Abschrift

C-794/19-1

Bundesverwaltungsgericht

Eingetragen in das Register des Gerichtshofes unter der Nr. 1132256
Luxemburg, den 29. 10. 2019
Fax/E-mail:
eingegangen am: 29.10.19
Der Kanzler, im Auftrag
Daniel Dittert
Referatsleiter

BESCHLUSS

BVerwG 6 C 13.18
VG 9 K 7417/17

Verkündet
am 25. September 2019
Harnisch
als Urkundsbeamtin der Geschäftsstelle

In der Verwaltungsstreitsache

der Telekom Deutschland GmbH,
vertreten durch die Geschäftsführung,
Landgrabenweg 151, 53227 Bonn,

Klägerin und Revisionsbeklagten,

- Prozessbevollmächtigte:
Rechtsanwälte Dolde Mayen & Partner,
Mildred-Scheel-Straße 1, 53175 Bonn -

g e g e n

die Bundesrepublik Deutschland,
vertreten durch die Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen,
Tulpenfeld 4, 53113 Bonn,

Beklagte und Revisionsklägerin,

ECLI:DE:BVerwG:2019:250919B6C13.18.0

hat der 6. Senat des Bundesverwaltungsgerichts
auf die mündliche Verhandlung am 25. September 2019
durch den Vorsitzenden Richter am Bundesverwaltungsgericht Prof. Dr. Kraft
und die Richter am Bundesverwaltungsgericht Dr. Heitz, Dr. Möller, Hahn
sowie die Richterin am Bundesverwaltungsgericht Steiner

beschlossen:

Das Verfahren wird ausgesetzt.

Es wird eine Entscheidung des Gerichtshofs der Europäischen Union zu folgender Frage eingeholt:

Ist Art. 15 der Richtlinie 2002/58/EG im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union einerseits und des Art. 6 der Charta der Grundrechte der Europäischen Union sowie des Art. 4 des Vertrags über die Europäische Union andererseits dahin auszulegen, dass er einer nationalen Regelung entgegensteht, welche die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste verpflichtet, Verkehrs- und Standortdaten der Endnutzer dieser Dienste auf Vorrat zu speichern, wenn diese Verpflichtung

- keinen spezifischen Anlass in örtlicher, zeitlicher oder räumlicher Hinsicht voraussetzt,

- Gegenstand der Pflicht zur Speicherung bei der Erbringung öffentlich zugänglicher Telefondienste - einschließlich der Übermittlung von Kurz-, Multimedia- oder ähnlichen Nachrichten sowie unbeantworteter oder erfolgloser Anrufe - folgende Daten sind:

  - die Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,

  - Datum und Uhrzeit von Beginn und Ende der Verbindung bzw. - bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht - die Zeitpunkte der Versendung und des Empfangs der Nachricht unter Angabe der zugrunde liegenden Zeitzone,

  - Angaben zu dem genutzten Dienst, wenn im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können,

  - im Fall mobiler Telefondienste ferner

- die internationale Kennung mobiler Teilnehmer für den anrufenden und den angerufenen Anschluss,

- die internationale Kennung des anrufenden und des angerufenen Endgerätes,

- Datum und Uhrzeit der ersten Aktivierung des Dienstes unter Angabe der zugrunde liegenden Zeitzone, wenn Dienste im Voraus bezahlt wurden,

- die Bezeichnungen der Funkzellen, die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt wurden,

- im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen,

- Gegenstand der Pflicht zur Speicherung bei der Erbringung öffentlich zugänglicher Internetzugangsdienste folgende Daten sind:

  - die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,

  - eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung,

  - Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse unter Angabe der zugrunde liegenden Zeitzone,

  - im Fall der mobilen Nutzung die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle,

- folgende Daten nicht gespeichert werden dürfen:

  - der Inhalt der Kommunikation,

  - Daten über aufgerufene Internetseiten,

  - Daten von Diensten der elektronischen Post,

  - Daten, die den Verbindungen zu oder von bestimmten Anschlüssen von Personen, Behörden

und Organisationen in sozialen oder kirchlichen Bereichen zugrunde liegen,

- die Dauer der Speicherung auf Vorrat für Standortdaten, d.h. die Bezeichnung der genutzten Funkzelle, vier Wochen und für die übrigen Daten zehn Wochen beträgt,

- ein wirksamer Schutz der auf Vorrat gespeicherten Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang gewährleistet ist, und

- die auf Vorrat gespeicherten Daten nur zur Verfolgung besonders schwerer Straftaten und zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes, verwendet werden dürfen, mit Ausnahme der dem Teilnehmer für eine Internetnutzung zugewiesenen Internetprotokoll-Adresse, deren Verwendung im Rahmen einer Bestandsdatenauskunft zur Verfolgung jeglicher Straftaten, zur Abwehr einer Gefahr für die öffentliche Sicherheit und Ordnung sowie zur Erfüllung der Aufgaben der Nachrichtendienste zulässig ist?

Gründe:

I

1 Die Klägerin erbringt öffentlich zugängliche Telefondienste und Internetzugangsdienste. Sie wendet sich mit der Feststellungsklage gegen die ihr durch § 113a Abs. 1 in Verbindung mit § 113b des Telekommunikationsgesetzes (TKG) in der Fassung des Gesetzes vom 10. Dezember 2015 auferlegte Pflicht, ab dem 1. Juli 2017 Telekommunikations-Verkehrsdaten ihrer Kunden auf Vorrat zu speichern.

