. Es scheint fast so, als sei der Gesetzgeber durch seine Regelungstechnik selbst in die Irre geführt worden und habe deshalb den besonderen verfassungsrechtlichen Anforderungen an die neuartige Maßnahme nicht ausreichend Rechnung getragen. Bei der erweiterten Quellen-TKÜ handelt es sich um eine Mischform einer Überwachung der laufenden Kommunikation und der ruhenden Kommunikation mithilfe einer Manipulation des Zielsystems. Von einem solch janusköpfigen Eingriff sind zwei unterschiedliche Grundrechte betroffen – auch das wurde schon hervorgehoben. Nämlich zum einen das Fernmeldegeheimnis in Artikel 10 und zum anderen das Recht auf die Integrität des Informationssystems aus dem Allgemeinen Persönlichkeitsrecht, da eben nicht nur die laufende, sondern eben auch die gespeicherte Kommunikation erfasst werden soll.

Da muss ich Bedenken äußern gegen die Regelung aus drei Gesichtspunkten. Zum einen lässt das Gesetz für mich nicht genau erkennen, inwieweit die gespeicherten Kommunikationsinhalte erfasst werden können. Die zeitliche Grenze ist hier unklar, da sie sich zwar einerseits auf den Zeitpunkt der Anordnung bezieht, aber unklar bleibt, ob damit auch Kommunikationsstränge und Historien erfasst werden können, die im Anordnungszeitraum vielleicht mit kommuniziert wurden aber weit hinter den Anordnungszeitpunkt zurückreichen. Insoweit bedarf es einer Klarstellung, da sich sonst die Intensität des Eingriffs kaum abschätzen lässt.

Zum anderen gelten jedenfalls für den Eingriff in das IT-Grundrecht besonders hohe Eingriffsschwellen, die das Gesetz nicht berücksichtigt, weil es so tut, als handele es sich bei der erweiterten Quellen-TKÜ lediglich um eine auch bisher schon geregelte Überwachungsmaßnahme. Dem gegenüber müsste der Katalog der Straftaten, jedenfalls für die nun eingeführte Mischform des Eingriffs angepasst werden. Das Verteilen von Flugblättern verbotener Vereine etwa erfüllt noch nicht die Anforderungen, die das Bundesverfassungsgericht für Eingriffe in das IT-Grundrecht hinsichtlich des Rechtsgüterschutzes gestellt hat.

Und schließlich erstreckt sich der Ausschluss des Rechtsschutzes in § 13 G10-G nun auch auf den Eingriff in das IT-Grundrecht. Beim Fernmeldegeheimnis sieht das Grundgesetz in Absatz 2 von Artikel 10 ausdrücklich eine Beschränkung des Rechtsschutzes vor. Hinsichtlich des IT-Grundrechts fehlt es aber an einer solchen verfassungsrechtlichen Grundlage und darin scheint mir doch eine recht eindeutige Verletzung der Rechtschutzgarantie zu liegen.

Lassen Sie mich schließen mit einer eher rechtspolitischen Überlegung: Sie betrifft dieses

Spannungsfeld, das hier ja jetzt auch schon thematisiert worden ist, von IT-Sicherheit und Verfassungsschutz. Hier ist es für den Gesetzgeber sicherlich nicht leicht zu navigieren. Denn einerseits hat er die Aufgabe des Verfassungsschutzes und andererseits ist der Staat grundsätzlich verpflichtet, zur Sicherheit der IT-Infrastruktur beizutragen oder sie jedenfalls nicht zu beeinträchtigen. Und auch wenn der Staat bei der Austarierung dieser beiden Aufgaben einen großen Gestaltungsspielraum hat, ist fraglich, ob der Nutzen einer mit einer Onlinedurchsuchung verknüpften Quellentelekommunikationsüberwachung für den Verfassungsschutz die damit verbundenen Risiken überwiegt. Aktuelle Zahlen zeigen, dass die Ermächtigungsgrundlage für die Quellen-TKÜ und die Onlinedurchsuchung nur äußerst selten genutzt werden. So hat etwa das BKA im Zeitraum von 2018 bis 2019 keine Onlinedurchsuchungen durchgeführt. Der Gesetzgeber sollte sich jedenfalls sehr gut überlegen, ob er Instrumente, die ganz wesentlich auch auf dem Verheimlichen von Sicherheitslücken beruhen können, die Millionen von Informationssystemen in allen Bereichen gefährden, weiter ausdehnt. Jedenfalls sollte er zuvor eine belastbare Kosten-Nutzen-Analyse vornehmen, die nicht nur den tatsächlichen Nutzen des Instrumentes, sondern auch seine Bedeutung für die Aufgabenerfüllung überprüft. Oder – wie Herr Haldenwang nun nahegelegt hat – die Ausnutzung und Aufrechterhaltung von Sicherheitslücken für die Quellen-TKÜ ausdrücklich im Gesetz ausschließen. Für Vorrats- oder gar symbolische Gesetzgebung eignen sich weder die Quellen-TKÜ noch die Onlinedurchsuchung. Haben Sie vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Und den Schluss in der Runde macht noch Herr Dr. Rusteberg.

SV **Dr. Benjamin Rusteberg** (Georg-August-Universität, Göttingen): Frau Vorsitzende, meine sehr geehrten Damen und Herren, vielen Dank.

Ich möchte zunächst einmal ganz kurz die Ergebnisse meiner schriftlichen Stellungnahme zusammenfassen: Meines Erachtens vertieft der vorliegende Gesetzesentwurf die Rolle des Verfassungsschutzes als besondere Gefahrenabwehrbehörde, womit nicht nur das Trennungsgebot und eine sich daraus ergebende mögliche Eingriffsprivilegierung der Verfassungsschutzbehörden zusätzlich in Frage gestellt werden, sondern angesichts der Kompetenzüberschneidung mit der Polizei auch die Existenz der Verfassungsschutzbehörden selbst.

Auch vor diesem Hintergrund ist die Erweiterung des Einbezuges der Beobachtung von Einzelpersonen durch den § 4 des vorliegenden Entwurfes für das Bundesverfassungsschutzgesetz abzulehnen. Sie ist gerade angesichts der in der Entwurfsbegründung genannten Beispiele auch schon nicht erforderlich. Wenn hier gerade eben die schrecklichen Taten von Hanau und Halle angeführt werden, dann wären diese ja ohne weiteres unter die bisherige Regelung zu subsumieren gewesen. Insofern finde ich es eher irritierend, wenn das jetzt herangezogen wird, um diese Änderung zu rechtfertigen.

Die Regelung zur Quellen-TKÜ allgemein partizipiert – haben wir ja auch schon gehört – an den bekannten Mängeln des Anforderungskataloges in § 3 Absatz 1 G10-G und leidet auch nach wie vor am völligen Fehlen verfahrensrechtlicher Regelungen, wie denn eine solche Begrenzung der Überwachung technisch und rechtlich sichergestellt werden kann. Also hier bleibt der Gesetzentwurf auf dem Stand der bisherigen Überlegungen völlig stehen.

Im Übrigen, was den zusätzlichen Eingriff angeht – um da keine Falschinformation hier stehen zu lassen: Natürlich kann man auch bei Messenger-Diensten die laufende Kommunikation überwachen und abgreifen. Man muss dann in dem Moment, in dem die Informationen gesendet und übermittelt werden, zugreifen.

Wie wir jetzt auch mehrfach schon gehört haben, greift die zusätzliche Regelung der nachträglichen Onlinedurchsuchung in die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ein, ohne dabei an die damit korrespondierenden Voraussetzungen gebunden zu werden und ist somit offensichtlich als verfassungswidrig einzuschätzen.

Was bisher noch nicht angesprochen wurde – ich halte sie ebenfalls für bedenklich – ist die Regelung des § 11 Absatz 1b G10-G, die wesentliche verfahrensrechtliche Vorkehrungen für weitere Telekommunikationsanschlüsse aufhebt und damit

letztlich, wenn einmal eine Anordnung zur Telekommunikationsüberwachung für eine Person ergangen ist, mehr oder weniger eine Rundumüberwachung ermöglicht, ohne dass die G10-Kommission vorab eingreifen kann. Insofern, denke ich, ist das auch eine unverhältnismäßige Regelung, zumal mir im Bereich der Nachrichtendienste auch nach wie vor nicht ersichtlich ist, in welchen Eilfällen sie eigentlich zu tun haben, weil deren Aufgrabe doch eigentlich in der Langfrist- und Strukturüberwachung zu sehen ist.

Und schließlich – was die verschiedenen Möglichkeiten hier angeht, eben solch eine Überwachung der verschiedenen Systemgeräte zu ermöglichen – sieht § 2 Absatz 1a, 1b G10-Entwurf hier weitreichende Mitwirkungspflichten beziehungsweise Duldungspflichten der Diensteanbieter vor, die aus meiner Sicht für die Nachrichtendienste ein ganz erhebliches Missbrauchspotential bergen. Zentral ist dieser Punkt, dass nicht mehr länger nur einfach Kopien der Datenströme ausgeleitet werden, die dann überwacht und gelesen werden können, sondern dass hier gezielt eine Manipulation eben dieser Daten durch die Dienste ermöglicht werden soll. Das heißt, es kann im Prinzip jedem alles auf den Rechner gespielt werden. Also das ist rechtlich nicht zulässig, aber faktisch hiernach ohne weiteres möglich. Und das verstößt meines Erachtens gegen die objektive Dimension des Rechtes auf informationelle Selbstbestimmung.

Ich möchte noch ganz kurz darauf eingehen, einfach um noch einmal ein bisschen den Blick zu weiten – wo stehen wir eigentlich mit diesem Gesetzesentwurf? Also wir stehen jetzt etwa zwanzig Jahre – relativ genau – nach dem im Nachgang zum 11. September eine neue Generation von Sicherheitsgesetzen eingeführt und damit begonnen wurde, eben auch die Befugnisse der Nachrichtendienste ganz erheblich auszuweiten. Und wenn man sich einmal anschaut, was da am Anfang noch zumindest von Seiten des Gesetzgebers vorgesehen war – so etwas wie Befristungen und Evaluationen der Gesetze – dann muss man sagen, hat doch der Gesetzgeber zumindest zum Ausdruck gebracht, was immer auch da hinterher geworden ist, dass hier eine gewisse Gefährdungslage besteht, dass hier Neuland betreten wird und eine gewisse Reflexion notwendig ist. Und mittlerweile sind eben diese Instrumente – haben sich erübrigt, also sie sind sang- und klanglos verabschiedet worden. Und stattdessen stehen wir an einem Punkt, wo eine Regelung übernommen wird aus dem § 100a StPO, die in der Fachwelt ganz einhellig als verfassungswidrig angesehen wird. Also wenn Sie einmal in die Stellungnahmen der strafprozessualen Schrifttums schauen – ich habe da nichts gefunden, was nicht davon ausgehen würde, dass diese Art der erweiterten Quellen-TKÜ dass die nicht als verfassungswidrig anzusehen wäre. Und trotzdem wird hier einfach das übernommen. Es wird im Gesetz, auch im Entwurf, kein Wort dazu verloren, es werden keinerlei Regelungsanstalten gemacht, das irgendwie einzugrenzen, auch auf verfahrensmäßiger Ebene. Also die goldene Brücke, die das Verfassungsgericht hier dem Gesetzgeber eigentlich einmal für die Quellen-TKÜ gebaut hat, durch diese Schutzbereichsausnahme, die wird links liegen gelassen und stattdessen wird hier sehenden Auges in die Verfassungswidrigkeit spaziert.

Zuletzt bleibt natürlich immer der Einwand: Wenn es dem Verfassungsschutz in den letzten zwanzig Jahren an einem, glaube ich, nicht gefehlt hat, dann sind es die Fähigkeiten und Befugnisse zur Informationserhebung gewesen, sondern die Fähigkeiten diese Informationen auszuwerten, daraus die richtigen Schlüsse zu ziehen und verantwortungsvoll mit diesen Informationen umzugehen. Und wenn ich mir anschaue, dass einer Behörde, die in den letzten Jahren von einer Person geleitet wurde, die keinerlei Gewähr dafür geboten hat, jederzeit für die freiheitlich-demokratische Grundordnung einzustehen, hier solche weitergehenden Möglichkeiten einfach zum Missbrauch dieser Befugnisse eingeräumt bekommt, dann kann ich mich nur fragen, ob das eigentlich der Schritt ist, den wir im Moment aus rechtlicher Sicht gehen sollten. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Allerdings muss ich sagen, Herr Dr. Rusteberg, die letzte Bemerkung hätten Sie sich sparen können – als Sachverständiger zu Besetzungen des Bundesamtes für Verfassungsschutz Stellung zu nehmen oder einfach eine Behauptung in den Raum zu stellen, obwohl die betreffende Person hier nicht anwesend ist und dazu keine Stellung beziehen kann. Wir wissen alle, von wem Sie gesprochen haben und diese Person ist nicht hier und kann auch dazu keine Stellung beziehen. Das ist auch

nicht Gegenstand unserer heutigen Anhörung, um das ganz klar zu sagen. Jetzt steigen wir ein in die Fragerunde.

SV **Dr. Benjamin Rusteberg** (Georg-August-Universität, Göttingen): Ich glaube nicht, dass ich mir hier reinreden lassen muss, zu dem, was ich hier vortrage.

Vors. **Andrea Lindholz** (CDU/CSU): Ich habe als Vorsitzende sehr wohl die Möglichkeit, meine Meinung kundzutun, was Thema einer Anhörung ist und was nicht. Herr Throm, in die Fragerunde steigt die Union ein? Mit Herrn Brand.

BE Abg. **Michael Brand** (CDU/CSU): Ganz herzlichen Dank. Ich hoffe, ich bin zu verstehen und sage ein herzliches Dankeschön für die Unionsfraktion den Sachverständigen.

Ich habe eine Frage an Herrn Haldenwang und Herrn Professor Dietrich. Mit Herrn Haldenwang beginnend, will ich sagen, dass ich und die Union die geplante Stärkung des personenbezogenen Aufklärungsansatzes hier im Gesetzentwurf für sehr wichtig halten. Im Übrigen finde ich, sollten wir nicht allein Hanau und Halle erwähnen, sondern auch die Zäsur in der Geschichte unseres Landes mit dem Mord an Walter Lübcke – denn dort hat der Verfassungsschutz in den vergangenen Jahren ja auch den späteren Täter eingeschätzt als jemanden, der sozusagen erkaltet ist, was sich als falsche Schlussfolgerung herausgestellt hat. Es gibt hier sicherlich auch noch andere im Umfeld, aber ich denke, wir sollten neben Hanau und Halle und anderen Mordtaten auch diese nicht unter den Tisch fallen lassen.

Ich will zu dem Thema Quellen-TKÜ – das passt zu der letzten Stellungnahme, glaube ich, ganz gut – zur Konkretisierung des Bedarfes für die neue Quellen-TKÜ – Herrn Haldenwang fragen: Die Gesetzesbegründung bezieht sich ja auf die Messenger-Dienste und insofern wäre es aus meiner Sicht hier noch notwendig, Herr Haldenwang, dass Sie uns noch einmal etwas mit auf den Weg geben zur Notwendigkeit der Quellen-TKÜ. Welche Bedeutung die Messenger-Dienste bei der Kommunikation von nach G10-zulässigen Zielpersonen der TKÜ hat und inwieweit die herkömmlichen nachrichtendienstlichen Mittel nicht ausreichend zur Aufklärung sind.

Die zweite Frage, die ich stellen möchte, richtet sich an Herrn Professor Dietrich. Sie bezieht sich auch auf eine Stellungnahme von journalistischen Verbänden und Institutionen, die davon sprechen, dass im Referentenentwurf und auch jetzt im Gesetzesentwurf vorgesehene Regelungen zur Quellen-TKÜ die Einschnitte in den journalistischen Quellenschutz weiter vertiefen und dass es Abgrenzungsschwierigkeiten zur Onlinedurchsuchung geben würde. Und hier möchte ich Sie gern fragen, wie Sie das einschätzen. Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann kommen wir zu Herrn Dr. Wirth.

BE Abg. **Dr. Christian Wirth** (AfD): Vielen Dank, Frau Vorsitzende. Danke an die Sachverständigen.

Ich hätte eine Frage jeweils an Herrn Professor Bäcker und Herrn Professor Dietrich und zwar sind die verlockenden und eigentlich auch wünschenswerten Erweiterungen auf Einzelpersonen meines Erachtens nicht ganz unproblematisch. Ich hätte dahingehend eine Frage, inwieweit es da eine Vermischung zwischen Verfassungsschutzaufgabe und Polizeiaufgaben geben könnte – gerade unter Einbeziehung des Militärischen Abschirmdienstes – um Ressortprobleme zwischen Bundes- und Länderkompetenzen zu vermeiden. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann kommen wir zu Herrn Grötsch.

BE Abg. **Uli Grötsch** (SPD): Vielen Dank, Frau Vorsitzende.

Herr Professor Dr. Graulich, Sie kritisieren in Ihrer Stellungnahme den Umstand, dass die erweiterte Quellen-TKÜ für alle Dienste vorgesehen wird, als unverhältnismäßig oder gar verfassungswidrig. Jetzt haben wir hier in den Stellungnahmen der Sachverständigen sehr deutliche und unmissverständliche Worte gehört, was die erweiterte Quellen-TKÜ angeht. Ich würde Sie fragen wollen, Herr Graulich, können Sie uns Ihre Kritik konkreter erläutern, die Sie in Ihrer Stellungnahme dahingehend üben – also was die erweiterte Quellen-TKÜ für alle Dienste angeht. Und wie hätte Ihrer Meinung nach die Regelung ausgestaltet werden können, sodass sie aus Ihrer Sicht verfassungskonform wird?

Und dann noch eine weitere Frage: Wir haben im Koalitionsvertrag vereinbart, dass jede Befugniserweiterung auch mit mehr Kontrolle einhergehen muss. Im vorliegenden Gesetzentwurf haben wir hierzu einige Verbesserungen bezüglich der G10-Kommission gemacht. Aus verfassungsrechtlicher Sicht und gemessen an der Tiefe der Grundrechtseingriffe bei der erweiterten Quellen-TKÜ – ist das aus Ihrer Sicht ausreichend, was wir hier im Gesetzentwurf machen? Oder was würden Sie vorschlagen, wie wir noch effektiver in diesem Bereich, in der Kontrolle werden könnten? Danke.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Strasser, bitte.

BE Abg. **Benjamin Strasser** (FDP): Vielen Dank, Frau Vorsitzende.

Ich glaube, es ist zunächst einmal wichtig, in der Debatte hier zu betonen, dass es allen im Raum darum geht, dass natürlich Sicherheitsbehörden auch bei Gefährdern und Terroristen Kommunikation mitlesen können. Es geht gar nicht um die Frage des „Ob?“, sondern um die Frage des „Wie?“ und des konkreten Vorschlages hier der Bundesregierung. Und unter dieser Überschrift hätte ich eine Frage an Professor Dr. Bäcker und eine an Präsident Haldenwang.

Meine erste Frage an Professor Dr. Bäcker: Wenn man jetzt einmal schaut, wie die Reaktion derjenigen ist, die diese Maßnahmen umsetzen sollen, nämlich der Unternehmen, dann trifft das auf einhellige Ablehnung. Der Verband eco hat eine Stellungnahme eingereicht, in der „eine Vielzahl an rechtlichen und prozessualen Fragen im Zusammenhang mit der Umleitung von Datenströmen nach § 2 Absatz 1 Satz 1 Nummer 4 des G10-Gesetzesentwurfes“ bemängelt – unter anderem wolle man mit der Regelung „sowohl die inhaltliche Veränderung von Daten als auch ein Hinzufügen oder Unterdrücken von Daten ermöglichen.“ Und deswegen fordert dieser Verband eine Veränderung von Kommunikation auszuschließen und stellt die Frage, ob derartige Eingriffe überhaupt durch die Beschränkungsmöglichkeit des Art. 10 GG gedeckt sind. Und da würde mich Ihre rechtliche Einschätzung interessieren, ob sie diese Analyse teilen oder ob Sie gegebenenfalls eine andere Auffassung haben?

Und die zweite Frage geht an Präsident Haldenwang. Herr Haldenwang, Sie hatten in Ihrem Eingangsstatement die Anschläge von Halle und Hanau als Beispiel genommen und ich weiß nicht, ob das wirklich die richtigen Beispiele sind, weil sie ja vor diesen Anschlägen gar keine Namen hatten. Und eine Quellen-TKÜ bei Attentätern, die vor dem Attentat den Sicherheitsbehörden gar nicht bekannt sind, ist ein bisschen – finde ich ein schwieriges Beispiel. Aber die entscheidende Frage ist doch, ob Ihre Einschätzungen, so hatte ich Sie immer verstanden, dass Sicherheitsbehörden, insbesondere der Verfassungsschutz, bei verschlüsselten Messenger-Diensten blind und taub seien, ob die wirklich so stimmt. Vor kurzem wurde eine interne BKA-Stellungnahme im Volltext veröffentlicht beim WDR und beim Bayerischen Rundfunk und da steht zu lesen – vom BKA selbst – und ich möchte ganz kurz daraus zitieren: „Das BKA verfügt über eine Methode, die es ermöglichen kann, Text-, Video-, Bild- und Sprachnachrichten aus einem WhatsApp-Konto in Echtzeit nachzuvollziehen.“ Neben der genannten Kommunikation könnten darüber hinaus die WhatsApp-Kontakte der Zielperson bekannt gemacht werden. Und weiter: „Im Zusammenhang mit der Erhebung der Kommunikation erfolgt BKA-seitig eine Anmeldung mittels WhatsApp-Web unter Zuhilfenahme des Telefons der Zielperson. Der gesamte Vorgang erfolgt durch Verwendung regulär nutzbarer Funktionen der WhatsApp-Software.“ Und genau das ist ja beispielsweise bei Anis Amri passiert, wo Polizeibehörden Zugriff auf Telegram-Chats von Amri genommen haben und nicht durch ausländische Nachrichtendienste, sondern polizeiseitig Zugriff genommen haben. Und meine schlichte Frage ist, ob der Verfassungsschutz das, was das BKA offensichtlich seit Jahren tut, nicht selbst machen kann und falls ja, warum? Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann haben wir Frau Renner.

Abg. **Martina Renner** (DIE LINKE.): Danke Frau Vorsitzende. Ich möchte gern zwei Fragen an Herrn Rusteberg richten, aber vorab sei eine Bemerkung erlaubt: Ich habe seine zuletzt ausgeführten Hinweise durchaus nicht nur als zulässig sondern auch als notwendig erachtet – es geht ja hier auch darum, in wessen Hände wir welche Befugnisse geben und da gibt es Erfahrungen, die wir ja im Innenausschuss teilen, dass dies wenigstens kritisch mit der Personalie des ehemaligen

Präsidenten des BfV verbunden ist. Herr Maaßen ist ja hier nicht als Privatperson adressiert…

Vors. **Andrea Lindholz** (CDU/CSU): Frau Renner, es geht um die Aussage, er wäre kein Vertreter der freiheitlich-demokratischen Grundordnung. Und das geht nicht. Das weise ich mit aller Entschiedenheit zurück und das hat hier nichts zu suchen!

Abg. **Martina Renner** (DIE LINKE.): …wenn man weiß, wo er sich mittlerweile rumtreibt – also da machen wir uns, glaube ich, nichts vor, wenn wir sagen: Es steht außerhalb dieser Rechtsordnung.

Und dann würde ich gern die zwei Fragen formulieren. Das Eine: Es gibt ja da erhebliche Abgrenzungsschwierigkeiten zwischen Quellen-TKÜ und Onlinedurchsuchung – die Grenzen sind fließend. Wenn man jetzt so einen Trojaner unbemerkt installiert, glaube ich, ist es technisch kein Problem, auch auf die gespeicherte Kommunikation zuzugreifen, was aber nach den Vorgaben des Bundesverfassungsgerichtes nicht zulässig ist. Wie kann denn überhaupt sichergestellt werden, dass nur die laufende Kommunikation überwacht wird? Also was müsste rechtlich und materiell passieren, um das sicherzustellen? Oder um es einmal ein bisschen zuzuspitzen: Ist das überhaupt möglich, auszuschließen, dass nicht auch auf die ruhende Kommunikation dann zugegriffen wird?

Und die zweite Frage bezieht sich auf die Pflichtenausweitung der TK-Provider. Die werden ja nun dazu gebracht, bei der Infiltration technisch mitzuwirken. Da würde mich die rechtliche Dimension interessieren, Herr Rusteberg: Wie sieht es aus mit den Grundrechten der Anbieter von Telekommunikationsdiensten? Also wenn sie vom passiven Akteur quasi zum aktiven Gehilfen werden. Und ist es nicht auch möglich, das ist mehr eine technische Beurteilung, dass dann bei dieser Mitwirkung gegebenenfalls nicht nur Endgeräte infiltriert werden, sondern ganze Server oder Betriebssysteme? Dankeschön.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Dr. von Notz noch.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Ich möchte auch vorwegschicken, dass die Bedeutung der Gesetzesverfahren, die wir hier besprechen, für die innere Sicherheit und ihre Platzierung im Laufe der Legislatur einer harten Diskrepanz ausgesetzt sind. Wenn das so wichtig ist, was wir hier machen, dann muss man wirklich fragen, warum man hier in der drittletzten Sitzungswoche der 19. Wahlperiode sitzt und wieder im Schweinsgalopp so grundrechtlich sensible Fragen durchpushen muss. Ich verstehe es nicht. Ich verstehe es nicht! Ja, es hat Konflikte gegeben, das gehört wohl zu Koalitionen dazu, habe ich gehört. Aber wenn man das so sagt, „die innere Sicherheit“ und „so wichtig“ und „gerade der Antisemitismus“ und so weiter – warum muss das jetzt im Schweinsgalopp passieren? Das wird der Sache nicht gerecht!

Ich hätte eine Frage an Herrn Professor Poscher. Erst einmal vielen Dank für Ihre Stellungnahme, insgesamt danke ich allen Sachverständigen sehr für die interessanten und guten Ausführungen, die uns, glaube ich, weiterhelfen. Interessant wird es sein, ob all die guten Hinweise Berücksichtigung finden – da haben wir auch traurige Erfahrungen gesammelt die letzten Monate. Aber Herr Professor Poscher, vielleicht können Sie noch einmal genau ausführen, wo bei der Überprüfung der verfassungsrechtlichen Tragfähigkeit der hier in Rede stehenden Normen in Karlsruhe das Problem liegen kann, wenn es zu einer Überprüfung kommt, wovon ich fest ausgehe.

Meine zweite Frage geht an den geschätzten Präsidenten des Bundesamtes für Verfassungsschutz, Herrn Haldenwang: Wenn hier schon alle Leute meinen, Personalien thematisieren zu müssen, dann muss man ja auch sagen, das Argument auf die Vergangenheit bezogen ist dann in der Gegenwart wenig tragfähig. Trotzdem teile ich grundsätzlich die Grundhaltung zu sagen, die Gesetze, die wir machen, müssen auf lange Perspektive gedacht werden – das finde ich auch richtig. Aber Herr Haldenwang, vielleicht können Sie einmal sagen, weil es mich interessiert, aus Ihrer nachrichtendienstlichen Perspektive: Wir geben jetzt hier ein Instrument, das schon bei der Polizei massiv in der Kritik steht, geben wir jetzt den Nachrichtendiensten. Ebnen wir nicht auch damit immer weiter die Trennungslogik zwischen Nachrichtendiensten und Polizei ein? Alles irgendwie gefährlich und Gefahrenabwehr, eigentlich machen wir dem Bundesamt für Verfassungsschutz einen Vorwurf, wenn das in Halle passiert, oder ist nicht doch die Polizei zuständig? Aber beide hätten sie die Messenger doch lesen müssen und so. Also verunklart nicht diese Instrumentenverteilung –

und gerade die Verteilung von umstrittenen Instrumenten – die klare Aufteilung zwischen Nachrichtendiensten und Polizeien, die wir eigentlich verfassungsrechtlich bräuchten? Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Zum Schluss hätte ich auch noch zwei Fragen. Der Gesetzentwurf liegt ja schon seit letztem Jahr im Oktober vor. Es ist auch kein Geheimnis, dass es insbesondere an dem Punkt der Quellen-TKÜ hängt – insofern sei die Frage des „Schweinsgalopps“ einmal dahingestellt.

Ich hätte jetzt zwei Fragen. Einmal an Herrn Professor Dietrich – Ich habe Ihre Stellungnahme auch gelesen: Wenn Sie beim Thema Quellen-TKÜ noch etwas ändern wollen würden, was würden Sie uns dann konkret empfehlen? Oder sagen Sie, die Regelung ist so, wie sie jetzt getroffen worden ist, passend? Ich gehe da insbesondere auf den letzten Absatz in Ihrer Stellungnahme ein, da kommen Sie ja eigentlich zu dem Ergebnis, dass die Rechtfertigung des Eingriffes, so wie sie vorgenommen worden ist, in Ordnung ist. Aber vielleicht, wenn Sie uns noch einmal darlegen, ob Sie noch etwas ändern würden oder ob Sie es jetzt genau so lassen würden?

Ebenso an Herrn Haldenwang: Sie haben ja jetzt die vielen Fragen und Kritikpunkte auch zur Quellen-TKÜ vernommen. Die jetzige Regelung, so wie sie gefasst ist, ist die aus Ihrer Sicht genau so, wie Sie sie brauchen, oder gibt es noch einen Punkt, den Sie klarstellen würden oder wo Sie noch etwas ändern würden oder sagen Sie: Wir brauchen das so, ansonsten ist das für uns nicht sinnvoll.

Dann kommen wir jetzt zur Antwortrunde, wieder in alphabetischer Reihenfolge von vorn, beginnend mit Herrn Professor Bäcker.

SV **Prof. Dr. Matthias Bäcker** (Johannes Gutenberg-Universität, Mainz): Vielen Dank, Frau Vorsitzende.

An mich sind zwei Fragen gestellt worden. Die erste kam von Herrn Dr. Wirth, der gefragt hat, ob nicht die Ausweitung des Beobachtungsauftrages auf Einzelpersonen so eine Art Vermischung von Verfassungsschutz und Polizei und auch ein Durcheinander im föderalen Gefüge, insbesondere wegen der Rolle des Militärischen Abschirmdienstes, bewirkt.

Was es schwierig macht für mich, diese Frage zu beantworten, ist, dass dahinter natürlich die Idee des Trennungsprinzips steht, das davon ausgeht, dass zwischen Nachrichtendiensten und Polizeibehörden im Prinzip ein grundlegender funktionaler Unterschied besteht. Das entspricht weder geltendem Recht, so, wie es inzwischen dasteht, noch entspricht es der Wirklichkeit der Tätigkeiten dieser Behörden. Das wäre vielleicht wünschenswert, dieses Trennungsprinzip einmal wieder etwas stärker zu machen, aber tatsächlich sind die Beobachtungsaufträge von Polizei und Nachrichtendiensten einander in den letzten Jahren so stark angenähert worden, dass es gar nicht mehr so einfach ist, da wirklich einen Unterschied zu sehen. Die Polizeibehörden dürfen immer weiter im Vorfeld konkreter Gefahren zahlreiche Überwachungsmaßnahmen einsetzen; die Nachrichtendienste begreifen sich zunehmend – und inzwischen auch mit Billigung des Bundesverfassungsgerichtes im BNDG-Urteil – als eine Art Frühwarnsystem, das eben nicht nur politische Beratungsleistungen anbietet, sondern auch dazu da ist, Gefahren frühzeitig zu erkennen, um sie dann gegebenenfalls, sobald sie sich verdichtet haben, abzuwehren. Das hat das Bundesverfassungsgericht im BNDG-Urteil für den BND akzeptiert – ich gehe davon aus, dass es das für die Verfassungsschutzbehörden auch tun würde. Dementsprechend würde ich sagen: Ja, wenn man das Trennungsprinzip quasi ernster nehmen würde, als es das geltende Recht und gar die Behördenpraxis tut, dann könnte man sagen, die Verfassungsschutzbehörden als Inlandsnachrichtendienste sind eigentlich dafür da, eine Strukturaufklärung zu betreiben und politisch verwertbare Informationen zu generieren und das setzt weitgehend eigentlich voraus, dass es hier um Personenzusammenschlüsse geht, die auch eine gewisse Mächtigkeit aufweisen. Wenn dann der Beobachtungsauftrag der Verfassungsschutzbehörden generell auf Einzelpersonen ausgedehnt wird, stellt sich die Frage: Geht es hier nicht eigentlich um Gefahrenabwehr? Denn eine Einzelperson kann nicht die freiheitlich-demokratische Grundordnung beseitigen, das kann ich mir nicht vorstellen, das geht immer nur im Rahmen eines Personenzusammenschlusses.

