19. Wahlperiode

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Wortprotokoll
der 117. Sitzung

Ausschuss für Inneres und Heimat
Berlin, den 25. Januar 2021, 10:00 Uhr
10557 Berlin
Konrad-Adenauer-Str. 1
Paul-Löbe-Haus, Raum 4 900

Vorsitz: Andrea Lindholz, MdB

Tagesordnung - Öffentliche Anhörung

Gesetzentwurf der Fraktionen der CDU/CSU und SPD

Entwurf eines Gesetzes zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020

BT-Drucksache 19/25294

Federführend:
Ausschuss für Inneres und Heimat

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

Berichterstatter/in:
Abg. Nina Warken [CDU/CSU]
Abg. Uli Grötsch [SPD]
Abg. Dr. Christian Wirth [AfD]
Abg. Manuel Höferlin [FDP]
Abg. Petra Pau [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

Inhaltsverzeichnis

Mitglieder des Ausschusses

	Ordentliche Mitglieder	**Stellvertretende Mitglieder**
CDU/CSU	Lindholz, Andrea Müller, Axel Throm, Alexander Warken, Nina	
SPD	Grötsch, Uli	
AfD	Wirth, Dr. Christian	
FDP	Höferlin, Manuel Kuhle, Konstantin	
DIE LINKE.		Movassat, Niema
BÜNDNIS 90/DIE GRÜNEN	Notz, Dr. Konstantin von	
fraktionslos		

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 25. Januar 2021, 10.00 Uhr
„Bestandsdatenauskunft“

Prof. Dr. Matthias Bäcker
Johannes Gutenberg-Universität Mainz

Jonas Breyer
Rechtsanwalt und zertifizierter Datenschutzbeauftragter, Wiesbaden

Prof. Ulrich Kelber
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn

Prof. Dr. Markus Löffelmann
Hochschule des Bundes für öffentliche Verwaltung
Nationales und internationales Sicherheitsrecht, Berlin

Holger Münch
Präsident des Bundeskriminalamts, Wiesbaden

Prof. Dr. Kyrill-Alexander Schwarz
Julius-Maximilians-Universität Würzburg

Einziger Tagesordnungspunkt

Gesetzentwurf der Fraktionen der CDU/CSU und SPD

Entwurf eines Gesetzes zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020

BT-Drucksache 19/25294

Vors. **Andrea Lindholz** (CDU/CSU): Dann darf ich Sie alle ganz herzlich begrüßen heute Morgen und unsere Sitzung hiermit auch eröffnen. Es ist unsere 117. Sitzung – die öffentliche Anhörung zum Thema Bestandsdatenauskunft von 10:00 bis 12:00 Uhr. Ich darf Ihnen allen zunächst, die ich noch nicht gesehen habe, auch noch mal ein gutes neues Jahr wünschen. Und dann würden wir mit der Anhörung wie üblich wie folgt vorgehen: Wir werden auch heute wieder live übertragen. Es wird im Anschluss danach das Protokoll, das heute erstellt wird, allen zusammen mit den von Ihnen eingereichten Stellungnahmen in einer Gesamtdrucksache übersandt. Ich bedanke mich an dieser Stelle auch ganz herzlich für die hier eingegangenen Stellungnahmen. Von der Anhörung wird wie üblich ein Wortprotokoll angefertigt. Zeitfenster hatte ich schon gesagt: zwei Stunden. Wir werden zunächst jedem Sachverständigen wieder die Gelegenheit geben, ein kurzes Einführungsstatement zu geben. Wenn möglich sollte es so um die fünf Minuten dauern. Danach kommt die Fragerunde der Kolleginnen und Kollegen. Bei der Fragerunde haben wir uns auf folgendes Prozedere geeinigt: Es werden erst alle Fragen gestellt. Jeder Kollege jeder Fraktion hat die Möglichkeit, in der ersten Runde entweder zwei Fragen an einen Sachverständigen zu stellen, eine gleiche Frage an zwei Sachverständige oder an zwei Sachverständige jeweils eine unterschiedliche Frage. Wenn wir dann noch eine zweite Runde zeitlich hinbekommen, schauen wir, wie wir es dann machen. Und im Anschluss an die gestellten Fragen erhält dann wieder jeder Sachverständige die Möglichkeit, darauf gesammelt zu antworten. Ich hoffe, ich habe nichts vergessen. Dann können wir loslegen. Und wir beginnen mit Herrn Professor Bäcker, der uns zugeschaltet ist. Herr Professor Bäcker, bitte.

SV **Prof. Dr. Matthias Bäcker** (Johannes Gutenberg-Universität Mainz): Vielen Dank, Frau Vorsitzende und meine Damen und Herren. Ich bedanke mich für die Gelegenheit, zu dem Gesetzentwurf Stellung zu nehmen. Der Gesetzentwurf hat eine doppelte Reparaturfunktion. Er soll zum einen die Regelungen über die Auskunft über Telekommunikationsbestandsdaten an die jüngste Entscheidung des Bundesverfassungsgerichts anpassen, die diese Regelungen im geltenden Recht teilweise beanstandet hat. Und er soll einen Teil des Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität reparieren, der in der Folge dieser Entscheidung des Bundesverfassungsgerichts offensichtlich den verfassungsrechtlichen Anforderungen nicht genügt hat und darum auch vom Bundespräsidenten nicht ausgefertigt worden ist. Das Gesetz erfüllt seine Funktion im Wesentlichen im Hinblick auf die Telekommunikationsdaten. Da werden die Vorgaben des Bundesverfassungsgerichts grundsätzlich eingearbeitet. Es weist aber zwei Haken auf. Das eine betrifft die Regelung der Bestandsdatenauskunft wieder über Telekommunikationsdaten, weil hier eine Rechtsschicht noch mit zu beachten ist, nämlich das Unionsrecht. Der Gesetzentwurf repariert die Regelungen auf dem Niveau, das das Bundesverfassungsgericht vorgegeben hat, aber das Niveau, das aus dem Unionsrecht für die Anforderungen an Bestandsdatenabrufe folgt, das ist teilweise höher und das wird nicht abgebildet.

Konkret geht es um Folgendes: Das Gesetz regelt unter anderem, dass Bestandsdaten durch ein Telekommunikationsunternehmen an eine Sicherheitsbehörde übermittelt werden dürfen, wobei es hier darum geht, dass eine dynamische IP-Adresse aufgelöst wird und dann die Kontaktdaten der betroffenen Personen herausgegeben werden. Das ist im Prinzip auch in Ordnung, so wie das Gesetz das regelt, aber nicht in einem Sonderfall, nämlich in dem Sonderfall, dass die IP-Adresse ein Datum ist, das auf Vorrat gespeichert worden ist nach den § 113a ff. TKG (Telekommunikationsgesetz). Der Gerichtshof der Europäischen Union (EuGH) hat in einer Grundsatzentscheidung zur Vorratsdatenspeicherung am 6. Oktober des letzten Jahres gesagt, dass zwar IP-Zuordnungsdaten, anders als andere Verkehrsdaten, im Prinzip auf Vorrat anlasslos gespeichert werden dürfen, dass dann aber relativ strenge Anforderungen an den Abruf dieser Daten bestehen. Es muss konkret gehen um den Schutz der nationalen Sicherheit, um die Bekämpfung einer schweren Straftat oder um die

Abwehr einer schwerwiegenden Gefahr für die öffentliche Sicherheit, wobei der unionsrechtliche Begriff der öffentlichen Sicherheit enger ist als der Begriff, den wir aus dem deutschen Recht kennen, der die ganze Rechtsordnung umfasst. Das Gesetz sieht nun vor, dass eine Übermittlung von solchen „Vorratsdatenverwendungsdaten“ generell zulässig ist zur Aufgabenerfüllung der Nachrichtendienste, zur Verfolgung jeglicher Straftaten ohne jede Einschränkung und zur Abwehr einer Gefahr für ein Rechtsgut von hervorgehobenem Gewicht. Das ist eine Formulierung, die vom Bundesverfassungsgericht übernommen wird und die bedeutet, dass es sich um ein Rechtsgut handeln muss, das zwar schon ein bisschen mehr ist als völlig bagatellarisch, das aber kein erhebliches Gewicht haben muss. Keine dieser Anforderungen genügt meiner Ansicht nach der Entscheidung des Europäischen Gerichtshofs, was dazu führt, dass die Regelung in Verbindung mit der Vorratsdatenspeicherung unionsrechtswidrig ist.

Das zweite und etwas grundlegendere und auch konzeptionelle Problem ist, dass das Gesetz neben dem Abruf von Telekommunikationsdaten auch die Übermittlung und den Abruf von Telemediendaten ermöglicht. Und die werden im Wesentlichen genauso behandelt wie Telekommunikationsdaten. Dafür gibt es andere Regelungen, aber in denen steht, was die Schwelle der Datenverwendung angeht, mehr oder weniger dasselbe. Das Problem ist, dass diese Parallelisierung nicht ganz aufgeht. Telemediendaten sind viel heterogener als Telekommunikationsdaten, weil es viel mehr viel unterschiedlichere Telemediendienste gibt. Es ist auch gar nicht so einfach, die unterschiedlichen Kategorien von Telemediendaten auseinanderzuhalten. Es ist zum Beispiel nicht so klar, ob es neben den im Gesetzentwurf angesprochenen Bestands- und Nutzungsdaten noch eine weitere Kategorie der Inhaltsdaten gibt. Jedenfalls aber kann man meiner Ansicht nach bei einer gebotenen pauschalen typisierenden Betrachtung feststellen, dass Telemediendaten eine höhere Sensibilität aufweisen als Telekommunikationsdaten. Das führt zum einen dazu, dass die vorgesehene Übermittlung von Bestandsdaten unter denselben Voraussetzungen wie Telekommunikationsbestandsdaten eine zu niedrige Schwelle aufweist. Und was meiner Ansicht nach definitiv nicht geht, ist, dass Telemediennutzungsdaten, die mit Sicherheit sehr sensibel sein können, unter denselben Voraussetzungen übermittelt werden können wie Telemedienbestandsdaten. In diesem Punkt ist der Gesetzentwurf meiner Ansicht nach evident unzureichend. Und ich kann mir nicht vorstellen, dass die Regelungen insoweit halten. Bei den Bestandsdaten würde ich fairerweise einräumen, dass man es probieren kann, bei den Nutzungsdaten sehe ich es nicht. Jedenfalls in diesem Punkt sollte die Reparatur nochmals repariert werden. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann ist uns zugeschaltet Herr Breyer, bitte.

SV **Jonas Breyer** (Rechtsanwalt, Wiesbaden): Vielen Dank für die Möglichkeit, dass ich kurz Stellung nehmen kann zu Ihrem Gesetzentwurf zur Neuregelung der Bestandsdatenauskunft. Ich habe in dem letzten Verfahren vor dem Bundesverfassungsgericht die Beschwerdeführer vertreten. Und der Entwurf beseitigt die Mängel, die das Bundesverfassungsgericht genannt hat, leider nur teilweise, weswegen ich fürchte, dass es zu einer weiteren Entscheidung Bestandsdatenabfrage III kommen wird. Es ist zunächst mal kurz daran zu erinnern, dass nach der Rechtsprechung des Bundesverfassungsgerichts auch die Abfrage von Bestandsdaten von hoher Bedeutung ist, weil die Anonymität der Telekommunikation damit durchbrochen wird, wie artikuliert worden ist in der Entscheidung Bestandsdatenauskunft I. Und die Daten liegen deshalb im Umfeld verfassungsrechtlich besonders geschützter Informationsbeziehungen, wie es heißt. Ich habe zehn kurze Kritikpunkte herausgegriffen, wobei ich mich kurz fassen werde oder es zumindest versuchen will, insbesondere dort, wo sich der Sachverständige Professor Bäcker auch schon dazu gehäußert hat.

Erstens: Das Erfordernis der konkreten Gefahr. In verschiedenen Abrufgesetzen, nämlich dem Bundesverfassungsschutzgesetz, dem MAD-Gesetz und dem BND-Gesetz, fehlt das Erfordernis einer konkreten oder zumindest einmal einer drohenden Gefahr. Und in der Begründung heißt es dazu, dass die Nachrichtendienste ohnehin dem Schutz besonders gewichtiger Rechtsgüter dienten. Aber dieses geringe Erfordernis hat das Bundesverfassungsgericht nur für einen speziellen Fall genügen lassen, nämlich, wenn die Auskunft zur Aufklärung einer bestimmten nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten ist. Und das bildet der

Entwurf nach meiner Überzeugung nicht ab, insbesondere reicht es auch nicht, auf die allgemeine Aufgabenbeschreibung im Bundesverfassungsschutzgesetz und den entsprechenden Fachvorschriften hinzuweisen. Und dementsprechend sind auch die Übermittlungsregelungen anzupassen.

Punkt 2 betrifft die konkrete Gefahr bei IP-Adressen. Der Entwurf regelt bekanntermaßen auch den Abruf von Bestandsdaten anhand dynamisch zugeteilter IP-Adressen. Er verzichtet aber auf das Vorliegen einer konkreten Gefahr im Bereich des Polizeirechts. Und wegen des sogenannten erhöhten Eingriffsgewichts, wie es das Bundesverfassungsgericht formuliert hat, ist das aber unzulässig und das Erfordernis gilt insbesondere auch für Nachrichtendienste. Ich verweise auf Randnummer 176 der Entscheidung.

Punkt 3 betrifft die Mitwirkung an der Mitwirkung. Ist nicht so ganz tragisch vielleicht, aber ist ein handwerklicher Fehler, nämlich der Gesetzentwurf verpflichtet in einer ganzen Reihe von Vorschriften auch diejenigen, die an der Erbringung von Telekommunikationsdiensten mitwirken. Aber wer an Telekommunikationsdiensten mitwirkt, ist schon selbst ein Telekommunikationsanbieter – siehe § 3 Nummer 6 TKG. Von daher wird hier geregelt eine Mitwirkung an der Mitwirkung, die wahrscheinlich nicht beabsichtigt ist.

Punkt 4 betrifft die sehr unbestimmten Eingriffsschwellen. So knüpft der Entwurf unter anderem im Bundespolizeigesetz, im BKA-Gesetz an, im Einzelnen ist das in meiner schriftlichen Stellungnahme dann noch nachzulesen, da knüpft ja die Bestandsdatenauskunft von dynamischen IP-Adressen an sogenannte bedrohte Rechtsgüter von erheblichem Gewicht, an Rechtsgüter von hervorgehobenem Gewicht, an gewichtige Rechtsgüter und an besonders gewichtige Rechtsgüter. Es trifft zwar zu, dass diese Terminologie vom Bundesverfassungsgericht so verwendet worden ist in seiner Entscheidung und dass man es damit auch so ungefähr eingrenzen kann, wenn man die Rechtsprechung des Bundesverfassungsgerichts kennt; es ist aber dennoch, selbst wenn man sie kennt, relativ unkontrolliert und sehr rechtsanwenderunfreundlich und wird meines Erachtens zu einer großen Rechtsunsicherheit und zu unzulässigen Datenabrufen führen. Und Entsprechendes gilt auch für Straftaten von erheblicher Bedeutung, auf die Bezug genommen wird. Außerdem spricht der Entwurf beispielsweise in § 40 BKA-Gesetz nur von einer Gefahr, ohne überhaupt irgendein Rechtsgut zu nennen. Das ist zu wenig. Ich schlage vor, dass man hier auf bestehende Kataloge zurückgreift, etwa in § 100a Absatz 2 StPO.

Punkt 5 betrifft die fehlende Erforderlichkeit, nämlich in mehreren Normen, dem Zollfahndungsdienstegesetz, dem TMG (Telemediengesetz) und dem TKG muss ein Auskunftsverlangen die Abwehr einer Gefahr nur zum Gegenstand haben, wie es dort heißt. Richtigerweise muss sie aber dafür erforderlich sein. Darauf hat das Bundesverfassungsgericht auch hingewiesen. Und es wäre ansonsten eine Vorratsdatenspeicherung möglich, wenn es denn nur der Aufgabe der Behörde dient – und das genügt nicht.

Punkt 6 betrifft das zeitlich absehbare Geschehen. Im Bundespolizeigesetz, im BKA-Gesetz, in anderen Vorschriften werden Eingriffe daran geknüpft, dass „Tatsachen den Schluss auf einen wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, an dem bestimmte Personen beteiligt sein werden“. Auch dabei handelt es sich um eine abstrakte Formel, die kopiert worden ist aus der Entscheidung des Bundesverfassungsgerichts, die aber unscharf ist. Und es wäre Aufgabe des politischen Gesetzgebers, diese mit Leben zu füllen und entsprechend Zeitfaktor, Geschehen und die benannten beteiligten Personen zu benennen, ansonsten drohen auch hier Rechtsunsicherheiten.

Punkt 7 betrifft weitere Unklarheiten in den Übermittlungsregelungen. Ich versuche, mich hier kurz zu halten. Zunächst mal gibt es ja bereits heute schon Regelungen zur Datenübermittlung an Behörden in § 14 des Telemediengesetzes. Es ist aus meiner Sicht unklar, wie sich die neuen Übermittlungsregelungen im § 15a und b TMG eigentlich hierzu verhalten. In § 15a Absatz 2 des Telemediengesetzes ist die Rede von einer elektronischen Bestätigung. Hier ist es meines Erachtens unklar, ob eigentlich die elektronische Form nach § 126a BGB oder vielleicht auch nach § 3a VwVfG oder ob einfach nur eine E-Mail gemeint ist. Dann regelt der Entwurf zwar zunächst im Ansatz richtigerweise in § 15a Absatz 6 des Telemediengesetzes, dass eine Übermittlung an die Behörden nur erfolgen darf, wenn die Voraussetzungen auch der Abrufnorm erfüllt sind. Und nur dann ist auch

die Übermittlung zulässig. Das ist richtig und hat das Bundesverfassungsgericht in Randnummer 201 seiner Entscheidung auch betont. Aber die privaten Diensteanbieter, die die Daten übermitteln sollen, haben mangels Informationen überhaupt nicht die Möglichkeit, in der Praxis das Vorliegen dieser Voraussetzungen zu prüfen.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Breyer, wir sind schon bei sieben Minuten, wenn ich darauf hinweisen dürfte.

SV **Jonas Breyer** (Rechtsanwalt, Wiesbaden): Ja, okay. Gut, ich habe in meiner schriftlichen Stellungnahme angeregt, dass den Anbietern, also in Kurzform zumindest, die entsprechenden Informationen übermittelt werden.

Dann geht es noch um die Nutzungsdaten – Punkt 8 – in der StPO und im TMG. Und hier schließe ich mich dem an, was auch Herr Professor Bäcker schon gesagt hat: Es wird der Tiefe des Grundrechts eigentlich nicht gerecht, wenn also die Übermittlung von Nutzungsdaten so ermöglicht wird, wie derzeit im Entwurf. Sie müssen vielmehr den Telekommunikationsinhaltsdaten gleichgestellt werden. Es handelt sich unter anderem um URLs, also um aufgerufene Internetseiten.

Dann der vorletzte Punkt ist der Abruf von Zugangsdaten im Bundespolizeigesetz, im BKA-Gesetz und noch mehr. Auch hier versucht man, wieder Zugangsdaten abzurufen, hinter denen sich allerdings oft auch andere Dienste, wie zum Beispiel Cloudspeicher, verbergen, weswegen auch hier unzulässige Datenzugriffe drohen. In vielen Fällen müssen Passwörter auch verschlüsselt gespeichert werden, sodass eine Herausgabe nicht möglich ist.

Der letzte Punkt betrifft die fehlende Statistik. So regelt der Entwurf leider keine statistischen Aufzeichnungspflichten, die aber der Öffentlichkeit zugänglich gemacht werden sollten, sodass das Ausmaß der Eingriffe für die Bürger nachvollziehbar wird. Auch hier habe ich in meiner schriftlichen Stellungnahme einen Formulierungsvorschlag vorbereitet. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Breyer, vielen Dank. Es liegt uns allerdings keine schriftliche Stellungnahme vor. Die ist bei uns bis heute nicht eingegangen. Und vielleicht noch eine kleine Anmerkung: Also, ich bin irgendwann nicht mehr in der Lage gewesen, dem Vortrag zu folgen. Es macht Sinn für die Kolleginnen und Kollegen, wenn man sich auf die wesentlichsten Sachen konzentriert, den Rest in der schriftlichen Stellungnahme nachliefert, weil, vielleicht ging es ja auch nur mir so, aber ich bin nicht in der Lage, so viele Fakten auf einmal zu erfassen. Herr Professor Kelber ist als nächstes in der alphabetischen Reihenfolge dran.

SV **Prof. Ulrich Kelber** (BfDI, Bonn): Vielen Dank, Frau Vorsitzende. Einen grundsätzlichen Punkt vielleicht zu Beginn: Gegenstand der Anhörung ist ein Korrekturgesetz, weil das Bundesverfassungsgericht erneut gesetzliche Vorschriften für unvereinbar mit der Verfassung erklärt hat. Und ich darf daran erinnern, das steht in einer Reihe mit anderen Entscheidungen, die den gleichen Kern betreffen: Die jüngste Entscheidung zur Auslandsauslandsüberwachung, zur Vorratsdatenspeicherung, zur Onlinedurchsuchung, zur präventiven Telekommunikationsüberwachung, zur Antiterrordatei und zu heimlichen Ermittlungsmaßnahmen nach dem BKA-Gesetz. Der Geist dieser Entscheidungen sollte insgesamt in den Blick genommen und umgesetzt werden. Wir brauchen eine Gesetzgebung und eine Behördenpraxis, die sich planvoll an grundrechteschützenden Konzepten orientiert und diese Zusammenhänge in den Blick nimmt und eben nicht geforderte oder gewünschte Einzelbefugnisse in den Mittelpunkt stellt.

Zum konkreten Entwurf: Die Auskunft über Bestandsdaten ist für die Tätigkeit der Sicherheitsbehörden von großer praktischer Bedeutung. Jede Erhebung und Übermittlung von Bestandsdaten ist dabei mit einem Eingriff in die informationelle Selbstbestimmung der betroffenen Person und gegebenenfalls in das Telekommunikationsgeheimnis verbunden. Mittlerweile umfasst die Bestandsdatenauskunft nicht mehr nur die klassischen Bestandsdaten wie Name, Anschrift oder Rufnummer eines Teilnehmers, sondern auch Karten- und Gerätenummer von Mobilfunkkunden, Zugangscodes wie PIN und PUKs, auch dynamische IP-Adressen können herangezogen werden. Dementsprechend müssen die die Bestandsdatenauskunft betreffenden Regelungen bestimmten verfassungsrechtlichen Anforderungen genügen. Die wurden einmal im Jahr 2012 durch das Verfassungsgericht konkretisiert und jetzt noch mal am 27. Mai 2020. Dass die Vorgaben aus dieser

neuen Entscheidung so zeitnah umgesetzt werden, begrüße ich ausdrücklich. Bei einem solchen komplexen und bedeutenden Gesetzesvorhaben mit hoher Grundrechtsrelevanz ist aber eine Stellungnahmefrist zur abschließenden Version von knapp einer Woche weder sachgerecht noch angemessen. Einige Kritikpunkte, die ich in dem Verfahren vorgebracht hatte, sind offensichtlich berücksichtigt worden. Dafür vielen Dank. Die drei Schwerpunkte meiner verbleibenden Kritik möchte ich im Folgenden aufzeigen – bei weiteren Einzelheiten verweise ich auf die schriftliche Stellungnahme:

Erstens. Bestandsdatenauskünfte zur Verfolgung von Ordnungswidrigkeiten halte ich für unverhältnismäßig, § 113 TKG, § 15a TMG, § 30 Zollfahndungsdienstgesetz ermöglichen diese aber. Die im TMG vorgesehene Befugnis zur Übermittlung von Nutzungsdaten hat sogar eine noch höhere Eingriffsqualität als die Übermittlung klassischer Bestandsdaten.

Zweitens. Um beim TMG zu bleiben: Die in § 15a und 15b vorgesehene Berücksichtigung sämtlicher unternehmensinterner Datenquellen lässt die Herausgabe umfangreicher Nutzungsprofile befürchten und sollte deshalb gestrichen werden. Außerdem sehe ich die Regelung in § 15b zur Passwortherausgabe weiterhin sehr kritisch. Der mit dieser Regelung verbundene Verlust an Datensicherheit ist nicht gerechtfertigt. Es sind weitreichende Befugnisse auch dort vorgesehen, wo diese nicht erforderlich sind, beispielhaft sei § 22a Bundespolizeigesetz genannt. Situationen, in denen die Bundespolizei in ihrer Funktion als Sonderpolizei mit begrenztem Aufgabenspektrum Daten von Telemedienanbietern benötigt, dürften sich wenn überhaupt nur auf wenige Fälle beschränken. Die Regelung sollte entfallen.

Drittens. Die Änderung der nachrichtendienstlichen Vorschriften decken grundlegende Mängel der Gesetzessystematik auf. Die in § 8d Bundesverfassungsschutzgesetz und § 4b MAD-Gesetz aufgenommene Formulierung „zur Aufklärung bestimmter Bestrebungen oder Tätigkeiten“ bleibt zu stark auslegungsbedürftig und genügt damit eben nicht dem Bestimmtheitsgrundsatz. Die Voraussetzungen zur Festlegung dieser bestimmten Bestrebungen oder Tätigkeiten müssen sich im Gesetzestext finden. Grundlegende Fragestellungen wie die Voraussetzung zur Überschreitung der Schwelle zur Beobachtungsbedürftigkeit müssen in den nachrichtendienstlichen Gesetzen und nicht wie bislang in untergesetzlichen als Verschlusssache eingestuften Vorschriften bestimmt werden. In diesem Kontext kann ich nur meine Forderung nach einer Atempause für neue Eingriffsbefugnisse und einer dringend notwendigen umfassenden Gesamtreform wiederholen, auch in den Bereichen, die vom Bundesverfassungsgericht noch nicht spezifisch behandelt wurden Vielen Dank soweit.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank, Herr Professor Kelber. Als nächstes hätten wir dann Herrn Professor Löffelmann, bitte.

SV **Prof. Dr. Markus Löffelmann** (HS Bund, Berlin): Vielen Dank. Sehr geehrte Frau Vorsitzende, meine Damen und Herren Abgeordnete, zunächst einmal herzlichen Dank für die Einladung zu dieser Sachverständigenanhörung. Ich habe Ihnen in meiner schriftlichen Stellungnahme eine ganze Reihe von eher technischen Problempunkten aufgezeigt, auf die ich hier nicht näher eingehen kann. Ich möchte mich aus Zeitgründen auf vier etwas grundsätzlichere Aspekte beschränken.

Der erste Punkt betrifft den schillernden Begriff der „drohenden Gefahr“. Bei diesem Begriff handelt es sich um einen neuen, höchst umstrittenen technischen Gefahrbegriff, der erstmals vom bayerischen Gesetzgeber 2017 eingeführt wurde. Im Bund und auf Länderebene hat er sich seitdem nicht durchgesetzt. Im hiesigen Gesetzentwurf taucht er 23-mal auf. Dieser Begriff führt zwangsläufig zu sprachlichen Irritationen im Sinne eines Drohens einer drohenden Gefahr. Ich habe Ihnen das auch in meiner schriftlichen Stellungnahme an zwei Beispielen aus der Gesetzesbegründung nachgewiesen. Bei diesen sprachlichen Unschärfen handelt es sich, meine Damen und Herren, um keine Kleinigkeit, sondern sie betreffen die Schaffung eines neuen Gefahrbegriffs, der das gesamte Polizeirecht überspannt und neue Handlungsräume eröffnet. Ich denke, man sollte mit diesem Begriff sehr vorsichtig umgehen. Und man kann auf ihn verzichten. Er führt zu Verwirrung, er beinhaltet deshalb ein Bestimmtheitsproblem, und er ist ganz und gar unnötig, um das Gefahrenvorfeld, um das es geht, zu kennzeichnen.

Zweitens. Dieser Punkt wurde teilweise schon von dem Vorredner, Rechtsanwalt Breyer, angesprochen. Der Gesetzentwurf übernimmt, wie zuvor

schon andere Gesetzgebungsvorhaben, wörtlich Formulierungen des Bundesverfassungsgerichts zum Gefahrenvorfeld in den Gesetzestext. Aber damit nicht genug. Darüber hinaus kennzeichnet er materielle Eingriffsschwellen durch vom Bundesverfassungsgericht verwendete Begriffe wie herausragendes Rechtsgut, Rechtsgut von erheblichem Gewicht oder Rechtsgut von besonderem Gewicht. Der Inhalt dieser Begriffe lässt sich aber weder aus dem Gesetz erschließen noch ist er durch eine ständige Rechtsprechung ausgefüllt. Nun kann man füglich über die Konsistenz dieses verfassungsgerichtlichen Begriffssystems streiten. Auf jeden Fall macht es einen bedeutenden Unterschied, ob das Bundesverfassungsgericht solche Begriffe aus einer Haltung des *judicial restraint* heraus verwendet und dem Gesetzgeber dadurch gerade Gestaltungsspielräume öffnet oder ob der Gesetzgeber sie in den Gesetztext übernimmt. Zugespitzt sind die Attribute „besonders“ oder „hervorgehoben“ nicht so besonders, dass dadurch ein besonderes oder hervorgehobenes Gewicht eines Rechtsguts präzise und normenklar charakterisiert würde.

Drittens. Der Umfang der Prüfpflichten der Anbieter. Das Doppeltür-Modell unterscheidet bekanntlich zwischen Übermittlung und Abfrage. Bei der Anwendung der Übermittlungsnorm stellt sich nun ein sehr grundlegendes Problem, das bislang überhaupt nicht thematisiert wurde, was mich auch etwas verwundert. In welchem Umfang sind die Anbieter eigentlich zur Prüfung ihrer Berechtigung zur Datenübermittlung verpflichtet? Nach den Übermittlungsnormen des TMG und TKG müssen sie zwei Voraussetzungen prüfen: Erstens, ob die abfragende Stelle die Auskunft unter Angabe einer gesetzlichen Bestimmung verlangt, die eine Erhebung der Daten erlaubt. Und zweitens, ob die abfragende Stelle eine der in der Übermittlungsnorm sehr detailliert ausbuchstabierten Aufgaben wahrnimmt. Beides, meine Damen und Herren, beinhaltet eine materielle Prüfung anhand des Gesetzestextes und stellt keine rein formale Prüfung dar. An anderer Stelle heißt es dann, – ich zitiere aus dem Gesetzentwurf – „die Verantwortung für die Zulässigkeit der Auskunft tragen die um Auskunft ersuchenden Stellen“. Aber was soll das bedeuten? Welche Art von Verantwortung? Die zivilrechtliche für etwaige Schadenersatzansprüche? Eine disziplinarrechtliche, eine politische oder ethische? Resultieren daraus Überwachungspflichten für die abfragenden Stellen? Wie sind diese ausgestaltet? Eines ist klar: Wenn man die rechtliche Prüfung der Voraussetzungen für die Übermittlung nicht den Anbietern, sondern vollständig den Fachbehörden auferlegt, widerspricht das fundamental der Systematik des Gesetzes und dann macht das gesamte Doppeltür-Modell überhaupt keinen Sinn.

Das führt mich nun zu meinem vierten Punkt, der die Praktikabilität des Gesetzes betrifft. Hier möchte ich zu Ihnen, meine Damen und Herren, als ehemaliger langjähriger Justizpraktiker sprechen, der heute für die Nachrichtendienste die Personen ausbildet, die letztlich für die Anwendung des Gesetzes verantwortlich sind. Das gegenständliche Gesetz hat in meinen Augen einen derart hohen Grad an Ausdifferenziertheit und Komplexität erreicht, dass darunter die Verlässlichkeit der Rechtsanwendung leidet. Dabei betrifft die Bestandsdatenabfrage nur einen kleinen Ausschnitt der Datentransfers im Sicherheitsrecht. Ein so kompliziertes System dient aus Praktikersicht weder der Rechtssicherheit noch dem Grundrechtsschutz. Meines Erachtens ist über die Thematik der Bestandsdatenabfrage hinausreichend ein einfacheres, leichter verständliches und anwendbares Ordnungssystem zwingend erforderlich. Wie ein solches System aussehen könnte, das habe ich vor zwei Jahren einmal in einem Zeitschriftenbeitrag skizziert. Ich denke wirklich, wir müssen die Einfachheit und Anwendungsfreundlichkeit von Gesetzen wieder als wichtigen Eigenwert begreifen. Davon profitieren der Grundrechtsschutz und die Rechtssicherheit und das schuldet man all den Praktikern, die die Gesetze anwenden sollen und auch den Bürgerinnen und Bürgern, deren Grundrechte eingeschränkt werden. Ich bedanke mich für Ihre Aufmerksamkeit.

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

SV **Holger Münch** (Bundeskriminalamt, Wiesbaden): Vielen Dank, Frau Vorsitzende. Ich würde mich gerne auf die praktische Bedeutung von manuellen Bestandsabfragen, hier insbesondere jetzt für das BKA, konzentrieren, die aufgabenübergreifend eben eine hohe Bedeutung haben. Sie stellen in vielen Fällen einen wichtigen, wenn nicht gar den einzigen Ermittlungsansatz zur Identifizierung etwa eines Beschuldigten oder Gefährders dar, sei es im Bereich der klassischen Telefonie, bei der Nutzung von Messenger-

Diensten, E-Mail-Anbietern oder von sonstigen Kommunikationsdiensten über das Internet. Ziel jeder dieser Bestandsdatenauskunftsanfragen ist es, den jeweiligen Telekommunikationsteilnehmer über seine Rufnummer oder Kennung als Anschlussinhaber einschließlich anhand einer bereits polizeilich bekannten dynamischen IP-Adresse und Zeitstempel zu ermitteln. So kann der Nutzer identifiziert beziehungsweise weitere Ermittlungsansätze können gewonnen werden. Ohne jetzt auf eine detaillierte Statistik im BKA für Bestandsdatenabfragen zurückgreifen zu können, ist mittelbar über die Kosten, die uns entstehen für die Entschädigungsleistungen an die Provider von mehreren tausend Anschlussinhaberfeststellungen pro Jahr im manuellen Verfahren allein im BKA auszugehen.

Ohne die Möglichkeit, manuell Bestandsdaten bei den Verpflichteten abfragen zu können, wäre die Arbeit des BKA in vielen Bereichen erheblich eingeschränkt. So wäre zum Beispiel die künftige Bearbeitung der Meldung strafbarer Inhalte durch die sozialen Netzwerke nach § 3a des NetzDG neu ohne die Möglichkeit von manuellen Bestandsdatenabfragen für das BKA praktisch ausgeschlossen. Ebenso lassen sich in anderen Phänomenbereichen der Zentralstelle, etwa im Prüfverfahren des BKA im Bereich der politisch motivierten Kriminalität, vielfach mittels Bestandsdatenabfragen neue Ermittlungsansätze generieren und so Hinweise auf Netzwerke aufklären; somit kann der Vorgang an die erkennbare zuständige Strafverfolgungsbehörde abverfügt werden. Gleiches gilt für die Aufgabe der Abwehr von Gefahren des internationalen Terrorismus. In Verfahren, in denen Störer hochkonspirativ kommunizieren, ist es immer wieder erforderlich, neu verwendete oder erst im Rahmen der Ermittlungen bekannt gewordene Nutzerkonten oder Rufnummern mittels entsprechender Abfragen abzuklären, um bestehende oder bislang unbekannte Störer oder mögliche Kontaktpersonen diese zuzuordnen beziehungsweise diese identifizieren zu können. Auch die Sicherungsgruppe des BKA oder die Zeugenschutzdienststellen im BKA profitieren von diesem Instrument. Es wird bei der Prüfung von Gefährdung von Schutzpersonen gemäß § 6 und § 7 BKA-Gesetz herangezogen, um die jeweilige Gefährdungslage einschätzen und die Verursacher identifizieren zu können. So ist es in solchen Fällen notwendig, Personen, die Straftaten zum Nachteil von Schutzpersonen per E-Mail, telefonisch oder schriftlich oder über soziale Netzwerke androhen, zu identifizieren und zu prüfen, ob sie in der Lage wären, diese angedrohten Taten auch wirklich umzusetzen. Um das bei einem Beispiel konkret zu machen: Im letzten Jahr erlangte das BKA im Zuge einer Veranstaltungstour des Bundesministers für Gesundheit zur Corona-Krise Kenntnis von E-Mails und Postings in sozialen Netzwerken, in denen auch die Gewaltanwendung gegen den Minister angedroht wurde. Und diese manifestierten sich in öffentlichen Aufrufen zu Straftaten. Im Rahmen von OSINT-Recherchen (Open Source Intelligence) wurden E-Mail-Adressen und IP-Adressen festgestellt, welche dann mittels Bestandsdatenabfrage zur Identifizierung der Störer führten. Und dann kann das BKA auf die jeweils aktuellen Situationen vor Ort reagieren und konkrete Maßnahmen zum Schutz der Schutzperson einleiten.

Für eine erfolgreiche Kriminalitätsbekämpfung in Deutschland und für eine erfolgreiche Wahrnehmung unserer Aufgaben im BKA ist es daher von großer Bedeutung, dass die Bestandsdatenauskunft in angemessener Weise für die Polizei nutzbar und handlungs- und rechtssicher formuliert ist. Der Gesetzentwurf zur Bestandsdatenauskunft dient der Umsetzung der Vorgaben des Bundesverfassungsgerichts und er dient der Anpassung der Vorschriften des Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, das sich bezüglich der Bestandsdatenbefugnis des BKAG noch auf die in Teilen verfassungswidrig erklärten Normen bezog, was nun mit einer neuen Formulierung angepasst werden wird. Grundsätzlich war die bisherige, das heißt noch geltende Normausgestaltung der Regelung zur manuellen Bestandsdatenauskunft im BKA-Gesetz, relativ allgemein formuliert. Und sie muss nun entsprechend der Vorgaben konkretisiert werden. Und dabei muss eben sichergestellt werden, dass mit den neuen Regelungen weiterhin die Fallkonstellationen erfasst werden, in denen das BKA im Rahmen seiner gesetzlichen Aufgaben auf die Erhebung von Bestandsdaten angewiesen ist. Es ist den Vorgaben des Bundesverfassungsgerichts geschuldet, dass für die Zulässigkeit von manuellen Bestandsdatenabfragen im BKA künftig entweder ein Anfangsverdacht für die Aufgabe der Unterstützung der Polizeien des Bundes und der Länder bei der Strafverfolgung oder – je nach zu schützendem Rechtsgut – ein

entsprechender Gefahrengrad für die Gefahrenabwehr beziehungsweise Verhütung von Straftaten vorliegen muss. Diese Vorgaben gilt es einzuhalten. Und sie dürfen auch nicht unterschritten werden.

Der Gesetzentwurf umfasst im Kern damit die eingangs dargestellten Fallkonstellationen. Es bleibt dem BKA als Zentralstelle damit auch künftig möglich, bei Vorliegen eines erkennbaren Anfangsverdachts beziehungsweise im Bereich der Verhütung von Straftaten zur Feststellung der zuständigen Strafverfolgungs- oder Gefahrenabwehrbehörde sowie im Rahmen der polizeilichen Rechtshilfe, manuelle Bestandsdatenabfragen durchzuführen. Beides sind ganz wesentliche Aufgaben des BKA als Zentralstelle, die bereits jetzt zum Beispiel im Rahmen des sogenannten NCMEC-Prozesses (National Centre for Missing and Exploited Children) – Kinderpornografie – und des internationalen polizeilichen Dienstverkehrs wie auch in Zukunft beispielsweise durch die zentrale Meldestelle für strafbare Inhalte im Internet wahrgenommen werden. Ebenso bleiben manuelle Bestandsdatenabfragen für das BKA auch für die Abwehr von Gefahren des internationalen Terrorismus sowie für den Personen- und Zeugenschutz erhalten. Der Gesetzentwurf setzt dabei die Vorgaben des Bundesverfassungsgerichts um, wobei die Möglichkeit auch im Vorfeld einer konkreten Gefahr, Bestandsdaten erheben zu können, für das BKA von hoher Bedeutung ist, je nach Schwere der möglichen Rechtsgüterbeeinträchtigung. Dem so vorgelagerten Gefahrengrad wird dabei durch die hohe Bedeutung der zu schützenden Rechtsgüter im Gesetz ausreichend Rechnung getragen.

Im Ergebnis ist festzuhalten, dass der vom Bundesverfassungsgericht vorgegebene Rahmen für manuelle Bestandsdatenabfragen durch das BKA im vorliegenden Gesetzentwurf deutlich erkennbar und für die praktische Anwendung auch handlungs- und rechtssicher formuliert ist. Die bislang dem BKA zur Verfügung stehenden Möglichkeiten manueller Bestandsdatenauskünfte können daher im Kern auch mit der künftigen Neuregelung wahrgenommen werden. Und zudem wird durch die bereits zum Teil im Gesetzentwurf Hasskriminalität vorgesehene explizite Aufnahme der Telemediendienste in die Regelungen zur manuellen Bestandsdatenauskunft im BKA-Gesetz nunmehr eine eindeutige Rechtsgrundlage für die Aufgaben des BKA geschaffen, mit der die Telemediendienste auch zur Auskunft von Bestandsdaten verpflichtet werden. Das ist aus Sicht des BKA zu begrüßen. Es muss aber auch beachtet werden, dass im jeweils konkreten Fall ein Ersuchen an die Betreiber auf Bestandsdatenauskunft nur dann einen Mehrwert für die polizeiliche Arbeit darstellt, wenn der Anbieter auch die Kundendaten gespeichert hat, um hieraus auch Auskunft erteilen zu können. Das gilt insbesondere für dynamische IP-Adressen. So erhielt das BKA allein im letzten Jahr rund 29.000 strafrechtlich relevante Meldungen des US-amerikanischen National Center for Missing and Exploited Children und in 2.594 Fällen war dabei die IP-Adresse der einzige Ermittlungsansatz. Eine manuelle Bestandsdatenabfrage anhand dieser IP-Adresse war aber nicht möglich, weil die Regelungen zur Vorratsdatenspeicherung aktuell nicht umgesetzt werden. Die Meldungen konnten also in diesen Fällen strafrechtlich nicht weiter verfolgt werden. Und das heißt ganz konkret: Der Missbrauch und das Leid hinter diesen Meldungen konnte nicht bekämpft, nicht beendet werden. Unabhängig davon ist mit diesem Gesetzentwurf jetzt ein guter Schritt gegangen worden oder wird gegangen in Richtung Rechts- und Handlungssicherheit. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Münch, vielen Dank. In der Zwischenzeit ist die Stellungnahme von Herrn Breyer um 10:17 Uhr eingegangen und wurde in der Zwischenzeit auch verteilt. Den Schluss in der ersten Runde der Einführung macht jetzt Herr Professor Schwarz.