2 Mit Urteil vom 20. April 2018 hat das Verwaltungsgericht auf die Klage festgestellt, dass die Klägerin nicht verpflichtet ist, die in § 113b Abs. 3 Nr. 1 bis 3 TKG genannten Telekommunikations-Verkehrsdaten ihrer Kunden, denen sie den lnternetzugang vermittelt, zu speichern und die in § 113b Abs. 2 Satz 1 und 2 TKG genannten Telekommunikations-Verkehrsdaten ihrer Kunden, denen sie den Zugang zu öffentlichen Telefondiensten vermittelt, zu speichern. Die Speicherpflicht verstoße gegen Unionsrecht und sei daher im Fall der Klägerin un-

anwendbar. Die grundsätzlichen Rechtsfragen zur Reichweite und zu den materiellrechtlichen Anforderungen des im vorliegenden Zusammenhang maßgeblichen Unionsrechts seien durch das Urteil des Gerichtshofs der Europäischen Union vom 21. Dezember 2016 in den verbundenen Rechtssachen C-203/15 (Tele2 Sverige) und C-698/15 (Watson u.a.) [ECLI:EU:C:2016:970] geklärt.

3 Gegen die erstinstanzliche Entscheidung hat die Beklagte die vom Verwaltungsgericht zugelassene (Sprung-)Revision eingelegt. Sie beantragt, das angefochtene Urteil des Verwaltungsgerichts abzuändern und die Klage abzuweisen.

II

4 Der Rechtsstreit ist auszusetzen, weil sein Ausgang von einer vorab einzuholenden Entscheidung des Gerichtshofs der Europäischen Union über die Auslegung der Verträge abhängt (Art. 267 des Vertrags über die Arbeitsweise der Europäischen Union <AEUV>).

5 1. Die Revision der Beklagten gegen das Feststellungsurteil des Verwaltungsgerichts ist nur dann begründet, wenn die Regelung in § 113a Abs. 1 Satz 1, § 113b TKG mit den vorrangigen Vorschriften des Unionsrechts vereinbar ist. Anderenfalls ist die Revision zurückzuweisen. Verstößt die in § 113a Abs. 1 Satz 1 i.V.m. § 113b TKG angeordnete Pflicht der Erbringer öffentlich zugänglicher Telekommunikationsdienste zur Speicherung von Telekommunikations-Verkehrsdaten auf Vorrat gegen Unionsrecht, kann die Revision auch nicht aus dem Grund Erfolg haben, dass keine Rechte der Klägerin verletzt sind (vgl. § 113 Abs. 1 Satz 1 VwGO). Dabei kommt es nicht darauf an, ob sich die Klägerin in ihrer Eigenschaft als Telekommunikationsunternehmen - und damit nicht als Teilnehmer, sondern lediglich als Übermittler der Kommunikation - auch auf die in den Art. 7 und 8 der Charta der Grundrechte der Europäischen Union (GRC) verankerten Grundrechte auf Achtung der Privatsphäre und auf Schutz personenbezogener Daten berufen kann. Denn die Speicherpflicht stellt angesichts des damit verbundenen technischen und finanziellen Aufwandes jedenfalls einen Eingriff in die durch Art. 16 GRC garantierte unternehmerische Freiheit der Klägerin dar. Ist die Regelung in § 113a Abs. 1 Satz 1, § 113b TKG mit dem Unionsrecht nicht vereinbar, darf sie - da eine unionsrechtskonforme Aus-

legung nicht in Betracht kommt - wegen des Grundsatzes des Vorrangs des Unionsrechts nicht angewendet werden (ständige Rechtsprechung des Gerichtshofs der Europäischen Union, vgl. EuGH, Urteile vom 9. März 1978 - Rs. 106/77 [ECLI:EU:C:1978:49], Simmenthal - Rn. 24, vom 3. Mai 2005 - C-387/02, C-391/02 und C-403/02 [ECLI:EU:C:2005:270], Berlusconi u.a. - Rn. 72, vom 22. Juni 2010 - C-188/10 und C-189/10 [ECLI:EU:C:2010:363], Melki und Abdeli - Rn. 43, sowie vom 18. September 2014 - C-487/12 [ECLI:EU:C:2014:2232], Vueling Airlines - Rn. 48). Die Unanwendbarkeit der Regelung hat zur Folge, dass die Grundrechtseinschränkung nicht im Sinne des Art. 52 Abs. 1 Satz 1 GRC "gesetzlich vorgesehen" ist.