Wenn man allerdings akzeptiert – und ich fühle mich im Rahmen dieser Anhörung nicht dazu berufen, das generell ganz anders machen zu wollen – wenn man akzeptiert, dass die Verfassungsschutzbehörden auf der einen Seite auch so eine Rolle bei der Gefahrenfrüherkennung haben und wenn man auch akzeptiert, dass der Beobachtungsauftrag der Polizeibehörden eben von der konkreten Gefahr immer weiter in das Gefahrenvorfeld verlagert wird, dann gleicht sich das einander an: Die Polizei ist an Strukturen interessiert, die Verfassungsschutzbehörden können dann auch an Einzelpersonen interessiert sein. Das ist für mich aus meiner Sicht, so wie die Dinge im Moment dastehen, weniger eine verfassungsrechtliche Frage als eine sicherheitspolitische Frage, ob man das so will. Und die Probleme, die man sich damit einhandelt, scheinen mir auf der Hand zu liegen, wurden von Herrn Dr. von Notz dann auch in seiner Frage angedeutet: Es kommt zu Verantwortungsdiffusionen – es ist völlig unklar, wem man jetzt eigentlich vorwerfen kann, was schiefgelaufen ist, und so weiter. Diese Probleme sehe ich alle, ich glaube nur eben, dass man da grundlegender herangehen müsste, genauso wie man an die Nachrichtendienstgesetze aus hundert anderen Gründen grundlegender herangehen müsste. Das ist nur, glaube ich, etwas, was heute nicht zu leisten ist. Ich habe das in anderen Zusammenhängen in meiner Stellungnahme versucht anzudeuten, was da alles für Probleme bestehen.

Die zweite Frage, von Herrn Strasser, betrifft die Rolle der Unternehmen bei der Ermöglichung der Quellentelekommunikationsüberwachung. Um die Frage zu beantworten, muss man, glaube ich, zwei Aspekte auseinanderhalten. Der eine Aspekt betrifft die Belastung der Unternehmen selbst, dadurch, dass sie zur Mitwirkung verpflichtet werden. Da hat Herr Dietrich gesagt, die Unternehmen würden eigentlich ja weniger stark belastet als bei der klassischen Telekommunikationsüberwachung, sie müssten lediglich gewissermaßen ermöglichen, dass die Nachrichtendienste ihnen Gegenstände in ihre technischen Anlagen hineinstellen und die Datenströme da hineinleiten, gewissermaßen einen Stecker hineinstecken und alles andere machen die Dienste und das belastet die Unternehmen doch viel weniger, als wenn sie selbst stärker verpflichtet werden, Datenströme auszuleiten, fortlaufend. Und das stimmt wahrscheinlich auch. Also die Belastung der Unternehmen selbst, Artikel 12 GG, scheint mir nicht das Problem zu sein.

Fragen, die dieser Infiltrationsweg aufwirft, sind vor allem solche der IT-Sicherheit. Die eine Frage ist: Wenn die Datenströme hier umgeleitet werden und dann vom Verfassungsschutz manipuliert werden – so soll das ja wohl laufen – und dann anschließend weitergeleitet werden, kann man sicher sein, dass das Ganze nicht möglicherweise in Wechselwirkungen eintritt mit der sonstigen Netzinfrastruktur, die man so gar nicht absehen kann. Da müsste man eigentlich viel stärker Tests durchführen, um zu gucken, ob es da nicht zu Problemen kommt. Das ist also ein ähnliches Problem, wie ich es im Zusammenhang mit den Infiltrationsmechanismen selbst angedeutet habe: Hier kann es zu Schwierigkeiten kommen, die gegebenenfalls dann auch Dritte bedrohen können. Das ist ein Problem.

Ein anderes Problem ist, dass sich bei der Umleitung des Datenstroms die Frage stellt, wie genau denn dann die Dienste eigentlich vorgehen, um die Zielsysteme der Überwachung zu infiltrieren. Wenn alles gut läuft, ist der Datenstrom verschlüsselt. Es wäre ein Kunstfehler sozusagen, wenn auf der Übertragungsstrecke Daten unterwegs wären, die man jetzt einfach verändern kann, indem man an eine Datei noch irgendetwas heranhängt, das dann den Trojaner installiert. Das dürfte eigentlich nicht sein, sondern es muss sich eigentlich um verschlüsselte Datenströme handeln – dann wiederum kann man sich eigentlich fast nur noch vorstellen, dass Sicherheitslücken der Zielsysteme ausgenutzt werden, und da kommt man eben in Teufels Küche. Das ist sozusagen das große Problem, was für mich zu der Schlussfolgerung führt: Die Verpflichtung der Unternehmen für sich genommen lässt sich schon rechtfertigen, die Frage ist aber, worauf genau diese Verpflichtung eigentlich praktisch hinausläuft. Und da habe ich erhebliche Bedenken.

In gewisser Weise der unter IT-Sicherheitsgesichtspunkten möglicherweise sogar unproblematischste Weg wäre, die Unternehmen nicht nur dazu zu verpflichten, Datenströme umzuleiten, sondern geeignete Unternehmen, zum Beispiel die Hersteller von Betriebssystemen dazu zu verpflichten, bei Zielpersonen von Überwachungsmaßnahmen eine manipulierte Version des Betriebssystems beim nächsten Update auszuleiten, sodass sich dann der

Trojaner quasi mitinstalliert. Man müsste also an Unternehmen wie Apple oder Microsoft herantreten und diese zu einer Mitwirkung verpflichten, die über die Umleitung von Datenströmen ganz erheblich hinausgeht. Das würden diese natürlich nicht gern machen, das würde zweifellos auch in deren Grundrechte eingreifen. Ich glaube aber tatsächlich, dass unter dem Gesichtspunkt der IT-Sicherheit das vielleicht sogar der vorzugswürdige Weg wäre. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann Herr Professor Dietrich.

SV **Prof. Dr. Jan-Hendrik Dietrich** (HS Bund, Berlin): Ja, danke.

Ich beginne mit der Frage des Abgeordneten Brand. Sie hatten danach gefragt, ob es wesentliche Einschnitte in den journalistischen Quellenschutz durch die Gesetzesnovelle gibt. Nun, das ist die Frage, inwieweit das sogenannte Redaktionsgeheimnis der Journalistinnen und Journalisten berührt ist. Das wird durch die Presse- und Rundfunkfreiheit in Art. 5 Abs. 1 GG geschützt. Das Verfassungsgericht versteht darunter die Eigenständigkeit der Presse, das geht von der Beschaffung der Information bis hin zu der Verbreitung von Nachrichten und Meinungen. Die Redaktionstätigkeit darf unter keinen Umständen von staatlichen Maßnahmen gestört werden – darunter fällt dann auch der Informantenschutz. Nun nimmt das Gesetz dazu auch Stellung, nämlich im § 3b. Danach werden sogenannte Berufsgeheimnisträger in einem besonderen Maße geschützt. Ich verstehe, dass Journalistinnen und Journalisten sich wünschen, dass der Schutz, der hier über den Verweis auf die Strafprozessordnung bewerkstelligt wird, noch weitergeht. Tatsächlich ist es aber so, dass sich dieser Schutz im Rahmen der Rechtsprechung des Bundesverfassungsgerichts hält. In der BKA-Gesetzentscheidung und auch zuletzt in der Entscheidung zum BND-Gesetz hat das Verfassungsgericht diesen Schutz als ausreichend erachtet.

Ich fahre fort mit der Frage des Abgeordneten Dr. Wirth. Da ging es um die Vermischung von Polizei- und Nachrichtendienstaufgaben durch die Anpassung von § 4 Bundesverfassungsschutzgesetz. Da kann ich mich in weiten Teilen den Äußerungen des Kollegen Bäcker anschließen. Also zunächst einmal sehe ich jetzt hier keine Gefährdung des sogenannten Trennungsgebotes durch eben diese Vorschrift. Gleichzeitig bin ich aber der Auffassung, dass die Gleichstellung begrifflicher Art von Personenzusammenschlüssen und Einzelpersonen zumindest wertungswidersprüchlich ist. Denn Personenzusammenschlüsse sind abstrakt gefährlich, nicht? Also man kann aus einem Personenzusammenschluss viel weniger leicht austreten, es entsteht eine Gruppendynamik. Und all das ist bei den Einzelpersonen nicht gegeben. Tatsächlich gibt es ja auch, wie wir vorhin schon gehört haben, eine Regelung, die Einzelperson als Bestrebung zu werten. Ich schlage in meiner Stellungnahme vor, eben für die von Herrn Präsident Haldenwang genannten Fälle, diese Regelung noch einmal zu modifizieren – Herr Bäcker hat das ja auch so ausgeführt.

Zur letzten Frage, von Ihnen, Frau Vorsitzende, zur Änderung der Regelungen der Quellen-TKÜ. Nun, also ein Vorschlag, der sich doch sehr hören lässt, den ich hier vorhin gehört habe, nämlich vom Kollegen Poscher, ist, eine eigenständige Regelung für die Quellen-TKÜ zu schaffen. Das kann man sicherlich tun, zur Klarstellung eines Instruments, wenngleich die Quellen-TKÜ auch eine Telekommunikationsüberwachung bleibt. Aber eine eigenständige Vorschrift würde vielleicht noch einmal beim Rechtsanwender für Klarheit sorgen. Auch kann ich mir durchaus vorstellen, dass man nach Zielsystemen differenziert. Also den Gesetzestext zum Beispiel auf die von mir genannten Messenger-Dienste hin genauer spezifiziert. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann Herr Professor Graulich.

SV **Prof. Dr. Kurt Graulich** (Richter a. D. am BVerwG, Berlin): Vielen Dank Frau Vorsitzende!

Ich beantworte zwei Fragen des Abgeordneten Grötsch. Die Erste bezieht sich darauf, also sie betreffen beide, wenn ich es recht sehe, den § 11 Abs. 1a. Die erste betrifft die Frage, ob man diese Regelung verfassungskonform regeln könnte bzw. wie. Ich meine – ich habe es ja angedeutet, dass ich auf zwei Ebenen große Probleme sehe: Einmal bei der Formulierung des Tatbestandes und dann aber auch beim Verhältnismäßigkeitsgrundsatz – auf beiden Ebenen wäre anzusetzen.

Also beim Tatbestand müsste erst einmal offengelegt werden, unter welchen besonderen Gefährlichkeitsvoraussetzungen zu diesem sehr schwer wiegenden Instrument gegriffen werden soll, also es müsste zum Beispiel die Hochwertigkeit von Rechtsgütern benannt werden, die für bedroht erachtet werden durch Personen oder durch Personengruppen und die dann diese hochinvasive Maßnahme auslösen. Das würde vielleicht auch den Gesetzgeber in die Verlegenheit bringen, da wirklich Ross und Reiter zu nennen. Das was auf keinen Fall geht, ist – wenn ich das einmal etwas salopp ausdrücken darf: Weil wir gerade bei einer G10-Maßnahme sind, dann könnte man sich doch auch noch dieses andere, nämlich Quellen-TKÜ oder Onlinerecherche dazu nehmen. Das geht eben einfach nicht. Das ist ein Quantensprung an Rechtseingriff und dessen Voraussetzungen müssen benannt und auch in das Gesetz geschrieben werden. Dabei kann ich allerdings mit meiner Fantasie nicht dienen, weil das müssen diejenigen sagen, die sich da angesprochen fühlen in ihrem Schutzauftrag.

Dann will ich aber im selben Zusammenhang auf etwas hinweisen, was ja Hermann Reuter schon einmal in der Rechtswissenschaft diskutiert hat: Sind wir eigentlich im richtigen Gebiet? Das heißt, wir sind jetzt im Augenblick hier in dem Gebiet der G10-Aufklärung/Nachrichtendienst, aber sind wir nicht eigentlich im Strafrecht? Also das, worüber hier immer nachgedacht wird und das sind ja auch die Bezugspunkte, also diese schweren Mordtaten, wie gegen Regierungspräsident Lübcke oder diesen gescheiterten, sehr gravierenden Anschlag in Halle, das sind alles Dinge, die im Strafrecht wurzeln und wo infolgedessen die Schutzbedürftigkeit aus dem Strafrecht kommt. Einer der Vorgänger von Herrn Poscher, nämlich Professor Sieber hat sich ja mit der Frage des Paradigmenwechsels vom Strafrecht zum Sicherheitsrecht beschäftigt – als einer der Direktoren des MPI in Freiburg – und hat da sozusagen diesen Wal zum Tanzen gebracht. Und an dieser Stelle müsste man in der Tat die Frage zum Tanzen bringen, wie der Schutz organisiert werden soll. Und ich vermute einmal, dass man in dem Fall weniger im ND-Recht (Nachrichtendienste-Recht) landen würde, als vielmehr im Strafrecht. Man müsste sich dann in der Tat überlegen, ob es hier Rechtsgüterbedrohung gibt, für die man sich Straftatbestände ausdenken muss und nicht nach einer Lösung im ND-Recht suchen und dann auch noch in dieser zweifelhaften Weise mit dieser Quellen-TKÜ und Onlinerecherche.

Die zweite Frage war, wie man das Kontrollregime – also wenn man schon das Ganze macht – das Kontrollregime verbessern könnte. Also, was mich wundert ist, dass wenn man schon eine solche, wirklich spektakuläre Regelung wie diesen § 11 Absatz 1a schafft, dass man nicht wirklich mit Ausrufezeichen klarmacht, dass hier nichts unternommen werden darf, bevor die G10-Kommission ihr „Go!“ gegeben hat. Also das ist in keiner Weise ein Maßnahme, die erst ergriffen werden und danach gesagt werden darf: „Ja gut, jetzt haben die Maßnahme schon gemacht, gehen wir hinterher bei der G10-Kommission vorbei und fragen, ob die einverstanden sind.“ Sondern das ist zum Beispiel ein Fall, wo ohne dass die G10-Kommission ihr Plazet gegeben hat, überhaupt nicht begonnen werden darf. Also das ist eine Maßnahme, die da meines Erachtens ergriffen werden muss. Und dann – das hat ja der Kollege Bäcker auch schon angedeutet – wir reden hier über Dinge, von denen voraussichtlich, wenn überhaupt, in einer so geringen Anzahl von Fällen Gebrauch gemacht werden wird, dass man wirklich sagen muss – also die schmale Basis von Erfahrungen, die hier gesammelt worden ist oder gegebenenfalls gesammelt sein werden wird, die muss wirklich permanent erläutert werden. Und dann muss der Gesetzgeber in diesem Fall wirklich eine zeitliche Befristung einführen, wie das nach den 9/11-Gesetzen zunächst einmal guter Brauch war. Und die muss auch exkulpiert werden – das heißt, wenn das Gesetz nach einer geringen Zahl von Jahren nicht angewandt worden ist, dann muss es eben wieder auslaufen. So. Davon sollte wirklich Gebrauch gemacht werden.

Also Nachschärfen des G10-Vorbehaltes selbst und zeitliche Limitierung des Gesetzes würde ich für unverzichtbar halten. Aber für mich lautet der Obersatz, dass dieses Gesetz nicht kommen sollte!

Vors. **Andrea Lindholz** (CDU/CSU): Dann Herr Haldenwang.

SV Präs. **Thomas Haldenwang** (BfV): Ich möchte vielleicht, weil mehrere Fragen sich auf das Thema bezogen, vorweg schicken: Was ist eigentlich die Aufgabe des Verfassungsschutzes? Wie grenzt sich der Verfassungsschutz von der Polizei ab? Warum braucht der Verfassungsschutz hier eine eigene Regelung, wo vielleicht die Polizei eben auch über

entsprechende Regeln verfügt. Ich rufe noch einmal in Erinnerung: Verfassungsschutz ist das Frühwarnsystem. Wir werden tätig lange bevor Eingriffsbefugnisse der Polizei da sind und insofern ist es natürlich auch unsere wichtigste Aufgabe, Extremismus zu überwachen. Und mit Extremismus hat Polizei zunächst überhaupt nichts zu tun und da haben die auch überhaupt keine Befugnisse. Und leider haben wir in der Vergangenheit eben oft genug die Feststellung machen müssen, dass sich eben aus dem Extremismus heraus dann auch Gewalt und Terrorismus entwickeln, terroristische Gruppierungen entstehen – und insofern ist es dann eben von Vorteil, dass eine weitere Bearbeitung auch der Verfassungsschutzbehörden stattfindet in diesen Fällen. Einfach aufgrund der Vorkenntnisse, die man schon im Rahmen der Extremismus-Bearbeitung in diesen Fällen gewonnen hat.

Und es ist auch notwendig, dass die Verfassungsschutzbehörden diese Vorfeldaufklärung machen, denn wir verfügen über Informationen, die Polizeibehörden oft nicht zugänglich sind. Wenn ich erinnern darf an die Bekämpfung des Islamistischen Terrorismus: Viele Hinweise auf entsprechend gefährliche Gruppierungen kommen von internationalen Diensten, von Nachrichtendiensten, die eben – in der Natur der Sache liegend – nicht mit Polizeidienststellen kommunizieren, sondern ausschließlich mit anderen Nachrichtendiensten. Würde nicht das Bundesamt für Verfassungsschutz diese Informationen entgegen nehmen – oder der Bundesnachrichtendienst –, dann kämen diese Informationen bei deutschen Sicherheitsbehörden nicht an! Also schon aus dem Grund ist es notwendig, dass man eine Vorfeldorganisation hat, die dieses nachrichtendienstliche Wissen mit bearbeiten kann, bevor überhaupt eine Zuständigkeit der Polizei entsteht. So, Vorfeldaufklärung.

Und im Rahmen der Vorfeldaufklärung ist es seit jeher auch unbestritten, dass dazu auch nachrichtendienstliches Instrumentarium gehört, wie auch im extremsten Fall, als Ultima Ratio die Kommunikationsüberwachung. Dafür haben wir das G10-Gesetz und das ging bisher analog. Und in der Vergangenheit, zwanzig Jahre zurück, war es eben möglich – wir reden allerdings, das ist mir ja auch bewusst, da nur über das gesprochene Wort – aber das gesprochene Wort in vollem Umfang über eine G10-Maßnahme zu erfassen im Zusammenhang eben mit analoger Kommunikation. Ich muss jetzt, glaube ich, hier keine großen Ausführungen machen, wie sich die Dinge entwickelt haben, aber da bin ich dann jetzt auch bei der Frage von Herrn Brand: Welche Bedeutung hat denn dann heute diese Quellen-TKÜ, welche Bedeutung haben denn eben diese Messenger-Dienste in der Kommunikation unserer Kundschaft insgesamt? Und da muss man eben einfach feststellen, es findet ohnehin analoge Kommunikation gar nicht mehr statt. Es ist alles internetbasiert. Aber diese Kommunikation findet dann auch nicht mehr über die Anschlussanbieter statt, sondern zu 90% über die Dienstanbieter, die also praktisch over the top, oberhalb der Anschlussanbieter angesiedelt sind. Und das sind solche Anbieter wie WhatsApp, Telegram, Instagram, Threema, Facebook und so weiter. Und da ist es gerade so, dass – diese Dienste-Anbieter werben damit! – und dazu haben sie auch allen Anlass – dass bei ihnen kryptiert kommuniziert wird, dass diese Kommunikation gerade nicht zugänglich ist, für nichts und niemanden. Und insofern –

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Deshalb nutzen wir es alle!

SV Präs. **Thomas Haldenwang** (BfV): Deshalb nutzen Sie das ja alle auch und nur weil manche so leichtsinnig sind, wird dann auch schon einmal das ein- oder andere Telefon gehackt. Aber das ist dann eine Frage des persönlichen Leichtsinnes damit. Meistens sind unsere Kunden, jedenfalls in bestimmten Bereichen, durchaus auch vorsichtig und wir haben dann eben keinen Zugriff mehr auf diese kryptierte Kommunikation. Und ich weiß jetzt nicht, was das BKA da von sich gegeben hat, aber ich sage einfach nur, dass –

BE Abg. **Benjamin Strasser** (FDP): Ich habe es ja vorgelesen. Die greifen über die Webversion auf das Gerät ohne Staatstrojaner zu. Mich wundert, dass das BKA das kann, aber der Verfassungsschutz das nicht macht.

SV Präs. **Thomas Haldenwang** (BfV): Ich will das jetzt nicht kommentieren, aber ich sage jetzt einfach einmal – und da verrate ich auch kein Geheimnis – wir können WhatsApp nicht mitlesen! Und wenn das für das BKA so einfach möglich wäre, Herr Strasser, wie Sie das jetzt darstellen, dann verstehe ich eigentlich die ganze aufgeregte Debatte hier nicht, die wir führen, denn dann

können viele andere auch Zugriff nehmen. Es ist notwendig, dass wir doch auch legal eine Möglichkeit haben, so wie früher auch, Kommunikation in besonders extremen Fallkonstellationen zu überwachen – nur darüber reden wir hier, noch einmal: wir reden nicht über Massenüberwachung. Es wurde auch schon gesagt, da reden wir zukünftig über Fälle, die kann man im Jahr vielleicht an zwei Händen abzählen oder so. Aber das sind nun einmal dann die gefährlichen Fälle. Das sind die Fälle, wo die Gefahr besteht, dass jemand sich vielleicht von einem Schwätzer im Internet auf einmal zu einem Täter in der realen Welt entwickelt. Und deshalb, Herr Strasser, hatte ich auch diese Fälle von Hanau und Halle genannt, als Beispielsfälle – ja, wir hatten die beiden Täter vorher nicht auf dem Schirm, aber weil wir auch keine Befugnisse hatten, Einzelpersonen zu überwachen. Inzwischen hat sich die Welt wieder weiter gedreht, wir sind – und ich bin dankbar für die Personalaufwüchse – wir sind mit virtuellen Agenten auf den einschlägigen Internetplattformen unterwegs und stellen dabei immer wieder fest, da gibt es Einzelpersonen, die sich sehr extrem äußern. Und die haben auf einmal auch eine ganz hohe Anzahl von Likes und Followern und da kann es tatsächlich sein und insofern unterscheidet sich die heutige Zeit von der früheren – früher konnte nur eine Gruppierung wirkmächtig werden und irgendetwas erreichen. Heute kann eine Einzelperson tatsächlich im Internet so eine Bedeutung erlangen, so viele Follower erwerben, dass eine Einzelperson gefährlicher sein kann als eine Bestrebung. Das Beispiel Amerika wurde vorhin auch schon einmal hier genannt. Und deshalb ist es wichtig, dass wir dann auf diese Einzelpersonen gucken und hätten wir vielleicht die Befugnis, die wir heute anstreben mit dem Gesetz, vor einem Jahr oder zwei Jahren schon gehabt, dann wären uns eben im Rahmen unserer Internetbearbeitung auch Täter von Halle oder Hanau möglicherweise aufgefallen – ich weiß es nicht. Aber eines darf man auch nicht machen: Sowenig, wie man der Feuerwehr irgendwie das Löschfahrzeug nicht bewilligt, weil sie in der Vergangenheit einmal einen Brand nicht gelöscht hat, sowenig sollte man sagen: Wir geben dem Verfassungsschutz dieses notwendige Instrument nicht. Wenn es nur einmal klappt, einen Anschlag zu verhindern, dann war es die Sache doch schon wert. Und dafür werbe ich an der Stelle.

Herr Dr. von Notz, in Teilen habe ich Ihre Frage schon beantwortet. Polizei – eben doch erst deutlich späterer Zeitpunkt als Verfassungsschutz. Und wir müssen einfach diese Möglichkeiten, die wir im Vorfeld haben – das Frühwarnsystem – müssen wir nutzen und uns dann allerdings auch weiter in die Zusammenarbeit mit der Polizei einbringen, wenn der Fall auch polizeilich bearbeitet wird. Darum ist es ja so notwendig, dass wir im Gemeinsamen Terrorismusabwehrzentrum zusammensitzen – Polizei und Nachrichtendienste – und die verschiedenen Erkenntnisse, soweit das es eben durch Übermittlungsvorschriften erlaubt ist, auch zusammenführen. Ich glaube, dieses System ist sinnvoll und vor allem auch wichtig in der aktuellen Bedrohungssituation. Da eine Abschaffung des Verfassungsschutzes zu verlangen und das alles auf die Polizei übertragen zu wollen – das trennt viel zu viel an Information – an Vorfeldinformation – ab.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Dann verteidigen Sie einmal diesen Vorfeldbereich für den Verfassungsschutz. Weil das ist ja wirklich wahr: Die polizeilichen Befugnisse dehnen sich weiter und weiter in den Präventivbereich aus und das verschwimmt einfach. Und da muss man den eigenen Bereich einmal verteidigen. Ich fordere ja nicht die Abschaffung, aber ich sehe, dass es verunklart wird.

SV Präs. **Thomas Haldenwang** (BfV): Aber ich kann nur für meinen Bereich streiten. Und das tue ich. Und ich glaube, wir wollen da auch maßvoll agieren, weil wir es hier ja eben tatsächlich auch mit schwerwiegenden Eingriffen zu tun haben und deshalb, Frau Lindholz, auf Ihre Frage, wird die Regelung so gebraucht, wie sie ist: Sechs Juristen – sechs Meinungen. Ich bin der Meinung, diese Vorschriften, so wie sie hier formuliert sind, sind verfassungskonform und wir wären dankbar, wenn wir diese Regelungen in Bälde anwenden könnten. Dankeschön.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann Herr Professor Poscher.

SV **Prof. Dr. Ralf Poscher** (Max-Planck-Institut, Freiburg): Ich bin noch einmal gebeten worden, auf die verfassungsrechtlichen Schwierigkeiten einzugehen. Gut, ich denke, die Hauptschwierigkeit ist eben, dass man versucht, diese

neuartige Kompetenz gleichsam zu mainstreamen und zu normalisieren und so zu tun, als sei es einfach nur eine ganz übliche Telekommunikationsüberwachung, die dann über eine Verfahrensänderung eingeführt werden kann. Und das führt das Gesetz einfach in die Irre. Deshalb tauchen verschiedene verfassungsrechtliche Probleme auf.

Ich finde das deutlichste ist wirklich die Frage des Rechtsschutzes: Sie können doch jetzt nicht einfach – bloß, weil das G10-Gesetz und Art. 10 GG es für Telekommunikationsüberwachungen erlauben, den Rechtsschutz einzuschränken und diese Einschränkung des Rechtsschutzes auf eine Onlinedurchsuchung ausweiten – auch wenn Sie die Onlinedurchsuchung ihrerseits beschränken. Es gibt überhaupt keinen Anhaltspunkt im Grundgesetz dafür, dass die Rechtsschutzgarantie auch gegenüber solchen Maßnahmen beschränkt werden kann und in § 13 steht es aber ausdrücklich drin. Und ich habe weder in der Gesetzesbegründung noch sonst irgendwo etwas dazu gesehen und ich fürchte einfach, dass der Gesetzgeber das vielleicht übersehen hat: Dann sollte man sich das dringend noch einmal angucken, weil das natürlich eine harte Einschränkung von Art. 19 Abs. 4 GG ist, bei der nicht absehbar ist, wie sie gerechtfertigt werden soll. Das ist ein Punkt.

Der zweite Punkt ist ja auch ein paarmal angesprochen worden: Dadurch, dass jetzt diese Regelung, die sehr viel intensiver eingreift, auch andere Grundrechte betrifft, für die, wie für das IT-Grundrecht, besondere verfassungsrechtliche Anforderungen bestehen, muss man noch einmal auf die Eingriffsschwellen schauen. So wie die Eingriffsschwellen jetzt einfach von der herkömmlichen Telekommunikationsüberwachung übernommen worden sind, passen sie eben nicht mehr auf Zugriffe, die den Charakter einer Onlinedurchsuchung haben. Das zeigt sich an den Rechtsgütern aber auch an den betroffenen Personen. Da muss man einfach noch einmal ran und ich kann Herrn Dietrich nur unterstützen, dass man sich wirklich noch einmal hinsetzen und eine eigenständige Regelung machen sollte, die das Phänomen auch als solches dann eigenständig erfasst.

Ich will jetzt doch noch einmal etwas sagen, das damit ja zusammenhängt, weil das bislang so klang – außer bei Herrn Haldenwang – als seien Verfassungsschutz und Polizei doch jetzt eins und als sei es lediglich eine verfassungspolitische Frage, ob diese Dienste durch die Einführung dieser Bestimmung weiter aneinander angenähert werden. Ich möchte dem ausdrücklich widersprechen und Herrn Haldenwang da unbedingt zustimmen, dass der Verfassungsschutz eine eigene Aufgabe hat, die durch das Grundgesetz definiert ist und die nicht darin besteht, Gefahren abzuwehren und Verbrechensverfolgung zu betreiben – das ist Aufgabe der Polizei. Sondern der Verfassungsschutz hat im Vorfeld den Strukturanalyse- und Aufklärungsauftrag, der sich natürlich teilweise, was die Informationen angeht, mit den Aufgaben der Polizei überschneidet, aber dann eben auch nur an diesen Schnittstellen bearbeitet werden kann. Und ich sehe das ausdrücklich nicht so, dass das bloß eine rechtspolitische Frage ist, den Verfassungsschutz jetzt hier als eine weitere Polizeibehörde auszustatten. Der Verfassungsschutz ist Kraft des Grundgesetzes keine Polizeibehörde und auch keine Strafverfolgungsbehörde, sondern hat einen verfassungsrechtlich eigenen Auftrag. Und wenn man das ändern wollte, dann müsste man das Grundgesetz ändern!

Vors. **Andrea Lindholz** (CDU/CSU): Dann Herr Dr. Rusteberg, bitte noch.

SV **Dr. Benjamin Rusteberg** (Georg-August-Universität, Göttingen): Ja, vielen Dank. Ich hatte zwei Fragen von Frau Renner. Zum einen ging es um die Frage, wie man denn oder ob man denn nun eigentlich sicherstellen kann, dass eben bei der Quellen-TKÜ tatsächlich nur Überwachung der laufenden Kommunikation betrieben wird. Und das ist eben die große Frage, die sich an der Stelle stellt, die das Bundesverfassungsgericht mehr oder weniger der Praxis überlassen hat, indem es gesagt hat: „Uns interessiert das eigentlich gar nicht, ob das überhaupt geht, weil die gesetzlichen Regelungen sagen ja klar, dass das technisch sichergestellt sein muss, bevor eine solche Praxis umgesetzt werden darf.“ Ich entnehme den Äußerungen insoweit, dass man offenbar beim Bundesverfassungsschutz zuversichtlich ist, das sicherstellen zu können, weil man ja den Eindruck erweckt, man könne sozusagen morgen loslegen mit dieser Technik, sobald man diese Befugnis hat. Alles, was dazu in der Literatur zu finden ist – ich bin nun Rechtswissenschaftler, kein Informatiker – aber eben auch in den Quellen, die sich da auf

Informationswissenschaften beziehen, wird weiterhin davon ausgegangen, dass eine solche Trennung, eine solche Sicherstellung technisch eigentlich nach wie vor nicht möglich ist – also das der Anwender tatsächlich bereits durch die technische Ausgestaltung unfähig gemacht wird, Daten zu erheben, die er nicht erheben darf. Das hängt letzten Endes weiter an dieser rechtlichen Befugnis. Die Daten werden nicht erhoben, weil sie nicht erhoben werden dürfen, aber nicht: Die Daten werden nicht erhoben, weil sie nicht erhoben werden können. Das steht nach wie vor im Raum. Und das ist auch nach wie vor etwas, wozu sich auch der Gesetzentwurf überhaupt nicht äußert. Weder in der Begründung noch wird irgendwie den Versuch unternommen, hier tatsächlich – wie es eben seit Langem gefordert wird, wenn man so eine Regelung denn haben will – dort irgendwelche verfahrensrechtlichen Sicherungen einzuziehen. Also man könnte sich – es gibt Vorschläge in der Literatur, etwa die entsprechenden Programme, die da verwendet werden, vorher einer Begutachtung zu unterziehen oder so etwas, um sicherzustellen, dass da die entsprechenden Codes auch wirklich nur das zulassen. Mit allen Problemen, die natürlich da dranhängen auch bei den Anbietern entsprechende Sicherheitssoftware, die sich da natürlich eigentlich nicht in die Karten schauen lassen wollen.