SV **Prof. Dr. Kyrill-Alexander Schwarz** (Julius-Maximilians-Universität Würzburg): Frau Vorsitzende, meine sehr geehrten Damen und Herren Abgeordnete, ganz herzlichen Dank auch von meiner Seite zunächst für die Gelegenheit, hier zu diesem Gesetzentwurf Stellung nehmen zu können. Ich will in Ansehung der vielen Feststellungen, die bereits getroffen worden sind, mich auf einige ganz wenige Bereiche hier auch noch einmal beschränken, um da auch noch entsprechend mehr Zeit für eventuelle Fragen hier zur Verfügung stellen zu können. Ich glaube, es ist zunächst einmal völlig zutreffend, vorhin ist auch auf die ganze Reihe an Entscheidungen des Bundesverfassungsgerichts hingewiesen worden, die das Thema Begrenzung des Gesetzgebers im Bereich des Aus-

tarierens von Freiheit und Sicherheit auch darstellen. Ich will hier nur noch einmal kurz die Stichworte nennen, die eben mit der Entscheidung zur Online-Durchsuchung anfangen. Wir haben dann in den letzten knapp 15 Jahren die Entscheidung zum BKA-Gesetz, zur Auslandsauslandsaufklärung und jetzt auch – und das ist vielleicht ein Schlussstein, der aber auch gleichzeitig deutlich machen soll, dass man diese Entscheidungen nicht alle über einen Kamm scheren kann – die Bestandsdaten-II-Entscheidung. Es ist völlig offensichtlich, wenn man sich diese Reihe von Entscheidungen anschaut, dass wir es mit durchaus unterschiedlich intensiven Eingriffsinstrumentarien zu tun haben. Und das Bundesverfassungsgericht hat in der Bestandsdaten-II-Auskunft auch sehr deutlich gemacht, dass wir uns jetzt, wenn ich es einmal so formulieren möchte, am unteren Ende der Eingriffsbefugnisse bewegen können. Das wirkt sich aber auch aus für die Problematik der Rechtfertigung entsprechender Grundrechtseingriffe, bei der wir nämlich von sehr viel geringeren Anforderungen ausgehen können.

Meines Erachtens genügt der Gesetzentwurf in den wesentlichen Zügen genau den Anforderungen, die das Bundesverfassungsgericht in der Bestandsdaten-II-Auskunftsentscheidung auch aufgestellt hat. Dabei ist vor allem zu berücksichtigen, dass das Korsett, das das Bundesverfassungsgericht in der Zwischenzeit dem Gesetzgeber angelegt hat, so engmaschig ist, dass meines Erachtens völlig zurecht auch im juristischen fachwissenschaftlichen Schrifttum von einer Art juristischen Overkills in der Form des Verhältnismäßigkeitsgrundsatzes gesprochen werden kann. Man kann es auch anders formulieren: Der Gesetzgeber befindet sich mittlerweile in der Situation, dass er eigentlich in einer Art Komplexitätsfalle sitzt. Er nimmt auf der einen Seite die Vorgaben des Bundesverfassungsgerichts auf, mit Blick auf drohende weitere Verfahren versucht er, sie kleinteilig umzusetzen. Und er befindet sich damit – und Herr Kollege Löffelmann hat das sehr schön auch in seiner Stellungnahme dargelegt – eigentlich in einer Situation, dass man sich grundlegend einmal Gedanken machen müsste über eine neue Architektur der Sicherheitsbefugnisse in Deutschland. Es geht nicht um eine Entgrenzung der Befugnisse, und dafür kann auch dieses Gesetz sicherlich nicht herangezogen werden, sondern es geht tatsächlich um eine verhältnismäßige Begrenzung von Eingriffen, die auf durchaus niederschwelligem Niveau anzusiedeln sind.

Ich möchte auf einen Punkt besonders hinweisen: Dieses Gesetz ist in meinen Augen eben nicht nur ein reines Reparaturgesetz. Es beschränkt sich zwar im Wesentlichen darin, die Vorgaben des Bundesverfassungsgerichts aus der Bestandsdaten-II-Auskunftsentscheidung zu übernehmen. Aber in einem Aspekt geht der Gesetzgeber vielleicht auch ebenfalls in Anlehnung an die Vorgaben des ersten Senats aber doch einen Schritt weiter. Und das ist die Aufnahme der Kategorie der drohenden Gefahr. Man kann über diesen Begriff lange inhaltlich diskutieren, ob er überhaupt erforderlich ist, ob er nicht eine gewisse gesetzgeberische Redundanz vielleicht auch zum Ausdruck bringt in Ansehung der Tatsache, dass eine Gefahr als solches schon immer ein drohendes Element in sich hat. Aber ich will nur darauf hinweisen, dass dieser Begriff auch als Einfallstor verstanden werden kann für weitere verfassungsgerichtliche Verfahren. Man betritt als Gesetzgeber damit juristisches Neuland. Es gibt bisher keine weitergehenden verfassungsgerichtlichen Entscheidungen über den Begriff der drohenden Gefahr. Dieser Begriff ist in der Rechtsprechung des Bundesverfassungsgerichts in der BKA-Gesetz-Entscheidung erstmals verwendet worden, aber – und das ist in meinen Augen der entscheidende Punkt – wenn man dem Gesetzgeber vorhalten möchte, er agiert nur noch als nachgeordnete Stelle des Bundesverfassungsgerichts, dann hat er hier mit diesem Begriff ebenfalls etwas aus der Judikatur des Gerichts aufgegriffen. Aber in Ansehung all der offenen Fragen, die mit diesem Begriff verbunden sind, stellt sich in der Tat die Frage, ob man dieses sicherlich gegebene verfassungsrechtliche Risiko weiterer Verfahren hier auch tatsächlich eingehen sollte. Das ist zunächst einmal von meiner Seite aus der wesentliche Punkt, bei dem ich tatsächlich zumindest eine Gefahr innerhalb des Gesetzes sehe.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Professor Schwarz, vielen herzlichen Dank. Dann kommen wir jetzt erst mal zur Fragerunde. Wir beginnen mit der Unionsfraktion und es meldet sich hierzu Herr Müller. Bitte schön.

Abg. **Axel Müller** (CDU/CSU): Vielen Dank, Frau Vorsitzende. Vielen Dank an die Sachverständigen für die Vorträge. Ich hätte zwei Fragen an Herrn Professor Dr. Schwarz. Die kritische Einstellung

zum Begriff der drohenden Gefahr ist sehr deutlich geworden, aber ich möchte noch mal ganz am Anfang ansetzen und einfach fragen: Sie haben es zusammengefasst gesagt. Erfüllt denn nun das, was wir als Reparaturgesetz hier vorliegen haben, die Voraussetzungen, die das Bundesverfassungsgericht an uns gestellt hat, insbesondere wenn es um die Differenzierung zwischen den Bestandsdaten und den Nutzungsdaten sowie den Inhaltsdaten geht, insbesondere, wenn es darum geht, dass man Abstufungen vornehmen muss, was den Eingriff in die jeweiligen Rechtsgüter anbelangt und dass das Ganze auch dem Verhältnismäßigkeitsgrundsatz entsprechen muss? Da würde mich interessieren, ob Sie – zusammengefasst haben Sie es ja gesagt, aber noch mal konkreter jetzt, was diese einzelnen Begriffe anbelangt – zur Überzeugung gelangt sind, dass das Gesetz dem gerecht wird. Und die zweite Frage, weil das auch in den Vorträgen anklang – der Unterschied zwischen den Telekommunikationsdaten und den Telemediendaten – die Frage an Sie: Wird dieser Gesetzesentwurf auch diesem Unterschied, was Eingriffsvoraussetzungen und die Eingriffstiefe und die entsprechend vorzunehmenden Abstufungen anbelangt, gerecht? Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Müller, vielen Dank. Herr Dr. Wirth.

BE Abg. **Dr. Christian Wirth** (AfD): Auch meinen Dank an die Sachverständigen. Meine erste Frage an Professor Löffelmann: Die Bundesrechtsanwaltskammer bemängelt Dokumentationspflichten und stellt fest, dass eine interne Dokumentationspflicht lediglich beim Bundespolizeigesetz und Zollfahndungsgesetz vorgesehen ist und dahingehend, dass Datenschutzbeauftragte und die Verwaltungsgerichte zuständig sein sollen. Hier wird gefordert, dass eine eigenständige Überprüfung und Anforderung der Vorgänge natürlich eher selten sein wird durch die Datenschutzbeauftragten und die Gesetzesvorlagen um eine unverzügliche Informationspflicht ergänzt werden sollen. Wie stehen Sie hierzu? Und eine Frage an Herrn Kollegen Breyer: Herausgabe von Passwörtern. Wie steht das in Verhältnismäßigkeit, wenn man wohl davon ausgehen muss, dass Passwörter ja wohl in klarem Wortlaut gespeichert werden müssen? Steht das in irgendwelcher Verhältnismäßigkeit und ist nicht die Gefahr zu groß, dass Dritte, namentlich Hacker und andere Kriminelle, hier Zugriff nehmen können? Vielen Dank.

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

BE Abg. **Uli Grötsch** (SPD): Vielen Dank, Frau Vorsitzende. Meine erste Frage richtet sich an Herrn Professor Dr. Löffelmann und an Herrn Präsident Münch. Und ich habe eine Frage zum Thema Dokumentationspflichten. Nun haben wir den Umstand, dass in § 112 TKG im automatisierten Verfahren jährlich ungefähr 16 Millionen Abfragen getätigt werden, das sind 100.000 pro Tag, und wir dort eine Dokumentation haben. Was die manuelle Abfrage angeht, ist das viel, viel weniger. Das sind drei- bis fünfstellige Zahlen im ganzen Jahr. Und trotzdem können Sie hier auf keine Dokumentation zurückgreifen. Herr Münch, Sie sind eben schon mal darauf eingegangen, aber ich wollte trotzdem bei Ihnen beiden nachfragen: Inwiefern halten Sie eine statistische Erfassung der Abfrage der Bestandsdaten im manuellen Verfahren über die vorgesehenen Dokumentationspflichten hinaus für erforderlich?

Meine zweite Frage richtet sich an Herrn Professor Dr. Löffelmann und es geht um das Thema der Entschlüsselung übermittelter Passwörter: Sie haben in Ihrer Stellungnahme auch Bedenken geäußert, was die Sicherheitsbehörden mit in der Regel verschlüsselten Passwörtern anstellen sollen. Ich habe das mal beim BMI nachgefragt. Die Antwort von dort war, dass die jeweilig abrufenden Behörden das gegebenenfalls entschlüsseln sollen. Das sei technisch nicht ausgeschlossen. Andere sagen wieder, das sei technisch doch ausgeschlossen. Und ich frage Sie, Herr Professor Dr. Löffelmann: Gibt es angesichts dieser uneindeutigen Situation verfassungsrechtliche Bedenken Ihrerseits, etwa hinsichtlich der Geeignetheit?

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank, Herr Grötsch. Dann für die FDP Herr Höferlin.

BE Abg. **Manuel Höferlin** (FDP): Danke, Frau Vorsitzende. Vielen Dank auch von mir an die Sachverständigen für die sehr interessanten Ausführungen. Ich finde es schon beachtenswert, dass gleich zwei Sachverständige, die von den Koalitionsfraktionen benannt sind, thematisieren, wie komplex kleinteilig doch die Sicherheitsgesetzgebung inzwischen geworden ist. Ich kann da nur empfehlen, mal über eine Überwachungsgesamt-

rechnung nachzudenken, damit man mal rausfindet, was eigentlich überhaupt auf dem Tisch liegt. Ich habe zwei Fragen an den Sachverständigen Herrn Professor Kelber. Einmal möchte ich auch auf den Themenpunkt Herausgabe von Passwörtern eingehen. Sie haben ja auch in Ihrer Stellungnahme, Herr Kelber, da intensiv darüber etwas gesagt und das auch kritisiert. Für mich wäre mal interessant, dass Sie noch mal darlegen, warum Sie ein Herausstreichen der Möglichkeit von der Passwortherausgabe für so essenziell halten. Das ist ja gerade eben auch in der Frage angeklungen, das ist ja eher die Ausnahme, dass sie unverschlüsselt vorliegen. Manche vermuten ja dann auch eine möglicherweise Verpflichtung von Providern, die unverschlüsselt irgendwie bereitzuhalten. Ich glaube, das ist mit dem Datenschutz nicht vereinbar, also sind wir da in einer Schere. Und vielleicht können Sie das noch mal erklären: Warum öffnet die bisherige Formulierung Ihrer Ansicht nach Tür und Tor für die Herausgabe von Passwörtern, sogar bei der Begehung von Ordnungswidrigkeiten?

Und die zweite Frage auch an Sie, Herr Kelber: Sie haben in Ihrem Statement ja auch gesagt, man kann dieses sogenannte Reparaturgesetz ja auch in einem größeren Kontext sehen. Ich sehe das auch so. Ich habe das auch im Plenum gesagt. Sie haben sich auch zweimal in den öffentlichen Stellungnahmen kritisch zum Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität geäußert und Sie kritisieren ja auch die neue Ausleitungsverpflichtung von Inhalten, die bald die Social Media-Anbieter treffen soll. Ist für Sie das Gesetz gegen Rechtsextremismus und Hasskriminalität repariert, wenn nun die Regelungen der Bestandsdatenauskunft abgeändert werden oder fehlen Ihnen Regelungen, damit Sie dem Gesetz gegen Rechtsextremismus und Hasskriminalität zustimmen könnten? Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank, Herr Höferlin. Dann für die Fraktion DIE LINKE. Herr Movassat, bitte.

Abg. **Niema Movassat** (DIE LINKE.): Ja, danke schön. Ich habe zwei Fragen an Herrn Breyer, will aber auch vorweg sagen: Also, dass man glaube ich den Ausführungen nicht allen im Detail folgen konnte, ist ja nicht Herrn Breyers Schuld, sondern ist natürlich das Problem, dass bei diesem Gesetzentwurf eben auch viele Kritikpunkte bestehen und verfassungsrechtliche Kritikpunkte bestehen. Aber zu den Fragen. Herr Breyer, sowohl in der Entscheidung des Bundesverfassungsgerichts zur Bestandsdatenauskunft als auch in der Literatur wird ja deutlich, dass Nutzungsdaten von Telemedien nicht einfach den Bestandsdaten im Bereich der Telekommunikation entsprechen, sondern Informationen über die Personen enthalten, die weit über das hinausgehen, was in den Telekommunikationsdaten enthalten ist, es sich also um deutlich sensiblere Daten handelt. Können Sie hier noch mal vielleicht kurz erläutern, was eigentlich diese Nutzungsdaten enthalten können und warum man sie nicht einfach mit den Bestandsdaten gleichstellen kann? Und meine zweite Frage schließt sich daran an. Wie müssten die Auskünfte über Nutzungsdaten rechtlich behandelt werden, wenn man berücksichtigt, dass sie weit sensibler sind als bloße Bestandsdaten? Danke schön.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Movassat, vielen Dank. Und den Schluss in dieser Runde macht Herr von Notz.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Frau Vorsitzende. Auch ich danke ganz herzlich allen Sachverständigen für den Sachverstand und die Vorträge. Zwei Fragen haben wir. Die erste geht an Herrn Münch, die zweite an Herrn Bäcker. Herr Präsident, mich würde von Ihrer Seite, die Sie jetzt im Weisungsstrang des BMI stehen, interessieren, mit was für konkreten Zahlen rechnen Sie? Wie viel an Daten, die kommen? Wie viele Leute haben Sie bereitgestellt? Wie werden die Daten gespeichert? Wie werden sie verarbeitet? In was für Programmen soll das erfolgen? Erfolgt das automatisiert oder wird jedes einzelne Datum, das kommt, ich sag mal händisch von einem Beamten angeguckt und bewertet, rechtlich eingeordnet? Gibt es da einen Vermerk? Wie läuft das konkret? Denn das ist ja sozusagen die Perspektive glaube ich, die nachher auch sehr relevant ist für die rechtliche Beurteilung, was hier passiert.

Meine zweite Frage geht an Herrn Professor Bäcker. Vielleicht auch gerade noch mal im Hinblick darauf, was Herr Löffelmann ausgeführt hat, was ich auch sehr interessant fand. Inwieweit genügen sozusagen die Regelungen jetzt auch dem Bestimmtheitsgrundsatz? Also hat dieses Gesetz vielleicht auch mit der europäischen Dimension,

die hier nicht voll mit erfasst wird offensichtlich, nicht eine Komplexität erreicht, die diese Frage der ausreichenden Bestimmtheit in Frage stellt? Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Ich würde noch gerade zwei Fragen anschließen. Eine Frage an Herrn Münch, und zwar auch im Hinblick auf die Stellungnahme von Herrn Professor Löffelmann. Herr Münch, für die Praktiker sag ich jetzt mal: Zu unübersichtlich, zu wenig einfach zu handhaben, zu kompliziert. Das ist mal ein ernst zu nehmender Hinweis. Mich würde mal interessieren, was die Praxis dazu sagt. Gesetze sollten normalerweise einfach, verständlich und klar sein. Eine zweite Frage hätte ich noch an Herrn Professor Schwarz im Hinblick auf die drohende Gefahr, die Sie ja auch kritisiert haben, die Verwendung des Begriffes. Was würden Sie uns denn jetzt an der Stelle empfehlen, wie man es vielleicht noch ändern könnte, um dieses Risiko abzuwenden, dass es eben nicht konkret genug ist und damit wieder aufgehoben werden könnte vom Gericht?

Dann würde ich jetzt die Antwortrunde einleiten. Und wir beginnen alphabetisch wieder von vorne und damit mit Herrn Professor Bäcker.

SV **Prof. Dr. Matthias Bäcker** (Johannes Gutenberg-Universität Mainz): Herzlichen Dank. An mich ist die Frage gerichtet worden von Herrn von Notz, wie es mit der Bestimmtheit des Gesetzes aussieht, auch im Lichte der Anmerkungen von Herrn Löffelmann. Also, die kurze Antwort ist: Ich vertrete die gegenteilige Position. Ich will das kurz begründen. Das Bundesverfassungsgericht hat in seiner Rechtsprechung zum Sicherheitsrecht zweifellos, das kann man gut finden, das kann man schlecht finden, aber es ist mit Sicherheit so, immer kleinteiligere Vorgaben an den Gesetzgeber errichtet. Es sind immer mehr Punkte angesprochen worden, zu denen Regelungen gefordert wurden und es ist auch hinsichtlich der Regelungen ein immer größerer Detailgrad verlangt worden. Wenn Sie die Anforderungen, die das Bundesverfassungsgericht aufgestellt hat, in tragfähiger Weise umsetzen wollen, kommen Sie um lange Vorschriften nicht herum. Ich weiß nicht, wie das anders gehen soll. Der Vorschlag, alles einfacher zu machen, alles verständlicher zu machen, klingt gut, führt aber in der Tat zu hoher Unbestimmtheit, weil Sie dann letztlich mit sehr abstrakten Begriffen arbeiten müssen, die das Gesagte und das Gemeinte nicht unbedingt ausdrücken.

Tatsächlich bin ich der Meinung, dass wir in puncto Bestimmtheit eigentlich große Fortschritte machen. Und auch, dass dieses Gesetz sehr viel klarer ist als das, was wir früher im Sicherheitsrecht hatten. In der ersten Phase der Ausarbeitung des grundrechtlichen Datenschutzes im Polizei- und Sicherheitsrecht sind in die Polizeigesetze, später dann auch in die Nachrichtendienstgesetze, lauter Generalklauseln aufgenommen worden. Irgendwas ist zulässig, wenn es erforderlich ist, um die Aufgaben des Dienstes oder der Polizei zu erfüllen. Das sagt überhaupt nichts aus. Kein Mensch weiß, was das bedeutet. Gerade vor etwas mehr als einem Jahr in der mündlichen Verhandlung des Bundesverfassungsgerichts zur Ausland-Ausland-Fernmeldeaufklärung hat genau so eine Regelung noch einmal auf dem Tisch gelegen. Und der Bundesnachrichtendienst ist gefragt worden: Was bedeutet das denn eigentlich, erforderlich, damit Ihr eure Aufgaben erfüllen könnt? Und da kam nichts als Antwort. Das wussten die nicht. Und Sie können, wenn Sie das Urteil nachlesen, die erkennbare Verstimmung des Senats über den Umstand finden, dass der BND ihnen das nicht erklären konnte. Das ist aber auch verständlich, dass da nichts kam, weil das so schwammig und unklar ist.

Wenn Sie grundrechtliche Anforderungen schon im Gesetz abbilden wollen und wenn schon das Gesetz sicherstellen soll, dass der Verhältnismäßigkeitsgrundsatz gewahrt wird, und das ist die Stoßrichtung der ganzen Rechtsprechung des Bundesverfassungsgerichts: Es soll eben nicht der behördlichen Tätigkeit überlassen werden, ein unklares Gesetz oder ein offen formuliertes Gesetz zu konkretisieren und auf diesem Wege den Verhältnismäßigkeitsgrundsatz zu wahren. Das ist der Weg des klassischen Polizeirechts, der polizeilichen Generalklausel. Die Polizei darf das Erforderliche tun, wenn eine Gefahr vorliegt. Das soll gerade nicht geschehen, sondern das Gesetz selber soll die Tätigkeit viel stärker und viel enger anleiten als wir das aus dem klassischen Polizeirecht gewohnt sind. Wenn man das will, muss man detailliert regeln. Ich habe auch mit der Bestimmtheit der Regelungen offen gestanden überhaupt kein Problem. Die sagen eigentlich alle relativ klar, was sie meinen. Selbst der Begriff der drohenden Gefahr, den man für sich genommen sicherlich schwierig finden

kann, wird ja dann weiter spezifiziert durch Konditionalsätze. Und das entspricht der Rechtsprechung. Man kann sich fragen: Hätte das der Gesetzgeber in anderer Weise konkretisieren können? Wäre es dann vielleicht plausibler gewesen? Kann schon sein. Aber zu unbestimmt scheint mir dies nicht zu sein. Das scheint mir nicht das Problem des Gesetzes zu sein. Das Problem ist, dass die für sich genommen bestimmten Regelungen nicht in jeder Hinsicht tatsächlich dem Verhältnismäßigkeitsgrundsatz genügen. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Professor Bäcker, vielen Dank. Herr Breyer.

SV **Jonas Breyer** (Rechtsanwalt, Wiesbaden): Vielen Dank. Es sind jetzt drei Fragen an mich gerichtet worden. Soll ich jetzt eine Viertelstunde durchreden oder alle drei in fünf Minuten oder wie haben Sie das vorgesehen?

Vors. **Andrea Lindholz** (CDU/CSU): Ich sage immer, das Beste ist, so zügig wie möglich die Dinge auf den Punkt zu bringen, ohne dass ich Sie jetzt festnagele. Versuchen Sie halt einfach, es so präzise und zügig wie möglich zu machen. Das gilt für alle, nicht nur für einen.

SV **Jonas Breyer** (Rechtsanwalt, Wiesbaden): Okay, gut. Die erste Frage, wenn ich sie richtig verstanden habe, war sinngemäß: Ist das Gesetz nicht unverhältnismäßig, weil auf unverschlüsselte Passwörter auch Hacker zugreifen können und der Gesetzentwurf deren Abruf ermöglicht? Also, ich hoffe, ich habe die Frage richtig verstanden.

Vors. **Andrea Lindholz** (CDU/CSU): Ja, Herr Dr. Wirth nickt, dass die Frage richtig verstanden ist.

SV **Jonas Breyer** (Rechtsanwalt, Wiesbaden): Okay, dann vielen Dank. Der Gesetzentwurf, soweit ich ihn in der Kürze der Zeit lesen konnte jedenfalls, verpflichtet aus meiner Sicht die Anbieter nicht, PINs oder Passwörter unverschlüsselt zu speichern. Im Gegenteil dürfte das meines Erachtens sogar europarechtswidrig sein, wenn der deutsche Gesetzgeber das versuchen würde. Ich habe ja in meinem Eingangsstatement schon auf Artikel 32 der DSGVO (Datenschutz-Grundverordnung) hingewiesen. Der regelt Vorgaben zur Datensicherheit. Auch der Bundesdatenschutzbeauftragte hat darauf in seiner schriftlichen Stellungnahme schon zu Recht hingewiesen. Das heißt, der Gesetzentwurf fordert nicht, dass die unverschlüsselt gespeichert werden, sondern er läuft einfach leer, weil sie sehr häufig verschlüsselt gespeichert werden. Es ist bei bestimmten weit verbreiteten Standards oder wenn die Passwörter unsicher sind, wie zum Beispiel bei Handy-PINs. Das ist natürlich sehr schwierig, solche internationalen Standards von heute auf morgen zu ändern oder die Länge der Mobilfunk-PIN zu erhöhen. Deswegen ist das in der nächsten Zeit nicht zu erwarten in der Praxis, aber ja, soweit Daten unverschlüsselt gespeichert würden, wäre es natürlich ein hohes Risiko und dürfte wahrscheinlich auch verfassungswidrig sein, wenn es dazu käme. Und würde das vorgeschrieben, dann wäre das europarechtswidrig und auch unverhältnismäßig. In dem Zusammenhang wurde auch noch eine Stellungnahme des BSI angesprochen. Ist eine Entschlüsselung möglich? Das muss man differenziert betrachten, und zwar, normalerweise werden sogenannte mathematische Hashfunktionen benutzt, also das muss man auch technisch nicht genau verstehen, aber man kann vielleicht zusammenfassend sagen, so lange die Passwörter oder PINs nicht trivial sind, also zum Beispiel nur eine vierstellige Zahl, sodass man dann alle denkbaren PINs oder Passwörter schnell durchprobieren kann, wie die verschlüsselte Version dann lauten müsste, sodass man die dann abgleichen kann, also den sogenannten Hashwert. Normalerweise, wenn die nicht trivial sind, ist eine solche Entschlüsselung nicht möglich. Das ist auf jeden Fall der Anspruch dieser mathematischen Algorithmen. Wenn die Passwörter trivial sind, dann kann es möglich sein.

Ich fahre fort mit der nächsten Frage. Wenn Sie das aufgesplittet haben wollen, können Sie sich ja melden. Die nächste Frage war von Herrn Movassat, wenn ich das richtig verstanden habe, sinngemäß: Was hat es mit den Nutzungsdaten im Bereich der Telemedien auf sich und warum darf keine Gleichbehandlung mit Bestandsdaten erfolgen, wie sie der Gesetzentwurf ja nicht zu hundert Prozent, aber doch teilweise tatsächlich vorsieht? Ja, wie bereits angesprochen sieht der Entwurf in der Neufassung des Telemediengesetzes den Abruf von Bestands- und von Nutzungsdaten vor. Bei den Bestandsdaten handelt es sich beispielsweise etwa darum, welche Pseudonyme hat ein Benutzer in einem Internetforum benutzt, unter denen er dort Beiträge geschrieben hat. Es können darüber weitreichende Schlüsse gezogen werden, etwa wenn es sich um die Inanspruchnahme irgendeines Selbsthilfeforums handelt. Und

diese Foren erheben auch manchmal, also sei es auch freiwillig, sensible Daten wie den Beziehungsstatus, irgendwelche sexuellen Vorlieben oder auch die Religion. Und der Entwurf sieht da auch keine Ausnahme vor für beispielsweise Presseinformanten, Berufsgeheimnisträger oder auch die Seelsorge. Die Abfragen sind nicht auf den Einzelfall beschränkt. Es wäre also möglich, eine Liste aller Nutzer auch abzufragen und das stellt einen besonders schwerwiegenden Grundrechtseingriff dar. Und wenn man all diese Informationsaustausche offline macht außerhalb von Internetforen oder ähnlichen Telemediendiensten, dann wäre eine Aufzeichnung nicht möglich, das heißt, da werden substanzielle neue Befugnisse geschaffen.

Was jetzt speziell die Nutzungsdaten angeht, um das vielleicht noch mal ein bisschen zu veranschaulichen. Welche Daten fallen denn in der Praxis darunter? Da fällt beispielsweise darunter: Welche Internetseiten hat der Nutzer aufgerufen, welche Onlinevideos hat er gesehen oder auch selbst hochgeladen auf YouTube oder anderen Plattformen? Welche Artikel in welchen politischen Onlinezeitungen hat er aufgerufen? Oder welche Beiträge hat er in einem Aidshilfe-Forum oder auch in einem Gewerkschaftsforum geschrieben? Und diese Beispiele zeigen meines Erachtens, dass durch die Abfrage von Nutzungsdaten sehr viel tiefere Einblicke in unsere Persönlichkeit, in unser Privatleben, in unsere Interessen und Vorlieben möglich sind als das bisher der Fall war oder auch bei der Lektüre bisheriger Zeitungen. Und dieser Sensibilität der Nutzungsdaten hat der Gesetzgeber ursprünglich auch Rechnung getragen, indem er in den §§ 13 und 15 des Telemediengesetzes festgelegt hat, dass Informationen, die nicht abrechnungsrelevant sind, über die Nutzung der Telemedien eigentlich direkt nach der Beendigung des Zugriffs zu löschen sind. Und zum Teil kommt es aber nicht zu dieser Löschung, weil die Daten sich dann doch als abrechnungsrelevant erweisen oder die Löschungen aus verschiedenen Gründen wie technische Gründe oder Bequemlichkeit nicht durchgeführt werden oder zum Teil von den Aufsichtsbehörden auch etwas halbherzig durchgesetzt werden. Und so sind diese Informationen da und müssen entsprechend geschützt werden. Wir müssen uns vor Augen halten, dass Telemedien unsere bisherigen klassischen Medien immer weiter ersetzen und auch in vielen Bereichen die Telemedien unverzichtbar geworden sind. Ich erinnere beispielsweise an die Online-Steuererklärung für Gewerbetreibende, die ja schon heute vorgeschrieben ist. Die Dienste sind Voraussetzung für die Ausübung von grundrechtlich geschützten Freiheiten, insbesondere des Rechts, seine Meinung in Wort und Schrift und Bild zu äußern und zu verbreiten. Ich weise auf Artikel 5 des Grundgesetzes hin. Und es ist ein grundlegendes Bedürfnis, dass man sich ungehindert und unbefangen informieren kann. Und nur dann kann der Einzelne in der Gemeinschaft auch mit einem freien Informationszugang informierte politische Entscheidungen treffen und am freiheitlichen demokratischen Gemeinwesen mitwirken. Auch für Nutzungsdaten ist mir aufgefallen, dass die Abrufe nicht auf Einzelvorgänge beschränkt sind und deswegen wird der Entwurf der Sensibilität der abzurufenden Telemediennutzungsdaten nach meiner festen Überzeugung nicht gerecht und wird vor dem Bundesverfassungsgericht scheitern.

Wenn Sie erlauben, komme ich jetzt zur dritten und letzten Frage an mich. Die lautete, wenn ich das richtig verstanden habe, sinngemäß: Wie müssten die Daten richtigerweise behandelt werden, also wohl die Telemediennutzungsdaten? Ja, wenn man die Sensibilität sich anschaut, sind sie eigentlich mit Telekommunikationsinhalten zu vergleichen. Auch der Sachverständige Professor Bäcker hatte das zumindest schon mal fragend erwähnt. Also so wie eine Telekommunikationsüberwachung. Und dementsprechend sind sie auch vom Gesetzgeber so zu behandeln. Was bedeutet das konkret? Das bedeutet, dass im Bereich der Strafverfolgung die Anforderungen der §§ 100a und 100b der Strafprozessordnung einzuhalten sind, also beispielsweise, dass eine gerichtliche Anordnung gefordert wird und dass auch eine Begrenzung stattfindet auf einen festgelegten Katalog von schweren Straftaten, bei denen das nur zulässig ist. Im Bereich der Gefahrenabwehr kann ich das in der Kürze der Zeit nicht ohne Weiteres beantworten, weil die Anforderungen dort sehr komplex sind. Es gibt aber eine Entscheidung aus dem Jahr 2005 – glaube ich – des Bundesverfassungsgerichts, unter welchen Voraussetzungen denn eine präventive Telekommunikationsüberwachung zulässig ist. Insbesondere wurde da formuliert, dass es nur bei Vorliegen einer konkreten Gefahr erforderlich ist, weil es eben einen erheblichen Grundrechtsreingriff bedeutet. Das kann dann also im Einzelnen nachgelesen werden in der

Entscheidung des Bundesverfassungsgerichts. Da ging es um das Sicherheits- und Ordnungsgesetz des Landes Niedersachsen. Dort wurde das schon mal versucht. Im Bereich der Nachrichtendienste wäre nach meiner Überzeugung eine Orientierung am Verfahren des G 10-Gesetzes nötig, so wie es ja heute auch schon dort enthalten ist, wobei ich allerdings zugegebenermaßen eine Erforderlichkeit nicht erkennen kann, warum die Nachrichtendienste Nutzungsdaten für ihre Aufgaben benötigen würden. Das ist auch vom Vertreter des BKA vorhin eigentlich nicht vorgetragen worden. Damit bin ich am Ende. Vielen Dank.

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

SV **Prof. Ulrich Kelber** (BfDI, Bonn): Vielen Dank, Frau Vorsitzende. An mich sind zwei Fragen gegangen. Die erste war zur Herausgabe der Passwörter. Ich sehe hier eine Inkonsistenz unterschiedlicher gesetzlicher Anforderungen. Insbesondere steht natürlich auch die Fragestellung im Raum: Sollte es tatsächlich möglich sein, über eine Verschlüsselung, eine Verhashung, Passwörter zu schützen, ist die Regelung dann überhaupt geeignet? Weil natürlich gerade diejenigen, die man bekommen will im Sicherheitsbereich, von solchen Maßnahmen dann auch Gebrauch machen würden. Ist aber daran gedacht, über indirekte Methoden so viel Kenntnis zu bekommen zur Entschlüsselung oder auch wieder zur Re-Identifikation von einem Hashwert, indem man zum Beispiel über den Zwang der Herausgabe sonstiger Daten des Unternehmens Kenntnisse über den Hashprozess oder über die Zwei-Faktor-Authentifizierung an anderen Stellen gelangt, dann ist es wiederum eine Sicherheitsfrage. Da komme ich zur Inkonsistenz zurück. Sie haben als Gesetzgeber an verschiedenen Stellen Vorgaben gemacht für die Sicherheit solcher Verfahren. Das ist einmal der Artikel 32 der Datenschutz-Grundverordnung, aber auch Vorgaben zum Beispiel in der Zahlungsdiensterichtlinie, wo sichergestellt sein muss, dass klar ist, wer welchen Vorgang angenommen hat. Oder ein großes Vorhaben, das immer wieder angesprochen wird, eine E-Identität auf Smartphones, ohne die Pflicht, es immer wieder mit der physikalischen Karte zu synchronisieren. Alles das wäre bei einer Gefährdung von Passwortvorgängen natürlich an der Stelle in der Form nicht mehr durchhaltbar.

Zweite Fragestellung: Ist der Gesetzentwurf gegen Rechtsextremismus und Hasskriminalität dadurch vollständig repariert? Nein, die grundsätzliche Kritik bleibt. Und ich will das noch mal an drei Beispielen zeigen. Wenn man wirklich sämtliche Quellen von Daten in dem Zusammenhang offenlegt, ist völlig offen, wie bestimmte Grundsätze eingehalten werden sollen. Ich nenne nur das Beispiel der Zweckbindung, wenn ich erst mal eine riesige Menge von Daten an der Stelle bekomme. Ich glaube, es ist nicht zutreffend, dass man die Eingriffsschwellen und andere Fragepunkte bei Bestandsdaten einfach übertragen kann auf Nutzungsdaten, die eine völlig andere Dimension in der Qualität haben. Und ein weiteres Beispiel. Wir haben ja schon vom Doppeltür-Modell gesprochen. Die §§ 15a und 15b sehen vor, dass ein Gericht eine solche Abfrage anordnen muss, aber mit § 100 Strafprozessordnung soll jetzt eine Eilkompetenz eingeführt werden, die trotz unseres Hinweises auch nicht aus dem Entwurf herausgenommen wurde. Das widerspricht der Idee des Doppeltür-Modells. Der Gesetzgeber der einen Tür kann nicht die andere Tür einfach weiter aufstoßen.

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

SV **Prof. Dr. Markus Löffelmann** (HS Bund, Berlin): Vielen Dank. Herr Dr. Wirth fragte nach den Dokumentationspflichten, die nur im Bundespolizeigesetz und ZFdG geregelt seien. Ich habe das gerade noch mal kurz überprüft. Also, es gibt auch entsprechende Regelungen im BNDG, im BKAG. Also ich glaube, das wurde schon insgesamt harmonisch ausgestaltet und man muss darauf hinweisen, dass diese Dokumentationspflicht nur im Zusammenhang mit der Verarbeitung von IP-Adressen zum Zwecke der Beauskunftung von Bestandsdaten vorgesehen ist. Ich vermute, dass hinter diesen Regelungen die Rechtsprechung des Bundesverfassungsgerichts zu den verfahrensrechtlichen Absicherungen, nämlich Dokumentationspflichten, Kennzeichnungspflichten und dergleichen bei Eingriffen in Artikel 10 Grundgesetz steht, und das Bundesverfassungsgericht ordnet ja diese automatisierte Verarbeitung der IP-Adressen zum Zwecke der Beauskunftung von Bestandsdaten auch dem Artikel 10 Grundgesetz zu. Ich finde das nicht furchtbar überzeugend, ist aber so. Und deshalb ist der Gesetzgeber sicher auf der richtigen

Seite, wenn er solche Regelungen absichernd vorsieht. Ich würde mal, ohne dass ich mir das genau überlegt habe, aus dem Bauch heraus sagen, das ist eine überobligationsgemäße Vorschrift, die hier geschaffen wurde, die eben dann dem nachträglichen Rechtsschutz dient. Nur, wenn wir wissen, was passiert ist, dann können wir auch die Gerichte dazu anrufen.

Die Frage hängt auch eng zusammen mit der ersten von Herrn Grötsch gestellten Frage. Herr Grötsch hat auf das automatisierte Bestandsdatenauskunftsverfahren hingewiesen. In dem Zusammenhang denke ich, dass auch eine gewisse Schieflage besteht. Es ist natürlich so, dass hier viel mehr Bestandsdaten verarbeitet und an die Behörden schlussendlich weitergegeben werden als im manuellen Verfahren. Ja, Herr Grötsch sprach von 16 Millionen. Das scheint der aktuelle Stand zu sein. Zwei Prozent davon sind Daten über das manuelle Auskunftsverfahren. Immer noch sehr viel! Also, das sind auch noch einige Hunderttausend. Also, man kann sich schon fragen, warum eigentlich das Bundesverfassungsgericht zwar das manuelle Verfahren beanstandet hat und dieses deshalb hier repariert wird, nicht aber das automatisierte Verfahren, das einen viel breiteren Anwendungsbereich hat und deshalb auch unter Verhältnismäßigkeitsgesichtspunkten schon die Eingriffsintensität dort auch nicht ganz unerheblich ist. Also, ein Gleichziehen dieser beiden Verfahren würde durchaus Sinn machen. Das muss aber nicht zwingend so ausgestaltet sein, dass man dann die Regelungen für das automatisierte Verfahren verschärft, sondern das kann auch andersrum erfolgen. Eine statistische Erfassung bei manuellen Verfahren, Herr Grötsch? Ja, statistische Erfassungen machen immer Sinn. Das ist die rechtstatsächliche Grundlage. Ich persönlich finde, dass der Gesetzgeber viel zu wenig über solche rechtstatsächlichen Grundlagen verfügt. Wir stoßen an diese Grenze immer wieder, dass man im Gesetzgebungsverfahren dann Behörden anspricht, anschreibt und um Fallbeispiele bittet und die Behörden sind aber nur bedingt auskunftsfähig. Ich meine, wir leben in einem digitalen Zeitalter, in dem jeder Vorgang irgendwo digital erfasst wird. Es sollte keine Schwierigkeit sein, eine Statistik auf dieser Grundlage zu bilden. Bei vielen anderen Maßnahmen von geringerer oder höherer Eingriffsintensität hat man das auch gemacht. Ich nenne als Beispiel nur den IMSI/IMEI-Catcher. Da gibt es auch diese Berichtspflichten, an anderen Orten auch.

Dann die Frage zur Entschlüsselung und ob sich daraus verfassungsrechtliche Probleme ergeben. Herr Rechtsanwalt Breyer hat ja schon etwas gesagt zur Möglichkeit der Entschlüsselung. Verfassungsrechtlich ist es so, dass für die Geeignetheit einer gesetzgeberischen Entscheidung es ausreicht, dass die Maßnahme förderlich ist. Es reicht also ein fördernder Beitrag. Wenn in Einzelfällen eine Entschlüsselung möglich ist, was ich nicht abschließend beurteilen kann, weil ich kein technischer Sachverständiger bin, dann ist das sicherlich geeignet. Hinzu kommt, dass es wohl auch um Zugangsdaten geht, die die Diensteanbieter vergeben. Und ich weiß nicht, ob die dann auch verschlüsselt mit Hashwert gespeichert sind. Aber der Diensteanbieter sollte dann eigentlich Zugriff auf den Klartext des von ihm vergebenen Passworts haben. Also da bestünde dann auch tatsächlich ein substanzieller Anwendungsbereich.

Gestatten Sie mir bitte abschließend noch eine ganz kurze Bemerkung zum Thema Komplexität. Mir geht es überhaupt nicht um Simplifizierungen. Mir geht es um Kategorisierungen. Ich denke, man sollte Schutzwürdigkeitsklassen von Daten bilden, denen dann gesetzgeberische Zwecke zugeordnet werden, woraus sich dann eine Art Ampelsystem generieren ließe, das es jedem Rechtsanwender ermöglicht, auf einen Blick zu sehen, welche Daten an wen übermittelt werden dürfen. Der Gesetzentwurf sieht zehn Minuten Prüfungszeit vor für die Diensteanbieter. Über die Frage, wie weit die Prüfungspflichten der Diensteanbieter gehen, haben wir noch gar nicht gesprochen. Ich habe mir erlaubt, am vergangenen Wochenende ein kleines Experiment zu machen mit Kolleginnen und Kollegen und denen zwei Beispielfälle gegeben. Alles gestandene Juristen mit 20, 30 Jahren Berufserfahrung. Das Ergebnis war ernüchternd. Die sind nicht mit diesem Gesetz zurechtgekommen! Die haben noch nicht mal die richtigen Grundlagen gefunden. Ich lade Sie ein, machen Sie diesen Versuch selbst. Versuchen Sie mal, so kleine Fallbeispiele aus der Praxis durchzuexerzieren. Man kommt irgendwann damit zurecht, aber nicht in zehn Minuten, also das setzt einen gehörigen Sachverstand voraus. Und wir haben hier Anwendungsfälle im Hunderttausenderbereich. Da geht es um viele Prüfungen. Vielen Dank noch für diese

Bemerkung.

