L e i t s ä t z e

zum Beschluss des Ersten Senats vom 27. Mai 2020

- 1 BvR 1873/13 -
- 1 BvR 2618/13 -

(Bestandsdatenauskunft II)

1. Der Gesetzgeber muss bei der Einrichtung eines Auskunftsverfahrens auf Grundlage jeweils eigener Kompetenzen für sich genommen verhältnismäßige Rechtsgrundlagen sowohl für die Übermittlung als auch für den Abruf der Daten schaffen.

   Übermittlungs- und Abrufregelungen für Bestandsdaten von Telekommunikationsdiensteanbietern müssen die Verwendungszwecke der Daten hinreichend begrenzen, mithin die Datenverwendung an bestimmte Zwecke, tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz binden.

2. Schon dem Gesetzgeber der Übermittlungsregelung obliegt die normenklare Begrenzung der Zwecke der möglichen Datenverwendung. Eine Begrenzung der Verwendungszwecke erst zusammen mit der Abrufregelung kommt nur in Betracht, wenn die Übermittlungsregelung Materien betrifft, die allein im Kompetenzbereich des Bundes liegen und die Regelungen eine in ihrem Zusammenwirken normenklare und abschließende Zweckbestimmung der Datenverwendung enthalten.

3. Die Befugnis zum Datenabruf muss nicht nur für sich genommen verhältnismäßig sein, sondern ist – auch aus Gründen der Normenklarheit – zudem an die in der Übermittlungsregelung begrenzten Verwendungszwecke gebunden. Dabei steht es dem Gesetzgeber der Abrufregelung frei, den Abruf der Daten an weitergehende Anforderungen zu binden.

4. Trotz ihres gemäßigten Eingriffsgewichts bedürfen die allgemeinen Befugnisse zur Übermittlung und zum Abruf von Bestandsdaten für die Gefahrenabwehr und die Tätigkeit der Nachrichtendienste grundsätzlich einer im Einzelfall vorliegenden konkreten Gefahr und für die Strafverfolgung eines Anfangsverdachts.

   Die Zuordnung dynamischer IP-Adressen muss im Hinblick auf ihr erhöhtes Eingriffsgewicht darüber hinaus auch dem Schutz oder der Bewehrung von Rechtsgütern von hervorgehobenem Gewicht dienen. Es bedarf ferner einer nachvollziehbaren und überprüfbaren Dokumentation der Entscheidungsgrundlagen.

Als Eingriffsschwelle kann im Bereich der Gefahrenabwehr und der nachrichtendienstlichen Tätigkeit das Vorliegen einer konkretisierten Gefahr ausreichen, soweit es um den Schutz von Rechtsgütern oder die Verhütung von Straftaten von zumindest erheblichem Gewicht (allgemeine Bestandsdatenauskunft) oder besonderem Gewicht (Zuordnung dynamischer IP-Adressen) geht.

BUNDESVERFASSUNGSGERICHT

- 1 BvR 1873/13 -
- 1 BvR 2618/13 -

IM NAMEN DES VOLKES

In den Verfahren
über
die Verfassungsbeschwerden

I. 1. der Frau N … ,

2. des Herrn Dr. B … ,

- Bevollmächtigter: … -

gegen § 113 des Telekommunikationsgesetzes,
§ 22a des Gesetzes über die Bundespolizei (Bundespolizeigesetz),
§ 8d des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz),
§ 4b des Gesetzes über den militärischen Abschirmdienst (MAD-Gesetz)
in der Fassung des Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft vom 20. Juni 2013 (Bundesgesetzblatt I Seite 1602),

§ 7 Absatz 5 bis 9, § 15 Absatz 2 bis 6 des Gesetzes über das Zollkriminalamt und die Zollfahndungsämter (Zollfahnungsdienstgesetz)
in der Fassung des Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft vom 20. Juni 2013 (Bundesgesetzblatt I Seite 1602), zuletzt geändert durch Artikel 4 des Gesetzes zur Neuorganisation der Zollverwaltung vom 3. Dezember 2015 (Bundesgesetzblatt I Seite 2178),

§ 2b des Gesetzes über den Bundesnachrichtendienst (BND-Gesetz)
in der Fassung des Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft vom 20. Juni

2013 (Bundesgesetzblatt I Seite 1602), neu bezeichnet als § 4 Gesetz über den Bundesnachrichtendienst (BND-Gesetz) in der Fassung des Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23. Dezember 2016 (Bundesgesetzblatt I Seite 3346),

§§ 10, 40 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz) in der Fassung des Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes vom 1. Juni 2017 (Bundesgesetzblatt I Seite 1354)

- 1 BvR 1873/13 -,

II. des Herrn S … ,

und 5.827 weiterer Beschwerdeführender

- Bevollmächtigter: … -

gegen § 113 des Telekommunikationsgesetzes,
§ 7 Absatz 3 bis 7, § 20b Absatz 3 bis 7, § 22 Absatz 2 bis 4 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz),
§ 22a des Gesetzes über die Bundespolizei (Bundespolizeigesetz),
§ 7 Absatz 5 bis 9, § 15 Absatz 2 bis 6 des Gesetzes über das Zollkriminalamt und die Zollfahndungsämter (Zollfahndungsdienstgesetz),
§ 8d des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz),
§ 2b des Gesetzes über den Bundesnachrichtendienst (BND-Gesetz),
§ 4b des Gesetzes über den militärischen Abschirmdienst (MAD-Gesetz)
in der Fassung des Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft vom 20. Juni 2013 (Bundesgesetzblatt I Seite 1602)

- 1 BvR 2618/13 -

hat das Bundesverfassungsgericht – Erster Senat –
unter Mitwirkung der Richterinnen und Richter
Vizepräsident Harbarth,
Masing,
Paulus,
Baer,
Britz,
Ott,
Christ,
Radtke

am 27. Mai 2020 beschlossen:

1. a) § 113 des Telekommunikationsgesetzes,

b) § 22a Absatz 1 Satz 1, soweit er nicht auf § 21 Absatz 2 Nummer 2 verweist, und Absatz 2 des Gesetzes über die Bundespolizei (Bundespolizeigesetz),

c) § 7 Absatz 5 Satz 1 und Absatz 6 und § 15 Absatz 2 Satz 1 und Absatz 3 des Gesetzes über das Zollkriminalamt und die Zollfahndungsämter (Zollfahndungsdienstgesetz),

d) § 8d Absatz 1 Satz 1 und Absatz 2 Satz 1 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz),

e) § 2b Satz 1 des Gesetzes über den Bundesnachrichtendienst (BND-Gesetz) und § 4b Satz 1 des Gesetzes über den militärischen Abschirmdienst (MAD-Gesetz), soweit sie auf § 8d Absatz 1 Satz 1 und Absatz 2 Satz 1 Bundesverfassungsschutzgesetz verweisen,

alle in der Fassung des Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Be-

standsdatenauskunft vom 20. Juni 2013 (Bundesgesetzblatt I Seite 1602) sowie

f) § 4 Satz 1 des Gesetzes über den Bundesnachrichtendienst (BND-Gesetz), soweit er auf § 8d Absatz 1 Satz 1 und Absatz 2 Satz 1 Bundesverfassungsschutzgesetz verweist, in der Fassung des Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23. Dezember 2016 (Bundesgesetzblatt I Seite 3346) und

g) § 10 Absatz 1 Satz 1 und Absatz 2 und § 40 Absatz 1 Satz 1, soweit er nicht auf § 39 Absatz 2 Nummer 2 verweist, und Absatz 2 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz) in der Fassung des Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes vom 1. Juni 2017 (Bundesgesetzblatt I Seite 1354)

sind nach Maßgabe der Gründe mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 und Artikel 10 Absatz 1 des Grundgesetzes unvereinbar.

2. Bis zur Neuregelung, längstens jedoch bis 31. Dezember 2021, bleiben die für mit dem Grundgesetz unvereinbar erklärten Vorschriften nach Maßgabe der Gründe weiter anwendbar.

3. Im Übrigen werden die Verfassungsbeschwerden zurückgewiesen.

4. Die Bundesrepublik Deutschland hat den Beschwerdeführenden ihre notwendigen Auslagen aus den Verfassungsbeschwerdeverfahren zu erstatten.

Inhaltsverzeichnis

G r ü n d e :

A.

Die Verfassungsbeschwerden richten sich gegen § 113 des Telekommunikationsgesetzes (TKG) sowie gegen mehrere Fachgesetze des Bundes, die die manuelle Bestandsdatenauskunft regeln. 1

Die Beschwerdeführenden wandten sich zunächst gegen § 113 TKG, § 7 Abs. 3 bis 7, § 20b Abs. 3 bis 7 und § 22 Abs. 2 bis 4 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz – BKAG), § 22a des Gesetzes über die Bundespolizei (Bundespolizeigesetz – BPolG), § 7 Abs. 5 bis 9, § 15 Abs. 2 bis 6 des Gesetzes über das Zollkriminalamt und die Zollfahndungsämter (Zollfahndungsdienstgesetz – ZFdG), § 8d des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG), § 2b des Gesetzes über den Bundesnachrichtendienst (BND-Gesetz – BNDG) und § 4b des Gesetzes über den militärischen Abschirmdienst (MAD-Gesetz – MADG), jeweils in der Fassung des Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft vom 20. Juni 2013 (BGBl I S. 1602). 2

Nach der Änderung der § 7 Abs. 7, § 15 Abs. 4 ZFdG durch Art. 4 des Gesetzes zur Neuorganisation der Zollverwaltung vom 3. Dezember 2015 (BGBl I S. 2178) mit Wirkung zum 1. Januar 2016, der Neubezeichnung von § 2b BNDG als § 4 BNDG durch das Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23. Dezember 2016 (BGBl I S. 3346) mit Wirkung zum 31. Dezember 2016 und der Ersetzung der § 7 Abs. 3 bis 7, § 20b Abs. 3 bis 7, § 22 Abs. 2 bis 4 BKAG mit den § 10 und § 40 BKAG durch das Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes vom 1. Juni 2017 (BGBl I S. 1354) mit Wirkung zum 25. Mai 2018 haben die Beschwerdeführenden zu I. ihren Antrag mit Schreiben vom 31. März 2019 den Änderungen angepasst. 3

I.

Der angegriffene § 113 TKG berechtigt Anbieter von Telekommunikationsdiensten zur Übermittlung von Bestandsdaten im sogenannten manuellen Auskunftsverfahren. Die weiteren angegriffenen Normen regeln den Abruf dieser Da- 4

ten durch verschiedene Sicherheitsbehörden des Bundes. Alle Neuregelungen dienen der Umsetzung der Entscheidung des Bundesverfassungsgerichts vom 24. Januar 2012 (BVerfGE 130, 151 – Bestandsdatenauskunft I), mit der § 113 TKG in seiner Fassung vom 22. Juni 2004 (im Folgenden: § 113 TKG a.F.) teilweise für verfassungswidrig erklärt und das Fehlen fachrechtlicher Abrufregelungen beanstandet wurde.

1. Als Grundlage für eine Bestandsdatenauskunft verpflichtet § 111 TKG geschäftsmäßige Anbieter von Telekommunikationsdiensten, die von ihnen vergebenen oder bereitgestellten Rufnummern, Anschlusskennungen und Mobilfunkendgerätenummern sowie die zugehörigen persönlichen Daten der Anschlussinhaber einschließlich der Daten des Vertragsbeginns und – bei Bekanntwerden – des Vertragsendes zu erheben und zu speichern. Zudem sind Kennungen und Kundendaten von elektronischen Postfächern zu speichern, soweit sie ohnehin erhoben werden. 5

Zur Erlangung dieser Bestandsdaten kann sich die um Auskunft ersuchende Behörde entweder im automatisierten Verfahren an die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (im Folgenden: Bundesnetzagentur) oder im manuellen Verfahren unmittelbar an die Diensteanbieter wenden. Den Zugriff auf die Daten im automatisierten Verfahren regelt § 112 TKG. Danach hat, wer öffentlich zugängliche Telekommunikationsdienste erbringt, zu gewährleisten, dass die Bundesnetzagentur die nach § 111 TKG gespeicherten Daten jederzeit automatisiert abrufen kann. Ein Abruf erfolgt insbesondere aufgrund eines an die Bundesnetzagentur gerichteten Ersuchens einer der in § 112 Abs. 2 TKG näher bezeichneten Behörden. 6

Die Auskunft im manuellen Verfahren regelt § 113 TKG. Sie erfolgt unmittelbar aufgrund eines Ersuchens einer der in § 113 Abs. 3 TKG abschließend genannten Stellen. Zur Auskunft verpflichtet sind alle diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, mithin alle Diensteanbieter im Sinne des Telekommunikationsgesetzes (vgl. § 3 Nr. 6 TKG). Da das geschäftsmäßige Erbringen von Telekommunikationsdiensten gemäß § 3 Nr. 10 TKG das nachhaltige Angebot von Telekommunikation für Dritte sowohl mit als auch ohne Gewinnerzielungsabsicht erfasst, sind gemäß § 113 TKG zum Beispiel auch Betreiber eines Hotspots oder Einrichtungen, die im Rahmen von Geschäftsbeziehungen WLAN-Netze zur Verfügung stellen, auskunftsverpflichtet. 7

a) Während im automatisierten Verfahren allein die gemäß § 111 TKG verpflichtend zu speichernden Bestandsdaten beauskunftet werden können, umfasst § 113 Abs. 1 Satz 1 TKG auch die von den Diensteanbietern nach § 95 TKG zu betrieblichen Zwecken gespeicherten Daten, zu deren Speicherung keine Pflicht besteht. Hierbei handelt es sich um solche Bestandsdaten, die die Diensteanbieter zur Begründung, inhaltlichen Ausgestaltung, Änderung oder Beendigung ihrer Vertragsverhältnisse erheben und verwenden. Dazu gehören üblicherweise Name und Anschrift der Vertragspartner, Art des kontrahierten Dienstes und die den Teilnehmenden zum Gebrauch überlassenen Einrichtungen sowie die Anschlussnummer, aber auch rechnungsrelevante Daten wie zum Beispiel Rechnungsanschrift, Bankverbindung, Lastschriftermächtigung und besondere Tarifmerkmale. 8

b) Der Anwendungsbereich des § 113 TKG wird dadurch erweitert, dass nach § 113 Abs. 1 Satz 2 TKG eine Auskunft auch über solche Bestandsdaten zu erteilen ist, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen geschützt wird, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden (Zugangsdaten). Hierbei handelt es sich um vom Diensteanbieter vergebene Zugangssicherungscodes wie zum Beispiel die Persönliche Identifikationsnummer (PIN) und die als Personal Unblocking Key (PUK) bezeichnete Nummer, die einen Zugriff auf Speichereinrichtungen wie SIM-Karten oder Endgeräte wie etwa Mobiltelefone oder Tablets ermöglichen können. Erfasst werden auch weitere, vom Diensteanbieter vergebene Zugangsdaten für externe Speichereinrichtungen, wie etwa sogenannte Voice-Mailboxen oder E-Mail-Postfächer, soweit sie auch nach der Entscheidung des Europäischen Gerichtshofs (EuGH, Urteil vom 13. Juni 2019, Gmail, C-193/18, EU:C:2019:498) noch als Telekommunikationsdienste angesehen werden können. Da § 111 Abs. 1 TKG die Diensteanbieter nicht zur Speicherung von Zugangsdaten verpflichtet, kommt die Erteilung einer Auskunft nur in Betracht, wenn die Diensteanbieter sie gemäß § 95 TKG zu betrieblichen Zwecken speichern. Von Nutzerinnen und Nutzern selbst vergebene Zugangsdaten, mit denen diese ihre Endgeräte oder Speichereinrichtungen vor einem Zugriff Dritter sichern, werden von den Diensteanbietern üblicherweise nur verschlüsselt gespeichert (vgl. § 109 Abs. 1 und 2 TKG sowie § 109 Abs. 6 TKG in Verbindung mit dem Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG)). Eine Auskunft kann insoweit nicht erteilt werden. 9

c) Bestandsdaten dürfen gemäß § 113 Abs. 1 Satz 3 TKG auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokolladresse (dynamische IP-Adresse) bestimmt werden. Die IP-Adresse ist eine Nummer, die die Adressierung von Computern und anderen technischen Geräten in einem Netzwerk, insbesondere im Internet, erlaubt; sie kann vereinfacht als „Telefonnummer“ des Computers beschrieben werden. Dabei wird zwischen statischen und dynamischen IP-Adressen unterschieden. Während eine statische IP-Adresse einem bestimmten Anschlussinhaber (genauer: der Netzwerkschnittstelle eines bestimmten Geräts des Anschlussinhabers) fest zugewiesen wird, wird im Fall der dynamischen Adressierung dem Anschlussinhaber (genauer: der Netzwerkschnittstelle des mit dem Internet kommunizierenden Geräts des Anschlussinhabers) bei jeder neuen Aufnahme der Netzwerkverbindung eine IP-Adresse neu zugewiesen (BVerfGE 130, 151 <162>). 10

Gegenstand der Auskunft ist die Zuordnung der IP-Adresse zu einem bestimmten Anschlussinhaber und damit selbst ein Bestandsdatum (vgl. BVerfGE 130, 151 <163>). Dies ist nur möglich, wenn die Diensteanbieter zuvor bei ihnen gespeicherte Verkehrsdaten auswerten, um festzustellen, welchem Anschluss die verwendete IP-Adresse zu dem angefragten Zeitpunkt zugeordnet war. Auskünfte beziehen sich dadurch immer auch auf eine konkrete Verbindung. Bei den Verkehrsdaten, die zu diesem Zweck ausgewertet werden, handelt es sich zunächst um die nach § 96 TKG zu betrieblichen Zwecken gespeicherten Daten. Die Praxis der Speicherung ist insoweit je nach Diensteanbieter, Vertragsgestaltung und in Anspruch genommener Dienstleistung sehr unterschiedlich. Ohne konkreten Anlass ist eine Speicherung zur Erkennung, Eingrenzung oder Beseitigung von Störungen oder Fehlern (§ 96 Abs. 1 Satz 2, § 100 Abs. 1 TKG) jedenfalls bis zu sieben Tage nach Ende der Verbindung zulässig (vgl. BGH, Urteil vom 3. Juli 2014 - III ZR 391/13 -, Rn. 23). 11

Diensteanbieter, die öffentlich zugängliche Telekommunikationsdienste erbringen, dürfen gemäß § 113c Abs. 1 Nr. 3 TKG aber auch Verkehrsdaten auswerten, zu deren Speicherung sie gemäß § 113a Abs. 1, § 113b Abs. 1 und 3 TKG in der Fassung von Art. 2 Nr. 2 des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl I S. 2218) seit dem 1. Juli 2017 verpflichtet sind. Zwar sieht die Bundesnetzagentur derzeit von Anordnungen und sonstigen Maßnahmen zur Durchsetzung der Speicherungsverpflichtung ab. Ihre entsprechende Erklärung vom 28. Juni 2017 erging als Folge einer Entscheidung des Oberverwaltungsgerichts für das Land Nord- 12

rhein-Westfalen in einem einstweiligen Rechtsschutzverfahren (OVG Nordrhein-Westfalen, Beschluss vom 22. Juni 2017 - 13 B 238/17 -), in dem festgestellt wurde, dass der dort klagende Diensteanbieter bis zum rechtskräftigen Abschluss des Hauptsacheverfahrens nicht verpflichtet ist, die in § 113b Abs. 3 TKG genannten Verkehrsdaten zu speichern. Das Hauptsacheverfahren ist weiterhin anhängig und das Bundesverwaltungsgericht hat zwischenzeitlich in diesem und einem weiteren Verfahren dem Europäischen Gerichtshof die Frage vorgelegt, ob das Unionsrecht der Vorratsdatenspeicherung in der Ausgestaltung durch §§ 113a f. TKG entgegensteht (BVerwG, Beschlüsse vom 25. September 2019 - 6 C 12.18 - und - 6 C 13.18 -). Die Entscheidungen des Oberverwaltungsgerichts und des Bundesverwaltungsgerichts ändern jedoch nichts an der formellen Weitergeltung der Speicherungspflichten der Diensteanbieter, wenngleich in Reaktion auf die Erklärung der Bundesnetzagentur fast alle Diensteanbieter vorerst davon absehen, die Vorratsdatenspeicherung umzusetzen, und auch das Oberverwaltungsgericht aufgrund der Erklärung der Bundesnetzagentur gegenwärtig das Rechtsschutzinteresse für den Erlass einstweiliger Anordnungen zugunsten weiterer Diensteanbieter verneint (vgl. OVG Nordrhein-Westfalen, Beschluss vom 25. August 2017 - 13 B 762/17 -, Rn. 19 ff.).

d) Gemäß § 113 Abs. 2 Satz 1 TKG darf eine Auskunft nur erteilt werden, soweit eine in § 113 Abs. 3 TKG genannte Stelle dies in Textform im Einzelfall zum Zweck der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste unter Angabe einer gesetzlichen Bestimmung verlangt, die ihr eine Erhebung der angefragten Daten erlaubt. 13

2. Die mit den Verfassungsbeschwerden angegriffenen Abrufregelungen des Bundes bestimmen, dass die Sicherheitsbehörden zur Erfüllung ihrer jeweils genannten Aufgaben von den Diensteanbietern Auskunft über die nach den §§ 95 und 111 TKG erhobenen Daten verlangen dürfen. Die Auskunft über Zugangsdaten ist daran gebunden, dass die gesetzlichen Voraussetzungen für deren Nutzung vorliegen. Die Vorschriften sehen jeweils vor, dass auch Auskunft von anhand einer dynamischen IP-Adresse bestimmter Bestandsdaten verlangt werden darf. Die angegriffenen Abrufregelungen unterscheiden sich hauptsächlich hinsichtlich der Eingriffsvoraussetzungen, die jeweils auf die Aufgaben der abrufberechtigten Behörde zugeschnitten sind, sowie hinsichtlich der Ausgestaltung der Benachrichtigungspflichten. 14

3. Die angegriffenen Vorschriften lauten in ihrer maßgeblichen Fassung vom 20. Juni 2013, die zum 1. Juli 2013 in Kraft getreten ist, wie folgt: 15

§ 113 TKG Manuelles Auskunftsverfahren

(1) [1]Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, darf nach Maßgabe des Absatzes 2 die nach den §§ 95 und 111 erhobenen Daten nach Maßgabe dieser Vorschrift zur Erfüllung von Auskunftspflichten gegenüber den in Absatz 3 genannten Stellen verwenden. [2]Dies gilt auch für Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird. [3]Die in eine Auskunft aufzunehmenden Daten dürfen auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden; hierfür dürfen Verkehrsdaten auch automatisiert ausgewertet werden. [4]Für die Auskunftserteilung nach Satz 3 sind sämtliche unternehmensinternen Datenquellen zu berücksichtigen.

(2) [1]Die Auskunft darf nur erteilt werden, soweit eine in Absatz 3 genannte Stelle dies in Textform im Einzelfall zum Zweck der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der in Absatz 3 Nummer 3 genannten Stellen unter Angabe einer gesetzlichen Bestimmung verlangt, die ihr eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt; an andere öffentliche und nichtöffentliche Stellen dürfen Daten nach Absatz 1 nicht übermittelt werden. [2]Bei Gefahr im Verzug darf die Auskunft auch erteilt werden, wenn das Verlangen in anderer Form gestellt wird. [3]In diesem Fall ist das Verlangen unverzüglich nachträglich in Textform zu bestätigen. [4]Die Verantwortung für die Zulässigkeit des Auskunftsverlangens tragen die in Absatz 3 genannten Stellen.

(3) Stellen im Sinne des Absatzes 1 sind

1. die für die Verfolgung von Straftaten oder Ordnungswidrigkeiten zuständigen Behörden;

2. die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden;

3. die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst.

(4) [1]Derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat die zu beauskunftenden Daten unverzüglich und vollständig zu übermitteln. [2]Über das Auskunftsersuchen und die Auskunftserteilung haben die Verpflichteten gegenüber den Betroffenen sowie Dritten Stillschweigen zu wahren.

(5) [1]Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat die in seinem Verantwortungsbereich für die Auskunftserteilung erforderlichen Vorkehrungen auf seine Kosten zu treffen. [2]Wer mehr als 100 000 Kunden hat, hat für die Entgegennahme der Auskunftsverlangen sowie für die Erteilung der zugehörigen Auskünfte eine gesicherte elektronische Schnittstelle nach Maßgabe der Technischen Richtlinie nach § 110 Absatz 3 bereitzuhalten, durch die auch die gegen die Kenntnisnahme der Daten durch Unbefugte gesicherte Übertragung gewährleistet ist. [3]Dabei ist dafür Sorge zu tragen, dass jedes Auskunftsverlangen durch eine verantwortliche Fachkraft auf Einhaltung der in Absatz 2 genannten formalen Voraussetzungen geprüft und die weitere Bearbeitung des Verlangens erst nach einem positiven Prüfergebnis freigegeben wird.

§ 22a BPolG Erhebung von Telekommunikationsdaten

(1) [1]Soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes einer Person nach Maßgabe von § 21 Absatz 1 und 2 erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten verlangt werden (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). [2]Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes).

(3) [1]Auskunftsverlangen nach Absatz 1 Satz 2 dürfen nur auf Antrag des Leiters der in der Rechtsverordnung nach § 58 Absatz 1 bestimmten Bundespolizeibehörde oder seines Vertreters durch das Gericht angeordnet werden. [2]Bei Gefahr im Verzug kann die Anordnung durch den Leiter der in der Rechtsverordnung nach § 58 Absatz 1 bestimmten Bundespolizeibehörde oder seinen Vertreter getroffen werden. [3]In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. [4]Die Sätze 1 bis 3 finden keine Anwendung,

wenn der Betroffene vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird. [5]Das Vorliegen der Voraussetzungen nach Satz 4 ist aktenkundig zu machen. [6]§ 28 Absatz 3 Satz 5 und 6 gilt entsprechend.

(4) [1]Die betroffene Person ist in den Fällen des Absatzes 1 Satz 2 und des Absatzes 2 über die Beauskunftung zu benachrichtigen. [2]Die Benachrichtigung erfolgt, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird. [3]Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. [4]Wird die Benachrichtigung nach Satz 2 zurückgestellt oder nach Satz 3 von ihr abgesehen, sind die Gründe aktenkundig zu machen.

(5) [1]Auf Grund eines Auskunftsverlangens nach Absatz 1 oder 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich zu übermitteln. [2]Für die Entschädigung der Diensteanbieter ist § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend anzuwenden.

§ 7 ZFdG Datenerhebung und -verarbeitung der Zentralstelle

…

(5) [1]Soweit es zur Erfüllung der Aufgaben als Zentralstelle nach § 3 erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten verlangt werden (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). [2]Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(6) Die Auskunft nach Absatz 5 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes).

(7) [1]Auskunftsverlangen nach Absatz 5 Satz 2 dürfen nur auf Antrag des Behördenleiters oder seines Vertreters durch das Gericht angeordnet werden. [2]Bei Gefahr im Verzug kann die Anordnung durch den Behördenleiter oder seinen Vertreter getroffen werden. [3]In die-

sem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. [4]Die Sätze 1 bis 3 finden keine Anwendung, wenn der Betroffene vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird. [5]Das Vorliegen der Voraussetzungen nach Satz 4 ist aktenkundig zu machen. [6]§ 18 Absatz 3 Satz 5 und 6 gilt entsprechend.

(8) [1]Die betroffene Person ist in den Fällen des Absatzes 5 Satz 2 und des Absatzes 6 über die Beauskunftung zu benachrichtigen. [2]Die Benachrichtigung erfolgt, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird. [3]Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. [4]Wird die Benachrichtigung nach Satz 2 zurückgestellt oder nach Satz 3 von ihr abgesehen, sind die Gründe aktenkundig zu machen.

(9) Auf Grund eines Auskunftsverlangens nach Absatz 5 oder 6 hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich zu übermitteln.

§ 15 ZFdG Erhebung und Sammlung personenbezogener Daten zur Erfüllung eigener Aufgaben

…

(2) [1]Soweit dies zur Erfüllung der Aufgaben nach § 4 Absatz 2 bis 4 erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten verlangt werden (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). [2]Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(3) Die Auskunft nach Absatz 2 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes).

(4) [1]Auskunftsverlangen nach Absatz 2 Satz 2 dürfen nur auf Antrag des Behördenleiters oder seines Vertreters durch das Gericht angeordnet werden. [2]Bei Gefahr im Verzug kann die Anordnung durch

den Behördenleiter oder seinen Vertreter getroffen werden. [3]In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. [4]Die Sätze 1 bis 3 finden keine Anwendung, wenn der Betroffene vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird. [5]Das Vorliegen der Voraussetzungen nach Satz 4 ist aktenkundig zu machen. [6]§ 18 Absatz 3 Satz 5 und 6 gilt entsprechend.

(5) [1]Die betroffene Person ist in den Fällen des Absatzes 2 Satz 2 und des Absatzes 3 über die Beauskunftung zu benachrichtigen. [2]Die Benachrichtigung erfolgt, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird. [3]Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. [4]Wird die Benachrichtigung nach Satz 2 zurückgestellt oder nach Satz 3 von ihr abgesehen, sind die Gründe aktenkundig zu machen.

(6) Auf Grund eines Auskunftsverlangens nach Absatz 2 oder 3 hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich zu übermitteln.

§ 8d BVerfSchG Weitere Auskunftsverlangen

(1) [1]Soweit dies zur Erfüllung der Aufgaben des Bundesamts für Verfassungsschutz erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten verlangt werden (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). [2]Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) [1]Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes). [2]Für Auskunftsverlangen nach Absatz 1 Satz 2 gilt § 8b Absatz 1 Satz 1 und 2 und Absatz 2 entsprechend.

(3) [1]Die betroffene Person ist in den Fällen des Absatzes 1 Satz 2 und des Absatzes 2 Satz 1 über die Beauskunftung zu benachrichtigen. [2]Die Benachrichtigung erfolgt, soweit und sobald eine Gefähr-

dung des Zwecks der Auskunft und der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes ausgeschlossen werden können. [3]Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. [4]Wird die Benachrichtigung nach Satz 2 zurückgestellt oder nach Satz 3 von ihr abgesehen, sind die Gründe aktenkundig zu machen.

(4) Auf Grund eines Auskunftsverlangens nach Absatz 1 oder 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich, vollständig und richtig zu übermitteln.

(5) Das Bundesamt für Verfassungsschutz hat für ihm erteilte Auskünfte eine Entschädigung zu gewähren, deren Umfang sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes bemisst; die Vorschriften über die Verjährung in § 2 Absatz 1 und 4 des Justizvergütungs- und -entschädigungsgesetzes finden entsprechend Anwendung.

(6) Das Grundrecht des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird nach Maßgabe des Absatzes 2 eingeschränkt.

§ 4b MADG Weitere Auskunftsverlangen

[1]Soweit dies zur Erfüllung der Aufgaben des Militärischen Abschirmdienstes erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten entsprechend § 8d des Bundesverfassungsschutzgesetzes verlangt werden. [2]Die Auskunftserteilung ist nach § 8d Absatz 5 des Bundesverfassungsschutzgesetzes zu entschädigen. [3]Das Grundrecht des Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird nach Maßgabe des § 8d Absatz 2 des Bundesverfassungsschutzgesetzes eingeschränkt.

§ 2b BNDG Weitere Auskunftsverlangen

[1]Soweit dies zur Erfüllung der Aufgaben des Bundesnachrichtendienstes nach § 1 Absatz 2 erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten entsprechend § 8d des Bundesverfassungsschutzgesetzes verlangt werden. [2]Die Auskunftserteilung ist nach § 8d Absatz 5 des Bundesverfassungsschutzgesetzes zu entschädigen. [3]Das Grundrecht des Fernmeldegeheimnisses (Ar-

tikel 10 des Grundgesetzes) wird nach Maßgabe des § 8d Absatz 2 des Bundesverfassungsschutzgesetzes eingeschränkt.

Die zunächst angegriffenen § 7 Abs. 3 bis 7, § 20b Abs. 3 bis 7 und § 22 Abs. 2 bis 4 BKAG in der Fassung vom 20. Juni 2013 wurden zwischenzeitlich durch das Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes vom 1. Juni 2017 (BGBl I S. 1354) mit Wirkung zum 25. Mai 2018 durch die §§ 10, 40 BKAG ersetzt. Diese lauten: 16

§ 10 BKAG Bestandsdatenauskunft

(1) [1]Soweit dies zur Erfüllung der Aufgabe des Bundeskriminalamtes

1. als Zentralstelle nach § 2 Absatz 2 Nummer 1 und Absatz 6 zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung,

2. zum Schutz von Mitgliedern der Verfassungsorgane und der Leitung des Bundeskriminalamtes nach § 6 sowie

3. zum Zeugenschutz nach § 7

erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten verlangt werden (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). [2]Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes).

(3) [1]Auskunftsverlangen nach Absatz 1 Satz 2 dürfen nur auf Antrag der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung durch das Gericht angeordnet werden. [2]Bei Gefahr im Verzug kann die Anordnung durch die Präsidentin oder den Präsidenten des Bundeskriminalamtes oder ihre oder seine Vertretung getroffen werden. [3]In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. [4]Die Sätze 1 bis 3 finden keine

Anwendung, wenn die betroffene Person vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird. [5]Das Vorliegen der Voraussetzungen nach Satz 4 ist aktenkundig zu machen.

(4) [1]Die betroffene Person ist in den Fällen des Absatzes 1 Satz 2 und des Absatzes 2 über die Beauskunftung zu benachrichtigen. [2]Die Benachrichtigung erfolgt, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird. [3]Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. [4]Wird die Benachrichtigung nach Satz 2 zurückgestellt oder nach Satz 3 von ihr abgesehen, sind die Gründe aktenkundig zu machen.

(5) [1]Aufgrund eines Auskunftsverlangens nach Absatz 1 oder Absatz 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich zu übermitteln. [2]Für die Entschädigung der Diensteanbieter ist § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend anzuwenden.

§ 40 BKAG Bestandsdatenauskunft

(1) [1]Soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes einer Person nach Maßgabe des § 39 Absatz 1 und 2 erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten verlangt werden (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). [2]Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes).

(3) [1]Auskunftsverlangen nach Absatz 1 Satz 2 dürfen nur auf Antrag der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung durch das Gericht angeordnet werden. [2]Bei Gefahr im Verzug kann die Anordnung durch die Präsidentin oder den Präsidenten des Bundeskriminalamtes oder ihre oder seine

> Vertretung getroffen werden. [3]In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. [4]Die Sätze 1 bis 3 finden keine Anwendung, wenn die betroffene Person vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird. [5]Das Vorliegen der Voraussetzungen nach Satz 4 ist aktenkundig zu machen.
>
> (4) [1]Die betroffene Person ist in den Fällen des Absatzes 1 Satz 2 und des Absatzes 2 über die Beauskunftung zu benachrichtigen. [2]Die Benachrichtigung erfolgt, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird. [3]Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. [4]Wird die Benachrichtigung nach Satz 2 zurückgestellt oder nach Satz 3 von ihr abgesehen, sind die Gründe aktenkundig zu machen.
>
> (5) [1]Aufgrund eines Auskunftsverlangens nach Absatz 1 oder Absatz 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich zu übermitteln. [2]Für die Entschädigung der Diensteanbieter ist § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend anzuwenden.