Das Problem bei der ganzen Sache bleibt auch, dass es nachträglich wirklich kaum zu kontrollieren ist. Zumindest müsste man dann tatsächlich sagen, dass im Vorfeld durch die G10-Kommission tatsächlich eine Kontrolle vorgenommen wird, wo wirklich ausgeschlossen wird, dass entsprechende technische Befugnisse vorhanden sind. Also dass wirklich auch technisch diese Begrenzung vorgenommen wird. Wie gesagt, das nachträglich zu kontrollieren, ist aus vielerlei Gründen eigentlich fast ausgeschlossen. Das fängt damit an, dass in dem Bereich, in dem wir uns bewegen, jede gerichtliche Kontrolle praktisch extrem schwach ist, auch aufgrund der Befugnisse der Nachrichtendienste, Unterlagen nicht vorzulegen. Aber natürlich eben auch die kaum mögliche Kontrolle, im Nachhinein zu schauen, was eigentlich da tatsächlich getan wurde bei dieser Überwachung.

Die zweite Frage bezog sich auf die Provider, auf die Telekommunikationsanbieter, die tatsächlich ja auch alles andere als begeistert sind von diesem Vorhaben. Ich glaube, der Wirtschaftsausschuss hat auch aus ähnlichen Gründen eigentlich dem Verfahren nicht zugestimmt. Also der hat sich das auch soweit zu Eigen gemacht. Da muss man sagen, soweit es dort Verfassungsrechtsprechung gibt – die gibt es insbesondere in einer Entscheidung des Zweiten Senates, der eigentlich im Sicherheitsbereich nicht zuständig ist, aber aufgrund der prozessualen Konstellation eben dort Entscheidungskompetenz bekommen hat, der weitestgehend bejaht hat, dass die Berufsfreiheit, die Unternehmensfreiheit in den Telekommunikationsunternehmen das zulässt, diese zu entsprechenden Mitarbeiten zu verpflichten. Nun muss man allerdings auch sagen, das bezog sich auf andere Situationen, so dass man natürlich überlegen müsste, wenn tatsächlich auch – also da ging es vor allen Dingen um die finanziellen Belastungen. Man müsste also auch überlegen – wenn hier tatsächlich strukturell Fehlermöglichkeiten also Beeinträchtigungen des Anbietersystems zu befürchten sind – ob das nicht auch auf die Rechte der Provider durchschlagen müsste, sich dagegen wehren zu können. Und man muss auch sagen, dass in dieser Entscheidung sich eben nicht ausdrücklich zu den datenschutzrechtlichen Voraussetzungen insgesamt geäußert wurde, also zum Recht auf informationelle Selbstbestimmung. Das ist dann natürlich gar nicht unbedingt in erster Linie eine Rechtsverletzung der Provider, sondern aller Personen, die auf die Dienste dieser Anbieter angewiesen sind. Wenn dort strukturelle Fehler, strukturelle Verzerrungen, strukturelle Probleme in diesen Systemen hergestellt werden durch diese Überwachungen – dass dann möglicherweise jeder, der diese Anbieter nutzt, sich auch grundrechtlich dagegen zur Wehr setzen können müsste.

Das letzte bleibt der Punkt, dass man natürlich auch sagen kann, es wird insgesamt das Vertrauen in Information, in Datensicherheit, in Kommunikation, denke ich, hier in großem Maße erschüttert werden, weil eben keiner mehr weiß, was ihm eigentlich auf die Festplatte gespielt wird – wenn da von außen Zugriff erfolgt, wenn da Manipulationen der Daten möglich sind. Also dieses Szenario, was Professor Bäcker beschrieben hatte, dass etwa bei einem Windows-Update eben ein Trojaner aufgespielt wird – das ist ja tatsächlich, wie es jetzt auch schon funktionieren soll, nur ohne Mithilfe von Microsoft. Also das erfolgt dann unter Ausnutzung externer IT-Kompetenz. Wie

gesagt, die Anbieter können jedenfalls keine Garantie dafür übernehmen, was hinterher bei Ihnen ankommt. Danke.

Vors. **Andrea Lindholz** (CDU/CSU): So, wir haben noch 20 Minuten, jeder könnte noch eine Frage stellen. Das kriegen wir noch hin. Die Union hat keine Fragen mehr. Herr Dr. Wirth, hat die AfD-Fraktion auch keine Fragen mehr? Dann Herr Grötsch?

BE Abg. **Michael Brand** (CDU/CSU): Ich habe noch eine Frage.

Vors. **Andrea Lindholz** (CDU/CSU): Dann Herr Brand nach Herrn Grötsch, wenn das jetzt in Ordnung ist.

BE Abg. **Uli Grötsch** (SPD): Vielen Dank, Frau Vorsitzende. Ich habe eine Frage noch einmal an Herrn Graulich hinsichtlich der Mitwirkungspflichten. Es liegt ein Gutachten der Wissenschaftlichen Dienste des Bundestages vor, das sagt, dass es ein Vertrauensproblem geben könnte. Aber, ich zitiere einmal, „Es ist nicht ersichtlich, wie dieser Aspekt im Verhältnis zu dem hohen Gewicht der in Rede stehenden Rechtsgüter die Unangemessenheit eines Eingriffs in die Berufsfreiheit begründen könnte.“ Jetzt glaube ich, haben wir alle ziemlich viele Zuschriften erhalten, von den großen Dienste-Anbietern und deshalb die Frage an Sie: Gibt es aus Ihrer Sicht verfassungsrechtliche oder aber auch praktische Bedenken gegen die Mitwirkungspflicht der Diensteanbieter?

Und dann hätte ich noch eine Frage an Herrn Präsidenten Haldenwang. Herr Haldenwang, Sie begrüßen in Ihrer Stellungnahme die Stärkung des personenbezogenen Ansatzes, das hatten wir hier heute schon einmal angetextet. Also die Regelung, dass das BfV gewaltorientierte Einzelpersonen in Zukunft besser beobachten kann. Können Sie uns einmal ganz praktisch erläutern, wie wir Radikalisierungsverläufe von Einzeltätern künftig besser im Blick haben können und vielleicht sogar solche Radikalisierungsverläufe verhindern können? Danke.

Vors. **Andrea Lindholz** (CDU/CSU): Dann nehmen wir Herrn Brand wieder rein.

BE Abg. **Michael Brand** (CDU/CSU): Herzlichen Dank. Ich habe an Herrn Haldenwang eine Frage zu dem Thema Mitwirkungspflicht von Dienste-anbietern. Da gibt es in der Tat ja auch Kritik von verschiedenen Verbänden und ich möchte Sie gern bitten, dass Sie uns noch einmal einen Eindruck geben, warum es so wichtig ist und wie die Mitwirkung konkret aussieht. Und wenn die Zeit es zulässt an Professor Dietrich noch die Frage, dass er uns die Einbindung in das System der informationellen Zusammenarbeit, Stichwort Militärischer Abschirmdienst (MAD), und Bundesverfassungsschutzgesetz erläutert.

Vors. **Andrea Lindholz** (CDU/CSU): Danach Herr Strasser oder Herr Kuhle?

Abg. **Konstantin Kuhle** (FDP): Vielen Dank, ich habe auch zwei Fragen und zwar an Herrn Bäcker und Herrn Poscher. Die erste Frage betrifft genauso wie die zweite die Systematik, einmal in dem vorgelegten Gesetzesentwurf aber auch im Gesamtzusammenhang mit anderen Eingriffsbefugnissen.

Es ist ja so, dass der Gesetzentwurf ursprünglich einmal den Titel „Gesetzentwurf zur Harmonisierung des Verfassungsschutzrechtes“ trug. Das weiß ich noch – da habe ich mich gefreut. Und jetzt heißt er nur noch „zur Anpassung des Verfassungsschutzrechtes“. Jetzt will ich das auch nicht überbewerten, dass „Harmonisierung“ durch „Anpassung“ ersetzt wurde, aber angesichts der Tatsache, dass die Eingriffsbefugnisse sich nach wie vor auf verschiedene Gesetze verteilen und es damit ja relativ unübersichtlich ist, wäre es nicht besser gewesen, die Prämisse der Harmonisierung beizubehalten und alle Eingriffsbefugnisse des Bundesamtes für Verfassungsschutz in einem Gesetz transparent aufzulisten, sodass sowohl der Rechtsanwender als auch die Bürgerinnen und Bürger als auch die Geheimdienstkontrolleure und alle, die dazu gehören, sehen können, was es eigentlich an Befugnissen gibt und nach welchen Kriterien die angewendet werden dürfen. Das ist meine erste Frage an Herrn Bäcker und Herrn Poscher.

Und die zweite Frage ist auch eine systematische Frage: Wir haben ja eine bestimmte Ausgestaltung der sogenannten Quellentelekommunikationsüberwachung, nämlich in Form der zwischen den Koalitionsfraktionen konsentierten Quellen-TKÜ plus. Mich würde interessieren, wie Sie diese Ermächtigungsgrundlage einordnen in das System der anderen Ermächtigungsgrundlagen zur Quellentelekommunikationsüberwachung. Wir haben ja eine im BKA-Gesetz – da haben wir schon gehört,

die kommt relativ selten zur Anwendung. Wir haben eine in der Strafprozessordnung – die ist Gegenstand einer Verfassungsbeschwerde. Wir haben verschiedene Eingriffsbefugnisse in den Landespolizeigesetzen – da gibt es immer großes Theater, wenn so etwas eingeführt wird. Musterpolizeigesetz wird, glaube ich, nichts mehr in dieser Legislaturperiode, also geht die Diskussion auch weiter in den nächsten Jahren. Wir haben, viertens, einzelne Länder, die das im Verfassungsschutzgesetz verankert haben – ich meine auf jeden Fall Bayern – und wir haben, fünftens, dieselbe Diskussion bei der Bundespolizei – also insgesamt fünf Baustellen, davon sozusagen eine gerade gestoppt. Und jetzt ist die Frage: Wie ordnen wir die neue Quellen-TKÜ plus in dieses System aus verschiedenen Ermächtigungsgrundlagen ein? Sind die eigentlich überall gleich formuliert? Ich habe jetzt gehört, hier ist es eher eine prozessuale Norm…

Vors. **Andrea Lindholz** (CDU/CSU): Herr Kuhle, wir haben noch eine Viertelstunde.

Abg. **Konstantin Kuhle** (FDP): Also alles sehr kompliziert. Wie verhält sich das zueinander, das, was hier vorgeschlagen ist zu den anderen Ermächtigungsgrundlagen zur Quellen-TKÜ, die es so gibt? Und ist das eigentlich übersichtlich genug?

Vors. **Andrea Lindholz** (CDU/CSU): Ich hatte eigentlich gesagt: Jeder hat die Möglichkeit, eine Frage zu stellen! Jetzt haben alle zwei gestellt – das bedeutet, dass die Sachverständigen noch kürzer antworten müssen! Dann Frau Renner.

Abg. **Martina Renner** (DIE LINKE.): Ich stelle tatsächlich nur eine Frage, wie verabredet. Und zwar erneut an Herrn Rusteberg. Ich muss Sie leider wieder zu einer Problematik fragen, die im Grenzbereich zwischen reiner juristischer Bewertung und den technischen Voraussetzungen liegt. Und zwar geht es mir um die digitalen Sprachassistenzsysteme wie ALEXA oder Siri oder auch natürlich das, was wir zum Beispiel im Automobil nutzen. Ich würde Sie erst einmal zum Gesetz fragen: Schließt der Wortlaut des vorgelegten Gesetzes eigentlich aus, dass man auch auf diese informationstechnischen Systeme zugreift? Und zum Zweiten dann: Wenn Sie dies bejahen würden, macht das nicht eigentlich aus der Quellen-TKÜ so etwas wie einen „großen Lauschangriff“, weil ich ja zum Beispiel über entsprechende Sprachassistentensysteme dann Wohnraumüberwachungen durchführen kann und ähnliches. Danke.

Vors. **Andrea Lindholz** (CDU/CSU): So, und Herr Dr. von Notz noch.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Ich wollte meine eine Frage noch einmal an Herrn Professor Poscher stellen, der ja vom Spannungsfeld zwischen IT-Sicherheit und dem Verfassungsschutz spricht. Auch wenn hier eben anklang, dass man eigentlich gar keine Zero Days braucht, ist es doch dieser Technik zumindest von Seiten der Bundesregierung immanent, dass man auch Sicherheitslücken ankauft – das tut die Bundesregierung mit Staatsknete – dass Sie vielleicht doch noch einmal herausstreichen können, was eigentlich die Problematik daran ist. Wir befassen uns alle damit jeden Tag, aber es ist ja eine öffentliche Anhörung und deswegen ist es glaube ich gut, diesen Interessenkonflikt gerade in Sicherheitsfragen in Zeiten, in denen Deutschland auch massiv über die IT-Infrastruktur angegriffen wird, noch einmal herauszustreichen. Um es ein bisschen zuzuspitzen die Frage: Wenn staatliche Behörden von relevanten IT-Sicherheitslücken wissen, und diese nicht weitergeben, kann das eigentlich haftungsmäßig etwas bedeuten? Also wenn dann am nächsten Tag irgendwie erfolgreich die Verkehrsinfrastruktur – oder sagen wir einmal in den USA ist gerade eine Pipeline angegriffen worden, jetzt bricht da in einem Landesteil die Versorgung mit Benzin zusammen – dass Sie das einmal einordnen, was Sie ja auch in Ihrem Gutachten herausgestrichen haben, diesen Konflikt, der da liegt. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Ich würde Herrn Haldenwang dann die Möglichkeit geben, zum Thema Sicherheitslücken noch einmal etwas zu sagen, insbesondere zu der Äußerung von Herrn Dr. von Notz, Sicherheitslücken seien ausgenutzt und möglicherweise nicht weitergegeben worden.

Dann kommen wir zur Antwortrunde, diesmal in rückwärtiger Reihenfolge und beginnen mit Herrn Dr. Rusteberg.

SV **Dr. Benjamin Rusteberg** (Georg-August-Universität, Göttingen): Vielen Dank.

Frau Renner, Sie hatten danach gefragt, wie das mit digitalen Sprachassistenten aussieht, wie die hierbei betroffen sind. Also betroffen können sie natürlich in jedem Fall sein, wenn die Befugnisse auf eine Onlinedurchsuchung hinauslaufen würden. Das tun sie in vollem Umfang vorliegend nicht. Auch wenn sie in dieser zweiten Variante in das Grundrecht eingreifen, orientieren sie sich ja trotzdem auch da in der Reichweite an dem Begriff der Telekommunikation. Also die Frage ist eben was unter diesem Begriff der Telekommunikation gefasst wird. Grundsätzlich ist dieser Begriff erst einmal sehr, sehr weit gefasst. Es ist eben nicht mehr nur das normale, klassische Telefonieren über Festnetz- und Mobiltelefon erfasst, sonst würden wir hier über die Dinge ja auch gar nicht reden, sondern es sind letzten Endes alle Arten von irgendwie netzvermittelter oder sonstig technisch vermittelter Kommunikation unter Abwesenden einbezogen.

Auf der Gegenseite nicht unter Art. 10 GG gefasst, also nicht als Telekommunikation angesehen, wird die sogenannte Variante, dass ausschließlich Maschinen miteinander kommunizieren, also dass zwar Daten ausgetauscht werden, aber tatsächlich keine menschliche Kommunikation stattfindet. Und jetzt befinden wir uns eben mit dieser Art von Geräten, die Sie da angesprochen haben, sozusagen genau dazwischen. Also hier findet eine Kommunikation statt zwischen einem Grundrechtsträger und seinem Gerät. Ich muss sagen, ich kann es nicht hundertprozentig beantworten, ohne vorab noch einmal nachzulesen, da müsste ich noch einmal nachschauen, wie genau sich das Bundesverfassungsgericht dazu geäußert hat. Ich würde allerdings sagen, dass die Situation jedenfalls nicht eindeutig ist; dass jedenfalls eine Argumentation möglich ist an dieser Stelle – ohne Arglist sozusagen – eine Interpretation eines Anwenders dieser Vorschrift, die es auch erlauben würde, auf diese Kommunikation als Telekommunikation zuzugreifen.

Dass damit ein „großer Lauschangriff“ stattfindet, die Gefahr bestünde nach der rechtlichen Situation nicht, weil jedenfalls nur die Kommunikation überwacht werden dürfte, die tatsächlich aktiv von Seiten des Anwenders mit dem Gerät stattfindet. Es dürfte aber nicht auf „Mithören“ geschaltet werden und ich benutze das als Wanze, die alles aufzeichnet, was ansonsten gesprochen wird – das wäre technisch wahrscheinlich auch kein größeres Problem, aber das wäre jedenfalls in der Befugnis nicht enthalten. Also der Teil, der zwischen Siri/ALEXA/wie immer es heißt und dem Anwender besteht, da würde ich nicht ausschließen, dass man vertreten könnte, dass auch dies von der Grundlage hier erfasst ist. In der Kürze der Zeit kann ich dazu aber ehrlich gesagt kein ganz abschließendes Urteil abgeben.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann Herr Professor Poscher.

SV **Prof. Dr. Ralf Poscher** (Max-Planck-Institut, Freiburg): Also die Frage der Harmonisierung. Zunächst einmal kann man feststellen, dass jedenfalls jede der Bundesregelungen unterschiedlich ist: Das BKA-Gesetz kennt gar keine erweiterte Telekommunikationsüberwachung, sondern beschränkt sich auf die Quellen-TKÜ. In der StPO ist es wieder anders geregelt als im jetzigen Gesetz. Und jetzt hat man in der geplanten Neufassung für § 11 so eine Formulierung aufgenommen, dass die Informationen auf dem System ab dem Zeitpunkt der Anordnung miterhoben werden dürfen. Und da, das hatte ich ja vorhin schon ausgeführt, ist mir unklar, was das bedeuten soll. Sollen das Informationen sein, die bis zu diesem Zeitpunkt reichen oder ist es so– und das scheint mir ja das wirklich Gefährliche dabei zu sein –, dass dann unter Umständen Kommunikationsketten und -fäden miterhoben werden dürfen, die unter Umständen Jahre zurückreichen. Denn zum Teil werden diese ja bei den Messenger-Diensten mitkommuniziert. Das ist teilweise von den Benutzereinstellungen, von den Diensten abhängig. Das würde aber bedeuten, dass man dann nicht nur auf einen kleinen Ausschnitt der ruhenden Kommunikation zurückgreifen könnte, sondern auf Kommunikationen, die sich unter Umständen über Jahre erstrecken und eine Vielzahl von Personen betreffen. Und ich finde, es müsste unbedingt in der jetzigen Fassung dann auch klargestellt werden, was damit eigentlich gemeint ist und wie das wirksam begrenzt werden kann.

Natürlich wäre es schön, wenn man das alles harmonisieren könnte. Der Bund kann das natürlich nur für die Gesetze machen, für die er zuständig ist. Natürlich wäre es auch schön, wenn die gesamten Sicherheitsgesetze klarer strukturiert und

mit weniger Verweisketten und Ähnlichem versehen wären, die den Zugang für jeden, der sich mit der Materie nicht sehr intensiv beschäftigt, doch sehr erschweren, um so die Regelungssystematik zu vereinfachen. Vielleicht wäre auch eine Integration des G10-Gesetzes in die entsprechenden Fachgesetze sinnvoll, damit man alle Befugnisse für die einzelnen Dienste in den entsprechenden Gesetzen auch vollständig regelt. Das könnte man sicherlich überlegen, aber in dem Bereich gibt es natürlich ungeheuer viel zu tun, denn gerade auch über diese unsäglichen Verweisungsketten sind diese Gesetze für jemanden, der sich nicht sehr intensiv damit beschäftigt, eigentlich kaum noch verständlich.

Die nächste Frage ging dahin, wie sich das Spannungsverhältnis von IT-Sicherheit und Verfassungsschutz verhält und ob ich das erläutern könnte. Naja, das Beispiel, was da ja immer angeführt wird – und Herr Bäcker hat es ja auch sehr schön ausgeführt in seiner Stellungnahme –, ist natürlich die Wanna-cry-Sicherheitslücke. Die NSA hat damals wohl eine Sicherheitslücke benutzt, um Systeme zu infiltrieren und ist dann aber selbst gehackt worden und diese Hacker haben dann diese Sicherheitslücke benutzt, um andere Systeme anzugreifen. Ich kenne die Zahlen jetzt nicht genau, aber es sind wohl Schäden in Höhe von hunderten Billionen Dollar entstanden. Und bei der entsprechenden Anhörung in Hessen wusste dann der Chaos Computer Club noch zu berichten, dass Hacker auch die Kommunikation nach dem Aufdecken dieses Problems zwischen der NSA und dem Departement of Defense (DoD) gehackt haben und sich das DoD bei der NSA nachhaltig darüber beschwert hat, dass sie es zugelassen haben, dass das System des Verteidigungsministeriums über Jahre angreifbar war, ohne dass die NSA selbst ihre eigenen Behörden darüber informiert hatten. Und das ist so ein bisschen der Hintergrund, der sich mit solchen Sicherheitslücken verbindet. Das sind eben nicht nur Sicherheitslücken, die dann die Dienste ausnutzen können oder die Polizei oder die Staatsanwaltschaft, sondern das sind eben Sicherheitslücken, die für alle Attacken genutzt werden können.

Und deshalb ist es eben anders, als bei anderen Befugnissen und das war mein Punkt: Man kann ja überlegen, etwa, wenn man so etwas wie eine akustische Wohnraumüberwachung einführen oder erweitern will und dann merkt, dass man das Instrument gar nicht so häufig braucht, dass es dann ja vielleicht nicht so schädlich ist, wenn das überhaupt im Gesetz steht. Aber hier bei dieser Regelung kann es einen wirklichen Schaden zufügen, wenn das Gesetz dazu führt, dass solche Sicherheitslücken offengehalten und nicht aufgedeckt werden, um diese Instrumente abzusichern. Nun sagt Herr Haldenwang, dass das nicht getan wird – das ist natürlich sehr beruhigend zu hören –, aber dann sollte der Gesetzgeber es ruhig auch ins Gesetz schreiben, dass das nicht geschehen darf. Das würde diese Spannungslage zwischen IT-Sicherheit und Verfassungsschutz deutlich entspannen.

Ansonsten müsste man aber wirklich einmal die Kosten-Nutzen-Analyse machen und dabei stellt man fest, dass dieses Instrument, weil es auch wohl nicht so ganz leicht zu handhaben ist, jedenfalls auf diesem Weg, doch extrem selten eingesetzt wird. Und wir müssten einmal sehen welche Bedeutung das Instrument in den wenigen Fällen, in denen es eingesetzt wurde, die man wohl mehr oder weniger an einer Hand abzählen kann, für die Aufgaben der entsprechenden Behörden gehabt hat. Und erst wenn man dazu käme, zu sagen: „doch, das sind ganz entscheidende Erkenntnisse, die wir so erlangt haben“, müsste man sie in ein Verhältnis dazu setzen, welchen Risiken man Millionen von IT-Systemen dadurch ausgesetzt hat, dass man diese Lücken weiter offengehalten hat. Und dass man weiterhin – das hat Herr Bäcker ja auch ausgeführt – einen Markt anfeuert, auf dem diese Lücken gehandelt werden. Und das, finde ich, ist wirklich eine Kosten-Nutzen-Relation, die sich der Gesetzgeber einmal vorlegen muss und ich fürchte, das kann man nicht machen, ohne das einmal ernsthaft empirisch zu untersuchen. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann Herr Haldenwang.

SV Präs. **Thomas Haldenwang** (BfV): Zunächst zur Frage von Herrn Grötsch – wie wollen wir zukünftig beim personenbezogenen Ansatz bessere Aufklärungsergebnisse erzielen? Ja, ich sehe da zwei große Bereiche: Einmal fallen uns bestimmte Personen auf in der realen Welt, also ganz klassisch, heißt meinetwegen – aktuelles Beispiel – auf diesen Corona-Demonstrationen fallen Einzelpersonen auf, die sich in besondere Weise verfassungswidrig äußern und verhalten und zum

Widerstand aufrufen. Da ist überhaupt nicht erkennbar, dass sie einer Organisationsstruktur angehören, sondern das sind einzelne Personen, die aber aufgrund ihres Auftritts eine Wirkung auf eine Gruppe entfalten können. Also das wäre so ein Beispiel. Oder Briefeschreiber, die auch nicht unbedingt zu einer Organisation gehören, uns aber auffallen, weil sie besonders extreme Hassbriefe schreiben an eine Vielzahl von Personen, wo es auch notwendig ist, dann den weiteren Verlauf zu überwachen. Und dann natürlich der neuere Ansatz in der virtuellen Welt, dass wir zukünftig virtuelle Agenten auf den einschlägigen Plattformen haben, die dort Auffälligkeiten wahrnehmen – einzelne beteiligte Personen, die sich besonders extrem äußern, besonders extremistisch, ohne dass da schon irgendwie ein Zusammenschluss erkennbar wäre. Und die wollen wir zukünftig dann eben auch schon erfassen können, was ja dann auch hieße, speichern können. Das wäre ja ohne diese neue Befugnis nicht vorstellbar.

Herr Brand, Mitwirkung, welche Rolle spielt die Mitwirkung der verschiedenen Provider? Nun ich sage einfach einmal: Ohne die Mitwirkung der Provider wäre dieses Instrument nur schwerlich umsetzbar. Es gibt natürlich durchaus Möglichkeiten, dass man mit Zugriff auf das Gerät als Verfassungsschutz selbst mit eigenen Technikern eine eigene Technik aufbringt. Da muss ich allerdings auch sagen, ich glaube, wenn wir den Weg gehen würden, hätte dieses Instrument kaum noch Anwendungsfälle. Das ist technisch komplex in der Durchführung, zeitaufwendig und, um schnelle Ergebnisse zu erzielen, kein probates Mittel. Deshalb sind wir auf die Mitwirkung der Provider angewiesen. Wobei ja Mitwirkung durchaus ein breites Spektrum umfasst: Mitwirkung bedeutet ja auch schon, dass die Provider nur bestimmte Personen in solchen Angelegenheiten einsetzen können, also dass Personen, die bei G10-Maßnahmen eingesetzt werden, auch sicherheitsüberprüft werden. Dann geht es aber in die Umsetzung unserer Maßnahme und dass die Provider uns die Einbringung von technischen Mitteln ermöglichen müssen. Dass wir ihre Betriebsräume aufsuchen können, um dort Geräte aufzustellen, mit denen die Durchführung dann stattfinden kann. Heißt aber umgekehrt auch, wir erwarten gerade nicht von dem Provider, dass er jetzt den Datenstrom hackt und mit eigenen Mitteln ausleitet, sondern er muss uns die Möglichkeit verschaffen, mit unserem technischen Gerät die Maßnahme dann durchzuführen. Und dafür brauchen wir den Provider. Und dafür braucht es dann eben diese spezielle Vorschrift für den Provider, denn wir müssen nicht nur auf der einen Seite die Ermächtigungsnorm für den Verfassungsschutz haben, sondern wir müssen auch die Verpflichtungsnorm haben für den Provider, der damit auch gegenüber seinen Kunden berechtigt ist, diese Maßnahmen umzusetzen. Das gibt auch den Providern dann die entsprechende Rechtssicherheit gegenüber ihren Kunden, wenn sie an den Maßnahmen in der geschilderten Weise mitwirken. Beides ist auch nach Rechtsprechung des Verfassungsgerichts notwendig und insofern bedarf es dieser speziellen Mitwirkungsregelung hier in dem Gesetz.

Herr Dr. von Notz, Ihre Äußerungen zum Ankauf von Sicherheitslücken „mit Staatsknete“, wie Sie formuliert haben, und dass da jetzt wichtige Kenntnisse gewonnen werden, entzieht sich meiner Kenntnis. Der Verfassungsschutz tut so etwas nicht! Und das ist auch in keinster Weise mit diesem Gesetzentwurf intendiert. Dankeschön.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Herr Professor Graulich.

SV **Prof. Dr. Kurt Graulich** (Richter a. D. am BVerwG, Berlin): Ich hatte die Frage von Herrn Grötsch, was die Mitwirkungspflicht der Provider bei der Quellen-TKÜ oder der Onlinerecherche angeht. Ohne Zweifel bestehen solche Pflichten, also die Provider können sich ja in dem Zusammenhang nur auf Art. 12 und 14 GG berufen, nicht auf Art. 10 GG. Und soweit Artikel 14 GG im Raum steht, ist es natürlich eine Angelegenheit der Sozialbindung des Eigentums, dass sie mitwirken müssen. Und sobald es um Art. 12 GG geht, ist alles am Maßstab der Verhältnismäßigkeit zu überprüfen. Und da haben wir ja gigantische Beispiele, ich erinnere nur an die Vorratsdatenspeicherung, wo den Providern zum Teil über große Zeiträume erhebliche Lasten aufgebürdet wurden, ohne dass daraus etwas folgte. Und jetzt wird halt zu ermessen sein, welche Lasten in Vorbereitung solcher Maßnahmen nach § 11 Abs. 1a ins Haus stehen – das müssen die Fachleute beurteilen. Das wird ja umgesetzt werden müssen mithilfe einer Änderung der Telekommunikationsüberwachungsverordnung und in diesem Zusammenhang ist das

zu überprüfen. Wenn unverhältnismäßige Maßnahmen im Raum stehen, dann würde ich wirklich empfehlen, sich sofort gegen die Norm zu wenden, so, wie das im Falle der Vorratsdatenspeicherung auch mit Erfolg geschehen ist. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann Herr Professor Dietrich.

SV **Prof. Dr. Jan-Hendrik Dietrich** (HS Bund, Berlin): Ich beantworte die Frage des Abgeordneten Brand nach einer Einbeziehung des MAD in das informationstechnische System des Verfassungsschutzverbundes: Die gesetzliche Einbettung erfolgt über die §§ 5 und 6 des Bundesverfassungsschutzgesetzes. Hier werden in umfangreichem Maße Kooperationspflichten und Koordinationsrechte adressiert. Das BfV wird hier als Zentralstelle eingerichtet und die Länder werden mit Kooperationspflichten ausgestattet. Das heißt, sie müssten zum Beispiel Informationen an das Bundesamt liefern und das Bundesamt ist die zentrale Auswertungsstelle im Verfassungsschutzverbund. Dieser Weg der Information ist keine Einbahnstraße. Das Bundesamt ist selbstverständlich auch dazu angehalten, die Informationen dann wieder in dem Gesamtlagebild an die Länder zurückzugeben.

Und in diesem Kontext ist nun die Einrichtung von gemeinsamen Dateien zu sehen, so ist in § 5 Abs. 4 Nr. 1 Bundesverfassungsschutzgesetz das nachrichtendienstliche Informationssystem NADIS angesprochen. Alle Verfassungsschutzbehörden haben dazu Zugang und jetzt ist der MAD eben über die Neuregelung auch dabei. Das ist – Herr Haldenwang hat es ja ganz am Anfang einmal gesagt – das ist sehr zu begrüßen und man fragt sich, warum das eigentlich so lange gedauert hat, denn die Aufgabenbereiche des BAMAD, wie es jetzt heißt, und der Verfassungsschutzbehörden des Bundes und der Länder sind weitgehend identisch. So steht es in den gesetzlichen Vorschriften über den Verfassungsschutzauftrag und den Auftrag des Bundesamtes für den Militärischen Abschirmdienst. Was mich ein bisschen gewundert hat ist, dass hier dem BAMAD eine fakultative Teilnahme eingeräumt wird und keine obligatorische. Das sollte vielleicht in Zukunft noch angepasst werden. So, wie ich es der Gesetzesbegründung entnehme, mögen da wohl technische Voraussetzungen eine Rolle gespielt haben. Danke.

Vors. **Andrea Lindholz** (CDU/CSU): Und zum Abschluss noch Herr Professor Bäcker.

SV **Prof. Dr. Matthias Bäcker** (Johannes Gutenberg-Universität, Mainz): Vielen Dank.