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

SV **Holger Münch** (Bundeskriminalamt, Wiesbaden): Vielen Dank. Drei Fragen sind in meine Richtung gegangen. Erst einmal Herr Grötsch zum Thema Dokumentationspflicht. Da kann ich mich Herrn Löffelmann anschließen. Ich halte das auch für sehr, sehr sinnvoll, dass man nachhält, wie oft eigentlich eine solche Norm auch angewandt wird, wie die Entwicklung ist. Wir werden übrigens jetzt hier noch einen Schritt weiter gehen. Im Zuge der Umsetzung des neuen Rechts zum Aufbau der zentralen Meldestelle werden wir ein Controlling aufbauen, mit dem nicht nur die Quantität, sondern auch die Qualität mit erfasst wird, also auch die Erfolgsquoten, um am Ende auch so auf Schwachstellen aufmerksam zu machen, also auch Politikberatung am Ende betreiben zu können. Wir werden das auch so machen, dass wir im Prozess, das ist schon mal eine Antwort auch für Herrn von Notz, in unserem Vorgangsbearbeitungssystem die Bestandsdatenauskunft auch anstoßen und damit dokumentiert haben, damit wir sie auch hinterher an zentraler Stelle abrechnen können, das also möglichst einfach. Und damit fallen die Daten auch an. Damit spreche ich für das BKA und nicht für die Polizei in Deutschland, das heißt, wenn man das macht, muss man natürlich auch entsprechende Übergangsfristen schaffen; nicht alle arbeiten in gleicher Weise so, wie wir das tun, was die Dokumentationsmöglichkeiten angeht, es dürfen nicht zu viele manuelle Prozesse ausgelöst werden.

Gestatten Sie mir noch ein Wort zu dem Thema Passwörter, auch zu dem, was Herr Löffelmann schon gesagt hat. Es geht in der Praxis um insbesondere zwei Konstellationen: PIN und PUK sind wesentliche Dinge, um ein sichergestelltes Handy zum Beispiel auswerten zu können und Zugang zu bekommen, und da bietet gerade die PUK eine gewisse Erfolgswahrscheinlichkeit. Und das zweite sind die Zugangsdaten, die Sie genannt haben. Die Passwörter, da gebe ich Ihnen völlig Recht: Wenn sie verschlüsselt sind, und das will auch gar keiner antasten, dann sind Sie ab einer bestimmten Komplexität nach jetzigem Stand der Technik natürlich nicht mehr in der Lage, zu entschlüsseln. Ab acht Stellen wird es extrem schwierig dann auch ranzukommen. Das ist so. Aber, es ging ja auch darum, die Konstellationen zu erfassen, in denen man wirklich dann auch einen praktischen Nutzen hat, nämlich das Passwort im Einzelfall direkt beim Anbieter zu erheben.

Zur Umsetzung des Netzwerkdurchsetzungsgesetzes – Zentrale Meldestelle. Herr von Notz, wir rechnen nach wie vor mit den Zahlen aus dem Transparenzbericht. Bessere haben wir noch nicht. Das heißt, mit einem Arbeitsanfall von round about 250.000 Meldungen, die, wenn alle ihre Verpflichtungen erfüllen, beim BKA aufschlagen können und mit einer Annahme, dass davon etwa 150.000 auch wirklich in einer ersten Prüfung einen strafbewehrten Anfangsverdacht begründen und dann weiterbearbeitet werden. Ich halte das aber im digitalen Zeitalter für absolut notwendig auch, dass wir diesen Prozess so angehen. Wir werden immer mehr über diese digitalen Wege bekommen. Und wenn man sich anguckt: Insgesamt haben wir in Deutschland 5,6 Millionen Straftaten. Da muss man irgendwie 250.000 weitere Anzeigen auch bearbeiten können. Aktuell machen wir das mit etwa 60.000 in dem sogenannten NCMEC-Prozess, also Kinderpornografieverdachtsfälle, die aus den USA und Kanada kommen. Da schaffen wir das mit ungefähr 50 Mitarbeitern. Und das ergibt auch für uns eine Rechengröße plus weitere Automatisierung und Prozessverbesserung, dass wir sagen, wir kommen damit am Ende in der letzten Ausbaustufe hoffentlich mit 150 bis 200 Mitarbeitern hin, um diese Aufgabe zu erfüllen. Die Datenverarbeitung wird so laufen, dass wir in einem ersten Schritt mit gut 30 Mitarbeitern starten an einem Testpiloten in dieser zentralen Einheit. Wir haben weitere Mitarbeiter in den Facheinheiten für die Bewertung von kritischen Sachverhalten, insbesondere in solchen Fällen wie Volksverhetzung. Da ist das nicht so trivial. Es wird so sein, dass wir bei den Fällen, wo wir sagen, Straftaten erfüllt, aber nicht eindeutig zuzuordnen, immer mit der ZIT (Zentralstelle zur Bekämpfung der Internetkriminalität) zusammenarbeiten, mit der Justiz, dies ist soweit geklärt. Für die Frage der Beratung: Ist dieser Fall jetzt weiter zu bearbeiten, ja oder nein? Erfüllt er die Strafbarkeitsschwelle? Da hat sich die ZAC (Zentral- und Ansprechstelle Cybercrime) in Köln zur Verfügung gestellt, die für uns dann der Partner ist. Und wir haben die Prozesse mit den Ländern auch soweit geklärt, in welchem Format die Daten dann anschließend und auch die Beweismittel in die Länder gehen. Unsere

Schwachstelle ist momentan noch die Zusammenarbeit mit den Verpflichteten, weil noch rührt sich keiner, mit uns auch darüber zu reden. Die warten erst einmal auf geltendes Recht. Insofern werden wir in einem Piloten auch anfangen mit NGOs, „Hassmelden.de“ zum Beispiel, die uns dann Pakete geben, was bei ihnen ankommt, damit wir unsere Prozesse des Bewertens und des automatisierten Abarbeitens ausprobieren. Wir werden dann später aber natürlich wieder in die Bearbeitung der Meldungen nach dem NetzDG umschalten. Wir sind also relativ weit. Und ich glaube auch, wenn wir keine unliebsamen Überraschungen an dieser noch offenen Schnittstelle zu den Verpflichteten erleben, werden wir das auch packen. Und den festen Willen haben wir auch. Die weiteren Ausbaustufen haben wir da vorbereitet.

Dann haben Sie mich noch gefragt, ob ich das Urteil, die Regelungen seien „zu kompliziert“, teile. Wir haben früher mal gesagt, der Blick in das Gesetz erleichtert die Rechtsfindung. Das war so ein alter Spruch unter Polizisten. Das ist heute nicht mehr so, sondern heute erleichtert der Blick in die Auslegung des Gesetzes die Rechtsfindung. Das heißt, das was hier reinkommt, übersetzen wir über unsere Spezialbereiche in Erläuterungen, um Hinweise zu geben für die Mitarbeiter, in welchen Konstellationen kannst du, kannst du nicht, wo sind kritische Fälle und wen kannst du anrufen, um das zu klären. Also, es ist schon durch die Formulierung der Gesetze recht komplex geworden, wenn Sie nicht täglich damit arbeiten. Im BKA als eine spezialisierte Polizei finden wir uns damit zurecht. Allerdings würde ich diese Aussagen von Herrn Löffelmann durchaus teilen, dass es für denjenigen, der wirklich ins Gesetz gucken muss, um dann festzustellen, was kann ich, was darf ich, erhebliche Schwierigkeiten bedeutet; das kommt auch durch die Komplexität, die wir mittlerweile erreicht haben in den Formulierungen. Allerdings ist das ein Dilemma, wenn diese Bestimmtheitsanforderungen aus den Urteilen kommen, dann muss ich sie als Gesetzgeber auch umsetzen. Aber im Grunde würde ich diese Bewertung teilen. Ich frage mich, ob das dann wirklich immer zu einem Gewinn führt, wenn wir an weiteren Stellen dann wieder nochmals in Konkretisierung gehen müssen. Soviel zu Ihren Fragen.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Und zum Schluss noch Herr Professor Schwarz.

SV **Prof. Dr. Kyrill-Alexander Schwarz** (Julius-Maximilians-Universität Würzburg): Ganz herzlichen Dank. Das war ja eben ein sehr schöner Hinweis auf ein neues Verständnis der Rechtsbindung der Verwaltung, wenn man sich jetzt nur nach der Auslegung zunächst einmal bedienen muss. Aber, das zeigt natürlich auch, und ich möchte damit vielleicht auch auf die erste Frage unmittelbar antworten, ob das jetzt ein sozusagen taugliches Reparaturgesetz ist oder nicht. Die Komplexität beruht tatsächlich in erster Linie auf den Vorgaben des ersten Senats des Bundesverfassungsgerichts. Dahinter kommt man auch nicht zurück. Da hilft es auch nicht, mit Ockham's Razor zu versuchen, das Ganze zu simplifizieren. Dieses Gesetz, über das wir hier heute sprechen, ist das Ergebnis einer Rechtsprechung, die eben schlichtweg immer kleinteiliger geworden ist. Das kann man kritisieren, aber es ändert eben nichts daran, dass Sie als Gesetzgeber das im Wesentlichen umsetzen müssen in den durch Karlsruhe vorgezeichneten Räumen. Ich glaube in der Tat, wenn man sich die maßgeblichen Regelungen anschaut, hat der Gesetzgeber eigentlich diese Aufgabe sehr schön erfüllt. Er setzt das Doppeltür-Modell im Wesentlichen um, er differenziert zwischen den einzelnen Daten, er schafft abgestufte Eingriffsvoraussetzungen, er nimmt einen abgestuften Rechtsgüterschutz vor. Wenngleich ich gar nicht leugnen will, dass man über die Begrifflichkeiten im Einzelfall und über die unterschiedlich schweren, gewichtigen oder besonders gewichtigen Rechtsgüter natürlich diskutieren kann. Aber das ist eben das Aufgreifen der Fingerzeige, die die Rechtsprechung hier dem Gesetzgeber sicherlich aufgegeben hat. Und vor dem Hintergrund glaube ich auch, unbeschadet der hier ja heute auch in der Diskussion eigentlich aufzeigenden Differenzierungspotenziale hinsichtlich Telemedien, Telekommunikationsdaten, hinsichtlich der Frage Bestandsdaten, Nutzungsdaten oder Inhaltsdaten, dass der Gesetzgeber eben gerade nicht der Versuchung erlegen ist, hier einheitliche Regelungen zu schaffen. Im Zweifel wird man wohl sagen können, und das ist ja hier auch bereits angedeutet, dass es auch eine gewisse Übererfüllung des Gesetzgebers gibt. Ich habe das nur in anderen landesrechtlichen Anhörungen auch erlebt, eine Frage, die auch immer wieder auftauchte nach der Bedeutung des Richtervorbehalts für entsprechende Maßnahmen,

den Karlsruhe ja nun gerade auch nicht durchgängig gefordert hat. Nämlich in Ansehung offensichtlich doch der Erkenntnis, dass die Bestandsdatenauskunft als solche dem Grunde nach von einer geringeren Intensität ist. Das heißt, insgesamt bin ich tatsächlich der Auffassung, dass dieses Gesetz genau den Vorgaben auch genügt, die sich aus der Rechtsprechung des Bundesverfassungsgerichts ergeben haben.

Ich will auf einen zweiten Punkt noch hinweisen. Das war Ihre Frage, Frau Vorsitzende. Was ist die Alternative zur drohenden Gefahr? Also, zunächst einmal: Ich persönlich halte den Begriff der drohenden Gefahr für einen Weg, den der Gesetzgeber gehen kann. Ich habe das auch in der entsprechenden Anhörung im bayerischen Landtag auch immer so vertreten. Das geht. Das ist zwar mit einem Risiko verbunden, aber es ist der Versuch des Gesetzgebers, eine bestimmte Sachlage doch näher zu umschreiben. Das können Sie machen, wenn Sie den Begriff der drohenden Gefahr anders definieren wollen. Dann geht es letzten Endes darum, zu erkennen, dass wir im Gefahrenvorfeld hier mit Risiken, mit Bedrohungslagen zu tun haben und dass eben der Gesetzgeber hier weiter vorgreift und damit im Vorfeld dessen, was herkömmlich eigentlich polizeiliche Maßnahmen ausmachen, bereits Eingriffsbefugnisse schaffen will. Sie können das dann definieren als eine im Einzelfall gegebene, im Gefahrenvorfeld gegebene Bedrohungslage. Ob das sprachlich glücklicher ist, darüber kann man sicherlich streiten. Aber man hat dann zumindest das zum Ausdruck gebracht mit dieser Formulierung. Dass man gerade das Gefahrenvorfeld aufgegriffen hat und explizit benennt, bringt vielleicht zum Ausdruck, worum es nämlich in der Tat geht: Maßnahmen hier zu ermöglichen, die im Vorfeld klassischer, ausgeformter polizeirechtlicher Begrifflichkeiten sind, nämlich dem Gefahrenvorfeld. Das kann man sicherlich machen. Ich hoffe, Frau Vorsitzende, dass ich damit Ihre Frage auch hinreichend beantwortet habe.

Vors. **Andrea Lindholz** (CDU/CSU): Ja, vielen Dank. Dann wäre es aus Ihrer Sicht eine Konkretisierung und eine Klarstellung. Vielleicht kann man ja gucken, ob man noch was ändert oder sagen wir mal präzisiert oder klarstellt. Jetzt kommen wir noch zur zweiten Fragerunde. Frau Warken, bitte, für die Union.

BE Abg. **Nina Warken** (CDU/CSU): Ja, genau. Vielen Dank, Frau Vorsitzende. Vielen Dank auch an die Sachverständigen. Ich hätte zunächst eine Frage an den Herrn Münch, weil das in den Eingangsstatements jetzt auch mehrfach angesprochen wurde. Telemediengesetz, Telekommunikationsgesetz: Können Sie noch mal kurz den Unterschied von den Abläufen her von den Bestandsdatenabfragen zum einen nach dem TKG, zum anderen nach dem Telemediengesetz erklären? Und eine kurze Frage auch noch an den Herrn Schwarz. Das Thema Berufsgeheimnisträger und Passwortherausgabe war im Vorfeld auch immer mal wieder im Gespräch. Inwiefern sind denn die Berufsgeheimnisträger besonders geschützt bei der Passwortherausgabe? Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann Herr Dr. Wirth noch mal.

BE Abg. **Dr. Christian Wirth** (AfD): Ja, danke. Eine kurze Frage an Herrn Professor Bäcker und Herrn Professor Löffelmann. Wir haben vielfältige Probleme gesehen, sehr kleinteilige Regelungen und sehr kleinteilige Reparaturversuche. Wäre es eventuell angebracht, da das Bundesverfassungsgericht da eine Frist gesetzt hat auf Ende dieses Jahres, dass man diesen Gesetzesentwurf vielleicht zurückzieht und neu überarbeitet? Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Für die SPD noch mal Herr Grötsch.

BE Abg. **Uli Grötsch** (SPD): Vielen Dank, Frau Vorsitzende. Herr Präsident Münch, noch mal eine Frage an Sie, was die praktische Anwendung und die Auswirkungen auf Ihre Behörde angeht. Was würden Sie denn sagen, was sich für das Bundeskriminalamt im polizeilichen Praxisalltag ändern wird, speziell, wenn es etwa um die Umsetzung des Gesetzes zur Bekämpfung von Rechtsextremismus und Hasskriminalität geht? Würden Sie sagen, sind die vorgesehenen Voraussetzungen und Bedingungen praktikabel für Ihre Behörde oder sehen Sie vielleicht, dass die manuelle Bestandsdatenauskunft sogar erschwert wird? Und Herr Löffelmann eine Frage noch an Sie: Der Herr Professor Bäcker kritisiert in seiner Stellungnahme, dass die Übermittlung von Bestandsdaten aus Zuordnung dynamischer IP-Adressen womöglich gegen Unionsrecht verstößt, zumindest soweit für die Zuordnung Vorratsdaten verarbeitet werden dürfen. Wie sehen Sie das denn? Teilen Sie das?

Vors. **Andrea Lindholz** (CDU/CSU): Dann haben wir als nächstes noch mal Herrn Höferlin.

BE Abg. **Manuel Höferlin** (FDP): Danke schön, Frau Vorsitzende. Meine Fragen gehen an Herrn Professor Kelber. Es geht um die Abfrage von Bestandsdaten von dynamischen IP-Adressen. Werden dort hinreichende Kriterien geschaffen? Meine Frage an Sie: Welche Kriterien wären denn aus Ihrer Sicht notwendig, um eine Zuordnung von dynamischen IP-Adressen und Bestandsdaten vornehmen zu lassen? Und die zweite Frage an Herrn Professor Bäcker. Sie schreiben in Ihrer Stellungnahme, dass es sehr komplex und derzeit auch nicht in allen rechtlichen Facetten vorgesehen ist, wie bei Telemedien zwischen Bestandsdaten, Nutzungsdaten und Telemediendienst zu unterscheiden. Wenn die anstehende TKG-Novelle einige nicht nummerngebundene Dienste, also zum Beispiel Mail, bald als herkömmliche TK-Dienste einstuft, kann dann diese schwierige Abgrenzung ein Problem darstellen? Das waren jetzt zwei Fragen. Danke schön.

Vors. **Andrea Lindholz** (CDU/CSU): Dann kommt als nächstes noch mal Herr Movassat.

Abg. **Niema Movassat** (DIE LINKE.): Danke schön. Meine Fragen gehen an Herrn Breyer. Wir wissen ja, dass wichtige Elemente der Folgenabschätzung von Gesetzen im Bereich der Strafverfolgung und Gefahrenabwehr mittlerweile Statistikpflichten sind. Wir haben auch gelernt, dass bei der automatisierten Bestandsdatenauskunft eine solche Statistikpflicht besteht und heute auch zugleich gehört, dass es beim manuellen Auskunftsersuchen nicht besteht, auch bei sensiblen Daten nicht. Mich würde erstens interessieren, wie Sie das bewerten und zweitens wie eine Statistikpflicht in diesem Bereich gestaltet werden könnte.

Vors. **Andrea Lindholz** (CDU/CSU): Und zum Schluss noch Herr von Notz.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Frau Vorsitzende. Ich hätte noch mal zwei kurze Nachfragen an Herrn Münch und Herrn Bäcker im Hinblick auf die praktische Umsetzung. Im Gegensatz sozusagen zu ich nenne es jetzt mal die alte Praxis reden wir ja hier, wenn ich es richtig verstehe, über voll digitalisierte Prozesse der Datenweitergabe. Und da frage ich mich, also wenn man jetzt mal sagt, das stimmt von den Zahlen ungefähr, 250.000, 100.000 davon nicht relevant oder nicht strafrechtlich relevant, 150.000 Verfahren, die dann entstehen. Also, mit was für einer Software oder wie macht man denn das dann voll automatisiert? Und auch im Hinblick auf die Daten der Leute, die ohne strafrechtlichen Bezug bei Ihnen aufschlagen. Was passiert denn mit den Daten? Also, ich meine, alle im politischen Betrieb, unabhängig, aus welcher Himmelsrichtung sie kommen, erleben es jeden Tag. Wir werden natürlich bei Twitter alle jeden Tag gemeldet. Und die interessante Frage ist: Was passiert mit unseren Daten? Und das ist bei dem Umfang der Daten, wenn man sich das anguckt, glaube ich schon eine relevante Frage. Und Sie ziehen die praktische Frage, Herr Münch. Und Herr Bäcker für Sie die Frage: Was für einen Anspruch, also wahrscheinlich muss man das nicht rechtlich bis ins letzte Detail regeln, aber was für einen Anspruch hat man an die technische Umsetzung in diesen voll automatisierten Abläufen, die es dann geben wird, damit man diese Anzahl von Verfahren mit der Anzahl von Beamt*innen, die Herr Münch genannt hat, überhaupt stemmen kann?

Vors. **Andrea Lindholz** (CDU/CSU): Ich würde noch mal kurz zwei Ergänzungsfragen an Herrn Professor Löffelmann stellen. Herr Schwarz hat jetzt ja gerade noch mal näher präzisiert, was man eventuell noch machen könnte, um bei der drohenden Gefahr noch deutlicher zu machen, dass es um die Gefahr im Vorfeld geht und möglicherweise auch das dann konkreter ausgestaltet werden könnte oder sollte. Würden Sie diese Auffassung teilen? Und zum zweiten: Es ist jetzt noch mal recht deutlich geworden, Sie haben aber auch noch mal versucht, das klarzustellen, es geht Ihnen jetzt nicht darum, ein ganz einfach strukturiertes Gesetz zu machen, das ist auch schwierig bei solchen Dingen, aber einfach mehr Klarheit, so habe ich es zumindest verstanden. Wenn Sie sich jetzt „was wünschen“ dürften und diesen Text hier jetzt noch haben, was wäre dann das, wo Sie sagen, also damit könnte man tatsächlich noch für Verbesserung sorgen? Es ist mir klar, wenn man eine komplett andere Auffassung hat, es müsste eigentlich ganz anders ausschauen, ist das schwierig. Aber vielleicht finden Sie ja was, wo Sie sagen, das könnte den Anwendern in der Praxis dann doch noch helfen, wenn wir jetzt schon so weit sind, wie wir sind.

Dann kommen wir jetzt zur Antwortrunde. Diesmal im Alphabet rückwärts oder von hinten aufgerollt beginnen wir mit Herrn Professor Schwarz.

SV **Prof. Dr. Kyrill-Alexander Schwarz** (Julius-Maximilians-Universität Würzburg): Ich hatte nur eine ganz kurze Frage von Frau Warken zum Schutz von Berufsgeheimnisträgern. Also, hier sind zwei Aspekte zu berücksichtigen. Soweit sich eine Bestandsdatenauskunft als Ermittlungsmaßnahme erweist, bleibt es bei der Regelung des § 160a der Strafprozessordnung, der ein entsprechendes Schutzniveau vorsieht und einen entsprechenden Schutz von Berufsgeheimnisträgern dann auch entsprechend anordnet. Darüber hinausgehend ist jedenfalls – soweit kann man tatsächlich auch einmal von richterlicher Zurückhaltung sprechen – der Entscheidung Bestandsdatenauskunft II keine weitergehende Regelung oder kein weitergehendes Anforderungsprofil zum Schutz von Berufsgeheimnisträgern zu entnehmen, sodass diesbezüglich der Gesetzgeber tatsächlich frei ist in der Ausgestaltung dessen, was er machen möchte.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Professor Schwarz, vielen Dank. Herr Münch.

SV **Holger Münch** (Bundeskriminalamt, Wiesbaden): Die Fragen in meine Richtung waren zunächst erst einmal unterschiedliche Verfahren bei Bestandsdatenabfragen TKG und TMG. Ganz vereinfacht dargestellt behandeln wir im TKG meistens bei den Bestandsdaten Vertragsdaten von Mobilfunkverträgen, aber nicht nur Mobil, manchmal auch stationär, also Festnetz. Und dahinter versteckt sich die sogenannte Anschlussinhaberfeststellung, dass wir also wissen wollen, wer ist dort der Vertragsinhaber. Beim TMG reden wir über Dienstanbieter im Internet, bislang auch E-Mail-Anbieter oder Messengerdienste und hier die Nutzerkonten und die dort hinterlegten Daten, also die Namen, gegebenenfalls weitere Daten wie eine E-Mail-Adresse oder auch hier eine Telefonnummer. Der wesentliche Unterschied besteht im Weiteren darin, dass wir eine Verifizierungspflicht für einige Verpflichteten nach dem TKG, wenn auch nicht für alle, haben, also die Telekommunikationsanbieter, haben, aber nicht für die Telemediendienstanbieter. Das heißt, Sie bekommen bei TK-Anbietern schon ein geprüftes Datum bei einer Anschlussinhaberfeststellung, meistens also auch ein verlässliches Datum. Bei den Telemediendienstanbietern kann es Ihnen auch passieren, dass Sie da Donald Duck aus Entenhausen bekommen und damit weiterarbeiten müssen. Allerdings in der Praxis haben wir über die hinterlegten Daten auch häufig noch weitere Ermittlungsansätze, selbst wenn dort nur ein Pseudonym verwendet wird, ist das vielleicht auch im Netz verwendet worden oder wenn eine E-Mail-Adresse oder eine Telefonnummer angegeben ist, die dort hinterlegt worden ist, dann ist das wieder ein weiterer Ansatzpunkt, um tätig werden zu können. Insofern, wenn Sie mich fragen, was uns noch helfen würde, dann wäre das zumindest sowas wie eine Plausibilisierungsverpflichtung. Also, wir gehen nicht davon aus, dass Telemediendienstanbieter mit all ihren Geschäftsmodellen auch verifizieren können, das wäre viel zu kompliziert. Aber Sie plausibilisieren selbst, Sie kennen das, dass Sie immer eine SMS bestätigen müssen, die Sie bekommen oder dass Sie auf eine E-Mail, die Sie bekommen, antworten müssen, um ein Konto zu aktivieren. Dann hätten wir ein plausibilisiertes Datum. Das würde uns sehr helfen.

Die zweite Frage, Herr Grötsch, war, ob sich in der Umsetzung für uns jetzt etwas ändert gegenüber den Planungen durch dieses Gesetz, insbesondere was die Umsetzung Hasskriminalität angeht, also Netzwerkdurchsetzungsgesetz. Nein. Also mit diesem Gesetz werden wir die Prozesse auch hinbekommen und werden die Schwelle erreichen, um dann hier auch die Bestandsdatenabfragen stellen zu können. Und, Herr von Notz, zum Praktischen, wie wir das machen. Wir haben ein Vorgangsbearbeitungssystem im BKA, das mit Massendaten umgehen kann, es heute schon tut. Sämtlicher nationaler, internationaler Schriftverkehr wird darüber dokumentiert und gesteuert. Wir haben eine Brücke auch zu dem SIENA-Europol-System (Secure Information Exchange Network Application). Das heißt, diese Zahlen an sich schrecken uns noch nicht in der technischen Abarbeitung. Wir sind gerade dabei, auch die Ertüchtigung zu machen, dass wir dann auch hieraus in dem Format, was in allen Polizeien gelesen werden können muss, auch die Daten weitergeben an die Länder. Auch das ist soweit abgestimmt. Auch die Art und Weise, wie wir das automatisiert weitergeben, ist abgestimmt. Und auch die elektronischen Beweismittel werden wir auch übergeben können an die Länder, die sich dafür fit machen bis spätestens März. Und was mit den Daten passiert im Anschluss? Da verweise ich auf die §§ 12, 18, 19

des BKA-Gesetzes. Das heißt umgekehrt, dass wir die Daten, die wir zum Zwecke der Erhebung nicht mehr oder Verwendung für andere Zwecke nicht für erforderlich halten, dann auch zu löschen haben. Das heißt im Prinzip, sämtliche Daten, die wir dann weitergeben an die Länder, um das Strafverfahren durchzuführen, auch kein anderer Zweck im BKA mehr gesehen wird, das wäre eine Zweckänderung, dann wären sie zu löschen. Einzige Ausnahme wäre, dass wir sie bis zu einem Jahr in einem Prüftopf halten können, in einer Vorsorgedatei, wenn wir sagen, das ist für andere Belange, die auch im BKA relevant sind, von Interesse. Hier verweise ich auch auf die Anforderung, die an uns gestellt wird, ihr müsst auch Verbindungen, Personenverbindungen erkennen. Wir sind ja auch im Kontakt mit NGOs, die auch immer mal wieder sagen, ja, dahinter stehen Strukturen. Wenn wir nur erheben, weiterleiten und löschen, werden wir das nicht können. Also, die Auslegung dieser Norm, wann werden wir nach § 18 Absatz 3 BKAG oder 19 Absatz 3 BKAG die Daten zumindest übergangsweise speichern, um zu erkennen, erkennen wir hier besondere handelnde Personen, die wird noch mal sehr, sehr spannend in der Praxis. Und ich glaube, da sollten wir dann auch noch mal drüber reden, wenn wir in der Praxis sind.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Münch, vielen Dank. Herr Professor Löffelmann.

SV **Prof. Dr. Markus Löffelmann** (HS Bund, Berlin): Vielen Dank. Herr Dr. Wirth hat gefragt, ob es eine Option wäre, den Gesetzentwurf zurückzuziehen und zu überarbeiten. Ich meine, nein. Ich bin mir durchaus bewusst, wie viel Arbeit da drin steckt und was für langwierige Prozesse es sind, um so einen Gesetzentwurf überhaupt auf die Beine zu stellen. Und es ist ja auch keine ganz einfache Sache. Also ich denke, das würde man in der gegebenen Zeit nicht hinbekommen und, wie ich auch in meiner schriftlichen Stellungnahme ausgeführt habe, ich denke es geht vor allem auch darum, dieses enorm praxisrelevante Instrument der Bestandsdatenabfrage für die Sicherheitsbehörden zu erhalten. Also ein solches Risiko würde ich auf gar keinen Fall eingehen. Es gibt hier in diesem Gesetzentwurf noch zahlreiche technische Details, die man sich noch einmal ansehen wird, die ich auch in meiner schriftlichen Stellungnahme ausgeführt habe. Das wird in den zuständigen Ressorts sicher aufmerksam gelesen werden und das sollte man dann auch umsetzen.

Herr Grötsch hat nach der Vereinbarkeit des Gesetzentwurfs mit dem Unionsrecht gefragt. Wenn ich das richtig sehe, dann betrifft die von Herrn Professor Bäcker zitierte Entscheidung aus dem Oktober vergangenen Jahres „La Quadrature du Net“ die Speicherverpflichtung, und zwar die Pflicht, Daten auf Vorrat – auf Vorrat! – zu speichern. In dieser Entscheidung werden Bestandsdaten und IP-Adressen gleichgesetzt in den Anforderungsschwellen, um solche Daten auf Vorrat zu speichern. In einer anderen Entscheidung, die Herr Bäcker auch in seiner Stellungnahme zitiert hat, aus 2018, „Ministerio Fiscal“, da geht es um den *Zugriff* auf Daten und auf Bestandsdaten. Und der Zugriff auf Bestandsdaten ist auch nach den Vorgaben des EuGH nicht an eine erhöhte Schwelle gebunden, sondern auch zur Verfolgung einfacher Straftaten zulässig. Also, ich denke, wir sehen hier eben genau dieses Zusammenspiel, das wir auch in der verfassungsgerichtlichen Rechtsprechung sehen, dass nämlich der Aspekt eines Bevorratens von Daten zur späteren Verwendung immer an höhere Schwellen gebunden ist. Aber darum geht es ja in unserem Gesetzentwurf überhaupt nicht, sondern bei uns geht es um die Befugnisse zur Übermittlung und zur Abfrage von Daten, nicht um eine Pflicht zur Datenbevorratung. Also, von daher, ich denke, das ist vereinbar mit den Vorgaben des EuGH.

Und Sie, Frau Vorsitzende, Sie haben gefragt, wie ich das mit der drohenden Gefahr im Hinblick auf die Äußerungen von Herrn Professor Schwarz sehe. Zunächst einmal bin ich Herrn Professor Schwarz sehr dankbar, dass er dieses Thema so kundig angesprochen hat und auch die Formulierung, die ich in meiner schriftlichen Stellungnahme vorgeschlagen habe, in die Diskussion eingebracht hat, dass man nämlich formuliert „um im Einzelfall im Gefahrenvorfeld eine aufgrund tatsächlicher Anhaltspunkte gegebene Bedrohungslage für ein Rechtsgut von erheblichem Gewicht aufzuklären“. Mit einer solchen Klarstellung schlägt man mehrere Fliegen mit einer Klappe. Zum einen begibt man sich nicht auf das Glatteis dieser Begrifflichkeit „drohende Gefahr“, was eben mit einem verfassungsrechtlichen Risiko verbunden wäre, weil dieser Begriff amorph und verfassungsgerichtlich ungeklärt ist. Es besteht meines Erachtens über-

haupt kein Zweifel daran, dass die Sicherheitsbehörden, auch die Polizei, über informationelle Befugnisse im Gefahrenvorfeld verfügen sollten. Das macht sehr viel Sinn und das habe ich auch im bayerischen Landtag so vertreten, denn gerade weil die Polizeien mit intensiven aktionellen Befugnissen versehen sind, sollten sie natürlich wissen, was sie da tun. Das setzt zunächst mal voraus, Informationen zu bekommen, zu generieren. Und dafür sollten sie auch im Gefahrenvorfeld tätig werden. Aber das sollte dann eben auf informationelle Maßnahmen beschränkt sein. Deshalb passt auch die Rede von dem Abwehren von Gefahren in diesem Zusammenhang nicht so. Ich würde da eher von Aufklären sprechen. Die Tätigkeit der Polizeien gleicht in diesem Bereich viel mehr der der Nachrichtendienste, die auch Informationen sammeln und aufklären und bei denen man auch nicht von Gefahrenlagen spricht. Auch das Bundesverfassungsgericht tut das im Übrigen, wenn es sagt, auch bei den Nachrichtendiensten muss ja eine konkrete Gefahr als Voraussetzung bestehen. Das passt überhaupt nicht zur Systematik des Sicherheitsrechts, sondern es geht um Bedrohungslagen. Das G 10 zum Beispiel knüpft an diesen Begriff an – Bedrohungslagen. Und für eine Bedrohungslage müssen dann tatsächliche Anhaltspunkte bestehen. Also, das würde dann sehr viel Sinn machen und man müsste nicht auf diesen Begriff der drohenden Gefahr ausweichen, der sich im Übrigen auch von dem unterscheidet, den der bayerische Gesetzgeber in Artikel 11 des Bayerischen Polizeiaufgabengesetzes ausbuchstabiert hat. Wir haben also hier keine Kongruenz. Und wenn man das Recht anwenden möchte, dann muss man mit zwei unterschiedlichen Begriffen der drohenden Gefahr arbeiten, was einen eigentlich vor unlösbare Aufgaben stellt. Wenn man sich jetzt in den Diensteanbieter hineinversetzt, der liest „drohende Gefahr“ und dann muss er in das Bayerische Polizeiaufgabengesetz schauen und da findet er eine ganz andere drohende Gefahr.

BE Abg. **Uli Grötsch** (SPD): Können Sie diese Unterscheidung mal ein bisschen deutlich machen, was da der Unterschied zwischen dem aus Bayern ist und dem hier im Gesetz?

SV **Prof. Dr. Markus Löffelmann** (HS Bund, Berlin): Ja, der bayerische Begriff der drohenden Gefahr ist erstens vorgelagert, er wird geregelt in der polizeilichen Generalklausel. Das heißt, er bezieht sich übergreifend auf den ganzen Bereich des Polizeirechts und eben nicht nur auf informationelle Maßnahmen, sondern auch auf aktionelle Befugnisse, auf die in den Standardbefugnissen der Gesetzgeber dann wieder Bezug nimmt. Das ist eigentlich der entscheidende Punkt gewesen, der zur Kritik im Rahmen des Gesetzgebungsverfahrens geführt hat und jetzt auch das Bundesverfassungsgericht mit dieser abstrakten Normenkontrolle beschäftigt. Und dann ist der Begriff der drohenden Gefahr durch den Bezug auf bestimmte Rechtsgüter, die der bayerische Gesetzgeber als bedeutende Rechtsgüter bezeichnet – gibt es eigentlich nicht bedeutende Rechtsgüter? – eingeschränkt. Der Begriff der drohenden Gefahr, der *hier* verwendet wird, ist viel allgemeiner, sag ich mal. Wenn wir in die Details gehen, hier werden ja Formulierungen des Bundesverfassungsgerichts paraphrasiert, dann gibt es da, wenn man das vergleicht, noch im Detail einige andere Unterschiede. Das sind also keine wortgleichen Formulierungen und bekanntlich werden ja die Worte des Bundesverfassungsgerichts immer auf die Goldwaage gelegt. Man möchte das also so genau wie möglich übernehmen. Das Bundesverfassungsgericht hat in dieser Passage im BKAG-Urteil nie von einer drohenden Gefahr gesprochen mit drohend in einem attributiven Sinn, so wie wir von einer unmittelbaren Gefahr, gegenwärtigen Gefahr, konkreten Gefahr sprechen, sondern es hat davon gesprochen in einem prädikativen Sinne, von einer im Einzelfall drohenden Gefahr für ein Rechtsgut, das ist das drohend, was Herr Schwarz angesprochen hat, jeder Gefahr eignet irgendwie, dass sie droht. Wenn wir also den Begriff der drohenden Gefahr in diesen Kontext setzen, dann sind wir wieder bei der drohenden drohenden Gefahr. Und das macht keinen Sinn. Also, ich bin hier im Grunde genommen weitgehend d’accord mit Herrn Schwarz.

Und Sie haben – vielen Dank dafür – mich gefragt, was für Wünsche ich hätte. Also, das wäre der erste Wunsch, dass Sie diesen Begriff der drohenden Gefahr, dass Sie einfach darauf verzichten, das anders umschreiben. Dann der zweite wäre, dass Sie die Prüfpflichten der Anbieter klarstellen. Also, ich kann hier nur noch mal wiederholen: Für mich macht das keinen Sinn, materielle Übermittlungsschwellen festzuschreiben und dann zu sagen, jemand anders trägt die Verantwortung dafür. Das ist datenschutzrechtlich Nonsens, denn datenschutzrechtlich trägt die Person, die die Befugnis

hat, auch die Verantwortung. Und ich kann hier auch noch auf eine prominente Stimme verweisen. Der bayerische Datenschutzbeauftragte, Professor Petri, hat in einer Anmerkung zur gegenständlichen Entscheidung des Bundesverfassungsgerichts genau darauf hingewiesen. Er hat dort ausgeführt, dass sogar die Ausführungen des Bundesverfassungsgerichts – ich möchte das kurz zitieren in diesem Zusammenhang – dass die „missverständlich“ seien und „irritierend“, dass eben die Verantwortung für die Prüfung bei den Dienstanbietern liegen müsse. Vielleicht finden Sie einen Weg, das irgendwie doch klarzustellen, wer was prüfen muss. Und langfristig würde ich mir von Ihnen wünschen, dass Sie nicht darüber diskutieren, ob etwas ein hervorgehobenes Rechtsgut benötigt oder ein besonders gewichtiges Rechtsgut, worunter sich niemand wirklich was vorstellen kann, sondern dass Sie darüber streiten, ob beispielsweise Bestandsdaten der Schutzkategorie 1, 2 oder 3 zugehören, aus den und den und den Gründen. So würde man Gesetze viel, viel substanziierter gestalten können. Vielen Dank.

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

SV **Prof. Ulrich Kelber** (BfDI, Bonn): Vielen Dank, Frau Vorsitzende. Zur Frage des Abgeordneten Höferlin: Nach dem Bundesverfassungsgericht müssen Auskünfte anhand einer dynamischen IP-Adresse aufgrund der damit verbundenen erheblich größeren Persönlichkeitsrelevanz dem Schutz besonders gewichtiger Rechtsgüter dienen. Ich darf mal zitieren: „Soweit die Gefahrenabwehr auf die Verhütung von Straftaten bezogen ist, muss es sich um zumindest schwere Straftaten handeln. Diese Vorgabe erfüllen die vorgesehenen Formulierungen im § 63a und 66a Bundeskriminalamtsgesetz nicht.“ Das Verfassungsgericht sieht außerdem vor, dass der Gesetzgeber abschließend festlegt, welche Straftatbestände hiervon umfasst sein sollen. Auch hier darf ich zitieren: „Der Gesetzgeber, also er, kann dabei auf bestehende Kataloge zurückgreifen oder einen eigenen Katalog schaffen, etwa um Straftaten zu erfassen, für die die Zuordnung von IP-Adressen besondere Bedeutung hat. Die Qualifizierung einer Straftat als schwer muss aber in der Strafnorm etwa durch deren Strafrahmen einen objektivierten Ausdruck finden. Eine Generalklausel und die lediglich pauschale Verweisung auf nicht mehr eingegrenzte Straftaten reichen hingegen nicht aus.“ So das Verfassungsgericht. Aus meiner Sicht bietet es sich also an, die Straftatbestände schwerer Straftaten abschließend festzulegen, für die die Zuordnung von IP-Adressen besondere Bedeutung hat und deswegen es auch diese Zugriffsmöglichkeit gibt.

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

SV **Jonas Breyer** (Rechtsanwalt, Wiesbaden): Vielen Dank, Frau Vorsitzende. Die an mich gerichteten Fragen gehen hier zunächst einmal in die Richtung, dass eine Folgenabschätzung von Gesetzen doch Statistikpflichten vorsehen sollten, die es bei der automatisierten Bestandsdatenabfrage nach § 112 des TKG gibt, bei der manuellen Bestandsdatenabfrage aber nicht. Das ist richtig. Und da war die Frage, wie ich das bewerte. Ja, ich hatte es schon in meiner Eingangsstellungnahme kurz angesprochen, dass ja der Entwurf keine statistischen Aufzeichnungspflichten vorsieht. Es gibt zwar im Zusammenhang mit dem Abruf von Zugangsdaten und mit der Bestandsdatenabfrage im Zusammenhang mit dynamischen IP-Adressen gewisse Pflichten, das aktenkundig zu machen. Das ist aber keine Statistik insgesamt zu den manuellen Bestandsdatenabfragen. Und die Anzahl dieser Zugriffe sollte also nach meiner Überzeugung der Öffentlichkeit zugänglich gemacht werden, sodass das Ausmaß transparent wird. Es sollte auch im Interesse des Gesetzgebers liegen, dass er sich davon überzeugt, dass seine Maßnahmen auch wirken und dass man bei nicht wirksamen Maßnahmen die wieder außer Kraft setzt oder nachbessert. Und solche Statistiken sind auch erforderlich, um nicht nur die Notwendigkeit von Normen zu ermitteln, sondern auch, um deren Missbrauch überhaupt erst einmal sichtbar zu machen. Und es handelt sich bei dem Ganzen um Eingriffe in die Vertraulichkeit von Telekommunikationsverhältnissen, darunter die Identifizierung von Internetnutzern, um die Übermittlung von Codes und Zugangssicherungen zu überwinden.