4. a) Anlass der Neuregelung der manuellen Bestandsdatenauskunft war die Entscheidung des Bundesverfassungsgerichts vom 24. Januar 2012 (BVerfGE 130, 151 – Bestandsdatenauskunft I). Danach ist zwischen der Datenübermittlung seitens der auskunftsberechtigten Stelle und dem Datenabruf seitens der auskunftsuchenden Stelle zu unterscheiden. Ein Datenaustausch vollzieht sich durch die miteinander korrespondierenden Eingriffe von Abfrage und Übermittlung, die jeweils einer eigenen Rechtsgrundlage bedürfen. Der Gesetzgeber muss, bildlich gesprochen, nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür zu deren Abfrage. Erst beide Rechtsgrundlagen gemeinsam, die wie eine Doppeltür zusammenwirken müssen, berechtigen zu einem Austausch personenbezogener Daten (BVerfGE 130, 151 <184>). Damit bedarf es auch für bundesrechtliche Materien qualifizierter Abrufregelungen, die über eine schlichte Datenerhebungsbefugnis hinausgehen und die eine Auskunftsverpflichtung der Diensteanbieter eigenständig begründen (vgl. BVerfGE 130, 151 <202>). 17

Der zur Überprüfung gestellte § 113 Abs. 1 Satz 1 TKG a.F. konnte dementsprechend nur so verstanden werden, dass er zwar zur Übermittlung der Daten durch die Diensteanbieter ermächtigte, für den Datenabruf selbst aber qualifizierte Abrufregelungen voraussetzte (vgl. BVerfGE 130, 151 <202>). Darüber hinaus 18

entschied das Bundesverfassungsgericht, dass § 113 Abs. 1 Satz 1 TKG a.F. verfassungskonform dahin auszulegen sei, dass in ihm keine Rechtsgrundlage für die Zuordnung dynamischer IP-Adressen gesehen werden konnte (vgl. BVerfGE 130, 151 <204 f.>), und erklärte § 113 Abs. 1 Satz 2 TKG a.F. aus Gründen der Verhältnismäßigkeit für verfassungswidrig, weil die Regelung zur Erteilung einer Auskunft über Zugangsdaten unabhängig von den Voraussetzungen für deren Nutzung ermächtigte (vgl. BVerfGE 130, 151 <208 f.>).

b) Nach der Begründung des Gesetzentwurfs der Bundesregierung dienen die angegriffenen Regelungen vom 20. Juni 2013 sämtlich der Umsetzung der Entscheidung des Bundesverfassungsgerichts; neue Befugnisse der Sicherheitsbehörden sollten nicht geschaffen werden (vgl. BTDrucks 17/12034, S. 10). Nach dem Bild einer Doppeltür soll § 113 TKG die erste der zwei notwendigen Türen darstellen. Die Regelung wurde daher ausdrücklich nur als bloße Öffnungsklausel ausgestaltet, die die Diensteanbieter lediglich bei Vorliegen eines auf eine fachrechtliche Abrufregelung gestützten Verlangens zur Datenübermittlung berechtigt und verpflichtet. Dementsprechend bestimmt § 113 Abs. 2 Satz 1 TKG, dass der Abruf einer qualifizierten Rechtsgrundlage für die abrufende Stelle bedarf (vgl. BTDrucks 17/12034, S. 12). Die Maßgabe des Bundesverfassungsgerichts, dass ein Zugriff auf Zugangsdaten nur zulässig ist, wenn auch die Voraussetzungen für deren Nutzung vorliegen, wurde nicht in § 113 TKG umgesetzt, sondern in den verschiedenen Abrufregelungen des Fachrechts. Mit § 113 Abs. 1 Satz 3 TKG wurde schließlich eine Rechtsgrundlage dafür geschaffen, zu beauskunftende Bestandsdaten auch anhand einer dynamischen IP-Adresse zu bestimmen. 19

Die in den Fachgesetzen des Bundes erstmals geschaffenen Abrufregelungen sollen die für den Datenaustausch erforderliche zweite Tür bilden. Sie ermächtigen die verschiedenen auskunftsberechtigten Bundesbehörden zum Abruf der nach §§ 95 und 111 TKG erhobenen Daten und begründen eigenständig eine Auskunftsverpflichtung der Diensteanbieter (vgl. BTDrucks 17/12034, S. 13). Für den Abruf von Zugangsdaten und die identifizierende Zuordnung dynamischer IP-Adressen wurden Benachrichtigungspflichten und für den Abruf von Zugangsdaten zudem ein Richtervorbehalt vorgesehen (vgl. BTDrucks 17/12879, S. 4 ff., 11). 20

II.

Die Beschwerdeführenden sind Inhaber von Festnetz- sowie Mobilfunkanschlüssen und nutzen Internetzugangsleistungen verschiedener Diensteanbieter. 21

Sie sehen sich durch die angegriffenen Vorschriften in ihren Grundrechten aus Art. 10 Abs. 1 GG sowie Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG verletzt.

1. Die Verfassungsbeschwerden seien zulässig. Die Beschwerdeführenden seien alle mit einiger Wahrscheinlichkeit von Abfragen der gespeicherten Daten betroffen. Hiervon würden sie voraussichtlich keine Kenntnis erlangen, da eine Benachrichtigung entweder nicht vorgesehen sei oder Einschränkungen unterliege. 22

2. Die Verfassungsbeschwerden seien auch begründet. 23

a) § 113 TKG sei verfassungswidrig. Für die Regelungsinhalte seiner Absätze 3 und 4 bestehe schon keine Gesetzgebungskompetenz des Bundes. In welcher Form, in welchem Zeitrahmen und in welchem Umfang Auskünfte zu erteilen seien und ob Diensteanbieter ihre Kunden über eine Beauskunftung informieren dürften, betreffe nicht lediglich die Öffnung der Datenbestände. 24

Die Übermittlungsregelung des § 113 TKG verletze das Verhältnismäßigkeitsgebot. Sowohl in § 113 TKG als auch in den fachrechtlichen Abrufregelungen fehle die noch in der Vorgängerregelung enthaltene Bestimmung, dass Auskünfte nur „im Einzelfall“ und damit nicht routinemäßig und massenhaft eingeholt werden dürften, obgleich die weiten Auskunftsrechte unverändert beibehalten worden seien. Die Verpflichtung zur Bereithaltung einer gesicherten elektronischen Schnittstelle (§ 113 Abs. 5 Satz 2 TKG) weite den staatlichen Zugriff zusätzlich aus. 25

§ 113 Abs. 2 TKG setze keine spezifische Rechtsgrundlage für den Abruf der Daten voraus. Gefordert werde nur eine gesetzliche Bestimmung, die eine Erhebung der in Absatz 1 der Vorschrift in Bezug genommenen Daten erlaube. Dafür genüge eine allgemeine Datenerhebungsbefugnis. Eine erneute verfassungskonforme Auslegung dahin, dass die Regelung eine spezifische Rechtsgrundlage voraussetze, komme aus Gründen der Normenklarheit nicht in Betracht. Notwendig sei ein „einfachgesetzliches Zitiergebot“: § 113 TKG dürfe zur Auskunftserteilung nur aufgrund solcher Abrufregelungen berechtigen, die einen Abruf unter ausdrücklicher Nennung der Vorschrift ermöglichten. 26

Die Identifizierung von Personen, die das Internet nutzen, stelle einen besonders schwerwiegenden Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG dar. Die mögliche Persönlichkeitsrelevanz einer Abfrage des Inhabers einer IP-Adresse sei 27

eine andere als diejenige der Abfrage des Inhabers einer Telefonnummer. Zur Wahrung der Verhältnismäßigkeit sei insoweit im Bereich der Strafverfolgung eine richterliche Anordnung notwendig. Darüber hinaus erfordere die Aufhebung der Anonymität im Internet eine Rechtsgutbeeinträchtigung, der von der Rechtsordnung auch sonst ein hervorgehobenes Gewicht beigemessen werde. Sie sei nur zur Verfolgung von Straftaten von erheblichem Gewicht oder zur Abwehr von Gefahren für wichtige Rechtsgüter verhältnismäßig. Ein Abruf zur Verfolgung jedweder Ordnungswidrigkeiten genüge dem nicht (mit Verweis auf BVerfGE 125, 260 <344>). Ein solcher werde auch durch § 46 Abs. 3 Gesetz über Ordnungswidrigkeiten (OWiG) nicht normenklar ausgeschlossen.

Es sei unverhältnismäßig, dass § 113 Abs. 1 Satz 4 TKG von den Anbietern die Heranziehung „sämtlicher unternehmensinterner Datenquellen“ zur Auskunftserteilung fordere, weil dies rechtswidrig gespeicherte Daten einschließe. Die Formulierung berge auch die Gefahr, dass die Vorschriften über die Verkehrsdatenerhebung umgangen werden könnten, indem offene Anfragen zu Anschlussinhabern gestellt würden, deren Telekommunikationsverbindungen den Behörden nicht bekannt seien. 28

b) Die angegriffenen Abrufregelungen regelten die gesetzlichen Voraussetzungen des Abrufs von Zugangsdaten nicht normenklar und präzise. Die bloße Bezugnahme auf „die gesetzlichen Voraussetzungen für die Nutzung der Daten“ lasse nicht erkennen, welche konkreten Voraussetzungen vorliegen müssten. 29

Die fachgesetzlichen Abrufregelungen genügten in verschiedener Hinsicht nicht dem Verhältnismäßigkeitsgrundsatz. Zugangsdaten ermöglichten den Zugriff auf äußerst sensible Inhalte der Telekommunikation und persönliche Inhalte wie Fotos, Tagebücher und Dokumente. Erforderlich sei daher eine Subsidiaritätsklausel, nach der der Staat Zugangsdaten allenfalls dann erheben dürfe, wenn die damit bezweckte Datenerhebung nicht auf andere Weise erfolgen könne. In Betracht komme eine unmittelbare Inanspruchnahme der Diensteanbieter auf Herausgabe inhaltlich oder zeitlich begrenzter Daten. Die dem Bundes- und Zollkriminalamt jeweils in ihrer Funktion als Zentralstelle eingeräumte Befugnis, Zugangsdaten abzufragen, sei unzulässig, weil diese insoweit nicht zur Nutzung der Daten befugt seien. 30

Alle fachrechtlichen Abrufregelungen seien mangels hinreichend begrenzter Zweckbestimmungen verfassungswidrig. Die Regelungen zur Zuordnung von IP- 31

Adressen verletzten zudem das Verhältnismäßigkeitsgebot, weil sie diese eingriffsintensive Maßnahme unter denselben weitreichenden Voraussetzungen zuließen wie die allgemeine Bestandsdatenauskunft. § 8d BVerfSchG, § 2b BNDG und § 4b MADG berücksichtigten nicht die Rechtsprechung des Bundesverfassungsgerichts, nach der Nachrichtendiensten die Identifizierung von Internetnutzern nur erlaubt werden dürfe, wenn aufgrund tatsächlicher Anhaltspunkte vom Vorliegen einer konkreten Gefahr auszugehen sei (mit Verweis auf BVerfGE 125, 260 <343 f.>).

Art. 9 des Änderungsgesetzes (BGBl I 2013 S. 1602) stelle fest, dass das Fernmeldegeheimnis durch die Art. 1 bis 8 des Gesetzes eingeschränkt werde, ohne dies auf die Zuordnung von IP-Adressen zu beschränken. Von daher könnte die Befugnis zu Eingriffen in das Fernmeldegeheimnis auch anderen Regelungen entnommen werden. 32

Der Richtervorbehalt für die Erhebung von Zugangsdaten sei unzureichend ausgestaltet. Die vorgesehenen Ausnahmen gingen zu weit. Auch werde es dem Verhältnismäßigkeitsgebot nicht gerecht, dass das Gesetz keinerlei Vorkehrungen zur Gewährleistung der Sicherheit erhobener Zugangsdaten treffe und dass eine statistische Erfassung der erfolgten Abfragen dynamischer IP-Adressen und der Nutzung der elektronischen Schnittstelle nicht vorgesehen sei. 33

III.

Zu den Verfassungsbeschwerden haben die Bundesregierung und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Stellung genommen. 34

1. Die Bundesregierung hält die Verfassungsbeschwerden für unbegründet. Die Öffnungsregelung zur manuellen Bestandsdatenauskunft in § 113 TKG und die einzelnen Abrufregelungen des Bundesrechts seien verfassungsgemäß. 35

a) aa) In tatsächlicher Hinsicht weist die Bundesregierung darauf hin, dass für die Praxis vor allem das automatisierte Abrufverfahren nach § 112 TKG von Bedeutung sei. So habe etwa beim Bundesamt für Verfassungsschutz die Zahl der Abrufe im manuellen Verfahren im Jahr 2016 nur 2 % der Anfragen nach § 112 TKG betragen. Beide Abrufverfahren würden in erster Linie zu Zwecken der Strafverfolgung genutzt. Abfragen zur Gefahrenabwehr oder zu nachrichtendienst- 36

lichen Zwecken seien nicht ohne praktische Relevanz, stünden aber zahlenmäßig im Hintergrund. Die absoluten Zahlen der Anfragen seien auch nach der Neufassung des § 113 TKG kaum angestiegen.

Das manuelle Auskunftsverfahren komme typischerweise in Betracht, wenn eine vorherige Abfrage im automatisierten Verfahren ergebnislos geblieben sei oder über die übermittelten Daten hinaus die nach § 95 TKG gespeicherten Daten für die Aufklärung eines Sachverhalts oder die eindeutige Identifizierung des Anschlussinhabers erforderlich seien. Es sei auch dann erforderlich, wenn etwa weitere auf den Anschlussinhaber früher oder aktuell ausgegebene Rufnummern oder Anschlusskennungen in Erfahrung gebracht werden sollten. Eine Abfrage mehrerer Rufnummern oder IP-Adressen erfolge nicht. 37

Da die Behörden vielfach keine Statistiken führten, beruhten Angaben zur Häufigkeit der Abfragen teilweise auf Schätzungen. Es ergebe sich folgendes Bild: 38

Die Bundespolizei erhebe Bestandsdaten ganz überwiegend nur im Rahmen von repressiv-polizeilichen Ermittlungen. Es gebe insgesamt relativ konstant circa 4.600 Anfragen pro Jahr. Im Bereich des Zolls seien seit dem Jahr 2013 jährlich insgesamt zwischen 2.354 und 4.391 Bestandsdatensätze manuell abgefragt worden. Die Abfragen durch die Nachrichtendienste bewegten sich in den letzten Jahren relativ konstant im dreistelligen Bereich. 39

Auskunftsverlangen zu Bestandsdaten nach § 10 Abs. 1 Satz 1 Nr. 1 BKAG erfolgten zum einen zur Beantwortung polizeilicher Rechtshilfeersuchen, die ausländische Polizeibehörden an das Bundeskriminalamt richteten. Zum anderen erfolgten zeitkritische Abfragen zur Feststellung einer Länderzuständigkeit in Gefahrenlagen. Beispielhafte Anlässe für Auskunftsersuchen im Rahmen der Zentralstellenfunktion des Bundeskriminalamts seien Suizidankündigungen sowie Amokdrohungen im Internet, die ein unverzügliches Einschreiten zur Ermittlung der suizidgefährdeten Person beziehungsweise des Gefahrenverantwortlichen erforderlich machten. In Fällen, in denen der einzige Ermittlungsansatz eine IP-Adresse oder Rufnummer sei, könne die örtliche Zuständigkeit einer Länderdienststelle fast nur über die Abfrage nach § 112 oder § 113 TKG festgestellt werden. Im Rahmen der Aufgabenwahrnehmung nach § 2 BKAG (Zentralstelle) und § 4 BKAG (Strafverfolgung) sei insoweit eine Steigerung von 2.001 im Jahr 2013 auf 17.428 Abfragen im Jahr 2017 zu vermerken. Hauptursache für diese Steigerung sei ein seit Jahren zu verzeichnender Anstieg von Meldungen der US-amerikanischen Zent- 40

ralstelle National Center for Missing and Exploited Children (NCMEC) bezüglich des Besitzes, der Besitzverschaffung und der Verbreitung von Kinder- und Jugendpornografie durch deutsche Internetnutzer an das Bundeskriminalamt. Zu berücksichtigen sei auch ein verändertes Nutzerverhalten, das durch eine vermehrte Nutzung von Smartphones und des Internets sowie der Zuordnung mehrerer Geräte und Kennungen zu einer Person geprägt sei. Von seiner Befugnis Zugangsdaten abzufragen, habe das Bundeskriminalamt im Rahmen seiner Zentralstellenaufgaben bisher keinen Gebrauch gemacht.

Die Zahlen der insgesamt erfolgten Abfragen von Zugangsdaten und Abfragen zum Zwecke der Zuordnung dynamischer IP-Adressen könnten für das Bundeskriminalamt und die Bundespolizei nicht angegeben werden. Im Bereich des Zolls seien sie auf jeweils etwa bis zu 100 Abfragen jährlich zu schätzen. Von den Nachrichtendiensten habe lediglich das Bundesamt für Verfassungsschutz in den letzten Jahren Zugangsdaten in einstelliger Anzahl abgefragt. Alle Nachrichtendienste hätten jedoch Bestandsdaten anhand von IP-Adressen abgefragt, wobei deren Anzahl schwanke. So habe der Militärische Abschirmdienst in den Jahren 2016 bis 2018 eine einzige Abfrage anhand einer IP-Adresse vorgenommen, während der Bundesnachrichtendienst 166 Abfragen im Jahr 2017 vorgenommen habe. Die Zahlen für das Bundesamt für Verfassungsschutz wiesen eine steigende Tendenz von circa 50 Abfragen im Jahr 2013 bis auf circa 850 Abfragen im Jahr 2017 auf. 41

bb) Zur technischen Entwicklung bei der Vergabe von IP-Adressen teilt die Bundesregierung mit: Da der Adressraum des überkommenen Internetprotokolls Version 4 (IPv4) nicht ausreiche, um allen netzfähigen Geräten eine eigene IP-Adresse zuzuweisen, solle diese Version auf lange Sicht durch das Internetprotokoll Version 6 (IPv6) abgelöst werden. Die neue Version verfüge über einen hinreichend großen Adressraum, um auf absehbare Zeit alle netzfähigen Geräte mit einer eigenen IP-Adresse auszustatten. Die Umstellung erfolge sukzessive. Während der Übergangsphase nutzten viele Diensteanbieter aber eine Technik, mittels derer sich viele Nutzer eine einzige öffentliche IPv4-Adresse unter Zuteilung sogenannter Source Port Numbers teilten. Diese Übergangslösung habe sich zwischenzeitlich zu einem dauerhaften Ersatz für das IPv6 entwickelt, da sie die Nutzungsmöglichkeiten von IPv4-Adressen unbegrenzt vervielfache und die kostenintensive Umstellung hinausgezögert werden könne. Um einen Nutzer in diesem Fall zweifelsfrei identifizieren zu können, müsste neben der IPv4-Adresse insbesondere auch dessen Source Port Number bekannt sein. Diese läge den Sicher- 42

heitsbehörden häufig nicht vor und werde von den Providern nicht zuverlässig gespeichert.

Obgleich bei dem IPv6 nicht mehr das Problem der Mangelverwaltung bestehe, würden auch die IPv6-Adressen vor allem im Privatkundenbereich im Regelfall dynamisch und nicht statisch zugewiesen. Eine statische IP-Adresse könne auf ausdrücklichen Wunsch des Kunden zugewiesen werden, was vor allem im Bereich der Geschäftskunden genutzt werde. 43

b) Die angegriffenen Normen seien verfassungsgemäß. Der Bundesgesetzgeber sei zuständig. § 113 Abs. 4 TKG begründe keine selbständige Auskunftspflicht, sondern richte sich allein an die betroffenen Unternehmen und präzisiere deren Pflichten auf dem Gebiet der Telekommunikation. 44

§ 113 TKG erlaube keine vom Einzelfall losgelöste Massenabfrage. Eine Unverhältnismäßigkeit ergebe sich auch nicht aus § 113 Abs. 5 Satz 2 TKG. Zwar könne einer Regelung, die Datenabfragen sehr vereinfache, indem sie durch ein zentral zusammengefasstes und automatisiertes Verfahren die Daten ohne zeitliche Verzögerungen oder Reibungsverluste durch Prüferfordernisse zur Verfügung stelle, ein erhöhtes Eingriffsgewicht zukommen. Da die Auskunft aber weiterhin nur in Textform und im Einzelfall verlangt werden könne, sei sichergestellt, dass eine Abfrage nicht pauschal und ohne konkreten Anlass erfolge. Auch der mit einem manuellen Verfahren verbundene Verfahrensaufwand bleibe bestehen. Die Schnittstelle erhöhe lediglich die Datensicherheit. 45

§ 113 TKG genüge dem Gebot der Normenklarheit. Der Gesetzgeber habe mit § 113 Abs. 2 Satz 1 TKG klargestellt, dass es für die Datenabfrage einer qualifizierten Rechtsgrundlage für die abrufende Stelle bedürfe und die dafür in Frage kommenden Stellen eindeutig und abschließend bestimmt. Die geschaffenen Abrufregelungen seien durch eine jeweils ausdrückliche Bezugnahme auf die nach §§ 95, 111 TKG erhobenen Daten hinreichend qualifiziert. 46

Die durch § 113 Abs. 1 Satz 3 TKG ermöglichte Identifizierung von IP-Adressen anhand von Verkehrsdaten verstoße nicht gegen Art. 10 Abs. 1 GG. Bei der verfassungsrechtlichen Bewertung sei zu berücksichtigen, dass ein Eingriff durch die Verwendung von Verkehrsdaten nur unvollständig in der Norm selbst geregelt werde. Die Pflicht der Unternehmen, Verkehrsdaten auszuwerten, verwirkliche sich erst in der konkreten Abfrage. Nicht alle verfassungsrechtlich gebo- 47

tenen materiellen und verfahrensrechtlichen Vorgaben könnten aber in der Öffnungsnorm geregelt werden, weil diese nicht als „Vollnorm“ ausgestaltet werden dürfe. Insoweit ergebe sich eine abschließende verfassungsrechtliche Beurteilung nur aus der Zusammenschau von Öffnungsnorm und Abrufbefugnis.

Für die Verwendung von Verkehrsdaten durch die Diensteanbieter zur Identifizierung einer IP-Adresse gälten weniger strenge verfassungsrechtliche Maßstäbe als für deren unmittelbare Verwendung durch Behörden, da diese selbst keinen Einblick in die Verkehrsdaten erhielten. Darüber hinaus werde immer nur ein bestimmter Teil der vorhandenen Verkehrsdaten verwendet. Eine Beschränkung des Anwendungsbereichs auf Straftaten von erheblichem Gewicht sowie auf Gefahren für wichtige Rechtsgüter sei verfassungsrechtlich ebenso wenig geboten wie ein Richtervorbehalt. Sicherzustellen sei lediglich, dass eine Auskunft nur bei Vorliegen eines Anfangsverdachts oder einer konkreten Gefahr auf einzelfallbezogener Tatsachenbasis erfolgen dürfe. Dies gelte auch für die Nachrichtendienste. § 113 Abs. 2 TKG werde diesen Vorgaben gerecht. Die fachgesetzlichen Ermächtigungsgrundlagen setzten auch voraus, dass die Datenerhebung erforderlich sei. Die Rückbindung an einen Einzelfall sei damit gewährleistet. Das Verfahren nach § 113 Abs. 1 Satz 3 TKG könne nicht zur Verfolgung von Ordnungswidrigkeiten genutzt werden, da § 46 Abs. 3 Satz 1 OWiG dem entgegen stehe. Die Formulierung des § 113 Abs. 1 Satz 3 TKG mache auch deutlich, dass es sich um eine Ausnahmeregelung handele und eine Auswertung von Verkehrsdaten zu anderen Zwecken unzulässig sei. 48

Die angegriffenen Abrufregelungen seien ebenfalls verfassungsgemäß. Die Vorgaben des Bundesverfassungsgerichts seien durch den in § 113 Abs. 2 TKG angeordneten Einzelfallbezug in Verbindung mit dem Verweis auf die gesetzlichen Aufgaben der ermächtigten Behörden in den Abrufregelungen eingehalten. Diese Normen enthielten den Bezug auf „die Verhütung und Verfolgung von Straftaten“ (§ 2 Abs. 2 Nr. 1 in Verbindung mit § 7 Abs. 3 Satz 1 BKAG a.F., vgl. § 10 Abs. 1 Satz 1 Nr. 1 BKAG), „auf eine im Einzelfall bestehende Gefahr für Zeugen“ (§ 26 Abs. 1 Satz 1 BKAG a.F.), „auf die konkrete Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes einer Person“ (§ 22a Abs. 1 Satz 1 BPolG) oder auf die allgemeinen gesetzlichen Aufgabenbestimmungen der Nachrichtendienste. Deren Aufgabe der Informationssammlung sei etwa nach § 3 Abs. 1 BVerfSchG auf die Aufklärung bestimmter Beobachtungsobjekte beschränkt. Voraussetzung sei jeweils das Vorliegen tatsächlicher Anhaltspunkte (§ 4 Abs. 1 Satz 3 BVerfSchG), also ein nachrichtendienstlicher Anfangsverdacht. 49

Das Bundeskriminalamt werde ermächtigt, Bestandsdaten abzufragen, soweit dies zur Erfüllung seiner Aufgabe als Zentralstelle nach § 2 Abs. 2 Nr. 1 BKAG für die Wahrnehmung der in § 2 Abs. 1 BKAG beschriebenen Aufgabe erforderlich sei. Nach § 2 Abs. 1 BKAG unterstütze das Bundeskriminalamt als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei die Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung. Nur dazu seien Bestandsdatenabfragen erlaubt und nicht zur bloßen Gefahrenvorsorge. Mit dem Hinweis auf die „Gefahrverhütung“ öffne das Gesetz die Bestandsdatenabfrage lediglich für eine auf spezielle individualisierte Tatsachen begründete Form der Gefahrenabwehr. 50

Die gefahrenabwehrrechtlichen Abrufregelungen wiesen den erforderlichen Einzelfallbezug auf. § 22a Abs. 1 BPolG etwa setze voraus, dass das Auskunftsverlangen der Erforschung des Sachverhalts oder der Ermittlung des Aufenthaltsortes einer Person diene. Soweit § 15 Abs. 2 ZFdG auf § 4 Abs. 2 und 3 ZFdG verweise und durch die Einbeziehung von Vorsorgeaufgaben über den Maßstab einer individuell tatsachenbasierten Abfragebefugnis hinausgehen könnte, dürfte eine allein auf Vorsorge abzielende Abfrage schon wegen § 113 Abs. 2 Satz 1 TKG ausgeschlossen sein, da der Einzelfallbezug einer derartigen Abfrage entgegenstehe. Ergänzend erscheine eine verfassungskonforme Einschränkung der Verweisungsnormen möglich, die diese auf die Gefahren- und Straftatenverhütung beschränke. 51

Auch hinreichende Eingriffsschwellen seien vorgesehen. Alle Abrufregelungen setzten die Erforderlichkeit der Auskunft zur Aufgabenerfüllung voraus. § 20b Abs. 3 BKAG a.F. (vgl. § 40 BKAG) beziehe sich auf § 4a Abs. 1 BKAG a.F. (vgl. § 5 Abs. 1 BKAG) und knüpfe damit an die Abwehr von konkreten Gefahren des internationalen Terrorismus an. Für die Aufgabe des Zeugenschutzes nach § 6 BKAG a.F. (vgl. § 7 BKAG) werde ausdrücklich eine im Einzelfall bestehende Gefahr vorausgesetzt. 52

Es sei unbedenklich, dass § 8d BVerfSchG, § 2b BNDG und § 4b MADG eine Auskunft bereits „zur Erfüllung der Aufgaben“ des jeweiligen Nachrichtendienstes zuließen. Das Fehlen einer besonderen Eingriffsschwelle rechtfertige sich aus den beschränkten Aufgaben der Nachrichtendienste. Das Bundesverfassungsgericht habe angenommen, dass sich aus dem Erfordernis der Erforderlichkeit im Einzelfall ergebe, dass eine Auskunft gemäß § 113 Abs. 1 Satz 1 TKG a.F. zur Aufklä- 53

rung einer bestimmten nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung geboten sein müsse, ohne dass dieses Erfordernis speziell geregelt werden müsste. Insoweit unterscheide sich die Neuregelung nicht von der Vorgängervorschrift.

Es stelle keinen unverhältnismäßigen Eingriff in Art. 10 Abs. 1 GG dar, dass die Bestandsdatenauskunft, die sich dynamischer IP-Adressen bediene, unter denselben Voraussetzungen wie die allgemeine Bestandsdatenauskunft möglich sei. Aufgrund der nur mittelbaren Verwendung von Verkehrsdaten könnten derartige Auskunftsansprüche auch unabhängig von begrenzenden Rechtsgüter- oder Straftatenkatalogen vorgesehen werden. Für Abfragen durch die Nachrichtendienste sei sichergestellt, dass die Erforderlichkeit der Identifizierung in jedem Einzelfall geprüft werde. 54

Soweit das Bundesverfassungsgericht für die Abfrage von Zugangsdaten sichergestellt wissen wolle, dass auch die gesetzlichen Voraussetzungen für die Nutzung der Daten gegeben seien, sei diese Einschränkung in allen Abrufregelungen aufgenommen worden. Die Subsidiarität der Abfrage dieser Daten müsse nicht ausdrücklich geregelt werden. Eine Abfrage ergehe nur nach einer Einzelfallprüfung. Soweit dies verfassungsrechtlich geboten sei, enthielten zudem die Normen, die die Nutzung der abgefragten Daten regelten, besondere Verhältnismäßigkeitsregelungen. Der Eingriff in das Grundrecht auf informationelle Selbstbestimmung sei auch nicht deshalb unverhältnismäßig, weil von einer vorherigen gerichtlichen Entscheidung abgesehen werden könne, wenn der Betroffene Kenntnis von der Abfrage der Zugangsdaten habe oder haben müsse. Es sei gerade die Heimlichkeit einer Maßnahme, die besondere Verfahrenssicherungen wie den Vorbehalt richterlicher Anordnung erfordern könne. Wenn aber der Betroffene Kenntnis vom Herausgabeverlangen habe oder haben müsse, sei ein richterlicher Beschluss entbehrlich. 55

2. Die Bundesdatenschutzbeauftragte erachtet die angegriffenen Regelungen zu einem Teil als verfassungswidrig. Es widerspreche der Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung, dass § 113 Abs. 1 Satz 3 TKG die Auskunft über die Zuordnung einer dynamischen IP-Adresse auch zur Verfolgung einfacher Ordnungswidrigkeiten zulasse (mit Verweis auf BVerfGE 125, 260 <344>). 56

§ 10 Abs. 1 Satz 1 Nr. 1 BKAG in Verbindung mit dem in Bezug genommenen § 2 Abs. 2 Nr. 1 BKAG knüpfe nicht an eine konkrete Aufgabe zur Gefahrenabwehr an, sondern nur an die Aufgaben des Bundeskriminalamts als Zentralstelle. Damit verlange die Vorschrift keinen konkreten Anlass für Datenerhebungen. Die Daten müssten lediglich der Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung dienlich sein, um Gegenstand einer Abfrage zu sein. Die Datenerhebung sei zudem zum Zweck der Erstellung von Analysen erlaubt (§ 2 Abs. 6 Nr. 1 BKAG). Dies lasse Zweifel an der hinreichenden Bestimmtheit und Verhältnismäßigkeit zu. Ein praktischer Bedarf für eine Erhebung von Zugangsdaten zur Erfüllung der Zentralstellenaufgaben bestehe nicht. Die entsprechende Regelung ergebe mangels denkbarer Nutzungsmöglichkeiten keinen Sinn. Die Möglichkeit der Bestandsdatenauskunft anhand von IP-Adressen knüpfe weder an ein konkretes Ermittlungsverfahren noch an eine Gefahrenlage an. Auch die Zuordnung dynamischer IP-Adressen lasse der Wortlaut bereits zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung zu. Bei enger Auslegung könne eine einzelne Abfrage aber noch als verhältnismäßig anzusehen sein, wenn etwa das Bundeskriminalamt auf einer „Internetstreife“ Erkenntnisse über den Anfangsverdacht einer Straftat oder einer Gefahrenlage erhalte. Dann sei die Abfrage der IP-Adresse ein erster Anknüpfungspunkt, um den Sachverhalt an eine zuständige Strafverfolgungs- oder Polizeibehörde weiterzuleiten. 57

§ 7 ZFdG sei noch allgemeiner formuliert und knüpfe lediglich an die Aufgaben des Zollkriminalamts als Zentralstelle nach § 3 ZFdG an. Zu den Zentralstellenaufgaben gehöre es, gemäß § 3 Abs. 9 ZFdG alle notwendigen Informationen zu sammeln und auszuwerten. Über diese Vorschrift würden die Zentralstellenaufgaben gleichzeitig mit den Aufgaben des Zollkriminalamts nach §§ 4 und 5 ZFdG verknüpft (eigene Strafverfolgungsaufgaben, Sicherungs- und Schutzmaßnahmen). § 15 ZFdG setze ebenfalls nur die Erforderlichkeit zur Aufgabenerfüllung für das Zollkriminalamt voraus. 58

§ 22a BPolG knüpfe die Bestandsdatenabfrage nicht durchgehend an das Vorliegen einer konkreten Gefahr. Die Regelung stelle die Voraussetzungen der Bestandsdatenabfrage denen der Generalklausel für Datenerhebungen nach § 21 Abs. 1 und 2 BPolG gleich. § 21 Abs. 1 BPolG lasse es aber bereits ausreichen, dass die Abfrage erforderlich sei, um irgendeine Aufgabe der Bundespolizei zu erfüllen. Gemäß § 21 Abs. 2 Nr. 1 BPolG sei die Datenerhebung zur Verhütung von Straftaten zulässig, soweit Tatsachen die Annahme rechtfertigten, dass betroffene Personen bestimmte Straftaten begehen wollten. Dies schließe aber nicht 59

aus, dass sich die Prognose allein auf allgemeine Erfahrungssätze stütze (mit Verweis auf BVerfGE 141, 220 <291 Rn. 165>). Auch soweit § 22a Abs. 1 Satz 1 BPolG zusätzlich bestimme, dass die Datenerhebung zur Erforschung des Sachverhalts oder des Aufenthaltsorts einer Person erforderlich sein müsse, führe dies nicht zu einer hinreichenden Begrenzung.