Zwei Fragen von Herrn Kuhle sind an mich gerichtet worden, die ich, glaube ich, ein bisschen zusammenfassen kann: Hätte man das Verfassungsschutzrecht lieber harmonisieren sollen? Das sollte man wahrscheinlich tun. Ich glaube, dass das Nachrichtendienstrecht insgesamt sich in einem beklagenswerten Zustand befindet und nicht lesbar, in sich zersplittert und auch mit den Regeln juristischer Auslegungskunst kaum zu bewältigen ist. Das liegt daran, dass da einfach eine Vielzahl von Rechtsschichten zusammenwirkt, dass mit sehr komplizierten Verweisungen gearbeitet wird – Herr Poscher hat es schon gesagt – und dass man insgesamt diese Gesetze kaum versteht und auch nicht wirklich kohärent auslegen kann. Das G10-G finde ich besonders schlimm, weil das G10-G – auch vielleicht aufgrund seiner Genese, das ist viel älter als die Regelungen im Bundesverfassungsschutzgesetz – eine völlig andere Normstruktur aufweist. Die Eingriffsvoraussetzungen im § 3 G10-G haben nichts zu tun mit dem, was wir sonst im Bundesverfassungsschutzgesetz zum Beispiel finden und lassen sich da auch kaum einpassen.

Ich verstehe allerdings gut, dass das zum jetzigen Zeitpunkt der Legislaturperiode ein bisschen viel gewesen wäre, das alles zu machen. Von daher ist es nachvollziehbar, dass das Gesetz so kommt, wie es jetzt geplant ist und sich eben auf die punktuelle Erweiterung der Befugnisse des Bundesamtes beschränkt. Ob man die für eine gute Idee hält oder nicht, darüber haben wir heute intensiv gesprochen. Ob das Bundesamt die Quellentelekommunikationsüberwachung und andere Überwachungsbefugnisse braucht, hat auch etwas zu tun mit der Frage, wie man die Rolle der Nachrichtendienste im Verhältnis zu anderen Sicherheitsbehörden sieht: Was ist eigentlich Polizeiaufgabe, was ist Aufgabe der Strafverfolgung und des Strafrechts, wo und wie spielen die Nachrichtendienste da hinein? Mir scheint das keineswegs besonders klar zu sein, wie es im Moment ist. Ich würde daran festhalten, dass das meiner Ansicht nach vor allem verfassungspolitische Fragen sind, die hier bestehen. Das ist aber auch in Ordnung. Herr Poscher sieht die IT-Sicherheit als Verfassungspolitik – die sehe ich als harte Grundrechtsfrage.

Ich sehe dafür das Trennungsgebot als verfassungspolitische Frage – das sieht Herr Poscher anders. Das ist völlig in Ordnung. Ich glaube, dass wir in der Stoßrichtung unserer Positionen da ohnehin nicht auseinandergehen und die normative Ableitung ist da vielleicht eher nachrangig.

Letztlich ist es so: Es wäre schön, wenn in der nächsten Legislaturperiode – wenn mehr Zeit bleibt – vielleicht auch die Zeit darauf verwendet werden könnte, sich einmal grundlegendere konzeptionelle Gedanken gerade über das Nachrichtendienstrecht zu machen. Wenn ich mir von der Innenpolitik etwas wünschen dürfte, so als Staatsbürger, dann wäre das die Baustelle, von der ich sehr begrüßen würde, wenn sie angegangen würde. Zumal eben auch weiterhin punktueller Nachbesserungsbedarf nach meiner Überzeugung entstehen wird, einfach, weil so viele Verfassungsbeschwerden anhängig sind gegen unterschiedliche Regelungen in Nachrichtendienstgesetzen, von denen auch viele nach meiner Einschätzung Erfolg haben werden. Die Einführung der Quellentelekommunikationsüberwachung in das G10-G hat jedenfalls den Vorzug, dass sie, glaube ich, ermöglicht, das komplette G10-G einmal mit einer Verfassungsbeschwerde anzugreifen und zu gucken, ob das eigentlich dem aktuellen Stand der Verfassungsrechtsprechung entspricht – was ich verneinen würde, sodass man vielleicht den § 3 auf diesem Weg allgemein geknackt bekommt. Wenn das herauskommt bei diesem Gesetz, wäre das aus der bürgerrechtlichen Perspektive durchaus ein erfreuliches Ergebnis. Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann bedanke ich mich bei allen für die Teilnahme an der Sachverständigenanhörung, darf die Anhörung damit schließen und wünsche allen noch eine gute Woche.

Schluss der Sitzung: 14:08 Uhr

Andrea Lindholz, MdB
Vorsitzende

Anlage A

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)844 A

JOHANNES GUTENBERG UNIVERSITÄT MAINZ

JOHANNES GUTENBERG-UNIVERSITÄT MAINZ - 55099 Mainz

FACHBEREICH 03
JURA
Lehrstuhl für Öffentliches Recht und Informationsrecht, insbesondere Datenschutzrecht

Universitätsprofessor
Dr. Matthias Bäcker

Johannes Gutenberg-Universität Mainz
Jakob-Welder-Weg 9
55128 Mainz

Tel. +49 6131 39 28173
Fax +49 6131 39 28172

matthias.baecker@uni-mainz.de
www.baecker.jura.uni-mainz.de/

Stellungnahme

zu dem Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts

(BT-Drs. 19/24785)

Gliederung

3

Ergebnisse

1. Die generelle Ausweitung des Bestrebungsbegriffs auf Einzelpersonen überdehnt die Aufgabe des Verfassungsschutzes und führt zu (zusätzlichen) verfassungsrechtlichen Mängeln einiger Eingriffsermächtigungen des Verfassungsschutzrechts.
2. Das nachrichtendienstliche Informationssystem ist (nach wie vor) unzureichend geregelt. Die teilnehmenden Behörden sind ermächtigt, umfangreiche und sensible Datenbestände mit Bezug auch zu unverdächtigen Personen anzulegen und nahezu anlasslos weiterzuverarbeiten. Dies trägt der hohen Eingriffsintensität eines so umfassenden Datenverbunds nicht Rechnung.
3. Die Ermächtigung zu Quellen-Telekommunikationsüberwachungen muss mit Schutzvorkehrungen verbunden werden, die eine Ausnutzung noch unbekannter IT-Sicherheitslücken (Zero-Days) zur Infiltration des Zielsystems ausschließen oder zumindest einem strengen Risikomanagement unterwerfen.
4. Die Erstreckung der Quellen-Telekommunikationsüberwachung auf lokal gespeicherte frühere Kommunikationsinhalte geht fehl. Hierbei handelt es sich um eine Online-Durchsuchung, an die strengere Anforderungen zu stellen sind.
5. Die Ermächtigung zu Quellen-Telekommunikationsüberwachungen führt die zahlreichen verfassungsrechtlichen Mängel des Artikel 10-Gesetzes fort und vertieft sie.

4 I. Einzelpersonen als Bestrebungen

Die in § 4 Abs. 1 Sätze 3 und 4 BVerfSchG-E vorgesehene generelle Erstreckung des Begriffs der verfassungsschutzrelevanten Bestrebung auf Einzelpersonen überdehnt die Aufgabe des Verfassungsschutzes und führt zu (zusätzlichen) verfassungsrechtlichen Zweifeln an einem Teil der Eingriffsermächtigungen des Gesetzes.

Die Ausweitung des Beobachtungsauftrags überdehnt die Aufgabe des Verfassungsschutzes, weil sie die Verfassungsschutzbehörden potenziell mit einer weitreichenden Ausforschung des *Forum Internum* von Menschen betraut. Die von einer Einzelperson ausgehende Bestrebung wird gemäß § 4 Abs. 1 Satz 4 BVerfSchG-E anhand der Zielrichtung des Verhaltens dieser Person bestimmt. Damit knüpft der Beobachtungsauftrag primär an die inneren Befindlichkeiten der Person an, die ihrem Verhalten zumeist erst seinen verfassungsfeindlichen Sinn vermitteln.[1] Anders als bei Personenzusammenschlüssen, deren Angehörige zwangsläufig zumindest miteinander kommunizieren und damit ihre Ziele nach außen manifestieren müssen, lädt die vorgesehene Regelung geradezu zu einer Beobachtungspraxis ein, die statt von objektiv verfassungsschutzrelevanten Handlungen von (vermuteten) persönlichen Eigenschaften oder sozialen Einbindungen der betroffenen Person ausgeht.

Ein Bedürfnis hierfür ist nicht erkennbar. Eine rechtsstaatlich handelnde Verfassungsschutzbehörde hat kein Interesse daran, Einzelpersonen allein wegen ihrer mutmaßlichen Gesinnung zu beobachten. Die Gesetzesbegründung beruft sich zwar zum einen auf eruptive Radikalisierungsverläufe von Einzelpersonen, die zu militanten Aktionen führen können, zum anderen auf die auch von Einzelpersonen aktivierbare Eigendynamik sozialer Medien.[2] Beide Szenarien erfordern jedoch keine so weitreichende Ausweitung des Beobachtungsauftrags. Gewaltgeneigte Einzelpersonen werden bereits heute durch § 4 Abs. 1 Satz 6 BVerfSchG vom Bestrebungsbegriff erfasst. Da der Beobachtungsauftrag des Verfassungsschutzes generell bereits im Vorfeld konkreter Gefahren einsetzt, lassen sich fortgeschrittene Instrumente der personenbezogenen Risikobewertung, auf die sich die Gesetzesbegründung bezieht, in die gebotene Bewertung des Gewaltpotenzials einer Person zwanglos integrieren. Wo sich ein solches Potenzial auch mit solchen Instrumenten nicht erkennen lässt, verbleibt vor allem eine faktische Beobachtungslücke, die sich durch eine Ausdehnung des gesetzlichen Beobachtungsauftrags nicht schließen lässt. Soweit eine Beobachtung an die agitierende oder einschüchternde öffentliche Kommunikation von selbst nicht gewaltbereiten Personen anknüpfen soll, könnte eine auf das spezifische Gefährdungspotenzial solcher Personen und ihres Kommunikationsverhaltens zugeschnittene Regelung geschaffen werden, ohne den Beobachtungsauftrag hinsichtlich von Einzelpersonen

[1] Wenn Verhaltensweisen von Einzelpersonen auf die Verwirklichung bestimmter Ziele „gerichtet sein“ müssen, geht aus dem Normtext klar hervor, dass es zumindest auch auf die Intentionen der Person ankommt, vgl. allgemein zu der Diskussion um subjektive Erfordernisse im Rahmen von § 4 Abs. 1 BVerfSchG einerseits Warg, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, V § 1 Rn. 38 f., andererseits Roth, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 4 BVerfSchG Rn. 39 ff., beide m.w.N. auch zur – uneinheitlichen – Rechtsprechung.

[2] BT-Drs. 19/24785, S. 17.

5 uferlos auszuweiten. Gegen eine derartige Regelung bestünden keine grundlegenden Bedenken.

Die einschränkungslose Ausweitung des Beobachtungsauftrags auf Einzelpersonen erzeugt im Übrigen auch systematische Unstimmigkeiten. In der Folge können isoliert handelnde Einzelpersonen leichter zum Beobachtungsobjekt werden als Personen, die für einen Personenzusammenschluss handeln. Denn Personen handeln gemäß § 4 Abs. 1 Satz 2 BVerfSchG nur dann für einen Personenzusammenschluss, wenn sie ihn in seinen Bestrebungen nachdrücklich unterstützen. Dies setzt eine Unterstützung von bedeutendem Gewicht voraus.[3] Hingegen sollen fortan Einzelpersonen ohne Bezug zu einem Personenzusammenschluss auch dann dem Beobachtungsauftrag des Verfassungsschutzes unterfallen, wenn von ihnen bislang lediglich Handlungen ohne besonderes Bedrohungspotenzial für die Schutzgüter des Verfassungsschutzes ausgegangen sind. Maßgeblich ist nach § 4 Abs. 1 Satz 4 BVerfSchG-E lediglich die Zielrichtung dieser Handlungen. Nach allgemein anerkannter Wertung, die auch die Gesetzesbegründung nicht grundsätzlich in Frage stellt,[4] sind jedoch Personenzusammenschlüsse gefährlicher als Einzelpersonen, da sie typischerweise über weitergehende Handlungsmöglichkeiten verfügen und eine Gruppendynamik aufbauen können.[5] Es ist darum wenig folgerichtig, den Beobachtungsauftrag gegenüber Einzelpersonen weiter zu fassen als gegenüber Personen, die einen solchen Zusammenschluss unterstützen.

Die Erweiterung des Beobachtungsauftrags birgt als Folgeproblem erhebliche (zusätzliche) verfassungsrechtliche Bedenken gegen einige Eingriffsermächtigungen des Verfassungsschutzrechts. Diese Ermächtigungen erlauben den Einsatz nachrichtendienstlicher Mittel, wenn Tatsachen die Annahme rechtfertigen, dass dadurch Erkenntnisse über verfassungsfeindliche Bestrebungen erlangt werden können.[6] Eingriffsermächtigungen des Nachrichtendienstrechts müssen jedoch aus verfassungsrechtlichen Gründen zumindest daran anknüpfen, dass der Eingriff „zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten ist“.[7] Solange der Bestrebungsbegriff an gewaltgerichtete bzw. besonders schadensgeneigte Verhaltensweisen von Einzelpersonen (Aktionen) oder an Personenzusammenschlüsse (Gruppierungen) anknüpft, mögen die genannten Eingriffsermächtigungen diesem Erfordernis noch genügen.[8] Wird der Bestrebungsbegriff aber für Einzelpersonen

[3] Roth, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 4 BVerfSchG Rn. 35.
[4] Vgl. BT-Drs. 19/24785, S. 17.
[5] Vgl. Warg, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, V § 1 Rn. 28; Roth, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 4 BVerfSchG Rn. 38.
[6] § 9 Abs. 1 Satz 1 Nr. 1, § 9a Abs. 1 Satz 1, § 9b Abs. 1 Satz 1 BVerfSchG; vgl. ferner zur Weiterverarbeitung erhobener Daten § 10 Abs. 1 Nr. 1 und 2 BVerfSchG.
[7] BVerfGE 130, 151 (206); BVerfG, Beschluss vom 27. Mai 2020 - 1 BvR 1873/13 -,Rn. 151.
[8] Vgl. aber generell zur Reformbedürftigkeit der Eingriffstatbestände des Nachrichtendienstrechts Bäcker, in: Dietrich u.a., Nachrichtendienste im demokratischen Rechtsstaat, 2018, S. 137 (144 ff.).

6 derart ausgedehnt, dass er im Wesentlichen von deren subjektiven Zielsetzungen ausgeht, sind die verfassungsrechtlichen Grenzen überschritten.[9]

Die ausufernde Erweiterung des Beobachtungsauftrags lässt sich nicht – wie es die Gesetzesbegründung anscheinend annimmt – dadurch kompensieren, dass den Verfassungsschutzbehörden für die Beobachtung von Einzelpersonen anders als für die Beobachtung von Personenzusammenschlüssen ein Entschließungsermessen eingeräumt wird. Insbesondere soweit der Bestrebungsbegriff in gesetzlichen Eingriffsermächtigungen in Bezug genommen wird, ist es Sache des Gesetzgebers, durch eine hinreichend restriktive Normfassung zu gewährleisten, dass der Verhältnismäßigkeitsgrundsatz gewahrt bleibt. Dies darf nicht dem behördlichen Ermessen überlassen werden. Im Übrigen ist der geplanten Regelung nicht zu entnehmen, dass ein Entschließungsermessen bestehen soll. Dass die Verfassungsschutzbehörden grundsätzlich über kein solches Ermessen verfügen, wird gemeinhin nicht aus § 4 BVerfSchG, sondern primär aus § 3 Abs. 1 BVerfSchG abgeleitet.[10] Die vorgesehene Formulierung in § 4 Abs. 1 Satz 3 BVerfSchG-E „Bestrebungen… können auch von Einzelpersonen ausgehen…“ gibt für ein behördliches Ermessen nichts her. Das Verb „können“ bezieht sich nicht auf die Beobachtungstätigkeit der Verfassungsschutzbehörden, sondern auf den Gegenstand der Beobachtung. Wenn ein Entschließungsermessen bestehen soll, müsste § 3 Abs. 1 BVerfSchG ergänzt werden.

II. Informationssystem der Verfassungsschutzbehörden

Gegen die durch § 6 Abs. 2 Satz 2 BVerfSchG-E eröffnete Möglichkeit, den MAD in das nachrichtendienstliche Informationssystem einzubinden, und gegen die in § 6 Abs. 2 Satz 4 BVerfSchG-E vorgesehene technische Verkoppelung des Informationssystems mit gemeinsamen Dateien bestehen für sich genommen keine Bedenken.

Die geplanten Regelungen vertiefen jedoch die erheblichen rechtsstaatlichen Mängel des geltenden Rechts. Das nachrichtendienstliche Informationswesen ist insgesamt unzureichend geregelt und bedarf einer grundlegenden Überarbeitung. Mit Blick auf das nachrichtendienstliche Informationssystem habe ich dies bereits in meiner Stellungnahme zu dem Entwurf eines Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes näher ausgeführt.[11] Die wesentlichen Kritikpunkte, an denen die vorgesehenen Regelungen nichts ändern, seien hier lediglich noch einmal kurz zusammengefasst:

– Die gesetzlichen Bevorratungsregelungen ermöglichen es den Verfassungsschutzbehörden, einander personenbezogene Daten jeglicher Art und Herkunft zur Verfügung zu stellen.

---

[9] Vgl. zum Polizeirecht BVerfGE 141, 220 (273); zur Übertragbarkeit des verfassungsrechtlichen Maßstabs für präventivpolizeiliche Eingriffsermächtigungen auf das Nachrichtendienstrecht BVerfG, Beschluss vom 27. Mai 2020 - 1 BvR 1873/13 -,Rn. 151.

[10] Warg, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, V § 1 Rn.40; Roth, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 4 BVerfSchG Rn. 131.

[11] BT-Ausschussdrs. 18(4)328 A; vgl. daneben Bergemann, NVwZ 2015, S. 1705 f.

7 – Die tatbestandlichen Voraussetzungen einer Datenspeicherung im nachrichtendienstlichen Informationssystem sind sehr niedrig angesetzt. Das Gesetz sieht weder einen besonderen Speicherungsanlass vor noch beschränkt es die Speicherung auf bestimmte Personenkreise.

– Die am Informationssystem teilnehmenden Behörden können die gespeicherten Daten umfassend abrufen, mit beliebigen Analysemethoden auswerten und weiterverarbeiten. Voraussetzung ist lediglich, dass dies zur Aufgabenerfüllung erforderlich ist. Damit ist ein besonderer Weiterverarbeitungsanlass nicht benannt. Das Gesetz ermöglicht auch etwa Datenabrufe und Datenanalysen aufgrund strategischer Erkenntnisinteressen oder zur Abrundung eigener Datenbestände.[12]

– Der durch das Informationssystem geschaffene umfassende Datenverbund der Verfassungsschutzbehörden greift damit intensiv in die Grundrechte der betroffenen Personen ein. Die äußerst weit gefassten Ermächtigungen zur Speicherung und Weiterverarbeitung personenbezogener Daten im Informationssystem verfehlen die grundrechtlichen Anforderungen weit.

III. Quellen-Telekommunikationsüberwachung

Die vorgesehene Ermächtigung der Nachrichtendienste zu Quellen-Telekommunikationsüberwachungen in § 11 Abs. 1a G 10-E i.V.m. § 3 G 10 weist mehrere verfassungsrechtliche Defizite auf: Sie enthält keine hinreichenden Vorkehrungen zum Schutz der IT-Sicherheit in der Bundesrepublik (unten 1), ermöglicht eine Datenerhebung auch außerhalb laufender Kommunikationsvorgänge (unten 2) und teilt im Übrigen die Mängel des bereits geltenden Rechts (unten 3).

1. Ausnutzung von IT-Sicherheitslücken

In tatsächlicher Hinsicht besteht ein Hauptproblem von Überwachungsmaßnahmen, die auf der Infiltration eines informationstechnischen Systems beruhen, in der Installation der Überwachungssoftware. Hierfür sind verschiedene Wege denkbar. Einer von ihnen besteht darin, Sicherheitslücken der Hardware oder der Software des Zielsystems auszunutzen. Dass dieser Infiltrationsweg tatsächlich ins Auge genommen wird, zeigt die vorgesehene Pflicht der Anbieter von Telekommunikationsdiensten in § 2 Abs. 1a Satz 1 Nr. 4 G 10-E, bei der Umleitung von Telekommunikation zu Infiltrationszwecken mitzuwirken. Eine Infiltration mithilfe eines technisch manipulierten Datenstroms muss zwar nicht zwangsläufig auf der Ausnutzung von Sicherheitslücken des Zielsystems oder seines informationstechnischen Umfelds (etwa eines Routers) beruhen. Dies dürfte aber das bedeutsamste Szenario sein.

Die Ausnutzung von IT-Sicherheitslücken zur Vorbereitung einer Quellen-Telekommunikationsüberwachung lässt sich jedoch nicht in jedem Fall verfassungsrechtlich legitimieren. Ihr steht partiell das von dem Bundesverfassungsgericht entwickelte Grundrecht auf Gewährleistung der

[12] Vgl. BVerfG, Beschluss vom 27. Mai 2020 - 1 BvR 1873/13 -,Rn. 218.

8 Vertraulichkeit und Integrität informationstechnischer Systeme[13] entgegen. Dieses Grundrecht vermittelt nicht nur ein subjektives Abwehrrecht gegen staatliche Eingriffe. Es begründet – wie schon der Begriff der Gewährleistung zeigt – auch eine staatliche Pflicht dazu beizutragen, dass die Sicherheit der informationstechnischen Infrastruktur der Bundesrepublik ein hohes Niveau erreicht. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme trägt so einerseits der hohen Bedeutung der Informationstechnik für die Funktionsfähigkeit von Staat und Gesellschaft, andererseits der erheblichen Verwundbarkeit dieser Technologie Rechnung.[14]

Die objektiv-rechtliche Dimension des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist praktisch hoch bedeutsam, weil solche Systeme strukturell bedingt stets eine Vielzahl von Sicherheitslücken aufweisen, die eigenständig zu Fehlfunktionen führen oder durch Dritte missbräuchlich ausgenutzt werden können. Die Sicherheit informationstechnischer Systeme ist daher als dauerhafte öffentliche Aufgabe anzusehen. Diese Aufgabe kann der Staat allerdings weitgehend nicht eigenhändig erfüllen, da es ihm hierfür sowohl an Ressourcen als auch an Expertise fehlt. In erster Linie obliegt es vielmehr den Herstellern und Betreibern von informationstechnischen Systemen und der darauf laufenden Software, vermeidbare Sicherheitslücken nicht entstehen zu lassen und später erkannte Sicherheitslücken zeitnah zu schließen. Die staatliche Gewalt kann hierbei lediglich eine unterstützende Rolle einnehmen. Welche Beiträge sie dazu übernimmt, hängt von Gestaltungsentscheidungen ab, für die das Grundgesetz beträchtliche Spielräume lässt. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist in seiner objektiv-rechtlichen Dimension erst verletzt, wenn die staatlichen Anstrengungen offenkundig unzureichend sind.[15]

Der grundrechtliche Mindeststandard wird allerdings zumindest dann unterschritten, wenn eine staatliche Stelle ohne zureichenden Grund eine Gefährdungslage für die Vertraulichkeit und Integrität der informationstechnischen Infrastruktur in der Bundesrepublik bewusst aufrechterhält oder sogar selbst schafft. Eine solche Situation kann im Zusammenhang mit Quellen-Telekommunikationsüberwachungen abhängig von dem genutzten Infiltrationsweg auftreten. Insbesondere ist dies der Fall, wenn für die Infiltration des Zielsystems eine noch unbekannte Sicherheitslücke von Hardware oder Software ausgenutzt wird (sogenannter Zero-Day).

Da ein Zero-Day dem Hersteller und den Nutzer*innen des betroffenen informationstechnischen Systems noch unbekannt ist, gibt es gegen ihn aus Sicht dieser Personen keine wirksamen Gegenmaßnahmen. Soweit die Sicherheitslücke sich prinzipiell durch eine Anpassung des Sys-

---

[13] BVerfGE 120, 274 (302 ff.).

[14] Vgl. etwa Sachs/Krings, JuS 2008, 481 (486); Kutscha, NJW 2008, 1042 (1044); Roßnagel/Schnabel, NJW 2008, 3534 (3535); Heckmann, in: FS Käfer, 2009, S. 129 (133 ff.); Hoffmann-Riem, JZ 2009, S. 165 ff.; ders., AöR 134 (2009), S. 513 ff.; ders., JZ 2014, S. 53 ff.; Becker, NVwZ 2015, 1335 (1339 f.).

[15] Vgl. zu aus unterschiedlichen Grundrechten hergeleiteten staatlichen Schutzpflichten etwa BVerfGE 49, 89 (142); 77, 17 (214 f.); 88, 203 (251 ff.); 92, 26 (46); 106, 28 (37); 125, 39 (78 f.); 143, 313 (337 f.); BVerfG, Beschluss vom 24. März 2021 - 1 BvR 2656/18 u.a. -, Rn. 143 ff.

9 tems (etwa ein Software-Update) schließen ließe, steht der dafür erforderliche technische Baustein noch nicht zur Verfügung. Für die ansonsten notfalls gebotene vollständige oder partielle Außerbetriebnahme des Systems besteht aus Sicht der betroffenen Personen kein Anlass, solange die Sicherheitslücke nicht bekannt ist.

Sicherheitsbehörden können Zero-Days ausnutzen, um informationstechnische Systeme zu infiltrieren und so eine Quellen-Telekommunikationsüberwachung zu ermöglichen. Dieser Infiltrationsweg erzeugt jedoch einen Zielkonflikt zwischen den Sicherheitsbelangen, denen die Maßnahme dient, und dem durch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität gewährleisteten Anliegen, dass der Staat zur Sicherheit der informationstechnischen Infrastruktur in der Bundesrepublik beiträgt.[16]

Im Sinne der Effektivität der Überwachungsmaßnahme muss die Sicherheitslücke möglichst lange geheim gehalten werden. Wird die Sicherheitslücke bekannt, besteht die Gefahr, dass sie geschlossen wird und darum die Infiltration von vornherein misslingt oder die Maßnahme vorzeitig abgebrochen werden muss. Selbst nach Beendigung der einzelnen Überwachungsmaßnahme besteht ein Anreiz, den Zero-Day weiterhin geheim zu halten, um ihn für weitere Quellen-Telekommunikationsüberwachungen nutzen zu können.

Die Ausnutzung von Zero-Days durch staatliche Stellen kann zugleich in mehrfacher Hinsicht die ohnehin gegebene Bedrohungslage für die informationstechnische Infrastruktur in der Bundesrepublik aufrechterhalten oder sogar noch verschärfen.

Wird eine Sicherheitslücke aus den eben genannten Gründen geheim gehalten, so trägt die handelnde Behörde durch ihr Unterlassen dazu bei, dass diese Sicherheitslücke nicht geschlossen wird. Da sich aus technischer Sicht die Infiltration informationstechnischer Systeme durch staatliche Stellen und durch Kriminelle nicht unterscheiden, perpetuiert dieses Unterlassen das Risiko krimineller Übergriffe auf die informationstechnische Infrastruktur.

Einen darüber hinausgehenden Beitrag zur Schwächung der Informationssicherheit in der Bundesrepublik leistet der Staat dann, wenn eine Behörde Informationen über eine Sicherheitslücke nicht selbst generiert, sondern von Dritten bezieht. Dies ist kein unrealistisches Szenario. So hat der Präsident der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) noch im Jahr 2018 eingeräumt, seine Stelle verfüge nicht über die technische Expertise, um Sicherheitslücken im benötigten Umfang selbst aufzudecken.[17] Werden Zero-Days auf dem Markt eingekauft, so stützt die beschaffende staatliche Stelle diesen Markt aktiv. Schon wegen der strengen strafrechtlichen Regulierung des Umgangs mit Informationen und Software, die zum Ausspähen oder Abfangen von Daten bestimmt sind (vgl. § 202c StGB), ist anzunehmen, dass die Akteure

---

[16] Vgl. BVerfGE 120, 274 (326), wo jedoch dieser Zielkonflikt nicht näher analysiert und darum aus ihm keine weiteren Folgerungen gezogen werden. Dies war in dem damaligen Verfahren auch nicht angezeigt, da die seinerzeit angegriffene Eingriffsermächtigung bereits die subjektiv-rechtlichen Anforderungen des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (weit) verfehlte.

[17] Vgl. https://www.heise.de/newsticker/meldung/Schlagabtausch-zu-ZITiS-IT-Sicherheitsluecken-schliessen-oder-ausnutzen-3976587.html.

10 auf diesem Markt regelmäßig zumindest in einem rechtlichen Graubereich agieren. Die staatliche Teilnahme an diesem Markt birgt darum das erhebliche Risiko, Straftaten zu begünstigen. Sie setzt zudem einen Anreiz für IT-Sicherheitsexpert*innen, ihr Wissen um Sicherheitslücken zu monetarisieren statt damit zur Stärkung der Informationssicherheit beizutragen. So kann die staatliche Marktteilnahme zur Stabilisierung auch des illegalen Marktes und zur Vermehrung der angebotenen Sicherheitslücken beitragen, die von Dritten aufgekauft und ausgenutzt werden können.

Eine staatliche Stelle, die über einen geheim gehaltenen Bestand von Informationen über Zero-Days verfügt, ist schließlich selbst ein lohnendes Angriffsziel für Kriminelle, die sich diese Informationen beschaffen und für eigene Zwecke nutzen wollen. Hierbei handelt es sich nicht um ein weitgehend hypothetisches Szenario, das als Restrisiko der staatlichen Aufklärung außer Acht bleiben könnte. Solche Angriffe liegen vielmehr ausgesprochen nahe und sind schon vorgekommen. So hat im Mai 2017 das Schadprogramm „WannaCry“ weltweit erhebliche Schäden verursacht. In Deutschland war davon etwa die Deutsche Bahn betroffen. Besonders schwer traf es das Gesundheitssystem in Großbritannien. Zahlreiche Rechner des National Health Service waren befallen. Die Daten von Krebs- und Herzpatient*innen standen nicht mehr zur Verfügung. Viele Kranke mussten in andere Kliniken umgeleitet werden. Dieses Schadprogramm nutzte eine Sicherheitslücke in Windows-Betriebssystemen aus, welche die kriminellen Angreifer nach verbreiteter Einschätzung bei der US-amerikanischen National Security Agency (NSA) ausgespäht hatten, die ihrerseits diese Sicherheitslücke für eigene Zwecke eingesetzt und geheim gehalten hatte.[18] Chinesische Spione sollen die Sicherheitslücke bereits im Jahr 2016 von der NSA erlangt und für eigene Angriffe genutzt haben.[19] Es liegt fern, dass deutsche Sicherheitsbehörden die bei ihnen vorhandenen Informationen über Sicherheitslücken bedeutend besser schützen können als die NSA. Vielmehr ist anzunehmen, dass sich ein Verlust nie ausschließen lässt. Mit vergleichbaren Vorfällen infolge einer Sammlung von Sicherheitslücken bei deutschen Behörden ist daher zu rechnen.

Werden die Risiken und die möglichen Erträge der staatlichen Infiltration informationstechnischer Systeme mithilfe von Zero-Days einander gegenübergestellt, so ergibt sich, dass dieser Infiltrationsweg ausgeschlossen werden muss.

Die durch die Nutzung und Geheimhaltung von Zero-Days eröffneten oder zumindest erhöhten Risiken wiegen äußerst schwer.

Zum einen kann der kriminelle Missbrauch der geheim gehaltenen Sicherheitslücken hochrangige Rechtsgüter empfindlich bedrohen. Nahezu alle lebenswichtigen Leistungen werden heute mit informationstechnischer Unterstützung erbracht. Ebenso verfügen so gut wie alle staatlichen und gesellschaftlichen Einrichtungen, deren Ausfall oder Funktionsstörung schwere Schäden verursachen kann, über informationstechnische Komponenten. Werden solche informations-

[18] Vgl. https://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung.
[19] Vgl. https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html.