Zu den Zahlen kann ich beispielsweise beitragen aus dem verfassungsgerichtlichen Verfahren. Da wurde bekannt zu manuellen Bestandsdatenabfragen, also soweit überhaupt dazu Zahlen vorlagen, die beispielsweise aus Gebührenabrechnungen und Ähnlichem teilweise rekonstruiert werden konnten, dass in den Jahren 2013 bis 2017

manuelle IP-Abfragen durch das BKA sich vervielfacht haben von 2.001 auf über 17.000 Fälle. Auf der anderen Seite ist bekannt geworden, dass etwa Zugangsdatenabfragen in den Jahren 2016 bis 2018, die konnten da ermittelt werden, durch den BND und den MAD nie erfolgten, also in null Fällen. Und da kann man sich natürlich auch fragen: Warum ist ein solches Gesetz nötig, das in null Fällen eigentlich von den Behörden selbst aber angewandt wurde und welcher Sicherheitsgewinn soll sich daraus eigentlich ergeben durch ein solches Gesetz? Und das könnte und sollte behoben werden durch eine solche Statistik. Da möchte ich mich auch ausdrücklich anschließen Herrn Professor Löffelmann und auch Herrn Münch, der sich ja ebenfalls dafür ausgesprochen hat, wenn ich das richtig mitbekommen habe, zumal für automatisierte Bestandsdatenabfragen eine solche Statistik ohnehin auch schon heute besteht. Das ist ein logischer Bruch, warum das ausgerechnet für automatisierte Abfragen erfolgen soll und für manuelle nicht.

Ich komme dann direkt zur nächsten Frage, die auch inhaltlich im engen Zusammenhang damit steht. Wie könnte eine solche Statistikpflicht aussehen? Ich habe mich mal in meiner schriftlichen Stellungnahme auch an einer Ausformulierung versucht. Und man kann dabei Anleihen nehmen bei einem früheren Gesetzentwurf des Bundesjustizministeriums. Da ging es um das sogenannte Quick Freeze-Verfahren. Es stand auch im Umfeld der Vorratsdatenspeicherung, wo also entsprechend einer früheren Vorschrift der Strafprozessordnung, heute ist das der § 101b, bestimmte Daten zu statistischen Zwecken erfasst werden und einmal im Jahr dann von Bund und Ländern übermittelt werden, nämlich die Anzahl der Verfahren, in denen Bestandsdaten übermittelt wurden, die Anzahl der Verfahren, in denen Nutzungsdaten gegebenenfalls übermittelt wurden, wenn sich der Gesetzgeber dazu entschließen sollte, und die Anzahl der IP-Adressen, weil es sich ja da um einen noch tieferen Grundrechtseingriff handelt nach der Rechtsprechung des Bundesverfassungsgerichts, zu denen die Behörden um Auskunft ersucht haben und die Anzahl der Verfahren, in denen Passwörter und ähnliche Zugangscodes herausgegeben wurden. Und diese Daten sollten übermittelt werden an das Bundesamt für Justiz, das auch andere Statistiken heute schon erstellt und das sollte dieses dann jährlich im Internet der Öffentlichkeit zugänglich machen. Vielen Dank.

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

SV **Prof. Dr. Matthias Bäcker** (Johannes Gutenberg-Universität Mainz): Herzlichen Dank. Ich bin gefragt worden von Herrn Höferlin nach Telemedien und der Differenzierung unterschiedlicher Daten: Welche Rolle spielt da die anstehende Novelle des Telekommunikationsgesetzes? Also, im Moment ist es so – und das ist eine sehr missliche Situation aus sicherheitsrechtlicher Sicht – nach einer Entscheidung des Europäischen Gerichtshofs von 2019 sind Telemediendienste, die der Individualkommunikation dienen, sogenannte Over-the-Top-Dienste wie E-Mail oder Instant Messaging, das sind alles keine Telekommunikationsdienste, sondern Telemediendienste. Da kommen wir nicht dran vorbei, weil das vorgeprägt ist durch europäisches Recht. Die Überwachung von E-Mail ist in Deutschland immer als Telekommunikationsüberwachung angesehen worden und immer auf die entsprechenden Regelungen zum Beispiel in der StPO gestützt worden. Das geht eigentlich nicht mehr. Und das ist ein Problem, weil wir jetzt keine passende Regelung mehr haben im aktuellen Recht. Die Praxis behilft sich damit, das weiterhin als Telekommunikationsüberwachung anzusehen mit der Begründung, die E-Mail-Anbieter würden ja irgendwie auch an den Telekommunikationsdiensten der Internetprovider mitwirken. Das halte ich für absolut abwegig und unvertretbar, sodass wir hier einfach im Moment eine Lücke haben. Diese Lücke wird allerdings geschlossen, sobald das Telekommunikationsgesetz erneuert worden ist, denn dann sind diese Dienste Telekommunikation, sodass wir das Problem nicht mehr haben. Was verbleibt ist immer noch ein riesiger bunter Strauß an unterschiedlichen Telemediendiensten, wo ganz unterschiedliche Daten anfallen, die auch ganz unterschiedlich sensibel sind. Der Aufruf der statischen Internetseite des Innenausschusses ist genauso ein Vorgang der Telemediennutzung wie die Nutzung eines Social Media-Anbieters wie Facebook, und zwar alles, was ich mit Facebook mache. Und man kann mit den anfallenden Daten alles nachvollziehen, was ich jemals auf Facebook veröffentlicht habe oder auch nur einem beschränkten Personenkreis geschickt habe, alles, was ich zukünftig dort veröffentliche, das sind alles Telemediennutzungsdaten, die dann nach dem Entwurf

unter sehr niedrigen Voraussetzungen ausgeleitet werden können. Das haut nicht hin.

Wir brauchen da ein größeres Gespür für die Sensibilität dieser Daten. Und die Frage „Was sind eigentlich Telemediennutzungsdaten, was sind Telemedieninhaltsdaten?“ ist sehr, sehr schwierig, weil die Kategorie der Inhaltsdaten überhaupt nicht definiert ist und sich auch nicht wirklich trennscharf abgrenzen lässt. Mein Vorschlag wäre deswegen: Nehmen Sie eine Regelung ins Gesetz auf, wo Sie Nutzungsdaten und Inhalte, falls es die denn geben sollte, einfach gleich behandeln. Tragen Sie der Sensibilität dieser Daten Rechnung, indem Sie sagen, die Voraussetzungen sind dieselben wie für eine Telekommunikationsüberwachung. Damit wären Sie meiner Ansicht nach verfassungsrechtlich auf der sicheren Seite, hätten der Welt etwas Gutes getan und würden den berechtigten Anliegen der Sicherheitsbehörden genügen.

Herr von Notz hat mich gefragt, wenn ich das richtig verstanden habe, zu den Netz-DG-Daten, die jetzt an das BKA geschafft werden und vom BKA ausgewertet werden müssen: Wie läuft das eigentlich und was sind da die juristischen Desiderate? Herr Münch hat ja aus der praktischen Sicht geklärt, was man macht. Eine ausgeleitete Nachricht kommt ins Vorgangsbearbeitungssystem, wird ausgefiltert, wird weitergeleitet an die zuständige Strafverfolgungsbehörde und dann guckt man, ob man die Daten vielleicht noch für die Zwecke der Zentralstellenfunktion des BKA benötigt. Das ist die eine Sache. Das denke ich ist auch alles vollkommen zutreffend. Dagegen bestehen auch keine prinzipiellen Bedenken, auch nicht gegen die Datenbevorratung im Rahmen der Zentralstellenfunktion. Ich persönlich halte die Zentralstellenregelungen im BKA-Gesetz in §§ 12, 18, 19 teilweise für verfassungswidrig, aber das ist eine ganz andere Baustelle, nicht Gegenstand der heutigen Anhörung. Ich habe Herrn von Notz, und da würde ich gern nachfragen, jetzt so verstanden, dass Ihr Anliegen auch war: Was machen wir denn, wenn das BKA die Daten gewissermaßen automatisiert auswertet, da also einen Algorithmus drüber laufen lässt, um strafbare Inhalte automatisch zu erkennen? War das richtig, dass ich das so verstanden habe?

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Exakt.

SV **Prof. Dr. Matthias Bäcker** (Johannes Gutenberg-Universität Mainz): Ja, also das ist in der Tat so ein bisschen … da stoßen Sie in eine offene Flanke der verfassungsrechtlichen Diskussion, nämlich: Was mache ich eigentlich mit solchen Massendatenauswertungen auf automatisierter Basis? Das herkömmliche Sicherheitsrecht geht immer davon aus, wenn ich Daten erheben darf, dann darf ich sie im Rahmen des Erhebungszwecks eigentlich mit allen Mitteln verarbeiten, also auswerten, nutzen, die die Technik hergibt. Das ist sozusagen nachgelagert mitgeregelt. Wenn wir komplexe Datenanalysen durchführen, wie das hier der Fall ist, kann man sich natürlich schon fragen: Steigt dadurch nicht die Sensibilität des Vorgangs so erheblich, dass wir hier noch mal eine eigene Stufe einziehen müssen, wo wir auch besondere Anforderungen stellen müssen? Da sind wir einfach in der Diskussion noch nicht besonders weit. Es gibt zu dem Thema Open Source Intelligence, in dem wir hier drin sind, da gibt es jetzt erste Publikationen und erste Diskussionen darum, aber wirklich trennscharfe Lösungsvorschläge dafür kenne ich jedenfalls noch nicht und wir haben an meinem Lehrstuhl an solchen Projekten auch mitgearbeitet und haben das Problem versucht zu konkretisieren, aber haben jetzt auch noch keine Antwort darauf.

Das führt mich so ein bisschen zur letzten Frage von Herrn Wirth: Sollte man das nicht alles wegschmeißen und in der nächsten Legislaturperiode neu machen? Also, ob das politisch eine gute Idee und auch handhabbar wäre, das wissen Sie alle besser als ich. Als Staatsbürger würde es mich wundern, aber kann ja sein. Ich halte es aber auch nicht für erforderlich. Das Gesetz, so wie es steht, ist überarbeitungsbedürftig. Ich denke, dass die Kollegen und ich jetzt verschiedene Punkte hoffentlich aufgezeigt haben, wo Überarbeitungsbedarf besteht. Ich glaube, dass der aber auch abarbeitbar ist. Es gibt sicherlich auch Punkte, wo man sagen kann, da kann man Bedenken haben, kann man auch mal darauf ankommen lassen, vielleicht geht es schief, na gut. Den großen konzeptionellen Wurf werden Sie mit diesem Gesetz so oder so nicht geschafft bekommen, weil es dafür einer grundlegenderen Überarbeitung auch von vielen anderen Vorschriften bedürfte. Wenn Sie zum Beispiel die Löffelmannsche-Ampellösung einführen würden, die ich übrigens für durchaus etwas halte, worüber man nachdenken kann, dann

müssten Sie die Regelungen in der Strafprozessordnung zum Ermittlungsverfahren und entsprechende Regelungskomplexe im BKA-Gesetz oder in den Landespolizeigesetzen, die müssten Sie alle komplett aufbohren. Sie müssten also diese Ampel festlegen, dann müssten Sie die unterschiedlichen Datenerhebungs- und Datenverarbeitungsmechanismen unterschiedlichen Ampelfarben zuordnen und dann würde das vielleicht funktionieren. Das lässt sich aber nicht mit so einer Stückwerkregelung machen, wie die, über die wir heute reden, sondern da wäre es sicherlich sinnvoll, mal eine Kommission dranzusetzen, die auch ein bisschen Zeit bekommt und das mal sinnvoll ausarbeitet.

Was die unionsrechtliche Frage angeht würde ich Herrn Löffelmann insofern zustimmen, als der Unionsrechtsverstoß, der in der Neuregelung liegt, sich auf die Neuregelung, über die Sie hier beraten, eigentlich gar nicht auswirkt. Die Bestandsdatenauskunft als solche bleibt stehen. Was kippt, ist die Vorratsdatenspeicherung. Weil die Vorratsdatenspeicherung dann unverhältnismäßig bleibt, was sie im Moment ist und was sie dann eben auch weiterhin ist, weil Ihr Gesetz die Mängel der Vorratsdatenspeicherung nicht behebt. Das wäre die Konsequenz. Nun wird die Vorratsdatenspeicherung ja im Moment ohnehin weitgehend nicht vollzogen. Ich denke, dass auch allen klar ist, dass die Regelungen über die Vorratsdatenspeicherung, so wie sie im Moment stehen, so oder so nicht stehenbleiben können, sondern der Überarbeitung bedürfen aufgrund des Unionsrechts. Hier würde der Überarbeitungsbedarf ausgebaut. Ich persönlich bin mandatiert in einem Rechtsstreit eines Telekommunikationsunternehmens, der sich gegen die Vorratsdatenspeicherung richtet. Wenn Sie die Regelung so in Kraft setzen wie sie im Gesetz drinsteht, gewinne ich meinen Rechtsstreit, wenn Sie die Regelung nachbessern, verliere ich meinen Rechtsstreit. Von daher, aus rein persönlichen Motiven, würde ich sagen: Lassen Sie es so, wie es ist. Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank auch noch mal Herr Professor Bäcker. Ich danke allen Sachverständigen ganz herzlich für die Zeit, die Sie sich jetzt noch genommen haben in der Verlängerung. Ich glaube, wir haben vielleicht auch noch mal einige wichtige Anstöße bekommen, um vielleicht noch über ein, zwei Änderungen konkret nachzudenken und sie umzusetzen. Und ich glaube, dass wir noch eine Langfriststrategie brauchen, das hat sich heute auch noch mal herausgestellt, weil, Herr Münch, eigentlich sollte es schon so sein, dass der Blick ins Gesetz die Rechtsfindung erleichtert. Wenn wir dem gar nicht mehr gerecht werden, sollten wir es in der nächsten Legislaturperiode noch mal anpacken. Vielen Dank und eine gute Woche noch.

Schluss der Sitzung: 12:12 Uhr

Andrea Lindholz, MdB
Vorsitzende

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)696 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 der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020

(BT-Drs. 19/25294)

2

Gliederung

3

Ergebnisse

1. Die vorgesehenen Regelungen zur Übermittlung von und zum sicherheitsbehördlichen Zugriff auf Telemediendaten verfehlen teilweise die verfassungsrechtlichen Anforderungen.

    a) Die Erlaubnisse zur Übermittlung von Telemedien-Bestandsdaten in § 15a Abs. 1 Satz 1, Abs. 3 TMG-E tragen der spezifischen Sensibilität dieser Datenkategorie, die sie von Telekommunikations-Bestandsdaten abhebt, nicht hinreichend Rechnung. Unverhältnismäßig sind zumindest die Erlaubnisse, Telemedien-Bestandsdaten zur Abwehr einfacher Gefahren für die öffentliche Sicherheit und zur Verfolgung beliebiger Straftaten und Ordnungswidrigkeiten zu übermitteln. Ebenso unverhältnismäßig sind zumindest die korrespondierenden Zugriffsermächtigungen in § 22a Abs. 1 Satz 1 Nr. 2 BPolG-E, § 10 Abs. 1 Satz 1 und § 30 Abs. 1 Satz 1 ZFdG-E sowie § 100j Abs. 1 Satz 1 Nr. 2 StPO-E i.V.m. § 46 Abs. 1 OWiG.

    b) Erst recht unverhältnismäßig sind § 15a Abs. 1 Satz 1, Abs. 3 TMG-E, soweit diese Regelungen auch die Übermittlung von Telemedien-Nutzungsdaten zulassen, die intensiver in Grundrechte eingreift als die Übermittlung von Telemedien-Bestandsdaten. Ungeachtet ihrer etwas strengeren Fassung bestehen auch gegen die vorgesehene strafprozessuale Zugriffsermächtigung in § 100g Abs. 1 Satz 2 StPO-E verfassungsrechtliche Bedenken, da sie der potenziell hohen Sensibilität dieser Datenkategorie nicht vollumfänglich Rechnung trägt.

2. In dem Entwurf fehlen Ermächtigungen zur Inhaltsüberwachung von Telemedien. Solche Ermächtigungen sind nicht etwa deshalb entbehrlich, weil Überwachungen auf die Ermächtigungen der Sicherheitsbehörden zu Telekommunikationsüberwachungen (etwa in § 100a StPO) gestützt werden könnten. Die Übermittlung von und der Zugriff auf Telemedieninhalte und Telemedien-Nutzungsdaten sollten stattdessen einheitlich geregelt werden, um fruchtlose Abgrenzungsschwierigkeiten zwischen beiden Datenkategorien zu vermeiden. Wegen der hohen Sensibilität sowohl von Nutzungsdaten als auch von Inhalten sollten diese Eingriffe an die für Telekommunikationsüberwachungen geltenden Voraussetzungen gebunden werden.

3. Die in § 113 Abs. 1 Satz 3, Abs. 3 und Abs. 5 TKG-E enthaltenen Erlaubnisse zur Übermittlung von Bestandsdaten, die durch die Zuordnung einer dynamischen IP-Adresse ermittelt wurden, verletzen unionsrechtliche Vorgaben, soweit für die Zuordnung Vorratsdaten (§§ 113a ff. TKG) verarbeitet werden dürfen.

4 Der Gesetzentwurf behebt im Wesentlichen die Mängel des geltenden Telekommunikationsrechts und des Fachrechts der Sicherheitsbehörden, die das Bundesverfassungsgericht in seinem zweiten Bestandsdatenbeschluss vom 27. Mai 2020 (Az. 1 BvR 1873/13) aufgezeigt hat.

Gleichwohl stehen einige der vorgesehenen Regelungen mit höherrangigem Recht nicht in Einklang. Hierfür gibt es zwei Gründe: Erstens trägt der Gesetzentwurf der spezifischen Sensibilität von Telemediendaten nur unzureichend Rechnung (unten I). Zweitens entspricht die gesetzliche Erlaubnis zur Auflösung dynamischer IP-Adressen unter Verwendung bevorrateter Telekommunikations-Verkehrsdaten zwar den verfassungsrechtlichen Maßstäben des zweiten Bestandsdatenbeschlusses. Sie verfehlt jedoch die strengeren unionsrechtlichen Anforderungen, die der Gerichtshof der Europäischen Union in seinem dritten Vorratsdatenurteil vom 6. Oktober 2020 (Rs. C-511/18, C-512/18 und C-520 – La Quadrature du Net u.a.) herausgearbeitet hat.

I. Übermittlung von und Zugriff auf Telemediendaten[1]

Im Anschluss an das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität enthält der Entwurf Regelungen zur Übermittlung von Kundendaten durch die Anbieter von Telemediendiensten an Sicherheitsbehörden sowie zum behördlichen Zugriff auf diese Daten.[2] Diese Regelungen knüpfen überwiegend an die Regelungen zur Übermittlung von und zum Zugriff auf Telekommunikationsdaten an. Dieser Regelungsansatz wird jedoch der spezifischen Sensibilität von Telemediendaten nicht gerecht.

1. Vorklärungen

Um die verfassungsrechtlichen Mängel der vorgesehenen Übermittlungserlaubnisse und Zugriffsermächtigungen herauszuarbeiten, muss vorab geklärt werden, wie sich Telemedien- und Telekommunikationsdienste voneinander abgrenzen, welche Datenkategorien es für beide Diensttypen gibt und als wie sensibel Telemediendaten im Vergleich zu Telekommunikationsdaten anzusehen sind.

a) Differenzierung und Abgrenzung von Telemedien und Telekommunikation

Den Regelungen des Entwurfs liegt die in § 1 Abs. 1 Satz 1 TMG i.V.m. § 3 Nr. 24 TKG geregelte Differenzierung zwischen Telemedien- und Telekommunikationsdiensten zugrunde. Weil es sich um rechtlich getrennte Arten von Kommunikationsdiensten handelt, werden auch die Übermittlung der bei den Diensteanbietern anfallenden Daten an Sicherheitsbehörden sowie der behördliche Zugriff auf diese Daten ausdrücklich voneinander unterschieden.

---

[1] Die folgenden Ausführungen beruhen teilweise auf meiner Stellungnahme zu dem Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vom 4. Mai 2020. Ich habe sie jedoch an die zwischenzeitliche Entwicklung angepasst und meine früheren Positionen teils revidiert.

[2] Das sog. Doppeltürmodell, das diesem Regelungsansatz zugrunde liegt, wird im Folgenden als bekannt vorausgesetzt.

5 Die Differenzierung zwischen beiden Dienstetypen hat eine Wurzel im Unionsrecht, da der Begriff des Telekommunikationsdienstes auf Art. 2 lit. c der früheren Rahmenrichtlinie für die elektronische Kommunikation[3] beruht. Der Gerichtshof der Europäischen Union hat diese Norm eng ausgelegt, sodass viele verbreitete internetbasierte Kommunikationsdienste nicht unter den unionsrechtlichen Begriff des elektronischen Kommunikationsdienstes fallen, da sie nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen. Konkret entschieden hat der Gerichtshof dies für E-Mail-Dienste.[4] Ebenso dürften zahlreiche weitere sogenannte Over-the-Top-Dienste zu behandeln sein, etwa Messengerdienste wie WhatsApp oder Soziale Medien wie Facebook (letztere auch insoweit, als sie Funktionen für den Nachrichtenaustausch zwischen Individuen enthalten). Solche Kommunikationsdienste sind dementsprechend nach gegenwärtigem Recht als Telemediendienste einzustufen.

Die Übermittlungserlaubnisse für Diensteanbieter, die das Telekommunikationsrecht enthält, können nicht auf Telemedienanbieter angewandt werden. Zudem beschränkt sich der Anwendungsbereich einiger Überwachungsermächtigungen im geltenden Sicherheitsrecht auf Datenerhebungen mit Bezug zur Telekommunikation im telekommunikationsrechtlichen Sinne. Es bedarf daher für telemedienbezogene Überwachungsmaßnahmen spezifischer Rechtsgrundlagen für die Übermittlung von Telemediendaten an Sicherheitsbehörden und den behördlichen Zugriff auf solche Daten. Der Entwurf soll solche Regelungen schaffen und dabei einen prinzipiellen Gleichlauf zwischen telekommunikations- und telemedienbezogenen Überwachungsmaßnahmen herstellen.

Die Begrifflichkeiten werden sich voraussichtlich in naher Zukunft verschieben. Der die frühere Rahmenrichtlinie ablösende Kommunikationskodex[5] hat den Anwendungsbereich des europäischen Telekommunikationsrechts neu gefasst. Gemäß Art. 2 Nr. 4 Kommunikationskodex umfasst der zentrale Begriff des elektronischen Kommunikationsdienstes nunmehr unter anderem interpersonelle Kommunikationsdienste, die über elektronische Kommunikationsnetze erbracht werden. Es kommt nicht mehr darauf an, ob solche Dienste ganz oder überwiegend in der Übertragung von Signalen bestehen. Dementsprechend sieht der aktuelle Entwurf eines Telekommunikationsmodernisierungsgesetzes[6] in § 3 Nr. 61 TKG-E eine entsprechende Erweiterung des deutschen Begriffs des Telekommunikationsdienstes vor. Sollte dieser Entwurf in Kraft treten,

---

[3] Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), ABl. L 108 vom 24. April 2002, S. 33, zuletzt geändert durch die Richtlinie 2009/140/EG vom 25. November 2009, ABl. L 337 vom 18. Dezember 2009, S. 37.

[4] EuGH, Urteil vom 13. Juni 2019, Rs. C-193/18 – Google LLC gegen Bundesrepublik Deutschland.

[5] Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation, ABl. L 321 vom 17. Dezember 2018, S. 36.

[6] Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts (Telekommunikationsmodernisierungsgesetz), BR-Drs. 29/21.

6 so wird sich der Begriff des Telekommunikationsdienstes erweitern und der Begriff des Telemediendienstes entsprechend verengen.[7] Dementsprechend werden zukünftig die Übermittlung von und der behördliche Zugriff auf Daten aus interpersonellen Over-the-Top-Kommunikationsdiensten auf die Regelungen zu stützen sein, die sich auf Telekommunikationsdaten beziehen. Die praktische Relevanz der im vorliegenden Entwurf vorgesehenen Regelungen zu Telemediendaten wird sich damit deutlich vermindern.

Der voraussichtlich in Zukunft maßgebliche Begriff des interpersonellen Kommunikationsdienstes wird in § 3 Nr. 24 TKG-E legaldefiniert als

> „ein gewöhnlich gegen Entgelt erbrachter Dienst, der einen direkten interpersonellen und interaktiven Informationsaustausch über Telekommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Telekommunikation veranlassen oder daran beteiligt sind; dazu zählen keine Dienste, die eine interpersonelle und interaktive Telekommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen."

Diese Legaldefinition birgt nicht unbeträchtliche Interpretations- und Abgrenzungsprobleme, was angesichts der nahezu unüberschaubaren Vielfalt netzbasierter Kommunikationsdienste nicht überrascht. Klar als interpersonelle Kommunikationsdienste sind etwa E-Mail- oder auf den Austausch zwischen Einzelpersonen beschränkte Messengerdienste einzustufen. Öffentlich einsehbare Profile auf Sozialen Netzwerken unterfallen dem Begriff hingegen nicht. Abgrenzungsschwierigkeiten dürften zum einen bei Kommunikationsdiensten entstehen, die hinsichtlich der Adressaten von Nachrichten Konfigurationsmöglichkeiten eröffnen. So liegt es etwa, wenn ein Messengerdienst ermöglicht, Nachrichten über einen abonnierbaren Nachrichtenkanal an eine große oder sogar zahlenmäßig unbegrenzte Gruppe von Empfängern zu versenden, oder wenn ein Soziales Netzwerk ermöglicht, den Empfängerkreis von Veröffentlichungen auf einen abgegrenzten Personenkreis zu beschränken. Zum anderen stellt sich die Frage, wann genau eine interpersonelle Kommunikationsmöglichkeit als untrennbare und untergeordnete Nebenfunktion eines anderen Dienstes anzusehen ist. Diese Frage könnte etwa für Chatfunktionen von Online-Versandhändlern oder für Kommunikationskanäle von Online-Spielen relevant werden.[8]

b) Kategorien und Sensibilität von Telemediendaten[9]

Der Entwurf verfolgt den Regulierungsansatz, Telekommunikations- und Telemediendienste hinsichtlich der Übermittlung von Kommunikationsdaten an Sicherheitsbehörden und des behördlichen Zugriffs auf solche Daten weitgehend gleichzubehandeln. Eine solche Parallelisierung beider Dienstetypen fand sich schon bislang (zumindest teilweise) in einigen Fachgesetzen der

---

[7] Kiparski, CR 2019, S. 179 (180).
[8] Vgl. Erwägungsgrund 17 zum Kommunikationskodex
[9] Außer Betracht bleiben im Folgenden Zugangsdaten, die nach dem Entwurf bei Telemediendiensten einem höheren Schutzniveau unterliegen sollen als bei Telekommunikationsdiensten. Hiergegen bestehen meines Erachtens keine verfassungsrechtlichen Bedenken.

7 Sicherheitsbehörden.[10] Ihre Überzeugungskraft hängt allerdings maßgeblich davon ab, inwieweit sich für Telekommunikations- und Telemediendienste vergleichbare Datenkategorien bilden lassen, hinsichtlich derer einem behördlichen Zugriff eine vergleichbare Eingriffsintensität zukommt.

Das Telekommunikations- und das Telemedienrecht kennen gleichermaßen die Datenkategorie der Bestandsdaten.[11] Hierbei handelt es sich jeweils um Daten, die für „die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses“ zwischen dem Diensteanbieter und dem Nutzer benötigt werden. Bestandsdaten sind mithin Basisdaten eines Nutzungsvertrags, die sich nicht auf einen konkreten Kommunikationsvorgang beziehen. Beispiele bilden Name, Anschrift oder Bankverbindung des Nutzers. Die Sensibilität von Telekommunikations-Bestandsdaten und Telemedien-Bestandsdaten erscheint auf den ersten Blick ohne weiteres vergleichbar.[12] Bei näherer Betrachtung erweist sich diese Bewertung jedoch als fragwürdig.

Telekommunikations-Bestandsdaten sind für sich genommen wenig sensibel. Insbesondere ist die Information, dass eine bestimmte Person von einem bestimmten Telekommunikationsdienst Gebrauch macht, bei isolierter Betrachtung weitgehend banal. Denn Telekommunikationsdienste werden von nahezu jedermann genutzt. Zudem sind die Angebote unterschiedlicher Diensteanbieter funktional weitgehend austauschbar. Die Nutzung eines bestimmten Dienstes eines bestimmten Anbieters sagt darum über sensible Umstände wie persönliche Eigenschaften oder Vorlieben der Nutzerin sowie über die möglichen Kommunikationsinhalte kaum etwas aus.[13] Eine gesteigerte Sensibilität erlangen Telekommunikations-Bestandsdaten erst im Zusammenwirken mit anderen Informationen, etwa indem die Telefonnummer, von der ein inkriminierender Anruf ausging, dem Anschlussinhaber zugeordnet wird.

Hingegen umfasst der Begriff des Telemediendienstes nicht nur weit verbreitete und inhaltlich neutrale Kommunikationsdienste, sondern auch zahlreiche Dienste, bei denen schon der Umstand der Nutzung Schlussfolgerungen von hoher Sensibilität ermöglicht. Beispielhaft sei die Nutzung eines webbasierten Forums oder einer Gruppe auf einem Sozialen Netzwerk genannt, in denen sich Betroffene über bestimmte Krankheiten austauschen. Zudem können sich Telemedien-Bestandsdaten auf mehr und persönlichkeitsrelevantere Informationen erstrecken als Telekommunikations-Bestandsdaten, etwa wenn ein Telemediendienst darauf beruht, den Nutzern personalisierte Angebote aufgrund eines zu Beginn des Vertragsverhältnisses erstellten Interessenprofils zu unterbreiten. Hierbei handelt es sich auch nicht nur um vernachlässigbare Sonderfälle, sondern eine durchaus beträchtliche Teilmenge aller Telemedien, vor allem wenn

---

[10] Vgl. beispielhaft für den Zugriff auf Telekommunikations-Verkehrsdaten und Telemedien-Nutzungsdaten § 52 BKAG. Hingegen enthält das BKAG bislang keine ausdrückliche Ermächtigung zur Erhebung von Telemedien-Bestandsdaten.

[11] § 3 Nr. 3 TKG (§ 3 Nr. 6 TKG-E); § 14 Abs. 1 TMG.

[12] So noch meine Stellungnahme zu dem Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vom 4. Mai 2020.

[13] Dies gilt auch noch, wenn nach zukünftigem Recht die Nutzung interpersoneller Over-the-Top-Dienste wie E-Mail oder Instant Messaging einbezogen wird, da es sich hierbei zumindest in der Regel gleichfalls um weit verbreitete, inhaltlich neutrale und untereinander substituierbare Dienste handelt.

8 zukünftig die der Individualkommunikation dienenden Over-the-Top-Dienste als Telekommunikationsdienste eingestuft werden. Derartige Telemedien von erhöhter Persönlichkeitsrelevanz müssen bei einer typisierenden Einschätzung der Sensibilität von Telemedien-Bestandsdaten berücksichtigt werden. Auch wenn es für Telemedien-Bestandsdaten anders als für Telekommunikations-Bestandsdaten[14] keine gesetzliche Bevorratungspflicht gibt,[15] weisen daher die Übermittlung von und der Zugriff auf Telemedien-Bestandsdaten bei abstrakt-genereller Betrachtung eine im Vergleich zu Telekommunikations-Bestandsdaten erhöhte Eingriffsintensität auf.[16]

Im Telekommunikationsrecht werden des Weiteren zwei Kategorien von Daten unterschieden, die sich jeweils auf konkrete Kommunikationsvorgänge beziehen. Dabei handelt es sich zum einen um die Kommunikationsinhalte, zum anderen um die Verkehrsdaten, also Metadaten der Kommunikation, die „bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden."[17] Aus Verkehrsdaten ergibt sich beispielsweise die Information, zwischen welchen Rufnummern zu welcher Zeit ein Telefongespräch geführt wurde. Das geltende Sicherheitsrecht enthält uneinheitliche Wertungen dazu, inwieweit sich die Sensibilität beider Datenkategorien vergleichen lässt. Teilweise werden Zugriffe auf Telekommunikations-Verkehrsdaten und Inhaltsüberwachungen der Telekommunikation an dieselbe Eingriffsschwelle gebunden (so etwa § 51 Abs. 1 und § 52 Abs. 1 BKAG). Teilweise wird hingegen der Zugriff auf Telekommunikations-Verkehrsdaten wegen deren – vermeintlich – geringerer Sensibilität unter weniger strengen Voraussetzungen ermöglicht als Inhaltsüberwachungen der Telekommunikation (etwa in § 100a Abs. 1 und § 100g Abs. 1 StPO).

Schwieriger und kontroverser ist die Kategorisierung von Telemediendaten. Das Telemedienrecht nennt ausdrücklich neben den Bestandsdaten nur die Nutzungsdaten als weitere Datenkategorie. Hierbei handelt es sich gemäß § 15 Abs. 1 TMG um Daten, die erforderlich sind, „um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen". Beispielhaft nennt das Gesetz Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie den Umfang der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien. Die Telemedien-Nutzungsdaten entsprechen damit – zumindest auf den ersten Blick – den Telekommunikations-Verkehrsdaten. Hiervon geht auch der Entwurf erkennbar aus.

Hingegen findet sich im Telemedienrecht keine Datenkategorie, die den Inhalten der Telekommunikation entspräche. Dabei ist offenkundig, dass es auch Telemedieninhalte gibt, die sich kaum als Metadaten der Telemediennutzung begreifen lassen. Bestellt beispielsweise jemand Waren bei einem Online-Versandhändler, so sind die im Rahmen der Bestellung anfallenden technischen Metadaten (beispielsweise die IP-Adresse, unter der die Bestellung aufgegeben

---

[14] Vgl. § 111 TKG.
[15] Vgl. zu diesem Gesichtspunkt und seiner Bedeutung für die Eingriffsintensität von Datenübermittlung und Datenzugriff BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 –, Rn. 139.
[16] Anders wegen des Fehlens einer Bevorratungspflicht noch mein im Auftrag der Bundestagsfraktion Bündnis 90/Die Grünen erstelltes Rechtsgutachtem vom 16. September 2020.
[17] § 3 Nr. 30 TKG (ähnlich § 3 Nr. 70 TKG-E).

9 wird, oder die Uhrzeit der Bestellung) Nutzungsdaten. Die Angabe, welche Waren der Nutzer bestellt hat, ist hingegen kein auf das Telemedium (die Website des Versandhändlers) bezogenes Nutzungsdatum, sondern ein mithilfe des Telemediums transportiertes Datum, das sich auf den abgeschlossenen Kaufvertrag bezieht. Bei den der Individualkommunikation dienenden Over-the-Top-Diensten wie E-Mail oder Instant Messaging erscheint es zumindest fragwürdig, ob sich die übermittelten Nachrichten als Nutzungsdaten einordnen lassen. Gleiches gilt etwa für Kommunikationsinhalte, die auf einer Profilseite bei einem Sozialen Netzwerk veröffentlicht werden.[18]

Ob Telemedien-Inhaltsdaten als eigenständige Datenkategorie anzuerkennen und wie sie zu behandeln sind, war lange umstritten. Teils wurde eine direkte oder analoge Anwendung der Vorschriften über Nutzungsdaten vertreten. Nach der Gegenauffassung sollte die Verarbeitung der Inhaltsdaten nach allgemeinem Datenschutzrecht zu beurteilen sein – mit der Konsequenz eines im Vergleich zu Nutzungsdaten schwächeren Schutzes. Der Streit wird heute vielfach für überwunden gehalten, da Telemediendaten spätestens seit Inkrafttreten des novellierten europäischen Rechtsrahmens generell dem allgemeinen Datenschutzrecht unterfielen und die Datenschutzregelungen des Telemedienrechts wegen des Anwendungsvorrangs der DSGVO unanwendbar seien.[19] Dies dürfte für Datenverarbeitungen durch den Telemedienanbieter zu eigenen Zwecken zutreffen, gilt jedoch nicht für die zweckändernde Übermittlung von Telemediendaten an eine Sicherheitsbehörde sowie für den sicherheitsbehördlichen Zugriff auf die Daten. Hinsichtlich dieser Datenverarbeitungen bestehen mitgliedstaatliche Regelungsspielräume.[20] Zur Ausfüllung dieser Spielräume könnte durchaus zwischen Nutzungs- und Inhaltsdaten differenziert werden.

Die Abgrenzung dieser Datenkategorien bereitet allerdings im Detail erheblich größere Schwierigkeiten als die Abgrenzung zwischen Telekommunikationsinhalten und Telekommunikations-Verkehrsdaten. Grund hierfür ist, dass der Telemedienbegriff sich auf eine viel größere Zahl unterschiedlicher Dienste mit unterschiedlichen Funktionen und Wirkungsweisen bezieht. Eine statische Webseite im World Wide Web, die lediglich zum Leseabruf zur Verfügung steht, ist ebenso ein Telemedium wie ein E-Mail-Dienst, ein Online-Versandhandel oder ein Onlinespiel. Zudem ist der Telemedienbegriff unterschiedlichen Abstraktionsstufen zugänglich und kann darum über- und untergeordnete Dienste gleichermaßen umfassen. Beispielsweise lässt sich ein Soziales Netzwerk in seiner Gesamtheit ebenso als Telemedium einstufen wie eine einzelne auf diesem Netzwerk betriebene Profilseite eines Unternehmens. Je nach Dienst können Nutzungs- und Inhaltsebene verschwimmen (so beim Abruf der statischen Webseite). Denkbar ist auch, dieselben Daten für einen Dienst als Nutzungs- und für einen anderen Dienst als Inhaltsdaten

[18] Für eine Subsumtion solcher Kommunikationsinhalte unter § 15 TMG etwa Schmitz, in: Spindler/ders., TMG, 2. Aufl. 2018, § 15 Rn. 83.
[19] Schmitz, in: Spindler/ders., TMG, 2. Aufl. 2018, § 15 Rn. 84; Tinnefeld/Buchner, in: BeckOK DatenschutzR, Stand 2019, Syst. I Rn. 91 ff.
[20] Für die Übermittlung aus Art. 6 Abs. 1 lit. c, Abs. 3 sowie aus Art. 6 Abs. 4 i.V.m. Art. 23 Abs. 1 lit. a, c oder d DSGVO; für den Datenzugriff – soweit er nicht dem Anwendungsbereich des europäischen Datenschutzrechts ohnehin vollständig entzogen ist – aus Art. 8 RL (EU) 2016/680.

einzustufen (so etwa, wenn ein Besucher eine Nachricht auf der Profilseite eines Sportartikelherstellers in einem Sozialen Netzwerk hinterlässt – möglicherweise Inhaltsdatum im Verhältnis zu dem Sportartikelhersteller, an den sich die Nachricht richtet, möglicherweise Nutzungsdatum im Verhältnis zu dem Netzwerkbetreiber, der die Kommunikationsinfrastruktur bereitstellt). 10

Zudem liegt nahe, dass Nutzungsdaten und Kommunikationsinhalte je nach Telemediendienst unterschiedlich sensibel sein können. Die Information, dass jemand einen bestimmten Dienst genutzt und bestimmte Inhalte erzeugt oder auf sie zugegriffen hat, kann aussagekräftiger und für die betroffene Person kritischer sein als die Inhalte selbst (beispielsweise bei der Nutzung eines webbasierten Diskussionsforums, bei dem die Inhalte, nicht aber die Nutzungsdaten öffentlich zugänglich sind). In anderen Fällen erscheinen die Inhalte zumindest tendenziell sensibler als die Nutzungsdaten (beispielsweise bei Over-the-Top-Diensten, die der Individualkommunikation dienen, wie E-Mail oder Instant Messaging, sofern hier zwischen Nutzungs- und Inhaltsdaten unterschieden wird).

2. Übermittlung von und Zugriff auf Bestandsdaten

Aufgrund dieser Überlegungen unterliegen die Erlaubnisse zur Übermittlung von Telemedien-Bestandsdaten in § 15a Abs. 1 Satz 1, Abs. 3 TMG-E und die zugehörigen Zugriffsermächtigungen teilweise verfassungsrechtlichen Zweifeln.

Die Übermittlungserlaubnisse in § 15a Abs. 3 TMG-E sind weitgehend identisch mit den Erlaubnissen zur Übermittlung von Telekommunikations-Bestandsdaten in § 113 Abs. 3 TKG-E, die sich ihrerseits an den in den Bestandsdatenbeschlüssen des Bundesverfassungsgerichts formulierten (Mindest-)Anforderungen orientieren. Diese Parallelführung trägt der erhöhten Sensibilität von Telemedien-Bestandsdaten und dem damit einhergehenden erhöhten Eingriffsgewicht der Datenübermittlung nicht Rechnung.

Das erhöhte Eingriffsgewicht der Übermittlung von Telemedien-Bestandsdaten muss sich in den Voraussetzungen der Datenübermittlung und des Datenzugriffs niederschlagen. Insbesondere müssen die Anforderungen an die hiermit verfolgten materiellen öffentlichen Interesse qualifiziert werden. Zwar ist in einer Übermittlung von Telemedien-Bestandsdaten an eine Sicherheitsbehörde und dem anschließenden Datenzugriff noch kein Grundrechtseingriff von hoher Intensität zu sehen, an den vergleichbare Anforderungen wie etwa an Inhaltsüberwachungen der Telekommunikation oder an die Übermittlung von Telekommunikations-Verkehrsdaten zu stellen wären. Gleichwohl wiegt nicht der gesamte Aufgabenkreis der Sicherheitsbehörden schwer genug, um diesen Grundrechtseingriff materiell zu legitimieren. Zu weit geht die vorgesehene Übermittlungserlaubnis zumindest insoweit, als sie die Datenübermittlung zur Verfolgung jeglicher Ordnungswidrigkeiten (§ 15a Abs. 3 Nr. 1 TMG-E) oder zur Abwehr sämtlicher Gefahren für die öffentliche Sicherheit (§ 15a Abs. 3 Nr. 2 lit. a, Nr. 4 lit. b aa TMG-E) zulässt.