§ 20b Abs. 3 BKAG a.F. (vgl. § 40 Abs. 1 BKAG) verweise zunächst nur auf die dem Bundeskriminalamt obliegende Aufgabe der Abwehr von Gefahren des internationalen Terrorismus. Soweit die Datenerhebung auch zur Verhütung von Straftaten nach § 4a Abs. 1 Satz 2 BKAG a.F. (vgl. § 5 Abs. 1 Satz 2 BKAG) zulässig sei, wenn Tatsachen die Annahme rechtfertigten, dass betroffene Personen entsprechende Straftaten begehen wollten, sei wiederum nicht ausgeschlossen, dass sich die Prognose allein auf allgemeine Erfahrungssätze stütze. 60

Voraussetzung für eine Bestandsdatenabfrage durch die Nachrichtendienste sei lediglich, dass sie zur Erfüllung von deren Aufgaben erforderlich sei. Dies schränke die Befugnis faktisch nicht ein, da sich die Erforderlichkeit im Bereich der Nachrichtendienste leicht begründen lasse. 61

Es gebe zudem Defizite bei den verfahrenssichernden Maßnahmen. Die Einführung eines Richtervorbehalts für die Auskunft über den Inhaber einer IP-Adresse sei datenschutzrechtlich geboten, was maßgeblich mit dem Bedeutungszuwachs des Internets in den letzten Jahren zu begründen sei. Da für die allgemeine Bestandsdatenauskunft keine Benachrichtigungspflicht vorgesehen sei, erfolge die Abfrage heimlich. Dies wirke sich auf die Eingriffsintensität aus. Hierbei sei zu berücksichtigen, dass Betroffene über eine Speicherung beauskunfteter Daten in der Regel auch nicht auf anderem Wege informiert würden. Eine zentrale Protokollierung der Datenerhebungen durch die Behörden sei nicht vorgesehen. Dies könne die datenschutzrechtliche Kontrolle erschweren. Da die Daten gegenüber Betroffenen nicht offen erhoben würden, sei eine anlassunabhängige Datenschutzkontrolle notwendig, um den durch die Heimlichkeit eingeschränkten Rechtsschutz zu kompensieren. 62

B.

Die Verfassungsbeschwerden sind überwiegend zulässig. 63

I.

Die Beschwerdeführenden wenden sich mit ihren Rechtssatzverfassungsbeschwerden gegen Übermittlungs- und Abrufregelungen von Bestandsdaten im manuellen Auskunftsverfahren. Unmittelbar richten sich ihre Angriffe gegen die die Diensteanbieter jeweils ermächtigenden Befugnisnormen zur Übermittlung von Bestandsdaten im Allgemeinen (§ 113 Abs. 1 Satz 1 TKG), von Zugangsdaten (§ 113 Abs. 1 Satz 1 und 2 TKG) und von Bestandsdaten, die anhand dynamischer IP-Adressen bestimmt werden (§ 113 Abs. 1 Satz 1 und 3 TKG). Sie wenden sich zudem gegen die damit korrespondierenden Befugnisnormen, die die verschiedenen Sicherheitsbehörden jeweils zum Abruf dieser Daten ermächtigen. Mittelbar erstrecken sich die Angriffe auf die weiteren Regelungen der angegriffenen Normen, mit denen der Gesetzgeber die Befugnisse zur Gewährleistung der Verhältnismäßigkeit flankiert und ohne die deren Verfassungsmäßigkeit nicht beurteilt werden kann. 64

Die Verfassungsbeschwerden richten sich daher gegen § 113 TKG, § 7 Abs. 3 bis 7, § 20b Abs. 3 bis 7 und § 22 Abs. 2 bis 4 BKAG, § 22a BPolG, § 7 Abs. 5 bis 9, § 15 Abs. 2 bis 6 ZFdG, § 8d BVerfSchG, § 2b BNDG und § 4b MADG jeweils in der Fassung vom 20. Juni 2013 sowie gegen §§ 10, 40 BKAG in der Fassung vom 1. Juni 2017, § 4 BNDG in der Fassung vom 23. Dezember 2016 und § 7 Abs. 7, § 15 Abs. 4 ZFdG in der Fassung vom 3. Dezember 2015. Dabei erstrecken sich die Verfassungsbeschwerden nicht auf die Regelungen, die die Speicherung der im manuellen Auskunftsverfahren verwendeten Bestands- und Verkehrsdaten betreffen. Nicht Gegenstand der Verfassungsbeschwerden sind daher die §§ 95 ff. TKG, die die Speicherung dieser Daten zu betriebsinternen Zwecken erlauben, sowie die §§ 111, 113a ff. TKG, die Diensteanbieter zur Speicherung von Bestands- und Verkehrsdaten verpflichten. 65

II.

Die Verfassungsbeschwerden sind teilweise unzulässig. Soweit die Beschwerdeführenden zu I. mit nachgereichtem Schriftsatz ihre Angriffe auf § 4 BNDG in der Fassung vom 23. Dezember 2016 und § 7 Abs. 7, § 15 Abs. 4 ZFdG in der Fassung vom 3. Dezember 2015 erstreckt haben, ist ihre Verfassungsbeschwerde verfristet. Obgleich sie schon die jeweilige Vorgängerreglung fristgemäß angegriffen haben, erstreckt sich ihre Verfassungsbeschwerde nicht automatisch auf die an ihre Stelle getretene Norm; dies gilt selbst dann, wenn die 66

Neuregelung – wie hier § 4 BNDG – inhaltsgleich zu der Vorgängerregelung ist (vgl. BVerfGE 87, 181 <194>).

Zwar waren die Beschwerdeführenden nicht gehindert, ihre Verfassungsbeschwerde auf die neuen Regelungen umzustellen (vgl. BVerfGE 87, 181 <194>), wenngleich die Frist zur Erhebung einer Verfassungsbeschwerde durch – wie hier – bloß redaktionelle, nicht inhaltliche Änderungen der Vorschriften nicht erneut zu laufen beginnt (vgl. BVerfGE 12, 139 <141>; BVerfGK 18, 328 <335>; vgl. auch Peters, in: Barczak, BVerfGG, 2018, § 93 Rn. 141). Wird aber Beschwerdeführenden die Umstellung ihrer bereits gegen die vorherige Gesetzesfassung erhobenen Verfassungsbeschwerde ermöglicht, so muss die Umstellung ihrerseits die Jahresfrist wahren. Da aber § 4 BNDG bereits zum 31. Dezember 2016 und § 7 Abs. 7, § 15 Abs. 4 ZFdG zum 1. Januar 2016 in Kraft getreten sind, wahrte die am 1. April 2019 erfolgte Erstreckung der Verfassungsbeschwerde auf diese Vorschriften nicht mehr die Jahresfrist des § 93 Abs. 3 BVerfGG (siehe aber zur Erstreckung nach § 78 Satz 2 BVerfGG unten, Rn. 267). 67

Für die Verfassungsbeschwerde der Beschwerdeführenden zu II. gegen die § 7 Abs. 3 bis 7, § 20b Abs. 3 bis 7 und § 22 Abs. 2 bis 4 BKAG in der Fassung vom 20. Juni 2013 fehlt das Rechtsschutzinteresse, da die Regelungen am 25. Mai 2018 außer Kraft getreten sind (vgl. BVerfGE 100, 271 <281 f.>; 108, 370 <383>). Ein Rechtsschutzinteresse besteht hier auch nicht ausnahmsweise deshalb fort, weil ansonsten die Klärung verfassungsrechtlicher Fragen von grundsätzlicher Bedeutung unterbliebe (vgl. BVerfGE 81, 138 <140>; 100, 271 <281 f.>; stRspr). Die im Hinblick auf die Altregelungen auftretenden Fragen stellen sich in gleicher Weise bei den von den Beschwerdeführenden zu I. angegriffenen Neuregelungen in §§ 10, 40 BKAG, lassen sich also in diesem Zusammenhang klären. 68

III.

Im Übrigen sind die Verfassungsbeschwerden zulässig. 69

1. Die Beschwerdeführenden sind beschwerdebefugt. 70

a) Sie nutzen Mobilfunkkarten, Festnetzanschlüsse und Internetzugangsdienste und machen geltend, durch die Übermittlung und den Abruf ihrer nach §§ 95, 111 TKG gespeicherten Daten auf der Grundlage der hier angegriffenen Vorschriften in ihrem Recht auf informationelle Selbstbestimmung aus Art. 2 71

Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG sowie in ihrem Grundrecht auf Wahrung des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG verletzt zu sein. Eine Grundrechtsverletzung ist jedenfalls möglich.

b) Die angegriffenen Vorschriften betreffen die Beschwerdeführenden unmittelbar, selbst und gegenwärtig. Ihre Verfassungsbeschwerden erfüllen die spezifischen Anforderungen, die für unmittelbar gegen Gesetze gerichtete Verfassungsbeschwerden gelten. 72

aa) Die Beschwerdeführenden sind von den angegriffenen Vorschriften unmittelbar betroffen. Zwar werden die hier angegriffenen Regelungen zur Übermittlung und zum Abruf von Bestandsdaten erst auf der Grundlage weiterer Vollzugsakte in Form von Auskunftsverlangen und Auskunftserteilung wirksam. Von einer unmittelbaren Betroffenheit durch ein vollziehungsbedürftiges Gesetz ist jedoch auch dann auszugehen, wenn Beschwerdeführende den Rechtsweg nicht beschreiten können, weil sie keine Kenntnis von der Maßnahme erlangen oder wenn eine nachträgliche Bekanntgabe zwar vorgesehen ist, von ihr aber aufgrund weitreichender Ausnahmetatbestände auch langfristig abgesehen werden kann (vgl. BVerfGE 150, 309 <324 Rn. 35>; stRspr). So liegt es hier. 73

Die Beschwerdeführenden erlangen weder von dem an einen Diensteanbieter gerichteten Auskunftsverlangen noch von der Auskunftserteilung selbst verlässlich Kenntnis (vgl. auch BVerfGE 133, 277 <312 Rn. 84>; 150, 309 <324 f. Rn. 36>). Dies gilt auch, soweit die Abrufregelungen für die Beauskunftung von Zugangsdaten sowie der anhand dynamischer IP-Adressen bestimmten Daten Benachrichtigungspflichten vorsehen, da diese weitreichende Ausnahmen enthalten und möglicherweise erst spät greifen (vgl. BVerfGE 120, 378 <394>; 141, 220 <261 Rn. 82>). Für die allgemeine Bestandsdatenauskunft bestehen von vornherein keine Benachrichtigungspflichten. 74

bb) Die Beschwerdeführenden sind durch die angegriffenen Regelungen auch selbst und gegenwärtig betroffen. Da sie weithin keine verlässliche Kenntnis von den Vollzugsakten erlangen, reicht es, wenn sie darlegen, mit einiger Wahrscheinlichkeit von solchen Maßnahmen berührt zu werden. Maßgeblich hierfür ist, dass die durch § 113 TKG und die Abrufregelungen ermöglichten Auskünfte eine große Streubreite haben und Dritte auch zufällig erfassen können. Darlegungen, durch die sich die Beschwerdeführenden selbst einer Straftat bezichtigen müssten, sind zum Beleg der Selbstbetroffenheit ebenso wenig erforderlich wie der Vortrag, für 75

sicherheitsgefährdende oder nachrichtendienstlich relevante Aktivitäten verantwortlich zu sein (BVerfGE 130, 151 <176 f.>).

2. Die Verfassungsbeschwerden genügen den Anforderungen der Subsidiarität. 76

a) Auch vor Erhebung von Rechtssatzverfassungsbeschwerden sind nach dem Grundsatz der Subsidiarität grundsätzlich alle Mittel zu ergreifen, die der geltend gemachten Grundrechtsverletzung abhelfen können. Zu den zumutbaren Rechtsbehelfen kann die Erhebung einer Feststellungs- oder Unterlassungsklage gehören, die eine fachgerichtliche Klärung entscheidungserheblicher Tatsachen- oder Rechtsfragen des einfachen Rechts ermöglicht (vgl. zuletzt BVerfGE 150, 309 <326 ff. Rn. 41 ff.>; stRspr). Anders liegt dies jedoch, soweit es allein um die sich unmittelbar aus der Verfassung ergebenden Grenzen für die Auslegung der Normen geht. Soweit die Beurteilung einer Norm allein spezifisch verfassungsrechtliche Fragen aufwirft, die das Bundesverfassungsgericht zu beantworten hat, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung verbesserte Entscheidungsgrundlagen zu erwarten wären, bedarf es einer vorangehenden fachgerichtlichen Entscheidung nicht (vgl. BVerfGE 123, 148 <172 f.>; 143, 246 <322 Rn. 211>; stRspr). Insoweit bleibt es dabei, dass Verfassungsbeschwerden unmittelbar gegen ein Gesetz weithin auch ohne vorherige Anrufung der Fachgerichte zulässig sind (BVerfGE 150, 309 <326 f. Rn. 44>). Eine Pflicht zur Anrufung der Fachgerichte kann auch sonst unzumutbar sein (vgl. BVerfGE 150, 309 <327 f. Rn. 45>). 77

b) Danach mussten die Beschwerdeführenden vor Erhebung der Verfassungsbeschwerden keinen fachgerichtlichen Rechtsschutz gegen die angegriffenen Vorschriften suchen. Die ausschließlich gegen Gesetze gerichteten Verfassungsbeschwerden werfen im Kern allein spezifisch verfassungsrechtliche Fragen auf, die das Bundesverfassungsgericht zu beantworten hat, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung substantiell verbesserte Entscheidungsgrundlagen zu erwarten wären. Die verfassungsrechtliche Beurteilung hängt nicht von der fachrechtlichen Auslegung der einzelnen Tatbestandsmerkmale der angegriffenen Befugnisse zur Übermittlung und zum Abruf von Bestandsdaten ab, sondern maßgeblich von deren hinreichender gesetzlicher Begrenzung und Bestimmtheit. 78

3. a) Die Verfassungsbeschwerden gegen § 113 TKG und die fachrechtlichen Abrufregelungen in der Fassung vom 20. Juni 2013 wurden fristgerecht erhoben. Zwar regelte § 113 TKG schon in früheren Fassungen die manuelle Bestandsdatenauskunft. Die angegriffene Neuregelung wurde aber in weiten Teilen grundlegend geändert. § 113 TKG ist nun ausdrücklich nur als Übermittlungsbefugnis ausgestaltet, die fachrechtliche Abrufregelungen voraussetzt. Insbesondere die abrufberechtigten Behörden wurden neu geregelt und die Verwendungszwecke der Bestandsdaten abweichend begrenzt. Erstmals berechtigt die Vorschrift zur Auskunft über Bestandsdaten, die anhand einer dynamischen IP-Adresse bestimmt werden (§ 113 Abs. 1 Satz 3 TKG). 79

Auch § 113 Abs. 1 Satz 2 TKG konnte fristgerecht angegriffen werden. Zwar hat die Norm gegenüber der Vorgängerregelung vom 22. Juni 2004 (BGBl I S. 1190) – trotz geänderten Wortlauts und neuer Regelungsstruktur – für sich genommen keinen grundsätzlich neuen Gehalt. Die Vorgängerregelung wurde jedoch für verfassungswidrig erklärt (BVerfGE 130, 151). Wenn der Gesetzgeber nunmehr eine Regelung mit im Wesentlichen gleichem Inhalt wiederholt, stellt diese einen neuen verfassungsrechtlichen Prüfungsgegenstand dar (vgl. dazu BVerfGE 96, 260 <263>; 102, 127 <141>; vgl. auch BVerfGE 135, 259 <281 Rn. 36>). Die Jahresfrist des § 93 Abs. 3 BVerfGG begann daher mit Inkrafttreten der angegriffenen Regelungen zum 1. Juli 2013 neu zu laufen (vgl. auch BVerfGE 130, 151 <177> m.w.N.). 80

b) Soweit die Beschwerdeführenden zu I. ihre Verfassungsbeschwerde auf die am 25. Mai 2018 in Kraft getretenen §§ 10, 40 BKAG in der Fassung vom 1. Juni 2017 umgestellt haben, ist die Jahresfrist ebenfalls gewahrt. Dabei spielt es keine Rolle, dass die Neuregelungen weitgehend dem materiellen Gehalt der Vorgängerregelungen entsprechen, da schon die Vorgängerregelungen fristgerecht angegriffen wurden und die Umstellung ihrerseits innerhalb der Jahresfrist erfolgte. 81

4. Durch die geringfügige Änderung der § 7 Abs. 7, § 15 Abs. 4 ZFdG zum 1. Januar 2016 und die Neubezeichnung des § 2b BNDG als § 4 BNDG zum 31. Dezember 2016 ist das Rechtsschutzinteresse für die Verfassungsbeschwerden gegen die Vorschriften in ihrer Fassung vom 20. Juni 2013 insoweit nicht entfallen. Ihr Regelungsgehalt wurde nicht verändert und die Verfassungsbeschwerden sind von daher insoweit nicht gegenstandslos (vgl. auch BVerfGE 108, 370 <383>). 82

IV.

Die angegriffenen Vorschriften haben teilweise Bezüge zu datenschutzrechtlichen Bestimmungen in Richtlinien und Verordnungen der Europäischen Union. Gleichwohl ist die Zuständigkeit des Bundesverfassungsgerichts für die Prüfung dieser Normen eröffnet und die Verfassungsbeschwerden sind zulässig, da es sich jedenfalls nicht um die Umsetzung zwingenden Unionsrechts handelt. 83

1. Allerdings übt das Bundesverfassungsgericht grundsätzlich keine Kontrolle über unionsrechtliches Fachrecht aus und überprüft dieses Recht nicht am Maßstab der Grundrechte des Grundgesetzes, solange die Unionsgrundrechte einen wirksamen Schutz der Grundrechte generell bieten, der dem vom Grundgesetz jeweils als unabdingbar gebotenen Grundrechtsschutz im Wesentlichen gleich zu achten ist, zumal den Wesensgehalt der Grundrechte generell verbürgen; maßgeblich ist insoweit eine auf das jeweilige Grundrecht des Grundgesetzes bezogene generelle Betrachtung (vgl. BVerfGE 73, 339 <387>; 102, 147 <162 f.>; 125, 260 <306>; BVerfG, Beschluss des Ersten Senats vom 6. November 2019 - 1 BvR 276/17 -, Rn. 47 a.E. – Recht auf Vergessen II). Diese Grundsätze gelten nach der bisherigen Rechtsprechung des Bundesverfassungsgerichts auch für die Überprüfung innerstaatlicher Rechtsvorschriften, die zwingende Vorgaben in deutsches Recht umsetzen (vgl. BVerfGE 118, 79 <95 ff.>; BVerfG, Beschluss des Zweiten Senats vom 11. März 2020, - 2 BvL 5/17 -, Rn. 65). Verfassungsbeschwerden, die sich gegen in diesem Sinne verbindliches Fachrecht der Europäischen Union richten, sind danach grundsätzlich unzulässig (vgl. BVerfGE 118, 79 <95>; 121, 1 <15>; 125, 260 <306>; siehe hingegen zur bundesverfassungsgerichtlichen Kontrolle am Maßstab der Unionsgrundrechte im Fall der Überprüfung der *Anwendung* von zwingendem Recht der Europäischen Union und der *Anwendung* innerstaatlicher Vorschriften, die zwingendes Unionsrecht umsetzen, BVerfG, Beschluss des Ersten Senats vom 6. November 2019 - 1 BvR 276/17 -, Rn. 52; die Möglichkeit bundesverfassungsgerichtlicher Kontrolle am Maßstab der Unionsgrundrechte im Fall der *Normprüfung* offenlassend jetzt BVerfG, Beschluss des Ersten Senats vom 6. November 2019 - 1 BvR 276/17 -, Rn. 51 a.E.; Beschluss des Zweiten Senats vom 13. Februar 2020 - 2 BvR 739/17 -, Rn. 116 – Einheitliches Patentgericht). 84

2. Danach sind die angegriffenen Vorschriften am Maßstab des Grundgesetzes überprüfbar, denn sie beruhen nicht auf zwingenden Vorgaben des Unionsrechts. Sie setzen nicht vollständig vereinheitlichendes Unionsrecht um. Das gilt 85

zunächst, soweit die angegriffenen Vorschriften in den Anwendungsbereich der 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 EU, L 201 vom 31. Juli 2002, S. 37, im Folgenden: RL 2002/58/EG) oder der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl EU, L 119 vom 4. Mai 2016, S. 89, im Folgenden: RL 2016/680/EU) fallen könnten. Zielsetzung dieser Unionsrechtsakte ist der Schutz personenbezogener Daten. Sie enthalten dagegen keine Bestimmungen, die die Mitgliedstaaten zur Schaffung von Regelungen zum Abruf von Bestandsdaten verpflichten oder ihnen sonst hierzu abschließende Vorgaben machen. Vielmehr sehen sie mehr oder minder begrenzte Öffnungsklauseln vor, die den Mitgliedstaaten die Schaffung derartiger Regelungen zwar grundsätzlich ermöglichen, aber nicht gebieten (so etwa in Art. 15 Abs. 1 RL 2002/58/EG; vgl. EuGH, Urteil vom 29. Januar 2008, Promusicae, C-275/06, EU:C:2008:54, Rn. 50) oder gehen von vornherein nicht über die Verpflichtung zur Wahrung datenschutzrechtlicher Grundsätze hinaus (so etwa Kapitel II RL 2016/680/EU).

Nichts Anderes gilt auch insoweit, als die Vorschriften teilweise in den Anwendungsbereich der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, ABl EU, L 119 vom 4. Mai 2016, S. 1, im Folgenden: DSGVO) fallen mögen. Die Datenschutzgrundverordnung erstrebt zwar grundsätzlich eine unionsrechtliche Vereinheitlichung des Datenschutzes. Dies besagt aber nicht, dass alle Einzelregelungen unionsweit vereinheitlicht sind. So belassen für die hier in Frage stehenden Regelungen insbesondere Art. 6 Abs. 2 und 3 DSGVO den Mitgliedstaaten erhebliche Gestaltungsspielräume (vgl. Kühling/Martini u.a., Die Datenschutz-Grundverordnung und das nationale Recht, 2016, S. 28; anders hingegen für die dortige Rechtslage BVerfG, Beschluss des Ersten Senats vom 6. November 2019 - 1 BvR 276/17 -, Rn. 33 ff.). 86

Handelt es sich also – wie vorliegend – nicht um vollständig unionsrechtlich determiniertes Recht, sondern um innerstaatliche Normen im nicht voll vereinheit- 87

lichten Bereich, prüft das Bundesverfassungsgericht die angegriffenen Normen am Maßstab der Grundrechte des Grundgesetzes. Das gilt im Grundsatz unabhängig davon, ob und wieweit die angegriffenen Vorschriften nach der Rechtsprechung des Gerichtshofs der Europäischen Union zugleich als Durchführung des Unionsrechts im Sinne des Art. 51 Abs. 1 Satz 1 GRCh angesehen werden können (vgl. zur RL 2002/58/EG EuGH, Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u.a., C-203/15 u.a., EU:C:2016:970, Rn. 78 ff.; Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 29 ff.) und deshalb daneben auch die Unionsgrundrechte Geltung beanspruchen können (vgl. dazu BVerfG, Beschluss des Ersten Senats vom 6. November 2019 - 1 BvR 16/13 -, Rn. 39 – Recht auf Vergessen I; näher unter Rn. 261).

3. Unberührt bleibt hiervon die Frage, ob sich weitere rechtliche Anforderungen unmittelbar aus dem Sekundärrecht der Europäischen Union ergeben, insbesondere aus Art. 15 Abs. 1 RL 2002/58/EG hinsichtlich der Reichweite der den Diensteanbietern auferlegten Pflichten. Die Auslegung und Anwendung des Fachrechts der Europäischen Union ist nicht Sache des Bundesverfassungsgerichts, sondern obliegt den Fachgerichten im Verbund mit dem Europäischen Gerichtshof (BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 85 m.w.N. – BND – Ausland-Ausland-Aufklärung). 88

C.

Die Verfassungsbeschwerden sind überwiegend begründet. Die angegriffenen Vorschriften genügen in weiten Teilen nicht den Anforderungen an die Verhältnismäßigkeit. 89

I.

Die Regelungen zur Übermittlung und zum Abruf von Bestandsdaten greifen in das Recht auf informationelle Selbstbestimmung des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG ein. Soweit sie auch zur Übermittlung und zum Abruf von Bestandsdaten ermächtigen, die anhand dynamischer IP-Adressen bestimmt werden, liegt ein Eingriff in das speziellere Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG vor. 90

1. § 113 Abs. 1 Satz 1 und 2 TKG sowie die damit korrespondierenden fachrechtlichen Abrufregelungen (§ 10 Abs. 1 Satz 1 und 2, § 40 Abs. 1 Satz 1 91

und 2 BKAG, § 22a Abs. 1 Satz 1 und 2 BPolG, § 7 Abs. 5 Satz 1 und 2, § 15 Abs. 2 Satz 1 und 2 ZFdG, § 8d Abs. 1 Satz 1 und 2 BVerfSchG sowie § 2b Satz 1 BNDG und § 4b Satz 1 MADG, soweit sie Bezug auf § 8d Abs. 1 Satz 1 und 2 BVerfSchG nehmen) greifen in das Recht auf informationelle Selbstbestimmung ein.

a) Das Recht auf informationelle Selbstbestimmung trägt Gefährdungen und Verletzungen der Persönlichkeit Rechnung, die sich unter den Bedingungen moderner Datenverarbeitung aus informationsbezogenen Maßnahmen ergeben (vgl. BVerfGE 65, 1 <42>; 120, 378 <397>). Die freie Entfaltung der Persönlichkeit setzt den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist von dem Grundrecht aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (BVerfGE 113, 29 <46> m.w.N.). Die Gewährleistung greift insbesondere, wenn die Entfaltung der Persönlichkeit dadurch gefährdet wird, dass personenbezogene Informationen von staatlichen Behörden in einer Art und Weise genutzt und verknüpft werden, die Betroffene weder überschauen noch beherrschen können (vgl. BVerfGE 118, 168 <184>). Hierunter fallen auch personenbezogene Informationen zu den Modalitäten der Bereitstellung von Telekommunikation (vgl. BVerfGE 130, 151 <184>; vgl. auch EuGH, Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 51). 92

Vorschriften, die zum Umgang mit personenbezogenen Daten durch staatliche Behörden ermächtigen, begründen in der Regel verschiedene, aufeinander aufbauende Eingriffe. Es ist zwischen der Erhebung, Speicherung und Verwendung von Daten zu unterscheiden (vgl. BVerfGE 100, 313 <366 f.>; 120, 378 <400 f.>; 125, 260 <310>; vgl. auch EGMR (GK), S. and Marper v. The United Kingdom, Urteil vom 4. Dezember 2008, Nr. 30562/04 u.a., § 67; EuGH, Urteil vom 8. April 2014, Digital Rights Ireland und Seitlinger u.a., C-293/12 u.a., EU:C:2014:238, Rn. 34 ff.). Bei der Regelung eines Datenaustauschs zur staatlichen Aufgabenwahrnehmung ist darüber hinaus aber auch zwischen der Datenübermittlung seitens der auskunfterteilenden Stelle und dem Datenabruf seitens der auskunftsuchenden Stelle zu unterscheiden. Ein Datenaustausch vollzieht sich durch die einander korrespondierenden Eingriffe von Abfrage und Übermittlung, die jeweils einer eigenen Rechtsgrundlage bedürfen. Der Gesetzgeber muss, bildlich gesprochen, nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür 93

zu deren Abfrage. Erst beide Rechtsgrundlagen gemeinsam, die wie eine Doppeltür zusammenwirken müssen, berechtigen zu einem Austausch personenbezogener Daten (BVerfGE 130, 151 <184>).

b) Die angegriffenen Vorschriften greifen in das Recht auf informationelle Selbstbestimmung ein. 94

Einen eigenständigen Grundrechtseingriff begründen zunächst § 113 Abs. 1 Satz 1 und 2 TKG, die die Diensteanbieter auf Verlangen einer abrufberechtigten Behörde verpflichten, über die von ihnen nach den §§ 95 und 111 TKG gespeicherten Daten Auskunft zu erteilen (vgl. BVerfGE 130, 151 <185>). Zwar berechtigen die Regelungen allein noch nicht zum Datenaustausch. Vielmehr bedarf es – nach dem Bild einer Doppeltür – für den Abruf der Daten einer weiteren Rechtsgrundlage (vgl. BVerfGE 125, 260 <312>; 130, 151 <185>; 150, 244 <278 Rn. 80>; 150, 309 <335 Rn. 68>). Doch obgleich § 113 TKG seitens der abrufberechtigten Behörden eigene Erhebungsbefugnisse voraussetzt, haben § 113 Abs. 1 Satz 1 und 2 TKG allein als Rechtsgrundlage für die Übermittlung bereits Eingriffsqualität (vgl. BVerfGE 130, 151 <185>). Schon die Bestimmung der Verwendungszwecke und die Befugnis zur Datenübermittlung als Teil der Verwendungsregelung begründen den Eingriffscharakter. Dabei ist es unerheblich, dass § 113 TKG eine Übermittlung der Daten seitens privater Diensteanbieter betrifft (vgl. BVerfGE 125, 260 <312>). 95

Ein hiervon zu unterscheidender, eigenständiger Eingriff liegt in den mit § 113 Abs. 1 Satz 1 und 2 TKG korrespondierenden Abrufregelungen des Bundes, die den in § 113 TKG tatbestandlich vorausgesetzten Abruf der Daten seitens der auskunftsberechtigten Behörden regeln (vgl. BVerfGE 130, 151 <185>). 96

2. § 113 Abs. 1 Satz 3 TKG sowie die damit korrespondierenden fachrechtlichen Abrufregelungen (§ 10 Abs. 2, § 40 Abs. 2 BKAG, § 22a Abs. 2 BPolG, § 7 Abs. 6, § 15 Abs. 3 ZFdG, § 8d Abs. 2 Satz 1 BVerfSchG sowie § 2b Satz 1 BNDG und § 4b Satz 1 MADG, soweit sie Bezug auf § 8d Abs. 2 Satz 1 BVerfSchG nehmen), die eine Zuordnung dynamischer IP-Adressen ermöglichen, greifen in Art. 10 Abs. 1 GG ein. 97

a) Art. 10 Abs. 1 GG gewährleistet das Telekommunikationsgeheimnis, das die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs vor einer Kenntnisnahme durch die öffent- 98

liche Gewalt schützt. Dabei erfasst Art. 10 Abs. 1 GG nicht nur die Inhalte der Kommunikation. Geschützt ist vielmehr auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs, zu denen insbesondere gehört, ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist (vgl. BVerfGE 125, 260 <309> m.w.N.; stRspr). Art. 10 Abs. 1 GG schützt allerdings allein die Vertraulichkeit konkreter Telekommunikationsvorgänge und nicht die bloße Zuordnung einer Telekommunikationsnummer oder einer statischen IP-Adresse zu einem Anschlussinhaber als solche. Außerhalb der laufenden Telekommunikation verortet, geben diese Nummern lediglich abstrakt darüber Auskunft, welcher Bürger über welche Telekommunikationsmittel verfügt und über sie erreichbar ist, ohne dass unmittelbar ein Bezug zu einem konkreten Telekommunikationsvorgang besteht. Dies stellt für sich genommen die Vertraulichkeit einzelner Kommunikationsvorgänge nicht in Frage (vgl. BVerfGE 130, 151 <180 f.>).

Anders liegt es demgegenüber bei der identifizierenden Zuordnung dynami- 99
scher IP-Adressen. Diese fällt in den Schutzbereich des Art. 10 Abs. 1 GG (vgl. BVerfGE 130, 151 <181>; vgl. auch EGMR, Benedik v. Slovenia, Urteil vom 24. April 2018, Nr. 62357/14, §§ 130 ff., wonach derartige Maßnahmen das Recht auf Achtung des Privatlebens aus Art. 8 Abs. 1 EMRK berühren). Allerdings ergibt sich dies nicht schon daraus, dass sich die Zuordnung einer dynamischen IP-Adresse notwendig immer auf einen bestimmten Telekommunikationsvorgang bezieht, über den sie damit mittelbar ebenso Auskunft gibt. Denn auch insoweit betrifft die Auskunft selbst nur Daten, die einem Anschlussinhaber abstrakt zugewiesen sind. Die Betroffenheit des Art. 10 Abs. 1 GG wird hier vielmehr dadurch begründet, dass die Diensteanbieter für die Identifizierung einer dynamischen IP-Adresse in einem Zwischenschritt die entsprechenden Verbindungsdaten ihrer Kunden sichten und dafür auf konkrete Telekommunikationsvorgänge zugreifen müssen. Diese von den Diensteanbietern gespeicherten Telekommunikationsverbindungen unterliegen dem Schutz des Telekommunikationsgeheimnisses und zwar unabhängig davon, ob sie von den Diensteanbietern auf vertraglicher Grundlage (vgl. § 96 TKG) gespeichert (vgl. BVerfGE 130, 151 <181 ff.>) oder aufgrund gesetzlicher Verpflichtung (vgl. §§ 113a, 113b TKG) vorrätig gehalten werden müssen (vgl. BVerfGE 125, 260 <312>). Die staatlich auferlegte Pflicht zu deren Nutzung ist selbst dann an Art. 10 Abs. 1 GG zu messen, wenn die Verbindungsdaten selbst nicht herausgegeben werden (vgl. BVerfGE 130, 151 <182 f.>).