11 technischen Komponenten gestört, so kann dies zu Leistungsausfällen oder Schadensereignissen führen, die schlimmstenfalls den Verlust von Menschenleben zur Folge haben können. Beispielsweise hat das Schadprogramm „WannaCry“, wie oben erwähnt, informationstechnische Systeme in britischen Krankenhäusern infiltriert. In der Folge mussten unter anderem geplante Operationen verschoben werden. Die Infiltration von Rechnern der Deutschen Bahn führte unter anderem zum Ausfall einer regionalen Leitstelle. Ein weiterer Angriff, der auf von der NSA erbeuteter Technologie basierte, hatte zur Folge, dass bei dem Arzneimittelunternehmen Merck ein kritischer Minderbestand eines Impfstoffs eintrat. Im September 2020 verstarb eine Patientin eines Wuppertaler Krankenhauses nach erfolgloser Behandlung. Sie hätte eigentlich in der Uniklinik Düsseldorf sein sollen, wo ihre Behandlung bereits eine Stunde früher als in Wuppertal hätte stattfinden können. Die Uniklinik war jedoch zu diesem Zeitpunkt aufgrund eines Ausfalls ihrer IT-Systeme von der Notfallversorgung abgemeldet. Hacker hatten eine Sicherheitslücke in der IT des Klinikums ausgenutzt, um 30 Server zu verschlüsseln und ein Lösegeld für deren Freigabe zu erpressen.[20]

Zum anderen erstreckt sich die Bedrohung durch den Missbrauch von Zero-Days auf praktisch die gesamte Bevölkerung, also ganz überwiegend auf Menschen, die für sicherheitsbehördliche Überwachungsmaßnahmen keinen Anlass geben. Es fehlt mithin vollständig an einer Zurechnungsbeziehung zwischen diesen Menschen und den Belangen, die der Geheimhaltung von Sicherheitslücken zugrunde liegen. Angesichts dessen und wegen der drohenden schweren Schäden ist die Grenze der Aufopferungspflicht der Betroffenen für das Gemeinwohl weit überschritten.

Hingegen wiegt der Effektivitätsverlust, der durch ein Verbot der Ausnutzung von Zero-Days für die Aufgabenerfüllung der Sicherheitsbehörden droht, weniger schwer. Dies gilt besonders für die Nachrichtendienste, die Überwachungsmaßnahmen anders als die Polizei nicht unmittelbar zur Abwehr konkreter Gefahren oder zur Verhütung von Straftaten einsetzen. Zwar hat der Beobachtungsauftrag des Verfassungsschutzes hohes Gewicht. Jedoch kann er zumeist auch auf weniger riskanten Wegen erreicht werden. So ist es aus objektiv-rechtlicher Sicht beispielsweise unbedenklich, wenn zur Infiltration des Zielsystems einer Quellen-Telekommunikationsüberwachung eine psychische Einflussnahme auf die Nutzer des Zielsystems *(Social Engineering)*, eine physische Zugriffsmöglichkeit auf das Zielsystem oder eine bereits bekannte, auf diesem System jedoch noch nicht geschlossene Sicherheitslücke ausgenutzt werden. Soweit im Einzelfall eine Infiltration auf diesen Wegen nicht möglich sein sollte, ist der damit verbundene Ausfall dieser Überwachungsmaßnahme hinzunehmen und auf andere, gegebenenfalls aufwändigere Maßnahmen auszuweichen.

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verpflichtet die staatliche Gewalt mithin dazu, auf die Nutzung und Geheimhaltung von Zero-Days zum Zweck der Infiltration informationstechnischer Systeme zu verzichten. Es ist Sache des Gesetzgebers, diese Pflicht durch ein ausdrückliches gesetzliches Verbot umzusetzen.

---

[20] Vgl. https://heise.de/-4904134.

12 Nur durch ein ausdrückliches Verbot erhalten die Sicherheitsbehörden eine eindeutige Vorgabe, die das objektiv-grundrechtlich nicht hinzunehmende Risiko für die Sicherheit der informationstechnischen Infrastruktur der Bundesrepublik sicher ausschließt. Dass es einer solchen Vorgabe bedarf, illustriert beispielhaft die Antwort der Bundesregierung auf eine parlamentarische Kleine Anfrage, in der die Bundesregierung im Jahr 2018 mit Blick auf das Bundeskriminalamt eine Nutzung von Zero-Days zumindest nicht ausgeschlossen hat:

> „Ob und inwieweit im Spannungsfeld technischer Erfordernisse, rechtlicher Vorgaben, sicherheits- und rechtspolitischer Erwägungen sowie taktischer Einsatzrahmenbedingungen zukünftig eine Nutzung sog. ‚Zero-Day-Exploits' für die Durchführung von Maßnahmen der Quellen-TKÜ und Online-Durchsuchung durch Sicherheitsbehörden in Betracht kommt, ist durch die zuständigen Stellen der Bundesregierung in Abstimmung mit den zu beteiligenden nationalen und ggf. internationalen Stellen und Gremien zu prüfen."[21]

Selbst wenn entgegen der oben begründeten Auffassung eine staatliche Infiltration informationstechnischer Systeme mithilfe von noch unbekannten Sicherheitslücken verfassungsrechtlich überhaupt rechtfertigungsfähig wäre, müsste die gesetzliche Grundlage der Infiltration zumindest Vorgaben für ein behördliches Schwachstellen-Management enthalten. Nur aufgrund prozeduraler Sicherungen und materieller Kriterien für ein solches Schwachstellen-Management kann das enorme Risiko für die informationstechnische Infrastruktur der Bundesrepublik hinnehmbar sein. In diesem Rahmen wäre ein Bündel von maßstabsbildenden Faktoren zu beachten, etwa

- die Verbreitung der Sicherheitslücke:
  - in quantitativer Hinsicht: Zahl der betroffenen Nutzer*innen,
  - in qualitativer Hinsicht: Art der betroffenen Nutzer*innen,
- das Gewicht der Sicherheitslücke:
  - zur Ausnutzung erforderlicher Aufwand,
  - aus der Ausnutzung resultierender Schaden,
- die Wahrscheinlichkeit, dass Betroffene die Ausnutzung der Lücke bemerken und im Einzelfall Gegenmaßnahmen einleiten,
- die Wahrscheinlichkeit einer technischen Lösung für die Lücke,

---

[21] Antwort der Bundesregierung auf Fragen 26 bis 31 einer Kleinen Anfrage, BT-Drs. 18/13413. Die Antwort auf diese Fragen ist eingestuft, aber online zugänglich unter https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/#Antwort-Drucksache-18-13566-NfD.

13 – die Wahrscheinlichkeit einer Verbreitung der technischen Lösung,

– Möglichkeiten zur Linderung der Folgen bei einer (zeitweisen) Geheimhaltung der Lücke,

– die Wahrscheinlichkeit, dass Dritte die Lücke finden.[22]

Da es an derartigen Schutzregelungen in der vorgesehenen Ermächtigung zu Quellen-Telekommunikationsüberwachungen vollständig fehlt, steht sie insgesamt mit dem Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme nicht in Einklang.

2. Zugriff auf gespeicherte Kommunikationsinhalte

Nicht mehr als Quellen-Telekommunikationsüberwachung darstellbar ist die in § 11 Abs. 1a Satz 2, Satz 3 Nr. 1 lit. b G 10-E vorgesehene Überwachung gespeicherter Kommunikationsinhalte.

Die eigenständige Regulierung der Quellen-Telekommunikationsüberwachung erklärt sich daraus, dass nach dem Bundesverfassungsgericht die Infiltration eines informationstechnischen Systems, mit deren Hilfe ausschließlich laufende Telekommunikation überwacht werden soll, materiell lediglich am Fernmeldegeheimnis des Art. 10 GG zu messen ist. Eine Ermächtigung zu Quellen-Telekommunikationsüberwachungen muss daher nicht den strengeren Anforderungen genügen, die sich für Online-Durchsuchungen aus dem Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ergeben. Die Beschränkung des Überwachungszugriffs auf laufende Telekommunikation muss rechtlich und tatsächlich gewährleistet sein.[23]

Demgegenüber beschränkt sich die geplante Ermächtigung gerade nicht auf laufende Kommunikation. Die Nachrichtendienste sollen vielmehr auch lokal gespeicherte Kommunikationsinhalte auslesen dürfen, wenn diese ab dem Zeitpunkt der Anordnung der Maßnahme Gegenstand eines Kommunikationsvorgangs waren. Solche ehemaligen Kommunikationsinhalte unterfallen jedoch gerade nicht dem Fernmeldegeheimnis.[24] Sollen sie mit Hilfe einer Infiltration des informationstechnischen Systems erhoben werden, auf dem sie gespeichert sind, so handelt es sich verfassungsrechtlich um eine Online-Durchsuchung und nicht um eine Quellen-Telekommunikationsüberwachung. Dieses Ergebnis, das aus einer Zuordnung der Schutzbereiche von Art. 10 GG und Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG auf der Grundlage der Rechtsprechung des Bundesverfassungsgerichts folgt, überzeugt auch bei wertender Betrachtung. Soll die Überwachung auf ehemalige Kommunikationsinhalte erstreckt werden, so reicht es nicht aus, die Kommunikationssoftware lediglich so zu manipulieren, dass bei einem Kommunikationsvorgang die über-

[22] Vgl. Herpig, Schwachstellen-Management für mehr Sicherheit, 2018, abrufbar unter https://www.stiftung-nv.de/sites/default/files/vorschlag.schwachstellenmanagement.pdf.
[23] BVerfGE 120, 274 (308 f.).
[24] Vgl. BVerfGE 115, 166 (183 ff.); 120, 274 (307 f.); 124, 43 (54).

14 mittelten Inhalte zeitgleich an die Überwachungsbehörde ausgeleitet werden. Stattdessen müssen die auf dem Zielsystem gespeicherten Kommunikationsinhalte ausgelesen werden, um festzustellen, welche von ihnen im Zeitraum nach der Anordnung übermittelt und gespeichert wurden. Eine solche Auswertung der lokal gespeicherten Daten ist ein typisches Erkennungsmerkmal einer Online-Durchsuchung.

Die Ausweitung der Quellen-Telekommunikationsüberwachung zu einer „kleinen Online-Durchsuchung“ hat zur Folge, dass die vorgesehene Ermächtigung die verfassungsrechtlichen Anforderungen verfehlt. Unabhängig davon, dass der in Bezug genommene § 3 G 10 schon als Ermächtigung zu Telekommunikationsüberwachungen unzureichend ist (siehe sogleich unter 3), genügt diese Regelung den Anforderungen an Online-Durchsuchungen noch weniger. So ermöglicht § 3 Abs. 2 Satz 2 G 10 eine gezielte Überwachung sogenannter Nebenbetroffener.[25] Online-Durchsuchungen dürfen sich hingegen nur gegen die verdächtige Person richten.[26]

3. Allgemeine Defizite des Artikel 10-Gesetzes

Abgesehen von den originären Defiziten der vorgesehenen Ermächtigung zu Quellen-Telekommunikationsüberwachungen führt diese Ermächtigung die zahlreichen verfassungsrechtlichen Mängel fort, die schon das geltende Recht auszeichnen. Diese seien im Folgenden lediglich knapp und ohne Anspruch auf Vollständigkeit skizziert:

- Es ist fragwürdig, ob das G 10 mit der Kompetenzordnung in Einklang steht, soweit dieses Gesetz auch Telekommunikationsüberwachungen durch Landesverfassungsschutzbehörden regelt. Richtigerweise lässt sich dieser Regelungsumfang mit dem auf die Regelung der Zusammenarbeit von Bund und Ländern beschränkten Kompetenztitel des Art. 73 Abs. 1 Nr. 10 lit. b und c GG nicht vereinbaren.[27]
- Die in § 3 Abs. 1 G 10 geregelten Eingriffsvoraussetzungen sind in weitem Umfang zu weit und zu unbestimmt formuliert. Das Gesetz ermöglicht eine Telekommunikationsüberwachung teilweise bereits dann, wenn lediglich die Planung von vergleichsweise geringfügigen Straftaten im Raum steht. Zu nennen sind etwa das Verbreiten von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB, Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 3 G 10), die Zuwiderhandlung gegen ein Vereinsverbot (§ 20 Abs. 1 Nr. 1 bis 4 VereinsG, Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 3 G 10) und die Zugehörigkeit zu einer geheim gehaltenen Vereinigung von Ausländern (§ 95 Abs. 1 Nr. 8 AufenthG, Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 7 G 10). Darüber hinaus führt der Überwachungsansatz bereits im Planungsstadium im Zusammenwirken mit Straftatbeständen wie der Vorbereitung einer schweren staatsgefährden-

[25] Vgl. zum Begriff Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 3 G 10 Rn. 33.
[26] Vgl. BVerfGE 141, 220 (273 f.).
[27] Bäcker, DÖV 2011, S. 840 (844); ders., GSZ 2018, 213 (215 f.); Bergemann, NVwZ 2015, S. 1705 (1706); Pieroth, in: Jarass/Pieroth, GG, Art. 87 Rn. 5; a.A. Risse/Kathmann DÖV 2012, 555 ff.; Gärditz AöR 144 (2019), 81 (91 ff.); Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, Rn. 20 vor § 1 G 10.

15 den Gewalttat (§ 89a StGB, Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 2 G 10) oder der Beteiligung an einer terroristischen Vereinigung (§ 129a StGB, Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 6 lit. a G 10) zu einer weitreichenden Entgrenzung des tatsächlichen Überwachungsanlasses.

– Gleichfalls zu weit geraten sind die in § 4 Abs. 4 Satz 1 G 10 enthaltenen Ermächtigungen zur Übermittlung von Daten, die durch eine Überwachungsmaßnahme gewonnen wurden.

– Die Zurückstellung der grundrechtlich gebotenen Mitteilung an die betroffene Person wird in § 12 Abs. 1 Satz 2 G 10 deutlich zu pauschal und in zu weitem Umfang ermöglicht.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)844 B

Anlage A

Thomas Haldenwang
Präsident des BfV

Berlin, 14. Mai 2021

Schriftliche Stellungnahme

Seit den letzten wesentlichen Änderungen des Verfassungsschutzrechts sind sechs Jahre vergangen, in denen sich sowohl das Kommunikationsverhalten in der Gesellschaft als auch das Kommunikationsverhalten von Terroristen weiterhin verändert hat. Seitdem sind auch weitere Jahre vergangen, in denen sich verfassungsfeindliche Bestrebungen verändert haben: ihre Zusammensetzung, ihre Agitationsräume, ihre Radikalisierung und ihre Inszenierungen in der virtuellen und in der realen Welt unterliegen mehr denn je dem (digitalen) Wandel der Zeit. Diese Entwicklungen führen zwangsläufig zu neuen, fachlichen Bedarfen, die das bestehende Gesetz nicht in Gänze abzudecken vermag. Der Bereich der inneren Sicherheit ist den aktuellen Entwicklungen derart unterworfen, dass folgerichtig die gesetzlichen Regelungen dringend an die Veränderungen angepasst werden müssen.

So stellt die geplante Stärkung des personenbezogenen Aufklärungsansatzes eine entscheidende Verbesserung für die Bearbeitung von (noch) nicht gewaltorientierten Einzelpersonen – insbesondere bei der Erstbearbeitung von Internetsachverhalten dar. Insbesondere die Radikalisierung von Einzelpersonen, die im Internet agieren und dabei oftmals keine strukturelle Einbindung in Organisationen oder Gruppierungen haben, muss noch vor der Verfestigung einer Gewaltorientierung in den Blick genommen werden.

Gerade die Gewalttaten von Halle 2019 und Hanau 2020 sind deutliche Belege dafür, dass sich neue rechtsterroristische Ansätze gänzlich außerhalb der klassischen rechtsextremistischen Personenzusammenschlüsse entwickeln können.

Durch die geplante Neuregelung wird dem BfV ermöglicht, einschlägige Personenkreise zu einem früheren Zeitpunkt bearbeiten und Radikalisierungsverläufe von Einzelpersonen daher frühzeitiger erkennen zu können.

Daneben dürften die jüngst bekannt gewordenen Verdachtsfälle im Bereich des Rechtsextremismus innerhalb der Bundeswehr Anlass genug dafür geben, vorliegende Erkennt-

nisse der Behörden in diesem Bereich systemisch enger zu verzahnen, um Informationsverluste bei einer Gefährdungseinschätzung von Einzelpersonen zu vermeiden. Der Gesetzesentwurf schafft hier die notwendigen rechtlichen Voraussetzungen zur Ermöglichung einer Vollanbindung des BAMAD an das Nachrichtendienstliche Informationssystem.

Aus Sicht des Bundesamtes für Verfassungsschutz ist darüber hinaus die nun vorgesehene mehrstufige Kontrolle durch die unabhängige G10-Kommission ein richtiger Schritt. Die Anpassungen im Artikel 10-Gesetz zur Erhöhung der Anzahl der Kommissionsmitglieder sowie der Anzahl der Mitglieder mit Befähigung zum Richteramt wird daher ausdrücklich begrüßt. Und auch die Einführung eines technischen Sachverständigen wird klar befürwortet. Die Anpassungen stärken das Vertrauen der Gesellschaft in ein effektives Kontrollorgan und somit auch in die Arbeit des Bundesamtes für Verfassungsschutz.

Die Einführung der Befugnis zur Quellen-TKÜ ist im Hinblick auf das heutige Kommunikationsverhalten von Terroristen dringend geboten. Das Kommunikationsaufkommen über Messenger-Dienste wie Facebook, WhatsApp oder Telegram nimmt in allen Beobachtungsfeldern des Verfassungsschutzes exponentiell zu. Die Möglichkeit zur Detektion der Kommunikation über diese Dienste ist aufgrund komplexer Transportverschlüsselung und stetem technischem Wandel stark eingeschränkt. Die Quellen-TKÜ ist daher ein dringend notwendiges Instrument, um auf die gewandelten Kommunikationsgewohnheiten reagieren zu können und die Erkenntnislücken, die durch das Phänomen „going dark“ entstanden sind, im Einzelfall für hochgefährliche Personen kompensieren zu können. Hierbei handelt es sich auch nicht um ein Instrument der „Massenüberwachung“, sondern um eine nur unter den strengen Voraussetzungen des Artikel 10-Gesetzes zu ergreifende, individuelle Maßnahme, die wiederum einer qualifizierten Kontrolle unterliegt.

Das aktuelle Beispiel der sog. „Gruppe S.“ demonstriert deutlich, dass das Instrument der Quellen-TKÜ im virtuellen Raum nötig ist, um der gesetzlich vorgesehenen Frühwarnfunktion des Verfassungsschutzes Rechnung zu tragen. Die sog. „Gruppe S.“ ist eine rechtsextremistische Gruppierung, die verdächtigt wird, Anschläge auf ausgesuchte Moscheen geplant zu haben um dabei die anwesenden Besucher zu töten oder zumindest schwer zu verletzen. Die Gruppierung hatte sich in Chatgruppen organisiert und in diesen

insbesondere die Rekrutierung weiterer Mitglieder vorangetrieben. Durch die Befugnis zur Quellen-TKÜ kann in derartigen Fällen Ausmaß und Qualität des Gruppenumfangs, des Umfeldes und der Protagonisten wesentlich besser und früher aufgeklärt und eine zielgenaue Gefährdungseinschätzung der Gruppierung getroffen werden, mit deren Hilfe dann schwerste Gewalttaten verhindert werden können.

Die täglichen Nachrichten zeigen, dass die vielfältigen Gefahren für die Freiheit und Sicherheit in Deutschland durchaus konkret sind und keinesfalls unterschätzt werden dürfen. Umso wichtiger ist es, dass die Sicherheitsbehörden sich auch technologisch auf der Höhe der Zeit befinden und mit dem digitalen Wandel mithalten können. Es geht dabei nicht um eine materielle Erweiterung der Eingriffsbefugnisse des Verfassungsschutzes, sondern um einen bestmöglichen Kompetenzerhalt für unseren demokratischen Rechtsstaat und im Sinne der freiheitlichen demokratischen Grundordnung. Der Verfassungsschutz ist auf die Anpassung der Gesetzeslage daher dringend angewiesen, um weiterhin erfolgreiche Arbeit leisten zu können.

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

15. Mai 2021

Dr. Benjamin Rusteberg
z. Zt. Vertreter des Lehrstuhls für Öffentliches Recht,
insb. Kirchenrecht und Staatskirchenrecht
Georg-August-Universität Göttingen
Goßlerstraße 11
37073 Göttingen

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)844 D

Stellungnahme

zur Vorbereitung der öffentlichen Anhörung des

Ausschusses für Inneres und Heimat des Deutschen Bundestages

zum

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts

BT-Drucksachen 19/24785, 19/24900

Aufgrund der überaus knapp bemessenen Zeit für die Vorbereitung der Anhörung kann im Folgenden nicht zu sämtlichen Punkten und allen Anträgen Stellung genommen werden. Deshalb beschränken sich die folgenden Ausführungen auf den Gesetzesentwurf der Bundesregierung und bei diesem auf diejenigen Punkte, die als besonders relevant angesehen werden.

A. Vorbemerkungen

Die Nachrichtendienste werden in der Bundesrepublik traditionell insbesondere von der Polizei aber auch von den Strafverfolgungsbehörde und von anderen Verwaltungsbehörden abgegrenzt, die über außenwirksame Exekutivbefugnissen verfügen. Man spricht hier von dem sogenannten Trennungsgebot.

Insbesondere vor dem Hintergrund dieses Trennungsgebots kann jedoch die Frage, wie das Verhältnis der Nachrichtendienste – insbesondere der Verfassungsschutzämter – zu den übrigen Sicherheitsbehörden ausgestaltet ist und welche Funktion die Nachrichtendienste in der bundesdeutschen Sicherheitsarchitektur einnehmen, nach wie vor nicht wirklich befriedigend beantwortet werden kann.

Nach § 1 Abs. 1 BVerfSchG dient der Verfassungsschutz dem Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes und der Länder. Aufgabe der

Verfassungsschutzbehörden soll gem. § 3 Abs. 1 BVerfSchG die Sammlung und Auswertung von Informationen über eben solche Bestrebungen sein, die sich gegen die freiheitlich demokratisch Grundordnung richten bzw. Bestand und Sicherheit des Bundes und der Länder gefährden.

Das Sammeln von Informationen allein, schützt aber weder den Staat noch die Verfassung. Informationen zu sammeln ist kein Selbstzweck. Vielmehr kommt es darauf an, was mit diesen Informationen geschehen soll.

Das Bundesverfassungsschutzgesetz enthält zu dieser Frage bemerkenswerterweise keinerlei Angaben. In einigen Landesverfassungsschutzgesetzen wird die Aufgabe hingegen ausdrücklich dahingehend bestimmt, dass die Verfassungsschutzämter es den zuständigen Stellen zu ermöglichen haben, „rechtzeitig die erforderlichen Maßnahmen zur Abwehr von Gefahren für die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes und der Länder zu treffen."[1]

Auch diese Normierung wirft jedoch mehr Fragen auf, als sie beantwortet. So bleibt weiterhin unbenannt, welches diese Stellen sind, die die erforderlichen Abwehrmaßnahmen zu treffen haben.

Sollen dies gerade die Behörden sein, die über Exekutivbefugnisse verfügen, stellt sich die Frage, was vom Trennungsgebot bleibt, wenn die Aufgabe der Verfassungsschutzbehörden in erster Linie darin besteht, diesen Informationen zuzuliefern. Zugleich ist zu fragen, warum diese Aufgabe dann nicht einfach von den polizeilichen Staatsschutzabteilungen übernommen wird, deren Befugnisse zur Informationserhebung hinter denen des Verfassungsschutzes keineswegs zurückstehen.[2]

Legt man demgegenüber bei der Nutzung der Informationen den Schwerpunkt auf die Information der jeweiligen Bundes- bzw. Landesregierung stellt sich namentlich bei den Verfassungsschutzbehörden – beim BND mag dies in gewissem Rahmen anders sein – die Frage, ob für diese Aufgabe wirklich ein umfangreiches Arsenal an Befugnissen zur heimlichen Überwachung vonnöten ist. Dies gilt umso mehr, wenn man die Kosten in Betracht zieht, den der Einsatz derartiger Mittel für die Arbeit der übrigen Sicherheitsbehörden und die Allgemeinheit mit sich bringen kann.

Diese Problematik der nach wie vor ungeklärten Aufgabe des Verfassungsschutzes und der Rolle, die ihm in der bundesdeutschen Sicherheitsarchitektur zukommen soll, zieht sich auch durch den vorliegenden Gesetzesentwurf:

- § 4 Abs. 1 BVerfSchG-E bekräftigt die Rolle des Bundesamtes für Verfassungsschutz (BfV) noch weiter, indem anstelle von Strukturen verstärkt als gefährlich angesehene Einzelpersonen beobachtet werden sollen;
- § 11 Abs. 1a G10-E will den Nachrichtendiensten zusätzliche Befugnisse zu heimlichen Überwachungsmaßnahmen einräumen, die bislang Polizei- und Strafverfolgungsbehörden

[1] § 2 II 2 HessVSG; vgl. § 3 I BW ; § 1 II Th VSG.

[2] Vgl. hierzu R. Poscher/B.Rusteberg, Die Aufgabe des Verfassungsschutzes, KJ 2014, 57 ff.; dies., Ein Kooperationsverwaltungsrecht des Verfassungsschutzes?, in: Dietrich/Gärditz/Graulich/Gusy/Warg (Hrsg.), Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S.145 ff.; B. Rusteberg, Informationsherrschaft durch Polizei und Nachrichtendienste, in: Kulick/Goldhammer (Hrsg.), Der Terrorist als Feind?, 2020, S. 215 ff.

vorbehalten waren; dennoch sollen an den Einsatz derartiger Maßnahmen durch die Nachrichtendienste geringere Anforderungen zu stellen sein als bei den letztgenannten;

- § 2 Abs. 1a u. 1b G10-E soll den Nachrichtendiensten umfassende tatsächliche Zugriffs- und Manipulationsmöglichkeiten des gesamten Datenverkehrs im Bereich der Telekommunikation einräumen, die weit über das hinausgehen, was Polizei- und Strafverfolgungsbehörden möglich ist.

B. Artikel 1 – Änderung des Bundesverfassungsschutzgesetzes: Nummer 1 - § 4 Abs. 1 BVerfSchG-E

Geltende Gesetzeslage	Gesetzesentwurf	Neufasssung
§ 4 Begriffsbestimmungen (1) [1][…] [2]Für einen Personenzusammenschluß handelt, wer ihn in seinen Bestrebungen nachdrücklich unterstützt. [3]Voraussetzung für die Sammlung und Auswertung von Informationen im Sinne des § 3 Abs. 1 ist das Vorliegen tatsächlicher Anhaltspunkte. [4]Verhaltensweisen von Einzelpersonen, die nicht in einem oder für einen Personenzusammenschluß handeln, sind Bestrebungen im Sinne dieses Gesetzes, wenn sie auf Anwendung von Gewalt gerichtet sind oder aufgrund ihrer Wirkungsweise geeignet sind, ein Schutzgut dieses Gesetzes erheblich zu beschädigen.	**1. § 4 Absatz 1 wird wie folgt geändert:** a) Nach Satz 2 werden die folgenden Sätze eingefügt: „Bestrebungen im Sinne des § 3 Absatz 1 können auch von Einzelpersonen ausgehen, die nicht in einem oder für einen Personenzusammenschluss handeln. In diesem Fall gilt Satz 1 mit der Maßgabe, dass die Verhaltensweise der Einzelperson darauf gerichtet sein muss, die dort genannten Ziele zu verwirklichen.“ b) Der neue Satz 6 wird aufgehoben.	**§ 4 Begriffsbestimmungen** (1) [1][…] [2]Für einen Personenzusammenschluß handelt, wer ihn in seinen Bestrebungen nachdrücklich unterstützt. [3]Bestrebungen im Sinne des § 3 Absatz 1 können auch von Einzelpersonen ausgehen, die nicht in einem oder für einen Personenzusammenschluss handeln. [4]In diesem Fall gilt Satz 1 mit der Maßgabe, dass die Verhaltensweise der Einzelperson darauf gerichtet sein muss, die dort genannten Ziele zu verwirklichen. [5]Voraussetzung für die Sammlung und Auswertung von Informationen im Sinne des § 3 Abs. 1 ist das Vorliegen tatsächlicher Anhaltspunkte.

I. Gesetzesbegründung

Nach Art. 1 Nr. 1 des Entwurfs eines Gesetzes zur Anpassung des Verfassungsschutzrechts soll § 4 Abs.1 BVerfSchG dahingehend geändert werden, dass zukünftig die Beobachtung von Einzelpersonen unter denselben Voraussetzungen möglich ist, wie die Beobachtung von Personenzusammenschlüssen. Letztere bilden bislang den primären Gegenstand der Beobachtungstätigkeit, während Einzelpersonen gem. § 4 Abs. 1 S. 4 BVerfSchG, soweit sie nicht in einem oder für einen Personenzusammenschluss handeln, nur dann relevante Bestrebungen und damit ein zulässiges Beobachtungsobjekt darstellen, wenn ihre Verhaltensweisen „auf Anwendung von Gewalt gerichtet sind oder aufgrund ihrer Wirkungsweise geeignet sind, ein Schutzgut dieses Gesetzes erheblich zu beschädigen“.

Begründet wird die vorgesehene Änderung damit, dass „unter den Bedingungen der digitalen Moderne und Erkenntnissen zu Radikalisierungsverläufen“ nicht daran festgehalten werden könne, dass „bei Bestrebungen einerseits von Personenzusammenschlüssen und andererseits von Einzelpersonen grundsätzlich unterschiedlichen Bedrohungseinschätzung“ bestünden.[3] Beispielsweise eröffneten soziale Medien Einzelpersonen eine enorme Wirkungsbreite für Agitation und Hassbotschaften. Zudem erfordere die „Frühwarnfunktion des Verfassungsschutzes gerade nach den Anschlägen in Halle am 9. Oktober 2019 und Hanau am 19. Februar 2020 angesichts eruptiver Radikalisierungsverläufe von Einzelpersonen, Extremisten bereits im Vorfeld militanter Handlungen besser in den Blick nehmen zu können“. Die neue Regelung trage dem Rechnung, sehe dabei aber eine besondere Würdigung des Einzelfalls vor, „indem – anders als bei Personenzusammenschlüssen – zu Einzelpersonen ein Entschließungsermessen auszuüben ist, bei dem im Kern die Schutzgutrelevanz des Sachverhalts – auch in seinem Entwicklungspotenzial – zu beurteilen“ sei. Eine solche Risikoabschätzung sei bereits im Rahmen des personenbezogenen Bearbeitungsansatzes der Sicherheitsbehörden methodisch etabliert, etwa bei der sicherheitsbehördlichen Priorisierung in der Gefährderbearbeitung.

II. Rechtliche Bewertung

Die für die vorgesehene Gesetzesänderung gegebene Begründung kann nicht überzeugen. Insbesondere sprechen die angeführten Anschlägen von Halle und Hanau keineswegs für die Notwendigkeit einer derartigen Änderung.

Dies folgt schon daraus, dass in beiden Fällen die Verhaltensweise gerade auf die „Anwendung von Gewalt“ gerichtet waren, und somit auch bereits nach der geltenden Rechtslage in den Aufgabenbereich des Verfassungsschutzes fielen. Auch nach der geltenden Rechtslage ist es nach dem klaren Wortlaut von § 4 Abs. 1 S. 3 u. 4 BVerfSchG keineswegs so, dass die zu beobachtende Einzelperson etwaige Gewalthandlungen bereits begangen haben muss. Vielmehr reichen Anhaltspunkte aus, dass sie entsprechende Absichten verfolgt.

Die im Entwurf vorgesehene Änderung erweist sich damit in erster Linie als Ausdruck des bereits angesprochenen Bemühens, die Aufgabe des Verfassungsschutzes vom Ziel einer Strukturaufklärung weg, hin zu einer Zuständigkeit als besondere Gefahrenabwehrbehörde zu entwickeln. Damit vertiefen sich freilich die oben angesprochenen Zweifel an dem Eigenwert, der einer derartigen Behörde gegenüber den ebenfalls über umfassende Möglichkeiten der Informationsvorsorge verfügenden Polizeien zukommt. Zudem stellt eine solche Rolle des Verfassungsschutzes in letzter Konsequenz das Trennungsgebot in Frage. Ohne dieses verschwinden aber auch jegliche Argumente, warum die Anforderungen an die Eingriffsschwellen bei Überwachungsmaßnahmen der Nachrichtendienste nach dem G10 gegenüber Maßnahmen nach den Polizeigesetzen und der StPO abgesenkt werden sollten.

