Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)696 D

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.