Das aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG folgende Recht auf informationelle Selbstbestimmung kommt neben Art. 10 GG nicht zur Anwendung, denn bezogen auf die Telekommunikation enthält Art. 10 GG eine spezielle Garantie, die die allgemeine Vorschrift verdrängt und aus der sich besondere Anforderungen für die Daten ergeben, die durch Eingriffe in das Telekommunikationsgeheimnis erlangt werden. Insoweit lassen sich allerdings die Maßgaben, die das Bundesverfassungsgericht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG entwickelt hat, weitgehend auf die speziellere Garantie des Art. 10 GG übertragen (vgl. BVerfGE 100, 313 <358 f.>; 125, 260 <310>). 100

b) Nach diesen Maßstäben greift § 113 Abs. 1 Satz 3 TKG in das Grundrecht aus Art. 10 Abs. 1 GG ein, da er die Zuordnung dynamischer IP-Adressen zu ihren Anschlussinhabern ermöglicht. Gegenstand der Auskunft ist zwar allein der Anschlussinhaber der abgefragten IP-Adresse und damit ein Bestandsdatum. Soweit die Diensteanbieter hierüber Auskunft zu geben haben, müssen sie aber zunächst auf die von ihnen gespeicherten Verkehrsdaten sowie gegebenenfalls weitere unternehmensinterne Datenquellen (vgl. § 113 Abs. 1 Satz 4 TKG), bei denen es sich ebenfalls um Verbindungsdaten handeln kann, zugreifen und diese auswerten. Soweit § 113 Abs. 1 Satz 3 TKG die Nutzung von Verkehrsdaten eröffnet, die aufgrund der Regelungen zur Vorratsdatenspeicherung gespeichert wurden, ist die Vorschrift überdies schon deshalb an Art. 10 Abs. 1 GG zu messen, weil sie eine Folgeverwendung von Daten ermöglicht, die einmal in Form eines Eingriffs in Art. 10 Abs. 1 GG erhoben worden sind (vgl. BVerfGE 125, 260 <312 f.>). 101

c) Die angegriffenen fachrechtlichen Abrufregelungen begründen einen eigenständigen Eingriff in Art. 10 Abs. 1 GG, soweit sie zur Abfrage anhand einer dynamischen IP-Adresse bestimmter Bestandsdaten durch jeweils auskunftsberechtigte Behörden ermächtigen. 102

II.

Die angegriffenen Vorschriften sind formell verfassungsgemäß. Insbesondere steht dem Bund sowohl für § 113 TKG als auch für die Abrufregelungen in den jeweiligen Fachgesetzen die Gesetzgebungskompetenz zu. 103

1. Der Bund kann die in § 113 TKG enthaltenen Regelungen kraft Sachzu- 104
sammenhangs zu seiner Kompetenz für das Telekommunikationsrecht nach Art. 73 Abs. 1 Nr. 7 GG treffen.

a) Die Kompetenz kraft Sachzusammenhangs ermöglicht dem Bund die Rege- 105
lung solcher datenschutzrechtlicher Bestimmungen, die verständigerweise nur im Zusammenhang mit den Bestimmungen zur Errichtung einer Telekommunikationsinfrastruktur und zur Informationsübermittlung mit Hilfe von Telekommunikationsanlagen geregelt werden können (vgl. BVerfGE 125, 260 <314>; 130, 151 <192>). Dazu gehören neben Bestimmungen zum Schutz der Daten umgekehrt auch Bestimmungen, die die Grenzen dieses Schutzes bestimmen und festlegen, unter welchen Bedingungen und zu welchen Zwecken Daten für die Wahrnehmung öffentlicher Aufgaben zur Verfügung gestellt werden (BVerfGE 130, 151 <192 f.>). Hiernach kann der Bund die Telekommunikationsdiensteanbieter berechtigen und – in Korrespondenz zu einer fachrechtlich begründeten Auskunftspflicht – auch verpflichten, für bestimmte, von ihm im Einzelnen zu regelnde Zwecke solche Daten bei Vorliegen eines wirksamen Datenabrufs an bestimmte Behörden zu übermitteln (BVerfGE 130, 151 <200 f.> m.w.N.). Insbesondere kann er auch diejenigen Regelungen treffen, die notwendig sind, damit die Übermittlung von Daten an Strafverfolgungs- und Gefahrenabwehrbehörden sowie Nachrichtendienste den grundrechtlichen Anforderungen genügen (vgl. BVerfGE 125, 260 <315>). Demgegenüber endet die Gesetzgebungsbefugnis dort, wo es um den Abruf solcher Informationen geht. Die Ermächtigungen zum Datenabruf selbst bedürfen eines eigenen Kompetenztitels oder müssen den Ländern überlassen bleiben (vgl. BVerfGE 125, 260 <315>; 130, 151 <193>).

b) § 113 TKG hält sich innerhalb der so gezogenen Grenzen. Die Regelung ist 106
darauf beschränkt, die Diensteanbieter zur Übermittlung von Daten zu berechtigen und die Zwecke und Bedingungen für den staatlichen Zugriff auf die Daten zu bestimmen; sie entspricht insofern strukturell ihrer Vorgängervorschrift in deren verfassungskonformer Auslegung (vgl. BVerfGE 130, 151 <200 ff.>). Der staatliche Zugriff auf die Daten sowie die Inpflichtnahme der privaten Diensteanbieter bleiben – auch soweit dem Bund die fachrechtliche Kompetenz für derartige Regelungen zusteht – eigenen Abrufregelungen überlassen. Die Kompetenz des Bundes besteht auch, soweit § 113 Abs. 4 TKG den Diensteanbietern auferlegt, die Daten unverzüglich und vollständig zu übermitteln und über die Auskunftserteilung Stillschweigen zu wahren. Derartige Regelungen knüpfen an anderweitig begründete

Übermittlungspflichten an und präzisieren die Bedingungen, unter denen Daten zur Wahrnehmung öffentlicher Aufgaben zur Verfügung gestellt werden.

2. Der Bund kann auch die angegriffenen Abrufregelungen auf der Grundlage ihm zustehender Gesetzgebungskompetenzen erlassen. 107

a) Der Erlass von Bestimmungen, die den Datenabruf selbst regeln, richtet sich nach den allgemeinen Gesetzgebungskompetenzen. Dieser kann nicht auf Art. 73 Abs. 1 Nr. 7 GG gestützt werden, denn die Inpflichtnahme Privater, die diese zugleich zur Preisgabe der Daten ihrer Kunden zwingt, gehört nicht mehr zur Bestimmung der Grenzen des telekommunikationsbezogenen Datenschutzes, sondern ist untrennbarer Bestandteil des Datenabrufs (vgl. BVerfGE 130, 151 <201>). Abrufregelungen sind daher auf der Grundlage jeweils derjenigen Kompetenznorm zu schaffen, die die Gesetzgebung für die mit der Datenverwendung verfolgten Aufgaben regelt (vgl. BVerfGE 113, 348 <368>; 125, 260 <314, 346>). Die allgemeinen Gesetzgebungskompetenzen umfassen neben der Abrufermächtigung auch die Wahrung der weiteren verfassungsrechtlichen Anforderungen an die Ausgestaltung der Datenverwendung wie insbesondere die Regelungen zur Benachrichtigung der Betroffenen und zur Gewährleistung eines effektiven Rechtsschutzes (vgl. BVerfGE 125, 260 <346 f.>). 108

Im Bereich der Gefahrenabwehr (auch soweit die Verhütung von Straftaten betroffen ist) liegt die Gesetzgebungszuständigkeit weithin bei den Ländern (vgl. BVerfGE 113, 348 <368 f.>; 125, 260 <346>). Jedoch kommen dem Bund auch in diesen Bereichen partiell ausschließliche oder konkurrierende Gesetzgebungszuständigkeiten zu. 109

b) Für die hier angegriffenen Abrufregelungen bestehen Gesetzgebungszuständigkeiten des Bundes. 110

aa) Für den Datenabruf durch das Bundeskriminalamt im Rahmen seiner Aufgaben als Zentralstelle gemäß § 10 Abs. 1 Satz 1 Nr. 1 BKAG ergibt sich die Gesetzgebungskompetenz des Bundes aus Art. 73 Abs. 1 Nr. 10 Buchstabe a GG. Danach hat der Bund die ausschließliche Kompetenz zur Gesetzgebung über die Zusammenarbeit des Bundes und der Länder in der Kriminalpolizei, die internationale Verbrechensbekämpfung sowie die Einrichtung eines Bundeskriminalpolizeiamtes, welche ihn zur Errichtung des Bundeskriminalamts und gemeinsam mit der Verwaltungskompetenz des Art. 87 Abs. 1 Satz 2 GG zur Übertragung der von 111

§ 10 Abs. 1 Satz 1 Nr. 1 BKAG in Bezug genommenen Zentralstellenaufgaben ermächtigt. Dies schließt die Möglichkeit ein, dem Bundeskriminalamt im Rahmen dieser Aufgaben Befugnisse einzuräumen (vgl. BVerfGE 133, 277 <317 f. Rn. 97>; vgl. auch Uhle, in: Maunz/Dürig, GG, Art. 73 Rn. 250 (April 2010); Degenhart, in: Sachs, GG, 8. Aufl. 2018, Art. 73 Rn. 52).

Soweit § 10 Abs. 1 Satz 1 Nr. 2 BKAG die Bestandsdatenauskunft zum Schutz von Mitgliedern der (Bundes-)Verfassungsorgane und der Leitung des Bundeskriminalamts eröffnet, folgt die Gesetzgebungskompetenz des Bundes aus der Natur der Sache (vgl. BTDrucks 7/178, S. 7; 13/1550, S. 20; vgl. auch Graulich, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 6 BKAG Rn. 2; a.A. Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, 2009, S. 28). Die Regelung der dem Zeugenschutz dienenden Bestandsdatenauskunft nach § 10 Abs. 1 Satz 1 Nr. 3 BKAG steht dem Bund als Annex kraft Sachzusammenhangs zu der in Art. 74 Abs. 1 Nr. 1 Var. 4 GG geregelten Kompetenz für das gerichtliche Verfahren auf dem Gebiet des Strafrechts zu (vgl. Schreiber, NJW 1997, S. 2137 <2140>; Griesbaum, NStZ 1998, S. 433 <435>; Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, 2009, S. 27). 112

Die Gesetzgebungskompetenz des Bundes für die durch § 40 BKAG eröffnete Bestandsdatenauskunft ergibt sich aus Art. 73 Abs. 1 Nr. 9a GG. Die Befugnis dient mittels der Verweise über § 39 Abs. 1 und 2 BKAG auf § 5 Abs. 1 BKAG der Abwehr der in dem Kompetenztitel geregelten Gefahren des internationalen Terrorismus. 113

bb) § 22a BPolG eröffnet die Bestandsdatenauskunft über einen Verweis auf § 21 Abs. 1 BPolG für das gesamte Aufgabenspektrum der Bundespolizei. Für die innerhalb dieses Spektrums liegenden Aufgaben stehen dem Bund etwa nach Art. 73 Abs. 1 Nr. 5 GG für den Grenzschutz und nach Art. 73 Abs. 1 Nr. 6a GG für die Bahnpolizei (vgl. BVerfGE 97, 198 <221 f.>) Gesetzgebungskompetenzen zu. 114

cc) §§ 7, 15 ZFdG beruhen auf der in Art. 73 Abs. 1 Nr. 5 GG normierten Gesetzgebungskompetenz des Bundes für den Zoll- und Grenzschutz, die auch präventiv-polizeiliche Maßnahmen umfasst (vgl. BVerfGE 110, 33 <48>; 133, 277 <320 Rn. 102>). 115

dd) Die Zuständigkeit für § 8d BVerfSchG ergibt sich aus Art. 73 Nr. 10 Buchstabe b GG. Danach steht dem Bund die ausschließliche Kompetenz für die Zusammenarbeit des Bundes und der Länder im Bereich des Verfassungsschutzes zu. Diese umfasst zwar nicht die allgemeine Zuständigkeit für den Verfassungsschutz (vgl. BVerfGE 113, 63 <79>). Jedoch ermöglicht der Kompetenztitel dem Bund, auch in gewissem Umfang selbst im Bereich des Verfassungsschutzes tätig zu werden und dem Bundesamt für Verfassungsschutz die für seine Aufgaben erforderlichen Befugnisse einzuräumen (vgl. BVerfGE 30, 1 <20, 29>; 134, 141 <180 Rn. 113>). Hierzu gehören auch die hier in Frage stehenden Befugnisse. 116

ee) Soweit § 2b BNDG den Bundesnachrichtendienst zur Abfrage von Bestandsdaten ermächtigt, um Erkenntnisse über das Ausland von außen- und sicherheitspolitischer Bedeutung zu gewinnen, kann sich der Bund auf seine Kompetenz nach Art. 73 Abs. 1 Nr. 1 GG für auswärtige Angelegenheiten stützen. Der Kompetenztitel berechtigt den Bundesgesetzgeber zwar nicht dazu, Befugnisse einzuräumen, die auf die Verhütung, Verhinderung oder Verfolgung von Straftaten als solche gerichtet sind (vgl. BVerfGE 100, 313 <370>; 133, 277 <319 Rn. 101>). Dem Bundesnachrichtendienst kann aber auf dieser Kompetenzgrundlage über die Aufgabe einer für die politische Handlungsfähigkeit bedeutsamen Unterrichtung der Bundesregierung hinaus als eigene Aufgabe auch die Früherkennung von aus dem Ausland drohenden Gefahren anvertraut werden, wenn diese eine hinreichend internationale Dimension aufweisen, es sich mithin um Gefahren handelt, die sich ihrer Art und ihrem Gewicht nach auf die Stellung der Bundesrepublik Deutschland in der Staatengemeinschaft auswirken können und gerade in diesem Sinne von außen- und sicherheitspolitischer Bedeutung sind (vgl. BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 128). 117

ff) Die kompetenzrechtliche Grundlage für § 4b MADG ergibt sich aus Art. 73 Abs. 1 Nr. 1 GG (Verteidigung) (vgl. BVerfGE 133, 277 <320 Rn. 102>). 118

gg) Soweit die angegriffenen Abrufregelungen auch der Strafverfolgung (vgl. etwa § 10 Abs. 1 Satz 1 Nr. 1, § 2 Abs. 2 Nr. 1 und Abs. 6 BKAG) oder der Strafverfolgungsvorsorge (vgl. etwa § 15 Abs. 2 Satz 1, § 4 Abs. 2 und 3 ZFdG) dienen, verfügt der Bund nach Art. 74 Abs. 1 Nr. 1 Var. 4 GG über die Kompetenz zur Regelung des Strafverfahrens. Die Kompetenzmaterie „gerichtliches Verfahren“ im Sinne des Art. 74 Abs. 1 Nr. 1 Var. 4 GG ist weit zu verstehen. Sie erstreckt sich auf das Strafverfahrensrecht als das Recht der Aufklärung und Aburteilung von Straftaten; hierzu gehören die Ermittlung und Verfolgung von Straftätern ein- 119

schließlich der Fahndung nach ihnen (vgl. BVerfGE 150, 244 <273 Rn. 67>) und damit auch die angegriffenen Regelungen, soweit sie repressive Tätigkeiten der ermächtigten Behörden betreffen. Daneben erfasst Art. 74 Abs. 1 Nr. 1 Var. 4 GG auch die Strafverfolgungsvorsorge (vgl. BVerfGE 103, 21 <30>; 113, 348 <370 f.>; 150, 244 <274 Rn. 68>).

3. Die angegriffenen Regelungen über die Zuordnung dynamischer IP-Adressen genügen dem für Eingriffe in das Fernmeldegeheimnis geltenden Zitiergebot des Art. 19 Abs. 1 Satz 2 GG. Art. 9 des Änderungsgesetzes vom 20. Juni 2013 (BGBl I S. 1602) weist auf die Einschränkung des Art. 10 GG durch Art. 1 bis 8 des Änderungsgesetzes ausdrücklich hin. Der Warn- und Besinnungsfunktion des Zitiergebots (vgl. BVerfGE 64, 72 <79 f.>; 120, 274 <343>) wird damit genügt. Dass das eingeschränkte Grundrecht nur in einem Artikel des Änderungsgesetzes und zudem nicht durchgängig in der jeweils zur Einschränkung ermächtigenden Norm genannt wird, ist verfassungsrechtlich hinnehmbar, wenngleich die konkrete Bezugnahme in der Ermächtigungsnorm der Ratio des Zitiergebotes am besten entsprechen dürfte (vgl. Huber, in: von Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 19 Rn. 96; siehe auch Singer, DÖV 2007, S. 496 <501>; Krebs, in: von Münch/Kunig, GG, Bd. 1, 6. Aufl. 2012, Art. 19 Rn. 14; a.A. Axer, in: Merten/Papier, HGRe, Bd. III, 2009, § 67 Rn. 31), wie dies in den § 8d Abs. 6 BVerfSchG, § 2b Satz 3 BNDG und § 4b Satz 3 MADG klarstellend (vgl. BTDrucks 17/12034, S. 15) erfolgt ist. 120

Einer erneuten Beachtung des Zitiergebots bei der Einführung der §§ 10, 40 BKAG durch das Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes vom 1. Juni 2017 bedurfte es nicht. Die Warn- und Besinnungsfunktion betrifft zwar nicht nur die erstmalige Grundrechtseinschränkung, sondern wird bei jeder erheblichen Veränderung der Eingriffsvoraussetzungen bedeutsam, die zu neuen Grundrechtseinschränkungen führt. Bei Gesetzen, die lediglich bereits geltende Grundrechtseinschränkungen unverändert oder – wie hier – mit geringen Abweichungen wiederholen, findet das Zitiergebot hingegen keine Anwendung (vgl. BVerfGE 129, 208 <237> m.w.N.). 121

III.

Die angegriffenen Übermittlungsbefugnisse in § 113 TKG genügen in materieller Hinsicht nicht den verfassungsrechtlichen Anforderungen des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG sowie des Art. 10 Abs. 1 GG. 122

1. Eingriffe in das Recht auf informationelle Selbstbestimmung und das Telekommunikationsgeheimnis bedürfen wie jede Grundrechtsbeschränkung einer gesetzlichen Ermächtigung, die einen legitimen Gemeinwohlzweck verfolgt und im Übrigen den Grundsatz der Verhältnismäßigkeit wahrt (vgl. BVerfGE 65, 1 <44>; 100, 313 <359 f.>; stRspr). Sie müssen daher zur Erreichung des legitimen Zwecks geeignet, erforderlich und verhältnismäßig im engeren Sinne sein (vgl. BVerfGE 141, 220 <265 Rn. 93>; stRspr). Dabei bedürfen sie einer gesetzlichen Grundlage, welche die Datenverwendung auf spezifische Zwecke hinreichend begrenzt. Alle angegriffenen Befugnisse sind zudem am Grundsatz der Normenklarheit und Bestimmtheit zu messen, der der Vorhersehbarkeit von Eingriffen für die Bürgerinnen und Bürger, einer wirksamen Begrenzung der Befugnisse gegenüber der Verwaltung sowie der Ermöglichung einer effektiven Kontrolle durch die Gerichte dient (BVerfGE 141, 220 <265 Rn. 94>; vgl. auch EuGH, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 91; EGMR (GK), S. and Marper v. The United Kingdom, Urteil vom 4. Dezember 2008, Nr. 30562/04 u.a., § 99). 123

2. Die angegriffenen Übermittlungsregelungen dienen legitimen Zwecken und sind hierfür geeignet und erforderlich. 124

a) Die Regelungen ermöglichen den Sicherheitsbehörden insbesondere, Telekommunikationsanschlüsse und dynamische IP-Adressen individuellen Anschlussinhabern zuzuordnen sowie Zugangsdaten von Endgeräten und Speichereinrichtungen zu erfragen. Die hiermit erstrebte Unterstützung der staatlichen Aufgabenwahrnehmung dient der Effektivierung der Strafverfolgung und der Gefahrenabwehr sowie der Erfüllung der Aufgaben der Nachrichtendienste, mithin legitimen Zwecken, die einen Eingriff sowohl in das Recht auf informationelle Selbstbestimmung als auch in das Telekommunikationsgeheimnis grundsätzlich rechtfertigen können (vgl. BVerfGE 125, 260 <316 f.>; 130, 151 <187, 205>; vgl. auch EuGH, Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 57). 125

b) Die in § 113 TKG gewährten Übermittlungsbefugnisse sind zum Erreichen dieser Zwecke auch geeignet. Sie schaffen Aufklärungsmöglichkeiten, die sonst nicht bestünden, und die angesichts der zunehmenden Bedeutung der Telekommunikation auch für die Vorbereitung und Begehung von Straftaten in vielen Fällen erfolgversprechend sind. Auch wenn das manuelle Auskunftsverfahren nicht sicherstellen kann, dass Bestandsdaten verlässlich mitgeteilt werden können, weil (potentielle) Straftäter und sonstige Zielpersonen etwa öffentliche Hotspots, Internetcafés oder unter Falschpersonalien angemeldete Anschlüsse nutzen oder die ihnen zugewiesene IP-Adresse durch Nutzung spezieller Programme verschleiern, wird die Zweckerreichung jedenfalls gefördert. Die verschiedenen Befugnisse sind hierfür auch erforderlich. Andere Mittel, die vergleichbar effektiv die Informationsmöglichkeiten der Behörden in weniger einschneidender Weise ermöglichten, sind nicht ersichtlich. 126

3. Mit den Anforderungen der Verhältnismäßigkeit im engeren Sinne sind die Übermittlungsregelungen nur vereinbar, wenn sie die Verwendungszwecke der einzelnen Befugnisse gemessen an ihrem Eingriffsgewicht selbst hinreichend normenklar begrenzen (a). Diesen Anforderungen genügen die angegriffenen Befugnisse zur allgemeinen Übermittlung von Bestandsdaten (b), zur Übermittlung von Zugangsdaten (c) und zur Übermittlung von anhand einer dynamischen IP-Adresse bestimmter Bestandsdaten (d) nicht, wenngleich die Regelungen zur Datensicherheit keinen Bedenken begegnen (e). 127

a) Dem Verhältnismäßigkeitsgebot im engeren Sinne genügen die Übermittlungsregelungen, wenn der mit ihnen verfolgte Zweck und die zu erwartende Zweckerreichung nicht außer Verhältnis zu der Schwere des Eingriffs stehen (vgl. BVerfGE 141, 220 <267 Rn. 98>; 148, 40 <57 f. Rn. 49>). Das Eingriffsgewicht bestimmt sich maßgeblich nach Art, Umfang und denkbarer Verwendung der Daten sowie der Gefahr ihres Missbrauchs (aa). Die Verwendungszwecke der Daten sind schon durch den Gesetzgeber der Übermittlungsregelung für sich genommen verhältnismäßig und normenklar zu begrenzen (bb). Im Übrigen muss die verfassungsrechtlich gebotene Datensicherheit bei Übermittlung der Daten gewährleistet sein (cc). 128

aa) Das Eingriffsgewicht wird vor allem durch Art, Umfang und denkbare Verwendung der Daten sowie die Gefahr ihres Missbrauchs bestimmt (vgl. BVerfGE 65, 1 <45 f.>). Dabei ist bedeutsam, welche und wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind und unter welchen Voraussetzun- 129

gen dies geschieht, insbesondere, ob diese Personen hierfür einen Anlass gegeben haben. Maßgebliche Kriterien sind also die Zahl der Betroffenen und die Intensität der Beeinträchtigungen (vgl. BVerfGE 100, 313 <376>), die sich vor allem nach der Aussagekraft und den Verwendungsmöglichkeiten der Daten bestimmt. Auch die Heimlichkeit einer staatlichen Eingriffsmaßnahme führt zur Erhöhung des Eingriffsgewichts (vgl. BVerfGE 115, 320 <353>; 141, 220 <265 Rn. 94>; vgl. auch EuGH, Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u.a., C-203/15 u.a., EU:C:2016:970, Rn. 100).

bb) Verpflichtet der Gesetzgeber zur Schaffung von Datenbeständen oder öffnet er diese über den primären Zweck hinaus, wie hier die Datenbestände privater Unternehmen für eine Verwendung zur staatlichen Aufgabenwahrnehmung, obliegt es ihm zugleich, die für deren verfassungsrechtliche Rechtfertigung erforderlichen Verwendungszwecke und Eingriffsschwellen sowie die für die Gewährleistung der Zweckbindung gegebenenfalls erforderlichen Folgeregelungen verbindlich festzulegen (Gebot der Zweckbindung, vgl. BVerfGE 118, 168 <187>; 120, 378 <408>; 125, 260 <344 f., 355>; vgl. auch EuGH, Urteil vom 8. April 2014, Digital Rights Ireland und Seitlinger u.a., C-293/12 u.a., EU:C:2014:238, Rn. 57 ff.; Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 93). Die grundrechtliche Rechtfertigungslast für eine solche Zweckbestimmung oder -änderung ist dabei schon in der Übermittlungsregelung abzudecken, die zur Schaffung der Datenbestände verpflichtet oder sie zur staatlichen Aufgabenwahrnehmung öffnet. Schon diese – obgleich nur erste Tür – selbst hat die Verwendungszwecke hinreichend zu begrenzen (vgl. BVerfGE 125, 260 <344 f., 355>), muss also die Datenverwendung an bestimmte Zwecke, tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz binden, sodass insgesamt die verfassungsrechtlichen Anforderungen gewahrt werden. Dabei steht es dem Gesetzgeber der Abrufregelung – als zweiter Tür – frei, den Abruf der Daten an (noch) höhere Anforderungen zu binden. Unzulässig ist es dagegen, unabhängig von solchen Zweckbestimmungen einen Datenvorrat zu schaffen, dessen Nutzung je nach Bedarf und politischem Ermessen der späteren Entscheidung verschiedener staatlicher Instanzen überlassen bleibt (vgl. BVerfGE 65, 1 <46>; 100, 313 <360>; 125, 260 <345>; 130, 151 <187>; vgl. auch EuGH, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 93 f.). 130

(1) Dies gilt zunächst für den Fall, dass der Gesetzgeber Datenbestände öffnet, für die er selbst die Speicherung von Daten anordnet. Diese Speicherungsanordnung kann nicht abstrakt gerechtfertigt werden, sondern nur insoweit, als sie 131

hinreichend gewichtigen, konkret benannten Zwecken dient (vgl. BVerfGE 65, 1 <46>; 118, 168 <187 f.>; 125, 260 <327, 345 f.>). Ist der Verwendungszweck nicht festgelegt, fehlt es an der erforderlichen Zweckbindung und es entsteht das Risiko einer Nutzung der Daten für Zwecke, für die sie nicht erhoben wurden (vgl. BVerfGE 120, 378 <408>). Die Bereitstellung eines solchen seiner Zwecksetzung nach offenen Datenvorrats würde den notwendigen Zusammenhang zwischen Speicherung und Speicherungszweck aufheben (vgl. BVerfGE 125, 260 <345, 355 f.>). Auch wäre die Tragweite für die Bürgerinnen und Bürger nicht vorhersehbar. Verwendungsregeln sind insofern unerlässliche Voraussetzung für die Verfassungsmäßigkeit der Speicherungsverpflichtung. Dies schließt nicht aus, dass sie – im Rahmen der Kompetenzordnung – gesondert geregelt werden. Die verhältnismäßige Ausgestaltung dieser Verwendungsregeln entscheidet damit nicht nur darüber, ob diese einen eigenen Eingriff begründenden Regelungen selbst verfassungsgemäß sind, sondern wirkt auf die Verfassungsmäßigkeit schon der Speicherung als solcher zurück (vgl. BVerfGE 125, 260 <327 f.>).

(2) Das Gleiche gilt für die Öffnung privater Datenbestände zur staatlichen Aufgabenwahrnehmung. Der Gesetzgeber ist grundsätzlich nicht gehindert, auch den Zugriff auf Daten zu erlauben, die Diensteanbieter zur Durchführung ihrer Verträge speichern. In einem dynamischen Sektor wie der Telekommunikation können auch andere als die aufgrund staatlicher Anordnung zu speichernden Daten für die staatliche Aufgabenwahrnehmung von Bedeutung sein und deshalb zugänglich gemacht werden (vgl. BVerfGE 130, 151 <206 f.>). Werden aber Datenbestände zu Zwecken geöffnet, die vom Zweck der ursprünglichen Datenerhebung abweichen, kommt dem Gebot der Zweckbindung für die Bestimmung der Anforderungen, die an eine auf solche Daten zugreifende Befugnisnorm zu stellen sind, herausgehobene Bedeutung zu. Sieht der Gesetzgeber eine den ursprünglichen Speicherungszweck ändernde Verwendung von Daten vor, muss er daher den – neuen – Verwendungszweck möglichst präzise festlegen (vgl. BVerfGE 100, 313 <360>; 120, 351 <366 f.>). 132

(3) Ermächtigt eine gesetzliche Regelung zu einem Eingriff in das Recht auf informationelle Selbstbestimmung oder das Telekommunikationsgeheimnis, so hat das Gebot der Bestimmtheit und Klarheit auch die spezifische Funktion, eine hinreichend präzise Umgrenzung des Verwendungszwecks der betroffenen Informationen sicherzustellen (vgl. BVerfGE 118, 168 <187>; 125, 260 <345>). Auf diese Weise wird das verfassungsrechtliche Gebot der Zweckbindung der erhobenen Information verstärkt (vgl. BVerfGE 130, 151 <202> m.w.N.). Anlass, Zweck und 133

Umfang des jeweiligen Eingriffs sind daher durch den Gesetzgeber bereichsspezifisch, präzise und normenklar festzulegen (vgl. BVerfGE 65, 1 <44 ff.>; 100, 313 <359 f.>; 125, 260 <328>; 130, 151 <202>; stRspr). Im Einzelnen unterscheiden sich hierbei die Anforderungen maßgeblich nach dem Gewicht des Eingriffs und sind insoweit mit den jeweiligen materiellen Anforderungen der Verhältnismäßigkeit eng verbunden (BVerfGE 141, 220 <265 Rn. 94> mit Verweis auf BVerfGE 110, 33 <55>).

(4) Die derart qualifizierten Voraussetzungen für eine Verwendung der Daten zum Zwecke der Strafverfolgung, der Gefahrenabwehr oder der Aufgabenerfüllung der Nachrichtendienste sind bereits vom Bund als Gesetzgeber der Übermittlungsregelung festzulegen (vgl. BVerfGE 125, 260 <346>). Deren Konkretisierung darf er nicht späterer Gesetzgebung – insbesondere der Länder – überlassen (vgl. BVerfGE 125, 260 <355 f.>). Er muss seiner Regelungsverantwortung bereits in der Übermittlungsregelung vollständig gerecht werden und diese für sich genommen verhältnismäßig ausgestalten. Das gilt aus Gründen der Normenklarheit nicht nur dann, wenn er Datenbestände in Materien öffnet, in denen die Regelung des Abrufs den Ländern vorbehalten ist, sondern auch dann, wenn ihm selbst die Gesetzgebungskompetenz für die Abrufregelungen zukommt. Dies schließt nicht aus, dass er Übermittlung und Abruf von Daten für die in seinem Kompetenzbereich liegenden Materien auch in einer Norm zusammenfassen kann (vgl. BVerfGE 130, 151 <184, 203>). Eine Begrenzung der Verwendungszwecke erst in der Abrufregelung kommt allerdings nur in Betracht, wenn die Datenöffnung Materien betrifft, die allein im Kompetenzbereich des Bundes liegen, und wenn die getroffenen Übermittlungs- und Abrufregelungen – nach Maßgabe der Anforderungen der Normenklarheit – eine in ihrem Zusammenwirken abschließende Zweckbestimmung der Datenverwendung treffen (vgl. dazu BVerfGE 125, 260 <351 f.>). 134

cc) Verfassungsrechtlich geboten ist schließlich die Gewährleistung der Datensicherheit. Hierzu gehören, soweit es die hier angegriffenen Übermittlungsregelungen betrifft, Regelungen zur Sicherheit der Übermittlung der Daten. 135

b) Diesen Anforderungen genügt die in § 113 Abs. 1 Satz 1 TKG geregelte Befugnis zur allgemeinen Bestandsdatenauskunft nicht. Ihre Reichweite ist mangels begrenzender Eingriffsschwellen unverhältnismäßig. 136

aa) Als Verwendungsregel für die nach §§ 95 und 111 TKG erhobenen Daten berechtigt § 113 Abs. 1 Satz 1 TKG die Diensteanbieter zu deren Übermittlung. 137

Die Regelung ist nunmehr normenklar als bloße Öffnungsklausel ausgestaltet (vgl. BVerfGE 130, 151 <202>), die die Diensteanbieter erst dann zur Datenübermittlung verpflichtet, wenn ein eigens begründetes, auf eine fachrechtliche Abrufregelung gestütztes Verlangen einer in § 113 Abs. 3 TKG genannten Stelle vorliegt. Vorausgesetzt werden insoweit gesetzliche Regelungen, die einen Abruf der konkret nach §§ 95 und 111 TKG erhobenen Daten erlauben (vgl. § 113 Abs. 2 Satz 1 TKG). Der Gesetzgeber hat damit hinreichend klargestellt, dass es zur Datenabfrage einer entsprechend qualifizierten Rechtsgrundlage bedarf (vgl. BTDrucks 17/12034, S. 12), die über eine schlichte Datenerhebungsbefugnis hinausgeht und die dafür in Frage kommenden Behörden in § 113 Abs. 3 TKG auch eindeutig und abschließend bestimmt (vgl. auch BVerfGE 130, 151 <202>).

bb) Die in § 113 Abs. 1 Satz 1 TKG eröffnete allgemeine Bestandsdatenauskunft begründet einen Eingriff in das Recht auf informationelle Selbstbestimmung von gewissem, wenn auch nicht sehr großem Gewicht. 138

(1) Ein nicht unerhebliches Eingriffsgewicht erhält die Regelung allerdings dadurch, dass für die Auskunft auf die nach § 111 TKG annähernd flächendeckend vorrätig gehaltenen Daten zugegriffen und damit praktisch jede Telekommunikationsnummer und jeder Anschlussinhaber ermittelt und beauskunftet werden kann. Gegenstand der Auskunft können auch individualisierende Angaben wie zum Beispiel das Geburtsdatum oder die Anschrift (vgl. BVerfGE 130, 151 <188>) sowie die nach § 95 TKG erhobenen Daten sein, zu denen je nach Vertragsgestaltung zum Beispiel auch die Bankverbindung, der Beruf oder die Namen von Angehörigen oder Partnern eines Anschlussinhabers gehören können (vgl. BVerfGE 130, 151 <206 f.>). Das Eingriffsgewicht wird zudem durch die Heimlichkeit der Auskunftserteilung erhöht. 139

(2) Gleichwohl ist der durch § 113 Abs. 1 Satz 1 TKG begründete Eingriff nicht von sehr großem Gewicht (vgl. auch EuGH, Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 61). Die Auskunft beschränkt sich auf inhaltlich eng begrenzte Daten, die weder höchstpersönliche Informationen erfassen noch die Erstellung von Persönlichkeits- oder Bewegungsprofilen ermöglichen (vgl. BVerfGE 130, 151 <189 f.>; vgl. auch EGMR, Breyer v. Germany, Urteil vom 30. Januar 2020, Nr. 50001/12, § 92 (nicht endgültig)). Auch wenn sich im Rahmen konkreter Erhebungszusammenhänge daraus sensible Informationen ergeben können, bleibt der Informationsgehalt der Auskünfte als solcher doch begrenzt und hängt im Übrigen von weiteren Ermittlungen ab, deren Rechtmäßigkeit nach 140

anderen Vorschriften zu beurteilen ist (BVerfGE 130, 151 <197>). Umstände und Inhalte der Telekommunikation werden nicht mitgeteilt; soweit Anschlussinhaber abgefragt werden, sind die Umstände oder Inhalte den Behörden bereits bekannt. Eingriffsmindernd wirkt zudem, dass jedenfalls die nach § 95 TKG erhobenen Daten nicht verpflichtend gespeichert werden müssen und der Umfang möglicher Auskünfte davon abhängt, ob und inwieweit der jeweilige Diensteanbieter überhaupt einen über § 111 TKG hinausgehenden Datenbestand angelegt hat. Allerdings wird die Preisgabe dieser Daten zur Erlangung wesentlicher Telekommunikationsdienste praktisch regelmäßig unvermeidbar sein.