Dabei geht die Entwurfsbegründung in nicht nachvollziehbarerweise von der Existenz eines Entschließungsermessens des BfV nach § 4 Abs. 1 BVerfSchG-E aus.[4] Soweit die Entwurfsbegründung diesbezüglich auf die Notwendigkeit einer Risikoabschätzung verweist, die „bereits im Rahmen des personenbezogenen Bearbeitungsansatzes der Sicherheitsbehörden methodisch etabliert“ sei,[5] drängt

[3] BT-Drs. 19/24785, S. 17.
[4] BT-Drs. 19/24785, S. 17; dazu 19(4)844 A - Stellungnahme Prof. Dr. Matthias Bäcker, S. 6.
[5] BT-Drs. 19/24785, S. 17.

sich der Verdacht auf, dass die Gesetzesänderung in erster Linie zur nachträglichen Legitimation einer bereits jetzt contra legem eingeübten behördlichen Praxis dienen soll.

C. Artikel 5 – Änderung des Artikel 10-Gesetzes

I. Nummer 7 lit. a) - § 11 Abs. 1a G10-E

7. § 11 wird wie folgt geändert:

a) Nach Absatz 1 werden die folgenden Absätze 1a und 1b eingefügt:

„(1a) 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. Bei den Maßnahmen nach den Sätzen 1 und 2 ist technisch sicherzustellen, dass

1. ausschließlich überwacht und aufgezeichnet werden können:

   a) die laufende Kommunikation (Satz 1) und

   b) Inhalte und Umstände der Kommunikation, die auch während des laufenden Kommunikationsvorgangs ab dem Zeitpunkt der Anordnung im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können (Satz 2),

2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind,

3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen. Bei jedem Einsatz sind zu protokollieren:

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

4. die Organisationseinheit, die die Maßnahme durchführt. […]

1. Übersicht

a) Gesetzesbegründung

Ausweislich der Entwurfsbegründung soll mit Artikel 5 Nr. 7 lit. a) eine Aufklärungslücke geschlossen werden, die sich aufgrund der gegenwärtigen Entscheidungspraxis der G10-Kommission bei sog. Messengerdiensten ergebe, die technisch aus dem Speicherplatz des Endgeräts – unverschlüsselt –

ausgelesen werden müssten („ruhende Kommunikation“). Diese Lücke werde mit der Regelung in Absatz 1a Satz 2 geschlossen. Diese orientiere sich an dem Modell der Strafprozessordnung (§ 100a Abs. 1 S. 2 u.3 sowie Absatz 5 und 6).[6]

b) Vergleich mit bestehenden Regelungen

§ 11 G10 - Neufassung	**§ 100a StPO**	**§ 51 BKAG**
(1a)	(1) [1] […]	(2)
[1]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.	[2]Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen.	[1]Die Überwachung und Aufzeichnung der Telekommunikation darf ohne Wissen der betroffenen Person in der Weise erfolgen, dass mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird, wenn […]
[2]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. […]	[3]Auf dem informationstechnischen System des Betroffenen 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.	

[6] BT-Drs. . 19/24785, S. 22 f.

(1a) […] [3]Bei den Maßnahmen nach den Sätzen 1 und 2 ist technisch sicherzustellen, dass	(5) Bei Maßnahmen nach Absatz 1 Satz 2 und 3 ist technisch sicherzustellen, dass	(2) […] wenn
1. ausschließlich überwacht und aufgezeichnet werden können:	1. ausschließlich überwacht und aufgezeichnet werden können:	1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird und
a) die laufende Kommunikation (Satz 1) und	a) die laufende Telekommunikation (Absatz 1 Satz 2), oder	2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.
b) Inhalte und Umstände der Kommunikation, die auch während des laufenden Kommunikationsvorgangs ab dem Zeitpunkt der Anordnung im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können (Satz 2),	b) Inhalte und Umstände der Kommunikation, die ab dem Zeitpunkt der Anordnung nach § 100e Absatz 1 auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können (Absatz 1 Satz 3),	§ 49 Absatz 2 gilt entsprechend. § 49 bleibt im Übrigen unberührt.
		§ 49 BKAG
2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind,	2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und	(2) Es ist technisch sicherzustellen, dass
3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.	3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.	1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
		2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.
[4]Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.	Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.	Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

[5]Bei jedem Einsatz sind zu protokollieren:	(6) Bei jedem Einsatz des technischen Mittels sind zu protokollieren	→ **§ 82 BKAG**
1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,	1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,	
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,	2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,	
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und	3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und	
4. die Organisationseinheit, die die Maßnahme durchführt.	4. die Organisationseinheit, die die Maßnahme durchführt.	

Wie bereits die Gesetzesbegründung deutlich macht, orientiert sich die vorgeschlagene Regelung an § 100a Abs. 1 S. 2 u. 3, Abs. 5 u. 6 StPO. Diese wurden mit dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017[7] in die Strafprozessordnung eingefügt.

Insbesondere in der Rechtsfolge stimmen § 100a Abs. 1 S. 3 StPO und § 11 Abs.1a S. 2 G10-E dahingehend überein, dass sie den Eingriff in ein informationstechnisches System nicht nur für die Überwachung der laufenden Telekommunikation, sondern auch für Inhalte und Umstände der Kommunikation zulassen, die ab dem Zeitpunkt der Anordnung gespeichert wurden, wenn diese hypothetisch auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.

Beide Regelungen gehen damit insbesondere über § 51 Abs. 2 BKAG hinaus, der lediglich die Überwachung und Aufzeichnung laufender Telekommunikation erlaubt, wenn dafür mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird.

2. Verfassungsrechtliche Maßstäbe

Die auf § 11 Abs. 1a G10-E anwendbaren verfassungsrechtlichen Maßstäbe unterscheiden sich signifikant, je nachdem ob in der Regelung ein Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG enthalten ist, oder sie sich auf Eingriffe in das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG bzw. das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG beschränkt.

[7] BGBl. 2017 I, S. 3202 ff.

a) Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt vor einem Zugriff auf informationstechnische Systeme zur geheimen Durchführung von Online-Durchsuchungen, mit denen private, von den Betroffenen auf eigenen oder vernetzten fremden Computern (wie etwa der sogenannten Cloud) abgelegte oder hinterlassene Daten erhoben werden können und die es ermöglichen, das Verhalten der Betroffen im Netz nachzuvollziehen.[8]

Nach der Rechtsprechung des Bundesverfassungsgerichts trägt die Verfassung mit dieser eigenständigen Ausprägung des allgemeinen Persönlichkeitsrechts der heute weit in die Privatsphäre hineinreichenden Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung Rechnung. Wegen der oft höchstpersönlichen Natur dieser Daten, die sich insbesondere auch aus deren Verknüpfung ergebe, sei ein Eingriff in dieses Grundrecht von besonderer Intensität und seinem Gewicht nach mit dem Eingriff in die Unverletzlichkeit der Wohnung vergleichbar.[9]

Für Eingriffe in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gelten deshalb besonders strenge Anforderungen: Insbesondere müssen die gesetzlichen Ermächtigungsgrundlagen vorsehen, dass mindestens tatsächliche Anhaltspunkte für eine im Einzelfall drohende konkrete Gefahr für ein überragend wichtiges Rechtsgut vorliegen.[10]

b) Fernmeldegeheimnis, Art. 10 Abs. 1 GG

Der Schutz des Fernmeldegeheimnisses bezieht sich nach der Rechtsprechung des Bundesverfassungsgerichts auf alle mittels der Fernmeldetechnik ausgetauschten Informationen und umfasst sowohl den Kommunikationsinhalt als auch die Kommunikationsumstände. Die öffentliche Gewalt soll grundsätzlich nicht die Möglichkeit haben, sich Kenntnis vom Inhalt der über Fernmeldeanlagen abgewickelten mündlichen oder schriftlichen Information zu verschaffen.[11] Eines besonderen grundrechtlichen Schutzes bedarf es aufgrund der spezifischen Verletzlichkeit, sobald Informationen unter Einschaltung eines Kommunikationsmittlers über eine Distanz hinweg ausgetauscht werden.[12]

Dabei hat das Bundesverfassungsgericht zwar auch Zugriffe „am Endgerät“ in den Schutzbereich des Art. 10 Abs. 1 GG einbezogen. Nicht mehr durch Art. 10 Abs. 1 GG geschützt sind aber Zugriffe auf ehemalige oder zukünftige Kommunikationsinhalte oder Kommunikationsumstände im Machtbereich

[8] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220, Rn. 209; BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274, Rn. 201 ff.
[9] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 210.
[10] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 212; BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274, Rn. 242 ff.
[11] BVerfG, Urteil vom 27. Juli 2005 – 1 BvR 668/04 –, BVerfGE 113, 348-392, Rn. 82.
[12] U. Buermeyer, Zum Begriff der »laufenden Kommunikation« bei der Quellen-Telekommunikationsüberwachung (»Quellen-TKÜ«), StV 2013, 470 (473), m.w.N.

der Kommunikationspartner: Sobald der Kommunikationsinhalt beim Empfänger angekommen ist, endet der Schutz des Art. 10 Abs. 1 GG.[13]

Ein Eingriff in das Fernmeldegeheimnis liegt demnach vor, wenn staatliche Stellen sich ohne Zustimmung der Beteiligten Kenntnis von dem Inhalt oder den Umständen eines fernmeldetechnisch vermittelten Kommunikationsvorgangs verschaffen.[14]

Für die Eingriffsintensität einer konkreten Maßnahme bedeutsam ist u.a. die Streubreite der Eingriffe, insofern nicht nur potenziellen Störer oder Straftäter erfasst werden, sondern alle, mit denen diese in dem betreffenden Zeitraum Telekommunikationsverbindungen nutzen.[15] Zur weiteren Intensivierung des Eingriffs trägt bei, dass die Betroffenen den Überwachungsmaßnahmen in einer Situation vermeintlicher Vertraulichkeit ausgesetzt sind.[16] Noch weitere werde die Schwere des Eingriffs durch eine Datenerhebung im Vorfeld erhöht, da hieraus die Möglichkeit einer Verwendung der erhobenen Daten zu unbestimmten oder noch nicht bestimmbaren Zwecken resultiere.[17]

Für die Rechtfertigung setzen Eingriffe in das Fernmeldegeheimnis grundsätzlich hinreichend gewichtige Schutzgüter sowie ausreichend konkretisierte Eingriffsschwellen voraus.[18]

c) Einordnung und Voraussetzungen der sog. Quellen-TKÜ

aa) Schutzbereichsausnahme

Der Begriff „Quellen-TKÜ“ bezeichnet die Telekommunikationsüberwachung durch Infektion des verwendeten Endgeräts mit einer Überwachungssoftware, dem sog. Trojaner. Sie bezieht sich damit insbesondere auf Telefongespräche, die nicht über klassische Telefonverbindungen, sondern über das Internet geführt werden, aber etwa auch auf E-Mails, Chats und Messengerdienste oder die Inhalte aufgerufener WWW-Seiten. Der technische Nutzen der Quellen-TKÜ besteht darin, dass die Daten in den beteiligten Rechnern oder Smartphones regelmäßig noch vor dem Versand der Daten über das Internet verschlüsselt werden. Ein erfolgversprechender Zugriff auf solche Kommunikation ist daher regelmäßig nicht durch Zugriff entlang der Übertragungsstrecke, sondern nur noch durch das „Anzapfen“ eines der beteiligten Endgeräte möglich, um dort die noch bzw. bereits wieder entschlüsselten Daten „an der Quelle“ abgreifen zu können.[19]

Das Bundesverfassungsgericht hat diese sog. Quellen-TKÜ privilegiert, indem es für sie eine Schutzbereichsausnahme vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vorgenommen hat: Obwohl sich die Quellen-TKÜ gerade dadurch auszeichnet, dass bei ihr verdeckte Eingriffe in informationstechnische Systeme notwendig sind, soll sie grundsätzlich keinen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und

---

[13] U. Buermeyer, Zum Begriff der »laufenden Kommunikation« bei der Quellen-Telekommunikationsüberwachung (»Quellen-TKÜ«), StV 2013, 470 (473), m.w.N.
[14] BVerfG, Beschluss vom 12. Oktober 2011 – 2 BvR 236/08 –, BVerfGE 129, 208-268, Rn. 198 f.
[15] BVerfG, Urteil vom 27. Juli 2005 – 1 BvR 668/04 –, BVerfGE 113, 348-392, Rn. 142.
[16] BVerfG, Urteil vom 27. Juli 2005 – 1 BvR 668/04 –, BVerfGE 113, 348-392, Rn. 143.
[17] BVerfG, Urteil vom 27. Juli 2005 – 1 BvR 668/04 –, BVerfGE 113, 348-392, Rn. 146.
[18] B. Rusteberg, Die Entscheidung des Bundesverfassungsgerichts zum Bundeskriminalamtsgesetz, KritV 2017, 24 (30).
[19] U. Buermeyer, Zum Begriff der »laufenden Kommunikation« bei der Quellen-Telekommunikationsüberwachung (»Quellen-TKÜ«), StV 2013, 470 f.

Integrität informationstechnischer Systeme darstellen, sondern sich ausschließlich nach den Vorgaben richten, die auch sonst für die Telekommunikationsüberwachung gelten.[20]

Ausdrückliche Voraussetzung ist insofern jedoch, dass die hierfür notwendigen Eingriffe in das informationstechnische System rechtlich voraussetzen und technisch sicherstellen, dass eine Überwachung nur für die laufende Telekommunikation erfolgt. Andernfalls komme allein ein Vorgehen nach den Vorschriften in Betracht, die für einen Eingriff in informationstechnische Systeme gelten.[21] Maßgeblich sei insoweit, „ob das Programm so ausgestaltet ist, dass es - hinreichend abgesichert auch gegenüber Dritten - den mit der Überwachung betrauten Mitarbeiterinnen und Mitarbeitern des Bundeskriminalamts inhaltlich eine ausschließlich auf die laufenden Kommunikationsinhalte begrenzte Kenntnisnahme ermöglicht." Hingegen komme es nicht darauf an, „ob durch eine technisch aufwendige Änderung des Überwachungsprogramms selbst – sei es durch die Behörde, sei es durch Dritte – dessen Begrenzung auf eine Erfassung der laufenden Telekommunikation aufgehoben werden" könne.[22]

Für die Gültigkeit der gesetzlichen Ermächtigungsgrundlage soll nach der Rechtsprechung des Bundesverfassungsgerichts dabei unerheblich sein, inwieweit tatsächlich technische Maßnahmen existieren, die sicherstellen, dass ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet wird. Diese Frage betreffe „die Anwendung der Norm, nicht aber ihre Gültigkeit". Sollten diese Anforderungen zum jeweiligen Zeitpunkt nicht erfüllbar sein, laufe die Vorschrift schlicht leer.[23]

bb) Laufende Kommunikation

Die Schutzbereiche beider Grundrechte sind insoweit komplementär angelegt: Sobald die engen Grenzen der „laufenden Kommunikation" überschritten sind, also insbesondere auf bereits übermittelte oder zukünftig (möglicherweise) einmal zu übermittelnde Daten zugegriffen werden soll, und damit der verfassungsrechtlich zulässige Anwendungsbereich der Quellen-TKÜ verlassen wird, stellt sich der Eingriff ohne weiteres als Online-Durchsuchung dar.[24]

Datenverarbeitungsvorgänge im alleinigen Machtbereich eines der beteiligten Kommunikationspartner können dabei nur so lange als Teil der laufenden Kommunikation angesehen und damit vom Schutzbereich des Art. 10 Abs. 1 GG erfasst werden, als sie noch als Teil einer Verwendung als „Telefonie-Endgerät" angesehen werden können. Dies umfasst allein solche technischen Vorgänge, die unmittelbar der Übergabe von Kommunikationsinhalten an einen Informationsmittler dienen und sich somit als integraler Bestandteil der Telekommunikation im Sinne des Fernmeldegeheimnisses darstellen.[25] Nicht umfasst sind hingegen insbesondere solche Vorgänge im Machtbereich eines Kommunikationspartners, die lediglich der Vorbereitung von Daten auf eine

[20] BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274, Rn. 190; Buermeyer, Zum Begriff der »laufenden Kommunikation« bei der QuellenTelekommunikationsüberwachung (»Quellen-TKÜ«), StV 2013, 470 (473).
[21] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 234.
[22] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 234.
[23] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 234.
[24] U. Buermeyer, Zum Begriff der »laufenden Kommunikation« bei der Quellen-Telekommunikationsüberwachung (»Quellen-TKÜ«), StV 2013, 470 (473).
[25] U. Buermeyer, Zum Begriff der »laufenden Kommunikation« bei der Quellen-Telekommunikationsüberwachung (»Quellen-TKÜ«), StV 2013, 470 (473).

mögliche spätere Kommunikation oder der Weiterverarbeitung bereits empfangener Daten, also früherer Kommunikation, dienen.[26]

Laufende Telekommunikation umfasst damit Datenverarbeitungsvorgänge, die sich entweder im Herrschaftsbereich eines Informationsmittlers oder im Herrschaftsbereich eines der Kommunikationspartner abspielen, dabei aber unmittelbar – d.h. ohne weitere Zwischenschritte – der Übergabe von Kommunikationsinhalten an einen Informationsmittler dienen.[27]

3. Schutzbereichszuordnung der Ermächtigung des § 11 Abs. 1a G10

Gesetzessystematisch bestimmt sich der Anwendungsbereich des § 11 G10 nach § 1 Abs. 1 G10. Die materiellen Voraussetzungen einer derartigen Beschränkung des Fernmeldegeheimnisses im Einzelfall ergeben sich aus den §§ 3 bis 3b G10, die formellen Voraussetzungen, soweit sie nicht in § 11 G10 geregelt sind, aus den §§ 9 ff. G10.

a) Begriff der „Telekommunikation“

Gem. § 1 Abs. 1 Nr. 1 G10 sind die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes berechtigt, die Telekommunikation zu überwachen und aufzuzeichnen.

Zur Konkretisierung des Begriffs der Telekommunikation wird insoweit grundsätzlich auf § 3 Nr. 22 TKG zurückgegriffen. Nach der dortigen Legaldefinition ist „Telekommunikation“ der technische Vorgang des Aussendens von Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen. Damit werden alle Formen der Nachrichtenübermittlung unter Raumüberwindung in nicht-körperlicher Weise mittels technischer Einrichtungen erfasst. Hierzu zählen u.a. die Telefonie über Festnetz oder Mobilfunk, der SMS-Versand und der E-Mail-Verkehr sowie weitere Anwendungen des Internets.[28]

Das Überwachen und Aufzeichnen dieser mittels Telekommunikationsanlagen übermittelten Daten stellt damit grundsätzlich einen Eingriff in das Fernmeldegeheimnis des Art. 10 Abs. 1 GG dar.

b) Abgrenzung laufender von abgeschlossener Telekommunikation

aa) § 11 Abs. 1a S. 1, 3 Nr. 1 lit. a) G10-E

§ 11 Abs. 1a S. 1 G10-E ermächtigt zunächst dazu, die Überwachung und Aufzeichnung der laufenden Telekommunikation in der Art und Weise vorzunehmen, „dass in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen wird, wenn dies notwendig ist, um die Überwachung und

[26] U. Buermeyer, Zum Begriff der »laufenden Kommunikation« bei der Quellen-Telekommunikationsüberwachung (»Quellen-TKÜ«), StV 2013, 470 (474): Insoweit verlaufe die verfassungsrechtliche Abgrenzung parallel zur technischen Abgrenzung zwischen Inhalts- und Transportverschlüsselung; vgl. auch M. Martini/S. Fröhlingsdorf, Catch me if you can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik, NVwZ-Extra 24/2020, 1 (6).

[27] U. Buermeyer, Zum Begriff der »laufenden Kommunikation« bei der QuellenTelekommunikationsüberwachung (»Quellen-TKÜ«), StV 2013, 470 (473 f.).

[28] F. Roggan, G10, 2. Aufl. 2018, G 10 § 1 Rn. 12; vgl. zum ähnlich weiten Begriff der Telekommunikation in § 100a StPO BVerfG, Nichtannahmebeschluss vom 06. Juli 2016 – 2 BvR 1454/13 –, juris; BVerfG, Nichtannahmebeschluss vom 20. Dezember 2018 – 2 BvR 2377/16 –, juris, Rn. 42.

Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen“. Gem. § 11 Abs. 1a S. 3 Nr. 1 lit. a) G10-E ist überdies technisch sicherzustellen, dass ausschließlich die laufende Kommunikation überwacht und aufgezeichnet werden kann. Zudem dürfen gem. § 11 Abs. 1a S. 3 Nr. 2 u. 3 G10-E 2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und die vorgenommenen Veränderungen müssen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

Insoweit entspricht die Regelung den dargestellten Voraussetzungen, um als sog. Quellen-TKÜ eine Schutzbereichsausnahme aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu erfahren.

Irritierend ist jedoch bereits an dieser Stelle die Formulierung, die § 11 Abs. 1a S. 1 G10-E – insoweit abweichend von § 100a Abs. 1 S. 2 StPO – verwendet, wonach die Überwachung und Aufzeichnung der laufenden Telekommunikation, *die nach dem Zeitpunkt der Anordnung übertragen worden ist*, in der beschriebenen Art und Weise erfolgen darf. Nach der Systematik der Sätze 1 u. 2 – siehe dazu sogleich – ist davon auszugehen, dass Satz 1 sich ausschließlich auf die laufende Übertragung beziehen soll. Würde Satz 1 hingegen so gelesen, dass auch er sich auf bereits abgeschlossene Übertragungen bezieht, wäre auch er als Ermächtigung nicht bloß zur Quellen-TKÜ, sondern zur Online-Durchsuchung zu qualifizieren.

Insofern ist eine dies klarstellende Formulierung erforderlich, etwa dass eine Überwachung und Aufzeichnung der laufenden Telekommunikation, die nach dem Zeitpunkt der Anordnung übertragen *wird*, in der beschriebenen Art und Weise erfolgen darf.

bb) § 11 Abs. 1a S. 2, 3 Nr. 1 lit. b) G10-E

Gem. § 11 Abs. 1a S. 2 G10-E soll es den Nachrichtendiensten zudem erlaubt sein, *ab dem Zeitpunkt der Anordnung gespeicherte* Inhalte und Umstände der Kommunikation auf dem informationstechnischen System des Betroffenen zu überwachen und aufzuzeichnen, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.

Dem korrespondierend ist gem. § 11 Abs. 1a S. 3 Nr. 1 lit. b) G10-E auch technisch lediglich sicherzustellen, dass neben der laufenden Kommunikation nur Inhalte und Umstände der Kommunikation, die auch während des laufenden Kommunikationsvorgangs ab dem Zeitpunkt der Anordnung im öffentlichen Telekommunikationsnetz *hätten überwacht und aufgezeichnet werden können*, überwacht und aufgezeichnet werden.

Damit geht aber bereits der Wortlaut des Gesetzentwurfs davon aus, dass mit der Ermächtigung des § 11 Abs. 1a S. 2 G10-E die Überwachung über die laufende Kommunikation hinaus ausgedehnt werden soll. Insoweit bewegt sich die Maßnahme jedoch außerhalb der vom Bundesverfassungsgericht vorgenommenen Schutzbereichsausnahme und stellt nicht mehr nur einen Eingriff in den Schutzbereich des Art. 10 Abs. 1 GG dar, sondern greift in den Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ein.

Diese Bewertung deckt sich im Übrigen mit der ganz herrschenden Meinung der Literatur zur Regelung des § 100a Abs. 1 S. 3 StPO, der § 11 Abs. 1a S. 2 G10-E nachgebildet ist.[29]

[29] Siehe etwa BeckOK IT-Recht/Brodowski, 1. Ed. 1.9.2020, StPO § 100a Rn. 10: „Ohnehin verkennt diese Regelung, dass die gespeicherten Daten – jedenfalls in der Regel – nicht mehr Art. 10 GG unterliegen, sodass der Eingriff am Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG) zu messen ist, zu dem § 100a nicht legitimiert."
Ders./U. Sieber, in: Hoeren/Sieber/Holznagel MMR-HdB, 54. EL Oktober 2020, Teil 19.3 Strafprozessrecht, Rn. 151: „Besonders kritisch zu beurteilen ist schließlich die Erweiterung in § 100 a Abs. 1 Satz 3 StPO, der zufolge auch mit technischen Mitteln retrospektiv „Inhalte und Umstände der Telekommunikation […] überwacht und aufgezeichnet werden [dürfen], wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können" (hypothetische Kommunikationsinhalte). Diese sind gem. § 100 a Abs. 5 Nr. 1 lit. b StPO auf Daten begrenzt, „die ab dem Zeitpunkt der Anordnung nach § 100 e Absatz 1 auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können", wenn sie denn nicht verschlüsselt worden wären. Indessen ist es bereits aus forensischer Sicht sehr zweifelhaft, ob sich im Nachhinein treffsicher diese (und nur diese) Inhalte und Umstände rekonstruieren lassen. Zudem geben diese unter Umständen bei nur teilweise möglicher Rekonstruktion ein unvollständiges Bild wieder. Am gravierendsten ist jedoch, dass der anwendbare Grundrechtsmaßstab verkannt wurde: Es wird auf Daten zugegriffen, die – eventuell – in der Vergangenheit zwar Gegenstand von Telekommunikation waren, die aber jetzt nicht mehr dem Schutz des Art. 10 GG unterliegen, sondern dem (strengeren) Schutz des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG). Hinzu kommt, dass durch die weite Fassung der Zieldaten möglicherweise eine noch umfassendere Suche nach solchen Daten auf dem infiltrierten Computersystem möglich wird. Es sprechen deswegen gute Gründe für eine – zumindest teilweise – Verfassungswidrigkeit von § 100 a Abs. 1 Satz 3 StPO."
M. Martini/S. Fröhlingsdorf, Catch me if you can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik, NVwZ 2020, 1803: „Die StPO erlaubt darüber hinaus, im Rahmen der Quellen-TKÜ auf gespeicherte Kommunikation zuzugreifen, wenn diese zuvor Gegenstand eines Übertragungsvorgangs war (vgl. § 100 a I 3 StPO). Sie gestattet damit rückwirkend den Zugriff auf vergangene Kommunikationsdaten, namentlich solche, die eine Zielperson zwischen Anordnungszeitpunkt und Inbetriebnahme der Überwachungssoftware übertragen oder erhalten hat (vgl. § 100 a V 1 Nr. 1 b StPO; BT-Drs. 18/12785, 52 f.). Damit überschreitet die Norm die kritische Grenze zur Online-Durchsuchung; der Eingriff muss sich am so genannten IT-Grundrecht messen. Die Vorschrift ist daher verfassungswidrig." Ausf. auch dies., NVwZ – Extra 24/2020, 1 (7 f.).
S. Großmann, Telekommunikationsüberwachung und Online-Durchsuchung, JA 2019, 241 (243): „Überzeugen kann dies nicht: Die Betroffenheit eines Grundrechts bemisst sich nach der Art des Eingriffs und kann nicht rückwirkend durch das durch die Maßnahme erlangte Ergebnis relativiert werden. Das Auslesen und Aufzeichnen gespeicherter Kommunikationsinhalte setzt ein Eindringen und Durchsuchen des gesamten Systems nach relevanten Kommunikationsinhalten voraus. Aufgrund der enormen Sensibilität der auf informationstechnischen Geräten gespeicherten Daten wiegt ein Eingriff hierin stets erheblich schwerer als ein bloßes „Anzapfen" externer Leitungen. Es verwundert sehr, wie leichtfertig der Gesetzgeber den vom BVerfG durch das IT-Grundrecht geschaffenen Schutzbereich ignoriert."
F. Freiling/C. Safferling/C. Rückert, Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung, JR 2018, 9 (21): „Die vom BVerfG der Entscheidung zugrunde gelegte Parallelität zwischen TKÜ und Quellen-TKÜ trägt aber nur soweit, wie tatsächlich laufende Telekommunikation überwacht wird. Das betonen die Verfassungsrichter auch hinsichtlich der Kernbereichsnähe der TKÜ. Bei Daten nach § 100a Abs. 5 Nr. 1 b StPO n.F. (Daten, die nach Anordnung aber vor tatsächlichem technischen Zugriff gespeichert werden) versagt demnach die Eingriffsrechtfertigung durch das BVerfG. Hier handelt es sich tatsächlich um eine (beschränkte) Online-Durchsuchung."
T. Singelnstein/B. Derin, Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, NJW 2017, 2646 (2648): „Auch bei einem derart engen Verständnis ist die Regelung gleichwohl nicht mit der Rechtsprechung des BVerfG in Einklang zu bringen. Dieser zufolge markiert die Beschränkung auf laufende Kommunikation in Abgrenzung zu gespeicherten Daten gerade die Grenze zwischen Art. 10 I GG und dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Die Vorschrift ist daher nicht mehr nur am Fernmeldegeheimnis, sondern am deutlich strengeren Computer-Grundrecht zu messen, dessen Anforderungen die Voraussetzungen des § 100 a StPO nicht genügen."

4. Anordnungsvoraussetzungen

a) § 11 Abs. 1a S. 1, 3 Nr. 1 lit. a) G10-E iVm. § 3 Abs. 1 G10

Für die Rechtfertigung setzen Eingriffe in das Fernmeldegeheimnis grundsätzlich hinreichend gewichtige Schutzgüter sowie ausreichend konkretisierte Eingriffsschwellen voraus.[30]

aa) Eingriffsschwelle

§ 3 Abs. 1 G10 sieht als Voraussetzung eines Eingriffs in das Fernmeldegeheimnis tatsächliche Anhaltspunkte einer künftigen oder in der Vergangenheit liegenden Straftatbegehung vor.[31]

Die hiermit für eine Beschränkung des Fernmeldegeheimnisses im Einzelfall vorgesehenen Anforderungen begegnen – unabhängig von der geplanten Neuregelung – grundsätzlichen verfassungsrechtlichen Bedenken:

Gerade im Vorfeldbereich ist die Gefahr von Fehlprognosen besonders hoch. Für entsprechend zu charakterisierende Befugnisse verlangt das Bundesverfassungsgericht deshalb handlungsbegrenzende Tatbestandselemente, die einen Standard an Vorhersehbarkeit und Kontrollierbarkeit vergleichbar dem schaffen, der für die überkommenen Aufgaben der Gefahrenabwehr und der Strafverfolgung rechtsstaatlich geboten sind.[32]

Einer von diesen Voraussetzungen abweichender, „geheimdienstspezifischer“ Maßstab für die Eingriffstatbestände wäre nur dann zu rechtfertigen, wenn die Gefahr der Betroffenen, aufgrund falsch positiver Prognosen zum Adressaten von Folgemaßnahmen zur werden, bei Maßnahmen nach § 1 Nr. 1 iVm. § 3 G10 gegenüber Maßnahmen der Polizei oder Strafverfolgungsbehörden signifikant gesenkt wäre. Dies kann jedoch allenfalls insoweit angenommen werden, soweit – wie etwa bei der Auslandsaufklärung durch den BND – die Maßnahmen eindeutig zur Information der Bundesregierung für Tätigkeiten der Staatsleitung erhoben werden.[33] Soweit die Aufgabe des Verfassungsschutzes aber gerade und zunehmend in der vorbereitenden Gefahrenabwehr gesehen wird, bestehen keine Gründe, eine Absenkung der Anforderungen vorzunehmen.[34]

[30] B. Rusteberg, Die Entscheidung des Bundesverfassungsgerichts zum Bundeskriminalamtsgesetz, KritV 2017, 24 (30).
[31] F. Roggan, G10, 2. Aufl. 2018, G 10 § 1 Rn. 12.
[32] F. Roggan, G10, 2. Aufl. 2018, G 10 § 3 Rn. 7, m.w.N.
[33] BVerfG, Urteil vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 1-332, Rn. 223 ff.; BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94 –, BVerfGE 100, 313-403, Rn. 283 ff.; vgl. BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274-350, Rn. 255; BVerfG, Urteil vom 02. März 2010 – 1 BvR 256/08 –, BVerfGE 125, 260-385, Rn. 232; insoweit übersieht Huber, in: Schenke/Graulich/Ruthig (Hrsg.), 2. Aufl. 2018, G 10 § 3 Rn. 9, dass sich die Ausführungen gerade auf die strategische Überwachung beziehen.
[34] F. Roggan, G10, 2. Aufl. 2018, G 10 § 3 Rn. 7, m.w.N.

bb) Rechtsgüter

Der Regelungsansatz des § 3 Abs. 1 G10 kann schon deshalb nicht überzeugen, weil dieser als Voraussetzung präventiver Befugnisse nicht auf die maßgeblichen Rechtsgüter, sondern ausschließlich auf die Verhinderung bestimmter Straftaten abgestellt wird.[35]

Auch die im Einzelnen vorgesehenen Anlassdelikte stehen zu Recht in der Kritik: Bei vielen von ihnen handelt es sich wiederum um Gefährdungsdelikte, die mithin keine konkrete Rechtsgutsverletzung und teilweise noch nicht einmal eine konkrete Gefährdung voraussetzen. In Verbindung mit der (unzureichenden) Eingriffsschwelle findet insofern eine sich gegenseitig potenzierende Vorverlagerung des Eingriffspunktes statt.[36]

Schließlich finden sich verschiedene Delikte im Katalog, die mit einer Höchststrafe von drei Jahren (vgl. § 130 Abs. 4 StGB) oder auch nur einem Jahr (vgl. etwa § 20 Abs. 1 VereinsG) bedroht sind. Wenn im Regelungsansatz gerade nicht auf die gefährdeten Rechtsgüter, sondern auf einzelne Delikte abgestellt wird, kann hier kaum von einem hinreichenden Gewicht dieser Straftaten für die Eingriffsrechtfertigung ausgegangen werden.[37]

b) § 11 Abs. 1a S. 2, 3 Nr. 1 lit. b) G10-E iVm. § 3 G10

Da § 11 Abs. 1a S. 2, 3 Nr. 1 lit. b) G10-E einen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme darstellt, unterliegt die Regelung strengen Anforderungen: Sie müsste insoweit gesetzlich voraussetzen, dass tatsächliche Anhaltspunkte für eine im Einzelfall drohende konkrete Gefahr für ein überragend wichtiges Rechtsgut vorliegen.

