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.

(Prof. Dr. Markus Löffelmann)