(a) Das Eingriffsgewicht wird derzeit auch nicht durch die individualisierende Zuordnung einer statischen IP-Adresse erhöht, sofern diese – anders als dynamische IP-Adressen – je nach Auslegung des Begriffs der „Anschlusskennung“ in § 111 Abs. 1 Nr. 1 TKG möglicherweise verpflichtend (ablehnend: Graulich, in: Arndt/Fetzer/Scherer/Graulich, TKG, 2. Aufl. 2015, § 111 Rn. 11; Hey/Pauly/Kartheuser, ZD 2012, S. 455 <456>; Dalby, CR 2013, S. 361 <362 Fn. 14>) oder aber nach § 95 TKG freiwillig gespeichert werden. Zwar ermöglicht die Zuordnung einer IP-Adresse zu einem Anschlussinhaber die Erschließung von nach Umfang und Inhalt wesentlich weitreichenderen Informationen als die Identifizierung einer Telefonnummer, da die Auskunft über den Anschlussinhaber einer IP-Adresse zugleich die Information über den Inhalt des Kontakts enthält, der elektronisch fixiert ist und auch länger wieder abrufbar sein kann (vgl. BVerfGE 125, 260 <342>; 130, 151 <198 f.>). Auch kann gegebenenfalls umgekehrt die statische IP-Adresse eines namentlich bekannten Anschlussinhabers abgefragt werden. Nach Angaben der Bundesregierung werden aber nach derzeitigem Stand der Technik und Praxis privaten Nutzerinnen und Nutzern als Einzelkunden in der Regel keine statischen IP-Adressen zugewiesen. Vielmehr erfolgt die Zuweisung von IP-Adressen auch während der laufenden Einführung des Internetprotokolls Version 6, das über einen im Vergleich zur Vorgängerversion deutlich größeren Adressraum verfügt und deshalb die Zuweisung fester IP-Adressen an alle Nutzerinnen und Nutzer grundsätzlich zuließe, weiterhin ganz überwiegend dynamisch. Die Zuweisung von statischen IP-Adressen, deren Zuordnung zurzeit ohnehin über außereuropäische Plattformen öffentlich zugänglich ist, beschränkt sich nach wie vor im Wesentlichen auf Institutionen und Großnutzer (vgl. dazu BVerfGE 130, 151 <198>). 141

(b) Das Eingriffsgewicht wird dagegen dadurch begrenzt, dass Auskünfte nur dann erteilt werden dürfen, wenn eine in § 113 Abs. 3 TKG genannte Stelle dies in 142

Textform im Einzelfall zu ihrer Aufgabenwahrnehmung verlangt (vgl. § 113 Abs. 2 Satz 1 TKG). Die Übermittlungsregelung ermächtigt damit ausdrücklich nur zu einer aufgabenbezogenen Auskunft im Einzelfall. Entgegen der Ansicht der Beschwerdeführenden bleibt der Einzelfallbezug auch erhalten, wenn geschäftsmäßige Diensteanbieter mit mehr als 100.000 Kunden gemäß § 113 Abs. 5 Satz 2 TKG für die Entgegennahme eines Auskunftsersuchens sowie für die Erteilung der zugehörigen Auskünfte eine gesicherte elektronische Schnittstelle bereithalten. In § 113 Abs. 5 TKG wird allein das erforderliche technische Umfeld für die Entgegennahme des Auskunftsverlangens und die Erteilung der Auskunft geregelt. Die inhaltlichen und formalen Voraussetzungen für eine Auskunftserteilung werden durch die Verpflichtung, eine gesicherte elektronische Schnittstelle bereitzuhalten, nicht modifiziert. Auch bei Nutzung der Schnittstelle muss das Auskunftsverlangen gegenüber den Diensteanbietern vielmehr einzelfallbezogen geäußert werden. Dies verdeutlicht § 113 Abs. 5 Satz 3 TKG, wonach auch bei Entgegennahme eines Auskunftsverlangens über eine elektronische Schnittstelle dafür Sorge zu tragen ist, dass jedes Verlangen durch eine verantwortliche Fachkraft auf Einhaltung der in § 113 Abs. 2 TKG genannten formalen Voraussetzungen geprüft und die weitere Bearbeitung des Verlangens erst nach einem positiven Prüfergebnis freigegeben wird. Damit soll sichergestellt werden, dass gerade keine automatisierte Datenabfrage stattfindet, sondern jede Anfrage auch providerseitig geprüft wird; eine automatisierte Prüfung ist dementsprechend nicht zulässig (vgl. BTDrucks 17/12034, S. 12). Die Ermöglichung oder Erleichterung von Massenabfragen ist in der Norm auch nicht angelegt. Die Einrichtung einer gesicherten elektronischen Schnittstelle dient vielmehr vorrangig dazu, die Datensicherheit zu erhöhen (vgl. BTDrucks 17/12034, S. 12).

(c) Das manuelle Auskunftsverfahren bringt für die abfragende Behörde zudem einen gewissen Verfahrensaufwand mit sich, der dazu beitragen dürfte, dass die Behörde die Auskunft nur bei hinreichendem Bedarf einholt oder den benötigten Auskünften eine gewisse Bedeutung zukommt (vgl. zur Vorgängerregelung BVerfGE 130, 151 <206>). Dieser wird – wie ausgeführt – auch bei Nutzung einer elektronischen Schnittstellte nicht verringert. 143

cc) Trotz ihres gemäßigten Eingriffsgewichts erweist sich die Übermittlungsbefugnis aufgrund ihrer Reichweite, die durch keine Eingriffsschwellen begrenzt ist, als unverhältnismäßig. 144

(1) Auch unter Berücksichtigung des nicht sehr großen Eingriffsgewichts der in § 113 Abs. 1 Satz 1 TKG geregelten Übermittlungsbefugnis und ihrer Bedeutung für die staatliche Aufgabenwahrnehmung im Bereich der Gefahrenabwehr, der Strafverfolgung und der Nachrichtendienste bedarf es begrenzender, spezifischer Eingriffsschwellen. Auch Auskünfte über Daten, deren Aussagekraft und Verwendungsmöglichkeiten eng begrenzt sind, dürfen nicht ins Blaue hinein zugelassen werden (vgl. BVerfGE 130, 151 <205>). Dafür genügt es nicht, dass die Auskünfte – wie hier – nur einzelfallbezogen und zweckgebunden erteilt werden dürfen. Vielmehr bedarf es begrenzender Eingriffsschwellen, die sicherstellen, dass Auskünfte nur bei einem auf tatsächliche Anhaltspunkte gestützten Eingriffsanlass eingeholt werden können. Unzulässig ist die Schaffung eines offenen Datenvorrats für vielfältige und ohne äußeren Eingriffsanlass begrenzte Verwendungen im gesamten einer Behörde zugewiesenen Aufgabenbereich (vgl. dazu BVerfGE 125, 260 <355 f.>). 145

(a) Erforderlich ist demnach bezogen auf die Gefahrenabwehr grundsätzlich eine im Einzelfall vorliegende konkrete Gefahr im Sinne der polizeirechtlichen Generalklauseln. Diese Schwelle umfasst auch den Gefahrenverdacht. Ebenso beschränkt sie Auskünfte nicht von vornherein auf Polizeipflichtige im Sinne des allgemeinen Polizei- und Ordnungsrechts. Sie ist damit jedoch nicht so entgrenzt, dass sie angesichts des gemäßigten Eingriffsgewichts unverhältnismäßig wäre. Insbesondere werden damit Auskünfte nicht als allgemeines Mittel der Verwaltung ermöglicht, sondern setzen im Einzelfall einen sicherheitsrechtlich geprägten Charakter der betreffenden Aufgabe voraus (vgl. BVerfGE 130, 151 <206>). Bezogen auf die Strafverfolgung genügt das Vorliegen eines Anfangsverdachts (vgl. BVerfGE 130, 151 <206>). Das grundsätzliche Erfordernis einer auf Anhaltspunkte im Tatsächlichen gestützten konkreten Gefahr gilt für die Nachrichtendienste ebenso wie für alle zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung zuständigen Behörden (vgl. BVerfGE 125, 260 <343 f.>). Sind derart qualifizierte Eingriffsschwellen vorgesehen, bedarf es im Hinblick auf das gemäßigte Eingriffsgewicht der allgemeinen Bestandsdatenauskunft und ihrer großen Bedeutung für eine effektive Aufgabenwahrnehmung keines spezifisch erhöhten Rechtsgüterschutzes, um die Verhältnismäßigkeit der Datenübermittlung sicherzustellen. 146

(b) Der Gesetzgeber ist von Verfassungs wegen aber nicht von vornherein für jede Art der Aufgabenwahrnehmung auf die Schaffung von Eingriffstatbeständen beschränkt, die dem tradierten sicherheitsrechtlichen Modell der Abwehr konkre- 147

ter, unmittelbar bevorstehender oder gegenwärtiger Gefahren entsprechen. Vielmehr kann er die Grenzen unter besonderen Voraussetzungen auch weiter ziehen, indem er die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert (vgl. BVerfGE 141, 220 <272 Rn. 112>). Allerdings muss stets gewährleistet bleiben, dass Annahmen und Schlussfolgerungen einen konkret umrissenen Ausgangspunkt im Tatsächlichen haben (BVerfGE 113, 348 <386>). Je gewichtiger das gefährdete Rechtsgut ist und je weiterreichend es durch die jeweiligen Handlungen beeinträchtigt würde, desto geringere Anforderungen dürfen an den Grad der Wahrscheinlichkeit gestellt werden, mit der auf eine drohende Verletzung geschlossen werden kann, und desto weniger fundiert dürfen gegebenenfalls die Tatsachen sein, die auf die Gefährdung des Rechtsguts schließen lassen (vgl. BVerfGE 100, 313 <392>; siehe auch BVerfGE 110, 33 <55, 60>). Umgekehrt steigen bei einem geringen Gewicht des gefährdeten Rechtsguts die Anforderungen an die Prognosesicherheit sowohl hinsichtlich des Grads der Gefährdung als auch hinsichtlich ihrer Intensität (vgl. BVerfGE 113, 348 <386>).

Eingriffsgrundlagen müssen daher regelmäßig zumindest eine hinreichend konkretisierte Gefahr verlangen. Eine solche kann schon dann bestehen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr hinweisen. Die Tatsachen müssen dafür zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann (BVerfGE 141, 220 <272 Rn. 112> mit Verweis auf BVerfGE 120, 274 <328 f.> und 125, 260 <330 f.>). Eine solche Absenkung der Eingriffsschwellen ist aus Gründen der Verhältnismäßigkeit aber untrennbar verbunden mit erhöhten Anforderungen an die konkret geschützten Rechtsgüter (vgl. BVerfGE 141, 220 <272 Rn. 112>). 148

Zum Schutz herausgehobener Rechtsgüter, wie etwa zur Verhütung terroristischer Straftaten, können die Anforderungen an die Vorhersehbarkeit des Geschehensablaufs in dieser Weise auch dann weiter abgesenkt und Eingriffe erlaubt werden, wenn zwar noch kein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch zumindest das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird (vgl. BVerfGE 141, 220 <272 f. Rn. 112, 149

291 Rn. 164>). Zu berücksichtigen ist stets auch das Eingriffsgewicht der konkreten Maßnahme. Während der Absenkung von Eingriffsschwellen bei tief in die Privatsphäre eingreifenden Maßnahmen deutliche Grenzen gesetzt sind, bestehen bei weniger gewichtigen Eingriffen auch weiterreichende Gestaltungsmöglichkeiten (vgl. BVerfGE 141, 220 <269 Rn. 104>).

Weniger gewichtige Eingriffe – wie sie die allgemeine Bestandsdatenauskunft begründet – können daher beim Vorliegen einer konkretisierten Gefahr bereits dann zu rechtfertigen sein, wenn sie dem Schutz von Rechtsgütern von zumindest erheblichem Gewicht dienen (vgl. dazu BVerfGE 150, 244 <284 Rn. 99>; 150, 309 <336 Rn. 73>), wie dies etwa bei der Verhütung von Straftaten von zumindest erheblicher Bedeutung (vgl. dazu BVerfGE 141, 220 <270 Rn. 107> m.w.N.) der Fall ist. Hochrangige, überragend wichtige oder auch besonders gewichtige Rechtsgüter (vgl. BVerfGE 115, 320 <346>; 120, 274 <328>; 141, 220 <270 Rn. 108>) sind demgegenüber nur dann erforderlich, wenn die Eingriffsschwelle noch weiter hinter einer konkretisierten Gefahr zurückbleiben sollte oder es sich etwa um tief in die Privatsphäre eingreifende Befugnisse handelte. 150

(c) Diese verfassungsrechtlichen Anforderungen gelten grundsätzlich für alle Eingriffsermächtigungen mit präventiver Zielrichtung. Sie gelten damit auch für die Verwendung der Daten durch Nachrichtendienste (vgl. BVerfGE 125, 260 <331>). Auch für ihre Tätigkeiten genügen damit Eingriffsgrundlagen, die eine hinreichend konkretisierte Gefahr (oben Rn. 148 f.) verlangen, den verfassungsrechtlichen Anforderungen. Zwar sind auch insoweit stets tatsächliche Anhaltspunkte erforderlich (vgl. BVerfGE 120, 274 <330>). Bei – wie vorliegend – nicht tief in die Privatsphäre eingreifenden und insgesamt weniger gewichtigen Eingriffen kann es jedoch genügen, dass eine Auskunft zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten ist (vgl. dazu BVerfGE 130, 151 <206>), denn damit wird ein wenigstens der Art nach konkretisiertes und absehbares Geschehen vorausgesetzt. Im Hinblick darauf, dass der Aufgabenbereich der Nachrichtendienste von vornherein dadurch gekennzeichnet ist, dass er dem Schutz besonders gewichtiger Rechtsgüter dient (vgl. BVerfGE 141, 220 <339 Rn. 320>; vgl. auch BVerfGE 133, 277 <326 Rn. 118>), bedarf es keiner weitergehenden Anforderungen an den Rechtsgüterschutz. 151

(d) Demgegenüber kann im Bereich der Strafverfolgung eine in tatsächlicher Hinsicht unterhalb des Anfangsverdachts liegende Eingriffsschwelle zur Vornahme 152

von grundrechtsrelevanten Eingriffen nicht genügen. Zwar können für Maßnahmen mit präventiver Zielsetzung die Grenzen für bestimmte Bereiche auch weiter gezogen werden, indem die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert werden (oben Rn. 147). Voraussetzung ist aber stets eine tatsachenbezogene Grundlage. Auch die im Gefahrenabwehrrecht anerkannten Eingriffsschwellen der „konkretisierten Gefahr“ und der „drohenden Gefahr“, die in zeitlicher Hinsicht ins Vorfeld verlagert sind, setzen tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr voraus (vgl. BVerfGE 141, 220 <272 Rn. 112>). Nichts Anderes gilt für Maßnahmen der Strafverfolgung. Auch im Vorfeldbereich kommen sie nur bei Vorliegen tatsächlicher Anhaltspunkte in Betracht (vgl. BVerfGE 113, 348 <386>; 117, 244 <263>). Vage Anhaltspunkte oder Vermutungen reichen demgegenüber nicht aus (vgl. BVerfGE 115, 166 <197 f.>; 124, 43 <66 f.>).

Danach reicht eine in tatsächlicher Hinsicht unterhalb des Anfangsverdachts angesiedelte Eingriffsschwelle im Bereich der Strafverfolgung nicht aus. Die Annahme eines Anfangsverdachts setzt lediglich das Vorliegen zureichender tatsächlicher Anhaltspunkte für eine Straftat voraus (vgl. BGH, Beschluss vom 12. Januar 2005 - 5 StR 191/04 -, Rn. 7). Solche tatsächlichen Anhaltspunkte liegen hinsichtlich ihrer Aussagekraft noch unter den für manche Ermittlungsmaßnahmen geforderten „bestimmten Tatsachen“, weshalb der Anfangsverdacht bereits die Verdachtsstufe mit den geringsten in der Strafprozessordnung vorgesehenen tatsächlichen Voraussetzungen ist (vgl. BVerfGE 109, 279 <350>; 129, 208 <268>). Würden die Voraussetzungen noch weiter zurückgenommen, wären nur noch vage Anhaltspunkte gefordert. 153

(2) Diesen verfassungsrechtlichen Anforderungen genügt § 113 Abs. 1 Satz 1 TKG nicht. Die Übermittlungsregelung öffnet das manuelle Auskunftsverfahren sehr weit, indem sie Auskünfte allgemein zum Zweck der Gefahrenabwehr, zur Verfolgung von Straftaten oder Ordnungswidrigkeiten sowie zur Erfüllung nachrichtendienstlicher Aufgaben erlaubt (§ 113 Abs. 2 Satz 1 TKG) und dabei keine ihre Reichweite näher begrenzenden Eingriffsschwellen (vgl. BVerfGE 130, 151 <205>) enthält. Die Regelung ermöglicht die Erteilung einer Auskunft im Einzelfall vielmehr bereits dann, wenn dies zur Wahrnehmung der Aufgaben erfolgt. 154

(a) Trotz des für sich gesehen begrenzten Informationsgehalts der betreffenden Daten, ihrer engen Verwendungsmöglichkeiten sowie ihrer großen Bedeutung für eine effektive Aufgabenwahrnehmung der abfrageberechtigten Behörden sind 155

die Verwendungszwecke nicht hinreichend begrenzt. Zwar handelt es sich bei den gesetzlich bestimmten Verwendungszwecken um zentrale Aufgaben der Gewährleistung von Sicherheit. In Anbetracht der zunehmenden Bedeutung der elektronischen Kommunikationsmittel und des heutigen Kommunikationsverhaltens der Menschen in allen Lebensbereichen sind die Behörden darauf angewiesen, insbesondere auch Telekommunikationsnummern individuell zuordnen zu können. Doch auch unter Berücksichtigung ihres nur gemäßigten Eingriffsgewichts ist die hier angegriffene Regelung zu weit gefasst, da Auskünfte bereits dann erteilt werden können, wenn sie in irgendeinem Zusammenhang zu der staatlichen Aufgabenwahrnehmung stehen und einen Einzelfallbezug erkennen lassen, ohne dass ein auf tatsächliche Anhaltspunkte gestützter Eingriffsanlass vorausgesetzt wird. Eröffnet sind damit vielfältige und in jeder Hinsicht unbegrenzte Verwendungen.

(b) Die erforderlichen Eingriffsschwellen können § 113 TKG auch nicht – wie noch der Vorgängerregelung – im Wege der Auslegung entnommen werden. 156

Zwar enthielt der im Wesentlichen gleichlautende § 113 TKG a.F. ebenfalls keine begrenzenden Eingriffsschwellen. Diese konnten jedoch durch das Bundesverfassungsgericht im Wege der Auslegung ermittelt werden. Dabei stützte es sich maßgeblich auf die begrenzende Wirkung der tatbestandlichen Voraussetzungen, nach denen Auskünfte nur im Einzelfall angefordert werden durften und zur Aufgabenwahrnehmung erforderlich sein mussten. Davon ausgehend legte das Bundesverfassungsgericht die Regelung bezogen auf die Gefahrenabwehr dahin aus, dass eine Auskunft eine „konkrete Gefahr“ voraussetze und dass im Aufgabenbereich der Nachrichtendienste die Auskunft zumindest zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten sein müsse. Auch soweit sich Auskünfte auf die Verfolgung von Straftaten und Ordnungswidrigkeiten bezogen, leitete es aus dem Erfordernis der Erforderlichkeit im Einzelfall ab, dass zumindest ein Anfangsverdacht vorliegen müsse (vgl. BVerfGE 130, 151 <205 f.>). 157

Die hier angegriffene Übermittlungsregelung kann nicht erneut in diesem Sinne verständig ausgelegt werden. Dem stehen sowohl ihr Wortlaut als auch der klar erkennbare gesetzgeberische Wille entgegen. Anders als die Vorgängerregelung setzt § 113 Abs. 2 Satz 1 TKG, der die näheren Voraussetzungen der durch § 113 Abs. 1 Satz 1 TKG erlaubten Übermittlung regelt, schon nicht voraus, dass die zu erteilenden Auskünfte zur Aufgabenwahrnehmung der abfrageberechtigten Stellen „erforderlich“ sein müssen. Genau darauf aber hat das Bundesverfassungsgericht 158

in seiner Entscheidung zur Vorgängerregelung neben der Einzelfallbezogenheit maßgeblich abgestellt. Gerade aus dem Erfordernis der Erforderlichkeit im Einzelfall hat es abgeleitet, dass dem § 113 TKG a.F. – wenngleich niedrige – Eingriffsschwellen zu entnehmen waren. Wenn der Gesetzgeber vor diesem Hintergrund nunmehr wiederum nur die Verwendungszwecke als solche regelt, keine begrenzenden Eingriffsschwellen bestimmt und dabei gleichzeitig auf das Merkmal der Erforderlichkeit der Auskunftserteilung für die Aufgabenwahrnehmung verzichtet, kann das Bundesverfassungsgericht darüber im Rahmen einer neuerlichen Auslegung nicht hinweggehen. Dies entspräche auch nicht dem gesetzgeberischen Willen. So sah der von der Bundesregierung eingebrachte Gesetzentwurf zunächst gar keine aufgabenbezogene Begrenzung der Auskunftserteilung vor (vgl. BTDrucks 17/12034, S. 5), da – so die Gegenerklärung auf Einwände des Bundesrats (vgl. BRDrucks 664/12 [Beschluss], S. 1 f.; BTDrucks 17/12034, S. 17) – aus der neuen, seitens des Bundesverfassungsgerichts vorgegebenen dualen Gesetzessystematik folge, dass die erforderliche aufgabenbezogene Begrenzung der Auskunftserteilung nicht mehr in § 113 TKG geregelt werden könne. Sie betreffe nicht die Übermittlungsbefugnis der Diensteanbieter, sondern die Erhebungsbefugnis der Behörden. Die Voraussetzungen der Auskunftserteilung seien deshalb – wie der Entwurf ausgehend von einem Missverständnis der verfassungsgerichtlichen Rechtsprechung (vgl. BVerfGE 125, 260 <344 f., 355>; 130, 151 <184 f.; 202 f., 207 ff.>) ausführt – ausschließlich im jeweiligen Fachrecht zu verankern (vgl. BTDrucks 17/12034, S. 20). Der Gesetzgeber ist dem zwar letztlich nicht vollständig gefolgt und hat zumindest eine Beschränkung der Auskunft auf den Einzelfall eingefügt und die Verwendungszwecke der Auskunftserteilung bestimmt, womit er die materiellen Grenzen der jeweils bereichsspezifisch zu schaffenden Befugnisregelungen klarstellen wollte (vgl. BTDrucks 17/12879, S. 10). Weitergehende Begrenzungen wollte er aber ersichtlich nicht setzen. Dies lassen auch die gleichzeitig geschaffenen fachrechtlichen Abrufregelungen erkennen, die weitgehend keine begrenzenden Eingriffsschwellen enthalten und insbesondere nicht das Vorliegen einer konkreten Gefahr voraussetzen (dazu im Folgenden Rn. 206 ff.).

c) § 113 Abs. 1 Satz 2 TKG, der zur Übermittlung von Zugangsdaten berechtigt, ist mit Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG unvereinbar. 159

aa) § 113 Abs. 1 Satz 2 TKG erlaubt die Erteilung einer Auskunft von Daten, die als Zugangsdaten den Zugriff auf Endgeräte oder externe Speichereinrichtungen sichern. Die Vorschrift berechtigt zur Auskunftserteilung über diese Daten un- 160

abhängig von den Voraussetzungen für ihre Nutzung und entspricht inhaltlich insoweit – trotz geänderten Wortlauts – § 113 Abs. 1 Satz 2 TKG in der Fassung des Telekommunikationsgesetzes vom 22. Juni 2004, den das Bundesverfassungsgericht mit Beschluss vom 24. Januar 2012 für unvereinbar mit Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG erklärt hat (vgl. BVerfGE 130, 151 <152>). Zur Begründung führte es aus, die Regelung sei unverhältnismäßig, weil Behörden ohne ersichtlichen Grund Zugangsdaten auch unabhängig von den Anforderungen an deren Nutzung und damit gegebenenfalls unter leichteren Voraussetzungen abfragen könnten. Die Erhebung der Zugangsdaten sei mit Blick auf die verfolgten Zwecke nur dann erforderlich, wenn auch die Voraussetzungen für deren Nutzung gegeben seien (vgl. BVerfGE 130, 151 <209>).

Die Erklärung der Verfassungswidrigkeit einer Norm hindert den Gesetzgeber zwar nicht daran, eine inhaltlich gleichlautende Bestimmung wiederum zu erlassen (vgl. BVerfGE 77, 84 <103 f.>). Dabei kann er aber die vom Bundesverfassungsgericht festgestellten Gründe der Verfassungswidrigkeit des ursprünglichen Gesetzes nicht übergehen. Eine Normwiederholung verlangt vielmehr ihrerseits besondere Gründe, die sich vor allem aus einer wesentlichen Änderung der für die verfassungsrechtliche Beurteilung maßgeblichen tatsächlichen oder rechtlichen Verhältnisse oder der ihr zugrundeliegenden Anschauungen ergeben können. Fehlen solche Gründe, ist das Bundesverfassungsgericht nicht gehalten, die bereits entschiedenen verfassungsrechtlichen Fragen erneut zu erörtern (BVerfGE 96, 260 <263>). 161

bb) Solche Gründe sind hier nicht ersichtlich. Dass die Neuregelung in § 113 Abs. 1 Satz 2 TKG die aus Gründen der Verhältnismäßigkeit erforderliche Beschränkung nicht enthält, beruht darauf, dass der Gesetzgeber davon ausgegangen ist, es genüge, diese in den neu geschaffenen Abrufregelungen des bundesrechtlichen Fachrechts vorzusehen, um den Vorgaben des Bundesverfassungsgerichts zu entsprechen (vgl. BTDrucks 17/12034, S. 13, 20). Dem liegt indes ein unzutreffendes Verständnis der grundrechtlichen Regelungsverantwortung des Bundes für die Öffnung der Datenbestände zugrunde. Schon die Datenöffnung für die staatliche Aufgabenwahrnehmung hat den Anforderungen an eine normenklare Begrenzung der späteren Datenverwendung Rechnung zu tragen (vgl. BVerfGE 125, 260 <344 f., 355>; oben Rn. 130). Insofern hat das Bundesverfassungsgericht die Vorgängerregelung – ungeachtet von Bund und Ländern zu schaffender Abrufregelungen – wegen der nicht hinreichenden Verwendungsbegrenzung für verfassungswidrig erklärt (vgl. BVerfGE 130, 151 <207 ff.>). Defizite der ersten 162

Tür können nicht durch eine – wie hier erfolgte – „Verstärkung“ der zweiten Tür kompensiert werden (vgl. Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, Abschnitt G Rn. 177).

d) Die in § 113 Abs. 1 Satz 3 TKG neu geschaffene Befugnis, auch anhand einer dynamischen IP-Adresse bestimmte Bestandsdaten zu übermitteln, genügt nicht den Anforderungen der Verhältnismäßigkeit und verstößt damit gegen Art. 10 Abs. 1 GG. 163

aa) § 113 Abs. 1 Satz 3 TKG regelt mit der erforderlichen Normenklarheit, dass auch über solche Bestandsdaten Auskunft erteilt werden darf, die anhand einer dynamischen IP-Adresse bestimmt werden. Die Regelung stellt ebenfalls klar, dass zur Vorbereitung solcher Auskünfte Verkehrsdaten ausgewertet werden dürfen. Der Gesetzgeber trifft damit zugleich eine eigene Verwendungsregel für die nach § 96 TKG zu betrieblichen Zwecken erhobenen Verkehrsdaten (vgl. BTDrucks 17/12034, S. 12), die er zweckgebunden für die Vorbereitung der Auskunft nach § 113 Abs. 1 Satz 3 TKG und damit für die staatliche Aufgabenwahrnehmung öffnet (oben Rn. 132). Obgleich zum Zeitpunkt der Neuregelung des § 113 Abs. 1 Satz 3 TKG im Jahr 2013 Verkehrsdaten von den Diensteanbietern lediglich auf Grundlage des § 96 TKG erhoben wurden, werden durch die nicht weiter eingeschränkte, allgemein formulierte Berechtigung, Verkehrsdaten auszuwerten, jedenfalls vom Wortlaut der Norm tatsächlich auch die seit dem 1. Juli 2017 gemäß §§ 113a, 113b TKG von Erbringern öffentlich zugänglicher Telekommunikationsdienste verpflichtend zu speichernden Verkehrsdaten (siehe allerdings zur derzeitigen Handhabung der Speicherungspflicht oben Rn. 12) erfasst. Da die Verwendung dieser Daten zur Erteilung einer Auskunft nach § 113 Abs. 1 Satz 3 TKG durch § 113c Abs. 1 Nr. 3 TKG aber ausdrücklich angeordnet wird, bestehen im Zusammenwirken beider Normen im Hinblick auf die gebotene Normenklarheit des § 113 Abs. 1 Satz 3 TKG keine Bedenken. 164

bb) § 113 Abs. 1 Satz 3 TKG hat ein gegenüber der allgemeinen Bestandsdatenauskunft erhöhtes Eingriffsgewicht. Er begründet einen Eingriff in Art. 10 Abs. 1 GG und hat im Hinblick auf die Aussagekraft und Verwendungsmöglichkeiten sowohl der zu beauskunftenden Bestandsdaten als auch der zu deren Bestimmung von den Diensteanbietern auszuwertenden Verkehrsdaten eine erheblich größere Persönlichkeitsrelevanz. 165

(1) Die Begründung behördlicher Auskunftsansprüche zur Identifizierung dynamischer IP-Adressen hat aufgrund der Aussagekraft und der Verwendungsmöglichkeiten der zu beauskunftenden Bestandsdaten ein erhebliches Gewicht. Der Gesetzgeber wirkt damit auf die Kommunikationsbedingungen im Internet ein und begrenzt den Umfang ihrer Anonymität. Auf Grundlage der Zuordnung dynamischer IP-Adressen kann in Verbindung mit der anlasslosen und systematischen Speicherung von Internetzugangsdaten nach § 113b Abs. 3 TKG in weitem Umfang die Identität derjenigen ermittelt werden, die das Internet nutzen (vgl. BVerfGE 125, 260 <341 f.>). Diese gesetzliche Konzeption wird durch die gegenwärtig ausgesetzte Durchsetzung der Verpflichtung zur Speicherung dieser Daten (vgl. dazu oben Rn. 12) dem Grunde nach nicht berührt. 166

Zwar hat die Zuordnung einer dynamischen IP-Adresse eine gewisse Ähnlichkeit mit der Identifizierung einer Telefonnummer. Die Abfrage des Inhabers einer Telefonnummer erbringt jedoch nicht ohne weiteres auch Informationen zu konkreten Telekommunikationsakten. Demgegenüber enthält eine Auskunft über den Anschlussinhaber einer dynamischen IP-Adresse in sich notwendig zugleich die Information, dass und von welchem Anschluss aus diese IP-Adresse zu einer bestimmten Zeit genutzt wurde. Da der Inhalt von Internetseiten elektronisch fixiert und länger wieder abrufbar ist, gibt die Individualisierung der IP-Adresse zugleich Auskunft über den Inhalt des Kontakts. Schon vom Umfang, vor allem aber vom Inhalt der Kontakte her, über die sie Auskunft geben kann, hat sie damit eine erheblich größere Persönlichkeitsrelevanz als die Identifizierung einer Telefonnummer und kann mit ihr nicht gleichgesetzt werden (vgl. BVerfGE 130, 151 <204> mit Verweis auf BVerfGE 125, 260 <341 ff.>). 167

(2) Das Eingriffsgewicht erhöhend wirkt sich weiter aus, dass die Diensteanbieter zur Bestimmung der zu beauskunftenden Daten auch Verkehrsdaten auswerten, denen von vornherein eine höhere Persönlichkeitsrelevanz zukommt als reinen Bestandsdaten. Zwar handelt es sich bei Verkehrsdaten nur um Verbindungsdaten, ohne dass dabei auch der Inhalt der Kommunikation erfasst würde. Aus Verkehrsdaten lassen sich aber bei umfassender Erhebung und Auswertung grundsätzlich aussagekräftige Persönlichkeits- und Bewegungsprofile erstellen (vgl. BVerfGE 125, 260 <319>). 168

Das Gewicht des Eingriffs wird hier jedoch dadurch abgemildert, dass die um Auskunft ersuchenden Behörden bei der Zuordnung dynamischer IP-Adressen keine Kenntnis der Verkehrsdaten erhalten. Die Behörden rufen diese nicht selbst 169

ab, sondern erhalten lediglich personenbezogene Auskünfte über den Inhaber eines bestimmten Anschlusses, der von den Diensteanbietern unter Rückgriff auf die Verkehrsdaten sowie gegebenenfalls weitere Daten (etwa der Source Port Number, vgl. Rn. 42) ermittelt wurde. Die Aussagekraft des beauskunfteten Bestandsdatums bleibt eng begrenzt. Die Verwendung der Verkehrsdaten führt allein zu der Auskunft, welcher Anschlussinhaber unter einer den Sicherheitsbehörden bereits bekannten IP-Adresse zu einem bestimmten Zeitpunkt im Internet angemeldet war (vgl. BVerfGE 125, 260 <341>). Ihr Erkenntniswert bleibt punktuell. Systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen lassen sich allein auf Grundlage solcher Auskünfte gerade nicht verwirklichen (vgl. BVerfGE 125, 260 <341>).