Derartige Anforderungen finden sich in dem auch an dieser Stelle insoweit maßgeblichen § 3 G10 gerade nicht. § 11 Abs. 1a S. 2, 3 Nr. 1 lit. b) G10-E ist somit offensichtlich verfassungswidrig.

5. Verfahrensanforderungen und Umsetzbarkeit

Indem § 11 Abs. 1a S. 3 G10-E verlangt, dass technisch sicherzustellen sei, dass ausschließlich die laufende Kommunikation überwacht und aufgezeichnet werden kann, dass an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und dass die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden müssen, greift die Regelung zum Teil wortwörtlich Formulierungen des Bundesverfassungsgerichts auf. Damit kann zwar sichergestellt werden, dass die Regelung insoweit unter die Schutzbereichsausnahme des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme fällt.

[35] Vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 105 f.: „Für Maßnahmen, die der Strafverfolgung dienen und damit repressiven Charakter haben, kommt es auf das Gewicht der verfolgten Straftaten an […]. Für Maßnahmen, die der Gefahrenabwehr dienen und damit präventiven Charakter haben, kommt es unmittelbar auf das Gewicht der zu schützenden Rechtsgüter an."

[36] F. Roggan, G10, 2. Aufl. 2018, G 10 § 3 Rn. 10, m.w.N.

[37] F. Roggan, G10, 2. Aufl. 2018, G 10 § 3 Rn. 10, m.w.N.

Es bleibt aber – wie schon bei der Neuregelung des § 100a StPO[38] – weiterhin vollkommen offen, wie eine solche Sicherstellung technisch erreicht werden kann. Auch die Entwurfsbegründung schweigt sich offensiv hinsichtlich dieses Punktes aus.

Mehr als fünf Jahre nach der Entscheidung des Bundesverfassungsgerichts zum BKA-Gesetz machen es Bestimmtheitsgrundsatz und Wesentlichkeitsgebot aber notwendig – ggf. im Wege der delegierten Normsetzung durch Verordnung –, mindestens im Grundsatz festzulegen, welche technischen Anforderungen zu treffen sind, um diese Punkte tatsächlich sicherzustellen.[39]

Auch verfahrensmäßige Sicherungen – etwa durch eine Vorabkontrolle der Software – sind insoweit nicht vorgesehen.[40] Eine nachträgliche Kontrolle wird hingegen dadurch nahezu verunmöglicht, dass momentan auch keinerlei erprobte technische Verfahren bekannt, die nachweisen könnten, was für eine Software auf einem kontrolliertem System zu einem bestimmten Zeitpunkt lief und was diese dort bewirkt hat.[41]

Eine Begrenz- und Kontrollierbarkeit des tatsächlich erfolgenden Einsatzes der Überwachungssoftware ist – soweit ersichtlich – momentan weder rechtlich- noch technisch erreichbar.

6. Verhältnismäßigkeit im Übrigen

Offen bleibt nach der Gesetzesbegründung auch, inwieweit tatsächlich ein Bedürfnis für eine derartige Quellen-TKÜ besteht. Dabei ist zwar die Erforderlichkeit der Maßnahme nach § 11 Abs. 1a G10-E insoweit sichergestellt, als diese nur eingesetzt werden darf, „wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen“. Ein Einsatz der Quellen-TKÜ scheidet demnach also von vornherein in allen Situationen aus, in denen eine Überwachung auf anderem Wege möglich ist.

Tatsächlich bestehen mittlerweile aber auch bei verschlüsselten Datentransfers durchaus Alternativen zum Einsatz der Quellen-TKÜ.[42] Überdies ist kommt die Technik bislang auch dort, wo gesetzliche Ermächtigungen für ihren Einsatz bestehen, nur äußerst sporadisch zum Einsatz gekommen: So haben Polizei und Ermittlungsbehörden nach der Justizstatistik des Jahres 2019 die Online-Durchsuchung nach der StPO in 21 Verfahren 33 Mal angeordnet und in 12 Fällen tatsächlich eingesetzt. Die Quellen-TKÜ wurde bei 31 Anordnungen sogar lediglich in drei Fällen tatsächlich eingesetzt.[43]

---

[38] Siehe D. Brodowski/U. Sieber, in: Hoeren/Sieber/Holznagel MMR-HdB, 54. EL Oktober 2020, Teil 19.3 Strafprozessrecht, Rn.150.

[39] M. Martini/S. Fröhlingsdorf, Catch me if you can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik, NVwZ-Extra, 24/20, 1 (8), auch zu möglichen technischen Ansätzen.

[40] M. Martini/S. Fröhlingsdorf, Catch me if you can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik, NVwZ-Extra, 24/20, 1 (10 f.).

[41] F. Freiling/C. Safferling/C. Rückert, Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung, JR 2018, 9 (20).

[42] Vgl. etwa die diesbezüglichen Ausführungen M. Martini/S. Fröhlingsdorf, Catch me if you can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik, NVwZ-Extra 24/2020, 1 (12 ff.).
etwa https://netzpolitik.org/2021/ohne-staatstrojaner-polizei-und-geheimdienste-koennen-whatsapp-mitlesen/.

[43] https://netzpolitik.org/2021/justizstatistik-2019-polizei-nutzt-staatstrojaner-vor-allem-bei-erpressung-und-drogen/.

Angesichts der erheblichen Nachteile, die das Vorhalten einer entsprechenden Technik bereits strukturell für die Freiheitsrechte mit sich bringt – Vertrauenseinbußen, Sicherheitslücken[44], Missbrauchsgefahr – werfen diese Punkte weitere dringende Fragen bezüglich der Angemessenheit der Regelungen auf, die die Gesetzesbegründung bislang nicht einmal ansatzweise adressiert.

II. Nummer 7 lit. a) - § 11 Abs. 1b G10-E

7. § 11 wird wie folgt geändert:

a) Nach Absatz 1 werden die folgenden Absätze 1a und 1b eingefügt: […]

(1b) Werden nach der Anordnung weitere Kennungen von Telekommunikationsanschlüssen der Person, gegen die sich die Anordnung richtet, bekannt, darf die Durchführung der Beschränkungsmaßnahme auch auf diese Kennungen erstreckt werden. Satz 1 findet keine Anwendung auf weitere Kennungen von Telekommunikationsanschlüssen von Personen, gegen die sich die Anordnung richtet, weil auf Grund bestimmter Tatsachen anzunehmen ist, dass der Verdächtige ihren Anschluss benutzt (§ 3 Absatz 2 Satz 2 Variante 3). Bevor die Durchführung der Beschränkungsmaßnahme nach Satz 1 auf eine weitere Kennung erstreckt wird, ist dies der nach § 10 Absatz 1 zur Anordnung zuständigen Behörde anzuzeigen. Das nach § 10 Absatz 1 zuständige Bundesministerium unterrichtet monatlich die G 10-Kommission über die ihm nach Satz 3 angezeigten Erstreckungen.“

Nach § 11 Abs. 1b G10-E darf die Durchführung der Beschränkungsmaßnahme auf Kennungen von Telekommunikationsanschlüssen der Person, gegen die sich die Anordnung richtet, erstreckt werden, soweit diese Kennungen nach der Anordnung bekannt werden.

Durch diese Regelung werden zunächst die Verfahrensregelungen der §§ 9 f. G10 ausgehebelt, die Beschränkungsmaßnahmen von einer auf einen vorherigen Antrag erteilten Anordnung durch die zuständigen Landesministerium bzw. das Bundesinnenministerium abhängig machen. Zugleich wird damit das Erfordernis beseitigt, den Vollzug der Maßnahme bis zur Zustimmung der G10-Kommission aufzuschieben, da sich diese nach § 15 Abs. 6 G10-E nur auf die vom Bundesministerium angeordneten Beschränkungsmaßnahmen bezieht. In den Fällen des § 11 Abs. 1b G10-E wird das Bundesministerium aber gerade nur über die Erweiterung der Beschränkungsmaßnahmen informiert, ordnet diese aber nicht selbst an.

Angesichts der weiten Auslegung des Begriffs der Telekommunikation[45] ist dabei kaum abzuschätzen, was als „Kennung von Telekommunikationsanschlüssen“ in den Anwendungsbereich des § 11 Abs. 1b G10-E fällt. Betroffen können keineswegs nur „klassische“ Telefonnummern, Email-Adressen oder Messengerprofile sein, sondern letztlich sämtliche Kennungen, die im Internetverkehr eine Zuordnung zu einer Adresse ermöglichen. Letztlich wird hier eine Rundumüberwachung ohne nennenswerte verfahrensrechtliche Sicherungen ermöglicht.

[44] Dazu ausf. 19(4)844 A - Stellungnahme Prof. Dr. Matthias Bäcker, S. 7 ff.
[45] Siehe oben I.3.a).

Die Regelung des § 11 Abs. 1b G10-E ist deshalb als unangemessen und unverhältnismäßig zu charakterisieren.

Soweit es der Regelung gerade um die Vermeidung von Verzögerungen im Vollzug geht, kann dabei ohne Weiteres auf die neu geschaffene Eilanordnung nach § 15a G10-E zurückgegriffen werden. Bei dieser sind zumindest die Nachvollziehbarkeit des Verfahrens und eine zeitige Interventionsmöglichkeit der G10-Kommission sichergestellt.

Freilich ist auch an dieser Stelle zu fragen, inwieweit eine nachrichtendienstliche Voraufklärung überhaupt ein geeignetes Vorgehen in Eilfällen darstellt.

III. Nummer 5 - § 2 Abs. 1a u. 1b G10-E

Die Regelung des § 2 Abs. 1a u. 1b G10-E geht mit weitreichenden Eingriffen in die Rechte der Anbieter von Telekommunikationsdienstleistern einher. Diese haben der jeweiligen Behörde u.a. nach § 2 Abs. 1a S. 1 Nr. 4 G10-E die Einbringung von technischen Mitteln zur Durchführung einer Maßnahme nach § 11 Absatz 1a durch Unterstützung bei der Umleitung von Telekommunikation durch die berechtigte Stelle zu ermöglichen, Zugang zu ihren Einrichtungen während der üblichen Geschäftszeiten zu gewähren sowie die Aufstellung und den Betrieb von Geräten für die Durchführung der Maßnahme zu ermöglichen.

Anfallende Datenströme sollen danach nicht mehr nur einfach kopiert, sondern umgeleitet werden. Damit können die betroffenen Datenströme verändert werden, d.h. es können sowohl übermittelte Daten inhaltlich verändert, als auch Daten hinzugefügt oder unterdrückt werden.[46]

Der Eingriff in die Berufsfreiheit der Unternehmen, der durch entsprechende Pflichten – gleich ob aktiv oder zur Duldung – sowie die mit diesen verbundenen finanziellen Belastungen bewirkt wird, ist nach der Rechtsprechung des 2. Senats des Bundesverfassungsgerichts als grundsätzlich gerechtfertigt anzusehen.[47]

Dessen ungeachtet ist nicht nachvollziehbar, weshalb der Gesetzentwurf auf konkretisierende Regelungen, insbesondere in Hinblick auf die zahlreichen entstehenden Haftungsfragen vollständig verzichtet. So weist der Branchenverband „bitkom“ in seiner Stellungnahme etwa zutreffend darauf hin, dass im Gesetzentwurf offengelassen werde, was in Fällen passiere, in denen die an den informationstechnischen Systemen vorgenommenen Änderungen nicht gem. § 11 Abs. 1a S. 3 Nr. 3 G10-E rückgängig gemacht werden können.[48]

46 eco, Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts, Berlin, 30.06.2020, S. 5.
47 BVerfG, Nichtannahmebeschluss vom 20. Dezember 2018 – 2 BvR 2377/16 –, juris.
48 bitkom, Stellungnahme Anpassung des Verfassungsschutzrechts, 30.06.2020 S. 3.

Darüber hinaus hat sich das Bundesverfassungsgericht in der oben genannten Rechtsprechung ausdrücklich nicht hinsichtlich der datenschutzrechtlichen Konsequenzen etwaiger Verpflichtungen der Telekommunikationsanbieter geäußert.[49]

Diesbezüglich weisen die Diensteanbieter auch über ihren Branchenverband auf die mit entsprechenden Maßnahmen verbundenen hohen Risiken für die gesamte Netzintegrität hin, die dadurch entstehen, dass die Anbieter ihnen nicht näher bekannte Schadsoftware über ihre Netze in das entsprechende Computersystem einschleusen müssen. Überdies seien solche Maßnahmen jedenfalls geeignet, das Vertrauen in die Kommunikation einschließlich aller abgerufenen Informationen massiv und dauerhaft zu untergraben.[50]

Ergänzend ist auf das extreme Missbrauchspotential hinzuweisen, das die Eröffnung derart weitreichender und letztlich nicht kontrollierbarer Zugriffsmöglichkeiten durch die Nachrichtendienste mit sich bringt. Ohne dass dies von dritter Seite technisch in irgendeiner Weise nachvollziehbar ist, können die Nachrichtendienste faktisch nahezu beliebig gesendete Daten manipulieren und sich auf diesem Wege Zugriffsmöglichkeiten auf informationstechnische Systeme verschaffen. Inwiefern in informationstechnischen Systemen gespeicherten Daten damit zukünftig überhaupt noch ein Beweiswert zugeordnet werden kann, bleibt offen.

Demgegenüber zielt das Recht auf informationelle Selbstbestimmung gerade auch darauf ab, im Sinne eines vorgelagerten Grundrechtsschutzes derartige Missbrauchsgefahren zu verhindern.[51] Mit Blick auf die objektive Dimension des Rechts auf informationelle Selbstbestimmung ist deshalb bereits die Eröffnung derartiger Zugriffsmöglichkeiten für die Nachrichtendienste als unverhältnismäßig anzusehen.

D. Fazit

Der vorliegende Gesetzesentwurf vertieft die Rolle des Verfassungsschutzes als besondere Gefahrenabwehrbehörde. Damit werden jedoch nicht nur das Trennungsgebot und eine sich daraus ergebende mögliche Eingriffsprivilegierung der Verfassungsschutzbehörden zusätzlich in Frage gestellt, sondern – angesichts der Kompetenzüberschneidungen mit der Polizei – auch die Existenz der Verfassungsschutzbehörden selbst.

- Auch vor diesem Hintergrund ist die Erweiterung des Einbezugs der Beobachtung von Einzelpersonen durch das BfV nach § 4 Abs. 1 BVerfSchG-E abzulehnen. Sie ist, gerade angesichts der in der Entwurfsbegründung genannten Beispiele, schon nicht erforderlich.
- Die Regelung des § 11 Abs. 1a S. 1, 3 Nr. 1 a) G10-E partizipiert an den bekannten Mängeln des Anforderungskatalogs in § 3 Abs. 1 G10 und leidet an fehlenden verfahrensrechtlichen

49 BVerfG, Nichtannahmebeschluss vom 20. Dezember 2018 – 2 BvR 2377/16 –, juris, Rn. 51.
50 eco, Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts, Berlin, 30.06.2020, S. 2 f.
51 Dazu R. Poscher, Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen, in: Gander/Perron/ders./Riescher/Würtenberger (Hrsg.), Resilienz in der offenen Gesellschaft, 2012, S. 167 ff.; G. Britz, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561 ff.

Regelungen, wie eine Begrenzung der Überwachung technisch und rechtlich sichergestellt werden kann.

- Die Regelung des § 11 Abs. 1a S. 2, 3 Nr. 1 lit. b) G10-E greift in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ein, ohne an die damit korrespondierenden Voraussetzungen gebunden zu werden, und ist damit offensichtlich verfassungswidrig.
- § 11 Abs. 1b G10-E ermöglicht eine Rundumüberwachung ohne verfahrensrechtliche Kontrolle und ist deshalb unverhältnismäßig.
- Angesichts des sich aus der Regelung ergebenden erheblichen Missbrauchspotentials verstößt § 2 Abs. 1a u. 1b G10-E gegen die objektive Dimension des Rechts auf informationelle Selbstbestimmung.

Anlage A

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)844 E

Stellungnahme

zu dem Entwurf der Bundesregierung eines Gesetzes zur Anpassung des Verfassungsschutzrechts

vorgelegt von

Prof. Dr. Ralf Poscher
Direktor am Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht

unter Mitarbeit von
Dr. Katrin Kappler

im Mai 2021

Inhalt

A. Einleitung

Aufgrund der kurzen Stellungnahmefrist kann nicht auf alle Aspekte des Entwurfs eingegangen werden. Sie konzentriert sich deshalb allein auf die Einführung des § 11 G10-E. In den wenigen Tagen die den Sachverständigen zur Vorbereitung ihrer Stellungnahmen eingeräumt wurden, war eine umfassende Prüfung des Gesetzes nicht möglich.

Der Gesetzesentwurf sieht unter anderem Änderungen des Artikel 10-Gesetzes (G10) vor. Dort soll eine Regelung in § 11 Abs. 1a) G10-E eingefügt werden. Der Entwurf des § 11 Abs. 1a) sieht vor, dass zwei verschiedene Maßnahmen geregelt werden: In § 11 Abs. 1a) S. 1 wird die Quellen-TKÜ geregelt, also der Zugriff auf die laufende Kommunikation, in § 11 Abs. 1a S. 2 wird dann der Zugriff auf die ruhende Kommunikation geregelt und damit eine beschränkte Online-Durchsuchung eingeführt.

B. Zur Regelungssystematik

Bereits die Regelungssystematik ist bedenklich. Dies die in dem Entwurf vorgesehen Quellen-TKÜ ist mit einer auf vergangene Kommunikationsinhalte beschränkten Online-Durchsuchung verbunden. Das neue und für das G 10 neuartige Überwachungsinstrument ist nicht nur an Art. 10 Abs. 1 GG, sondern auch an Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zu messen, weil es sich hier um die Überwachung von ruhender Kommunikation handelt. Gleichzeitig handelt es sich bei den Eingriffsermächtigungen um besonders schwerwiegende neuartige Grundrechtseingriffe. Gleichwohl wird die Regelung in § 11 G 10, also in dem Abschnitt zu den Verfahrensregeln eingefügt. Dies verkennt, dass es sich hierbei um eine eingriffsintensivere Maßnahme handelt, als die bisher vorgesehenen Überwachungsmaßnahmen. Besonders die um den Zugriff auf gespeicherte Kommunikationsdaten erweiterte Überwachung sollte in einer eigenständigen materiellen Norm geregelt werden, die den Besonderheiten und der herausgehobenen Intensität des Eingriffs Rechnung trägt.

C. Keine ausreichend bestimmte Begrenzung der Online-Durchsuchung

Sowohl bei einer Quellen-TKÜ als auch bei einer Online-Durchsuchung werden informationstechnische Systeme infiltriert, sie haben aber unterschiedliche Zweckrichtungen. Während es bei der Quellen-TKÜ ausschließlich darum geht, zielgerichtet eine laufende Kommunikation zu überwachen, die auf Grund der verschlüsselten Daten anderweitig nicht ausgewertet werden könnte, soll mit der Online-Durchsuchung besonders auf den Speicher des Zielsystems zugegriffen werden, um nach bestimmten Dateien im Dateisystem des Rechners zu suchen.

Bär, in: BeckOK PolR Bayern, 15. Ed. 2020, Art. 42 PAG, Rn. 41.

Ermächtigungsgrundlage für staatliche Maßnahmen, durch welche die Inhalte und Umstände einer laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogenen Daten ausgewertet werden, sind an Art. 10 Abs. 1 GG zu messen.

BVerfGE 120, 274 (307).

Die in § 11 Abs. 1 S. 1 G10-E geregelte Quellen-TKÜ ist deshalb an Art. 10 Abs. 1 GG zu messen.

Art. 10 Abs. 1 GG schützt hingegen nicht davor, dass staatliche Stellen die Nutzung eines informationstechnischen Systems als solche überwacht oder die Speichermedien des Systems durchsucht.

BVerfGE 120, 274 (308).

Das Bundesverfassungsgericht hat schon in seinem Urteil zur Online-Durchsuchung herausgestellt, dass schon bei der Quellen-TKÜ durch die Infiltration die entscheidende Hürde genommen ist, um das System insgesamt auszuspähen und deshalb stets das Risiko besteht, dass über Inhalte und Umstände der Telekommunikation weitere persönlichkeitsrelevante Informationen erhoben werden. Diesen spezifischen Gefährdungen könne durch Art. 10 Abs. 1 GG nicht hinreichend begegnet werden. Deshalb ist Art. 10 Abs. 1 GG nur der alleinige Maßstab, wenn sich die Überwachung ausschließlich auf den laufenden

Kommunikationsvorgang beschränken und dies durch technische wie rechtliche Vorgaben sichergestellt ist.

BVerfGE 120, 274 (308-309).

Bei der Online-Durchsuchung hingegen können Datei auf dem Gerät untersucht werden, Maßstab ist hier das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sog. IT-Grundrecht) aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

BVerfGE 120, 274 (302).

Bei der im Entwurf vorgesehenen Form der Quellen-TKÜ handelt sich um eine Mischform zwischen der Quellen-TKÜ und der Online-Durchsuchung, wobei weder aus dem Gesetz noch aus der Gesetzesbegründung hinreichend deutlich wird, auf in welchem Umfang auf gespeicherte Informationen zugegriffen werden soll.

Insoweit ist es nicht ausreichend, darauf zu verweisen, dass nur solche Kommunikationsinhalte und -umstände erhoben werden, die auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form erhoben werden könnten. Die darauf bezogene Begrenzung des Anordnungszeitpunkt lässt nicht erkennen, ob es sich dann nur um Daten handeln darf, die ab diesem Zeitpunkt kommuniziert wurden oder ob die Regelung auch gespeicherte Kommunikationsverläufe erfassen soll, die u.U. Jahre zurückreichen, aber nach dem Anordnungszeitpunkt über einen Dienst noch mit der aktuellen Kommunikation mitkommuniziert wurden. Unklar ist auch, wie festgestellt werden soll, welche Kommunikation in verschlüsselter Form hätte erhoben werden können, da der Umfang der Kommunikation von Kommunikationsverläufen jedenfalls bei einigen Diensten von individuellen Nutzereinstellungen abhängig ist.

D. Eingriffsschwellen

Damit ist zugleich die Frage aufgeworfen, ob die Eingriffsschwellen für die Neuregelungen ausreichend sind.

§ 1 Abs. 1 sowie § 3 G10 wurden nicht geändert, legen aber auch die Eingriffsschwellen für die neuen Regelungen fest. Der Gesetzgeber knüpft die neuen Befugnisse der um eine Online-Durchsuchung erweiterten Quellen-TKÜ also an dieselben Voraussetzungen wie die bisherige Telekommunikationsüberwachung. Dadurch kann er den besonderen Anforderungen, die an die neuartige Quellen-TKÜ zu stellen sind, nicht gerecht werden.

1. Tatsächliche Anhaltspunkte oder bestimmte Tatsachen für den Verdacht einer Straftat

Neben der drohenden Gefahr für die freiheitliche demokratische Grundordnung wird durch die in dem Entwurf gewählte Regelungstechnik vor allem auf tatsächliche Anhaltspunkte für den Verdacht einer Straftat aus dem Katalog des § 3 G10 auf. Andere Ermächtigungsgrundlagen für die Quellen-TKÜ knüpfen allerdings an bestimmte Tatsachen an, weshalb sich die Frage aufdrängt, ob die Anknüpfung an bestimmte Tatsachen auch in § 3 G10 verfassungsrechtlich erforderlich ist.

Die Rechtsprechung des Bundesverfassungsgerichts ist dahingehend nicht eindeutig, es sprechen allerdings gute Gründe dafür, dass die Begriffe nicht als unterschiedliche Eingriffsschwellen aufgefasst dürfen. Teilweise nennt das Gericht beide Begriffe ohne diese voneinander zu differenzieren.

Vgl. nur BVerfGE 120, 274 (328).

An anderer Stelle stellt das Bundesverfassungsgericht zwar fest, dass die Eingriffsschwelle des G10, verglichen mit derjenigen, die etwa § 100a StPO für Überwachungen der Telekommunikation fordert, „relativ niedrig angesetzt ist".

BVerfGE 100, 313 (393).

In dem Urteil zur Vorratsdatenspeicherung aus dem Jahr 2010 fordert das Bundesverfassungsgericht für die Verfassungsmäßigkeit eines Eingriffs in Art. 10 Abs. 1 GG durch die Gefahrenabwehrbehörden auf der einen und die Nachrichtendienste auf der anderen Seite aber das Vorliegen derselben

Voraussetzungen. Die gesetzliche Ermächtigungsgrundlage müsse zumindest „tatsächliche Anhaltspunkte einer konkreten Gefahr" für die zu schützenden Rechtsgüter verlangen.

BVerfGE 125, 260 (330).

Daraus lässt sich schlussfolgern, dass es jedenfalls nicht verfassungswidrig ist, auf die gewählte Formulierung zurückzugreifen.

Vgl. dazu M. Ogorek, JZ 2019, 63 (67); M. Bäcker, Kriminalpräventionsrecht, 2015, S. 232; a.A. B. Huber in: W. Schenke/K. Graulich/J. Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 3 G10, Rn. 5-12.

In jedem Fall muss aber berücksichtigt werden, dass auch an das Vorliegen des Tatbestandsmerkmals „tatsächliche Anhaltspunkte" strenge Anforderungen zu stellen sind. Erforderlich ist, dass nicht allein Vermutungen, sondern konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht vorliegen.

BVerfGE 100, 313 (395).

Vage Anhaltspunkte oder bloße Vermutungen ohne greifbaren, auf den Einzelfall bezogenen Anlass reichen dagegen nicht aus.

BVerfGE 115, 320 (364).

Es bedarf daher gerade eines konkret umrissenen Ausgangspunktes im Tatsächlichen.

BVerfGE 113, 348 (386).

Dies wir in der ganz überwiegenden Anzahl der bisherigen Ermächtigungsgrundlagen dadurch zum Ausdruck gebracht, dass an „bestimmte Tatsachen" und nicht an tatsächliche Anhaltspunkte für den Verdacht einer Straftat angeknüpft wird.

z.B. § 51 BKAG, § 54 bwPolG, § 42 hmbgPolG. Vgl. dazu auch F. Rachor/K. Graulich in H. Lisken/E. Denninger, HB des PolR, 6. Aufl. 2018, Kap. E, Rn. 148.

Um die strengen Anforderungen deutlich zu machen und zur Rechtssicherheit und zu einer gewissen Konsistenz der Sicherheitsgesetze beizutragen, wäre es deshalb sinnvoll, auch in § 3 G10 an den Begriff der bestimmten Tatsachen anzuknüpfen.

2. Anpassung des Straftatenkatalogs

Durch die gewählte Form der Neuregelung wird auch die Festlegung der Schutzgüter pauschal übernommen. Insoweit entspricht der Strafenkatalog, der die neuartige Quellen-TKÜ legitimieren soll, nicht den verfassungsrechtlichen Anforderungen. Schon ohne die Einführung der neuartigen Quellen-TKÜ ist fraglich, ob der Straftatenkatalog den Anforderungen der Verfassung genügt. Dies ist insbesondere fraglich, weil der Katalog auch Straftaten erfasst, die im Mindestjahr nur mit einem Jahr bedroht sind (wie § 20 VereinsG).

Bei der um eine Online-Durchsuchung erweiterten Quellen-TKÜ ist darüber hinaus zu beachten, dass es sich um einen intensiven Grundrechtseingriff handelt, weil die heimliche Infiltration auch die längerfristige Überwachung und Nutzung des Systems ermöglicht.

BVerfGE 120, 274 (323-324).

Diese erhöhte Eingriffsintensität muss auch bei den Katalogstraftaten berücksichtigt werden. Dem kommt der Gesetzgeber nicht nach. Deshalb wird dringend empfohlen, den Straftatenkatalog jedenfalls für die der um eine Online-Durchsuchung erweiterte Quellen-TKÜ enger zu fassen und auf schwerwiegende Straftaten zu beschränken.

Ohnehin wäre es regelungstechnisch sinnvoller, nicht auf einen Straftatenkatalog zurückzugreifen, sondern die konkreten Rechtgüter zu benennen, die geschützt werden sollen.

BVerfGE 125, 260 (329).

Dies gilt umso mehr, weil das Bundesverfassungsgericht in Bezug auf den Eingriff in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG herausgestellt hat, dass tatsächliche

Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen müssen.

BVerfGE 120, 274 (328 -329)

3. Eingrenzung des Betroffenenkreises

Aufgrund der Eingriffsintensität und Heimlichkeit der Maßnahme hat das Bundesverfassungsgericht gefordert: „Der Zugriff auf informationstechnische Systeme und die Wohnraumüberwachung dürfen sich unmittelbar nur gegen diejenigen als Zielperson richten, die für die drohende oder dringende Gefahr verantwortlich sind."

BVerfGE 141, 220 (273).

§ 3 Abs. 2 S. 2 G 10 erlaubt hingegen Abhörmaßnahmen auch gegen weitere Personen. Auch hier zeigt sich wieder, dass die um eine Online-Durchsuchung erweiterte Quellen-TKÜ in § 11 als bloße Verfahrensregelung falsch rubriziert. Sie bedarf jedenfalls einer eigenständigen und neuen materiellen Regelung, die den besonderen Anforderungen und der gesteigerten Intensität des Eingriffs entspricht.

4. Ausschluss des Rechtsschutzes

Nach § 13 G 10 ist der Rechtsschutz für Maßnahmen nach § 3 G 10 pauschal ausgeschlossen. Für Eingriffe in Art. 10 GG hat dies seine verfassungsrechtliche Basis in Art. 10 Abs. 2 GG. Die mit der nun Quellen-TKÜ des Entwurfs eingeführte beschränkte Online-Durchsuchung verbindet sich aber auch mit einem Eingriff in Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG. Für Eingriffe in dieses Grundrecht fehlt es an einer verfassungsrechtlichen Grundlage für eine Ausnahme von der Rechtsschutzgarantie aus Art. 19 Abs. 4 GG.

E. Transparenz und parlamentarische Kontrollmechanismen

Nachrichtendienste zeichnen sich vor allem dadurch aus, dass ihnen nachrichtendienstliche Mittel und die Befugnis zur heimlichen Überwachung des Telekommunikationsverkehrs zur Verfügung stehen. Diese Heimlichkeit führt zum einen dazu, dass die Eingriffsintensität steigt, zum anderen aber auch dazu, dass die Rechtsschutzmöglichkeiten zum einen rechtlich und zum anderen aber auch faktisch eingeschränkt sind.

Vgl. nur C. GusyVerwArch 106 (2015), 437 ff.

Diesen Schwierigkeiten wird mit Kontrollmechanismen entgegengewirkt. Dazu gehört auch die parlamentarische Kontrolle. Die Kontrolle ist aber nur effektiv, wenn die Kontrollinstanz auch Zugang zu den notwendigen Informationen hat. Dies ist beispielsweise dann nicht mehr der Fall, wenn die technische Umsetzung der einfach- und verfassungsrechtlichen Anforderungen nicht mehr nachvollzogen werden kann.