6 Zwar wäre die Revision auch dann zurückzuweisen, wenn die gesetzlichen Vorschriften mit dem Unionsrecht vereinbar wären, aber gegen Grundrechte des Grundgesetzes verstießen und deshalb nichtig wären. In diesem Fall stellte sich die Entscheidung des Verwaltungsgerichts aus anderen Gründen als richtig dar (§ 144 Abs. 4 VwGO). Diese Möglichkeit kann hier jedoch außer Betracht bleiben. Denn die Feststellung der Nichtigkeit von § 113a Abs. 1 Satz 1 und § 113b TKG würde voraussetzen, dass der Senat das Verfahren aussetzt und dem Bundesverfassungsgericht die Frage der Vereinbarkeit mit den Grundrechten des Grundgesetzes gemäß Art. 100 Abs. 1 GG zur Entscheidung vorlegt. Die damit verbundene Verzögerung der Klärung der im vorliegenden Verfahren - auch aus Sicht der Beteiligten - im Vordergrund stehenden Vereinbarkeit der gesetzlichen Regelung mit dem Unionsrecht widerspräche der Prozessökonomie. Zudem kann eine nationale Verfahrensvorschrift nicht das Recht der nationalen Gerichte in Frage stellen, dem Gerichtshof ein Vorabentscheidungsersuchen vorzulegen, wenn sie Zweifel an der Auslegung des Unionsrechts haben (EuGH, Urteil vom 4. Juni 2015 - C-5/14 [ECLI:EU:C:2015:354], Kernkraftwerke Lippe-Ems - Rn. 37 mit weiteren Nachweisen).

7 2. Die Pflicht der Telekommunikationsanbieter, bestimmte Verkehrsdaten für eine beschränkte Zeit zu speichern, ist durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218 ff.) neu geregelt worden, nachdem das Bundesverfassungsgericht die §§ 113a und 113b TKG sowie § 100g Abs. 1 Satz 1 der Strafprozessordnung (StPO), soweit danach Verkehrsdaten nach § 113a TKG erhoben

werden durften, in der Fassung des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198) wegen Verstoßes gegen Art. 10 Abs. 1 GG für nichtig erklärt hatte (BVerfG, Urteil vom 2. März 2010 - 1 BvR 256, 263, 586/08 [ECLI:DE:BVerfG:2010:rs20100302.1bvr025608] - BVerfGE 125, 260). Der Neuregelung vorausgegangen war ferner das Urteil des Gerichtshofs der Europäischen Union vom 8. April 2014, mit dem die auch dem Gesetz vom 21. Dezember 2007 zugrunde liegende Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG für ungültig erklärt worden ist (EuGH, Urteil vom 8. April 2014 - C-293/12 und C-594/12 [ECLI:EU:C:2014:238], Digital Rights Ireland Ltd u.a.). Das Gesetz vom 10. Dezember 2015 soll Lücken bei der Strafverfolgung und bei der Gefahrenabwehr schließen und zugleich den sich aus den genannten Gerichtsentscheidungen ergebenden verfassungs- und europarechtlichen Vorgaben Rechnung tragen (vgl. BT-Drs. 18/5088 S. 1, 21 ff.). Es enthält u.a. die folgenden geänderten Vorschriften des Telekommunikationsgesetzes (TKG) und der Strafprozessordnung (StPO):

8 § 113a Abs. 1 Satz 1 TKG lautet:

> Die Verpflichtungen zur Speicherung von Verkehrsdaten, zur Verwendung der Daten und zur Datensicherheit nach den §§ 113b bis 113g beziehen sich auf Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer.

9 § 113b lautet:

> (1) Die in § 113a Absatz 1 Genannten sind verpflichtet, Daten wie folgt im Inland zu speichern:
> 1. Daten nach den Absätzen 2 und 3 für zehn Wochen,
> 2. Standortdaten nach Absatz 4 für vier Wochen.
>
> (2) Die Erbringer öffentlich zugänglicher Telefondienste speichern
> 1. die Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,
> 2. Datum und Uhrzeit von Beginn und Ende der Verbindung unter Angabe der zugrunde liegenden Zeitzone,
> 3. Angaben zu dem genutzten Dienst, wenn im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können,
> 4. im Fall mobiler Telefondienste ferner

a) die internationale Kennung mobiler Teilnehmer für den anrufenden und den angerufenen Anschluss,
b) die internationale Kennung des anrufenden und des angerufenen Endgerätes,
c) Datum und Uhrzeit der ersten Aktivierung des Dienstes unter Angabe der zugrunde liegenden Zeitzone, wenn Dienste im Voraus bezahlt wurden,

5. im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen.

Satz 1 gilt entsprechend

1. bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei treten an die Stelle der Angaben nach Satz 1 Nummer 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht;
2. für unbeantwortete oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe, soweit der Erbringer öffentlich zugänglicher Telefondienste die in Satz 1 genannten Verkehrsdaten für die in § 96 Absatz 1 Satz 2 genannten Zwecke speichert oder protokolliert.

(3) Die Erbringer öffentlich zugänglicher Internetzugangsdienste speichern

1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,
2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung,
3. Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse unter Angabe der zugrunde liegenden Zeitzone.

(4) Im Fall der Nutzung mobiler Telefondienste sind die Bezeichnungen der Funkzellen zu speichern, die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt wurden. Bei öffentlich zugänglichen Internetzugangsdiensten ist im Fall der mobilen Nutzung die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle zu speichern. Zusätzlich sind die Daten vorzuhalten, aus denen sich die geografische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben.

(5) Der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(6) Daten, die den in § 99 Absatz 2 genannten Verbindungen zugrunde liegen, dürfen auf Grund dieser Vorschrift nicht gespeichert werden. Dies gilt entsprechend für Telefonverbindungen, die von den in § 99 Absatz 2 genannten Stellen ausgehen. § 99 Absatz 2 Satz 2 bis 7 gilt entsprechend.