Gleichfalls nicht in vollem Umfang tragfähig sind die in dem Entwurf enthaltenen Ermächtigungen zum Zugriff auf Telemedien-Bestandsdaten. Zu weit reichen zumindest die präventiv ausgerichteten Ermächtigungen in § 22a Abs. 1 Satz 1 Nr. 2 BPolG-E sowie § 10 Abs. 1 Satz 1 und § 30 Abs. 1 Satz 1 ZFdG-E, die Bestandsdatenabrufe zur Abwehr einer einfachen konkreten Gefahr für die öffentliche Sicherheit zulassen. Ebenfalls verfassungsrechtlich nicht tragfähig ist

11 die strafprozessuale Ermächtigung in § 100j Abs. 1 Satz 1 Nr. 2 StPO-E, soweit diese Norm im Zusammenwirken mit § 46 Abs. 1 OWiG den Zugriff auf Telemedien-Bestandsdaten generell zur Verfolgung von Ordnungswidrigkeiten erlaubt, sowie in

3. Übermittlung von und Zugriff auf Nutzungsdaten

Zu weit gefasst sind die Übermittlungserlaubnisse in § 15a Abs. 1 Satz 1, Abs. 3 TMG-E erst recht insoweit, als diese Vorschrift eine Übermittlung auch von Telemedien-Nutzungsdaten erlaubt. Daten dieser Kategorie sind zumindest in der Regel erheblich sensibler als Bestandsdaten. Eine Übermittlung kann darum nicht generell durch weit gefasste Zwecke wie beispielsweise die Verfolgung von (irgendwelchen) Straftaten oder gar Ordnungswidrigkeiten (§ 15a Abs. 3 Nr. 1 TMG-E) oder die Abwehr von Gefahren für die öffentliche Sicherheit und damit von beliebigen rechtswidrigen Handlungen (§ 15a Abs. 3 Nr. 2 lit. a, Nr. 4 lit. b aa TMG-E) legitimiert werden. Auch etwa Datenübermittlungen zu nachrichtendienstlichen Zwecken (§ 15a Abs. 3 Nr. 6-8 TMG-E) bedürfen angesichts der hohen Sensibilität von Nutzungsdaten und ungeachtet des generell hohen Gewichts der Schutzgüter des Nachrichtendienstrechts[21] eines materiell qualifizierten Erlaubnistatbestands.

Folgerichtig enthalten die bundesrechtlichen Fachgesetze der Sicherheitsbehörden, soweit sie den Zugriff auf Telemedien-Nutzungsdaten regeln, durchweg materiell qualifizierte Eingriffsvoraussetzungen.[22] Die weit gefassten Übermittlungserlaubnisse des Gesetzentwurfs stehen zu diesen Zugriffsermächtigungen in einem Wertungswiderspruch. Gleichfalls wertungswidersprüchlich ist, dass § 15a Abs. 4 TMG-E für eine Bestandsdatenübermittlung anhand einer dynamischen IP-Adresse – also eines Nutzungsdatums – höhere Anforderungen errichtet als für die Übermittlung des verwendeten Nutzungsdatums selbst. Die enger gefassten fachrechtlichen Zugriffsermächtigungen können die Mängel der zu weiten Übermittlungserlaubnisse jedenfalls insoweit nicht beheben, als diese auch Datenübermittlungen an Landessicherheitsbehörden zulassen. Soweit § 15a Abs. 1 Satz 1, Abs. 3 TMG-E die Übermittlung von Telemedien-Nutzungsdaten zulässt, ist die Norm daher zumindest teilweise verfassungswidrig.

Verfassungsrechtlich zweifelhaft ist darüber hinaus die vorgesehene strafprozessuale Ermächtigung zum Zugriff auf Nutzungsdaten in § 100g Abs. 1 Satz 2 StPO-E. Die geplante Regelung verweist hinsichtlich der Eingriffsschwelle auf die Ermächtigung zum Zugriff auf Telekommunikations-Verkehrsdaten in § 100g Abs. 1 Satz 1 StPO. Danach ist der Datenzugriff zulässig zur Verfolgung von Straftaten von erheblicher Bedeutung[23] sowie von Straftaten, die mittels Telekommunikation begangen wurden. Ob diese recht offen gefasste Ermächtigung der Sensibilität von Telekommunikations-Verkehrsdaten vollauf gerecht wird, ist durchaus fragwürdig, mag hier

---

[21] Vgl. BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 –, Rn. 151.

[22] Vgl. § 8a Abs. 2 Satz 1 Nr. 5 BVerfSchG (auch i.V.m. § 4a MADG und § 3 Abs. 1 Satz 2 BNDG); § 52 Abs. 1, Abs. 2 Satz 1 BKAG. Einen Sonderfall des Zugriffs auf Nutzungsdaten regelt § 10a Abs. 1 BKAG-E. Der materielle Zugriffstatbestand dieser Regelung ist zwar eher niedrig angesetzt, jedoch werden die zu erhebenden Daten und das Erkenntnisziel der Datenerhebung so eng zugeschnitten, dass die Norm insgesamt keinen verfassungsrechtlichen Bedenken unterliegt.

[23] Der Straftatenkatalog des § 100a Abs. 2 StPO wird lediglich beispielhaft in Bezug genommen.

12 aber dahinstehen.[24] Beim Zugriff auf Telemedien-Nutzungsdaten verschärfen sich die verfassungsrechtlichen Zweifel jedenfalls noch, da diese Datenkategorie schwierig abzugrenzen ist und ein extrem weites Spektrum von Datentypen umfasst, deren Aussagekraft über Telekommunikations-Verkehrsdaten noch deutlich hinausgehen kann.

4. Inhaltsüberwachung von Telemedien

Sowohl wegen der Interpretationsprobleme im Zusammenhang mit dem Begriff des Nutzungsdatums als auch aus Gründen der Rechtssicherheit ist es misslich, dass der Entwurf keine Regelungen über die Überwachung von Telemedieninhalten vorsieht. Dem liegt anscheinend die Erwägung zugrunde, solche Überwachungen könnten auf § 100a StPO und entsprechende Regelungen im präventiven Sicherheitsrecht gestützt werden, da der dort verwendete Begriff der Telekommunikation auch die Kommunikation mittels Telemedien umfasse.[25] Diese Erwägung überzeugt nicht. Jedenfalls ist es nicht ratsam, sich bei der Überarbeitung der sicherheitsrechtlichen Eingriffsermächtigungen an ihr zu orientieren.

Es trifft zu, dass der strafprozessuale Zugriff auf Inhalte von Telemedien– soweit sie nicht offen zugänglich sind und darum durch eine Überwachungsmaßnahme beschafft werden müssen – herkömmlich üblicherweise auf § 100a StPO gestützt wurde. Dies galt insbesondere für die Inhaltsüberwachung von Over-the-Top-Diensten, die (primär) der Individualkommunikation dienen.[26] Dem lag allerdings die in der strafprozessualen Praxis über lange Zeit nicht in Frage gestellte Auffassung zugrunde, solche Dienste seien als Telekommunikationsdienste einzustufen. Nach der neueren Rechtsprechung des Gerichtshofs der Europäischen Union ist dies jedoch gerade nicht der Fall, solange der europäische Kommunikationskodex nicht in deutsches Recht umgesetzt ist. In der strafgerichtlichen Rechtsprechung wird nunmehr eine Anwendung von § 100a StPO auf Over-the-Top-Dienste teils mit dem Argument begründet, der Erbringer eines Over-the-Top-Dienstes wirke am Signaltransport durch die Netzbetreiber und Zugangsdienstleister mit, weil er Datenpakete über das Internet versende und empfange.[27] Dieses Argument läuft darauf hinaus, die gesetzliche Unterscheidung von Telekommunikations- und Telemediendiensten schlicht zu ignorieren. Es überzeugt daher nicht. Nach der Rechtsprechung des Bundesgerichtshofs deckt sich hingegen der Telekommunikationsbegriff des § 100a StPO mit dem telekommunikationsrechtlichen Telekommunikationsbegriff.[28] Daher ist davon auszugehen,

---

[24] Diese Frage zu der – allerdings noch weiter gefassten – Vorgängerregelung in § 12 FAG a.F. offenlassend BVerfGE 107, 299 (315 f.), vgl. auch ebd., S. 322.

[25] Vgl. die Begründung zu dem Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, BT-Drs. 19/17741, S. 36.

[26] Vgl. beispielhaft zu der (im Beschluss nicht problematisierten) Überwachung eines E-Mail-Accounts auf der Grundlage von § 100a StPO BGH, Beschluss vom 11. August 2016 – StB 12/16; ferner BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 20. Dezember 2018 – 2 BvR 2377/16.

[27] So etwa LG Köln BeckRS 2020, 30090, Rn. 6 m.w.N.

[28] BGH, Urteil vom 14. März 2003 – 2 StR 341/02 –, NJW 2003, S. 2034; Beschluss vom 31. Januar 2007 – StB 18/06, NJW 2007, S. 930 (931 f.). In der juristischen Literatur wird hingegen vertreten, der Telekommunikationsbegriff des § 100a StPO sei nicht an dem technisch ansetzenden telekommunikationsrechtlichen Telekommunikationsbegriff, sondern an dem – teils engeren, teils weiterreichenden – Fernmeldegeheimnis des Art. 10 GG zu orientieren, vgl. zur Diskussion Graf, in: BeckOK StPO, § 100a Rn. 18 ff.; Günther, in: MüKo

13 dass das geltende Recht keine Ermächtigungen für sicherheitsbehördliche Inhaltsüberwachungen von Telemediendiensten enthält.

Hierdurch entsteht eine Schutzlücke, die auch durch die anstehende Erweiterung des Telekommunikationsbegriffs auf interpersonelle Kommunikationsdienste nicht vollständig entfallen dürfte. Denn auch danach dürfte es weiterhin Kommunikationsdienste geben, die eine nichtöffentliche Kommunikation ermöglichen, ohne dass sie als Telekommunikationsdienste einzustufen wären. An einer Inhaltsüberwachung solcher Dienste könnte durchaus ein sicherheitsbehördliches Interesse bestehen. Hinzu kommt, dass durch eine ausdrückliche Ermächtigung zum Zugriff auf Telemedieninhalte die schwierige, weitgehend aber auch fruchtlose Abgrenzung zwischen Inhalten und Nutzungsdaten vermieden werden könnte.

Es erscheint daher ratsam, in die Fachgesetze der Sicherheitsbehörden ausdrückliche Ermächtigungen aufzunehmen, die neben der Erhebung von Telemedien-Nutzungsdaten auch die Inhaltsüberwachung von Telemedien unter denselben Voraussetzungen zulassen. Die Eingriffsvoraussetzungen sollten sich an die Ermächtigungen zu Telekommunikationsüberwachungen anlehnen, um der hohen Sensibilität von Telemediendaten Rechnung zu tragen.

II. Zuordnung dynamischer IP-Adressen

Gleichfalls nicht in jeder Hinsicht mit höherrangigem Recht vereinbar sind die in § 113 Abs. 1 Satz 3, Abs. 3 und Abs. 5 TKG-E enthaltenen Erlaubnisse für die Anbieter von Telekommunikationsdiensten, dynamische IP-Adressen einem Anschlussinhaber zuzuordnen und die resultierenden Bestandsdaten zu übermitteln. Diese Regelungen entsprechen zwar den verfassungsrechtlichen Anforderungen, die das Bundesverfassungsgericht in seinem zweiten Bestandsdatenbeschluss errichtet hat.[29] Sie verstoßen jedoch partiell gegen die unionsrechtlichen Vorgaben, die entgegen der Einschätzung des Bundesverfassungsgerichts[30] teilweise strenger ausfallen.

Die Übermittlungserlaubnisse des § 113 TKG sind am Unionsrecht zu messen, da der deutsche Gesetzgeber mit ihnen von den in Art. 6 Abs. 1 lit. c, Abs. 3 und Abs. 4 i.V.m. Art. 23 DSGVO und/oder in Art. 15 der Datenschutzrichtlinie für die elektronische Kommunikation[31] enthaltenen

---

StPO, 2014, § 100a Rn. 26 ff. Da zugleich aufgrund ausdrücklicher Verweise auf das Telekommunikationsgesetz unstreitig ist, dass der Telekommunikationsbegriff in den Ermächtigungen zur Erhebung von Bestands- und Verkehrsdaten (§ 100g und § 100j StPO) dem telekommunikationsrechtlichen Telekommunikationsbegriff entspricht, hat diese Auffassung zur Folge, dass der Begriff der Telekommunikation in unterschiedlichen strafprozessualen Eingriffsermächtigungen unterschiedlich zu verstehen ist. Dies erscheint normsystematisch wenig überzeugend.

[29] BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 –, Rn. 175 ff.

[30] BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 –, Rn. 261.

[31] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31. Juli 2002, S. 37, zuletzt geändert durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den

14 Öffnungsklauseln für mitgliedstaatliches Recht Gebrauch gemacht hat.[32] Diese Öffnungsklauseln sind im Licht der Grundrechte auf Achtung des Privat- und Familienlebens aus Art. 7 GRCh sowie auf Datenschutz aus Art. 8 GRCh auszulegen.

Nach der Rechtsprechung des Gerichtshofs der Europäischen Union bewirken die Übermittlung von und der behördliche Zugriff auf Bestandsdaten zur Identifizierung von Anschlussinhabern grundsätzlich keinen schweren Eingriff in diese Grundrechte. Dieser Eingriff darf darum allgemein zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten zugelassen werden, ohne dass diese Straftaten als schwerwiegend einzustufen sein müssten.[33] Dies gilt auch dann noch, wenn das mitgliedstaatliche Recht eine Pflicht zur allgemeinen Bevorratung bestimmter Identifikationsdaten vorsieht.[34]

Die unionsrechtlichen Anforderungen verschärfen sich hingegen, wenn zur Zuordnung dynamischer IP-Adressen Verkehrsdaten genutzt werden dürfen, die für sicherheitsbehördliche Zwecke bevorratet wurden. Der Gerichtshof hat in seinem dritten Vorratsdatenurteil klargestellt, dass die Mitgliedstaaten zwar eine anlasslose und flächendeckende Bevorratung von IP-Zuordnungsdaten (im Gegensatz zu anderen Verkehrsdaten) anordnen dürfen. Um dem Eingriffsgewicht der Datenbevorratung Rechnung zu tragen, muss die Bevorratung jedoch materiell qualifizierten öffentlichen Interessen dienen. Hinreichend gewichtige Interessen sind der Schutz der nationalen Sicherheit, die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit.[35]

Nach diesen Maßstäben dürften die Übermittlungserlaubnisse in § 113 Abs. 1 Satz 3, Abs. 3 und Abs. 5 TKG-E den unionsrechtlichen Anforderungen zwar insoweit entsprechen, als sie eine Zuordnung von IP-Adressen mithilfe von Verkehrsdaten zulassen, welche die Telekommunikationsanbieter zu eigenen Zwecken gespeichert haben. Hingegen stehen sie mit diesen Anforderungen insoweit nicht in Einklang, als sie in Verbindung mit § 113c Abs. 1 Nr. 3 TKG eine Bestandsdatenauskunft auch unter Verwendung von bevorrateten IP-Adressen ermöglichen.[36] Denn die Datenübermittlung wird nicht auf die vom Gerichtshof der Europäischen Union genannten qualifizierten Ziele oder gleichrangige Belange beschränkt. Sie wird vielmehr unter anderem

---

Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, ABl. L 337 vom 18. Dezember 2009, S. 11.

[32] Ob und inwieweit die Übermittlung von Bestandsdaten jeweils der DSGVO oder der Richtlinie 2002/58/EG unterfällt, ist durchaus problematisch, vgl. die wenig klaren Ausführungen in EuGH, Urteil vom 2. Oktober 2018, Rs. C-207/16 – Ministerio Fiscal, Rn. 40 ff. Für die vorliegende Stellungnahme kommt es allerdings auf die Abgrenzung der beiden Regelungswerke nicht entscheidend an, da in jedem Fall § 113 TKG einer Öffnungsklausel des europäischen Datenschutzrechts unterfällt und unionsrechtlichen Anforderungen genügen muss.

[33] EuGH, Urteil vom 2. Oktober 2018, Rs. C-207/16 – Ministerio Fiscal, Rn. 53 ff.

[34] EuGH, Urteil vom 6. Oktober 2020, Rs. C-511/18, C-512/18 und C-520/18 – La Quadrature du Net u.a., Rn. 157 ff.

[35] EuGH, Urteil vom 6. Oktober 2020, Rs. C-511/18, C-512/18 und C-520/18 – La Quadrature du Net u.a., Rn. 152 ff.

[36] Die Bewertung der vorgesehenen Regelungen ist unabhängig davon, dass die Vorratsdatenspeicherung aktuell faktisch weitgehend ausgesetzt ist, da hier die Vereinbarkeit der Gesetzeslage und nicht der gegenwärtigen behördlichen Praxis mit höherrangigem Recht zu prüfen ist, vgl. zu den Grundrechten des Grundgesetzes BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 –, Rn. 171.

15 zugelassen zur Verfolgung sämtlicher – also nicht nur schwerer – Straftaten (§ 113 Abs. 5 Nr. 1 TKG-E) sowie zur Abwehr von Gefahren für Rechtsgüter von hervorgehobenem – also nicht zwangsläufig von erheblichem oder gar überragendem[37] – Gewicht (§ 113 Abs. 5 Nr. 2 TKG-E). Zumindest fragwürdig ist darüber hinaus etwa, ob der gesamte Aufgabenbereich der Nachrichtendienste (§ 113 Abs. 3 Nr. 5-7, Abs. 5 Satz 2 TKG) dem engen unionsrechtlichen Begriff der nationalen Sicherheit unterfällt, der sich auf „die Verhütung und Repression von Tätigkeiten, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, wie insbesondere terroristische Aktivitäten“ beschränkt.[38]

[37] Vgl. zur Begriffsbildung BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 –, Rn. 178, sowie zu den höheren Anforderungen an Rechtsgüter von „erheblichem“ bzw. „besonderem“ Gewicht die Gesetzesbegründung, BT-Drs. 19/25294, S. 51.
[38] EuGH, Urteil vom 6. Oktober 2020, Rs. C-511/18, C-512/18 und C-520/18 – La Quadrature du Net u.a., Rn. 135.

Hochschule des Bundes
für öffentliche Verwaltung

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)696 B

POSTANSCHRIFT HS BUND, POSTFACH 40527, 10063 BERLIN

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin

Prof. Dr. Markus Löffelmann
HAUSANSCHRIFT Habersaathstr. 51, 10115 Berlin
POSTANSCHRIFT Postfach 40527, 10063 Berlin
TEL 030 – 22 00 89 – 85513
E-MAIL markus.loeffelmann@hsbund-nd.de

DATUM Berlin, 20.01.2021

BETREFF **Schriftliche Stellungnahme zur öffentlichen Anhörung am 25. Januar 2021 zu BT-Drs. 19/25294**

Stellungnahme zum

Gesetzentwurf

der Fraktionen der CDU/CSU und SPD

Entwurf eines Gesetzes zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020

BT-Drs. 19/25294

I. Vorbemerkung

Der Gesetzentwurf dient der Umsetzung der Vorgaben des BVerfG in seinem Beschluss vom 27.5.2020, 1 BvR 1873/13, 1 BvR 2618/13. Bereits mit seiner Entscheidung vom 24.1.2012 (BVerfGE 130, 151 ff.) hatte das BVerfG die Vorschriften der §§ 112, 111 TKG für das automatisierte Auskunftsverfahren zu Telekommunikationsbestandsdaten für verfassungskonform erklärt und die Vorschriften in § 113 Abs. 1 S. 1, §§ 111, 95 Abs. 1 TKG für das manuelle Auskunftsverfahren bei verfassungskonformer Auslegung als mit dem Grundgesetz vereinbar angesehen. In dieser Entscheidung hatte es - entsprechend der damals schon herrschenden datenschutzrechtlichen Meinung - das so genannte „Doppeltürmodell“ entwickelt, welches besagt, dass für die Übermittlung personenbezogener Daten durch die speichernde Stelle und den Abruf dieser Daten durch die empfangende Stelle jeweils eigenständige und einander korrespondierende Ermächtigungsgrundlagen erforderlich sind. In Folge dieser verfassungsrechtlichen Weichenstellung hatten Bundes- und Landesgesetzgeber in zahlreichen Sicherheitsgesetzen die Abfragebefugnisse für das manuelle Verfahren neu gefasst. Mit der gegenständlichen Entscheidung hat das BVerfG für das manuelle Bestandsdatenauskunftsverfahren klargestellt, dass die „qualifizierten Voraussetzungen für eine Verwendung der Daten zum Zwecke der Strafverfolgung, der Gefahrenabwehr oder der Aufgabenerfüllung der

Nachrichtendienste (…) bereits vom Bund als Gesetzgeber der Übermittlungsregelung festzulegen“ (Rn. 134) sind, und es nicht ausreicht, entsprechende Schwellen lediglich bei den Abrufbefugnissen vorzusehen. Bildlich gesprochen müssen beide Türen gleich groß sein; die durch eine zu große „Übermittlungstür“ eröffnete unverhältnismäßige Durchlässigkeit kann nicht durch eine kleinere „Abfragetür“ kompensiert werden. In der Konsequenz sind die Entscheidungen des für die Schaffung der „Übermittlungstür“ zuständigen Gesetzgebers verfassungsrechtlich auch für den für die „Abfragetür“ zuständigen Gesetzgeber verbindlich.

II. Kritische Würdigung

Die folgende kritische Würdigung folgt aus Gründen der besseren Übersichtlichkeit und Darstellung nicht der Gliederung des Gesetzentwurfs, sondern orientiert sich an den jeweils für die einzelnen Bereiche des Sicherheitsrechts korrespondierenden Übermittlungs- und Abfragebefugnissen in der in § 15a TMG-E und § 113 TKG-E vorgesehenen Reihenfolge.

1. Verfolgung von Straftaten und Ordnungswidrigkeiten

a) Bestandsdaten

Die Übermittlungsbefugnisse für Telekommunikations- (§ 113 Abs. 3 Nr. 1 TKG-E) und Telemedien-Bestandsdaten (§ 15a Abs. 3 Nr. 1 i. V. m. § 14 Abs. 1 TMG-E) zum Zwecke der Strafverfolgung korrespondieren mit den entsprechenden Abrufbefugnissen der Strafverfolgungsbehörden (§ 100j Abs. 1 S. 1 Nr. 1 und 2 StPO-E). Das Anknüpfen der Regelungen an den strafprozessualen Anfangsverdacht (§ 152 Abs. 2 StPO) ist für eine Maßnahme von eher niedriger Eingriffsintensität sachgerecht. Eine Inkonsistenz besteht allerdings insoweit, als die beiden Übermittlungsbefugnisse auch die Auskunftserteilung zum Zwecke der Strafvollstreckung erlauben. § 100j StPO betrifft nicht diesen Verfahrensabschnitt, sondern ausschließlich das Ermittlungsverfahren. Die Vorschriften der StPO zur Strafvollstreckung (§§ 449 ff. StPO) beinhalten keine allgemeine Befugnis zum Abruf von Bestandsdaten, sondern verweisen nur hinsichtlich der Vollstreckung von Freiheitsstrafen und den Zweck der Festnahme des Verurteilten auf die Befugnisse der Ermittlungsbehörden (§ 457 Abs. 3 StPO). Eine Befugnis zur Abfrage von Bestandsdaten für die Staatsanwaltschaft als Vollstreckungsbehörde erscheint aber darüber hinaus mit Blick auf andere Maßnahmen der Strafvollstreckung (etwa Vollstreckung einer Geldstrafe, Durchsetzung von Maßnahmen der Führungsaufsicht oder Bewährungsüberwachung, Vollstreckung von Nebenfolgen) sinnvoll, um das Auffinden einer Person, die sich der Strafvollstreckung entzieht, zu erleichtern. Dass den Zollfahndungsämtern und dem Zollkriminalamt keine Abfragebefugnisse eröffnet werden, soweit diese Behörden im Bereich der Strafverfolgung auch die Aufgabe der Vorsorge für die künftige Verfolgung von Straftaten wahrnehmen, erscheint sachgerecht.

Verfassungsrechtliche Bedenken ergeben sich, soweit § 100j Abs. 2 StPO i. V. m. § 113 Abs. 1 S. 3, Abs. 5 Nr. 1 TKG-E unverändert auch die Auswertung von dynamischen IP-Adressen zum Zwecke der Beauskunftung zulässt und diese Befugnis sogar auf Telemedien-Bestandsdaten erstreckt, § 15a Abs. 1 S. 3 TMG-E. Da dynamische IP-Adressen, welche dabei verarbeitet werden, nach der Rechtsprechung des BVerfG dem Schutzbereich des Art. 10 GG unterfallen (vgl. BVerfGE 130, 151, 181 f. und zuvor bereits BVerfGE 125,

260, 312 f.), müsste verfassungsrechtlich eigentlich ein engeres materielles und prozessuales Anordnungsregime geboten sein, zumal mit der unterschiedslosen Ermächtigung zur Zuordnung statischer und dynamischer IP-Adressen die Voraussetzungen für eine flächendeckende Rückverfolgbarkeit von Internetkommunikation gegeben sind [näher zur Problematik und Kritik an der verfassungsrechtlichen Einordnung Löffelmann, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, Teil VI § 5 Rn. 7, 10]. Die in § 15a Abs. 4 Nr. 1 TMG-E und § 113 Abs. 5 Nr. 1 TKG-E vorgesehene Beschränkung auf den Zweck der Verfolgung von Straftaten (also nicht Ordnungswidrigkeiten) stellt keine substanzielle Einschränkung dar.

Dem Zitiergebot wird in Artikel 16 mit den Verweisungen auf Artikel 8 Nummer 3, Artikel 12 Nummer 3 und Artikel 13 Nummer 1 Rechnung getragen.

b) Zugangsdaten

Die Übermittlungsbefugnis für im Zusammenhang mit Telemedienangeboten gespeicherte Zugangsdaten zu Endgeräten und Speichereinrichtungen (§ 15b Abs. 2 Nr. 1 TMG-E) korrespondiert mit der Abfragebefugnis gem. § 100j Abs. 1 S. 3 StPO-E. Die materielle Schwelle der Verfolgung von Straftaten gem. § 100b Abs. 2 StPO und der damit zugleich in Bezug genommene Richtervorbehalt sind unter Verhältnismäßigkeitsgesichtspunkten nicht zu beanstanden. Fraglich ist freilich, ob die Übermittlungsbefugnis überhaupt einen relevanten praktischen Anwendungsbereich hat und damit zur Zweckerreichung geeignet ist. In Umsetzung der Vorgaben der DSGVO speichern die Anbieter Passwörter in aller Regel verschlüsselt (vgl. die Stellungnahme des Bundesverbands Informationswirtschaft, Telekommunikation und Neue Medien e. V. BitKom vom 01.12.2020, S. 2 zum gegenständlichen Gesetzentwurf; ferner bereits BT-Drs. 19/17741, S. 41) und verfügen deshalb lediglich über Hashwerte, die für die Sicherheitsbehörden ohne Nutzen sind.

Eine andere Schieflage besteht angesichts der hohen Schwelle für die Übermittlung von Zugangsdaten zum Fall der Auswertung von Endgeräten und Speichereinrichtungen ohne Rückgriff auf bei den Anbietern gespeicherte Zugangsdaten (etwa bei Auffinden der Zugangsdaten beim Berechtigten oder anderen Dritten, Entschlüsselung von Zugangsbeschränkungen u. ä.; vgl. bereits im Zusammenhang mit dem Kernbereichsschutz Löffelmann, GSZ 2019, 190, 193).

Hinsichtlich von Zugangsdaten, die im Zusammenhang mit Telekommunikationsdiensten gespeichert werden, enthalten außerdem die entsprechenden Vorschriften des TKG (§ 113 Abs. 1 S. 2, Abs. 4 TKG-E) keine entsprechende Einschränkung. Um den Vorgaben des BVerfG zu genügen, jedenfalls aber, um einen Gleichklang mit dem TMG herzustellen, sollte § 113 Abs. 1 S. 2 TKG entsprechend § 15b Abs. 2 Nr. 1 TMG-E eingeschränkt werden.

c) Nutzungsdaten

Da Telemediennutzungsdaten alle Informationen umfassen, die bei der Interaktion zwischen Nutzer und Anbieter während und durch die Nutzung eines Telemediums entstehen (näher Bär in: KMR, StPO, 87. EL September 2018, Vor §§ 100a-100j, Rn. 58) und damit Eigenschaften von Bestands-, Verkehrs- und auch Inhaltsdaten in sich vereinen, ist ihre Verwen-

dung verfassungsrechtlich nur unter engeren Voraussetzungen als bei Bestandsdaten zulässig. Die beabsichtigte Gleichsetzung von Nutzungsdaten und Verkehrsdaten in § 100g Abs. 1 S. 2 StPO-E erscheint unter Verhältnismäßigkeitsgesichtspunkten daher nicht unproblematisch, weil Nutzungsdaten gegenüber Verkehrsdaten in deutlich größerem Umfang Rückschlüsse auf Kommunikationsinhalte zulassen und deshalb den Inhaltsdaten phänomenologisch näher stehen. Die Überwachung von Inhaltsdaten ist nach verfassungsrechtlichen Maßstäben jedoch nur unter höheren Voraussetzungen zulässig (vgl. BVerfGE 115, 166, 183 ff.; 120, 274, 307 f.; 124, 43, 54). Vor diesem Hintergrund wäre es verfassungsrechtlich unbedenklicher, wenn die Erhebungsbefugnis nach § 100g Abs. 1 Satz 2 StPO-E lediglich solche Nutzungsdaten erfasste, die die Qualität von Verkehrsdaten besitzen. Einen in diese Richtung weisenden Weg ist der Gesetzgeber mit § 8a Abs. 2 Satz 1 Nr. 5 BVerfSchG gegangen, wobei auch hier die Daten unter Buchst. c) der Vorschrift („Angaben über die vom Nutzer in Anspruch genommenen Teledienste“) etwas zu umfassend bezeichnet werden (gemeint sein dürfte „die Bezeichnung der vom Nutzer in Anspruch genommenen Dienste“). Alternativ könnte der Zugriff auf Telemediennutzungsdaten generell auf das Niveau der inhaltsbezogenen Telekommunikationsüberwachung angehoben werden (so § 5 Abs. 2 Nr. 14 i. V. m. § 7c Abs. 2, § 7a Abs. 1 und 2 VSG NRW). Soweit der Gesetzgeber mit der Reform des Bundeskriminalamtgesetzes in § 52 Abs. 2 BKAG eine entsprechende Befugnis nur für den präventiven Bereich geschaffen und dabei pauschal auf § 15 Abs. 1 TMG verwiesen hat, ist auch dort die Abfrage von Verkehrs- und Nutzungsdaten nur unter denselben Voraussetzungen wie die inhaltsbezogene Telekommunikationsüberwachung nach § 51 BKAG zulässig (vgl. BT-Drs. 16/10121, S. 33).

Die höhere Hürde des § 100g Abs. 1 S. 2 StPO-E wird außerdem nicht in der Übermittlungsbefugnis des § 15a TMG-E gespiegelt, was - ungeachtet des Umstands, dass das BVerfG angedeutet hat, Beschränkungen, für die derselbe Gesetzgeber zuständig ist, könnten auch über mehrere Gesetze verteilt sein (BVerfG, B. v. 27.5.2020, 1 BvR 1873/13 u. a., Rn. 186) - nicht der Methodik des gegenständlichen Gesetzentwurfs entspricht. Außerdem erschließt sich nicht, weshalb § 100g Abs. 1 S. 2 StPO-E als Kreis der Verpflichteten diejenigen bezeichnet, „die geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln“ und § 15a Abs. 1 S. 1 TMG-E hiervon abweichend denjenigen verpflichtet, der „geschäftsmäßig Telemediendienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt“. Ob mit diesen verschiedenen Formulierungen inhaltliche Unterschiede gekennzeichnet werden, ist unklar.

2. Gefahrenabwehr

a) Bestandsdaten

Im Zusammenhang mit Maßnahmen der Gefahrenabwehr ist zwischen drei Fallgruppen der Verwendung von Bestandsdaten zu differenzieren: der Abwehr konkreter Gefahren, der Verwendung im Gefahrenvorfeld und der Verhütung von Straftaten.

aa) Abwehr konkreter Gefahren

Die Befugnisse zur Übermittlung und zum Abruf von Bestandsdaten zum Zwecke der Gefahrenabwehr sind in § 15a Abs. 3 Nr. 2 Buchst. a) TMG-E, § 113 Abs. 3 Nr. 2 Buchst. a) TKG-E (Übermittlung) und § 22a Abs. 1 S. 2 Nr. 1 BPolG-E, § 40 Abs. 1 Nr. 1, Abs. 2, § 63a Abs. 1 Nr. 1, Abs. 2, § 66a Abs. 1 Nr. 1, Abs. 2 BKAG-E, § 10 Abs. 1 S. 2 Nr. 2 Buchst. a), § 30 Abs. 1 S. 2 Nr. 1 Buchst. a), Abs. 2 S. 2 Nr. 1 Buchst. a) ZFdG (Abfrage) übereinstimmend und grundsätzlich sachgerecht an das Vorliegen einer konkreten Gefahr im polizeirechtlichen Sinne im Einzelfall geknüpft. Soweit die Abfrage die Verarbeitung dynamischer IP-Adressen voraussetzt, bestimmen § 15a Abs. 4 Nr. 2 TMG-E und § 113 Abs. 5 Nr. 2 TKG-E sowie § 22a Abs. 3 Nr. 1 BPolG-E, dass eine konkrete Gefahr für ein „Rechtsgut von hervorgehobenem Gewicht“ vorliegen muss. Welche Rechtsgüter zu diesem Kreis zählen, erschließt sich aus dem Gesetz nicht. Abweichend hiervon sieht § 40 Abs. 4 BKAG-E keine erhöhte Schwelle vor, was angesichts des Bezugs auf die Abwehr terroristischer Straftaten schlüssig erscheint. Am Rande ist darauf hinzuweisen, dass in diesem Punkt die Normänderungsbefehle (GE S. 13) und die Begründung (GE S. 45 zu Doppelbuchstabe cc) nicht übereinstimmen. Wiederum abweichend von § 40 Abs. 4 BKAG-E sehen § 63a Abs. 4 Nr. 1 und § 66a Abs. 4 Nr. 1 BKAG-E das Erfordernis der Gefahr der Begehung einer (beliebigen) Straftat vor. Das dürfte sich daraus erklären, dass das BVerfG zu den Rechtsgütern von hervorgehobenem Gewicht unter anderem diejenigen zählt, die durch Straftatbestände geschützt werden (vgl. BVerfG, B. v. 27.5.2020, 1 BvR 1873/13 u. a., Rn. 178). Angesichts des Umstands, dass Straftatbestände von Verfassung wegen überhaupt nicht dem Rechtsgüterschutz dienen müssen (vgl. BVerfGE 120, 274, 241 f. m. w. N.), erscheint das freilich nur eingeschränkt schlüssig. Im Sinne einer größeren Anwendungsfreundlichkeit sollten maßnahmenübergreifend zumindest dieselben Begrifflichkeiten verwendet werden.

Soweit für das Zollkriminalamt nach § 30 Abs. 1 S. 2 Nr. 1 Buchst. a) ZFdG-E und die Zollfahndungsämter nach § 30 Abs. 2 S. 2 Nr. 1 Buchst. a) ZFdG-E Abfragebefugnisse zum Zwecke der Gefahrenabwehr geschaffen werden, ist darauf hinzuweisen, dass die allgemeine Gefahrenabwehr außerhalb der Verhütung von Straftaten und Ordnungswidrigkeiten und der Mitwirkung bei der Bekämpfung der international organisierten Geldwäsche - auch nach dem Gesetz zur Neustrukturierung des ZFdG (vgl. BT-Drs. 19/12088) - nicht zum gesetzlichen Aufgabenbereich dieser Behörden zählt (vgl. §§ 4, 5 ZFdG-neu). Für die Aufgabe der Straftatenverhütung sehen § 30 Abs. 1 S. 2 Nr. 2 und § 30 Abs. 2 S. 2 Nr. 2 ZFdG-E eigene Regelungen vor. Es werden hier also außerhalb des gesetzlichen Aufgabenbereichs liegende Befugnisnormen geschaffen. § 30 Abs. 1 S. 2 Nr. 1 ZFdG-E ist deshalb durch einen engeren Verweis auf die Verwendung der Bestandsdaten zum Zweck der Mitwirkung bei der Bekämpfung der international organisierten Geldwäsche (§ 4 Abs. 4 ZFdG-neu) zu ersetzen, § 30 Abs. 2 S. 2 Nr. 1 ZFdG-E ist ganz zu streichen. Im Übrigen trägt der Umstand, dass die Übermittlungsbefugnisse nach § 15a Abs. 3 Nr. 4 TMG-E und § 113 Abs. 3 Nr. 4 TKG-E zwar explizit auf das Zollkriminalamt zugeschnitten sind, dieses jedoch nur in seiner Funktion als Zentralstelle nach § 3 ZFdG-neu erfassen, während für die anderen Funktionen des Zollkriminalamts und der Zollfahndungsämter die Übermittlungsbefugnisse nach § 15a Abs. 3 Nr. 1 und 2 TMG-E und § 113 Abs. 3 Nr. 1 und 2 TKG-E einschlägig sind, nicht zur Anwendungsfreundlichkeit der Regelungen bei.

bb) Gefahrenvorfeld

Zur Abwehr einer „drohenden Gefahr“ sehen § 15a Abs. 3 Nr. 2 Buchst. b) und c) TMG-E und § 113 Abs. 3 Nr. 2 Buchst. b) und c) TKG-E Übermittlungsbefugnisse und § 22a Abs. 1 S. 2 Nr. 2 und 3 BPolG-E, § 63a Abs. 1 Nr. 2 und 3, § 66a Abs. 1 Nr. 2 und 3 BKAG-E sowie § 30 Abs. 1 S. 2 Nr. 1 Buchst. b) und c), Abs. 2 S. 2 Nr. 1 Buchst. b) und c) ZFdG Abfragebefugnisse vor.

Der Begriff der „drohenden Gefahr“ wurde erstmals vom bayerischen Gesetzgeber im Zusammenhang mit der Novellierung des Bayerischen Polizeiaufgabengesetzes im Jahr 2017 als weitere polizeirechtliche Gefahrkategorie eingeführt (vgl. Art. 11 Abs. 3 S. 1 BayPAG). Der Begriff geht auf eine Formulierung des BVerfG in seiner Entscheidung zum BKAG zurück (BVerfGE 141, 220, 272 f.) und verleiht der dortigen prädikativen Verwendung von „drohend“ einen attributiven Sinn, der zu unsinnigen sprachlichen Doppelungen führt (vgl. bereits Löffelmann, BayVBl. 2018, 145, 148; Dietrich, in: Fischer/Hilgendorf, Gefahr, 2020, S. 69, 79 f.). Das wird auch in der gegenständlichen Gesetzbegründung deutlich, wo ausgeführt wird, Regelungsgegenstand seien Situationen, „in denen eine konkrete Gefahr nicht vorliegt, sondern der Eintritt der Gefahr erst in der Zukunft droht“ (GE S. 51, 54). Wenn der Eintritt der Gefahr erst in der Zukunft droht, droht er aktuell folglich noch nicht und es handelt sich entweder nicht um eine drohende Gefahr oder um eine in der Zukunft drohende drohende Gefahr. Weiter (a. a. O.) heißt es in der Begründung, § 15a Abs. 3 Nr. 2 Buchst. b TMG-E erfasse „die Sachverhaltskonstellation, dass bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr hinweisen.“ Danach handelt es sich also um den Fall, dass solche Tatsachen auf eine im Einzelfall drohende konkrete Gefahr hinweisen, nicht auf eine im Einzelfall drohende drohende Gefahr. Dieser Widerspruch zwischen Gesetztext und Begründung ließe sich einfach durch eine syntaktische Umstellung mit der Folge einer prädikativen Verwendung von „drohend“ beheben („eine für ein Rechtsgut von erheblichem Gewicht drohende Gefahr abzuwehren“) - dies allerdings um den Preis der „drohenden Gefahr“. Im Schrifttum ist der Begriff der drohenden Gefahr nicht zuletzt aufgrund seiner sprachlichen Widerspenstigkeit hoch umstritten (vgl. zuletzt - befürwortend - Möstl, BayVBl. 2020, 649 m. w. N. zum Meinungsstreit). Er ist außerdem Gegenstand einer verfassungsgerichtlichen Überprüfung im Zusammenhang mit den gegen die Novellierung des BayPAG angebrachten Verfassungsbeschwerden und einer abstrakten Normenkontrolle. Das mit der Verwendung des Begriffs verbundene Anliegen, den Polizeibehörden informationelle Befugnisse bereits im Gefahrenvorfeld zu gewähren, ist dabei zum Teil durchaus berechtigt. Obschon das BVerfG den Begriff im gegenständlichen Beschluss überraschend und in der Sache fraglich als „anerkannte Eingriffsschwelle“ bezeichnet hat (Rn. 152), erscheint es vor diesem Hintergrund vorzugswürdig, auf ihn zu verzichten. Der vom BVerfG synonym verwendete Begriff der „konkretisierten Gefahr“ (BVerfG, B. v. 27.5.2020, 1 BvR 1873/13 u.a., Rn. 148) ist ebenfalls nicht sonderlich aussagekräftig, denn eine konkretisierte Gefahr ist nach dem allgemeinen Sprachgebrauch eine solche, bei der der Prozess der Konkretisierung abgeschlossen ist, also eine konkrete Gefahr. Der hinter beiden Begriffen stehende Gedanke kann aber unproblematisch z. B. durch die Formulierung „um im Einzelfall im Gefahrenvorfeld eine aufgrund tatsächlicher Anhaltspunkte gegebene Bedrohungslage für ein Rechtsgut von erheblichem Gewicht aufzuklären“ ausgedrückt werden. Situationen im Gefahrenvorfeld, die zu polizeilichem Handeln berechtigen können, sind keine Gefahren, sondern Bedrohungslagen oder (in verwaltungsrechtlicher Terminologie) Risiken (vgl. Dietrich, a. a. O., S. 72) und sollten als solche be-

zeichnet werden, um Missverständnisse zu vermeiden. Da zwar die Schaffung informationeller, nicht aber aktioneller polizeilicher Befugnisse im Gefahrenvorfeld sachgerecht ist, sollte ferner in diesem Zusammenhang auf die Terminologie des Abwehrens verzichtet und stattdessen von „aufklären“ gesprochen werden.