Wie andere gesetzliche Grundlagen der um eine Onlinedurchsuchung erweiterte Quellen-TKÜ macht auch der Entwurf bislang nicht hinreichend deutlich, wie die Abgrenzung zwischen den Inhalten der Kommunikation und anderen Inhalten technisch und organisatorisch gewährleistet werden soll.

Dabei kann nicht unbedingt erwartet werden, dass das Gesetz bereits selbst entsprechende technische Spezifikationen enthält. Doch sollte das Gesetz Regelungen enthalten, die sicherstellen, dass gerade auch die parlamentarische Kontrolle möglich bleibt. So könnte etwa eine Regelung aufgenommen werden, die sicherstellt, dass von Dritten erworbene Hard- oder Software daraufhin überprüft werden kann, ob sie die einfach- und verfassungsrechtlichen Vorgaben gewährleistet.

F. Spannungsfeld von IT-Sicherheit und Verfassungsschutz

Quellen-TKÜ und der Online-Durchsuchung liegen im Spannungsfeld von IT-Sicherheit und Verfassungsschutz. Relevant ist hier vor allem, dass neben die klassische abwehrrechtliche Dimension des IT-Grundrechts auch eine Schutzpflichtdimension hinzutritt. Diese verpflichtet den Staat grundsätzlich dazu zur Sicherheit der IT-Infrastruktur beizutragen und sie vor Zugriffen und Manipulationen Dritter zu schützen. Auch wenn der Gestaltungsspielraum des Staates ist hier groß ist,

R.Poscher/P.Lassahn, in: G. Hornung/M. Schallbruch (Hrsg.), Handbuch IT-Sicherheitsrecht, 2021, § 7 Rn. 41-42.

ist es dennoch bedenklich, wenn er Anreize setzt, Sicherheitslücken aufrechtzuerhalten.

Ob der Nutzen der um eine Online-Durchsuchung erweiterten Quellen-TKÜ die mit ihr verbundenen Risiken überwiegt, ist zweifelhaft. Aktuelle Zahlen zeigen,

dass die Ermächtigungsgrundlagen für die Quellen-TKÜ und die Online-Durchsuchung nur selten genutzt werden. So hat etwa das BKA im Zeitraum vom 25. Mai 2018 bis 30. April 2019 keine Online-Durchsuchung durchgeführt.

> BT-Drs. 19/15570, S. 4. Siehe z.B. auch Übersicht Telekommunikationsüberwachung für 2019 (Maßnahmen nach § 100a StPO) vom 12.02.2021.

Der Gesetzgeber sollte sich jedenfalls sehr gut überlegen, ob er Instrumente, die ganz wesentlich auch auf dem Verheimlichungen von Sicherheitslücken beruhen, Millionen von Informationssystemen aller Lebensbereiche gefährden und ein immenses Schadenpotential haben, weiter auszudehnt, ohne zuvor eine belastbare Kosten-Nutzen-Analyse vorgenommen zu haben, die nicht nur die tatsächliche Nutzung des Instruments, sondern auch seine Bedeutung für die Aufgabenerfüllung kritisch überprüft. Für Vorrats- oder gar symbolische Gesetzgebung eignen sich weder Quellen-TKÜ noch Onlinedurchsuchung.

G. Zusammenfassung der Ergebnisse

1. Der Gesetzgeber muss eine klarere Regelung der neuartigen Quellen-TKÜ vornehmen, aus der hervorgeht, welche Informationen überhaupt erhoben werden dürfen, um eine genaue Abgrenzung zur Online-Durchsuchung zu ermöglichen.

2. Die um eine Online-Durchsuchung erweiterte Quellen-TKÜ sollte nicht als Verfahrensregelung in das G 10 eingeführt werden. Sie bedarf einer eigenständigen materiellen Regelung, die den besonderen verfassungsrechtlichen Anforderungen, die an sie gestellt sind, ausreichend Rechnung trägt.

3. Der Gesetzgeber sollte dafür Sorge tragen, dass jedenfalls eine effektive parlamentarische Kontrolle auch der technischen Umsetzung der einfach- und verfassungsrechtlichen Anforderungen ermöglicht wird.

4. Angesichts des Spannungsverhältnisses von Verfassungsschutz auf der einen und der verfassungsrechtlichen Pflicht zum Schutz der Integrität der Informationssysteme auf der anderen Seite sollten Quellen-TKÜ und Online-Durchsuchung nur auf der Grundlage einer empirisch belastbaren Kosten-Nutzen-Analyse weiter ausgebaut werden.

Anlage A

Fachhochschule des Bundes
für öffentliche Verwaltung
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)

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)846

Eckpunkte zum Gesetzesentwurf zur Anpassung des Verfassungsschutzrechts (BT-Drs.: 19/24785)

Berlin, 11.05.2021

Mit dem Gesetzesentwurf soll den deutschen Nachrichtendiensten das Recht zur Quellen-TKÜ und zur Online-Durchsuchung von bestimmten, zurückliegenden Kommunikationsdaten eingeräumt werden. eco bewertet den Gesetzentwurf kritisch und sieht erheblichen Änderungsbedarf. Diese Ermittlungsmethoden schwächen die IT-Sicherheit, die Integrität von IT-Infrastrukturen und Vertrauenswürdigkeit von Kommunikation. eco erkennt an, dass es ein berechtigtes Interesse gibt, den Herausforderungen im Bereich des internationalen Terrorismus, des Rechtsterrorismus, und organisierter Kriminalität wirksam entgegenzutreten. Gleichwohl stehen nach Auffassung des eco stehen die zu erzielenden Ermittlungsergebnisse außer Verhältnis zu den vorgenannten Schwächungen und daraus resultierenden Gefährdungen für Bürger und Bürgerinnen, die Wirtschaft und nicht zuletzt den Staat selbst.

Nachfolgend möchten wir unseren zentralen Kritikpunkte noch einmal darlegen. Ergänzend weisen wir auf unsere ausführliche Stellungnahme hin.

I. Erweiterung der Befugnisse zur Online-Durchsuchung für alle 19 Geheimdienste

eco lehnt die Erweiterung der Befugnisse zur Online-Durchsuchung strikt ab. Entgegen allen öffentlichen Bekundungen sollen mit dem vorliegenden Gesetzentwurf zukünftig allen deutschen Nachrichtendiensten gem. § 2 Absatz 1 S. 1 Nr. 4 G10-Gesetz-E i. V. m. § 11 Abs. 1a S. 1 G10-Gesetz-E zur Online-Durchsuchung berechtigt werden. Aus technischer Perspektive besteht hinsichtlich der eingesetzten Trojaner-Software kein Unterschied bzgl. deren Ausforschungsfähigkeit, ob diese eine uneingeschränkte Online-Durchsuchung ermöglicht oder wie hier vorgesehen auf einen bestimmten Zeitraum sowie auf ruhende Kommunikation bezogen erfolgt. Zur Veranschaulichung: Am 10. Oktober wird der Einsatz des Trojaners gegenüber Person A angeordnet, am 17. Oktober gelingt die Infiltration des technischen Systems von A mit der Trojaner-Software. Der Trojaner soll dann die auf die zurückliegende und damit ruhende Kommunikation ab 10. Oktober zugreifen und auslesen dürfen. Technisch gesehen ist dabei jede Funktion, welche Zugriff auf ruhende Daten nimmt, grundsätzlich geeignet, auf alle älteren Daten im infizierten IT-System der Zielperson zuzugreifen, unabhängig davon ob es sich Kommunikations- oder andere Daten handelt.

II. Schwächung der IT-Sicherheit und Integrität (Ausnutzen v. Lücken)

Eine „Datenerhebung durch Eingriff in die informationstechnischen Systeme“ wird, wenn diese durch das Ausnutzen von Sicherheitslücken durchgeführt werden soll, von eco kritisch bewertet. Damit die IT-Sicherheit insgesamt gestärkt wird, müssen festgestellte Schwachstellen vielmehr unverzüglich gemeldet und beseitigt werden. Online-Durchsuchung und Quellen-TKÜ führen zu einer Schwächung der Sicherheit und der Integrität von IT-Systemen. Beiden Ermittlungsinstrumenten ist gemein, dass sie am einfachsten und besten zu nutzen sind, wenn sie durch die

Ausnutzung Lücken in handelsüblicher und weit verbreiteter Software (Betriebssysteme oder Standardbürosoftware) oder auf dem System des betroffenen Nutzers aufgebracht werden. Das verstärkt den Anreiz der Sicherheitsbehörden, solche Sicherheitslücken geheim zu halten und nicht offenzulegen. Zu Gunsten von Ermittlungen gegen eine einzelne Person Schwachstellen und Lücken offen zu halten, bedeutet für Millionen von privaten, gewerblichen und staatlichen Nutzern hierzulande Gefahren für deren Privatsphäre, deren Eigentum, mittelbar auch deren Vermögen, da auch Kriminelle sie nutzen können oder darüber gefährliche Botnetze aufgebaut werden. Hinzu kommt, dass die Fähigkeiten bzw. Reichweite von Staatstrojanern beim Durchsuchen von IT-Systemen mangels Dokumentationspflichten und Expertenwissen weder durch die Geheimdienste noch durch Gerichte oder die vorhandenen Aufsichtsgremien kontrolliert werden können.

III. Besonders intensiver Eingriff durch „Umleitung“

eco lehnt die Regelung nach § 2 Abs. 1a S. 1, Nr. 4 G10-Gesetz-E ab. Denn mit dem Tatbestandsmerkmal „Umleitung“ wird eine Vielzahl an rechtlichen und prozeduralen Fragen aufgeworfen. Die Anbieter, die geschäftsmäßig Telekommunikationsdienste erbringen oder diejenigen, die an der Erbringung solcher Dienste mitwirken, sollen nunmehr aktiv die Nachrichtendienste bei der Infiltration der Endgeräte Ihrer Kunden unterstützen. Die Datenverkehre der Zielperson sollen vom jeweiligen Anbieter an eine Schnittstelle des ausführenden Nachrichtendienstes umgeleitet und nach Aufspielen des Trojaners wieder durch den TK-Anbieter an die Zielperson zurückgeleitet werden. Dadurch soll eine Quellen-TKÜ und Online-Durchsuchung zeitnah und durch die Ausnutzung des Vertrauens der Kunden in scheinbar vertrauenswürdige Quellen ermöglicht werden. Zu bedenken ist ferner, dass mit dem neuen Telekommunikationsgesetzes (TKG) die Anzahl der grundsätzlich zur Unterstützung verpflichteten Unternehmen massiv ansteigen. Zukünftig werden dann auch Anbieter von E-Mail-, Messaging-, und VoIP-Dienste in die Verpflichtungen einbezogen. eco erachtet die damit verbundene qualitative und quantitative Ausdehnung auf diese genannten Dienste als zu weitreichend und lehnt diese ab.

Nach unserem Verständnis will der Gesetzgeber mit der Regelung in § 2 Abs. 1a S. 1 Nr. 4 G10-Gesetz-E die Befugnis zur Veränderung der betroffenen Datenströme schaffen. Damit würde die Vorschrift sowohl die inhaltliche Veränderung von Daten als auch ein Hinzufügen oder Unterdrücken von Daten ermöglichen. Unabhängig von der Frage, ob derartige Eingriffe überhaupt durch die Beschränkungsmöglichkeit des Art. 10 GG gedeckt sein können, sind solche Maßnahmen jedenfalls geeignet, das Vertrauen in die Kommunikation einschließlich aller abgerufenen Informationen massiv und dauerhaft zu untergraben. eco bewertet daher eine solche Regelung äußerst kritisch und lehnt insbesondere eine Veränderung und Manipulation der Kommunikation sowie deren Unterdrückung entschieden ab. Der gegenwärtige Wortlaut dieser Norm schließt eine Anwendung der Norm durch die Nachrichtendienste zur Veränderung und weitergehender Manipulation in seiner aktuellen Fassung nicht explizit aus. Dementsprechend muss durch den Gesetzgeber ausdrücklich klargestellt werden, dass eine Veränderung von Kommunikation von der Regelung des § 2 Abs. 1a G10-Gesetz-E nicht umfasst und ausgeschlossen ist.

IV. Erfüllungsaufwand der Wirtschaft

eco erachtet den angebenen, voraussichtlichen Erfüllungsaufwand der Wirtschaft mit 20.000€/Jahr für deutlich zu niedrig angesetzt, da die Befugnis zur Quellen-TKÜ sowohl dem BfV, den Landesämtern für Verfassungsschutz, dem BND und dem MAD eingeräumt werden soll. Die mit dem Gesetz vorgesehenen verdeckten Eingriffe in IT-Systeme setzen Expertenwissen im Bereich der Technik, entsprechendes technisches Equipment und Schulung des Personals voraus. Darüber hinaus sind geeignete Prozeduren und Vorgänge zur Umsetzung erarbeitet sowie Maßnahmen zur bestmöglichen Geheimhaltung der Maßnahmen sind zu etablieren. Dies verursacht weitaus höhere Kosten bei jedem einzelnen Unternehmen und übersteigt damit die angegeben Kosten für die gesamte Wirtschaft. Soweit die Aus- bzw. Umleitung unmittelbar in Echtzeit zu erfolgen hätte, bedarf es zudem einer gesicherten Übertragung, die weitere, erhebliche Kosten und Aufwände verursacht. Zudem ist die Höhe des Erfüllungsaufwandes davon abhängig, ob auf bestehende Infrastrukturen zur Datenspeicherung und -ausleitung zurückgegriffen werden kann. Soweit dies möglich ist, würden die Kosten für ggf. erforderliche Schnittstellen bis zu 100.000 € betragen. Wenn jedoch Daten angefordert werden, die bislang noch nicht in den vorhandenen Systemen erfasst sind und entsprechende Anpassungen vorzunehmen wären, sowie potentiell neue Infrastruktur installiert werden muss, wäre ein Kostenaufwand in mehrfacher Millionenhöhe zu erwarten.

V. Evaluierung

eco ist der Ansicht, dass eine Evaluierung von besonders schweren Grundrechtseingriffen wie der Quellen-TKÜ mindestens alle 2 Jahre verfassungsrechtlich zwingend geboten ist. Im Rahmen einer Evaluierung ist zu prüfen, ob sich die neu implementierten Befugnisse wie bspw. die Quellen-TKÜ als geeignet erwiesen haben, ob sie zum Zeitpunkt der Evaluierung weiter erforderlich sind, oder ob zum Zeitpunkt der Evaluierung nicht bereits mildere Mittel mit gleicher Wirksamkeit zur Verfügung stehen. Zudem ist dabei auch zu prüfen, ob diese Befugnisse immer noch als angemessen gelten können, konkret ob durch diese Eingriffe rechtfertigende Ermittlungsergebnisse vorgewiesen werden können. Insbesondere bei verdeckten Maßnahmen wie der Quellen-TKÜ, bei denen Rechtsschutz nur nachträglich möglich ist, und eine Rechtverletzung ggf. nur für die Zukunft unterbleibt, sollte eine Evaluierung unter verfassungsrechtlichen Gesichtspunkten zwingend vorgesehen werden.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)641

BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Vorsitzende des
Ausschusses für Inneres und Heimat
des Deutschen Bundestages
Frau Andrea Lindholz
- per E-Mail -
Andrea.Lindholz@Bundestag.de

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-5000
FAX (0228) 997799-5550
E-MAIL referat33@bfdi.bund.de
INTERNET www.bfdi.bund.de
DATUM Bonn, 04.11.2020
GESCHÄFTSZ. 33-651/089#0528

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

nachrichtlich:
Sekretariat des
Ausschusses für Inneres und Heimat
des Deutschen Bundestages
- per E-Mail -
Innenausschuss@Bundestag.de

BETREFF **Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts**
HIER Stellungnahme aus datenschutzrechtlicher Sicht

Sehr geehrte Frau Vorsitzende,

der von der Bundesregierung eingebrachte Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts ist mittlerweile an den Ausschuss für Inneres und Heimat des Deutschen Bundestages zur Beratung überwiesen worden. Da ich das Gesetzgebungsvorhaben in seiner konkreten Form aus datenschutzrechtlicher Sicht kritisch sehe, möchte ich Ihnen die aus meiner Sicht bestehenden Bedenken näher schildern, damit Sie die Möglichkeit haben, diese in die weitergehenden Beratungen des Entwurfs mit einfließen zu lassen. Ich wäre Ihnen dankbar, wenn mein Schreiben an die Ausschussmitglieder verteilt werden könnte. Für Rückfragen stehe ich dem Ausschuss gerne zur Verfügung.

I. Generelle Gesetzeslage

Bei der nunmehr beabsichtigten Gesetzesänderung wird der im Verfassungsschutzrecht des Bundes seit langem bestehende, grundlegende Reformbedarf weiterhin nicht angegangen. Wie dramatisch Umfang und Ausmaß des Reformbedarfs sind, zeigt sich auch deutlich an den diesjährigen Entscheidungen des Bundesverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BVerfG, Urteil vom

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

19. Mai 2020 – 1 BvR 2835/17) und zur Bestandsdatenauskunft (BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13). Regelungssystematik, -dichte und -tiefe der gesetzlichen Vorschriften über die Nachrichtendienste des Bundes weisen generell nicht die notwendige Konsistenz und Qualität auf, um die Nachrichtendienste im Einklang mit den verfassungsrechtlichen Vorgaben zu den Maßnahmen zu ermächtigen, die sie derzeit schon anwenden oder gar zukünftig anwenden können sollen.

Um dies nur anhand einiger Beispiele zu verdeutlichen: Es fehlt vollständig an gesetzlichen Regelungen für das sogenannte, beim Bundesamt für Verfassungsschutz seit 2017 durchgeführte Haber-Verfahren oder für nachrichtendienstliche Prüffälle, also Fälle, bei denen die nachrichtendienstliche Relevanz einer Person bzw. der von ihr gespeicherten Daten noch nicht feststeht und klärungsbedürftig ist. Die gesetzlichen Vorschriften für Datenübermittlungen weisen grundlegende Defizite hinsichtlich der Vorgaben für die Protokollierung der Übermittlung sowie bei der Nennung der für die Übermittlung in Anspruch genommenen Rechtsgrundlage auf. Darüber hinaus sehen sie zu einem Großteil nicht bzw. jedenfalls nicht hinreichend normenklar und bestimmt die verfassungsrechtlich zwingend erforderlichen Eingriffsschwellen vor. Die gesetzlich vorgesehene Kontrolle über die Nachrichtendienste bedarf einer durchgreifenden Überarbeitung, damit eine umfassende, unabhängige objektivrechtliche Kontrolle gewährleistet ist, die das Defizit an Transparenz und individuellen Rechtsschutzmöglichkeiten für betroffene Bürger effektiv kompensiert.

Ich möchte die Gelegenheit daher nochmals nutzen, auf meine bereits im vergangenen Jahr gemachte Anregung eines Sicherheitsgesetz-Moratoriums hinzuweisen. Dies würde die Möglichkeit zur Evaluation der Notwendigkeit und Wirksamkeit nachrichtendienstlicher Kompetenzen, zu einem grundlegenden Neuentwurf der Gesetzesarchitektur im nachrichtendienstlichen Bereich und zur Beseitigung der gesetzlichen Regelungsdefizite schaffen.

Genau das Gegenteil bewirkt hingegen der vorliegende Gesetzesentwurf. Die ohnehin schon verfassungsrechtlich nicht belastbare Gesetzeslage soll weitergehend strapaziert werden, in dem die Befugnisse der Nachrichtendienste in äußerst eingriffsintensiver Weise erweitert werden sollen.

II. Quellen-Telekommunikationsüberwachung (§ 11 Abs. 1a, Abs. 1b G10-GesetzE)

Gerade so tiefgreifende und folgenschwere Eingriffe wie der der Quellen-Telekommunikationsüberwachung bedürfen eines umfassenden, stringenten und belastbaren gesetzlichen Gesamtkonzepts, um vor dem Hintergrund der allgemeingültigen Vorgaben der bundesverfassungsgerichtlichen Rechtsprechung Bestand haben zu können.

BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Zu den im gegenständlichen Gesetzesentwurf nunmehr konkret vorgesehenen Regelungen ist aus meiner Sicht darüber hinaus vor allem Folgendes anzumerken:

Die gesetzliche Ermächtigung für eine Quellen-Telekommunikationsüberwachung muss ganz konkret und präzise gefasst sein und hat sich eng auf das für die nachrichtendienstliche Arbeit unerlässlich Notwendige zu beschränken.

Erforderlich ist dabei, dass sich die Befugnis ausschließlich auf laufende Telekommunikation bezieht, die unmittelbar ausgeleitet bzw. erhoben wird, bevor diese verschlüsselt wird oder nachdem diese wieder entschlüsselt worden ist. Es ist eine trennscharfe Abgrenzung zu sonstigen Eingriffen in informationstechnische Systeme und damit zur Ausleitung bzw. Erhebung von im Endgerät gespeicherten Daten erforderlich. Eine Manipulation des Datenstroms jenseits des Erhebens der Daten der laufenden Telekommunikation muss in jeder Hinsicht ausgeschlossen sein.

Die Regelungen in § 11 Abs. 1a, Abs. 1b G 10-GesetzE genügen dem nicht. In § 11 Abs. 1a S. 2 G 10-GesetzE wird die eigentliche Quellen-Telekommunikationsüberwachung in äußerst unbestimmter Art und Weise dahingehend erweitert, dass „auf dem informationstechnischen System des Betroffenen [...] 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."

Der Umfang der Informationserhebung ist ebenso wie ihr Zeitpunkt im Verhältnis zur Speicherung der Informationen im betroffenen System in der Folge nicht klar und präzise bestimmt. Die Erweiterung beschränkt sich nicht hinreichend auf die Erhebung von laufender Kommunikation, sondern lässt weitergehend die Erhebung von auf dem IT-System gespeicherten Daten zu. Sie betrifft daher auch Fälle des Eingriffs in ein informationstechnisches System, die gemeinhin als Fälle der sogenannten Onlinedurchsuchung eingeordnet werden. Die Grenze zwischen der Quellen-Telekommunikationsüberwachung und der Onlinedurchsuchung wird durch die Regelung unkontrollierbar verwischt und es besteht die Gefahr, dass eine missbräuchliche Manipulation der betroffenen technischen Systeme nicht gesichert ausgeschlossen werden kann.

Zudem ist auch unklar, in welche Arten von informationstechnischen Systemen eingegriffen können werden soll. Die gesetzlich vorgesehenen Regelungen beachten nicht die genauen Kommunikationswege (etwa welcher Messenger konkret überwacht werden soll), sondern lassen eine Überwachung des gesamten Endgeräts undifferenziert nach Kommu-

nikationsarten zu. Damit überschreitet die vorgesehene Überwachung die ihr eigentlich zugedachte Kompensationsfunktion für den Fall spezieller verschlüsselter Übertragungswege deutlich und ermöglicht eine schrankenlose Erhebung aller Kommunikationspfade. In dem Zusammenhang ist es besonders bedenklich, dass der Begriff des informationstechnischen Systems nicht nur nicht auf eine spezielle Anwendung bzw. einen besonderen Kommunikationspfad bei der Antragstellung einer solchen Maßnahme beschränkt werden muss. Vielmehr ist es in Zeiten zunehmend ubiquitärer Nutzung von digitalen Systemen, Vernetzung von Hausautomation und Sprachassistenzen im privaten Lebensbereich sowohl lokal als auch mittels Systemkomponenten in der Cloud, nach dem Wortlaut des Gesetzentwurfs erlaubt, die Grenzziehung dieses fraglichen informationstechnischen Systems generell vage zu lassen. Durch diese Unschärfe der Begrifflichkeiten besteht die Gefahr, eine nicht überschaubare Fülle möglicher Konstellationen von Überwachungsmaßnahmen zu ermöglichen, die nicht nur weit in das Feld der Online-Durchsuchung, sondern auch in das Feld der akustischen Wohnraumüberwachung hineinragen können.

Des Weiteren stellt die mit der Verankerung der Quellen-Telekommunikationsüberwachung in § 11 G 10-GesetzE gewählte Konstruktion hinsichtlich der Voraussetzungen für eine Beschränkungsmaßnahme maßgeblich darauf ab, dass der Verdacht einer Straftat des Straftatenkatalogs von § 3 Abs. 1 G 10-Gesetz besteht. Die dort genannten Straftaten sind weitgehend auch im Straftatenkatalog des § 100a Abs. 2 StPO enthalten. Die Folge ist, dass zukünftig sowohl die Strafverfolgungs- und Polizeibehörden als auch die Nachrichtendienste in vielen Vorgängen und Sachverhalten mehr oder weniger gleichzeitig gegenüber denselben Personen Quellen-Telekommunikationsüberwachungsmaßnahmen durchführen können. Dies ist aus meiner Sicht mit dem verfassungsrechtlichen Trennungsgebot zwischen Strafverfolgungs- und Polizeibehörden auf der einen sowie den Nachrichtendiensten auf der anderen Seite schwerlich zu vereinbaren. Stehen bereits konkrete Straftaten in Rede und ist es demzufolge angezeigt, dass die Polizeibehörden mit Gefahrenabwehr- oder Strafverfolgungsmaßnahmen operativ tätig werden, besteht insoweit kein Raum für eine zusätzliche nachrichtendienstliche Aktivität. Wie soll es bei einer derartigen „Befugnisparallelität" in der praktischen Anwendung noch möglich sein, die Summe der staatlichen Überwachungsmaßnahmen im Sinne der Überwachungs-Gesamtrechnung des Bundesverfassungsgerichts in einem für eine Demokratie erträglichen Maß zu halten?

In Anbetracht der derzeit schon sehr weitgehenden und umfangreichen Quellen-Telekommunikationsüberwachungsbefugnisse der Polizei- und Strafverfolgungsbehörden besteht bei der gegenwärtigen Gesetzeslage aus meiner Sicht kein Raum, für die Nachrichtendienste anknüpfend an einen Straftatenkatalog die Quellen-Telekommunikationsüberwachungsbefugnis flächendeckend einzuführen. Allenfalls für besonders gewichtige Ein-

zelfälle in Teilbereichen der nachrichtendienstlichen Aufgabenerfüllung erscheint die Schaffung von derartigen Befugnissen bei der gegenwärtig bestehenden Gesamtgesetzeslage überhaupt vorstellbar, wie etwa für die Verifizierung von Informationen eines ausländischen Nachrichtendienstes im Zusammenhang mit Spionagetätigkeiten fremder Mächte.

Im Ergebnis rate ich daher dazu, zum gegenwärtigen Zeitpunkt auf die Einführung der Befugnis der Quellen-Telekommunikationsüberwachung für die Nachrichtendienste vollständig zu verzichten, zunächst das Verfassungsschutzrecht entsprechend der verfassungsrechtlichen Anforderungen von Grund auf zu reformieren und erst anschließend eine verhältnismäßige, passgenaue und bestimmte gesetzliche Befugnis für die Quellen-Telekommunikationsüberwachung zu schaffen. Nur auf diese Weise kann eine Befugnis gestaltet werden, die nur dann und insoweit greift, als die Erkenntnismöglichkeiten der Polizei- und Strafverfolgungsbehörden nicht ausreichen und die über verfassungsrechtliche Bedenken erhaben ist.

In jedem Fall sollte aber § 11 Abs. 1a S. 2 G 10-GesetzE gestrichen werden, weil diese Regelung die Unbestimmtheit und Schrankenlosigkeit der Befugnis in besonderer Weise potenziert und insbesondere auch die Onlinedurchsuchung letztlich faktisch einführt, obwohl dies ausweislich der Aussagen der Bundesregierung gerade nicht gewollt ist.

III. Ausweitung der Pflichten von Telekommunikationsdiensteanbietern (§ 2 Abs. 1a, Abs. 1b G 10-GesetzE)

Um die Umsetzung der Quellen-Telekommunikationsüberwachung in der Praxis auch technisch realisieren zu können, ist vorgesehen, die Mitwirkungspflichten von Telekommunikationsdiensteanbietern auszuweiten. Hierzu werden u.a. in § 2 Abs. 1a Nr. 3 und Nr. 4 G 10-GesetzE für die Unternehmen Pflichten zur Zugangsgewährung, zur Einbringung von technischen Mitteln und zur Mitwirkung bei der Umleitung von Telekommunikation statuiert.

Ein Pflichtenkanon dieses Ausmaßes hat eine fundamental neue, einschneidende Qualität, weil er in dieser Art bisher nur für die Überwachung von internationalem Verkehr durch den BND im Sinne der §§ 5 und 8 G 10-Gesetz, § 110 Abs. 1 S. 1 Nr. 5 TKG sowie §§ 26 bis 29 TKÜV vergleichbar vorgesehen ist. Die Pflichtenausweitung stellt damit einen weitreichenden, bisher nicht dagewesenen Eingriff in die Souveränität der Unternehmen dar und ist deutlich mehr als das bloße Ausleiten einer Kopie der in Rede stehenden Daten. Insbesondere wird in die Integrität des gesamten vom Unternehmen zu verantwortenden informationstechnischen Systems massiv eingedrungen.

Der Gesetzesentwurf beantwortet die Frage nicht, warum die Quellen-Telekommunikationsüberwachung über das für ein Ausleiten Erforderliche hinausgehend ins System eingreifen muss. Unklar ist vor allem, inwieweit mit den Umleitungsmaßnahmen auch eine Manipulation der Telekommunikationsverkehre einhergehen können soll. Richten sich die Maßnahmen ausschließlich gegen individuell genutzte Endgeräte oder z.B. auch gegen Server oder gegen die Update-Prozesse von Software allgemein?

In Folge des enormen Ausmaßes und der bestehenden Unklarheiten beim Eingriff in die Systemintegrität sind die Risiken und Folgen der Umleitungsmaßnahmen in Bezug auf die potentiell betroffenen personenbezogenen Daten nicht abschätzbar und damit nicht minimierbar. Mittelbar wird auch das Vertrauen in Anbieter von Softwarelösungen und Betriebssystemen unterhöhlt.

Es sollte daher in keinem Fall ein Pflichtenumfang für die Telekommunikationsdiensteanbieter vorgesehen werden, der über das für eine Ausleitung der Daten Erforderliche hinausgeht.

IV. Ausbau der Zusammenarbeit zwischen Verfassungsschutzbehörden und Militärischem Abschirmdienst (§ 6 Abs. 2 BVerfSchGE, § 3 Abs. 3 MADGE)

Neben der Schaffung der Quellen-Telekommunikationsüberwachungsbefugnis will der Gesetzesentwurf als Zielstellung vor allem auch die Zusammenarbeit der Verfassungsschutzbehörden mit dem Militärischen Abschirmdienst verbessern. Hierzu sollen Änderungen in § 6 Abs. 2 BVerfSchG und § 3 Abs. 3 MADG vorgenommen werden.

Das sicherheitspolitische Bedürfnis, die Zusammenarbeit zwischen den Behörden in bestimmten Bereichen zu verbessern, ist durchaus anzuerkennen. Allerdings sind als Grundvoraussetzung dafür, dass die Zusammenarbeit zwischen den Inlandsgeheimdiensten intensiviert und ausgebaut werden kann, verfassungskonforme gesetzliche Übermittlungsregelungen zwischen den betreffenden Behörden unerlässlich. Ohne diese kann die Zielstellung nicht erreicht werden. § 6 Abs. 2 BVerfSchG und § 3 Abs. 3 MADG – auch in der avisierten Ausgestaltung – genügen in Bezug auf Datenübermittlungen den vom Bundesverfassungsgericht aufgestellten Anforderungen nicht (vgl. wiederum BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17). Ebenso wenig helfen §§ 18 ff. BVerfSchG bzw. §§ 10, 11 MADG diesbezüglich weiter. Daher verfehlen die angedachten Änderungen ihre Wirkung bzw. sie können die gesetzte Zielstellung nicht erreichen.

Die Übermittlungsregelungen des Bundesverfassungsschutzgesetzes und des Gesetzes über den militärischen Abschirmdienst bedürfen einer umfassenden grundlegenden

BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Reformierung. Losgelöst davon sollte der Gesetzgeber keine einzelnen Änderungen zur Stärkung der Zusammenarbeit zwischen den Inlandsgeheimdiensten ins Auge fassen.

Mit freundlichen Grüßen

[redacted]

Ulrich Kelber