(...)

10 Bei den in § 99 Abs. 2 TKG genannten Verbindungen, auf die § 113b Abs. 6 TKG Bezug nimmt, handelt es sich um Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die

grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen. Voraussetzung für die Ausnahme ist nach § 99 Abs. 2 Satz 2 und 4 TKG, dass die Bundesnetzagentur die angerufenen Anschlüsse auf Antrag in eine Liste aufgenommen hat, nachdem die Inhaber der Anschlüsse ihre Aufgabenbestimmung durch Bescheinigung einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts nachgewiesen haben.

11 § 113c TKG lautet:

> (1) Die auf Grund des § 113b gespeicherten Daten dürfen
> 1. an eine Strafverfolgungsbehörde übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b genannten Daten zur Verfolgung besonders schwerer Straftaten erlaubt, verlangt;
> 2. an eine Gefahrenabwehrbehörde der Länder übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b genannten Daten zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes erlaubt, verlangt;
> 3. durch den Erbringer öffentlich zugänglicher Telekommunikationsdienste für eine Auskunft nach § 113 Absatz 1 Satz 3 verwendet werden.
>
> (2) Für andere Zwecke als die in Absatz 1 genannten dürfen die auf Grund des § 113b gespeicherten Daten von den nach § 113a Absatz 1 Verpflichteten nicht verwendet werden.
>
> (...)

12 Nach der in § 113c Abs. 1 Nr. 3 TKG erwähnten Bestimmung des § 113 Abs. 1 Satz 3 TKG dürfen die in eine Auskunft an eine der in § 113 Abs. 3 TKG genannten Stellen aufzunehmenden (Bestands-)Daten auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden; hierfür dürfen Verkehrsdaten auch automatisiert ausgewertet werden. Die Auskunft darf nach § 113 Abs. 2 Satz 1 TKG nur erteilt werden, soweit eine in Abs. 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 Abs. 3 Nr. 3 genannten Stellen (Verfassungsschutzbehörden des Bundes und der Länder, Militärischer Abschirmdienst und Bundesnachrichtendienst)

unter Angabe einer gesetzlichen Bestimmung verlangt, die ihr eine Erhebung der in Abs. 1 in Bezug genommenen Daten erlaubt.

13 § 113d TKG lautet:

> Der nach § 113a Absatz 1 Verpflichtete hat sicherzustellen, dass die auf Grund der Speicherpflicht nach § 113b Absatz 1 gespeicherten Daten durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung geschützt werden. Die Maßnahmen umfassen insbesondere
> 1. den Einsatz eines besonders sicheren Verschlüsselungsverfahrens,
> 2. die Speicherung in gesonderten, von den für die üblichen betrieblichen Aufgaben getrennten Speichereinrichtungen,
> 3. die Speicherung mit einem hohen Schutz vor dem Zugriff aus dem Internet auf vom Internet entkoppelten Datenverarbeitungssystemen,
> 4. die Beschränkung des Zutritts zu den Datenverarbeitungsanlagen auf Personen, die durch den Verpflichteten besonders ermächtigt sind, und
> 5. die notwendige Mitwirkung von mindestens zwei Personen beim Zugriff auf die Daten, die dazu durch den Verpflichteten besonders ermächtigt worden sind.

14 § 113e TKG lautet:

> (1) Der nach § 113a Absatz 1 Verpflichtete hat sicherzustellen, dass für Zwecke der Datenschutzkontrolle jeder Zugriff, insbesondere das Lesen, Kopieren, Ändern, Löschen und Sperren der auf Grund der Speicherpflicht nach § 113b Absatz 1 gespeicherten Daten protokolliert wird. Zu protokollieren sind
> 1. der Zeitpunkt des Zugriffs,
> 2. die auf die Daten zugreifenden Personen,
> 3. Zweck und Art des Zugriffs.
>
> (2) Für andere Zwecke als die der Datenschutzkontrolle dürfen die Protokolldaten nicht verwendet werden.
>
> (3) Der nach § 113a Absatz 1 Verpflichtete hat sicherzustellen, dass die Protokolldaten nach einem Jahr gelöscht werden.

15 Zur Gewährleistung eines besonders hohen Standards der Datensicherheit und Datenqualität erstellt die Bundesnetzagentur nach § 113f Abs. 1 TKG einen Anforderungskatalog, der fortlaufend zu überprüfen und ggf. anzupassen ist (§ 113f Abs. 2 TKG). § 113g TKG verlangt die Aufnahme spezifischer Schutzmaßnahmen in das von dem Verpflichteten vorzulegende Sicherheitskonzept.

16 § 100g StPO lautet:

> (...)

(2) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine der in Satz 2 bezeichneten besonders schweren Straftaten begangen hat oder in Fällen, in denen der Versuch strafbar ist, eine solche Straftat zu begehen versucht hat, und wiegt die Tat auch im Einzelfall besonders schwer, dürfen die nach § 113b des Telekommunikationsgesetzes gespeicherten Verkehrsdaten erhoben werden, soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

(...)

(4) Die Erhebung von Verkehrsdaten nach Absatz 2, auch in Verbindung mit Absatz 3 Satz 2, die sich gegen eine der in § 53 Absatz 1 Satz 1 Nummer 1 bis 5 genannten Personen richtet und die voraussichtlich Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte, ist unzulässig. (...)