Darüber hinaus erscheint die bloße Paraphrasierung amorpher verfassungsgerichtlicher Formulierungen im Gesetztext („ein seiner Art nach konkretisiertes Geschehen“, „das individuelle Verhalten einer Person“, „die konkrete Wahrscheinlichkeit“, „Rechtsgut von erheblichem Gewicht“, „besonders gewichtiges Rechtsgut“) anstelle ihrer inhaltlichen Ausfüllung durch den Gesetzgeber angreifbar (vgl. bereits Löffelmann, GSZ 2018, 85, 87 f.). In welchen Situationen des Gefahrenvorfelds Befugnisse eröffnet sind, ist dem Rechtsanwender kaum erkennbar. Namentlich erschließt sich aus dem Gesetz nicht, was ein „Rechtsgut von erheblichem Gewicht“ und was ein „besonders gewichtiges Rechtsgut“ ist. Anders als die Gesetzbegründung insinuiert (GE S. 51, 54), werden die Kreise dieser Rechtsgüter vom BVerfG weder abschließend definiert noch klar gegeneinander abgegrenzt, noch auch hat das Gericht klargestellt, dass es die Attribute „hochrangig“, „überragend wichtig“ und „besonders gewichtig“ synonym versteht (die Aufzählung in BVerfG, B. v. 27.5.2020, 1 BvR 1873/13 u. a., Rn. 150 lässt sich zwanglos im Sinne semantischer Alterität nicht Identität verstehen). Die in den Gesetztext übernommenen verfassungsgerichtlichen Formulierungen zeichnen sich vielmehr durch eine gewisse - vermutlich mit Blick auf die Eröffnung gesetzgeberischer Handlungsspielräume beabsichtigte - begriffliche Unschärfe und Beliebigkeit aus (vgl. zur Kritik bereits Löffelmann, GSZ 2020, 184, 185 f.). Vor diesem Hintergrund eine „verfassungsgerichtliche Vorprägung“ der Begriffe, die einen ausdrücklichen Rechtsgutkatalog entbehrlich mache (GE S. 51) anzunehmen, stellt eine starke Übertreibung dar und genügt nicht der verfassungsgerichtlichen Forderung, der Gesetzgeber müsse „entweder die Rechtsgüter von besonderem Gewicht selbst konkret benennen oder zumindest das erforderliche Gewicht normenklar festhalten“ (BVerfG, B. v. 27.5.2020, 1 BvR 1873/13 u. a., Rn. 180). Mit anderen Worten ist das Attribut „besonders“ nicht so präzise und besonders, dass dadurch das besondere Gewicht der Rechtsgüter normenklar charakterisiert würde. Die entsprechenden Regelungen des BKAG, die auf bestimmte Rechtsgüter verweisen, sind im Vergleich konkreter gefasst. In § 40 Abs. 1 Nr. 2 BKAG-E wird sogar - vorzugswürdig - vollständig auf den Begriff der drohenden Gefahr verzichtet. Artikelübergreifend sollte mit dem Gesetzentwurf wenigstens eine kohärente Sprachregelung betreffend das Gefahrenvorfeld hergestellt werden.

Soweit die Abfrage die Verarbeitung dynamischer IP-Adressen voraussetzt, bestimmen § 15a Abs. 4 Nr. 3 TMG-E und § 113 Abs. 5 Nr. 3 TKG-E, dass eine Gefahr für ein „besonders gewichtiges Rechtsgut“ vorliegen oder das Auskunftsverlangen die Verfolgung einer schweren Straftat nach § 100a Abs. 2 StPO zu Gegenstand haben muss. Welche Rechtsgüter zum Kreis der „besonders gewichtigen“ zählen, erschließt sich aus dem Gesetz nicht. Der Bezug auf Maßnahmen der Strafverfolgung ist im Zusammenhang mit der Gefahrenabwehr verfehlt. Abweichend hiervon sehen § 63a Abs. 4 Nr. 2 und § 66a Abs. 4 Nr. 2 BKAG-E das Erfordernis einer drohenden Gefahr für Leib, Leben oder Freiheit einer zu schützenden Person bzw. eine zu schützende Räumlichkeit vor und damit keine gegenüber dem Regelfall erhöhte Schwelle. Dasselbe gilt für Fälle nach § 40 Abs. 4 BKAG-E.

Schließlich ist auch hier darauf hinzuweisen, dass die Abwehr „drohender Gefahren“ nicht zum gesetzlichen Aufgabenbereich des Zollkriminalamts und der Zollfahndungsämter gehört.

cc) Straftatenverhütung

Zur Verhütung von Straftaten enthalten § 15a Abs. 3 Nr. 2 Buchst. d) und e) TMG-E und § 113 Abs. 3 Nr. 2 Buchst. d) und e) TKG-E Übermittlungsbefugnisse und § 30 Abs. 1 S. 2 Nr. 2 Buchst. a) und b), Abs. 2 S. 2 Nr. 2 Buchst. a) und b) ZFdG Abfragebefugnisse. Auch Straftatenverhütung ist Handeln im Gefahrenvorfeld (vgl. BVerfGE 110, 33, 56; 113, 348, 386), zu dessen Umschreibung der Gesetztext deshalb konsequent auf dieselben Merkmale wie für die Umschreibung der „drohenden Gefahr“ Bezug nimmt. Abweichend von den dortigen Fällen wird die Befugnis der Bestandsdatenverarbeitung zum Zwecke der Straftatenverhütung allerdings durch den Bezug auf Straftaten von erheblicher Bedeutung bzw. schwere Straftaten i. S. d. § 100a Abs. 2 StPO begrenzt. Die Regelungen zur „drohenden Gefahr“ und zur Straftatenverhütung harmonieren unter wertenden Gesichtspunkten nicht miteinander, denn die Qualifizierung einer Rechtsgutsverletzung als Straftat beinhaltet bereits ein erhöhtes öffentliches Interesse an staatlichem Tätigwerden, weil der Einsatz des Strafrechts als Steuerungsinstrument als ultima ratio staatlichen Handelns begriffen wird (vgl. etwa BVerfGE 96, 245, 249; 120, 224, 240; 123, 267, 408). Erachtet man die hier vorgesehenen Schwellen zur Verwendung von Bestandsdaten zum Zwecke der Straftatenverhütung als angemessen, dürfte das umgekehrt für die bei „drohenden Gefahren“ vorgesehenen Schwellen nicht gelten. Freilich ist die im Entwurf vorgenommene Gleichsetzung von „Rechtsgütern von erheblichem Gewicht“ und „Straftaten von erheblicher Bedeutung“ sowie von „besonders gewichtigen Rechtsgütern“ und „schweren Straftaten“ in den - insoweit wenig überzeugenden - Ausführungen des BVerfG angelegt (BVerfG, B. v. 27.5.2020, 1 BvR 1873/13 u. a., Rn. 150, 181 f.).

Für Abfragen unter Verarbeitung dynamischer IP-Adressen besteht zum Zwecke der Straftatenverhütung, wie sich im Umkehrschluss aus § 15a Abs. 4 Nr. 3 TMG-E und § 113 Abs. 5 Nr. 3 TKG-E ergibt, welche nur auf § 15a Abs. 3 Nr. 2 Buchst. b) und c) TMG-E bzw. § 113 Abs. 3 Nr. 2 Buchst. b) und c) TKG-E verweisen, keine Befugnis. Auch das harmoniert nicht mit der entsprechenden Befugnis in Fällen der „drohenden Gefahr“.

b) Zugangsdaten

Die Übermittlung von Zugangsdaten zu Zwecken der Gefahrenabwehr ist, soweit solche Daten bei Telemedienanbietern gespeichert sind, gem. § 15b Abs. 2 Nr. 2 TMG-E an die hohe Hürde des Vorliegens einer konkreten Gefahr für eines der abschließend genannten hochrangigen Rechtsgüter (Leib, Leben, Freiheit der Person, Bestand des Bundes oder eines Landes) geknüpft und von einer gerichtlichen Anordnung abhängig. Für Zugangsdaten, welche bei Telekommunikationsanbietern gespeichert sind, gilt diese Voraussetzung nicht, § 113 Abs. 4 TKG-E. Warum das so ist, erschließt sich nicht. Eine entsprechende unterschiedliche Behandlung der Zugangsdaten findet sich auch auf der Ebene der Abfragebefugnisse in § 22a Abs. 2 S. 1 und 2 BPolG-E, § 40 Abs. 3 S. 1 und 2, § 63a Abs. 3 S. 1 und 2, § 66a Abs. 3 S. 1 und 2 BKAG-E und § 30 Abs. 3 ZFdG-E (wobei auch hier wieder zu berücksichti-

gen ist, dass die Gefahrenabwehr außerhalb der Verhütung von Straftaten nicht zu den gesetzlichen Aufgaben des ZKA und der Zollfahndungsämter gehört). Nur für Fälle nach § 113 Abs. 1 S. 2, Abs. 4 TKG-E kann außerdem auf eine gerichtliche Anordnung verzichtet werden, wenn die betroffene Person vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder die Verarbeitung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird (§ 22a Abs. 2 S. 4 BPolG-E, § 40 Abs. 5 S. 4, 6, § 63a Abs. 3 S. 4, § 66a Abs. 3 S. 4 BKAG-E, § 30 Abs. 6 S. 4 ZFdG-E). Die Ausnahme des Kenntnis-haben-müssens erscheint rechtsstaatlich bedenklich, da hierdurch nicht näher konkretisierte Sorgfaltspflichten der betroffenen Person begründet werden und der Zugang zu Rechtsschutz für sie faktisch in die Hände der anordnenden Stelle gelegt wird. Diese Ausnahme sollte gestrichen werden. In den Fällen des § 40 Abs. 3 BKAG-E ist der Gehalt dieser Regelung aufgrund der Konstruktion mittels einer doppelten Gegenausnahme (Abs. 5 S. 4 und 6) im Übrigen nur mit Mühe nachzuvollziehen; die Norm sollte einfacher formuliert werden. Warum diese Privilegierung der § 113 TKG-Fälle geboten ist, ist anhand der Gesetzbegründung nicht nachzuvollziehen. Der Hinweis (GE S. 43) auf die bisherige Regelung in § 22a Abs. 3 S. 4 bis 6 BPolG geht fehl, da Vorschrift bisher eine Abfragebefugnis für TMG-Daten nicht enthält.

c) Nutzungsdaten

Eine Abfragebefugnis für Telemedien-Nutzungsdaten zu Zwecken der Gefahrenabwehr ist nicht vorgesehen, auch nicht zur Abwehr schwerster Rechtsgutverletzungen, was unter Wertungsaspekten fragwürdig ist. Umgekehrt enthält § 15a Abs. 1 S. 1 TMG-E jedoch eine entsprechende Übermittlungsbefugnis. Das dürfte nicht der verfassungsgerichtlichen Vorgabe eines Korrespondierens der beiden „Türen“ entsprechen.

3. Zentralstellenfunktion des BKA

a) Bestandsdaten

Für die Übermittlung und Abfrage von Telekommunikations- und Telemedien-Bestandsdaten zum Zwecke der Aufgabenwahrnehmung des BKA als Zentralstelle i. S. d. § 2 BKAG enthalten § 15a Abs. 3 Nr. 3 TMG-E und § 113 Abs. 3 Nr. 3 TKG-E (Übermittlung) bzw. § 10 Abs. 1 BKAG-E (Abfrage) einander korrespondierende Vorschriften. Mit Blick auf die Zuständigkeit des BKA als Zentralstelle zur Verhütung und Verfolgung bestimmter Straftaten fallen die Regelungen des § 15a Abs. 3 Nr. 3 Buchst. c) TMG-E, § 113 Abs. 3 Nr. 3 Buchst. c) TKG-E und § 10 Abs. 1 Nr. 3 BKAG-E, die an die „konkrete Gefahr (…), dass eine Person an der Begehung einer Straftat (…) beteiligt sein wird“, anknüpfen, jedoch aus dem Rahmen, da dem BKA als Zentralstelle „polizeiliche Aufgaben der Gefahrenabwehr (…) nicht übertragen“ sind (BVerfG, B. v. 27.5.2020, 1 BvR 1873/13 u. a., Rn. 209). Lediglich mit „vielfältigen Fallgestaltungen“, in denen das BKA zur Unterstützung der Landespolizeien tätig werde (GE S. 52, 55), lässt sich diese Abweichung von der gesetzlichen Aufgabenzuschreibung nicht begründen. Für die gesetzlich normierte Aufgabe der Straftatenverhütung enthalten andererseits § 15a Abs. 3 Nr. 3 Buchst. d) und e) TMG-E, § 113 Abs. 3 Nr. 3 Buchst. d) und e) TKG-E und § 10 Abs. 1 Nr. 4 und 5 BKAG-E eigenständige, auf das Gefahrenvorfeld zugeschnittene Regelungen, die allerdings insoweit zu weit gefasst sind, als sie nicht lediglich auf Straftaten

i. S. d. § 2 Abs. 1 BKAG Bezug nehmen, sondern auf Straftaten von erheblicher Bedeutung und schwere Straftaten gem. § 100a Abs. 2 StPO. Danach sollten § 15a Abs. 3 Nr. 3 Buchst. c) TMG-E, § 113 Abs. 3 Nr. 3 Buchst. c) TKG-E und § 10 Abs. 1 Nr. 3 BKAG-E gestrichen und § 15a Abs. 3 Nr. 3 Buchst. d) und e) TMG-E, § 113 Abs. 3 Nr. 3 Buchst. d) und e) TKG-E und § 10 Abs. 1 Nr. 4 und 5 BKAG-E auf die Verhütung von Straftaten nach § 2 Abs. 1 BKAG bezogen werden. Für die Verarbeitung dynamischer IP-Adressen zum Zwecke der Beauskunftung enthält § 10 Abs. 3 BKAG-E nur für die Straftatenverhütung im Gefahrenvorfeld (§ 10 Abs. 1 Nr. 4 und 5 BKAG-E) eine einschränkende Sonderregelung. Im Übrigen sind die Regelungen betreffend das BKA als Zentralstelle nicht zu beanstanden.

b) Zugangsdaten

Als Zentralstelle ist das BKA nicht zur Abfrage von Zugangsdaten aus Telemedienangeboten berechtigt. Das ergibt sich einerseits aus dem Zuschnitt der Übermittlungsregelung gem. § 15b Abs. 2 S. 1 TMG-E und dem Übermittlungsverbot gem. § 15b Abs. 2 S. 2 TMG-E, andererseits aus dem Fehlen einer entsprechenden Abfragebefugnis in § 10 BKAG-E. Für Zugangsdaten aus Telekommunikationsangeboten gilt das nicht. Hier greift die allgemeine Übermittlungsbefugnis nach § 113 Abs. 1 S. 2, Abs. 4 TKG-E und besteht eine korrespondierende Abfragebefugnis nach § 10 Abs. 2 BKAG-E. Beide Vorschriften enthalten keine spezifischen Einschränkungen, sondern fordern lediglich, dass „im Einzelfall die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen“ bzw. die „Auskunft verlangende Stelle auch zur Nutzung der zu beauskunftenden Daten im Einzelfall berechtigt ist“. Das dürfte nicht den Anforderungen des BVerfG im gegenständlichen Beschluss nach einer bereichsspezifischen hinreichend bestimmten gesetzlichen Regelung entsprechen. Warum Zugangsdaten aus Telekommunikations- und aus Telemedienangeboten unterschiedlich behandelt werden, ist auch hier nicht erkennbar (vgl. GE S. 44).

c) Nutzungsdaten

Eine Sonderregelung zur Abfrage von Telemedien-Nutzungsdaten zum Zweck der Identifizierung des Nutzers ist mit § 10a BKAG-E vorgesehen. Die dort genannten spezifischen Voraussetzungen spiegeln sich jedoch (wie bei § 100g Abs. 1 S. 2 StPO-E) nicht in der Übermittlungsbefugnis des § 15a TMG-E.

4. Zentralstellenfunktion des ZKA

a) Bestandsdaten

Befugnisse zur Übermittlung von Bestandsdaten an das Zollkriminalamt als Zentralstelle enthalten § 15a Abs. 3 Nr. 4 TMG-E und § 113 Abs. 3 Nr. 4 TKG-E. Die korrespondierenden Abfragebefugnisse finden sich in § 10 ZFdG-E. Nach § 10 Abs. 1 S. 1 ZFdG-E ist die Befugnis zur Abfrage der Daten beschränkt auf Aufgaben des ZKA im Zusammenhang mit der Verhütung von Straftaten (Nr. 1), der Koordinierung und Lenkung der Ermittlungen der Zollfahndungsämter (Nr. 2) und der Zusammenarbeit mit ausländischen Stellen und den Verfassungsschutzbehörden (Nr. 3). Die Unterstützung der Behörden der Zollverwaltung bei der

Verfolgung von Straftaten zählt demnach nicht zu den eine Abfragebefugnis eröffnenden Aufgaben. Gleichwohl knüpfen § 10 Abs. 1 S. 2 Nr. 1 ZFdG-E und § 15a Abs. 3 Nr. 4 Buchst. a) TMG-E wie auch § 113 Abs. 3 Nr. 4 Buchst. a) TKG-E mit dem strafprozessualen Anfangsverdacht an Maßnahmen der Strafverfolgung an. Soweit Hintergrund dieser Regelungen die Aufgabe der Koordinierung und Lenkung der Ermittlungen der Zollfahndungsämter sein sollte, besteht bei diesen bereits ein Ermittlungsverfahren und ist deshalb eine Auskunft zur Ermittlung der zuständigen Strafverfolgungsbehörde gar nicht erforderlich. Die letztgenannten Vorschriften müssten konsequenter Weise gestrichen werden. Weiter enthalten § 10 Abs. 1 S. 2 Nr. 2 ZFdG-E und § 15a Abs. 3 Nr. 4 Buchst. b) aa), bb) und cc) wie auch § 113 Abs. 3 Nr. 4 Buchst. b) aa), bb) und cc) TKG-E differenzierte Regelungen zur Bestandsdatenabfrage zu Zwecken der Gefahrenabwehr, auch im Gefahrenvorfeld. Auch diese Zweckrichtung ist in § 10 Abs. 1 S. 1 ZFdG-E nicht enthalten. Allgemeine Aufgaben der Gefahrenabwehr (außerhalb der Sicherung des Steueraufkommens und der Überwachung der Ausgaben nach Unionsrecht sowie der Straftatenverhütung) zählen ferner nach § 3 ZFdG-neu - ungeachtet des Umstands, dass das ZKA, wie die Begründung (GE S. 48) erläutert, faktisch auch außerhalb der Bereiche der Verhütung und Verfolgung von Straftaten operativ tätig werden mag - nicht zu den gesetzlichen Aufgaben des ZKA als Zentralstelle. Die genannten Vorschriften müssten folglich gestrichen werden. Im Übrigen wird auf die bereits am Begriff der „drohenden Gefahr“ geäußerte Kritik Bezug genommen. Soweit die Übermittlungs- und Abfragebefugnisse auf die Verhütung von Straftaten bezogen sind, sind sie nicht zu beanstanden. Für die Verarbeitung dynamischer IP-Adressen enthalten § 10 Abs. 3 ZFdG-E und § 15a Abs. 4 Nr. 2 bis 5 TMG-E bzw. § 113 Abs. 5 Nr. 2 bis 5 TKG-E für die Gefahrenabwehr und die Verhütung von Straftaten im Gefahrenvorfeld einschränkende Sonderregelungen.

b) Zugangsdaten

Übermittlungs- und Abfragebefugnisse für Zugangsdaten aus Telemedienangeboten sind für das ZKA als Zentralstelle nicht vorgesehen. Anderes gilt für Zugangsdaten aus Telekommunikationsangeboten. Wie bei den für das BKA als Zentralstelle maßgeblichen Regelungen sind § 10 Abs. 2 ZFdG-E und § 113 Abs. 1 S. 2, Abs. 4 TKG-E aber zu unspezifisch.

c) Nutzungsdaten

Das ZKA hat als Zentralstelle nach dem Gesetzentwurf keinen Zugriff auf Nutzungsdaten aus Telemedienangeboten.

5. Bekämpfung von Schwarzarbeit

Für den Zweck der Aufdeckung von Schwarzarbeit oder illegaler Beschäftigung enthält § 15a Abs. 3 Nr. 5 TMG-E eine Übermittlungsbefugnis für Bestandsdaten aus Telemedienangeboten, dem eine Abfragebefugnis nach § 7 Abs. 2 S. 1 SchwarzArbG-E entspricht. Für die Verarbeitung dynamischer IP-Adressen sieht § 7 Abs. 2 S. 2 SchwarzArbG-E engere Voraussetzungen vor, denen § 15a Abs. 4 Nr. 6 TMG-E auf der Übermittlungsseite korrespondiert. Die genannten Vorschriften sind nicht zu beanstanden. Ein Zugriff der Behörden auf Zu-

gangs- und Nutzungsdaten ist nicht vorgesehen, desgleichen nicht auf Bestandsdaten aus Telekommunikationsangeboten.

6. Verfassungsschutz

a) Bestandsdaten

Befugnisse zur Übermittlung von Bestandsdaten aus Telemedien- und Telekommunikationsangeboten an die Verfassungsschutzbehörden von Bund und Ländern enthalten § 15a Abs. 3 Nr. 5 TMG-E und § 113 Abs. 3 Nr. 6 TKG-E. Soweit dort jeweils unter Buchstabe b) eine offene Klausel vorgesehen ist, die an im Landesrecht eröffnete Aufträge für die Landesämter für Verfassungsschutz anknüpfen, ist fraglich, ob damit dem vom BVerfG geforderten Regelungsauftrag des Bundesgesetzgebers ausreichend Rechnung getragen wird. Schon die Beauftragung eines Landesamts mit der Aufgabe der Beobachtung der Organisierten Kriminalität ist verfassungsrechtlich, jedenfalls aber einfachrechtlich nicht unumstritten. Wäre also - wie etwa vormals im Bundesland Sachsen (vgl. SächsVerfGH NVwZ 2005, 1310; in Folge der Entscheidung wurde § 2 Abs. 1 Nr. 5 SächsVerfSchG a. F. mit Wirkung zum 28.04.2006 durch den Sächsischen Landesgesetzgeber aufgehoben) - ein solcher Auftrag nicht mit der Landesverfassung vereinbar, würde die bundesgesetzliche Regelung dennoch zur Übermittlung von Daten zu diesem Zweck ermächtigen. Das widerspricht dem der gegenständlichen Entscheidung des BVerfG zugrunde liegenden Gedanken, dass der Bundesgesetzgeber selbst darüber zu entscheiden habe, unter welchen Voraussetzungen eine Datenübermittlung rechtmäßig und gewollt ist. Denkbar und von den Übermittlungsnormen vorausgesetzt („insbesondere“) ist außerdem, dass im Landesrecht weitere Beobachtungsaufträge (etwa allgemein die Beobachtung verfassungsfeindlicher Kriminalität) geschaffen werden, über deren Rechtmäßigkeit gegenwärtig keine Aussage getroffen werden kann und deren Beurteilung also dem Bundesgesetzgeber entzogen ist. Hierfür gewissermaßen „auf Vorrat“ eine Übermittlungsbefugnis zu schaffen, dürfte mit dem Geist der gegenständlichen Entscheidung des BVerfG nicht vereinbar sein. Buchstabe b) der beiden Übermittlungsbefugnisse sollte deshalb gestrichen werden.

Für das BfV wird in § 8d BVerfSchG-E eine überarbeitete Abfragebefugnis geschaffen. Voraussetzung der Abfrage wie auch der Übermittlung ist in materieller Hinsicht, dass der Datenaustausch „aufgrund tatsächlicher Anhaltspunkte im Einzelfall (…) erforderlich ist“ zur Wahrnehmung der Aufgabe des Verfassungsschutzes. Die tatsächliche Grundlage bezieht sich damit erstens auf das Vorliegen einer verfassungsfeindlichen Bestrebung oder Tätigkeit und zweitens auf die Aufklärungsbedeutung der Bestandsdaten, also deren Erforderlichkeit. Diese doppelte Verankerung im Tatsächlichen ist regelungstechnisch ungewöhnlich. Üblicherweise reicht es aus, dass tatsächliche Anhaltspunkte für einen Sachverhalt gegeben sind, der den Beobachtungsauftrag auslöst (vgl. etwa § 8a Abs. 1 S. 1 BVerfSchG-E). Warum das Erfordernis tatsächlicher Anhaltspunkte mit dem Gesetzentwurf auch auf den Gesichtspunkt der Erforderlichkeit erstreckt und damit der Rechtsanwendungspraxis zusätzliche Begründungslasten auferlegt werden, erschließt sich nicht. Das BVerfG fordert das Bestehen tatsächlicher Anhaltspunkte nur für das Bestehen des Beobachtungsanlasses (BVerfG, B. v. 27.5.2020, 1 BvR 1873/13 u. a., Rn. 151), woran die Gesetzbegründung anschließt (GE S. 52).

Die Verarbeitung dynamischer IP-Adressen ist hier unter nicht erhöhten Voraussetzungen zulässig (§ 8d Abs. 2 BVerfSchG-E). Das Zitiergebot ist insoweit gewahrt (§ 8d Abs. 7 BVerfSchG-E).

b) Zugangsdaten

Ein Zugriff der Verfassungsschutzbehörden auf Zugangsdaten aus Telemedienangeboten ist nicht vorgesehen (§ 15b Abs. 2 TMG-E). Für Zugangsdaten aus Telekommunikationsangeboten erlauben § 113 Abs. 1 S. 2, Abs. 4 TKG-E die Übermittlung und § 8d Abs. 3 S. 1 BVerfSchG-E die Abfrage, ohne aber spezifische materielle Voraussetzungen hierfür festzulegen. Nach § 8d Abs. 3 S. 2 BVerfSchG-E gelten hierfür allerdings die besonderen Verfahrensanforderungen des § 8b Abs. 1 und 2, Abs. 2 BVerfSchG (Behördenleitervorbehalt, Anordnung durch BMI, Einbindung der G 10-Kommission). Bei einer Gesamtbetrachtung ist diese Kombination nicht zu beanstanden.

c) Nutzungsdaten

Ein Zugriff der Verfassungsschutzbehörden auf Nutzungsdaten aus Telemedienangeboten ist nicht vorgesehen.

7. Militärischer Abschirmdienst

Die Übermittlungs- und Abfragebefugnisse betreffend die Tätigkeit des MAD sind in § 15a Abs. 3 Nr. 7 TMG-E und § 113 Abs. 3 Nr. 6 TKG-E sowie § 4b MADG-E parallel zu denen der Verfassungsschutzbehörden ausgestaltet. Auf die Erwägungen unter 6. wird deshalb Bezug genommen. Die Schaffung einer eigenständigen Regelung im MADG ist ausdrücklich zu begrüßen und sollte auch für andere Maßnahmen erfolgen.

8. Bundesnachrichtendienst

a) Bestandsdaten

Hinsichtlich der Übermittlung von Bestandsdaten an den BND unterscheiden § 15a Abs. 3 Nr. 8 TMG-E und § 113 Abs. 3 Nr. 7 TKG-E in Anlehnung an die Entscheidung des BVerfG vom 19.5.2020, 1 BvR 2835/17, zwischen der Aufgabe der politischen Unterrichtung der Bundesregierung und der Früherkennung von aus dem Ausland drohenden Gefahren von internationaler Bedeutung. Das entspricht auch dem im „Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts“ verfolgten Ansatz. Alleinige Voraussetzung für die Übermittlung von Bestandsdaten zum Zweck der politischen Unterrichtung sind tatsächliche Anhaltspunkte dafür, dass im Einklang mit dem Auftragsprofil der Bundesregierung relevante Informationen von außen- und sicherheitspolitischer Bedeutung gewonnen werden können. Das harmoniert mit dem hohen öffentlichen Interesse an dieser Tätigkeit, von dem auch das BVerfG ausgeht (vgl. BVerfG, Urteil v. 19.5.2020, 1 BvR 2835/17, Rn. 224). Hinsichtlich der Tätigkeit der Früherkennung von Gefahren verweisen § 15a Abs. 3 Nr. 8 Buchst. b) TMG-E

und § 113 Abs. 3 Nr. 7 Buchst. b) TKG-E - regelungstechnisch vorbildlich - auf einen detaillierten abschließenden Katalog von Gefahrenbereichen und zu schützenden Rechtsgütern in § 4 Abs. 3 Nr. 1, 2 und 3 BNDG-E, die aufgrund ihrer hohen Wertigkeit bzw. wichtigen außen- und sicherheitspolitischen Bedeutung unter Verhältnismäßigkeitsgesichtspunkten nicht zu beanstanden sind. Dabei ist zu sehen, dass es sich bei dieser Einhegung nicht um die Umsetzung eines verfassungsrechtlichen Gebots, sondern um eine verfassungsrechtlich überobligationsgemäße Einschränkung handelt, dem offenbar ein Bemühen um Kohärenz und regelungstechnische Vereinfachung zugrunde liegt. Diese Regelungstechnik wurde zunächst im Nachgang des Urteils des BVerfG vom 19.5.2020, 1 BvR 2835/17, im Zusammenhang mit der dadurch notwendig gewordenen (und noch nicht abgeschlossenen) Novellierung der Ausland-Ausland-Fernmeldeaufklärung entwickelt, bei der es sich um eine deutlich eingriffsintensivere Maßnahme als die Bestandsdatenabfrage handelt. Unter einem wertenden Blickwinkel wäre es daher durchaus denkbar, bei der Bestandsdatenabfrage ein anderes, weniger einschränkendes Regelungsmodell zu wählen, was freilich zu einer weiteren, wenig praktikablen Verkomplizierung der Rechtslage führen würde. Perspektivisch darf umgekehrt aus der hier vorgenommenen Übertragung der Maßstäbe auf die Bestandsdatenabfrage für die noch anstehende Überarbeitung anderer eingriffsintensiver Aufklärungsmaßnahmen (etwa den Einsatz von geheimen Mitarbeitern) nicht der Schluss gezogen werden, zur Vermeidung von Wertungswidersprüchen sei dort eine weitere Anhebung der Eingriffsschwelle geboten. Auch das würde das begrüßenswerte Bestreben nach Kohärenz konterkarieren. Mit der anstehenden Novellierung des BNDG dürfte es vielmehr sinnvoll erscheinen, den Katalog maßnahmenübergreifend für alle Standardbefugnisse „vor die Klammer“ zu ziehen. Konsequent ist es daher auch, dass unter denselben Voraussetzungen nach § 4 Abs. 4 BNDG-E dynamische IP-Adressen zur Ermöglichung der Auskunft verarbeitet werden dürfen.

Die Durchbrechung des Übermittlungsverbots nach § 4 Abs. 8 S. 2 BNDG-E zum Schutz höchstrangiger Rechtsgüter ist als Teilkompensierung einer vom BVerfG vorgegebenen künstlichen Differenzierung zwischen politischer Unterrichtung und Gefahrenfrüherkennung ausdrücklich zu begrüßen. Allerdings entspricht die Ausnahme nicht mehr der - weniger eng gefassten - Parallelvorschrift des § 29 Abs. 4 BNDG-E in Gestalt des Referentenentwurfs eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts (anders noch § 31 Abs. 4 BNDG-E in einer früheren Entwurfsfassung). Da die Erhebung und Übermittlung von Bestandsdaten einen weniger schweren Eingriff vermittelt als die von Telekommunikationsdaten, wäre auch für die zweckändernde Verwendung von zur politischen Unterrichtung erhobenen Bestandsdaten für sicherheitsbehördliche Zwecke ein eher weiterer Rahmen sachgerecht. Im Übrigen wäre gerade bei den zweckändernden Übermittlungsvorschriften mehr Kohärenz erstrebenswert.

b) Zugangsdaten

Zugangsdaten dürfen an den BND nur übermittelt und von diesem abgefragt werden, wenn sie aus Telekommunikationsangeboten stammen, § 113 Abs. 1 S. 2, Abs. 4 TKG-E, § 4 Abs. 5 S. 1 BNDG-E. Dabei ist das strengere Verfahren nach § 8b Abs. 1 S. 1, 2, Abs. 2 BVerfSchG unter Einbindung der G 10-Kommission zu beachten, § 4 Abs. 5 S. 2 BNDG-E. Der generelle Ausschluss von Zugangsdaten aus Telemedienangeboten erscheint hier ange-

sichts des hohen Rangs der zu schützenden Rechtsgüter und der großen Bedeutung der Gefahrenbereiche sowie der etwaig erforderlichen Anpassung des grundrechtlichen Schutzniveaus an tatsächliche Gegebenheiten im Ausland (vgl. BVerfG, Urteil v. 19.5.2020, 1 BvR 2835/17, Rn. 104, 196) zu streng. Es könnte darüber nachgedacht werden, dem BND, sofern hierfür ein praktischer Bedarf besteht (etwa bei der Auswertung von Endgeräten, die von ausländischen Nachrichtendiensten zur Verfügung gestellt werden), einen entsprechenden Zugriff zu ermöglichen.

c) Nutzungsdaten

Ein Zugriff auf Telemedien-Nutzungsdaten ist für den BND nicht vorgesehen.

III. Zusammenfassende Würdigung

Die deutsche Sicherheitsarchitektur ist mit der Verschränkung von Bundes- und Länderkompetenzen, der Beteiligung zahlreicher Behörden mit im Ansatz unterschiedlichen, sich aber überschneidenden Mandaten sowie hybriden Funktionsträgern in Gestalt von Zentralstellen von beträchtlicher Unübersichtlichkeit gekennzeichnet. Diese Struktur spiegelt sich in den verfassungsrechtlichen Anforderungen an den Datenaustausch. Gemeinsam mit den im hier gegebenen Zusammenhang weiter vorgenommenen Differenzierungen zwischen Bestandsdaten aus Telemedien- und Telekommunikationsangeboten, zwischen regulären Bestandsdatenauskünften und solchen unter Verarbeitung dynamischer IP-Adressen sowie zwischen einfachen Bestandsdaten, Zugangsdaten und Nutzungsdaten erreichen die im gegenständlichen Gesetzentwurf versammelten Regelungen ein im Verhältnis zum „gemäßigten“ Eingriffsgewicht der manuellen Bestandsdatenabfrage und deren großer Praxisbedeutung absurdes Komplexitätsniveau. Gepaart damit ist die Verwendung unbestimmter Rechtsbegriffe zur Kennzeichnung von materiellen Eingriffsschwellen (etwa „Rechtsgut von erheblichem Gewicht“, „besonders gewichtiges Rechtsgut“, „Rechtsgut von hervorgehobenem Gewicht“), die aus dem Gesetz heraus nicht gegeneinander abgrenzbar sind. Mit den - vom BVerfG nicht beanstandeten - Regelungen zum automatisierten Bestandsdatenauskunftsverfahren nach §§ 111, 112 TKG harmoniert diese überbordende Ausdifferenziertheit nicht mehr.

Der Gesetzentwurf begnügt sich bedauerlicherweise damit, zu versuchen, die vom BVerfG vorgegebenen Differenzierungen nachzuzeichnen oder wörtlich zu paraphrasieren und übernimmt damit die in diesen angelegten Unzulänglichkeiten und Ungereimtheiten, ohne ein eigenes Ordnungssystem zu entwickeln. Das spiegelt sich auch in der geringen Substanz der Entwurfsbegründung, die im besonderen Teil zur Erläuterung von knapp 30 Seiten Normänderungsbefehlen nur wenig mehr als 20 Seiten umfasst. Angesichts der für eine Neuregelung zur Verfügung stehenden kurzen Fortgeltungsfrist und der großen praktischen Bedeutung des Instruments der Bestandsdatenabfrage, dessen Erhalt für die Sicherheitsbehörden als vorrangiges Ziel des Gesetzentwurfs angesehen werden muss, kann dieser Befund den Verfassern des Gesetzentwurfs freilich kaum zum Vorwurf gereichen, sondern stellt das Bemühen um Umsetzung der kleinteiligen Vorgaben des BVerfG in zahlreichen Sicherheitsgesetzen in der Kürze der Zeit eine durchaus beachtliche Leistung dar.

Eine Rechtsanwendung, die zugleich praktikabel und grundrechtsschonend sein soll, erscheint auf der Grundlage der beabsichtigten Regelungen, welche in dem hohen Grad ihrer Ausdifferenziertheit intuitiv nicht mehr zu erfassen und nachvollziehen sind, jedoch kaum mehr möglich. Das betrifft nicht nur die anspruchsvolle Prüfung der materiellen Voraussetzungen einer Abfrage durch die Fachbehörden, sondern auch die Prüfung der formalen Voraussetzungen eines Auskunftsersuchens durch die Verpflichteten. Zu diesen formalen Voraussetzungen zählt die Prüfung, ob die in Anspruch genommene Abfragebefugnis materiell nicht über die zur Übermittlung berechtigende Befugnis hinausgeht, denn andernfalls sind die Diensteanbieter „zur Auskunft weder berechtigt noch verpflichtet“ (BVerfG, B. v. 27.5.2020, 1 BvR 1873/13 u. a., Rn. 201; vgl. auch Petri, ZD 2020, 589, der noch weiter gehende Prüfungspflichten annimmt). Namentlich wenn eine abfragende Behörde Aufgaben in verschiedenen Bereichen des Sicherheitsrechts wahrnimmt, wenn der Gesetzgeber der Abrufregelungen die Abfragebefugnis an noch engere Voraussetzungen bindet als sie die Übermittlungsregelungen kennzeichnen oder wenn die Übermittlung von Zugangsdaten zusätzlich von der Zulässigkeit ihrer Nutzung nach den Fachgesetzen abhängig ist, kann diese Zuordnung Schwierigkeiten bereiten.

Hinzu kommt, dass korrespondierend zur manuellen Bestandsdatenauskunft als Konsequenz der gegenständlichen Entscheidung des BVerfG differenzierende Neuregelungen auch hinsichtlich anderer sicherheitsbehördlicher Datenerhebungen und -übermittlungen mit qualifiziertem Eingriffsgewicht erforderlich sind. Generell ist das Recht der Datenübermittlung im gesamten Bereich des Sicherheitsrechts von beträchtlichen Unstimmigkeiten, Lücken und Redundanzen gekennzeichnet, die seine strukturierte Vermittlung an die für die Rechtsanwendung verantwortlichen Personen annähernd unmöglich machen. Vor diesem Hintergrund ist es perspektivisch unumgänglich und dringend geboten, für den Datentransfer im Sicherheitsrecht ein einfacheres, anwendungsfreundlicheres, transparenteres und materiell substanzielleres Ordnungssystem zu entwickeln. Da die zuständigen Ressorts erfahrungsgemäß erst anlassabhängig und reaktiv zu Entscheidungen des BVerfG tätig werden, sollte damit eine unabhängige Kommission betraut werden.

[redacted]

(Prof. Dr. Markus Löffelmann)

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)696 C

Entwurf eines Gesetzes zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020

Hier: Sachverständigenanhörung im Innenausschuss des Deutschen Bundestages

am Montag, 25. Januar 2021

- Eingangsstatement Holger Münch, Präsident beim Bundeskriminalamt -

1. Bedeutung manueller Bestandsdatenabfragen für die Arbeit des BKA

Manuelle Bestandsdatenabfragen sind für das BKA aufgabenübergreifend von hoher Bedeutung.

Sie stellen in vielen Fällen einen wichtigen, wenn nicht gar den einzigen Ermittlungsansatz zur Identifizierung etwa eines Beschuldigten oder Gefährders dar, sei es im Bereich der klassischen Telefonie, bei der Nutzung von Messenger Diensten, E-Mail-Anbietern oder von sonstigen Kommunikationsdiensten über das Internet.

Ziel jeder Bestandsdatenauskunft ist es, den jeweiligen Telekommunikationsteilnehmer/-in über seine Rufnummer oder Kennung als Anschlussinhaber einschließlich anhand einer bereits polizeilich bekannten dynamischen IP-Adresse und Zeitstempel zu ermitteln. So kann der Nutzer/-in identifiziert bzw. weitere Ermittlungsansätze gewonnen werden. Ohne auf eine detaillierte Statistik im BKA für die Bestandsdatenabfragen zurückgreifen zu können, ist mittelbar über die Kosten für die Entschädigungsleistungen an die Provider von mehreren Tausend Anschlussinhaberfeststellungen pro Jahr im manuellen Verfahren auszugehen.

Ohne die Möglichkeit, manuell Bestandsdaten bei Telekommunikations- oder Telemediendiensten abfragen zu können, wäre die Arbeit des BKA in vielen Bereichen erheblich eingeschränkt.

So wäre die künftige Bearbeitung der Meldungen strafbarer Inhalte durch die sozialen Netzwerke nach § 3a NetzDG-neu ohne die Möglichkeit manueller Bestandsdatenabfragen für das BKA praktisch ausgeschlossen.

Ebenso lassen sich in anderen Phänomenbereichen der Zentralstelle, etwa in Prüfverfahren des BKA im Bereich der politisch motivierten Kriminalität (PMK), vielfach mittels Bestandsdatenabfragen neue Ermittlungsansätze generieren und so Netzwerke aufklären.

Gleiches gilt für die Aufgabe der Abwehr von Gefahren des internationalen Terrorismus. In Verfahren, in denen Störer hoch konspirativ kommunizieren, ist es immer wieder erforderlich, neu verwendete oder erst im Rahmen der Ermittlungen bekannt gewordene Nutzerkonten oder Rufnummern mittels Bestandsdatenabfragen abzuklären, um bestehende oder bislang unbekannte Störer sowie mögliche Kontaktpersonen zuordnen bzw. identifizieren zu können.

Auch die Sicherungsgruppe des BKA oder die Zeugenschutzdienststelle im BKA profitieren maßgeblich vom Instrument der manuellen Bestandsdatenauskunft: Sie wird bei der Prüfung von Gefährdungen von Schutzpersonen gem. § 6 bzw. § 7 BKAG herangezogen, um die jeweilige Gefahrenlage einschätzen und ihre Verursacher identifizieren zu können. So ist es in solchen Fällen notwendig, Personen, die Straftaten zum Nachteil von Schutzpersonen per E-Mail, telefonisch, schriftlich oder über soziale Netzwerke androhen, zu identifizieren und zu prüfen, ob sie in der Lage wären, die angedrohten Straftaten auch in die Tat umzusetzen.

Um das an einem Beispiel konkret zu machen: Im Jahr 2020 erlangte das BKA im Zuge einer Veranstaltungstour des Bundesministers für Gesundheit zur Corona-Krise Kenntnis von E-Mails und Postings aus den sozialen Netzwerken, in denen auch die Gewaltanwendung gegen Schutzpersonen des BKA angedroht wurde. Diese manifestierten sich u.a. in öffentlichen Aufrufen zu Straftaten. Im Rahmen von OSINT-Recherchen wurden E-Mail-Adressen und IP-Adressen festgestellt, welche mittels Bestandsdatenabfrage zur Identifizierung der Störer führten. Somit konnte das BKA auf die jeweils aktuellen Situationen vor Ort reagieren und konkrete Maßnahmen zum Schutz des Bundesministers und weiterer Schutzpersonen einleiten.