(a) Dies gilt zunächst für die nach § 96 TKG erhobenen Verkehrsdaten. Hierbei handelt es sich um solche Verkehrsdaten, die die Diensteanbieter nach Maßgabe ihrer betrieblichen Erfordernisse in begrenztem Umfang und für den Einzelnen durch Vertragsgestaltung teilweise vermeidbar gemäß § 96 TKG speichern dürfen (vgl. BVerfGE 125, 260 <352>). Verkehrsdaten, zu denen auch die IP-Adresse selbst gehört, werden danach weder vollständig noch systematisch gespeichert. Die Praxis der Speicherung ist je nach Diensteanbieter, Vertragsgestaltung und in Anspruch genommener Dienstleistung vielmehr sehr unterschiedlich. Ohne konkreten Anlass ist eine Speicherung zur Erkennung, Eingrenzung oder Beseitigung von Störungen oder Fehlern (§ 96 Abs. 1 Satz 2, § 100 Abs. 1 TKG) nach der fachgerichtlichen Rechtsprechung jedenfalls bis zu sieben Tage nach Ende der Internetverbindung zulässig (vgl. BGH, Urteil vom 13. Januar 2011 - III ZR 146/10 -, Rn. 22; Urteil vom 3. Juli 2014 - III ZR 391/13 -, Rn. 23; vgl. auch Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten, Stand 19. Dezember 2012, S. 4 f.), wovon die Diensteanbieter in unterschiedlichem Umfang, teilweise aber auch gar nicht Gebrauch machen. Durch vertragliche Gestaltung teilweise abdingbar und durch die Nutzerinnen und Nutzer beeinflussbar ist zudem, wie oft eine Internetverbindung unterbrochen wird, und damit das für den Beginn der Speicherfrist relevante Ende der Verbindung. 170

(b) Für die Zuordnung einer dynamischen IP-Adresse können allerdings nicht nur die nach § 96 TKG erhobenen Verkehrsdaten ausgewertet werden, sondern grundsätzlich auch die von öffentlich zugänglichen Telekommunikationsdiensten für zehn Wochen (§ 113b Abs. 1 Nr. 1 TKG) anlasslos und systematisch gespeicherten Verkehrsdaten (vgl. BVerfGE 125, 260 <328, 352>; siehe aber zur derzeitigen Handhabung der Speicherungspflicht oben Rn. 12). Damit geht grundsätzlich 171

eine deutliche Erhöhung des Eingriffsgewichts einher. Neben dem Umstand, dass diese Daten selbst nicht Gegenstand der Auskunft sind, ist freilich zu berücksichtigen, dass für die Zuordnung einer IP-Adresse nur ein von vornherein feststehender kleiner Ausschnitt der Daten verwendet wird, deren Speicherung für sich genommen unter deutlich geringeren Voraussetzungen angeordnet werden könnte. Eine Speicherung allein der für solche Auskünfte erforderlichen Internetzugangsdaten zur Identifizierung dynamischer IP-Adressen hätte ein deutlich geringeres Gewicht als die nahezu vollständige Speicherung der Daten sämtlicher Telekommunikationsverbindungen (vgl. BVerfGE 125, 260 <341>). Die ansonsten für die Verwendung vorsorglich gespeicherter Verkehrsdaten maßgeblichen, besonders strengen Anforderungen gelten daher für solche Auskünfte nicht gleichermaßen (vgl. BVerfGE 125, 260 <340>).

(c) Soweit gemäß § 113 Abs. 1 Satz 4 TKG für die Auskunftserteilung anhand dynamischer IP-Adressen darüber hinaus sämtliche unternehmensinternen Datenquellen zu berücksichtigen sind, kommt dem keine weitere eingriffserhöhende Wirkung zu. Die Regelung bringt zum Ausdruck, dass es die Diensteanbieter nicht in der Hand haben, die für die Identifizierung von IP-Adressen erforderlichen Daten frei auszuwählen oder zu verknappen (vgl. Graulich, in: Arndt/Fetzer/Scherer/Graulich, TKG, 2. Aufl. 2015, § 113 Rn. 29; Löwnau/Ipsen, in: Scheurle/Mayen, TKG, 3. Aufl. 2018, § 113 Rn. 11). Es handelt sich insoweit lediglich um eine technikoffene Formulierung, die – entgegen der Auffassung der Beschwerdeführenden – jedenfalls nicht die Verwendung rechtswidrig gespeicherter Daten zur Zuordnung dynamischer IP-Adressen eröffnen kann. 172

(d) § 113 Abs. 1 Satz 3 TKG eröffnet schließlich auch keine spezifischen Missbrauchsgefahren. Insbesondere ermöglicht er keine über den dort ausdrücklich geregelten Zweck hinausgehende Verwendung von Verkehrsdaten. Der Gesetzgeber hat mit § 113 Abs. 1 Satz 3 TKG hinreichend klargestellt, dass nur Auskünfte zu einzelnen, den Behörden bereits bekannten IP-Adressen unter Verwendung von Verkehrsdaten erlaubt sind (vgl. auch BTDrucks 17/12034, S. 10, 12). Eine Ermächtigung zu offenen Anfragen der Behörden zu Anschlussinhabern, deren Telekommunikationsverbindungen nicht bekannt sind, enthält die Regelung – auch in Verbindung mit § 113 Abs. 1 Satz 4 TKG – nicht (vgl. dazu BVerfGE 125, 260 <357>). Die Übermittlung der einem Anschlussinhaber zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse, dessen weitere Daten (wie etwa der Name und die Adresse) der abfragenden Stelle bekannt sind, ist daher nicht zulässig (vgl. Graulich, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 173

2. Aufl. 2019, § 10 BKAG Rn. 20). Die Formulierung von § 113 Abs. 1 Satz 3 und 4 TKG bringt klar zum Ausdruck, dass Verkehrsdaten und alle sonstigen unternehmensinternen Datenquellen überhaupt nur für die Zuordnung einer IP-Adresse verwendet werden dürfen. Eine weitergehende Befugnis ergibt sich entgegen der Auffassung der Beschwerdeführenden auch nicht aus der in Art. 9 des Änderungsgesetzes (BGBl I 2013 S. 1602) enthaltenen allgemein gefassten Formulierung, dass durch die hier angegriffenen Neuregelungen das Fernmeldegeheimnis eingeschränkt sei. Eine gesetzliche Bestimmung zur Wahrung des Zitiergebots kann keine Befugnis zu Eingriffen in das Fernmeldegeheimnis begründen.

cc) Unter Berücksichtigung seines gleichwohl erhöhten Eingriffsgewichts erfüllt § 113 Abs. 1 Satz 3 TKG die sich aus dem Verhältnismäßigkeitsgebot ergebenden Anforderungen an eine hinreichende Begrenzung der Verwendungszwecke für die zu beauskunftenden Daten nicht. 174

(1) Soweit für die Zuordnung von IP-Adressen nicht nur auf die nach § 96 TKG erhobenen, sondern auch auf vorsorglich gespeicherte Verkehrsdaten zurückgegriffen werden darf, müssen verfassungsrechtlich zwar nicht die für die unmittelbare Verwendung der Gesamtheit der vorsorglich gespeicherten Verkehrsdaten geltenden besonders strengen Voraussetzungen gegeben sein (vgl. BVerfGE 125, 260 <340>). Dem erhöhten Eingriffsgewicht muss gleichwohl durch hinreichend begrenzte Verwendungszwecke Rechnung getragen werden. Erforderlich sind grundsätzlich die Reichweite des § 113 Abs. 1 Satz 3 TKG näher begrenzende Eingriffsschwellen sowie eine Beschränkung auf den Schutz oder die Bewehrung von Rechtsgütern von hervorgehobenem Gewicht. 175

(a) Die Zuordnung dynamischer IP-Adressen bedarf – wie die allgemeine Bestandsdatenauskunft – begrenzender Eingriffsschwellen, die sicherstellen, dass Auskünfte nicht ins Blaue hinein eingeholt werden können. Erforderlich sind daher grundsätzlich qualifizierte Eingriffsschwellen, die einen Anfangsverdacht oder eine konkrete Gefahr auf einzelfallbezogener Tatsachenbasis voraussetzen. Letzteres gilt für die Nachrichtendienste ebenso wie für alle zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung zuständigen Behörden (vgl. BVerfGE 125, 260 <343 f.>). 176

(b) Zu den Anforderungen des Übermaßverbots gehört es zudem, dass die in § 113 Abs. 1 Satz 3 TKG eröffnete Bestandsdatenauskunft durch einen im Verhältnis zum Grundrechtseingriff hinreichend gewichtigen Rechtsgüterschutz ge- 177

rechtfertigt sein muss. Zwar bedarf es hier grundsätzlich keiner begrenzenden Rechtsgüter- oder Straftatenkataloge. Das maßgeblich aufgrund Art, Umfang und Verwendungsmöglichkeiten der verarbeiteten Daten erhöhte Eingriffsgewicht der Zuordnung von IP-Adressen erlaubt es indessen nicht, diese allgemein und uneingeschränkt auch zur Abwehr jeglicher Gefahren sowie zur Verfolgung oder Verhinderung jedweder Ordnungswidrigkeiten zuzulassen. Auch unter Berücksichtigung des gesteigerten Interesses an der Möglichkeit, Kommunikationsverbindungen im Internet zum Rechtsgüterschutz oder zur Wahrung der Rechtsordnung dem jeweiligen Akteur zuordnen zu können und der angesichts der zunehmenden Bedeutung des Internets für die verschiedenartigen Bereiche des täglichen Lebens erhöhten Gefahr seiner Nutzung für Straftaten und Rechtverletzungen vielfältiger Art, bedarf die Aufhebung der Anonymität des Internets zumindest einer Rechtsgutbeeinträchtigung, der von der Rechtsordnung auch sonst ein hervorgehobenes Gewicht beigemessen wird. Dies schließt Auskünfte zur Verfolgung oder Verhinderung von Ordnungswidrigkeiten nicht vollständig aus. Es muss sich insoweit aber um – auch im Einzelfall – besonders gewichtige Ordnungswidrigkeiten handeln, die der Gesetzgeber zudem ausdrücklich benennen muss (vgl. BVerfGE 125, 260 <344>). Im Bereich der Gefahrenabwehr kann dementsprechend nicht jede Gefahr für ein Schutzgut als Eingriffsschwelle genügen (vgl. BVerfGE 150, 244 <286 Rn. 106>). Andernfalls könnte aufgrund des die Unverletzlichkeit der gesamten Rechtsordnung erfassenden Schutzumfangs des Gefahrenabwehrrechts jeglicher Verstoß gegen Rechtsvorschriften zum Anlass einer Zuordnung von IP-Adressen werden.

Dem Eingriffsgewicht der individualisierten Zuordnung dynamischer IP-Adressen entspricht es daher, dass sie zu ihrer Rechtfertigung jeweils auf Gründe gestützt werden muss, die dem Schutz oder der Bewehrung von Rechtsgütern von hervorgehobenem Gewicht (vgl. BVerfGE 125, 260 <344>) dienen. Eines darüber hinausgehenden erheblichen Gewichts bedarf es im Hinblick auf die ausschließlich anlassbezogene und punktuelle Zuordnung des Internetkontakts nicht. Zu den Rechtsgütern von hervorgehobenem Gewicht zählen jedenfalls die durch das Strafrecht geschützten Rechtsgüter. Der Gesetzgeber kann die Bestandsdatenauskunft aber auch zur Verfolgung oder Verhinderung anderer hinreichend gewichtiger Delikte zulassen, für deren Bekämpfung eine Zuordnung von IP-Adressen von Bedeutung ist, was besonders gewichtige Ordnungswidrigkeiten einschließen kann (vgl. dazu BVerfGE 125, 260 <344>; 150, 244 <284 Rn. 99>). 178

(c) Die gesetzliche Bestimmung der Eingriffsschwelle und des Schutzguts stehen allerdings in einem Wechselverhältnis, sodass auch die Befugnis zur Zuordnung von IP-Adressen nicht stets das Vorliegen einer konkreten Gefahr im tradierten Sinne erfordert. Die Eingriffsbefugnis kann daher auch mit abgesenkten Eingriffsschwellen den Anforderungen der Verhältnismäßigkeit genügen. Ausreichend ist dabei grundsätzlich das Vorliegen einer konkretisierten Gefahr (oben Rn. 148 f.). Je nach Gewicht des zu schützenden Rechtsguts kann es genügen, wenn entweder ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist oder alternativ das individuelle Verhalten von Betroffenen die konkrete Wahrscheinlichkeit begründet, dass sie bestimmte Straftaten in überschaubarer Zukunft begehen werden (vgl. BVerfGE 141, 220 <272 f. Rn. 112, 291 Rn. 164 f., 305 Rn. 213>). Dies gilt sowohl für die allgemeine Gefahrenabwehr als auch innerhalb des Aufgabenbereichs der Nachrichtendienste. 179

Soll eine solche konkretisierte Gefahr die Eingriffsbefugnis begründen, bedarf es im Hinblick auf das erhöhte Eingriffsgewicht der Zuordnung von IP-Adressen, das maßgeblich durch die Art, den Umfang und die Verwendungsmöglichkeiten der zu beauskunftenden Bestandsdaten und der dabei verwendeten Verkehrsdaten bestimmt wird, einer Begrenzung der Auskunft auf den Schutz von zumindest besonders gewichtigen Rechtsgütern (vgl. dazu BVerfGE 141, 220 <270 Rn. 108> m.w.N.). In der Übermittlungsregelung muss der Gesetzgeber entweder die Rechtsgüter von besonderem Gewicht selbst konkret benennen oder zumindest das erforderliche Gewicht normenklar festhalten. 180

Soweit die Gefahrenabwehr auf die Verhütung von Straftaten bezogen ist, muss es sich um zumindest schwere Straftaten handeln (vgl. auch BVerfGE 125, 260 <328 f.>). Welche Straftatbestände hiervon umfasst sein sollen, hat der Gesetzgeber abschließend mit der Öffnung der Datenbestände festzulegen. 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 (vgl. BVerfGE 109, 279 <343 ff., insbesondere 347 f.>). Eine Generalklausel oder die lediglich pauschale Verweisung auf nicht näher eingegrenzte Straftaten reichen hingegen nicht aus (vgl. auch BVerfGE 125, 260 <329>). 181

Für den Bereich der Nachrichtendienste muss demgegenüber eine derartige Begrenzung der Rechtsgüter nicht ausdrücklich angeordnet werden, da deren Tä- 182

tigkeit von vornherein dem Schutz besonders gewichtiger Rechtsgüter in diesem Sinne dient (vgl. BVerfGE 141, 220 <339 Rn. 320>; vgl. auch BVerfGE 133, 277 <326 Rn. 118>); schon die Voraussetzung einer hinreichend konkretisierten Gefahr als Eingriffsschwelle sichert hier, dass auch im Einzelfall hinreichend gewichtige Rechtsgüter in Frage stehen.

(2) Diesen Anforderungen genügt § 113 Abs. 1 Satz 3 TKG nicht. Die Zuordnung dynamischer IP-Adressen ist an keine begrenzenden Eingriffsschwellen gebunden und daher unverhältnismäßig. 183

(a) § 113 Abs. 2 Satz 1 TKG, der die Voraussetzungen der Übermittlung näher regelt und die Verwendungszwecke auch für die Zuordnung dynamischer IP-Adressen bestimmt, setzt weder einen Anfangsverdacht noch eine auf tatsächliche Anhaltspunkte gestützte konkrete Gefahr voraus. 184

Bezogen auf die allgemeine Gefahrenabwehr fehlt zudem die – auch unter Zugrundelegung solchermaßen qualifizierter Eingriffsschwellen – erforderliche Begrenzung der Befugnis auf einen hinreichend gewichtigen Rechtsgüterschutz. Soweit die Zuordnung einer IP-Adresse zur Abwehr einer Gefahr für die öffentliche Sicherheit und Ordnung (§ 113 Abs. 2 Satz 1 TKG) eröffnet ist, wird die Unverletzlichkeit der Rechtsordnung insgesamt in Bezug genommen, ohne hinsichtlich der in Frage stehenden Rechtsgüter zu gewichten (vgl. BVerfGE 150, 244 <286 Rn. 106>). Es fehlt eine Beschränkung auf die Abwehr von Gefahren für Rechtsgüter von hervorgehobenem Gewicht. 185

Das Gleiche gilt bezogen auf die Strafverfolgung, soweit § 113 Abs. 2 Satz 1 TKG die Auskunftserteilung zum Zweck der Verfolgung jeglicher Ordnungswidrigkeiten erlaubt. Es fehlt die erforderliche Beschränkung auf besonders gewichtige Ordnungswidrigkeiten. Diese kann auch durch § 46 Abs. 3 Satz 1 OWiG nicht mit der erforderlichen Normenklarheit getroffen werden. Die Regelung untersagt zwar generell – und damit sogar weitergehend – die Verfolgung von Ordnungswidrigkeiten in Bußgeldverfahren, wenn entsprechende Maßnahmen das Telekommunikationsgeheimnis betreffen würden, und dürfte damit auf tatsächlicher Ebene die Gefahr einer Zuordnung von IP-Adressen zur Verfolgung von Ordnungswidrigkeiten ausschließen. Auch können Verwendungsregeln durchaus in verschiedenen Regelungen – insgesamt verfassungskonform – abschließend bestimmt werden (vgl. BVerfGE 125, 260 <351 f.>), wenn, wie hier, die Übermittlung und der Abruf Materien betreffen, für die allein dem Bund die Gesetzgebung zusteht (oben 186

Rn. 110 ff.). Dies setzt aber voraus, dass die Normen in ihrem Zusammenwirken den Verwendungszweck der Daten hinreichend präzise und normenklar umgrenzen, sodass gewährleistet ist, dass der Datentransfer insgesamt den grundrechtlichen Anforderungen genügt. § 46 Abs. 3 Satz 1 OWiG und die hier angegriffene Übermittlungsregelung treffen aber – ohne auch nur aufeinander Bezug zu nehmen – für die Verwendung der Daten einander unauflösbar widersprechende Regelungen.

(b) Die Befugnis zur Zuordnung von IP-Adressen wird in § 113 Abs. 2 Satz 1 TKG auch nicht durch abgesenkte Eingriffsschwellen begrenzt. Insbesondere eine konkretisierte Gefahr wird weder für die allgemeine Gefahrenabwehr noch für die Tätigkeiten der Nachrichtendienste vorausgesetzt. § 113 Abs. 2 Satz 1 TKG erfordert, soweit die Auskunft nach § 113 Abs. 1 Satz 3 TKG betroffen ist, weder ein wenigstens der Art nach konkretisiertes und absehbares Geschehen noch alternativ, dass das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründen muss, dass sie in überschaubarer Zukunft eine Straftat begeht. In Bezug auf die allgemeine Gefahrenabwehr fehlen zudem die für eine solche Absenkung der Eingriffsschwellen erforderliche Begrenzung auf den Schutz zumindest besonders gewichtiger Rechtsgüter und – soweit die Straftatenverhütung betroffen ist – eine Beschränkung auf die Verhütung zumindest schwerer Straftaten. 187

e) Demgegenüber bestehen gegen die hier angegriffenen Übermittlungsregelungen keine Bedenken im Hinblick auf die verfassungsrechtlich gebotene Datensicherheit. Untrennbarer Bestandteil der Anordnung einer Speicherungsverpflichtung von Daten wie auch der Öffnung privater Datenbestände ist neben einer den Anforderungen genügenden normenklaren Begrenzung der Datenverwendung auch die verfassungsrechtlich gebotene Gewährleistung der Datensicherheit (vgl. für die Speicherungsverpflichtung BVerfGE 125, 260 <344>). Hierzu gehören neben den Regelungen zur Sicherheit der gespeicherten Daten auch die Regelungen zur Sicherheit der Datenübermittlung (vgl. BVerfGE 125, 260 <345>). Die erforderlichen Vorkehrungen betreffen damit zum einen die – für sich genommen – nicht angegriffene Speicherung der Daten nach §§ 95, 96, 111 und 113a, 113b TKG; die Datensicherheit regeln insoweit etwa §§ 109 f. und 113d TKG. Zum anderen ist die Sicherheit der Übermittlung der abgerufenen Daten zu gewährleisten. Insoweit sieht § 113 Abs. 5 Satz 2 TKG für Anbieter mit mehr als 100.000 Kunden die Einrichtung einer gesicherten elektronischen Schnittstelle vor. Die Regelung wird durch Teil B der Technischen Richtlinie zur Umsetzung gesetzlicher Maß- 188

nahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften (TR TKÜV) konkretisiert. Dass diese Pflicht für kleinere Diensteanbieter nicht gilt, führt nicht zu einer Unterschreitung des verfassungsrechtlich gebotenen Mindestmaßes der Sicherheit der Datenübermittlung. Insoweit ist jedenfalls die allgemeine Regelung des § 109 Abs. 1 TKG einschlägig, die sämtlichen Diensteanbietern auferlegt, nach dem Stand der Technik Vorkehrungen zum Datenschutz zu treffen.

IV.

Die mit § 113 TKG korrespondierenden Abrufregelungen genügen in materieller Hinsicht weitgehend nicht den verfassungsrechtlichen Anforderungen des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG und des Art. 10 Abs. 1 GG. 189

1. Da Übermittlung und Abruf personenbezogener Daten je eigenständige Grundrechtseingriffe begründen, müssen auch die einzelnen Abrufregelungen in Abhängigkeit von dem jeweils betroffenen Grundrecht und ihrem Eingriffsgewicht den Anforderungen der Verhältnismäßigkeit sowie der Normenklarheit und Bestimmtheit genügen. Die relevanten verfassungsrechtlichen Anforderungen ergeben sich vor allem aus dem Grundsatz der Verhältnismäßigkeit im engeren Sinne, der voraussetzt, dass die Abrufregelungen auf einer jeweils eigenen hinreichend bestimmten gesetzlichen Grundlage beruhen, die die Datenverwendung auf spezifische Zwecke hinreichend begrenzt. 190

2. Die angegriffenen Abrufregelungen dienen – wie schon § 113 TKG (oben Rn. 124 ff.) – legitimen Zwecken und sind hierfür geeignet und erforderlich. 191

Insbesondere bedarf es hinsichtlich der Abfrage von Zugangsdaten nicht der von den Beschwerdeführenden für erforderlich gehaltenen Subsidiaritätsklausel, wonach eine Abfrage von Zugangsdaten nur dann erfolgen darf, wenn die damit bezweckte Datenerhebung nicht auf andere Weise, insbesondere durch die unmittelbare Inanspruchnahme der Diensteanbieter auf Auskunft über die Inhaltsdaten erreicht werden kann. In Bezug auf die durch Zugangsdaten geschützten Inhalte, die auf Endgeräten und von dort aus zugänglichen externen Speichermedien gespeichert sind, ist eine unmittelbare Inanspruchnahme der Diensteanbieter schon nicht gleich geeignet, um das angestrebte Ziel zu erreichen. Die Diensteanbieter sind regelmäßig nicht im Besitz der Endgeräte und haben daher selbst dann, wenn sie etwa PIN und PUK einer SIM-Karte kennen und das Endgerät nicht zusätzlich durch einen persönlichen Zugangssicherungscode gesichert ist, keinen 192

Zugang zu den dort gespeicherten oder mittelbar zugänglichen Daten wie Fotos, Kontakten oder auch E-Mail-Postfächern anderer Diensteanbieter.

Demgegenüber kann zwar der mit einer Abfrage von Zugangsdaten erstrebte Zugriff auf die Inhalte externer Speichereinrichtungen, soweit diese wie etwa Voice-Mailboxen oder gegebenenfalls E-Mail-Postfächer (vgl. aber zu webbasierten E-Mail-Diensten EuGH, Urteil vom 13. Juni 2019, Gmail, C-193/18, EU:C:2019:498) dem Anwendungsbereich des Telekommunikationsgesetzes unterfallen, auch durch eine unmittelbare Inanspruchnahme der Diensteanbieter auf Herausgabe (Durchsuchung, Sicherstellung und Beschlagnahme) oder auf Überwachung der laufenden Kommunikation (Telekommunikationsüberwachung, Onlinedurchsuchung) erreicht werden (vgl. BVerfGE 124, 43 <55>). Diese Maßnahmen sind aus Gründen der Verhältnismäßigkeit regelmäßig auch auf bestimmte Zeiträume (etwa in § 100a, § 100e Abs. 1 Satz 4 und 5 StPO, § 100b, § 100e Abs. 2 Satz 4 und 5 StPO) oder auf bestimmte zeitlich oder sonst abgrenzbare Inhalte zu begrenzen (zur Beschlagnahme von Datenbeständen BVerfGE 113, 29 <55 f.>; 124, 43 <68>) und gewähren insoweit begrenztere Informationen als der durch Übermittlung des Zugangscodes verschaffte Zugang zu einer Speichereinrichtung (vgl. auch BTDrucks 19/17741, S. 38). Dies lässt freilich unberührt, dass auch die Anwendung der Abrufbefugnis für Zugangsdaten im Einzelfall dem Grundsatz der Erforderlichkeit zu folgen hat, der sicherstellt, dass Zugangsdaten nicht unabhängig von den Anforderungen an ihre Nutzung und damit gegebenenfalls unter leichteren Voraussetzungen abgefragt werden (vgl. insoweit BVerfGE 130, 151 <208 f.>). Auch die Nutzung von Zugangsdaten kann daher dahin beschränkt sein, dass sie nur für bestimmte Zeiträume oder anderweitig abgrenzbare Inhalte zulässig ist. Begründet wird insoweit ein begrenztes Erhebungsverbot. 193

3. Mit dem Verhältnismäßigkeitsgrundsatz im engeren Sinne sind die Abrufregelungen nur vereinbar, wenn die einzelnen Befugnisse zum Datenabruf hinreichend begrenzt und die notwendigen übergreifenden Anforderungen an Transparenz, Rechtsschutz und Kontrolle beachtet werden (a). Diesen Anforderungen genügen die angegriffenen Befugnisse zum allgemeinen Abruf von Bestandsdaten (b) im Gegensatz zu den Befugnissen zum Abruf von Zugangsdaten (c) weitgehend nicht. Ebenfalls in weitem Umfang nicht hinreichend eingegrenzt sind die Befugnisse zum Abruf von anhand einer dynamischen IP-Adresse bestimmter Bestandsdaten (d), welche zudem sämtlich nicht den verfassungsrechtlichen Anforderungen an die verfahrensrechtlichen Sicherungen genügen (e). 194

a) Den Anforderungen der Verhältnismäßigkeit im engeren Sinne genügen die angegriffenen Abrufregelungen, wenn der mit ihnen verfolgte Zweck seinerseits nicht außer Verhältnis zu der Schwere des Eingriffs steht. Die angegriffenen Regelungen müssen hinreichend bestimmt und normenklar eine qualifizierte Ermächtigungsgrundlage für den Datenabruf schaffen (aa). Sie müssen unter Berücksichtigung ihres Eingriffsgewichts und den jeweils verfolgten Zwecken hinreichende Verwendungsregeln enthalten und insoweit für sich genommen verhältnismäßig ausgestaltet sein (bb). Die Befugnisse zum Datenabruf sind darüber hinaus – aus Gründen der Normenklarheit – auch an die in den Übermittlungsregelungen begrenzten Verwendungszwecke gebunden (cc). Im Übrigen folgen aus dem Verhältnismäßigkeitsgrundsatz für alle Abrufregelungen gewisse übergreifende Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle sowie an Regelungen zur Datennutzung und -löschung (dd). 195

aa) Mit Rücksicht auf das Gebot der Normenklarheit, dem bei Eingriffen in das Recht auf informationelle Selbstbestimmung und das Telekommunikationsgeheimnis eine spezifische Funktion zukommt, bedarf es für den Datenabruf in Form eines unmittelbar an private Dritte gerichteten Auskunftsverlangens einer eindeutigen Rechtsgrundlage, die eine Auskunftsverpflichtung der Diensteanbieter eigenständig begründet. Erforderlich sind hinreichend qualifizierte Abrufregelungen, die über schlichte Datenerhebungsbefugnisse hinausgehen, und klar bestimmen, gegenüber welchen Behörden die Anbieter konkret zur Datenübermittlung verpflichtet sein sollen (vgl. BVerfGE 130, 151 <202 f.>). 196

bb) Entsprechend den für die Öffnung der Datenbestände entwickelten Maßstäben, müssen Abrufregelungen ihrerseits die Verwendungszwecke der Daten hinreichend begrenzen. Dabei sind Anlass, Zweck und Umfang des jeweiligen Eingriffs auch für den Datenabruf bereichsspezifisch, präzise und normenklar festzulegen (vgl. BVerfGE 130, 151 <202>). Erforderlich sind auch für den Abruf Eingriffsschwellen, die sicherstellen, dass Auskünfte nur bei einem auf tatsächliche Anhaltspunkte gestützten Eingriffsanlass eingeholt werden können. Unzulässig ist der Abruf für vielfältige und unbegrenzte Verwendungen im gesamten einer Behörde zugewiesenen Aufgabenbereich (vgl. BVerfGE 125, 260 <355 f.>). Unter Berücksichtigung des Gewichts des Eingriffs können die Eingriffsschwellen auch abgesenkt werden (oben Rn. 147 ff.), soweit ein entsprechend gewichtiger Rechtsgüterschutz gewährleistet ist. 197

cc) Die Befugnisse zum Datenabruf müssen nicht nur für sich genommen verhältnismäßig sein, sondern sind – aus Gründen der Normenklarheit – auch an die in den Übermittlungsregelungen begrenzten Verwendungszwecke gebunden. Dies gilt auch, soweit diese verfassungsrechtlich nicht geboten sind. 198

(1) In Materien, in denen die Länder die Abrufregelungen zu treffen haben, beruht dies bereits darauf, dass ihnen die Gesetzgebungskompetenz für die Öffnung der Datenbestände und die damit verbundene notwendige Begrenzung ihrer weiteren Verwendung fehlt. Die Länder können diese Datenbestände nicht aufgrund eigener Entscheidung weiter öffnen. 199

(2) Ungeachtet dessen können landes- wie bundesgesetzliche Abrufregelungen nur dann dem Gebot der Normenklarheit genügen, wenn sie den Rahmen der durch die Übermittlungsregelung begrenzten Verwendungszwecke einhalten. Nur dann können Übermittlungs- und Abrufregelung eine in ihrem Zusammenwirken hinreichend präzise Umgrenzung des Verwendungszwecks des Datenaustauschs sicherstellen. 200

Nach dem Bild einer Doppeltür müssen die – jeweils zuständigen – Gesetzgeber nicht nur die Tür zur Übermittlung der Daten öffnen, sondern auch die Tür zu deren Abfrage (vgl. BVerfGE 130, 151 <184>). Insoweit muss schon der Gesetzgeber der Übermittlungsregelung in eigener Regelungsverantwortung eine klare und abschließende Entscheidung treffen, zu welchen Zwecken und mit welchen Begrenzungen er die erste Tür öffnet (vgl. BVerfGE 125, 260 <355>). Diese erste Tür kann auch der Gesetzgeber der zweiten Tür nicht weiter öffnen. Er ist vielmehr insoweit an die in der Übermittlungsregelung getroffenen Verwendungsregeln gebunden (vgl. auch Brodowski, Verdeckte technische Überwachungsmaßnahmen im Polizei- und Strafverfahrensrecht, 2016, S. 137). Dabei steht es dem Gesetzgeber der Abrufregelungen zwar frei, den Datenabruf durch die berechtigten Behörden an noch engere Zwecke, höhere Eingriffsschwellen oder an den Schutz oder die Bewehrung noch gewichtigerer Rechtsgüter zu binden (vgl. Bäcker, Kriminalpräventionsrecht, 2015, S. 505). Aus Gründen der Normenklarheit darf er aber selbst dann, wenn er – wie vorliegend – zugleich Gesetzgeber der Abrufregelungen ist, nicht die in der Übermittlungsregelung begrenzten Verwendungszwecke unterlaufen und die Behörden zum Abruf zu anderen, weitergehenden Zwecken ermächtigen, niedrigere Eingriffsschwellen oder einen weniger gewichtigen Rechtsgüterschutz vorsehen. Abrufregelungen mit solchermaßen abgesenkten Verwendungsregeln könnten zwar die Behörden – im Rahmen des verfassungs- 201

rechtlich Zulässigen – zum Datenabruf ermächtigen; die Diensteanbieter wären jedoch zur Auskunft weder berechtigt noch verpflichtet (vgl. § 113 Abs. 2 Satz 1 TKG). Derartige Abrufregelungen enthielten von daher einen mit der Übermittlungsregelung von vornherein unvereinbaren Normbefehl. Die Verwendungszwecke der auszutauschenden Daten müssen aber gerade durch das Zusammenwirken der Übermittlungs- und Abrufregelung normenklar begrenzt sein. Es darf nicht der Anschein erweckt werden, dass eine Behörde losgelöst von den in der Übermittlungsregelung getroffenen Verwendungsregeln auf Daten zugreifen dürfte. Dadurch würden Zugriffsmöglichkeiten eröffnet, die missbräuchlich und unvorhersehbar genutzt werden könnten.