17 § 101a Abs. 1 StPO regelt für die Erhebung von Verkehrsdaten nach § 100g StPO durch Bezugnahme auf § 100b Abs. 1 StPO (nunmehr § 100e Abs. 1 StPO in der Fassung des Gesetzes vom 17. August 2017 <BGBl. I S. 3202>) einen Richtervorbehalt sowie Anforderungen an die Gestaltung der Entscheidungsformel. Die Begründung des Beschlusses muss nach § 101a Abs. 2 StPO einzelfallbezogen die wesentlichen Erwägungen zur Erforderlichkeit und Angemessenheit der Maßnahme darlegen. § 101a Abs. 6 StPO sieht eine Pflicht zur Benachrichtigung der Beteiligten der betroffenen Telekommunikation vor.

18 3. Ob der entscheidungstragende Rechtssatz des Verwaltungsgerichts, dass die in § 113a Abs. 1 i.V.m. § 113b TKG angeordnete Speicherpflicht gegen Unionsrecht verstößt, mit revisiblem Recht vereinbar ist, hängt von der Auslegung 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. L 201 S. 37) ab und lässt sich ohne eine Vorabentscheidung des Gerichtshofs der Europäischen Union nicht abschließend klären. Der beschließende Senat geht hierbei von folgenden Erwägungen aus:

19 a) Das Verwaltungsgericht hat die Richtlinie 2002/58/EG zu Recht für anwendbar gehalten und daher als Prüfungsmaßstab für die in § 113a Abs. 1 Satz 1 i.V.m. § 113b TKG getroffene Regelung herangezogen. Dass nationale Regelun-

gen über die Vorratsspeicherung von Verkehrs- und Standortdaten sowie den Zugang der nationalen Behörden grundsätzlich in den Geltungsbereich dieser Richtlinie fallen, hat der Gerichtshof abschließend geklärt (EuGH, Urteil vom 21. Dezember 2016 - C-203/15 und C-698/15 - Rn. 65 ff., 81).

20 b) Die in § 113a Abs. 1 Satz 1 i.V.m. § 113b TKG geregelte Pflicht zur Speicherung der Telekommunikations-Verkehrsdaten beschränkt die Rechte gemäß Art. 5 Abs. 1, Art. 6 Abs. 1 und Art. 9 Abs. 1 der Richtlinie 2002/58/EG. Sie stellt einen Eingriff in die durch Art. 5 Abs. 1 Satz 1 der Richtlinie geschützte Vertraulichkeit der elektronischen Kommunikation dar und widerspricht dem Grundsatz, dass es jeder anderen Person als dem Nutzer grundsätzlich untersagt ist, ohne dessen Einwilligung mit elektronischen Kommunikationen verbundene Verkehrsdaten zu speichern. Zudem hält sie nicht die in Art. 6 der Richtlinie geregelte Vorgabe ein, dass Verkehrsdaten nur zur Gebührenabrechnung für die Dienste, zu deren Vermarktung und zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und innerhalb des dazu erforderlichen Zeitraums verarbeitet und gespeichert werden dürfen. Für den Fall, dass andere Standortdaten als Verkehrsdaten in Bezug auf die Nutzer oder Teilnehmer von öffentlichen Kommunikationsnetzen oder öffentlich zugänglichen Kommunikationsdiensten verarbeitet werden können, bestimmt Art. 9 Abs. 1 Satz 1 der Richtlinie 2002/58/EG, dass diese Daten nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden dürfen, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben. Auch von dieser Vorgabe weicht die gesetzliche Regelung ab, soweit nach § 113b Abs. 1 Nr. 2 i.V.m. Abs. 4 TKG auch die dort genannten Standortdaten zu speichern sind.

21 c) Die Beschränkung der Rechte gemäß Art. 5 Abs. 1, Art. 6 Abs. 1 und Art. 9 Abs. 1 der Richtlinie 2002/58/EG ist nur dann gerechtfertigt, wenn die Regelung des § 113a Abs. 1 Satz 1 i.V.m. § 113b TKG auf die Ermächtigungsnorm des Art. 15 Abs. 1 der Richtlinie 2002/58/EG gestützt werden kann. Danach können die Mitgliedstaaten Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Art. 5, 6, 8 Abs. 1, 2, 3 und 4 sowie Art. 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Art. 13 Abs. 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d.h. die Sicherheit des Staates), die Landesvertei-

digung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Art. 6 Abs. 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen (Art. 15 Abs. 1 Satz 2 der Richtlinie 2002/58/EG).

22 aa) Nach der erwähnten Entscheidung des Gerichtshofs vom 21. Dezember 2016 ist Art. 15 Abs. 1 der Richtlinie 2002/58/EG im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 GRC dahin auszulegen, dass er einer nationalen Regelung entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht (EuGH, Urteil vom 21. Dezember 2016 - C-203/15 und C-698/15 - Rn. 82 ff.).