Für eine erfolgreiche Kriminalitätsbekämpfung in Deutschland und für eine erfolgreiche Wahrnehmung unserer Aufgaben im BKA ist es daher von großer Bedeutung, dass die Bestandsdatenauskunft in angemessener Weise für die Polizei nutzbar ist und handlungs- und rechtssicher formuliert wird.

2. Notwendigkeit des Gesetzentwurfs

Der Gesetzentwurf zur Bestandsdatenauskunft dient der Umsetzung der Vorgaben des Bundesverfassungsgerichts (BVerfG). Und er dient der Anpassung der Vorschriften des Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (GE Hasskriminalität), die inhaltlich mit den als verfassungswidrig erklärten Normen übereinstimmen.

Grundsätzlich war die bisherige, d.h. noch geltende Normausgestaltung der Regelungen zur manuellen Bestandsdatenauskunft im BKAG relativ allgemein formuliert. Sie muss nun nach den Vorgaben des BVerfG konkretisiert werden. Dabei muss sichergestellt werden, dass mit den neuen Regelungen weiterhin diejenigen Fallkonstellationen erfasst werden, in denen das BKA im Rahmen

seiner gesetzlichen Aufgaben auf die Erhebung von Bestandsdaten angewiesen ist.

Es ist den Vorgaben des BVerfG geschuldet, dass für die Zulässigkeit von manuellen Bestandsdatenabfragen im BKAG künftig entweder

- ein **Anfangsverdacht** für die Aufgabe der Unterstützung der Polizeien des Bundes und der Länder bei der Strafverfolgung (BKA als Zentralstelle) oder
- ein je nach zu schützendem Rechtsgut entsprechender **Gefahrengrad** für die Gefahrenabwehr bzw. Verhütung von Straftaten (Zentralstelle, Personen- oder Zeugenschutz, Gefahrenabwehr internationaler Terrorismus)

vorliegen muss.

Diese Vorgaben gilt es einzuhalten – sie dürfen auch nicht unterschritten werden.

3. Auswirkungen des Gesetzentwurfs auf die Aufgabenwahrnehmung des BKA

Der Gesetzentwurf erfasst im Kern die eingangs dargestellten Fallkonstellationen.

So bleibt es dem BKA als Zentralstelle künftig möglich,

- bei Vorliegen eines erkennbaren Anfangsverdachts bzw. im Bereich der Verhütung von Straftaten zur Feststellung der zuständigen Strafverfolgungs-/Gefahrenabwehrbehörde sowie
- im Rahmen der polizeilichen Rechtshilfe (d.h. Ersuchen von ausländischen Polizeibehörden)

manuelle Bestandsdatenabfragen durchzuführen.

Beides sind wesentliche Aufgaben des BKA als Zentralstelle, die bereits jetzt, z.B. im Rahmen des NCMEC-Prozesses und des internationalen polizeilichen Dienstverkehrs, wie auch in Zukunft, beispielsweise durch die Zentrale Meldestelle für strafbare Inhalte im Internet, wahrgenommen werden.

Ebenso bleiben manuelle Bestandsdatenabfragen für das BKA auch für die Abwehr von Gefahren des internationalen Terrorismus sowie für den Personen- und Zeugenschutz erhalten. Der Gesetzentwurf setzt dabei die Vorgaben des BVerfG um, wobei die Möglichkeit, auch im Vorfeld einer konkreten Gefahr Bestandsdaten erheben zu können, für das BKA von hoher Bedeutung ist. Dem so vorgelagerten Gefahrengrad wird dabei durch die hohe Bedeutung der zu schützenden Rechtsgüter im Gesetz ausreichend Rechnung getragen.

4. Fazit

Im Ergebnis ist festzuhalten, dass der vom BVerfG vorgegebene Rahmen für manuelle Bestandsdatenabfragen durch das BKA im vorliegenden Gesetzentwurf deutlich erkennbar und für die praktische Anwendung handlungs- und rechtssicher formuliert ist. Die bislang dem BKA zur Verfügung stehenden Möglichkeiten manueller Bestandsdatenauskünfte können daher im Kern auch mit der künftigen Neuregelung wahrgenommen werden.

Zudem wird durch die – bereits z.T. im GE Hasskriminalität vorgesehene – explizite Aufnahme der Telemediendienste in die Regelungen zur manuellen Bestandsdatenauskunft im BKAG nunmehr eine eindeutige Rechtsgrundlage für die Aufgaben des BKA geschaffen, mit der die Telemediendienste auch zur Auskunft von Bestandsdaten verpflichtet werden. Dies ist aus Sicht des BKA zu begrüßen.

Es muss aber beachtet werden, dass im jeweils konkreten Fall ein Ersuchen an den Betreiber auf Bestandsdatenauskunft nur dann einen Mehrwert für die polizeiliche Arbeit darstellt, wenn der Anbieter auch die Kundendaten gespeichert hat, um hieraus Auskunft erteilen zu können. Dies gilt insbesondere für dynamische IP-Adressen.

So erhielt des BKA allein im Jahr 2020 rund 29.000 strafrechtlich relevante Meldungen des US-amerikanischen National Center for Missing and Exploited Children (NCMEC). In 2.594 Fällen war dabei die IP-Adresse der einzige Ermittlungsansatz. Eine manuelle Bestandsdatenabfrage anhand dieser IP-Adresse war jedoch nicht möglich, weil die Regelungen zur Vorratsdatenspeicherung aktuell nicht umgesetzt werden. Die Meldungen konnten in diesen Fällen also strafrechtlich nicht weiterverfolgt werden – das heißt ganz konkret: Der Missbrauch und das Leid, dass hinter dieser Meldung gesteckt haben könnte, konnte nicht bekämpft und beendet werden.

Unabhängig davon ist der Gesetzgeber mit diesem Gesetzentwurf jetzt einen guten Schritt weiter in Richtung Rechts- und Handlungssicherheit.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)696 D

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 22.01.2021

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

für die öffentliche Anhörung des Ausschusses für Inneres und Heimat

des Deutschen Bundestages

am 25. Januar 2021

zum

Entwurf

eines Gesetzes zur Anpassung der

Regelungen über die Bestandsdatenauskunft an die

Vorgaben aus der Entscheidung des

Bundesverfassungsgerichts vom 27. Mai 2020

(BT-Drucksache 19/25294)

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

A. Vorbemerkung

In seiner Entscheidung vom 27. Mai 2020, Az.: 1 BvR 1873/13 und 1 BvR 2618/13, („Bestandsdatenauskunft II“) hat das Bundesverfassungsgericht die verfassungsrechtlichen Vorgaben für die gesetzliche Ausgestaltung des manuellen Auskunftsverfahrens konkretisiert und die in § 113 Abs. 1 TKG enthaltenen Übermittlungsregelungen sowie eine Reihe damit korrespondierender fachgesetzlicher Abrufregelungen für mit dem Grundgesetz unvereinbar erklärt (insbesondere aus dem BKAG, BPolG, ZFdG, BVerfSchG, BNDG, MADG). Darin sehe ich eine Bestätigung meines Standpunkts. An Kritik meines Hauses an den bisherigen Regelungen zur Bestandsdatenauskunft mangelte es in den vergangenen Jahren nicht.

Mit dem o.g. Entwurf will die Bundesregierung den Beschluss des Bundesverfassungsgerichts vom 27. Mai 2020 umsetzen. Ich begrüße es ausdrücklich, dass die Regelungen über die Bestandsdatenauskunft, die Gegenstand des Gesetzesentwurfs sind, so zeitnah an die Vorgaben des Bundesverfassungsgerichts angepasst werden sollen. Darüber hinaus halte ich es jedoch für notwendig, über das hier relevante Gesetzgebungsvorhaben hinaus alle anderen vergleichbaren Vorschriften in den Blick zu nehmen, die zum Austausch von personenbezogenen Daten ermächtigen. Auch diese sind im Lichte des Beschlusses des Bundesverfassungsgerichts zu überprüfen und gegebenenfalls verfassungskonform auszugestalten. Hierzu verweise ich auf die Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 25. November 2020.

In der Ressortabstimmung zum Referentenentwurf der Bundesregierung vom 20. November 2020 wurde ich beteiligt. Bei einem komplexen und bedeutenden Gesetzesvorhaben wie dem vorliegenden ist eine Stellungnahmefrist von knapp einer Woche allerdings weder sachgerecht noch angemessen.

Einige Kritikpunkte aus meiner Stellungnahme vom 1. Dezember 2020 wurden von der Bundesregierung berücksichtigt. Die vorliegende Stellungnahme beschränkt sich im Wesentlichen auf die Aspekte, die bislang nicht aufgegriffen wurden.

B. Im Einzelnen

Im Einzelnen nehme ich zu dem o.g. Gesetzesentwurf wie folgt Stellung:

Zu Artikel 1 Ziff. 4 (§ 8d BVerfSchG-E) und Artikel 3 (§ 4b MADG-E)

Die spezialgesetzlichen Abrufregeln für die Nachrichtendienste, im vorliegenden Entwurf § 8d BVerfSchG-E und § 4b MADG-E, genügen den vom Bundesverfassungsgericht aufgestellten Anforderungen nicht im vollem Umfang.

Die in § 8d BVerfSchG-E und § 4b MADG-E aufgenommene Formulierung „zur Aufklärung bestimmter Bestrebungen oder Tätigkeiten“ bleibt zu stark auslegungsbedürftig

und genügt damit nicht dem Bestimmtheitsgrundsatz. Die Voraussetzungen zur Festlegung dieser „bestimmten Bestrebungen oder Tätigkeiten“ müssen sich im Gesetzestext finden.

Grundlegende Fragestellungen, wie die Voraussetzungen zur Überschreitung der Schwelle zur Beobachtungsbedürftigkeit, müssen in den nachrichtendienstlichen Gesetzen und nicht wie bislang in untergesetzlichen als Verschlusssache eingestuften Vorschriften bestimmt werden. Auf Länderebene wurden diesbezüglich bereits entsprechende Regelungen in die einschlägigen Landesgesetze aufgenommen, so z.B. im zweiten Teil des niedersächsischen Landesverfassungsschutzgesetzes, der die Bestimmung zum Beobachtungsobjekt zum Thema hat.

In den nunmehr vorgelegten unzureichenden und zu unbestimmten Formulierung zeigt sich einmal mehr die Unzulänglichkeit der nachrichtendienstlichen Gesetzessystematik, hinsichtlich derer ich wiederholt eine umfassende Gesamtreform angemahnt habe, zuletzt als Sachverständiger in der öffentlichen Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestages am 2. November 2020 zum Gesetz zur Entfristung von Vorschriften nach den Terrorismusbekämpfungsgesetzen.

Das Bundesverfassungsgericht hat dem Gesetzgeber inzwischen zum Recht der Nachrichtendienste eine lange Aufgabenliste zugewiesen. Diese Aufgabenliste macht es allerdings nötig, die Nachrichtendienstgesetze grundlegend zu überarbeiten. Aus meiner Sicht wäre es geboten, diese endlich konsequent abzuarbeiten statt, mit einzelnen "Reparaturgesetzen" zu agieren.

Zu Artikel 4 (Änderung des BND-Gesetzes [BNDG])

Ziff. 2 (§ 4 BNDG-E)

Der im Referentenentwurf vom 20. November 2020 in § 4 Abs. 3 BNDG-E vorgesehene Verweis auf § 8b Abs. 1 S. 1 und 2, Abs. 2 BVerfSchG resultiert in einer zumindest erhöhten Gefahr für das Bestehen einer unzulässigen Verweisungskaskade, indem von § 8b BVerfSchG ausgehend unter anderem in andere Normen des BVerfSchG und andere Normen des Artikel 10-Gesetz verwiesen wurde. Dieser Verweis findet sich in der aktuellen Gesetzesentwurfsfassung nun deckungsgleich in § 4 Abs. 5 S. 3 BNDG-E wieder. Insofern bleibt es bei der Empfehlung, eine eigenständige Regelung im BNDG zu schaffen, um der Gefahr einer unzulässigen Verweisungskaskade zu begegnen. Vor dem Hintergrund einer besseren Verständlichkeit empfiehlt sich gesetzestechnisch generell eine Abstandnahme von der bisher im BNDG umfangreich genutzten Verweisungstechnik, insbesondere auf Normen des BVerfSchG, welche sodann häufig auf andere Normen im BVerfSchG bzw. auf andere Normen außerhalb des BVerfSchG in entsprechender Anwendung weiter verweisen.

Zu Artikel 6 (Änderung des Bundespolizeigesetzes [BPolG])

Ziff. 2 (§ 22a BPolG)

Die vorgeschlagene Änderung des BPolG stellt in erster Linie eine Befugniserweiterung dar. Die Bundespolizei soll künftig auch auf Passwörter und Bestandsdaten von Telemedienanbietern zugreifen können. Dies soll auch den Abruf von Bestandsdaten nach dem Telemediengesetz, die anhand dynamischer IP-Adressen bestimmt werden, umfassen. Situationen, in denen die Bundespolizei in ihrer Funktion als Sonderpolizei mit begrenztem Aufgabenspektrum Daten von Telemedienanbietern benötigt, dürften sich jedoch wenn überhaupt auf wenige Fälle beschränken. So wurde dann auch die ursprüngliche Darstellung in der Begründung des Referentenentwurfs, die auf Verabredungen im Internet zur Gewalt gegen Bahnpersonal abstellte (wohl mangels Realitätsbezugs) wieder gestrichen. Nunmehr wird in der Begründung des Gesetzesentwurfs nur noch auf ein Szenario abgestellt, nämlich auf Verabredungen im Internet zu Anschlägen an Bahnhöfen oder Flughäfen (S. 43). Dem entspricht die neue Rechtsgrundlage jedoch nicht. Sie ermöglicht eine Anforderung von Bestandsdaten von Telemedienanbietern bereits bei Gefahren für Rechtsgüter ohne erhebliches Gewicht (§ 22a Abs. 1 S. 2 Nr. 1 BPolG-E „eine Gefahr für die öffentliche Sicherheit abzuwehren“). Im Ergebnis wäre damit, sofern im Einzelfall notwendig, eine Abfrage von Telemedien-Bestandsdaten bei jeglichen Ordnungswidrigkeiten oder Straftaten im Aufgabenbereich der Bundespolizei prinzipiell möglich.

Zu Artikel 7 (Änderungen des Bundeskriminalamtsgesetzes [BKAG])

Ziff. 5 (§ 63a) und Ziff. 6 (§ 66a)

Nach dem Bundesverfassungsgericht müssen die Auskünfte, die anhand einer dynamischen IP-Adresse verlangt werden, aufgrund der damit verbundenen erheblich größeren Persönlichkeitsrelevanz dem Schutz besonders gewichtiger Rechtsgüter dienen. „Soweit die Gefahrenabwehr auf die Verhütung von Straftaten bezogen ist, muss es sich um zumindest schwere Straftaten handeln“ (BVerfG, a.a.O., Rz. 181). Eine solche Konstellation betreffen §§ 63a Abs. 4 und 66a Abs. 4 BKAG-E. So darf eine Bestandsdatenauskunft anhand einer dynamischen IP-Adresse zur Abwehr einer Gefahr für eine zu schützende Person oder für eine zu schützende Räumlichkeit nach § 6 gemäß § 63a Abs. 4 Nr. 1 in Verbindung mit Abs. 1 Nr. 1 BKAG-E nur bei Gefahr der Begehung einer Straftat erteilt werden. Mit dieser Formulierung ist nicht sichergestellt, dass es sich – entsprechend den Vorgaben des Bundesverfassungsgerichts – um eine schwere Straftat handelt. Zu beachten ist außerdem, dass das Bundesverfassungsgericht dem Gesetzgeber die Verpflichtung auferlegt hat, abschließend festzulegen, welche Straftatbestände hiervon umfasst sein sollen. Das Gericht führte weiter wie folgt aus: „Er [der

Gesetzgeber] kann dabei auf bestehende Kataloge zurückgreifen oder einen eigenen Katalog schaffen, etwa um Straftaten zu erfassen, für die die Zuordnung von IP-Adressen besondere Bedeutung hat. Die Qualifizierung einer Straftat als schwer muss aber in der Strafnorm – etwa durch deren Strafrahmen – einen objektivierten Ausdruck finden. Eine Generalklausel oder die lediglich pauschale Verweisung auf nicht näher eingegrenzte Straftaten reichen hingegen nicht aus“ (BVerfG, a.a.O., Rn. 181). Aus meiner Sicht bietet es sich an, die Straftatbestände schwerer Straftaten abschließend festzulegen, für die die Zuordnung von IP-Adressen besondere Bedeutung hat.

Zu Artikel 8 (Änderung der Strafprozessordnung [StPO])

Ziff. 3 (§ 100j StPO-E)

Das Bundesverfassungsgericht hat in der hier relevanten Entscheidung sein „Doppeltür-Modell“ insofern präzisiert, als schon der Gesetzgeber der Übermittlungsregelung in eigener Regelungsverantwortung eine klare und abschließende Entscheidung treffen muss, zu welchen Zwecken und mit welchen Begrenzungen er die erste Tür öffnet (BVerfG, a.a.O., Rz. 201). Eine solche abschließende Entscheidung des Gesetzgebers beinhaltet § 15b Abs. 2 TMG-E, der die Übermittlung von Passwörtern und anderen Zugangsdaten vom Vorliegen einer gerichtlichen Anordnung abhängig macht. Diese erste „Tür“ kann – mit den Worten des Bundesverfassungsgerichts – auch der Gesetzgeber der zweiten Tür nicht weiter öffnen (BVerfG, a.a.O., Rz. 201). Insofern begegnet es durchgreifenden Bedenken, dass § 100j Abs. 3 S. 2 StPO eine Eilkompetenz der Staatsanwaltschaft und ihrer Ermittlungspersonen begründet.

Zu Artikel 11 (Änderung des Zollfahndungsdienstgesetzes [ZFdG])

Ziff. 1 (§ 10 ZFdG-E)

Die Neufassung von § 10 Abs. 1 Satz 1 ZFdG-E sieht trotz der von mir in meiner Stellungnahme vom 1. Dezember 2020 geäußerten Kritik auch weiterhin eine Erweiterung der Abrufbefugnisse des Zollkriminalamtes (ZKA) vor. Neben der Erhebung von Bestandsdaten bei Telekommunikationsanbietern ermöglicht der Gesetzesentwurf künftig auch Bestandsdatenabfragen bei Telemedienanbietern sowie nach § 10 Abs. 2 ZFdG-E die Befugnis zum Abruf von Passwörtern und Zugangsdaten nach dem Telekommunikationsgesetz. Es entsteht insgesamt der Eindruck, dass die Anpassung der Vorschriften zur Bestandsdatenauskunft an die Vorgaben des Bundesverfassungsgerichts genutzt wird, die Eingriffsbefugnisse der Sicherheitsbehörden schleichend zu erweitern.

Ziff. 4 (§ 30 ZFdG-E)

§ 30 Abs. 1 Satz 1 ZFdG-E ermöglicht dem ZKA eine Bestandsdatenauskunft zur Erfüllung seiner Aufgaben nach § 4 Abs. 2 Nr. 1 ZFdG-E und nach § 4 Abs. 3 Nr. 1 ZFdG-E. Danach wirkt das ZKA im Zuständigkeitsbereich der Zollverwaltung bei der Überwachung des Außenwirtschaftsverkehrs und bei der Überwachung des grenzüberschreitenden Warenverkehrs durch Maßnahmen zur Verhütung von Straftaten und Ordnungswidrigkeiten mit. Die Erstreckung von Bestandsdatenauskünften auf bloße Ordnungswidrigkeitentatbestände setzt die Eingriffsschwelle sehr niedrig. Zudem dürfte es an einer hinreichenden Konkretisierung der Eingriffsschwelle fehlen. In der Gesetzesbegründung wird pauschal auf die Ausführungen zu § 10 Abs. 1 ZFdG-E verwiesen, der wiederum eine Erweiterung der Bestandsdatenauskunft auf derartige Tatbestände gar nicht vorsieht. Eine entsprechende Begründung fehlt mithin.

Nach § 30 Abs. 2 Satz 1 ZFdG-E können die Zollfahndungsämter zudem zur Erfüllung ihrer Aufgabe nach § 5 Abs. 2 ZFdG-E Bestandsdaten erheben. Der Verweis lässt jedoch die ursprüngliche Eingrenzung auf die Aufgabenwahrnehmung zur Verhütung von Straftaten vermissen und ist nicht deckungsgleich mit der Gesetzesbegründung. Ausweislich der Gesetzesbegründung (vgl. BT-Drs. 19/25294 S. 49) soll sich die die Befugnis der Zollfahndungsämter zur allgemeinen Bestandsdatenauskunft auf Aufgaben zur Straftatenverhütung beschränken. Insoweit ist der Gesetzeswortlaut des § 30 Abs. 2 Satz 1 ZFdG-E um eine entsprechende Formulierung zu ergänzen.

Zu Artikel 12 (Änderung des Telemediengesetzes [TMG])

Ziff. 3 (§§ 15a und 15b TMG-E)

Meine bereits mehrfach an § 15a und § 15b TMG-E geäußerte Kritik blieb bisher unberücksichtigt. Bereits in meiner Stellungnahme zum Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität hatte ich die geplante Passwortherausgabe kritisiert und in meiner Stellungnahme zu diesem Gesetzentwurf vom 1. Dezember 2020 auf diese Kritik Bezug genommen. Da § 15a TMG-E auch die Übermittlung von Nutzungsdaten erlauben soll, stellt er einen schwerwiegenderen Eingriff dar als die in § 113 Abs. 1 TKG-E vorgesehene Übermittlung von Bestandsdaten. Wegen der höheren Eingriffsintensität sollte sich § 15a Abs. 3 Nr. 1 TMG daher erst Recht auf die Verfolgung von Straftaten beschränken und die geplante Übermittlung zur Verfolgung von Ordnungswidrigkeiten sollte gestrichen werden. Die in den §§ 15a Abs. 1 S. 4 und 15b Abs. 1 S. 2 TMG-E vorgesehene Berücksichtigung sämtlicher unternehmensinterner Datenquellen lässt die Herausgabe umfangreicher Nutzungsprofile befürchten und sollte deshalb gestrichen werden.

Außerdem sehe ich die Regelung in § 15b Abs. 1 TMG-E zur Passwortherausgabe weiterhin sehr kritisch. Denn es stellt sich die Frage der Datensicherheit, wenn neben

Diensten wie Cloud-Speichern oder Online-Händlern beispielsweise auch das Online-Banking betroffen ist. Der Hinweis in § 15b Abs. 3 S. 2 TMG, nach dem eine Verschlüsselung der Daten unberührt bleibt, mag gut gemeint sein, steht aber technisch mit der Herausgabe von Passwörtern im Widerspruch. Denn bei einer tatsächlichen Verschlüsselung entscheidet alleine der jeweilige Nutzer, ob Dritte Zugriff auf seine Daten haben können. Eine Herausgabe von Passwörtern kann neben der Beeinträchtigung von Verbrauchern auch die sichere Kommunikation von Banken untereinander beeinträchtigen. Deshalb ist fraglich, ob deutsche Bankinstitute die nach der EU-Zahlungsdiensterichtlinie notwendige Authentifizierung noch gewährleisten können oder sich aus dem elektronischen Bankenverkehr zurückziehen müssten. Auch eine – ggfs. mittelbare – Pflicht zu einer einfach aufzuhebenden Verschlüsselung lehne ich ab, da diese gegen die unionsrechtliche Vorschrift des Art. 32 DSGVO verstoßen würde. Hiernach müssen Anbieter technische und organisatorische Maßnahmen zur Datensicherheit treffen. Dazu gehört auch die sichere Speicherung und Übermittlung von Passwörtern. Unklar bleibt auch, wie im Falle der Zwei-Faktor-Authentifizierung diese Sicherheit gewährleistet werden kann, nachdem diese Authentifizierung durch die EU-Zahlungsdiensterichtlinie verpflichtend eingeführt wurde.

Zu Artikel 13 (Änderung des Telekommunikationsgesetzes [TKG])

Ziff. 1 (§ 113 TKG-E)

Leider wurde die Forderung aus meiner Stellungnahme vom 1. Dezember 2020, den Passus "und Ordnungswidrigkeiten" in § 113 Abs. 3 Nr. 1 TKG-E zu streichen, im überarbeiteten Gesetzesentwurf vom 15. Dezember 2020 nicht berücksichtigt. 113 Abs. 3 Nr. 1 TKG-E genügt damit weiterhin nicht den verfassungsrechtlichen Vorgaben. Denn entgegen den Ausführungen zu § 113 Abs. 3 Nr. 1 TKG-E in der Begründung des Gesetzesentwurfs (S. 51) genügt nur ein Anfangsverdacht für eine Straftat den verfassungsrechtlichen Anforderungen. Dass ein Anfangsverdacht auch für die Verfolgung von Ordnungswidrigkeiten genügen soll, geht aus dem Beschluss des Bundesverfassungsgerichts nicht hervor (vgl. BVerfG, a.a.O., Rz. 146). Aus Verhältnismäßigkeitsgründen sollte sich die Vorschrift auf die Verfolgung von Straftaten beschränken.

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

Prof. Dr. Kyrill-Alexander Schwarz
Institut für Staats- und Verwaltungsrecht,
Rechtphilosophie

Prof. Dr. Kyrill-A. Schwarz, Domerschulstraße 16, 97070 Würzburg

97070 Würzburg
Domerschulstraße 16
Telefon: (0931) 31-8 82335
E-Mail: Kyrill-alexander.schwarz@uni-wuerzburg.de
Sekretariat: E. Fickenscher

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Die Vorsitzende
Frau Andrea Lindholz, MdB

per Mail

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)696 E

Würzburg, den 22.1.2021

Sachverständige Stellungnahme zum Entwurf eines Gesetzes zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020, BT-Drs. 19/25294

I. Vorbemerkung

Der Gesetzentwurf der Regierungsfraktionen von CDU/CSU und SPD vom 15.12.2020 ist mehr als ein reines Reparaturgesetz als notwendige Reaktion auf die Entscheidung des Bundesverfassungsgerichts vom 27.5.2020 in Sachen Bestandsdaten II; dieser Gesetzentwurf ist der Versuch, die in das Gewand des Verhältnismäßigkeitsprinzips eingekleideten immer kleinteiligeren Vorgaben des Bundesverfassungsgerichts im Bereich des Sicherheitsrechts auf ein Eingriffsinstrumentarium anzuwenden, dem das Bundesverfassungsgericht selbst grundsätzlich eine „geringe Eingriffsintensität" bescheinigt. Der Gesetzgeber findet sich in der unbequemen Lage eines Prokrustes-Bett wider, die ihn einerseits zwar zur Beachtung der verfassungsgerichtlichen Vorgaben zwingt, die aber andererseits so eng sind („*juristischer Overkill*"), dass von einem eigenen gesetzgeberischen Gestaltungsspielraum bei der Umsetzung dieser Vorgaben nicht mehr ausgegangen werden kann.

Wenn und soweit geltendes Recht – und dies gilt in Sonderheit für den sensiblen Bereich des Sicherheitsrechts – aus verfassungsrechtlichen Gründen nicht nur vorhersehbar, sondern zudem auch nachvollziehbar und verständlich sein soll, um so auch die Akzeptanz der entsprechenden Maßnahmen zu fördern, dann ist ein Konzept der Sicherheitsarchitektur – wie sie das Bundesverfassungsgericht entwickelt hat -, das zwischen Abruf- und Übermittlungsregelungen unterscheidet, diese unterschiedlichen Rechtsregimen unterwirft und damit die Datenerhebung ebenso wie die Datenübermittlung in den Bereich des schwer Bestimmbaren verbannt, nur schwer mit verfassungsrechtlichen Vorgaben zu vereinbaren. Erschwerend tritt der Befund hinzu, dass gerade das Doppeltüren-Modell in besonderem Maße geeignet, föderale Konflikte zu provozieren, wenn letzten Endes die Landesgesetzgeber, soweit sie Rechtsgrundlagen für das Handeln ihrer Behörden normieren, auf die Verfassungsmäßigkeit bundesgesetzlicher Regelungen angewiesen sind, deren Inhalt sie selbst aber nicht beeinflussen können.

Dies ist – um es so deutlich zu formulieren – keine Kritik am parlamentarischen Gesetzgeber, der sich in der schwierigen Situation befindet, entweder mit dem Vorwurf konfrontiert zu werden, er zeichne nur Karlsruher Vorgaben nach und beschränke sich auf einen Reparaturbetrieb oder dem vorgeworfen wird, er fülle ihm vermeintlich zustehende Spielräume mit verfassungswidrigen Regelungen aus und nehme sehenden Auges weitere verfassungsgerichtliche Verfahren in Kauf. Insgesamt dürfte in Ansehung der durch das Bundesverfassungsgericht gesetzten Maßstäbe für ein verfassungskonformes Sicherheitsrecht der Gesetzgeber vor der Aufgabe stehen, das Sicherheitsrecht des Bundes insgesamt neu zu entwickeln, um in einer systematischen und kohärenten Weise den Anforderungen an Grundrechtseingriffe – auch und gerade in Ansehung der unterschiedlichen Eingriffsintensität – Rechnung tragen zu können.

II. Die Kernaussagen der Entscheidung des Bundesverfassungsgerichts vom 27.5.2020

Nachdem das Bundesverfassungsgericht bereits in der ersten Entscheidung zur Bestandsdatenauskunft (*BVerfGE* 130, 151 ff.) die Maßstäbe und Kriterien eines grundsätzlich verfassungsrechtlich zulässigen Zugriffs auf die durch Telekommunikationsanbieter gespeicherten Bestandsdaten herausgearbeitet hatte, erweist sich der Beschluss vom 27.5.2020 als Konkretisierung und Erweiterung der zuvor gewonnenen Maßstäbe; in Sonderheit für das „Doppeltür-Modell", das letzten Endes vom Gesetzgeber sowohl für den Abruf als auch für die Übermittlung entsprechender Daten strenge Maßstäbe aufstellt. Dieses Modell fordert – auf einer einfachen Abstraktionsebene – für den Abruf von Bestandsdaten das Vorhandensein einer Übermittlungsnorm und fachgesetzlicher Abrufnormen, die die konkrete Auskunftsverpflichtung für die Anbieter entsprechender Telekommunikationsdienste darstellen.

Der am 27.05.2020 ergangenen Beschluss des BVerfG zur Bestandsdatenauskunft (*Bestandsdatenauskunft II*) hat den schon sehr weit durch die Rechtsprechung des BVerfG zur Sicherheitsarchitektur begrenzten Gestaltungsspielraum des Gesetzgebers noch einmal erheblich grundrechtlich koloriert und die dem Gesetzgeber angelegten Fesseln angezogen. Die Entscheidung geht dabei in eine zur aktuellen Kriminalitätsentwicklung und der besonderen Bedeutung des Telekommunikationsverkehrs in diesem Bereich gegenläufige Richtung und reguliert eine ermittlungstechnisch isoliert betrachtet wenig Erfolg versprechende Ermittlungsmethode unter dem Deckmantel des Grundrechtsschutzes in einem weitgehend unbedeutenden und eingriffsschwachen Bereich der Bestandsdatenauskunft erheblich nach. Der Zugriff auf Bestandsdaten, welcher zwar grundsätzlich als verfassungsrechtlich zulässig angesehen wird, genügt in der Form des § 113 TKG jedenfalls nicht den nun doch strengeren Anforderungen des BVerfG an die Verhältnismäßigkeit eines solchen Eingriffs vor dem Hintergrund des Art. 10 Abs. 1 GG und des aus dem Persönlichkeitsrecht wurzelnden Rechts auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Die entsprechend fachgesetzlichen Abrufnormen im Sinne des Doppeltürenmodells stellen ebenfalls keine hinreichend verhältnismäßigen Eingriffsschwellen auf und genügen auch in weiten Teilen nicht der erforderlichen Normenklarheit und Bestimmtheit. Ebenso mangelt es in Bezug auf die Abfrage auf Grundlage der Auswertung von Verkehrsdaten an hinreichenden verfahrenssichernden Dokumentationspflichten seitens der Auskunftsersuchenden Behörde, wenngleich das Gericht die geringe Eingriffsintensität der manuellen Bestandsdatenabfrage mehrfach betont.

Keinen verfassungsrechtlichen Bedenken unterliegt die Bestandsdatenauskunft des § 113 TKG als solche, womit diese verfassungsrechtlich zulässig zum herkömmlichen Instrumentarium der Sicherheitsbehörden gezählt werden kann Die Kritik des Verfassungsgerichts an der legislativen Ausgestaltung bezieht sich zunächst auf die Eingriffsschwellen der Übermittlungsnorm des § 113 TKG und der mangelnden Begrenzung der Übermittlungsbefugnis sowie der fehlenden spezifisch einzelfallbezogenen Stellung des Auskunftsersuchens und der gebundenen Weiterverwendung. § 113 TKG stellt sich in diesem Zusammenhang als unverhältnismäßig dar und wird insbesondere den verfassungsrechtlichen Anforderungen an die erste Türe des Doppeltürenmodells nicht gerecht. Das

BVerfG hat in seiner Entscheidung klargestellt, dass beide Türen spezifische und hinreichend bestimmte Eingriffsschwellen sowie den Verwendungszweck der zu beauskunftenden Bestandsdaten abschließend schon durch die Übermittlungsnorm vorgeben müssen. Mit Blick auf § 113 TKG insbesondere auch aus der Erwägung heraus, dass die darin vorgesehene Ermächtigung zum Datenabruf durch Sicherheitsbehörden der Länder die abschließend genutzte Gesetzgebungskompetenz des Bundes aus Art. 73 Abs. 1 Nr. 7 GG in Bezug auf § 113 TKG nicht aushöhlen darf. Fehlen der Übermittlungsbefugnis ihrerseits Begrenzungen hinsichtlich des beabsichtigten Verwendungszwecks und konkrete Eingriffsschwellen zum Erheben der Daten, können die Länder die Bestandsdatenauskunft in gewisser Hinsicht zu jedem legitimen Zweck fachgesetzlich zulassen, ohne den von § 113 TKG forcierten Rechtsgüterschutz zu beachten. Hierdurch hat das BVerfG klargestellt, dass eine entsprechend fachgesetzlich geregelte Auskunftsbefugnis der Länder, welche ihrerseits als zweite Türe in die durch § 113 TKG geöffneten Daten aufschlägt, nicht über die Voraussetzungen der bundesgesetzlichen Öffnungsnorm hinausgehen kann. Insoweit muss schon die bildlich erste Türe in vollem Umfang den Maßstäben der Verhältnismäßigkeit sowohl hinsichtlich der Eingriffsschwelle, der Zweckbindung als auch eines hinreichend bestimmten Rechtsgüterschutzes gerecht werden; diesen Anforderungen genügt § 113 TKG im Einzelnen nicht. Die ebenfalls in § 113 Abs. 1 S. 3 TKG geregelte Übermittlung der aus den ausgewerteten Verkehrsdaten gewonnenen dynamischen IP-Adressen stellt sich als unverhältnismäßig dar, da es sowohl an einer hinreichenden Eingriffsschwelle als auch an einer spezifischen Zweckbindung der erhobenen Daten mangelt. Insbesondere muss dem erhöhten Eingriffsgewicht dieser Daten durch einen hervorgehobenen Rechtsgüterschutz Rechnung getragen werden. Gleiches gilt mit Blick auf § 113 Abs. 1. S. 2 TKG, welcher die Übermittlung von Zugangsdaten im Rahmen einer Bestandsdatenabfrage gestattet.

Auch die fachgesetzlichen Zugriffsermächtigungen entsprechen ausweislich der Entscheidung weitgehend nicht den Anforderungen an die Verhältnismäßigkeit, die Bestimmtheit sowie Normenklarheit. Insbesondere mangelt es an konkretisierten Eingriffsschwellen, welche sich insbesondere nicht in einem Verweis auf die durch die entsprechende Sicherheitsbehörde allgemein wahrgenommenen Aufgaben erschöpfen dürfen. Auch ist ein Bezug zu den durch die Abfrage geschützten Rechtsgüter erforderlich, da sich die Verhältnismäßigkeit unmittelbar aus der Abwägung zwischen der informationellen Selbstbestimmung des Betroffenen, des Telekommunikationsgeheimnisses und dem durch die Auskunft geschützten Rechtsgut ergibt. Auch wenn das BVerfG die Eingriffsqualität gerade mit Blick auf die gegenständliche Bestandsdatenabfrage als grundsätzlich geringfügig einstuft, genügen die in den Abrufnormen angelegten Eingriffsschwellen – sofern überhaupt von der Existenz solcher gesprochen werden kann – weitgehend nicht. Insbesondere mangelt es einigen Normen auch an einer spezifischen Beschränkung auf den Einzelfall, was den inflationären Gebrauch der Auskunftsbefugnisse verhindern soll. Das BVerfG legt in dieser Frage den individuellen Grundrechtsschutz gegenüber den doch größtenteils verfolgten gewichtigen Interessen des Rechtsgüterschutzes entsprechender Abfragen sehr weit aus und fordert sowohl sehr konkrete Tatsachen, die eine entsprechende Auskunft rechtfertigen, als auch hinreichende verfahrenstechnische Maßnahmen, um die verletzten Grundrechte des Betroffenen ausreichend zu schützen. Ebenso weisen einige Normen Defizite hinsichtlich der Begrenzung des Verwendungszwecks der übermittelten und abgefragten Daten auf.

Eine aus der Entscheidung besonders hervorzuhebenden Thematik zeigt sich in der Bestandsdatenabfrage, welche sich der Auswertung dynamischer IP-Adressen bedient. Während das BVerfG schon in der ersten Entscheidung zur Bestandsdatenabfrage die Auswertung von dynamischen IP-Adressen, welche als Verkehrsdatenauswertung einzuordnen ist, vor den Hintergrund des Telekommunikationsgeheimnisses aus Art. 10 Abs. 1 GG gerückt ha, stellt der jüngste Beschluss die gegenüber den anderen Bestandsdaten bestehende erhöhten Verhältnismäßigkeitsanforderungen nochmals deutlich heraus. Das BVerfG stellt die „Aufhebung der Anonymität des Internets“ damit in eine andere grundrechtliche Ausleuchtung und erhebt eine nicht nur rechtspolitisch, sondern auch gesellschaftlich umstrittene Frage in einen nicht ungefährlichen Nahbereich des Grundrechtsschutzes.

Die rechtliche Würdigung der Bestandsdatenauskunft in Bezug auf dynamische IP-Adressen ist eine ergebnisorientierte Betrachtung, die eine ausgewertete dynamisch zugewiesene IP-Adresse als Bestandsdatum ansieht. Da die auskunftsersuchende Behörde nicht in die Auswertung der Verkehrsdaten eingebunden ist, liegt mithin keine Verkehrsdatenabfrage vor. Die Bestandsdatenabfrage bedient sich lediglich einer durch den Dienstanbieter extern zu leistenden Auswertung entsprechender Verkehrsdaten gem. § 96 TKG, mit welcher die auskunftsersuchende Behörde nicht in Berührung kommt; diese erhält lediglich die Auskunft über eine ermittelte IP-Adresse, welche sich insoweit nicht wesentlich von einer statisch zugewiesenen IP-Adresse unterscheidet, welche zweifelsohne als Bestandsdatum eingestuft wird.

Zugangsdaten nach § 113 Abs. 1 S. 2 TKG eine Besonderheit dar, da diese den Zugang zu Endgeräten und Speichereinrichtungen ermöglichen; der spezifische Verwendungszweck der Daten also schon aus der Natur des Datums heraus über den sonst eher informatorischen Charakter der Bestandsdaten hinausgeht. Die Bestandsdatenabfrage in Bezug auf die Zugangsdaten begegnet weder aus der Übermittlungsbefugnis des § 113 Abs. 1 S. 2 TKG noch aus den fachgesetzlichen Abrufnormen besonderen Bedenken seitens des BVerfG. Dabei wird jedoch die Einordnung vor dem Grundrecht der Vertraulichkeit und Integrität informationstechnischer Systeme (Computergrundrecht) weitgehend verkannt. Dieses durch das BVerfG geschaffene Grundrecht schützt das Vertrauen, das ein Nutzer entsprechend komplexer Systeme in das System selbst, als auch in die Vernetzung entsprechender Systeme und die im System oder zwischen den Systemen ablaufende Datenverarbeitung und deren Schutz vor unbefugtem Zugriff Dritter setzt. Hierbei stellt sich das geschützte Vertrauen als Ausprägung des allgemeinen Persönlichkeitsrechts und der damit verbundenen Privatsphäre dar, was insoweit zu der umstrittenen Frage führt, ob es dieser Ausprägung des allgemeinen Persönlichkeitsrechts überhaupt bedürft hätte. Auch wenn das BVerfG im Abgreifen der Daten durch das Instrument der Bestandsdatenauskunft augenscheinlich keinen Eingriff in die grundrechtlich geschützte Integritätserwartung sieht, sind die wesentlichen Hürden für einen Zugriff und Bruch der Integrität dadurch jedenfalls genommen, um sich behördenseitig Zugang zu dem entsprechenden System zu verschaffen. Während der tatsächliche Zugriff jedenfalls einen derartigen Eingriff begründet, verletzt gerade schon das Innehaben von Zugangsdaten durch Nichtberechtigte, in diesem Fall durch den Staat als entsprechende Sicherheitsbehörde, die Integritätserwartung, die der Betroffenen in das von ihm genutzte System legt. Die Forderungen der Konnexität zum Vorliegen der Verwendungsvoraussetzungen der Daten belegt dies. Somit liegt schon durch die Abfrage entsprechender Daten ein Eingriff in die Integrität eines informationstechnischen Systems vor, was das Gericht in diesem Zusammenhang verkannt hat. Gleichwohl gelten für die Verhältnismäßigkeit des Eingriffs ähnliche Voraussetzungen, auch wenn mit Blick auf die Verwendung der Daten, welche zumeist an einen entsprechenden Richtervorbehalt oder zumindest einen der Sache nach gleichwertigen Ersatz geknüpft ist, die Rechtfertigungslast einer derartigen Abfrage in jedem Fall nicht hinter den Maßstäben für die herkömmliche Bestandsdatenabfrage zurückbleiben kann.

Der jüngste Beschluss des BVerfG hat die schon geltenden Maßstäbe nun in drei Punkten erheblich konkretisiert: Dies betrifft erstens die Eingriffsschwellen zur Abfrage und Weiterleitung der Daten sowie die damit korrespondierende Zweckbindung bezogen auf die Verwendung, zweitens die Verhältnismäßigkeit der Auskunftsersuchen insbesondere durch den Grundsatz der Normenklarheit und Bestimmtheit ausgehend vom Rechtsgüterschutz und drittens die Verfahrensanforderungen insbesondere in Bezug auf die Bestandsdatenabfrage mittels Auswertung dynamischer IP-Adressen.