Ein Widerspruch zwischen Übermittlungsregelung und einer weniger begrenzten Abrufregelung könnte auch nicht dahin aufgelöst werden, dass ein Datenaustausch nur unter den engeren Voraussetzungen der Übermittlungsregelung erfolgen dürfte. Die Einhaltung dieser engeren Voraussetzungen können und dürfen die Diensteanbieter in materieller Hinsicht nicht überprüfen. Sie liegt vielmehr allein in der Verantwortung der abfrageberechtigten Stellen (vgl. § 113 Abs. 2 Satz 4 TKG) und kann auch nur dort zuverlässig beurteilt werden. Sie würden aber durch die fachrechtlichen Abrufregelungen zu einem weitergehenden Datenabruf ermächtigt, ohne dass eine behördeninterne Kontrolle am Maßstab der Übermittlungsregelung gewährleistet wäre. Auch insoweit würden Zugriffsmöglichkeiten eröffnet, die rechtsstaatlich nicht mehr eingehegt und vorhersehbar wären (dazu Dieterle, ZD 2016, S. 517 <521>). 202

dd) Aus dem Verhältnismäßigkeitsgrundsatz folgen darüber hinaus gewisse übergreifende Anforderungen an Transparenz, Rechtsschutz und aufsichtliche Kontrolle, die sich nach den jeweiligen Sachkompetenzen richten und in den Abrufregelungen sichergestellt werden müssen (vgl. BVerfGE 125, 260 <344 ff.>; 150, 244 <285 Rn. 101>; stRspr) und welche sich im Einzelnen nach dem Eingriffsgewicht der Regelungen bemessen. Verfassungsrechtlich geboten sind auch tragfähige Regelungen zur Nutzung der Daten sowie zur Datenlöschung (vgl. BVerfGE 65, 1 <46>; 150, 244 <285 Rn. 101>). 203

b) Die fachrechtlichen Regelungen, die allgemein zum Abruf von Bestandsdaten ermächtigen, genügen diesen verfassungsrechtlichen Anforderungen weitgehend nicht. Den übergreifenden verfahrensrechtlichen Anforderungen wird demgegenüber insoweit Genüge getan (vgl. unten e, Rn. 244 ff.). 204

aa) Die Abrufregelungen schaffen allerdings jeweils hinreichend bestimmt und normenklar spezifische Ermächtigungsgrundlagen für die durch § 113 TKG zur Übermittlung geöffneten Daten. Neben der Ermächtigung der abfrageberechtigten Behörden nehmen die Regelungen private Dritte in die Pflicht und schaffen damit spezifische Rechtsgrundlagen, die eigenständig eine Auskunftsverpflichtung der Diensteanbieter begründen. Alle Regelungen bezeichnen die jeweils abfrageberechtigte Behörde und nehmen ausdrücklich auf die „nach §§ 95 und 111 TKG erhobenen Daten“ sowie auf § 113 TKG Bezug. 205

bb) Die angegriffenen Regelungen sind jedoch mit Blick auf ihr Eingriffsgewicht, das sich maßgeblich nach Art, Umfang und Verwendungsmöglichkeiten der betroffenen Daten bestimmt, überwiegend nicht verhältnismäßig ausgestaltet. Fast alle Regelungen setzen keine den Datenabruf begrenzenden Eingriffsschwellen voraus und enthalten solche auch nicht durch normenklare Verweisungen. 206

(1) Die allgemein zum Abruf von Bestandsdaten ermächtigenden § 10 Abs. 1 Satz 1 BKAG, § 7 Abs. 5 Satz 1, § 15 Abs. 2 Satz 1 ZFdG, § 8d Abs. 1 Satz 1 BVerfSchG sowie § 2b Satz 1 BNDG und § 4b Satz 1 MADG, soweit sie auf § 8d Abs. 1 Satz 1 BVerfSchG verweisen, sind nicht hinreichend eingegrenzt und darum unverhältnismäßig. 207

(a) § 10 Abs. 1 Satz 1 Nr. 1 BKAG ermächtigt das Bundeskriminalamt als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei zum Abruf von Bestandsdaten. Die Vorschrift setzt allein die Erforderlichkeit der Auskunft zur Erfüllung einer dem Bundeskriminalamt nach § 2 Abs. 2 Nr. 1 oder Abs. 6 BKAG obliegenden Aufgabe voraus, ohne begrenzende Eingriffsschwellen vorzusehen. 208

Das Bundeskriminalamt ist als Zentralstelle im Wesentlichen auf die Wahrnehmung von Koordinationsaufgaben beschränkt (vgl. BVerfGE 110, 33 <51>). Polizeiliche Aufgaben der Gefahrenabwehr und Strafverfolgung sind insoweit nicht übertragen, sondern werden dort nur koordiniert und informationell verklammert. Im Rahmen seiner Zentralstellenaufgaben unterstützt das Bundeskriminalamt die Polizeibehörden bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung (§ 2 Abs. 1 BKAG). Zur Wahrnehmung dieser Aufgabe hat es alle hierfür erforderlichen Informationen zu sammeln und auszuwerten (§ 2 Abs. 2 Nr. 1 BKAG) sowie unter anderem strategische und operative kriminalpolizeiliche Analysen zu erstellen und Einrichtungen 209

für kriminaltechnische Untersuchungen zu unterhalten und zu koordinieren (vgl. § 2 Abs. 6 BKAG). Soweit es zur Erfüllung dieser Aufgaben erforderlich ist, ermächtigt § 10 Abs. 1 Satz 1 Nr. 1 BKAG dazu, Bestandsdaten abzufragen.

Dabei enthält die Vorschrift keine ihre Reichweite näher begrenzenden Eingriffsschwellen. Vielmehr erlaubt sie einen Datenabruf schon dann, wenn dieser zur Wahrnehmung der genannten Aufgaben erforderlich ist. Der Eingriffsanlass wird auch nicht dadurch begrenzt, dass Bestandsdaten gemäß § 10 Abs. 1 Satz 1 Nr. 1 BKAG nur zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung erhoben werden dürfen. Die Datenerhebung bleibt damit zwar auf den vorhandenen Informationsstand beschränkt, der nur ergänzt oder ausgewertet werden darf, weshalb die Vorschrift keine Datenerhebungen abdeckt, durch die völlig neue Erkenntnisse erstmals gewonnen werden sollen (vgl. Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, 2009, S. 23). Gleichwohl ändert diese Beschränkung nichts am Vorfeldcharakter der Auswertungstätigkeit. 210

Die Vorschrift kann auch nicht – anders als noch die frühere Übermittlungsregelung in § 113 TKG a.F. (vgl. BVerfGE 130, 151 <205 f.>) – verständig dahin ausgelegt werden, dass sie bezogen auf die Gefahrenabwehr eine konkrete oder hinreichend konkretisierte Gefahr voraussetzt. Denn der Regelung fehlt es nicht nur an einer Eingriffsschwelle, sondern bereits an einer Beschränkung auf den Einzelfall, was – neben dem Erfordernis der Erforderlichkeit zur Aufgabenwahrnehmung – grundlegend für eine entsprechende Auslegung ist (vgl. dazu BVerfGE 130, 151 <205 f.>). 211

Soweit das Bundeskriminalamt als Zentralstelle auch im Bereich der Strafverfolgung zur Abfrage von Bestandsdaten ermächtigt wird, kommt § 10 Abs. 1 Satz 1 Nr. 1 BKAG von vornherein nicht als Ermächtigungsgrundlage in Betracht. Handelt es sich um rein repressives Handeln, erfordert der Datenabruf das Vorliegen zumindest eines Anfangsverdachts (oben Rn. 146, 153). Sobald aber ein solcher vorliegt, findet grundsätzlich die Strafprozessordnung mit ihren Verfahrensgarantien Anwendung und das Bundeskriminalamt müsste gemäß § 2 Abs. 2 Nr. 2 BKAG die zuständige Strafverfolgungsbehörde des Bundes oder der Länder unterrichten und den Vorgang an diese abgeben. Der Abruf von Bestandsdaten richtet sich dann nicht mehr nach der hier angegriffenen Abrufregelung, sondern allein nach § 100j StPO (vgl. Graulich, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 10 BKAG Rn. 11; vgl. auch BTDrucks 17/12034, S. 13). Eine Befugnis des Bundeskriminalamts als Zentralstelle zur Bestandsdatenabfra- 212

ge kann vor diesem Hintergrund im Bereich der Strafverfolgung grundsätzlich nicht bestehen (vgl. dazu auch BTDrucks 19/17741, S. 15). Soweit es – wie die Anwendungsbeispiele aus der Praxis zeigen – notwendig sein sollte, in einem konkreten Fall die örtlich zuständige Strafverfolgungsbehörde zu ermitteln, um den Vorgang dann zuständigkeitshalber an diese abzugeben oder um zeitkritische Anfragen im internationalen polizeilichen Dienstverkehr zu bearbeiten (vgl. BTDrucks 17/12034, S. 13), betrifft diese Koordinierungsaufgabe zwar den Kern der Zentralstellenfunktion des Bundeskriminalamtes. Für eine Befugnis zum Datenabruf durch das Bundeskriminalamt als Zentralstelle fehlt jedoch eine – verfassungsrechtlich nicht ausgeschlossene – Regelung dahin, dass und unter welchen Voraussetzungen § 10 Abs. 1 Satz 1 Nr. 1 BKAG hier anwendbar sein kann.

(b) § 10 Abs. 1 Satz 1 Nr. 2 und 3 BKAG, die das Bundeskriminalamt im Rahmen des Schutzes von Verfassungsorganen und der eigenen Leitung (§ 6 BKAG) sowie des Zeugenschutzes (§ 7 BKAG) zum Datenabruf ermächtigen, soweit die verlangte Auskunft zur Erfüllung dieser Aufgaben erforderlich ist, sind ebenfalls nicht hinreichend begrenzt. Einen konkreten Eingriffsanlass setzen weder die Regelungen selbst noch die in Bezug genommenen Aufgabennormen in §§ 6 und 7 BKAG voraus. Zwar geht die Begründung des Gesetzentwurfs davon aus, dass in diesen Fällen eine konkrete Gefahr bestehen wird (vgl. BTDrucks 17/12034, S. 14). Der Gesetzestext lässt dies jedoch nicht erkennen. Insbesondere werden die mit den Aufgabenzuweisungen in §§ 6 und 7 BKAG korrespondierenden allgemeinen Befugnisnormen in §§ 63 bis 65 und § 66 BKAG, die jeweils eine im Einzelfall bestehende Gefahr oder auch andere Eingriffsschwellen voraussetzen, nicht in Bezug genommen. Unabhängig davon bestehen im Hinblick auf den allgemeinen Verweis auf die Aufgaben des Bundeskriminalamts nach §§ 6 und 7 BKAG auch Bedenken, ob dies dem Bestimmtheitserfordernis genügt (vgl. BVerfGE 141, 220 <333 Rn. 303>). 213

(c) Auch die in den § 15 Abs. 2 Satz 1 und § 7 Abs. 5 Satz 1 ZFdG geregelten Befugnisse zum Abruf von Bestandsdaten sind nicht hinreichend eingegrenzt und deshalb unverhältnismäßig. Von daher bedarf es keiner Entscheidung, ob die in beiden Normen gewählte Regelungstechnik mit Verweisungen und zahlreichen Weiterverweisungen noch den Anforderungen an eine hinreichende Normenklarheit genügt (vgl. BVerfGE 110, 33 <57 f., 61 ff.>; BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 215). 214

(aa) § 15 Abs. 2 Satz 1 ZFdG ermächtigt das Zollkriminalamt, zur Erfüllung seiner Aufgaben nach § 4 Abs. 2 bis 4 ZFdG Bestandsdaten abzufragen. Die Vorschrift knüpft allein an die Erforderlichkeit zur Erfüllung der Aufgaben des Zollkriminalamts bei der Überwachung des Außenwirtschaftsverkehrs, des grenzüberschreitenden Warenverkehrs und der Bekämpfung der international organisierten Geldwäsche an. Die bloße Erfüllung der verschiedenen Aufgaben setzt jedoch keinen Eingriffsanlass voraus (vgl. dazu Wamers, in: Fehn/Wamers, Hk-ZFdG, § 4 Rn. 15, 51). 215

Soweit dem Zollkriminalamt nach § 4 Abs. 2 und 3 ZFdG die Aufdeckung unbekannter Straftaten und die Vorsorge für künftige Strafverfahren als jeweils repressiv-polizeiliche Aufgaben obliegen (vgl. dazu BVerfGE 113, 348 <370>; Braun, in: Gola/Heckmann, BDSG, 13. Aufl. 2019, § 45 Rn. 17), kann § 15 Abs. 2 Satz 1 ZFdG von vornherein nicht zum Datenabruf ermächtigen (dazu oben Rn. 212). Das Gleiche gilt im Ergebnis, soweit das Zollkriminalamt bei der Bekämpfung der international organisierten Geldwäsche nach § 4 Abs. 4 ZFdG mitwirkt und insoweit – neben der präventiven Überwachung des Geldverkehrs – originär strafverfolgend tätig wird (vgl. § 12b, § 31a Abs. 6 Zollverwaltungsgesetz (ZollVG); Wamers, in: Fehn/Wamers, Hk-ZFdG, § 4 Rn. 62). 216

(bb) Die Erwägungen zu § 10 Abs. 1 Satz 1 Nr. 1 BKAG und § 15 Abs. 2 Satz 1 ZFdG lassen sich weitgehend auf § 7 Abs. 5 Satz 1 ZFdG übertragen, der das Zollkriminalamt zur Abfrage von Bestandsdaten zur Erfüllung seiner Aufgaben als Zentralstelle nach § 3 ZFdG ermächtigt. Die dort bestimmten Aufgaben sind noch weiter gefasst als die von § 10 Abs. 1 Satz 1 Nr. 1 BKAG in Bezug genommenen Zentralstellenaufgaben des Bundeskriminalamts. Das Zollkriminalamt unterstützt andere Behörden der Zollverwaltung bei der Sicherung des Steueraufkommens und der Überwachung der Ausgaben nach Unionsrecht sowie der Aufdeckung unbekannter Steuerfälle und der Aufdeckung, Verhütung und Verfolgung von Steuerstraftaten und -ordnungswidrigkeiten (§ 3 Abs. 1 ZFdG). Seine Aufgaben umfassen ebenfalls Datenerhebungen weit im Vorfeld einer Gefahrenlage, insbesondere auch zur Sammlung und Auswertung von Informationen unter anderem für kriminalwissenschaftliche und -technische Einrichtungen (§ 3 Abs. 8 und 9 Nr. 1 ZFdG). Soweit sich die Aufgaben im präventiv-polizeilichen Bereich bewegen, wird eine begrenzende Eingriffsschwelle an keiner Stelle vorausgesetzt. Soweit sich die Zentralstellenaufgaben auch im repressiven Bereich bewegen (vgl. etwa § 3 Abs. 1 Satz 1 Nr. 2 ZFdG), was der Gesetzgeber offensichtlich nicht im 217

Blick hatte (vgl. BTDrucks 17/12034, S. 14), ist der Anwendungsbereich des § 7 Abs. 5 Satz 1 ZFdG von vornherein nicht eröffnet.

(d) § 8d Abs. 1 Satz 1 BVerfSchG sowie § 2b Satz 1 BNDG und § 4b Satz 1 MADG, soweit sie auf § 8d Abs. 1 Satz 1 BVerfSchG verweisen, genügen gleichfalls nicht den Anforderungen an die Verhältnismäßigkeit im engeren Sinne. Die Regelungen enthalten weder begrenzende Eingriffsschwellen noch eine Beschränkung auf den Einzelfall, sondern stellen einzig auf die Erforderlichkeit zur Erfüllung der Aufgabe des jeweiligen Dienstes ab. Umfasst werden daher auch allein strategische Auskunftsinteressen oder die Abrundung eigener Informationsbestände. Entgegen der Annahme der Bundesregierung ist die Aufgabe des Bundesamts für Verfassungsschutz auch nicht auf die Aufklärung bestimmter Beobachtungsobjekte beschränkt. § 3 Abs. 1 BVerfSchG weist dem Bundesamt ohne Einschränkung die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen über die dort genannten Bestrebungen und Tätigkeiten zu. Dies lässt nicht den Schluss zu, dass die Auskunft auch im Einzelfall zumindest zur Aufklärung einer bestimmten beobachtungsbedürftigen Aktion oder Gruppierung selbst erforderlich sein müsste. 218

(2) Nur teilweise den Anforderungen der Verhältnismäßigkeit genügt § 40 Abs. 1 Satz 1 BKAG, der das Bundeskriminalamt allgemein zum Abruf von Bestandsdaten ermächtigt, soweit dies für die Erforschung eines Sachverhalts oder die Ermittlung des Aufenthalts einer Person nach Maßgabe des § 39 Abs. 1 und 2 BKAG erforderlich ist. 219

(a) Nicht verhältnismäßig im engeren Sinne ist § 40 Abs. 1 Satz 1 BKAG, soweit er auf § 39 Abs. 1 BKAG Bezug nimmt. Der als Befugnisnorm ausgestaltete § 39 Abs. 1 BKAG verweist seinerseits auf § 5 Abs. 1 BKAG, der die Aufgabe des Bundeskriminalamts zur Abwehr von Gefahren des internationalen Terrorismus beschreibt. Als Aufgabennorm umfasst § 5 Abs. 1 BKAG Ermittlungen auch weit im Vorfeld konkreter Gefahren (vgl. zu § 4a Abs. 1 Satz 1 BKAG a.F. BVerfGE 141, 220 <331 Rn. 297>). Diese tatbestandliche Weite wird durch die weiteren Glieder der Verweisungskette nicht eingehegt. Weder § 40 BKAG selbst noch § 39 BKAG setzen begrenzende Eingriffsschwellen oder auch nur einen Einzelfallbezug voraus. Vielmehr erlauben sie den Datenabruf bereits dann, wenn die Auskunft allgemein dazu dienen kann, Gefahren des internationalen Terrorismus zu begegnen. 220

Zwar bestimmt der den 5. Abschnitt des Bundeskriminalamtgesetzes einleitende § 38 Abs. 1 BKAG, dass das Bundeskriminalamt zur Erfüllung seiner Aufgabe nach § 5 Abs. 1 Satz 1 BKAG die notwendigen Maßnahmen treffen kann, um eine Gefahr abzuwenden, und § 38 Abs. 2 BKAG konkretisiert eine Gefahr im Sinne dieses Abschnitts als eine im Einzelfall bestehende Gefahr für die öffentliche Sicherheit im Zusammenhang mit Straftaten nach § 5 Abs. 1 Satz 2 BKAG (vgl. zur Vorgängerregelung § 20a Abs. 2 BKAG a.F. BVerfGE 141, 220 <288 Rn. 157>). § 38 Abs. 1 BKAG gilt aber von vornherein nur, soweit die Befugnisse des Bundeskriminalamts nicht besonders geregelt sind. §§ 39 und 40 BKAG stellen jedoch solche besonderen Regelungen dar und setzen ihrerseits gerade keine Gefahr voraus (anders als etwa § 20g Abs. 1 Satz 1 Nr. 1 BKAG a.F., vgl. BVerfGE 141, 220 <288 f. Rn. 158>). Sie gehen daher in ihrem Anwendungsbereich § 38 BKAG vor; nur soweit Befugnisnormen überhaupt eine Gefahr voraussetzen, kann auf § 38 Abs. 2 BKAG zurückgegriffen werden (vgl. zu den Vorgängerregelungen Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, 2009, S. 53). 221

Auch die weitere tatbestandliche Voraussetzung des § 40 Abs. 1 Satz 1 BKAG, dass der Datenabruf zur Erforschung eines Sachverhalts oder des Aufenthaltsorts einer Person erforderlich sein muss, führt zu keiner hinreichenden Begrenzung der Abrufregelung. Die Bedeutung dieses im Strafprozessrecht üblichen Zusatzes (vgl. etwa § 100a Abs. 1 Satz 1 Nr. 3, § 100f Abs. 1 StPO) im Zusammenhang mit Aufgaben der Gefahrenabwehr erschließt sich hier nicht. 222

(b) Soweit § 40 Abs. 1 Satz 1 BKAG auf § 39 Abs. 2 Nr. 1 BKAG Bezug nimmt, fehlen jedenfalls hinreichend begrenzte Eingriffsschwellen. 223

In dem gegenüber § 39 Abs. 1 BKAG spezielleren § 39 Abs. 2 BKAG wird die Erhebung personenbezogener Daten zur Verhütung von Straftaten geregelt, die nur unter engeren Voraussetzungen zugelassen wird (vgl. Graulich, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 39 BKAG Rn. 2). § 39 Abs. 2 BKAG ergänzt die auf die Gefahrenabwehr beschränkte Eingriffsgrundlage des § 39 Abs. 1 BKAG und setzt ausdrücklich schon früher, nämlich bereits bei der Verhütung künftiger Straftaten an. § 40 Abs. 1 Satz 1 BKAG in Verbindung mit § 39 Abs. 2 Nr. 1 BKAG ermächtigt zum Abruf von Bestandsdaten im Bereich des internationalen Terrorismus, soweit Tatsachen die Annahme rechtfertigen, dass eine Person eine Straftat nach § 5 Abs. 1 Satz 2 BKAG begehen will. 224

Zwar ist der Gesetzgeber nicht von vornherein auf die Schaffung von Eingriffstatbeständen beschränkt, die der Abwehr konkreter Gefahren dienen. Allerdings bedarf es auch bei Maßnahmen zur Straftatenverhütung zumindest einer auf bestimmte Tatsachen und nicht allein auf allgemeine Erfahrungssätze gestützten Prognose, die auf eine konkrete Gefahr bezogen ist (oben Rn. 147). Grundsätzlich gehört hierzu, dass ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist (BVerfGE 141, 220 <272 Rn. 112, 290 f. Rn. 164>). Insbesondere in Bezug auf terroristische Straftaten kann der Gesetzgeber stattdessen aber auch darauf abstellen, ob das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft solche Straftaten begehen wird (vgl. BVerfGE 141, 220 <272 Rn. 112, 291 Rn. 164>). 225

Dem wird § 39 Abs. 2 Nr. 1 BKAG, der im Wesentlichen dem verfassungsrechtlich beanstandeten § 20g Abs. 1 Satz 1 Nr. 2 BKAG a.F. entspricht (vgl. BVerfGE 141, 220 <291 Rn. 165>), nicht gerecht. Zwar knüpft er an die mögliche Begehung terroristischer Straftaten an und verlangt das Vorliegen von Tatsachen, die darauf schließen lassen. Die Regelung setzt aber weder die Erkennbarkeit eines wenigstens seiner Art nach konkretisierten und absehbaren Geschehens voraus noch alternativ, dass das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft Straftaten begehen wird (vgl. BVerfGE 141, 220 <291 Rn. 165>). Sie enthält damit keine begrenzenden Anforderungen an die Vorhersehbarkeit des Kausalverlaufs. 226

(c) Keinen verfassungsrechtlichen Bedenken unterliegt demgegenüber § 40 Abs. 1 Satz 1 BKAG, soweit er auf § 39 Abs. 2 Nr. 2 BKAG Bezug nimmt. 227

§ 39 Abs. 2 Nr. 2 BKAG erlaubt den Datenabruf gegenüber Kontaktpersonen und entspricht für sich genommen weitgehend dem vom Bundesverfassungsgericht verfassungsrechtlich nicht beanstandeten § 20g Abs. 1 Satz 1 Nr. 3 in Verbindung mit § 20b Abs. 2 Nr. 2 BKAG a.F. (vgl. BVerfGE 141, 220 <291 ff. Rn. 166 ff.>). Der Gesetzgeber eröffnet hier keine ins Blaue hineingehende Möglichkeit der Überwachung des gesamten Umfelds einer Zielperson. Die Vorschrift verlangt vielmehr eine im Einzelnen definierte Tatnähe. Tatsachen, die die Annahme rechtfertigen, dass eines der genannten Nähekriterien vorliegt, sind demnach Voraussetzung für entsprechende Maßnahmen (vgl. dazu im Einzelnen BVerfGE 141, 220 <292 f. Rn. 168 f.>). Auch die mit Herabsetzung der Eingriffsschwelle einhergehenden erhöhten Anforderungen an das Gewicht der zu schüt- 228

zenden Rechtsgüter sind ohne weiteres erfüllt. Angesichts des begrenzten Eingriffsgewichts der allgemeinen Bestandsdatenauskunft bedarf es einer Begrenzung auf die Verhütung von Straftaten von zumindest erheblichem Gewicht (oben Rn. 150). Die Verhütung der im Einzelnen präzisierten (vgl. § 5 Abs. 1 Satz 2 BKAG) terroristischen Straftaten (vgl. insoweit BVerfGE 141, 220 <272 f. Rn. 112>) genügt dem allemal.

(3) § 22a Abs. 1 Satz 1 BPolG, der die Bundespolizei zum Abruf von Bestandsdaten ermächtigt, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes einer Person nach Maßgabe des § 21 Abs. 1 und 2 BPolG erforderlich ist, genügt den verfassungsrechtlichen Anforderungen ebenfalls nur teilweise. 229

(a) Nicht verhältnismäßig ist § 22a Abs. 1 Satz 1 BPolG, soweit er auf § 21 Abs. 1 BPolG verweist. § 21 Abs. 1 BPolG, der den Abruf von Bestandsdaten von vornherein nur zu präventiv-polizeilichen Zwecken und nicht zur Verfolgung von Straftaten und Ordnungswidrigkeiten gemäß §§ 12, 13 BPolG gestattet (vgl. Schenke, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 14 BPolG Rn. 42; Wehr, BPolG, 2. Aufl. 2015, § 21 Rn. 4; Drewes, in: Drewes/Malmberg/Wagner/Walter, BPolG, 6. Aufl. 2019, § 22a Rn. 8, § 21 Rn. 10), setzt lediglich voraus, dass ein Abruf zum Zweck einer der Bundespolizei obliegenden Aufgabe erforderlich ist. Damit werden alle Aufgaben erfasst, die der Bundespolizei durch das Bundespolizeigesetz oder andere Bundesgesetze zugewiesen worden sind (§ 1 Abs. 2 BPolG). Weder § 22a Abs. 1 Satz 1 BPolG noch § 21 Abs. 1 BPolG enthalten dabei ihre Reichweite begrenzende Eingriffsschwellen oder auch nur eine Begrenzung des Abrufs auf Einzelfälle (vgl. Drewes, in: Drewes/Malmberg/Wagner/Walter, BPolG, 6. Aufl. 2019, § 21 Rn. 13). Zwar konkretisiert § 14 Abs. 2 BPolG eine Gefahr im Sinne des Abschnitts 2 des Bundespolizeigesetzes als konkrete Gefahr. § 21 BPolG geht jedoch als speziellere Regelung der Generalklausel in § 14 BPolG vor und schließt damit einen Rückgriff auf diese aus (vgl. Drewes, in: Drewes/Malmberg/Wagner/Walter, BPolG, 6. Aufl. 2019, § 21 Rn. 5; vgl. auch zu § 39 Abs. 1 Satz 1 BKAG bereits oben Rn. 221). 230

(b) § 22a Abs. 1 Satz 1 BPolG ist auch nicht hinreichend begrenzt, soweit er auf § 21 Abs. 2 Nr. 1 BPolG verweist. § 21 Abs. 2 BPolG enthält die gegenüber Absatz 1 speziellere Befugnis zur Erhebung personenbezogener Daten zum Zwecke der Verhütung von Straftaten. Er betrifft in Nummer 1 die Daten eines möglicherweise künftigen Täters. Eine Datenerhebung wird insoweit zwar nur zugelas- 231

sen, wenn Tatsachen die Annahme rechtfertigen, dass eine Person eine Straftat mit erheblicher Bedeutung im Sinne des § 12 Abs. 1 BPolG begehen will. § 21 Abs. 2 Nr. 1 BPolG enthält jedoch – ebenso wie § 39 Abs. 2 Nr. 1 BKAG (oben Rn. 223 ff.) – keine hinreichend ausgestalteten Prognoseanforderungen (vgl. BVerfGE 141, 220 <291 Rn. 165>).

(c) Dagegen genügt § 22a Abs. 1 Satz 1 BPolG, soweit er auf § 21 Abs. 2 Nr. 2 BPolG verweist, für sich genommen den verfassungsrechtlichen Anforderungen. Zwar bestimmt die Regelung, die die Kontaktpersonen erfasst, keine ins Einzelne gehenden konkreten Nähekriterien (dazu BVerfGE 141, 220 <292 Rn. 168>), sondern setzt allein voraus, dass Tatsachen die Annahme rechtfertigen, dass die Kontaktperson zu einer Zielperson in einer Weise in Verbindung steht, die erwarten lässt, dass eine Maßnahme zur Straftatenverhütung führen wird, oder eine solche Verbindung hergestellt wird. Der Gesetzgeber eröffnet hier aber keine ins Blaue gehende Möglichkeit der Überwachung des gesamten Umfelds einer Zielperson. Es muss vielmehr jenseits allgemeiner Erfahrungssätze eine auf Tatsachen gestützte konkrete Erwartung begründet sein. In der Anwendung der Vorschrift können daher der bloße Kontakt oder die persönliche Nähe des Betreffenden zur Zielperson die Voraussetzungen der Regelung nicht erfüllen. Dies genügt den Anforderungen an die Vorhersehbarkeit des Kausalverlaufs. 232

Auch die mit Herabsetzung der Eingriffsschwelle einhergehenden erhöhten Anforderungen an das Gewicht der zu schützenden Rechtsgüter sind erfüllt. Die Abrufbefugnis ist beschränkt auf die Verhütung von Straftaten im Sinne des § 12 Abs. 1 BPolG mit erheblicher Bedeutung. Wenngleich nicht ersichtlich ist, welche konkreten Strafvorschriften zu einer Abfrage von Bestandsdaten ermächtigen, werden diese zumindest ihrer Art nach bezeichnet. 233

c) Die angegriffenen Befugnisse zum Abruf von Zugangsdaten (vgl. § 10 Abs. 1 Satz 2, § 40 Abs. 1 Satz 2 BKAG, § 22a Abs. 1 Satz 2 BPolG, § 7 Abs. 5 Satz 2, § 15 Abs. 2 Satz 2 ZFdG, § 8d Abs. 1 Satz 2 BVerfSchG sowie § 2b Satz 1 BNDG und § 4b Satz 1 MADG, soweit sie auf § 8d Abs. 1 Satz 2 BVerfSchG verweisen) sind für sich genommen hinreichend begrenzt und verhältnismäßig. Sie genügen auch den übergreifenden verfahrensrechtlichen Anforderungen (vgl. unten e, Rn. 244 ff.). 234

Alle Abrufregelungen setzen gleichlautend voraus, dass eine Auskunft nur verlangt werden darf, wenn die gesetzlichen Voraussetzungen für die Nutzung der 235

Daten vorliegen. Die Regelungen stellen damit sicher, dass Zugangsdaten nicht unabhängig von den Anforderungen an deren Nutzung und damit gegebenenfalls unter leichteren Voraussetzungen abgefragt werden können (vgl. BVerfGE 130, 151 <208 f.>). Entgegen der Auffassung der Beschwerdeführenden bedurfte es keiner darüber hinausgehenden abschließenden Auflistung der jeweils in Betracht kommenden Ermächtigungsgrundlagen, die zu einer Nutzung der Daten berechtigen können. Die Fassung der Normen lässt keine Zweifel daran, dass die Zulässigkeit des Abrufs an die Voraussetzungen gebunden ist, die bezogen auf den in der Abfragesituation konkret erstrebten Nutzungszweck zu erfüllen sind (dazu BVerfGE 130, 151 <209>), mithin, dass die Voraussetzungen einer weiteren Ermächtigungsgrundlage, die eine solche Nutzung erlaubt, erfüllt sein müssen. Unklarheiten darüber, welche Normen hier in Betracht kommen können, bestehen nicht.

Dabei ist es von Verfassungs wegen unbeachtlich, dass es für den Abruf von Zugangsdaten nach § 10 Abs. 1 Satz 1 Nr. 1, Satz 2 BKAG und § 7 Abs. 5 Satz 2 ZFdG keinen praktischen Anwendungsbereich gibt, weil weder das Bundeskriminalamt noch das Zollkriminalamt im Rahmen ihrer präventiv-polizeilichen Zentralstellenfunktion über eine eigenständige Befugnis zur Nutzung von nicht offen zugänglichen Inhaltsdaten verfügen, die sie zum Abruf von Zugangsdaten berechtigen würde. 236

d) Die Regelungen zum Abruf von Bestandsdaten, die anhand einer dynamischen IP-Adresse bestimmt werden (§ 10 Abs. 2, § 40 Abs. 2 BKAG, § 22a Abs. 2 BPolG, § 7 Abs. 6, § 15 Abs. 3 ZFdG, § 8d Abs. 2 Satz 1 BVerfSchG sowie § 2b Satz 1 BNDG und § 4b Satz 1 MADG, soweit sie auf § 8d Abs. 2 Satz 1 BVerfSchG verweisen) sind ganz überwiegend nicht hinreichend eingegrenzt und schon deshalb unverhältnismäßig. Allein § 40 Abs. 2 BKAG genügt, soweit er auf § 39 Abs. 2 Nr. 2 BKAG Bezug nimmt, insoweit den verfassungsrechtlichen Anforderungen; er erfüllt jedoch seinerseits nicht die übergreifenden verfahrensrechtlichen Anforderungen (vgl. unten e, Rn. 244 ff.). 237

Zwar ist es aus Gründen der Verhältnismäßigkeit grundsätzlich nicht geboten, für den Abruf von Bestandsdaten, die anhand dynamischer IP-Adressen bestimmt werden, gegenüber der allgemeinen Bestandsdatenabfrage erhöhte Eingriffsschwellen vorzusehen (oben Rn. 176, 179). Erforderlich ist aber stets ein hinreichend gewichtiger Rechtsgüterschutz, der in Wechselwirkung mit der jeweiligen Eingriffsschwelle steht. Für die Zuordnung von IP-Adressen bedarf es selbst dann, 238

wenn Eingriffsschwellen vorgesehen werden, die bezogen auf die Gefahrenabwehr eine konkrete Gefahr und bezogen auf die Strafverfolgung einen Anfangsverdacht voraussetzen, einer Beschränkung der Eingriffsbefugnis auf den Schutz von Rechtsgütern von hervorgehobenem Gewicht (oben Rn. 177 f.). Sind die Eingriffsschwellen hingegen herabgesetzt und will der Gesetzgeber für die Auskunft die Abwehr konkretisierter Gefahren genügen lassen, ist unter Berücksichtigung des spezifischen Eingriffsgewichts der Zuordnung dynamischer IP-Adressen jedenfalls eine Beschränkung auf besonders gewichtige Rechtsgüter geboten (oben Rn. 180). Diesen verfassungsrechtlichen Anforderungen werden die angegriffenen Regelungen – zusätzlich zu dem weitgehenden Fehlen begrenzender Eingriffsschwellen – überwiegend nicht gerecht.

aa) Die Abrufregelungen in § 10 Abs. 2 BKAG, § 40 Abs. 2 in Verbindung mit § 39 Abs. 1 und 2 Nr. 1 BKAG, § 22a Abs. 2 in Verbindung mit § 21 Abs. 1 und 2 Nr. 1 BPolG, § 7 Abs. 6 und § 15 Abs. 3 ZFdG, § 8d Abs. 2 Satz 1 BVerfSchG sowie § 2b Satz 1 BNDG und § 4b Satz 1 MADG, soweit sie auf § 8d Abs. 2 Satz 1 BVerfSchG verweisen, knüpfen allein an die ihrerseits unverhältnismäßigen Voraussetzungen der Befugnis zum allgemeinen Abruf von Bestandsdaten an (oben Rn. 206 ff.) und sehen daher auch für die Zuordnung von IP-Adressen keine oder jedenfalls keine hinreichend begrenzenden Eingriffsschwellen vor. Sie genügen schon deshalb nicht den verfassungsrechtlichen Anforderungen und sind unverhältnismäßig. 239

(1) Hingegen sehen einige dieser Abrufregelungen einen Rechtsgüterschutz vor, der selbst in Kombination mit abgesenkten Eingriffsschwellen noch hinreichend wäre. So ermächtigt § 40 Abs. 2 BKAG zur Abfrage zum Zwecke der Abwehr von Gefahren des internationalen Terrorismus. Dies sind nach der Legaldefinition in § 5 Abs. 1 Satz 2 BKAG nur Gefahren der Verwirklichung von näher konkretisierten Straftaten nach § 129a Abs. 1 und 2 StGB, mithin jedenfalls schwere Straftaten. Auch die Abrufregelungen im Bereich der Nachrichtendienste sehen in jedem Fall einen hinreichend gewichtigen Rechtsgüterschutz vor. Die von § 8d Abs. 2 BVerfSchG, § 2b Satz 1 BNDG und § 4b Satz 1 MADG jeweils in Bezug genommenen Aufgabenbereiche der Nachrichtendienste (§ 1 Abs. 1 BVerfSchG, § 1 Abs. 1 und 2 MADG, § 1 Abs. 2 BNDG) sind von vornherein dadurch gekennzeichnet, dass sie dem Schutz besonders gewichtiger Rechtsgüter oder vergleichbar gewichtiger öffentlicher Interessen dienen (vgl. BVerfGE 133, 277 <326 Rn. 118>; 141, 220 <339 Rn. 320>), sodass sie an das Vorliegen einer nur konkretisierten Gefahrenlage geknüpft werden können. 240