23 Der Gerichtshof hat in der genannten Entscheidung, welche die auf der Richtlinie 2006/24/EG beruhenden Regelungen zur Vorratsdatenspeicherung in Schweden und im Vereinigten Königreich zum Gegenstand hat, zugleich Anforderungen für die Zulässigkeit einer auf Art. 15 Abs. 1 der Richtlinie 2002/58/EG gestützten nationalen Rechtsvorschrift aufgestellt (EuGH, Urteil vom 21. Dezember 2016 - C-203/15 und C-698/15 - Rn. 108 ff.). Danach untersagt Art. 15 Abs. 1 der Richtlinie 2002/58/EG im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 GRC einem Mitgliedstaat nicht, eine Regelung zu erlassen, die zur Bekämpfung schwerer Straftaten vorbeugend die gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern die Vorratsdatenspeicherung hinsichtlich der Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist. Um diesen Erfordernissen zu genügen, muss die betreffende nationale Regelung jedoch erstens klare und präzise Regeln über die Tragweite und die Anwendung

einer solchen Maßnahme der Vorratsdatenspeicherung vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme der Vorratsdatenspeicherung vorbeugend getroffen werden darf, um so zu gewährleisten, dass eine derartige Maßnahme auf das absolut Notwendige beschränkt wird. Zweitens können sich die materiellen Voraussetzungen, die eine nationale Regelung, die im Rahmen der Bekämpfung von Straftaten vorbeugend die Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, erfüllen muss, um zu gewährleisten, dass sie auf das absolut Notwendige beschränkt wird, zwar je nach den zur Verhütung, Ermittlung, Feststellung und Verfolgung schwerer Straftaten getroffenen Maßnahmen unterscheiden, doch muss die Vorratsspeicherung der Daten stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Diese Voraussetzungen müssen auch in der Praxis geeignet sein, den Umfang der Maßnahme und infolgedessen die betroffenen Personenkreise wirksam zu begrenzen. Bei der Begrenzung einer solchen Maßnahme im Hinblick auf die potenziell betroffenen Personenkreise und Situationen muss sich die nationale Regelung auf objektive Anknüpfungspunkte stützen, die es ermöglichen, Personenkreise zu erfassen, deren Daten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern. Eine solche Begrenzung lässt sich durch ein geografisches Kriterium gewährleisten, wenn die zuständigen nationalen Behörden aufgrund objektiver Anhaltspunkte annehmen, dass in einem oder mehreren geografischen Gebieten ein erhöhtes Risiko besteht, dass solche Taten vorbereitet oder begangen werden.

24 Nach dem Wortlaut der zitierten Ausführungen des Gerichtshofs setzt die Zulässigkeit einer nationalen Regelung der Vorratsdatenspeicherung nach Art. 15 Abs. 1 der Richtlinie 2002/58/EG mithin voraus, dass ein ausreichender Anlass besteht, dass nur diejenigen Personen erfasst werden, die einen Anhaltspunkt für einen Bezug zu schweren Straftaten bieten, dass eine Begrenzung auf dieje-

nige Region, denjenigen Zeitraum sowie diejenigen Kommunikationsmittel erfolgt, die für den Anlass relevant sind, und dass nur diejenigen Daten erfasst werden, die für die Aufklärung der bezeichneten Straftaten unerlässlich sind. Die Ansicht der Beklagten, schon der Umstand der Nutzung von Internetzugangs- oder Telefondiensten sei als hinreichender Anlass für die Speicherung zu werten, steht mit diesen Vorgaben offensichtlich nicht in Einklang. Die in den Ausführungen des Gerichtshofs zum Ausdruck kommende Annahme einer generellen Unionsrechtswidrigkeit jeder anlasslosen Vorratsdatenspeicherung wird auch nicht durch den Hinweis der Beklagten auf das - später ergangene - Gutachten des Gerichtshofs vom 26. Juli 2017 zu dem Abkommen zwischen Kanada und der Europäischen Union über die Übermittlung von Fluggastdatensätzen in Frage gestellt. Zwar hat der Gerichtshof im Rahmen der Erforderlichkeit der mit dem Abkommen verbundenen Eingriffe in die Grundrechte auf Achtung des Privatlebens (Art. 7 GRC) sowie auf Schutz personenbezogener Daten (Art. 8 GRC) hervorgehoben, dass die sog. PNR-Daten (Passenger Name Records) an Kanada unabhängig davon übermittelt werden, ob objektive Anhaltspunkte dafür vorliegen, dass von den Fluggästen eine Gefahr für die öffentliche Sicherheit in Kanada ausgeht (EuGH, Gutachten vom 26. Juli 2017 - 1/15 [ECLI:EU:C:2017:592] - Rn. 186). Um eine anlasslose Vorratsdatenspeicherung handelt es sich dabei jedoch deshalb nicht, weil die Speicherung und Übermittlung im Zusammenhang mit den Grenzkontrollen steht, denen sämtliche Fluggäste, die nach Kanada einreisen oder aus Kanada ausreisen möchten, nach den Vorschriften des geltenden kanadischen Rechts unterliegen (EuGH, Gutachten vom 26. Juli 2017 - 1/15 - Rn. 188). Mit der Ausreise der Fluggäste entfällt dieser Anlass für die Speicherung. Wie Nr. 3 Buchst. d des Tenors des Gutachtens zu entnehmen ist, setzt die weitere Speicherung nach diesem Zeitpunkt deshalb - als neuen Anlass - voraus, dass objektive Anhaltspunkte dafür vorliegen, dass von den betreffenden Fluggästen eine Gefahr im Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität ausgehen könnte.