Eine der wesentlichen Aussagen der Entscheidung ist die umfassend geforderte normenklare Zweckbindung der Bestandsdatenauskunft, welche sich nicht in einem Verweis auf die allgemeine Aufgabenzuständigkeit der entsprechenden Sicherheitsbehörde erschöpfen darf, sondern bereichsspezifisch und weitgehend konkretisiert werden muss. Damit wird die Bestandsdatenabfrage enger als bisher an den Grundsatz der Zweckbindung geknüpft und die Eingriffsschwellen konkretisiert.

Die Abfrage von Bestandsdaten bei Nichtbetroffenen aus dem Umfeld des Betroffenen genügt mithin den Anforderungen der Verfassung. Dabei lässt das BVerfG die spezifisch geforderte Nähebeziehung ausreichen, um einen Datenabruf auch gegenüber Nichtbetroffenen zuzulassen. Aufgrund der Notwendigkeit einer entsprechenden Datenabfrage im Vorfeld konkreter Gefahren und des Umstands einer allgemeinen Vorverlagerung der Gefahr stellt das BVerfG explizite Anforderungen an die Prognostizierbarkeit der zu erwartenden Geschehensabläufe. Allgemein ist nur das Vorliegen einer konkreten Gefahr respektive eines konkreten Gefahrenverdachts als verhältnismäßige Eingriffsschwelle zu begreifen, was insoweit auch schon in der ersten Entscheidung des BVerfG zur Bestandsdatenabfrage so im Wege der Auslegung des § 113 TKG a.F. angeklungen ist. Sind entsprechend konkrete Voraussetzungen des Eingriffs nicht in der Norm angelegt erweist sich die Abrufnorm dadurch zwar nicht per se als unverhältnismäßig, jedoch müssen sodann die in Rede stehenden Schutzgüter von proportional höherem (hervorgehobenem) Gewicht sein, was das BVerfG insbesondere in Bezug auf die Auswertung dynamischer IP-Adressen durch die Dienstanbieter fordert.

Das Spannungsfeld zwischen dem staatlichen Interesse einer möglichst effektiven und zeitgemäßen Gefahrenabwehr und Straftatenbekämpfung und dem Grundrechtsschutz wurde durch die Entscheidung zumindest hinsichtlich der Verhältnismäßigkeitsabwägung entladen. Insbesondere das Eingriffsgewicht bezogen auf die manuelle Bestandsdatenauskunft und das Recht auf informationelle Selbstbestimmung des Betroffenen wurden dabei konkretisiert und aktualisiert. Das BVerfG hat das Eingriffsgewicht der Bestandsdatenauskunft zwar als überwiegend gering eingestuft, allerdings die dennoch bestehenden Anforderungen eines effektiven Grundrechtsschutzes herausgestellt und dem Gesetzgeber eine konkret legislative Würdigung dieser Belange auferlegt. Dies begründet das Gericht insbesondere mit dem großen Spektrum der in §§ 95 und 111 TKG abrufbaren Daten. Damit führt die Entscheidung das Gebot der Zweckbindung, das Gebot der Verhältnismäßigkeit und das Gebot der Normenklarheit und Bestimmtheit zu einer durch den Gesetzgeber nun neu zu bestimmenden Einheit zusammen. Die unterschiedlichen Bestandsdaten unterliegen dabei nicht alle demselben Eingriffsgewicht, weshalb eine Differenzierung der Verhältnismäßigkeitsmaßstäbe durch verschiedene Parameter, wie bspw. Verfahrensanordnungen in Bezug auf die Abfrage dynamischer IP-Adressen oder die Beschränkung auf entsprechende Verwendungszwecke oder die Bindung an einen hervorgehobenen Rechtsgüterschutz in einer differenzierten Betrachtung der einzelnen Abfragen samt konkreten Abfragegegenständen geboten ist. Die Entscheidung zeigt, dass die durch die Bestandsdatenauskunft geschützten Rechtsgüter schon in der Norm den entsprechenden grundrechtlichen Schutzgehalten gegenübergestellt werden müssen und so eine Verhältnismäßigkeitsprüfung innerhalb der Norm weitgehend abschließend zulassen. Damit fordert das BVerfG den Gesetzgeber auf, den Sicherheitsbehörden durch die Gesetzgebung entsprechend klare Vorgaben zu geben, um schon von legislativer Seite eine möglichst hinreichende Wahrung der Grundrechte der Betroffenen sicherzustellen. Dies erschließt sich insbesondere vor dem Hintergrund, dass gerade in Bezug auf manuelle Auskunftsverfahren auch private Dritte zur Datenübermittlung durch entsprechende fachgesetzliche Abrufnormen herangezogen werden können und deshalb Rechtssicherheit für alle Beteiligten bestehen muss. Ein wesentliches Anliegen ist wohl auch für den Übermittlungsverpflichteten eine hinreichende Überprüfungsmöglichkeit der Rechtmäßigkeit eines entsprechenden Auskunftsersuchens zu schaffen.

Während die verfahrenstechnischen Anforderungen an die Bestandsdatenauskunft durch das BVerfG in der Entscheidung weitgehend nicht bemängelt wurden, besteht demgegenüber in Zusammenhang mit der Abfrage einer dynamischen IP-Adresse noch Nachbesserungsbedarf, da die überwiegenden Verfahrensanforderungen nicht verhältnismäßig sind. Die die Auswertung von Verkehrsdaten voraussetzende Abfrage dynamischer IP-Adressen zur Zuordnung eines Anschlusses muss ihrerseits durch die auskunftsersuchende Behörde so hinreichend dokumentiert werden, dass der Auskunftsverpflichtete Anbieter von Telekommunikationsdiensten das Vorliegen der Voraussetzungen der Auskunftsverpflichtung nachvollziehen kann. Damit stellt das BVerfG klar, dass die Auswertung der Verkehrsdaten über den bloßen Abruf eines üblichen Bestandsdatums hinausgeht, auch wenn die auskunftsersuchende Behörde an der Auswertung nicht beteiligt ist, der Eingriff in die dem Telekommunikationsge-

heimnis des Art. 10 Abs. 1 GG unterfallenden Daten jedenfalls nachvollziehbar zulässig sein muss. Einen Richtervorbehalt fordert das BVerfG gleichwohl nicht, da das Ergebnis der Auswertung selbst nicht als Verkehrsdatum einzustufen ist und der Informationsgehalt dennoch und tatsächlich relativ isoliert bleibt und keine weitergehenden dynamischen Rückschlüsse und den Verkehrsdaten wesensimmanente Bewegungs- und Inhaltsdaten zulässt.

Durch die *Bestandsdaten II Entscheidung* hat das BVerfG insgesamt die Maßstäbe an Übermittlungs- und Abrufnormen in sehr klarer und deutlicher Weise konkretisiert und die Gestaltungsspielräume des Gesetzgebers klar vorgezeichnet. Unmissverständlich klar ist, dass schon die Übermittlungsnorm des § 113 TKG sowohl hinsichtlich der Eingriffsschwellen als auch der beabsichtigten Verwendungszwecke der zu übermittelnden Bestandsdaten normenklare und bestimmte Vorgaben treffen muss, da es nicht allein in der Hand des Bundes liegt, zu welchen Zwecken die zu beauskunftenden Daten verwendet werden. Hierin liegt insbesondere bezogen auf § 113 TKG ein Anpassungsbedarf durch den Bundesgesetzgeber.

Darüber hinaus fehlt es den Abrufnormen der die Sicherheitsbehörden des Bundes ermächtigenden Fachgesetzen an verhältnismäßigen Eingriffsschwellen, die eine Abwägung zwischen den verletzten Grundrechten des Betroffenen und den mit der Abfrage geschützten Rechtsgütern verfassungskonform zulässt und einzelfallspezifisch einschränken. Klargestellt hat das BVerfG darüber hinaus, dass aus den Abrufnormen in transparenter Weise hervorgehen muss, welche Behörde zum Abruf der Daten befugt ist und hinsichtlich der Anforderungen an einen Datenabruf ein möglichst geringes Maß an Normauslegung erforderlich sein muss. Die Abrufnorm muss vielmehr weit überwiegend aus sich selbst heraus die Vorgaben für einen verhältnismäßigen Zugriff auf entsprechende Daten enthalten. Die sonst in den Fachgesetzen übliche und umfassende Verweisung auf Eingriffsschwellen anderer Befugnisse und der salvatorische Rückbezug auf die allgemeine Aufgabenbeschreibung der jeweiligen Behörde genügt nicht den verfassungsrechtlichen Anforderungen.

III. Die notwendigen Anpassungen im Gesetzentwurf und ihrer Bewertung

Die Entscheidung des Bundesverfassungsgerichts vom 27.5.2020 hat sowohl auf Bundes- als auch auf Landesebene zur Notwendigkeit einer Reparatur einer Vielzahl fachgesetzlicher Abrufnormen aber vor allem auch der Übermittlungsnormen auf Bundesebene (namentlich der Bestimmungen des TMG und des TKG) im manuellen Auskunftsverfahren geführt.

Als Ergebnis einer – in Ansehung der zur Verfügung stehenden Zeit von einer Woche allerdings nur kursorischen – Prüfung des Gesetzentwurfs können folgende Aussagen getroffen werden:

1. Wenngleich Telekommunikationsdaten und Telemediendaten unstreitig unterschiedlicher Natur gerade auch mit Blick auf die Sensibilität der entsprechenden Daten sind, so kann dem Gesetzgeber kein Vorwurf gemacht werden, er habe in nivellierender und damit unzulässiger Weise beide Datenkategorien gleichbehandelt. Gerade das durch den Gesetzgeber in den Übermittlungsregelungen der §§ 15a und 15b TMG einerseits und § 113 TKG andererseits gewählte Konzept lässt einen umfassenden und zugleich – sowohl nach Eingriffsvoraussetzungen als auch nach Rechtsgütern - abgestuften Zugriff auf die entsprechenden Daten zu. In Ansehung der unterschiedlichen – bereichsspezifisch und normenklar geregelten –Eingriffsvoraussetzungen und insbesondere unter Berücksichtigung der geringen Eingriffsintensität begegnen die Übermittlungsnormen keinen verfassungsrechtlichen Bedenken. Dies gilt sowohl für die Bestimmungen zur Übermittlung von und den Zugriff auf Bestandsdaten, aber auch für die Übermittlung und den Zugriff auf Nutzungsdaten

2. Keine Bedenken begegnet der Gesetzentwurf hinsichtlich der Zuordnung dynamischer IP-Adressen (§ 113 Abs. 1 Satz 3, Abs. 3 und Abs. 5 TKG); dies gilt auch in unionsrechtlicher Hinsicht. Die Regelungen entsprechen sowohl den Anforderungen des Bundesverfassungsgerichts als auch unionsrechtlichen Maßstäben, die indes

nicht unmittelbarer Maßstab der Gesetzgebung sind. Wenn aber auch nach der Rechtsprechung des EuGH die Übermittlung von und der Zugriff auf Bestandsdaten zur Identifizierung von Anschlussinhabern keinen schwerwiegenden Grundrechtseingriff darstellt und zur Verhütung , Ermittlung, Feststellung und Verfolgung von Straftaten statthaft ist und die Straftaten selbst nicht „schwerwiegend“ sein müssen, dann mag zwar die Nutzung bevorrateter IP-Adressen hier eine abweichende Behandlung und Wertung nach sich ziehen; zwingend ist dies indes nicht, da neben der Übermittlungsnorm im TKG auch immer die entsprechenden Abrufungsnormen in den Blick zu nehmen sind.

3. Als problematisch – aber nicht etwa als verfassungswidrig – erweist sich der Gesetzentwurf mit Blick auf die Implementierung des Begriffs der „drohenden“ Gefahr als Voraussetzung sowohl der Übermittlung als auch des Abrufs im Einzelfall. Dieser Begriff – über dessen normativen Gehalt man trefflich streiten kann – birgt zumindest das Risiko einer weiteren verfassungsgerichtlichen Auseinandersetzung (insoweit sei auf bereits anhängige Verfahren in Bayern nur verwiesen). Allerdings ist dem Gesetzentwurf dahingehend zuzustimmen, dass der Begriff der drohenden Gefahr gerade der Judikatur des Bundesverfassungsgerichts entstammt und der Bundesgesetzgeber mit dem hier vorliegenden Versuch auch keine Regelungsbefugnisse geschaffen hat, die ein Eingreifen in Kausalverläufe bei einer lediglich drohenden Gefahr rechtfertigen könnten. Vielmehr handelt es sich bei den in Rede stehenden Eingriffen um Grundrechtseingriffe geringer Intensität, sodass im Ergebnis auch die drohende Gefahr als Eingriffsvoraussetzung nicht zu einer Entgrenzung sicherheitsbehördlicher Befugnisse und damit zur Verfassungswidrigkeit der entsprechenden Regelung führt.

gez. Kyrill-A. Schwarz

JONAS BREYER
RECHTSANWALT
DATENSCHUTZBEAUFTRAGTER

Rechtsanwaltskanzlei Breyer
Schiersteiner Straße 37a
65187 Wiesbaden

Jonas Breyer
Rechtsanwalt
Datenschutzbeauftragter

T +49 611 141 056 89
F +49 611 141 056 90

jbreyer@ra-breyer.de
www.ra-breyer.de

Kanzlei Breyer • Schiersteiner Straße 37a • 65187 Wiesbaden

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin

22.01.2021

BT-Anhörung am 25.01.2021 (Bestandsdatenauskunft)

Sehr geehrte Damen und Herren,

nachfolgend übersende ich meine erbetene

Sachverständigen-Stellungnahme

im Rahmen der öffentlichen Anhörung zum Gesetzentwurf der Fraktionen der CDU/CSU und SPD „Entwurf eines Gesetzes zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020“ (BT-Drs. 19/25294).

Infolge der Kurzfristigkeit kann die Stellungnahme nur kursorischer Art sein.

Im vorgenannten Verfahren vor dem Bundesverfassungsgericht (1 BvR 1873/13 u. a.) habe ich die Beschwerdeführer anwaltlich vertreten. Der Regierungsentwurf behebt die rechtlichen Mängel auch im zweiten Anlauf nicht vollständig, sondern schafft stattdessen neue behördliche Befugnisse. Eine weitere Verfassungsbeschwerde ist daher absehbar.

Generell ist mit dem Bundesverfassungsgericht daran zu erinnern, dass der Schutz der Vertraulichkeit von Bestandsdaten von hoher Bedeutung ist, weil durch die Identifizierung eines Telefon- oder Internetnutzers die Anonymität der Telekommunikation durchbrochen wird. Durch die Identifizierung von Telefon- oder Internetkennungen lassen sich mittelbar Umstände und Inhalte von Telekommunikationsvorgängen individualisieren, etwa dann, wenn Inhalt oder Zeitpunkt eines bestimmten Anrufs, der unter der abgefragten Nummer geführt wurde, der Behörde durch Vorermittlungen bekannt ist (BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05, „Bestandsdatenauskunft I“, Rn. 114). Als Daten, die die Grundlagen von Telekommunikations-vorgängen betreffen, liegen Bestandsdaten deshalb im Umfeld verfassungsrechtlich besonders geschützter Informationsbeziehungen, deren Vertraulichkeit für eine freiheitliche Ordnung essentiell ist (BVerfG a. a. O., Rn. 137). Dem genügt der vorgelegte Regierungsentwurf nicht.

1. Konkrete Gefahr (Art. 1 [BVerfSchG], 3 [MADG] und 4 [BNDG])

In Bezug auf die Nachrichtendienste des Bundes (Art. 1, 3 und 4 des Änderungsgesetzes) fehlt das Erfordernis einer konkreten oder zumindest drohenden Gefahr für ein spezifiziertes Rechtsgut (Rn. 146 ff. der Entscheidung v. 27.05.2020 – 1 BvR 1873/13 u. a., „Bestandsdatenauskunft II“, nachfolgend „Entscheidung“). Der Entwurf stellt nur auf die vage formulierten Aufgaben der Nachrichtendienste ab. Die amtliche Begründung führt dazu aus, die Nachrichtendienste bezweckten ohnehin den Schutz besonders gewichtiger Rechtsgüter. Diese geringen Anforderungen an den zu normierenden Rechtsgüterschutz lässt das Bundesverfassungsgericht aber nur dann genügen, wenn die

> *„Auskunft zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten ist“,*

weil damit ein

> *„wenigstens der Art nach konkretisiertes und absehbares Geschehen vorausgesetzt“*

werde (Rn. 151 der Entscheidung). Ein solches konkretes Geschehen ergibt sich nicht pauschal aus der allgemeinen Aufgabenbeschreibung gemäß § 3 Abs. 1 BVerfSchG und den fachrechtlichen Parallelvorschriften. Ebenso wenig wird eine Störereigenschaft vorausgesetzt. In eine ähnliche Richtung gehen auch die Bedenken des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), denen ich mich anschließe.

Als Folgeänderung sind auch die korrespondierenden Übermittlungsregelungen anzupassen.

2. Konkrete Gefahr bei IP-Adressen (Art. 1 [BVerfSchG], 3 [MADG] und 4 [BNDG])

Die Vorschriften für die Nachrichtendienste ermöglichen Bestandsdatenauskünfte auch dann, wenn sie anhand von dynamisch zugeteilten IP-Adressen erteilt werden. Dabei wird auf das Vorliegen einer konkreten Gefahr verzichtet. Wegen des „erhöhten Eingriffsgewichts“ einer solchen Abfrage ist das aber erforderlich und zwar auch für Nachrichtendienste (Rn. 176 der Entscheidung). Zwar bezieht sich das Bundesverfassungsgericht hierbei auf eine Übermittlungsnorm, im konkreten Fall § 113 Abs. 1 TKG. Die Abrufnorm darf aber nicht darüber hinausgehen, anderenfalls ist bereits die Übermittlung unzulässig (Rn. 201 der Entscheidung). Der Entwurf treibt damit sowohl Behörden als auch Diensteanbieter in den Rechtsverstoß.

3. „Mitwirkung an der Mitwirkung“ (Art. 1 [BVerfSchG], 3 [MADG] und 4 [BNDG], 6 [BPolG], 7 [BKAG], 8 [StPO] und 11 [ZFdG])

Der Gesetzentwurf verpflichtet in mehreren Vorschriften, nicht nur bezüglich der Nachrichtendienste, auch diejenigen, die an der Erbringung von Telekommunikationsdiensten „mitwirken“. Wer an Telekommunikationsdiensten mitwirkt, ist aber bereits Telekommunikationsanbieter (§ 3 Nr. 6 TKG). Der Entwurf regelt insoweit eine „Mitwirkung an der Mitwirkung“.

4. Unbestimmte Eingriffsschwellen (Art. 6 [BPolG], 7 [BKAG], 11 [ZfdG], 12 [TMG] und 13 [TKG])

Der Entwurf knüpft an mehreren Stellen die Bestandsdatenauskunft, auch anhand von dynamischen IP-Adressen, an bedrohte

- Rechtsgüter von erheblichem Gewicht,
- Rechtsgüter von hervorgehobenem Gewicht,
- gewichtige Rechtsgüter und
- besonders gewichtige Rechtsgüter.

Diese Terminologie wird zwar vom Bundesverfassungsgericht aus verfassungsrechtlicher Perspektive verwendet, worauf auch die amtliche Begründung verweist (Seite 51). Auch nach der Rechtsprechung des Bundesverfassungsgerichts ist die Zuordnung einzelner Rechtsverstöße zu den jeweiligen Rechtsgütern aber unkonturiert und für den Rechtsanwender unklar. Dabei sollte das Rechtsgut gerade bei den nicht nachrichtendienstlichen Gefahrenabwehrbehörden einzugrenzen sein. Teilweise spricht der Entwurf sogar nur von einer „Gefahr", ohne irgendein Rechtsgut zu nennen, etwa in § 40 BKAG-E. Entsprechendes gilt für Straftaten von „erheblicher Bedeutung".

Es ist nicht Aufgabe der Gerichte, sondern des Gesetzgebers, zu prüfen und zu artikulieren, wofür er die begehrten Bestandsdatenauskünfte benötigt. Dabei kann er zur Vereinfachung auf bestehende Kataloge wie § 100a Abs. 2 StPO zurückgreifen. Kann der Gesetzgeber nicht artikulieren, wozu er die Daten benötigt, sind sie auch nicht erforderlich und die Regelungen sind nicht nur dysfunktional, da unbestimmt, sondern auch unverhältnismäßig.

5. Fehlende Erforderlichkeit (Art. 11 [ZFdG], 12 [TMG] und 13 [TKG])

Nach mehreren Normen muss eine Auskunftsverlangen die Abwehr einer Gefahr nur „zum Gegenstand" haben. Richtigerweise muss sie dafür erforderlich sein. Eine Bezugnahme auf die allgemeinen Aufgaben einer Behörde würde eine Vorratsspeicherung ermöglichen und genügt daher nicht (Rn. 197 der Entscheidung).

6. Zeitlich absehbares Geschehen (Art. 6 [BPolG], 7 [BKAG], 11 [ZFdG], 12 [TMG] und 13 [TKG])

In den genannten Vorschriften knüpft der Entwurf Eingriffe daran, dass

> *„Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, an dem bestimmte Personen beteiligt sein werden".*

Diese abstrakte Formel wurde aus der Entscheidung des Bundesverfassungsgerichts kopiert (etwa Rn. 148 der Entscheidung). Es ist Aufgabe des Gesetzgebers, sie politisch mit Leben zu füllen und den Zeitfaktor, das Geschehen und die beteiligten Personen konkret zu bestimmen. Anderenfalls drohen erhebliche Rechtsunsicherheit und rechtswidrige Datenverarbeitungen.

7. Unklare Übermittlungsregelungen (Art. 12 [TMG] und 13 [TKG])

Der Entwurf lässt den Rechtsanwender darüber im Unklaren, wie sich die neuen Übermittlungsnormen in §§ 15a, b TMG-E zu den bisherigen Übermittlungsregelungen in § 14 TMG verhalten, die ebenfalls Auskünfte zur Gefahrenabwehr und Strafverfolgung regeln.

Daneben verlangt §15a Abs. 2 TMG-E eine „elektronische“ Bestätigung. Es bleibt unklar, ob beispielsweise die elektronische Form nach § 126a BGB oder nach § 3a VwVfG gemeint ist.

Der Entwurf regelt zudem zwar theoretisch, dass eine Übermittlung nur erfolgen darf, wenn die Voraussetzungen der Abrufnorm erfüllt sind (§ 15a Abs. 6 TMG-E). Nur dann ist die Übermittlung zulässig (Rn. 201 der Entscheidung). Mangels Information hat der Diensteanbieter aber keine Möglichkeit, das Vorliegen der Voraussetzungen zu prüfen, was das verfassungsrechtliche Prinzip der Doppeltür aushöhlt. Auch bei einer Beschlagnahme muss ein überprüfbarer Beschluss vorgelegt werden. Die Diensteanbieter sollten bei dieser Prüfung unterstützt werden, zumal es sich gerade im Bereich von Telemedien überwiegend um Kleinunternehmer und Privatpersonen handelt. Es sollte daher nach § 15a Abs. 2 Satz 1 TMG-E folgender Satz eingefügt werden:

> *„Die ersuchende Stelle hat auch die ernstlich in Betracht kommenden rechtlichen Auskunftstatbestände unter Zitierung der jeweiligen Norm dieses Gesetzes und kurz den zur Prüfung erforderlichen Sachverhalt anzugeben sowie gegebenenfalls die gerichtliche Anordnung zu übermitteln.“*

Zwar hat das Bundesverfassungsgericht entschieden, auch das Vorliegen der Übermittlungs-Voraussetzungen müsse durch die jeweilige Abrufbehörde geprüft werden. Das hat das Gericht aber nicht verfassungsrechtlich, sondern nur anhand des fachrechtlichen Status quo in § 113 TKG begründet (Rn. 202 der Entscheidung).

Soweit § 15a Abs. 6 TMG-E eine Prüfung durch „Fachkräfte“ vorsieht, ist dies lebensfern und sollte dies gestrichen werden. Die Vorstellung, dass es sich etwa bei Betreibern von Websites mehrheitlich um große Anbieter wie Facebook handelt, entspricht nicht der Realität.

Entsprechende Vorschriften wie im TMG-E befinden sich im TKG-E.

8. Nutzungsdaten (Art. 8 [StPO] und 12 [TMG])

Der Gesetzentwurf verpflichtet Anbieter sozialer Netzwerke und anderer Telemediendienste, Auskunft über Bestands- und sogar Nutzungsdaten zu erteilen. Er wird der Tiefe des damit verbundenen Grundrechtseingriffs jedoch nicht gerecht. Möglich ist etwa die Zurückverfolgung der gesamten Aktivitäten eines Benutzers, indem ein Pseudonym in einem Meinungsforum oder sozialen Netzwerk aufgedeckt wird. Gespeichert werden bei solchen Diensten teilweise auch Bestandsdaten wie Krankheiten, sexuelle Orientierung oder Religion, etwa bei Selbsthilfeforen. Denkbar wäre auch eine Verknüpfung anhand sogenannter Browser-Fingerprints, also pseudonym- und sogar personenübergreifender Profile. Anders als in § 100b StPO muss die Stelle nicht einmal einen bestimmten Nutzer nennen, sodass ungezielt Auskünfte über alle Nutzer verlangt werden können. Privilegierungen für Berufsgeheimnisträger oder Presseinformanten fehlen.

Telemedien-Nutzungsdaten beantworten beispielsweise folgende Fragen:

- Welche Internetseiten hat ein Nutzer aufgerufen?
- Welche Suchbegriffe hat er in eine Suchmaschine eingegeben?
- Welche Online-Videos hat er gesehen oder selbst veröffentlicht?
- Welche Artikel welcher politischen Online-Zeitungen hat er abgerufen?
- Welche Nachrichten hat er in einem Online-Chat geschrieben und gelesen?
- Was hat er in einem geschlossenen Aidshilfe- oder Gewerkschaftsforum geschrieben?

Nutzungsdaten sind Telekommunikationsinhalten auch deshalb vergleichbar, weil sie regelmäßig den Inhalt der abgerufenen Informationen erkennen lassen (etwa URLs der gelesenen Internetseiten). Sie können sogar aussagekräftiger sein, da Telefongespräche nicht fixiert werden. Bei der Diskussion über die Praktiken der NSA ist deutlich geworden, dass die im Internet anfallenden „Metadaten“ sogar eine weiter reichende Durchleuchtung unseres Lebens erlauben als eine Auswertung des Inhalts von Individualkommunikation. Ihre automatisierte Zusammenführung ermöglicht die Erstellung umfassender Persönlichkeitsprofile.

Dementsprechend müssen Abruf- und Übermittlungsnormen formell und materiell denselben verfassungsrechtlichen Anforderungen genügen wie die Telekommunikationsüberwachung. Diese ist nur unter engen Voraussetzungen zulässig. Es ist nicht ersichtlich, warum die staatliche Befugnis zur Offenlegung der Internetnutzung weiter reichen dürfte als die Befugnis zur Offenlegung der Telefonnutzung. Im Bereich der Strafverfolgung wären daher die Anforderungen der §§ 100a, b StPO einzuhalten. Im polizeilichen Bereich hat das Bundesverfassungsgericht die Voraussetzungen einer verhältnismäßigen Befugnis zur Telekommunikationsüberwachung bereits geklärt (Az. 1 BvR 668/04), unter anderem bedarf es einer konkreten Gefahr. Im Bereich der Nachrichtendienste wäre eine Öffnung allenfalls unter den Voraussetzungen, in dem Verfahren und nach Maßgabe des G10-Gesetzes denkbar, wobei die Erforderlichkeit nicht ersichtlich ist. Dass verschiedene im Entwurf vorgesehene Abrufnormen an Telemedien- und Telekommunikations-Bestanddaten dieselben Anforderungen stellen, genügt nicht annähernd. Auch fehlt es dem geänderten § 100g StPO an einem abschließenden Straftatenkatalog, wie bei der Telekommunikationsüberwachung erforderlich. Der Kritik des Sachverständigen Prof. Dr. Bäcker ist hier zuzustimmen.

Telemedien ersetzen die klassischen Medien immer mehr und sind in vielen Bereichen unseres Lebens unverzichtbar geworden (etwa Internet-Steuererklärung für Unternehmer). Sie sind vielfach Voraussetzung für die Ausübung grundrechtlich geschützter Freiheiten, besonders des Rechts, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten (Art. 5 GG). Nur umfassende Informationen, die man ungehindert und unbefangen zur Kenntnis nehmen kann, ermöglichen eine freie Meinungsbildung und -äußerung für Einzelne wie für die Gemeinschaft. Nur auf der Grundlage eines freien und unbefangenen Informationszugangs kann der Bürger informiert politisch entscheiden und am freiheitlichen demokratischen Gemeinwesen mitwirken.

Der staatliche Zugriff auf Telemediendaten schon nach bisherigem Recht ist Gegenstand einer weiteren Verfassungsbeschwerde (Az. 1 BvR 1732/14). Der Gesetzentwurf sollte bezüglich der Beauskunftung von Telemediendaten grundsätzlich überdacht werden.

9. Abruf von Zugangsdaten (Art. 6 [BPolG], 7 [BKAG], 8 [StPO], 11 [ZfdG] und 12 [TMG])

Der Entwurf versucht erneut, den Behörden Zugangsdaten wie Passwörter zu verschaffen, ohne darzulegen, in wie vielen und in welchen Fällen neben den übrigen Befugnissen ein praktischer Bedarf danach besteht. Da ein Passwort regelmäßig mehrere Dienste schützt (etwa bieten bestimmte Telekommunikationsanbieter unter einem einheitlichen Kundenpasswort zugleich einen Cloud-Speicher an), drohen unzulässige Datenzugriffe.

Außerdem erweist sich der Entwurf auch hier in zahlreichen Fällen als dysfunktional. Es ist den Anbietern nämlich nach Art. 32 DS-GVO (Datensicherheit) untersagt, Passwörter im Klartext zu speichern, sodass diese nicht herausgegeben werden können. Stattdessen werden regelmäßig abgeleitete Hash-Werte gespeichert, deren Rückrechnung mathematisch unmöglich ist. Die Bedenken des BfDI sind insoweit korrekt. Außerdem müssen Anbieter nach Art. 32 DS-GVO für eine regelmäßige Änderung der Passwörter sorgen, sodass ihre Gültigkeit selbst bei Bekanntheit zeitnah abzulaufen droht. Da Art. 32 DS-GVO keine Öffnungsklausel kennt, können die Mitgliedstaaten dies auch nicht ändern. Der deutsche Gesetzgeber kann sich auch nicht dem Anwendungsbereich des europäischen Rechts entziehen. Denn der Europäische Gerichtshof hat im Zusammenhang mit der britischen Vorratsdatenspeicherung entschieden, dass eine alleinige Kompetenz der nationalen Mitgliedstaaten nach Art. 4 Abs. 2 EUV (nationale Sicherheit) jedenfalls dann nicht bestehe, wenn eine Datenverarbeitung zwar staatlichen Sicherheitszwecken diene, sie aber durch verpflichtete Privatanbieter erfolge (EuGH, Urt. v. 06.10.2020 – C-623/17, „Privacy International“, Rn. 30 ff.). Ähnliche Bedenken äußert zutreffend auch der Sachverständige Prof. Dr. Bäcker. Die Befugnisse bieten daher ein großes Schadpotential bei geringem Nutzen und sind als unverhältnismäßig zu streichen.

10. Fehlende Statistik (Art. 12 [TMG] und 13 [TKG])

Der Entwurf regelt keine statistischen Aufzeichnungspflichten, um die Erforderlichkeit manueller Bestandsdatenabfragen zu prüfen, obwohl der Datenzugriff erneut ausgeweitet werden soll. Eine statistische Erfassung der staatlichen Bestandsdatenabfragen ist für eine wissenschaftliche Prüfung und öffentliche Kontrolle der Grundrechtseingriffe unerlässlich. Die Anzahl der getätigten Zugriffe muss der Öffentlichkeit zugänglich gemacht und transparent gemacht werden, damit das Ausmaß der Eingriffe für die Bürger nachvollziehbar sind. Auch die Entwicklung der Nutzung der Zugriffsbefugnisse kann so nachverfolgt werden, und es kann eine übergriffige Nutzung erkannt werden. Dazu ist es notwendig, derartige Daten genau nach Abfragegrund, abfragende Behörde und weiteren Daten aufzuschlüsseln. Zwar ist der Gesetzgeber nicht allgemein verpflichtet, Eingriffe in das Recht auf informationelle Selbstbestimmung statistisch erfassen zu lassen. Im vorliegenden Fall handelt es sich aber um Eingriffe in die Vertraulichkeit von Telekommunikationsverhältnissen, darunter die Identifizierung von Internetnutzern und die Anforderung von Codes zur Überwindung von Zugangssicherungen.

Aus dem verfassungsgerichtlichen Verfahren ist mir bekannt, dass, soweit denn Zahlen rekonstruiert werden konnten, sich etwa in den Jahren 2013 bis 2017 manuelle IP-Abfragen durch das BKA von 2001 auf 17428 Fälle vervielfacht haben, während Zugangsdatenabfragen

in den insoweit beauskunfteten Jahren 2016 bis 2018 durch den BND und den MAD in null Fällen erfolgten (undatierter Schriftsatz der Bundesregierung mit Gerichts-Eingangsstempel vom 24.12.2018). Für automatisierte Abfragen nach § 112 TKG besteht eine solche Statistik.

Dem sollte abgeholfen werden, indem in Anlehnung an den Quick-Freeze-Referentenentwurf des Bundesjustizministeriums eine Statistik über die Identifizierung von Internetnutzern geführt wird, sodass der Gesetzgeber die Entwicklung der Fallzahlen beobachten kann (§ 100k Abs. 4 StPO-Ref-E, „Gesetz zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet“). Es sollte daher folgender neuer Absatz in die jeweiligen Übermittlungsnormen (TMG, TKG) eingefügt werden:

> *„Über die Übermittlungen nach dieser Vorschrift erstellen der Bund und die Länder entsprechend § 101b der Strafprozessordnung jährlich eine Übersicht, in der anzugeben sind*
>
> 1. *die Anzahl der Verfahren, in denen Bestandsdaten übermittelt wurden,*
> 2. *die Anzahl der Verfahren, in denen Nutzungsdaten übermittelt wurden,*
> 3. *die Anzahl der Internetprotokoll-Adressen, zu denen um Auskunft ersucht wurde,*
> 4. *die Anzahl der Verfahren, in denen Passwörter oder andere Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, übermittelt wurden,*
>
> *jeweils unterschieden danach, durch welche Behörde und aufgrund welcher genauen fachrechtlichen Abrufvorschrift die Abrufe erfolgten, nach Festnetz-, Mobilfunk- und Internettelekommunikation, weiterhin im Fall der Nr. 3 nach dem Alter. Das Alter bestimmt sich danach, wie viele Tage zwischen dem Zeitpunkt der Anordnung und dem in der Anordnung genannten Zeitpunkt, zu dem die Internetprotokoll-Adresse vergeben war, liegen. In der nach dieser Vorschrift zu erstellenden Übersicht ist das Alter für den Zeitraum bis zu einer Woche taggenau, bis zu einem Monat wochenweise und für darüber hinausgehende Zeiträume monatsweise zu erfassen. Das Bundesamt für Justiz erstellt eine Gesamtübersicht zu den im Berichtsjahr bundesweit durchgeführten Übermittlungen, aufgeschlüsselt nach den vorgenannten Merkmalen, und veröffentlicht diese im Internet.“*

Mit freundlichem Gruß

Jonas Breyer
(Rechtsanwalt)

BUNDESRECHTSANWALTSKAMMER

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)697

Stellungnahme Nr. 75/2020
Dezember 2020

zum

Entwurf eines Gesetzes zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020

Mitglieder des Ausschusses Datenschutzrecht

RA Klaus Brisch, LL.M.
RA Michael Dreßler
RAin Simone Eckert
RA Prof. Dr. Armin Herb, (Vorsitzender)
RA Dr. Wulf Kamlah
RAin Simone Kolb
RA Jörg Martin Mathis
RA Dr. Hendrik Schöttle
RA Prof. Dr. Ralph Wagner, LL.M.

RA André Haug, Vizepräsident BRAK
RA Sebastian Aurich, LL.M., BRAK

Verteiler: Bundesministerium des Innern
Bundesministerium für Justiz und Verbraucherschutz
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte
Rechtsausschuss des Deutschen Bundestages
Arbeitskreise Recht der Bundestagsfraktionen
Landesjustizminister/Justizsenatoren der Länder
Rechtsanwaltskammern
Bundesnotarkammer
Bundessteuerberaterkammer
Bundesverband der Freien Berufe
Deutscher Anwaltverein
Deutscher Juristinnenbund
Deutscher Notarverein
Deutscher Richterbund
Neue Richtervereinigung e.V.
Patentanwaltskammer
Deutscher Steuerberaterverband e.V.
Wirtschaftsprüferkammer
Gesellschaft für Datenschutz und Datensicherheit e. V.
Berufsverband der Datenschutzbeauftragten Deutschlands e. V.
Deutsche Vereinigung für Datenschutz e. V.
Bitkom e. V.
davit – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e. V.
eco – Verband der Internetwirtschaft e. V.
VAUNET – Verband Privater Medien e. V.
Stiftung Datenschutz
Datenschutzberater
Computer und Recht
Redaktionen der NJW, ZAP, AnwBl, DRiZ, FamRZ, FAZ, Süddeutsche Zeitung, Die Welt, taz, Handelsblatt, dpa, Spiegel, Focus, Deubner Verlag Online Recht, Beck aktuell, Jurion Expertenbriefing, Juris Nachrichten, LexisNexis Rechtsnews, Otto Schmidt Verlag

Die Bundesrechtsanwaltskammer (BRAK) ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

I. Vorbemerkung

Die BRAK dankt für die Gelegenheit zur Stellungnahme. Die Stellungnahmefrist wurde leider – einmal mehr – so kurz bemessen, dass eine eingehende Prüfung dieses komplexen Gesetzgebungsvorhabens in der Kürze der Zeit nicht erfolgen konnte. Die BRAK bittet das BMI daher eindringlich, künftig angemessene Fristen vorzusehen. Einwöchige Rückmeldezeiträume sind rechtsstaatlich bedenklich und der Qualität der Gesetzgebungsvorhaben in der Regel nicht zuträglich. Angesichts der vom Bundesverfassungsgericht bis zum 31.12.2021 gesetzten Umsetzungsfrist erscheint die Kürze der Frist vorliegend nicht objektiv geboten. Die damit möglicherweise bezweckte Beschleunigung des Gesetzgebungsverfahrens ist gerade dann gefährdet, wenn etwaiger Verbesserungsbedarf aufgrund der begrenzten anfänglichen Öffentlichkeitsbeteiligung erst spät im Verfahren erkannt wird.

II. Stellungnahme

In der diesen Umständen geschuldeten Kürze nimmt die BRAK wie folgt zum dem Entwurf Stellung:

Das vom Bundesverfassungsgericht entwickelte „Doppeltür-Modell“, nach welchem die Auskunft fordernde Behörde einerseits und der Auskunft gebende TK-Dienstleister andererseits je einer eigenen Verantwortlichkeit mit entsprechend spezifischen Anforderungen unterliegt, wird in der Begründung zwar erwähnt. Sie ist im Entwurf aber nicht adäquat umgesetzt.

1. Kontrollmechanismen

Für beide Seiten (Behörden und TK-Dienstleister) beschreibt der Referentenentwurf – teils sehr abstrakt – rechtliche Voraussetzungen für die Datenverarbeitung. Erforderliche Kontrollmechanismen sind jedoch nicht erkennbar und im Referentenentwurf nicht vorgesehen. Da die Regelung den Bereich der Gefahrenabwehr betrifft, entfällt der strafprozessuale Richtervorbehalt. Es sind jedoch weitere Sicherheitsvorkehrungen notwendig. Diese könnten etwa darin bestehen, dass eine obligatorische Beteiligung der betrieblichen, beziehungsweise behördlichen Datenschutzbeauftragten erfolgt, beispielsweise im Sinne einer vereinfachten Folgenabschätzung (vgl. § 67 BDSG bzw. Art. 35 DSGVO). Zudem sollten die beteiligten Behörden der G 10-Kommission jährlich eine Statistik der Anwendungsfälle zuleiten.

2. Flankierende Informationspflichten

Der Gesetzentwurf regelt nur in § 22a Abs. 3 Satz 2 Bundespolizeigesetz und in § 10 Abs. 3 Satz 3 Zollfahndungsdienstgesetz eine amtsinterne Dokumentation der Vorgänge. Die Gesetzesbegründung (Seite 37 betreffend Bundespolizeigesetz und Seite 43 betreffend Zollfahndungsdienstgesetz) sieht darin die Ermöglichung einer Kontrolle durch Datenschutzbeauftragte und Verwaltungsgerichte. Dies würde aber voraussetzen, dass die Datenschutzbeauftragten und/oder betroffene Personen entsprechende Vorgänge aktiv suchen und dann Akteninhalte kontrollieren. Bei praxisnaher Betrachtung wird beides in den seltensten Fällen stattfinden. Die Dokumentationspflicht sollte daher um eine korrelierende unverzügliche Informationspflicht ergänzt werden.

3. Irreführende Regelung zu Verantwortlichkeit

Irreführend hinsichtlich der Verantwortungs-Bereiche sind die geplanten Regelungen in § 15a Abs. 2 Satz 5, § 15b Abs. 2 Satz 3 TMG, § 113 Abs. 2 Satz 5 TKG, wonach die Verantwortung für das Auskunftsverlangen und die weitere Datenverarbeitung durch die jeweilige Behörde nicht beim TK-Dienstleister, sondern bei der Behörde liegt. Diese Verantwortungs-Aufteilung ist selbstverständlich und bedarf keiner gesetzlichen Regelung. Die zitierten Stellen (TMG und TKG) inmitten der Normierung zur Auskunftserteilung durch die Dienstleister schaffen den unzutreffenden Eindruck, dass die Verantwortung des Dienstleisters für die Auskunftserteilung in irgendeiner Weise eingeschränkt sei. Gerade das „Doppeltür-Modell“ verlangt, dass der private Dienstleister die Erteilung der Auskunft nach den für ihn geltenden gesetzlichen Vorgaben eigenverantwortlich prüft und gestaltet. Eine spiegelbildliche Regelung für den behördlichen Bereich existiert – richtigerweise – nicht.

* * *