(2) Eine differenziertere Betrachtung erfordert § 10 Abs. 2, Abs. 1 Satz 1 Nr. 1 BKAG. Die Vorschrift betrifft den Datenabruf durch das Bundeskriminalamt, dessen Aufgaben auf kriminalpolizeiliche Angelegenheiten beschränkt sind (vgl. § 1 Abs. 1 BKAG), in seiner Funktion als Zentralstelle nach § 2 BKAG. Der entsprechend dem Kompetenztitel in Art. 73 Abs. 1 Nr. 10 Buchstabe a GG verwendete Begriff „Kriminalpolizei“ dient der Beschränkung auf Regelungen, die sich auf bedeutsame Straftaten von Gewicht beziehen (vgl. BVerfGE 133, 277 <318 Rn. 98>); ausgeschlossen sind insoweit jedenfalls die allgemeine Gefahrenabwehr und die Bekämpfung von Ordnungswidrigkeiten (vgl. Uhle, in: Maunz/Dürig, GG, Art. 73 Rn. 239 (April 2010); Wittreck, in: Dreier, GG, 3. Aufl. 2015, Art. 73 Rn. 72). Dies gilt auch für die Zentralstellenaufgaben des Bundeskriminalamts, die gemäß § 2 Abs. 1 BKAG auf koordinierende und unterstützende Aufgaben bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung beschränkt sind. § 10 Abs. 2, Abs. 1 Satz 1 Nr. 1 BKAG dient damit zwar dem Schutz von Rechtsgütern von hervorgehobenem Gewicht. Da hier jedoch der vorgelagerte Bereich der Verhütung von Straftaten betroffen ist, bedarf es aber des Schutzes besonders gewichtiger Rechtsgüter, was die Verhütung von zumindest schweren Straftaten voraussetzt. Eine derartige Begrenzung enthält die Regelung nicht. Das Gleiche gilt für § 22a Abs. 2 BPolG in Verbindung mit § 21 Abs. 2 BPolG, der lediglich der Verhütung von Straftaten mit erheblicher Bedeutung dient. 241

(3) Andere Abrufregelungen enthalten von vornherein keine hinreichende Beschränkung auf die im Einzelfall zu schützenden Rechtsgüter. Dies gilt etwa für § 22a Abs. 2 in Verbindung mit § 21 Abs. 1 BPolG sowie für § 7 Abs. 6 und § 15 Abs. 3 ZFdG. Auch § 10 Abs. 2, Abs. 1 Satz 1 Nr. 2 und 3 BKAG regeln diese gebotenen Begrenzungen – anders als etwa § 63 Abs. 2 und § 66 Abs. 1 BKAG – nicht in normenklarer Weise. 242

bb) Dagegen enthalten zwar sowohl § 22a Abs. 2 BPolG in Verbindung mit § 21 Abs. 2 Nr. 2 BPolG, als auch § 40 Abs. 2 in Verbindung mit § 39 Abs. 2 Nr. 2 BKAG hinreichend begrenzte Eingriffsschwellen (oben Rn. 227 f., 232). Doch nur § 40 Abs. 2 BKAG erfüllt auch die unter Berücksichtigung des Eingriffsgewichts der Zuordnung dynamischer IP-Adressen zu stellenden Anforderungen an den Rechtsgüterschutz, wonach die Zuordnung dynamischer IP-Adressen bei – wie hier – abgesenkten Eingriffsschwellen im Bereich der Straftatenverhütung der Verhütung zumindest schwerer Straftaten dienen muss (oben Rn. 181). § 22a Abs. 2 in Verbindung mit § 21 Abs. 2 Nr. 2 BPolG, der die Zuordnung dynamischer 243

IP-Adressen bereits zur Verhütung von Straftaten mit erheblicher Bedeutung zulässt, genügt dem nicht.

e) Die angegriffenen Regelungen genügen im Wesentlichen den aus dem Verhältnismäßigkeitsgrundsatz folgenden übergreifenden Maßgaben an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle. Sie enthalten auch tragfähige Regelungen zur Nutzung der Daten sowie zur Datenlöschung. Verfassungsrechtlich zu beanstanden ist allerdings, dass den Behörden beim Abruf von anhand dynamischer IP-Adressen bestimmter Bestandsdaten keine Dokumentationspflichten auferlegt werden. 244

aa) Anders als für heimliche Maßnahmen von höherer Eingriffsintensität (vgl. BVerfGE 141, 220 <269 Rn. 105, 282 f. Rn. 134 ff.>) bedarf es für die allgemeine Bestandsdatenauskunft aufgrund ihrer vergleichsweise geringen Eingriffsintensität keiner Benachrichtigungspflichten (vgl. BVerfGE 130, 151 <210>; vgl. auch EGMR, Breyer v. Germany, Urteil vom 30. Januar 2020, Nr. 50001/12, § 107 (nicht endgültig); EuGH, Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 60 f.). Vielmehr reicht es unter Verhältnismäßigkeitsgesichtspunkten, wenn die Betroffenen von einer Auskunftserteilung im Rahmen von ihnen gegenüber ergriffenen Folgemaßnahmen erfahren und deren Rechtmäßigkeit dann fachgerichtlich überprüfen lassen können (vgl. BVerfGE 150, 244 <302 Rn. 154>). 245

Im Hinblick auf Auskünfte, die eine erhöhte Eingriffsintensität aufweisen, wie die Zuordnung von IP-Adressen und – potentiell – die Auskunft über Zugangsdaten, sehen die fachrechtlichen Abrufregelungen eine nachträgliche Benachrichtigung grundsätzlich vor. Die Regelungen genügen den verfassungsrechtlichen Anforderungen, obgleich eine Benachrichtigung nur erfolgt, soweit und sobald der Zweck der Bestandsdatenauskunft nicht vereitelt wird, aber unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder des Betroffenen entgegenstehen (vgl. BVerfGE 125, 260 <344>; 129, 208 <250 f.>). Dabei sichert die den Behörden auferlegte Pflicht zur Dokumentation insbesondere der Gründe der Zurückstellung, dass nach gebotener Zeit das Fortbestehen der Voraussetzungen überprüft wird. Einer richterlichen Bestätigung des Absehens von der Benachrichtigung bedarf es darüber hinaus nicht (vgl. BVerfGE 125, 260 <344>). Im Falle des Abrufs von Zugangsdaten können sich aber erhöhte Anforderungen aus den Ermächtigungsgrundlagen zur Nutzung der Daten ergeben. 246

bb) Eine aufsichtliche Kontrolle ist – wie verfassungsrechtlich geboten (vgl. BVerfGE 65, 1 <46>; 133, 277 <369 Rn. 214>; 141, 220 <284 f. Rn. 141>; stRspr) – vorgesehen. Neben der Fachaufsicht ist eine datenschutzrechtliche Kontrolle durch den Bundesdatenschutzbeauftragten (vgl. etwa §§ 8 ff. Bundesdatenschutzgesetz (BDSG), § 69 BKAG, § 26a Abs. 2 und 3 BVerfSchG, § 32 BNDG und § 12a MADG) und behördliche Datenschutzbeauftragte (vgl. etwa § 70 BKAG) gewährleistet. Da ein Abruf von Zugangsdaten einen Antrag der jeweiligen Behördenleitung voraussetzt (vgl. § 10 Abs. 3 Satz 1, § 40 Abs. 3 Satz 1 BKAG, § 22a Abs. 3 Satz 1 BPolG, § 7 Abs. 7 Satz 1, § 15 Abs. 4 Satz 1 ZFdG, § 8d Abs. 2 Satz 2, § 8b Abs. 1 Satz 1 BVerfSchG sowie § 4b Satz 1 MADG und § 2b Satz 1 BNDG, jeweils in Verbindung mit § 8d Abs. 2 Satz 2, § 8b Abs. 1 Satz 1 BVerfSchG), besteht insoweit eine darüber hinausgehende, zumindest formalisierte Ebene der internen Aufsicht. 247

cc) Demgegenüber ist es mit den Anforderungen der Verhältnismäßigkeit nicht vereinbar, dass keine Pflicht zur Dokumentation der Entscheidungsgrundlagen für den Abruf solcher Bestandsdaten vorgesehen ist, die anhand einer dynamischen IP-Adresse bestimmt werden. 248

Angesichts der nur geringen Eingriffsintensität der allgemeinen Bestandsdatenauskunft ist auch unter Berücksichtigung des Umstands, dass die Maßnahme regelmäßig geheim erfolgt und Betroffene auch im Nachhinein nicht über eine erteilte Auskunft benachrichtigt werden, keine Dokumentation der Entscheidungsgrundlagen erforderlich. Sie ist auch nicht deshalb geboten, weil sich die Entscheidung über eine Bestandsdatenabfrage allein im Inneren einer Behörde vollziehen würde (dazu BVerfGE 150, 244 <303 Rn. 157>). Zwar können allein die Behörden die materiellen Voraussetzungen eines Auskunftsverlangens sicherstellen. Sie treten aber jedenfalls insoweit nach außen, als sie ein schriftliches Auskunftsverlangen unter Angabe einer gesetzlichen Bestimmung an die Diensteanbieter richten müssen (vgl. § 113 Abs. 2 Satz 1 TKG). 249

Dagegen kann die Zuordnung dynamischer IP-Adressen angesichts ihres erhöhten Eingriffsgewichts nur dann als verhältnismäßig angesehen werden, wenn die Entscheidungsgrundlagen für die Durchführung einer solchen Maßnahme nachvollziehbar und überprüfbar dokumentiert werden. Die rechtlichen und tatsächlichen Grundlagen entsprechender Auskunftsbegehren sind aktenkundig zu machen (BVerfGE 125, 260 <344>). Zum einen rationalisiert und mäßigt es die Entscheidung, wenn die entscheidende Behörde sich selbst über ihre Entschei- 250

dungsgrundlagen Rechenschaft ablegen muss. Zum anderen ermöglicht erst die Dokumentation eine aufsichtliche Kontrolle durch die Datenschutzbeauftragten. Schließlich wird durch die Dokumentation die verwaltungsgerichtliche Kontrolle erleichtert (vgl. BVerfGE 150, 244 <303 Rn. 157>). Für den Abruf von Zugangsdaten bedarf es demgegenüber keiner Regelung genereller Dokumentationspflichten. Soweit sie aufgrund des Eingriffsgewichts im Einzelfall geboten sein sollten, ergeben sich entsprechende Anforderungen regelmäßig aus den jeweiligen Ermächtigungsgrundlagen zur Nutzung der Daten.

dd) Gesetzlich geregelter Berichtspflichten gegenüber Parlament und Öffent- 251
lichkeit bedarf es nicht. Die Notwendigkeit, durch parlamentarische Berichtspflichten eine unmittelbar demokratisch legitimierte Kontrolle und Überprüfung zu erreichen, besteht aus Gründen der Verhältnismäßigkeit nur für tief in die Privatsphäre eingreifende Ermittlungs- und Überwachungsbefugnisse mit spezifisch breitenwirksamem Grundrechtsgefährdungspotential (vgl. BVerfGE 141, 220 <268 f. Rn. 103, 285 Rn. 142 f.> m.w.N.). Bei – wie vorliegend – nicht besonders eingriffsintensiven Maßnahmen ist eine derartige Beobachtung und Evaluation entgegen der Auffassung der Beschwerdeführenden nicht geboten.

ee) Eine vorherige Kontrolle durch eine unabhängige Stelle, etwa in Form ei- 252
ner richterlichen Anordnung, ist aus Gründen der Verhältnismäßigkeit verfassungsrechtlich nicht geboten. Von daher begegnet es keinen Bedenken, dass die Abrufregelungen einfachrechtlich nur für den Abruf von Zugangsdaten einen Richtervorbehalt beziehungsweise im nachrichtendienstlichen Bereich eine vorherige Überprüfung durch die G 10-Kommission vorsehen und der für den Abruf von Zugangsdaten vorgesehene Richtervorbehalt zahlreiche Ausnahmen kennt.

(1) Ermöglicht eine Norm Maßnahmen einer Behörde, die gegenüber Be- 253
troffenen heimlich durchgeführt werden und die besonders geschützte Zonen der Privatheit berühren oder eine besonders hohe Eingriffsintensität aufweisen, ist dem Gewicht des Grundrechtseingriffs durch geeignete Verfahrensvorkehrungen Rechnung zu tragen und insbesondere eine vorherige Kontrolle durch eine unabhängige Stelle, etwa in Form einer richterlichen Anordnung, vorzusehen (vgl. BVerfGE 120, 274 <331>; 141, 220 <275 Rn. 117>; vgl. auch EGMR, Szabó und Vissy v. Hungary, Urteil vom 12. Januar 2016, Nr. 37138/14, § 77). Abzustellen ist neben der Heimlichkeit maßgeblich darauf, dass es sich um Maßnahmen handelt, bei denen damit zu rechnen ist, dass sie auch höchstprivate Informationen erfassen (vgl. BVerfGE 141, 220 <275 Rn. 117>; vgl. auch EuGH, Urteil vom

21. Dezember 2016, Tele2 Sverige und Watson u.a., C-203/15 u.a., EU:C:2016:970, Rn. 99, 120, 125). Eine vorbeugende Kontrolle kann dann bedeutsames Element eines effektiven Grundrechtsschutzes sein und gewährleisten, dass die Entscheidung über eine heimliche Maßnahme auf die Interessen des Betroffenen hinreichend Rücksicht nimmt, wenn dieser selbst seine Interessen aufgrund der Heimlichkeit der Maßnahme im Vorwege nicht wahrnehmen kann (vgl. BVerfGE 120, 274 <331 f.>).

(2) Für die Abfrage anhand dynamischer IP-Adressen bestimmter Bestands- 254
daten, die die Auswertung von sowohl auf vertraglicher Grundlage als auch vorsorglich gespeicherter Verkehrsdaten verlangt, ist trotz des gegenüber der allgemeinen Bestandsdatenauskunft erhöhten Eingriffsgewichts kein Richtervorbehalt erforderlich (vgl. BVerfGE 125, 260 <344>). Anders als für Abrufregelungen, die den Abruf der Gesamtheit bevorratend gespeicherter Verkehrsdaten ermöglichen und für die ein Richtervorbehalt grundsätzlich notwendig ist (vgl. BVerfGE 125, 260 <337 f.>; vgl. EuGH, Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u.a., C-203/15 u.a., EU:C:2016:970, Rn. 120, 125), bedarf es für eine Auskunft über einen Anschlussinhaber, der unter nur punktueller und mittelbarer Verwendung von Verkehrsdaten ermittelt wurde, keiner zusätzlichen Sicherungen in Form einer vorbeugenden unabhängigen Kontrolle.

(3) Das Gleiche gilt grundsätzlich auch für die Ermächtigung zum Abruf von 255
Zugangsdaten, welche an die Voraussetzungen für ihre Nutzung gebunden ist. Zwar hat schon die Zugangsdatenabfrage als solche jenseits der vorgesehenen Nutzung der Daten eine eigenständige Eingriffswirkung, weil sie den informationellen Selbstschutz der Betroffenen vereitelt und so ihr Vertrauen in die Privatheit ihrer Kommunikationsbeziehungen enttäuscht. Das Eingriffsgewicht wird jedoch maßgeblich erst durch die Nutzung der Zugangsdaten bestimmt, nach deren Voraussetzungen sich damit der Zugriff auf diese Daten auch in verfahrensrechtlicher Hinsicht richtet.

Die Verhältnismäßigkeit gebietet daher nicht, für die Erhebung der Zugangs- 256
daten als solche eigene Voraussetzungen vorzusehen und insoweit ausnahmslos einem Richtervorbehalt zu unterstellen. Rechtsstaatlich geboten ist nur, die Auskunftserteilung über die Zugangssicherung – materiell wie verfahrensrechtlich – auch an die Voraussetzungen zu binden, die in der jeweiligen Abfragesituation für den damit konkret erstrebten Nutzungszweck erfüllt sein müssen (vgl. BVerfGE 130, 151 <208 f.>). Diese bestimmen sich nach eigenständigen Rechtsgrundlagen

und unterscheiden sich je nach Art und Gewicht des Eingriffs sowohl in formeller als auch in materieller Hinsicht. Weil bei jeder Abfrage von Zugangsdaten gleichzeitig auch die Voraussetzungen für deren Nutzung vorliegen müssen, ist die vorherige richterliche Kontrolle dann, wenn sie aufgrund einer eingriffsintensiven Nutzung verfassungsrechtlich geboten ist, dort uneingeschränkt sichergestellt (vgl. Bäcker, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, Bd. 1, 2009, S. 99 <114 f.>).

Wenn gleichwohl auf einfachrechtlicher Ebene, sozusagen überschießend, für die Abfrage aller Zugangsdaten ein eigener Richtervorbehalt unabhängig von den Nutzungsvoraussetzungen vorgesehen ist, führen dessen Ausnahmen (vgl. § 10 Abs. 3 Satz 4, § 40 Abs. 3 Satz 4 BKAG, § 22a Abs. 3 Satz 4 BPolG, § 7 Abs. 7 Satz 4, § 15 Abs. 4 Satz 4 ZFdG) nicht zur Unverhältnismäßigkeit der Regelungen. Sofern der hier geregelte Richtervorbehalt allerdings dazu bestimmt wäre, die sich aus den jeweiligen Nutzungsregelungen ergebenden Anforderungen an den Richtervorbehalt zu ersetzen, begegnete die Reichweite der hier in Rede stehenden Ausnahmen aber für sich genommen verfassungsrechtlichen Bedenken. Soweit der vorgesehene Richtervorbehalt ausnahmsweise dann entfällt, wenn der Betroffene von einer beabsichtigten Zugangsdatenabfrage Kenntnis hat oder haben müsste, ist nicht ausgeschlossen, dass Rechtsschutz insoweit nur noch nachträglich stattfinden kann. Der Betroffene wäre dann nicht bessergestellt als im Falle der nachträglichen Benachrichtigung. Der Richtervorbehalt soll demgegenüber aber gerade eine vorbeugende Kontrolle sichern und einen Grundrechtseingriff gegebenenfalls von vornherein vermeiden. Soweit der Richtervorbehalt auch dann entfällt, wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird, ist nicht sichergestellt, dass gerade auch die abfragende Behörde zur Nutzung der Daten berechtigt ist und die dafür erforderlichen Voraussetzungen vorliegen (vgl. Hauck, StV 2014, S. 360 <364>). Da die Regelung jedoch die sich aus den jeweiligen Nutzungsregelungen ergebenden Anforderungen an einen Richtervorbehalt schon bei Zugriff auf die Zugangsdaten nicht ersetzt, sondern deren Vorliegen voraussetzt, ist sie verfassungsrechtlich nicht zu beanstanden. 257

ff) Die Regelungen zur Sicherheit, weiteren Nutzung und Löschung der Daten durch die abfragenden Behörden genügen den verfassungsrechtlichen Anforderungen. 258

(1) Für Bestandsdatenabfragen durch das Bundeskriminalamt, das Zollkriminalamt und die Bundespolizei regelt § 47 BDSG die allgemeinen Grundsätze der 259

Datenverarbeitung, darunter den Zweckbindungsgrundsatz (§ 47 Nr. 2 BDSG). Ferner stellt § 64 BDSG Anforderungen an die Datensicherheit, während § 74 BDSG Voraussetzungen der Datenübermittlung enthält. Zudem sind nach § 75 Abs. 2 BDSG personenbezogene Daten unverzüglich zu löschen, wenn ihre Verarbeitung unzulässig ist, sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist.

(2) Die Fachgesetze selbst enthalten ergänzende Regelungen. § 12 BKAG re- 260
gelt den Grundsatz der Zweckbindung, der auch gemäß den §§ 25 ff. BKAG der Übermittlung im innerstaatlichen und internationalen Bereich Grenzen setzt. Darüber hinaus enthalten die §§ 69 ff. BKAG Vorgaben zu Datenschutz, Datensicherheit und Rechten der Betroffenen. Die einzelnen Schutzvorschriften orientieren sich stark an den unterschiedlichen Eingriffsermächtigungen und sind daher differenziert ausgestaltet. Das Bundespolizeigesetz und das Zollfahndungsdienstgesetz enthalten entsprechende Vorschriften (Abschnitt 2 Unterabschnitt 2 Teil 2 BPolG, §§ 33 ff. ZFdG). Das insoweit schon durch das Bundesdatenschutzgesetz gewährleistete Schutzniveau wird durch diese Vorschriften ergänzt. Auch die gegenständlichen nachrichtendienstlichen Gesetze enthalten eigene flankierende Vorschriften. Sie verweisen etwa über § 27 Nr. 2 BVerfSchG, § 32a Nr. 2 BNDG und § 13 Nr. 2 MADG jeweils auf § 64 BDSG.

D.

Unabhängig davon, inwieweit das Bundesverfassungsgericht auch für eine 261
solche Prüfung zuständig wäre, ergeben sich aus den Unionsgrundrechten keine weiteren Maßgaben. Auch wenn die angegriffenen Vorschriften teilweise angesichts des Art. 15 RL 2002/58/EG oder des Art. 6 DSGVO (vgl. oben Rn. 85–87) als Durchführung des Unionsrechts im Sinne des Art. 51 Abs. 1 Satz 1 GRCh anzusehen sein sollten, gibt es schon keine konkreten und hinreichenden Anhaltspunkte dafür, dass die Grundrechte des Grundgesetzes in der vorliegenden Auslegung das Schutzniveau der Grundrechtecharta der Europäischen Union in der Rechtsprechung des Europäischen Gerichtshofs im hier zu entscheidenden Fall nicht mit gewährleisten könnten (vgl. BVerfG, Beschluss des Ersten Senats vom 6. November 2019 - 1 BvR 16/13 -, Rn. 67 ff.). Insbesondere ergeben sich solche Anhaltspunkte nicht aus den Entscheidungen des Europäischen Gerichtshofs zur Vorratsdatenspeicherungsrichtlinie (EuGH, Urteil vom 8. April 2014, Digital Rights Ireland und Seitlinger u.a., C-293/12 u.a., EU:C:2014:238) und zu Vorratsdaten-

speicherungsbefugnissen der Mitgliedstaaten (EuGH, Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u.a., C-203/15 u.a., EU:C:2016:970). In diesen Entscheidungen ging es um die Anforderungen an eine innerstaatlich vollständige Erfassung sämtlicher Telekommunikationsverbindungsdaten, die nahezu lückenlose Persönlichkeitsprofile einzelner Kommunikationsteilnehmer ermöglichen. Hiervon unterscheidet sich die bloß mittelbare und punktuelle Verwendung von Verkehrsdaten bei der Zuordnung dynamischer IP-Adressen grundlegend. Auch aus der Entscheidung des Europäischen Gerichtshofs im Fall „Ministerio Fiscal“ (EuGH, Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788) ergeben sich keine Anhaltspunkte für ein über die Grundrechte des Grundgesetzes hinausgehendes Schutzniveau der Grundrechtecharta. Klargestellt wurde dort vielmehr, dass der Zugang öffentlicher Stellen zu bei Diensteanbietern gespeicherten Bestandsdaten nicht als derart schwerer Grundrechtseingriff angesehen werden kann, dass er nur zur Bekämpfung schwerer Kriminalität zulässig wäre (vgl. EuGH, Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 63; vgl. auch EGMR, Breyer v. Germany, Urteil vom 30. Januar 2020, Nr. 50001/12, §§ 95, 101 (nicht endgültig)). Es ist nicht ersichtlich, dass der Grundrechtsschutz des Grundgesetzes hier das Schutzniveau der Grundrechtecharta der Europäischen Union im Rahmen eines auf Vielfalt angelegten Grundrechtsschutzes in Europa nicht gewährleistet (vgl. auch BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 326).

E.

Die angegriffenen Vorschriften sind überwiegend für mit Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 sowie mit Art. 10 Abs. 1 GG unvereinbar zu erklären. 262

I.

1. Die Feststellung einer Verfassungswidrigkeit gesetzlicher Vorschriften führt grundsätzlich zu deren Nichtigkeit (§ 95 Abs. 3 Satz 1 BVerfGG; vgl. BVerfGE 101, 397 <409>). Allerdings kann sich das Bundesverfassungsgericht, wie sich aus § 31 Abs. 2 Satz 2 und 3 BVerfGG ergibt, auch darauf beschränken, eine verfassungswidrige Norm nur für mit dem Grundgesetz unvereinbar zu erklären (vgl. BVerfGE 109, 190 <235>). Die Unvereinbarkeitserklärung kann das Bundesverfassungsgericht dabei zugleich mit der Anordnung einer befristeten Fortgeltung der verfassungswidrigen Regelung verbinden. Dies kommt in Betracht, wenn die sofortige Ungültigkeit der zu beanstandenden Norm dem Schutz überragender 263

Güter des Gemeinwohls die Grundlage entziehen würde und eine Abwägung mit den betroffenen Grundrechten ergibt, dass der Eingriff für eine Übergangszeit hinzunehmen ist (BVerfGE 150, 244 <306 Rn. 168> m.w.N.; stRspr). Für die Übergangszeit kann das Bundesverfassungsgericht vorläufige Anordnungen treffen, um die Befugnisse der Behörden bis zur Herstellung eines verfassungsmäßigen Zustandes durch den Gesetzgeber auf das zu reduzieren, was nach Maßgabe dieser Abwägung geboten ist (BVerfGE 141, 220 <351 Rn. 355> m.w.N.).

2. Nach diesen Maßstäben sind die Vorschriften, soweit sie verfassungswidrig sind, nicht für nichtig zu erklären. Die Verfassungswidrigkeit der zu beanstandenden Regelungen zu Übermittlung und Abruf von Bestandsdaten beruht insbesondere auf nicht hinreichenden Eingriffsschwellen und fehlenden Anforderungen an den Rechtsgüterschutz. Die Gründe für die Verfassungswidrigkeit betreffen nicht den Kern der durch die Vorschriften eingeräumten Befugnisse, sondern ihre rechtsstaatliche Ausgestaltung. Der Gesetzgeber kann die Vorschriften insoweit ohne weiteres nachbessern und damit den Kern der mit ihnen verfolgten Ziele auf verfassungsmäßige Weise verwirklichen. Angesichts der Bedeutung, die der Gesetzgeber der Bestandsdatenauskunft für die staatliche Aufgabenwahrnehmung beimessen darf, ist unter diesen Umständen deren vorübergehende Fortgeltung eher hinzunehmen als deren Nichtigkeitserklärung. 264

3. Die angegriffenen Regelungen sind daher – in dem aus dem Tenor ersichtlichen Umfang – für mit dem Grundgesetz unvereinbar zu erklären. 265

Dies betrifft zunächst § 113 TKG. Da alle in § 113 TKG geregelten Übermittlungsbefugnisse zu beanstanden sind, ist die Vorschrift in Gänze für verfassungswidrig zu erklären, weil für die flankierenden Regelungen kein selbständiger Anwendungsbereich verbleibt. Die angegriffenen Abrufregelungen sind demgegenüber nur insoweit für verfassungswidrig zu erklären, als die Befugnisse zum allgemeinen Abruf von Bestandsdaten und von anhand dynamischer IP-Adressen bestimmter Bestandsdaten betroffen sind. Ausgenommen hiervon sind § 40 Abs. 1 Satz 1 BKAG in Verbindung mit § 39 Abs. 2 Nr. 2 BKAG sowie § 22a Abs. 1 Satz 1 BPolG in Verbindung mit § 21 Abs. 2 Nr. 2 BPolG. Nicht zu beanstanden sind auch die in allen Fachgesetzen eingeräumten Befugnisse zum Abruf von Zugangsdaten, wenngleich diesen – unbeschadet der Anordnung der vorübergehenden Fortgeltung (dazu sogleich unter 4, Rn. 268) – weithin ein Anwendungsbereich fehlt, da die Regelungen jeweils auf die Befugnis zum allgemeinen Abruf von Bestandsdaten Bezug nehmen und diese ganz überwiegend verfassungswidrig 266

sind. Dies gilt insoweit auch für die Regelungen zum allgemeinen Abruf von Bestandsdaten nach § 40 Abs. 1 Satz 1 in Verbindung mit § 39 Abs. 2 Nr. 2 BKAG sowie § 22a Abs. 1 Satz 1 BPolG in Verbindung mit § 21 Abs. 2 Nr. 2 BPolG, die tatbestandlich an die Voraussetzungen des § 39 Abs. 2 Nr. 1 BKAG beziehungsweise § 21 Abs. 2 Nr. 1 BPolG anknüpfen, welche jedoch jeweils für sich genommen den verfassungsrechtlichen Anforderungen an die Bestandsdatenauskunft nicht genügen.

Die Gründe, die zur teilweisen Verfassungswidrigkeit von § 2b Satz 1 BNDG in der angegriffenen Fassung führen, treffen auf dessen Neubezeichnung als § 4 Satz 1 BNDG ebenso zu. Gemäß § 78 Satz 2 BVerfGG, der auch im Verfassungsbeschwerdeverfahren und auf zeitlich nachfolgende Gesetzesfassungen anwendbar ist (vgl. BVerfGE 133, 377 <423 Rn. 106>), ist daher § 4 Satz 1 BNDG in der Fassung des Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23. Dezember 2016 (BGBl I S. 3346) im Interesse der Rechtsklarheit in demselben Umfang ebenfalls für mit dem Grundgesetz unvereinbar zu erklären. Für die neu gefassten § 7 Abs. 7 Satz 1 und 2, § 15 Abs. 4 Satz 1 und 2 ZFdG besteht keine derartige Veranlassung. Sie enthalten lediglich Regelungen zum Verfahren des Abrufs von Zugangsdaten, die verfassungsrechtlich nicht zu beanstanden sind. 267

4. Die Unvereinbarkeitserklärung ist mit der Anordnung der vorübergehenden Fortgeltung bis zum Ablauf des 31. Dezember 2021 verbunden. Die Anordnung erstreckt sich auf alle für mit der Verfassung für unvereinbar erklärten Befugnisse einschließlich der in § 113 Abs. 2 bis 5 TKG geregelten verfahrensrechtlichen Anforderungen; sie bedarf mit Blick auf die betroffenen Grundrechte jedoch einschränkender Maßgaben. Diese orientieren sich an den bisherigen Regelungen. Dem Gesetzgeber stehen für eine Neuregelung freilich verschiedene Möglichkeiten zur Verfügung, insbesondere die verfassungsrechtlich geforderte Begrenzung der Verwendungszwecke der Bestandsdatenauskunft sicherzustellen. Erforderlich sind stets die Reichweite der Befugnis begrenzende Eingriffsschwellen und jedenfalls im Bereich der Zuordnung von IP-Adressen auch ein hinreichend gewichtiger Rechtsgüterschutz. Die Eingriffsschwellen können auch abgesenkt werden, wenn – unter Berücksichtigung von Art, Umfang und Verwendungsmöglichkeiten der verwendeten Daten – entsprechend höhere Anforderungen an den Rechtsgüterschutz gestellt werden (vgl. BVerfGE 141, 220 <272 f. Rn. 112>). Bis zur Neuregelung gelten nachfolgende Maßgaben: 268

a) § 113 Abs. 1 Satz 1 TKG und die hier angegriffenen Regelungen zum allgemeinen Abruf von Bestandsdaten können weiter angewendet werden, wenn eine Auskunft bezogen auf die Gefahrenabwehr zur Abwehr einer konkreten Gefahr im Sinne der polizeilichen Generalklausel erforderlich oder bezogen auf die Nachrichtendienste zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten ist. Bezogen auf die Verfolgung von Straftaten und Ordnungswidrigkeiten darf § 113 Abs. 1 Satz 1 TKG weiter angewendet werden, wenn zumindest ein Anfangsverdacht vorliegt. 269

b) Darüber hinaus können § 113 Abs. 1 Satz 1 TKG und § 40 Abs. 1 Satz 1 BKAG oder § 22a Abs. 1 Satz 1 BPolG im jeweiligen Zusammenwirken auch dann angewendet werden, wenn die Auskunft zur Verhütung von Straftaten nach § 39 Abs. 2 BKAG oder § 21 Abs. 2 BPolG erforderlich ist. Dabei sind § 39 Abs. 2 Nr. 1 BKAG und § 22a Abs. 2 Nr. 1 BPolG nur mit der Maßgabe anwendbar, dass bestimmte Tatsachen die Annahme rechtfertigen müssen, dass eine Person innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat nach § 5 Abs. 1 Satz 2 BKAG oder eine Straftat mit erheblicher Bedeutung nach § 12 Abs. 1 BPolG begehen wird oder dass deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines überschaubaren Zeitraums eine solche Straftat begehen wird (vgl. BVerfGE 141, 220 <272 f. Rn. 112>). 270

c) § 113 Abs. 1 Satz 2 TKG kann weiter angewendet werden, wenn auch die Voraussetzungen einer Nutzung der von ihm erfassten Daten im Einzelfall vorliegen (vgl. BVerfGE 130, 151 <210>). 271

d) § 113 Abs. 1 Satz 3 TKG und die hier angegriffenen Regelungen zum Abruf von Bestandsdaten, die anhand einer dynamischen IP-Adresse bestimmt werden, dürfen weiter angewendet werden, wenn über die zuvor unter a) formulierte Maßgaben hinaus die Auskunft zur Abwehr einer Gefahr für Rechtsgüter von hervorgehobenem Gewicht oder zur Verfolgung von Straftaten oder zumindest besonders gewichtigen Ordnungswidrigkeiten erfolgt. 272

e) Darüber hinaus können § 113 Abs. 1 Satz 3 TKG und § 40 Abs. 2 BKAG oder § 22a Abs. 2 BPolG im jeweiligen Zusammenwirken und soweit sie auf § 39 Abs. 2 BKAG beziehungsweise § 21 Abs. 2 BPolG Bezug nehmen unter Berücksichtigung der unter a) und b) formulierten Maßgaben weiter angewendet werden, 273

wobei im Falle des § 22a Abs. 2 BPolG die Auskunft zudem zur Verhütung einer schweren Straftat nach § 12 Abs. 1 BPolG erforderlich sein muss.

II.

Die Auslagenentscheidung beruht auf § 34a Abs. 2 und 3 BVerfGG. 274

Die Entscheidung ist zu der Frage, ob § 113 Abs. 1 Satz 1 in Verbindung mit Abs. 2 Satz 1 TKG den Anforderungen der Verhältnismäßigkeit genügt, mit einer Gegenstimme ergangen. 275

Harbarth Masing Paulus

Baer Britz Ott

Christ Radtke