25 bb) Ist die Rechtsprechung des Gerichtshofs so zu verstehen, dass eine anlasslose Vorratsdatenspeicherung unter keinen Umständen mit dem Unionsrecht vereinbar ist, kann die Revision der Beklagten gegen das angefochtene Urteil des Verwaltungsgerichts keinen Erfolg haben. Denn ebenso wie die schwedischen

und britischen Vorratsdatenspeicherungsregelungen, die Gegenstand des Urteils des Gerichtshofs vom 21. Dezember 2016 waren, verlangt § 113a Abs. 1 Satz 1 i.V.m. § 113b TKG weder einen - über die bloße Nutzung von Internetzugangs- oder Telefondiensten hinausgehenden - Anlass für die Speicherung noch einen Zusammenhang zwischen den gespeicherten Daten und einer Straftat bzw. einer Gefahr für die öffentliche Sicherheit. Vielmehr handelt es sich um eine Regelung, die eine anlasslose, flächendeckende und personell, zeitlich und geografisch undifferenzierte Speicherung eines Großteils aller relevanten Telekommunikations-Verkehrsdaten vorschreibt.

26 cc) Der Senat hält es jedoch ungeachtet der genannten Formulierungen in dem Urteil des Gerichtshofs vom 21. Dezember 2016 nicht für ausgeschlossen, dass die in § 113a Abs. 1 Satz 1 i.V.m. § 113b TKG geregelte Pflicht zur anlasslosen Vorratsdatenspeicherung von Telekommunikations-Verkehrsdaten auf Art. 15 Abs. 1 der Richtlinie 2002/58/EG gestützt werden kann. Diese Einschätzung beruht auf den folgenden Erwägungen:

27 (1) Zunächst ist festzustellen, dass die Regelung des § 113a Abs. 1 Satz 1 i.V.m. § 113b TKG nicht die Speicherung sämtlicher Telekommunikations-Verkehrsdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel im Sinne der auf die frühere Richtlinie 2006/24/EG und die hierauf gestützten schwedischen und britischen Regelungen bezogenen Rechtsprechung des Gerichtshofs fordert. Von der Speicherpflicht ausgenommen ist nicht nur der Inhalt der Kommunikation, sondern es dürfen auch Daten über aufgerufene Internetseiten, Daten von E-Mail-Diensten sowie Daten, die den Verbindungen zu oder von bestimmten Anschlüssen in sozialen oder kirchlichen Bereichen zugrunde liegen, nicht gespeichert werden (vgl. § 113b Abs. 5 und 6 TKG). Der Ansicht des Verwaltungsgerichts, die Unterschiede zu den schwedischen und britischen Regelungen, die Gegenstand der erwähnten Entscheidung des Gerichtshofs vom 21. Dezember 2016 waren, fielen in Anbetracht der durch den Gerichtshof dargelegten Anforderungen an die Zulässigkeit nationaler Vorschriften betreffend die Vorratsspeicherung von Telekommunikations-Verkehrsdaten nicht entscheidend ins Gewicht, vermag der beschließende Senat nicht ohne weiteres zu folgen. Denn der Gerichtshof hat zur Begründung seiner Entscheidung hervorgehoben, dass eine allgemeine und unterschiedslose

Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel sehr genaue Schlüsse auf das Privatleben derjenigen Personen zulässt, deren Daten auf Vorrat gespeichert wurden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren. Ermöglicht wird mithin die Erstellung des Profils der betroffenen Personen, das im Hinblick auf das Recht auf Achtung der Privatsphäre eine genauso sensible Information darstellt wie der Inhalt der Kommunikationen selbst (EuGH, Urteil vom 21. Dezember 2016 - C-203/15 und C-698/15 - Rn. 99). Werden insbesondere bestimmte Kommunikationsmittel oder Datenkategorien von der Speicherpflicht ausgenommen, kann dies das Risiko der Erstellung eines umfassenden Profils der betroffenen Personen zwar nicht beseitigen, aber zumindest erheblich reduzieren.

28 (2) Ein noch gewichtigerer Unterschied zwischen der Regelung des § 113a Abs. 1 Satz 1 i.V.m. § 113b TKG einerseits und der früheren Richtlinie 2006/24/EG andererseits, auf die die schwedischen und britischen Regelungen zur Vorratsdatenspeicherung gestützt waren, besteht darin, dass die Speicherungsfrist von sechs Monaten bis zu zwei Jahren (vgl. Art. 6 der Richtlinie 2006/24/EG) gemäß § 113b Abs. 1 TKG auf vier bzw. zehn Wochen deutlich verkürzt ist. Die vom Gerichtshof hervorgehobene Gefahr der Erstellung eines umfassenden Profils der betroffenen Personen ist jedoch als umso geringer anzusehen, je kürzer die Zeiträume sind, während derer die Verkehrsdaten gespeichert werden. Erst die Zusammenführung der unterschiedlichen Daten über einen längeren Zeitraum ermöglicht im Sinne der Rechtsprechung des Gerichtshofs hinreichend zuverlässige Schlüsse auf Gewohnheiten, Aufenthaltsorte, Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen und das soziale Umfeld der betroffenen Personen. Je kürzer der Speicherzeitraum ist, desto lückenhafter wird zwangsläufig das Persönlichkeitsprofil und desto geringer die Intensität des Grundrechtseingriffs.

29 (3) Weiter ist zu berücksichtigen, dass die durch das Gesetz vom 10. Dezember 2015 eingeführten Regelungen strenge Beschränkungen im Hinblick auf den

Schutz der gespeicherten Daten und den Zugang hierzu enthalten. Zum einen wird durch die Vorgaben der §§ 113d ff. TKG ein wirksamer Schutz der auf Vorrat gespeicherten Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang gewährleistet. Zum anderen dürfen die auf Vorrat gespeicherten Daten nach § 113c Abs. 1 TKG nur zur Bekämpfung schwerer Straftaten oder zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes verwendet werden. Die Erhebung der Verkehrsdaten zu Strafverfolgungszwecken setzt nach § 100g Abs. 2 StPO voraus, dass der Verdacht einer der im Gesetz abschließend bezeichneten besonders schweren Straftaten besteht, die Tat auch im Einzelfall besonders schwer wiegt, die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Die Erhebung oder Verwendung von Verkehrsdaten der in § 53 Abs. 1 Satz 1 Nr. 1 bis 5 StPO genannten Berufsgeheimnisträger, zu denen z.B. Rechtsanwälte, Ärzte oder Journalisten gehören, ist nach § 100g Abs. 4 StPO unzulässig. § 101a Abs. 1 StPO regelt zudem einen Richtervorbehalt für die Erhebung von Verkehrsdaten nach § 100g StPO sowie besondere Anforderungen an die Gestaltung der Entscheidungsformel. Die Begründung des Beschlusses muss nach § 101a Abs. 2 StPO einzelfallbezogen die wesentlichen Erwägungen zur Erforderlichkeit und Angemessenheit der Maßnahme darlegen. § 101a Abs. 6 StPO sieht eine Pflicht zur Benachrichtigung der Beteiligten der betroffenen Telekommunikation vor.

30 Diese einschränkenden Zugangsregelungen gelten zwar nicht in Bezug auf die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse; denn diese darf nach § 113c Abs. 1 Nr. 3 TKG auch im Rahmen einer Bestandsdatenauskunft zur Verfolgung jeglicher Straftaten, zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung sowie generell zur Erfüllung der Aufgaben der Nachrichtendienste verwendet werden. Allerdings ist davon auszugehen, dass die Auskunft, welcher Anschlussinhaber unter einer bereits bekannten Internetprotokoll-Adresse im Internet angemeldet war, nicht die Erstellung von Persönlichkeits- und Bewegungsprofilen zulässt (vgl. BVerfG, Urteil vom 2. März 2010 - 1 BvR 256, 263, 586/08 - BVerfGE 125, 260 <340 ff.>). Selbst wenn der Klägerin folgend unterstellt wird, dass zunehmend technische

Verfahren zum Einsatz kommen, bei denen eine Internetprotokoll-Adresse nicht mehr eindeutig auf einen bestimmten Telekommunikationsanschluss, sondern lediglich auf eine größere Gruppe von Anschlüssen zurückgeführt werden kann und sich die Bestandsdatenauskunft daher zu einer Maßnahme mit beträchtlicher Streubreite entwickelt hat, bleibt die Eingriffsintensität einer solchen Bestandsdatenauskunft weiterhin deutlich hinter derjenigen zurück, die bei der Abfrage und Verwendung der Telekommunikations-Verkehrsdaten selbst besteht.

31 (4) Für die Annahme, dass die in § 113a Abs. 1 Satz 1 i.V.m. § 113b TKG geregelte Pflicht zur anlasslosen Vorratsdatenspeicherung von Telekommunikations-Verkehrsdaten angesichts der dargelegten Beschränkungen auf Art. 15 Abs. 1 der Richtlinie 2002/58/EG gestützt werden kann, spricht im Rahmen einer Gesamtbetrachtung neben den einschränkenden Regelungen zu den erfassten Kommunikationsmitteln, Datenkategorien und Speicherzeiträumen sowie den strengen Vorgaben zur Datensicherheit und zum Datenabruf ferner auch der Umstand, dass der nationale Gesetzgeber damit den Handlungspflichten nachgekommen ist, die sich für die Mitgliedstaaten aus dem durch Art. 6 GRC garantierten Recht auf Sicherheit ergeben.

32 In seinem Urteil vom 8. April 2014 betreffend die Gültigkeit der Richtlinie 2006/24/EG hat der Gerichtshof Art. 6 GRC ausdrücklich erwähnt und in diesem Zusammenhang unter Bezugnahme auf seine Rechtsprechung darauf hingewiesen, dass die Bekämpfung des internationalen Terrorismus zur Wahrung des Weltfriedens und der internationalen Sicherheit eine dem Gemeinwohl dienende Zielsetzung der Union darstellt und dass das Gleiche für die Bekämpfung schwerer Kriminalität zur Gewährleistung der öffentlichen Sicherheit gilt (EuGH, Urteil vom 8. April 2014 - C-293/12 und C-594/12 - Rn. 42). Weiter hat der Gerichtshof allerdings ausgeführt, dass zwar die Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, von größter Bedeutung für die Gewährleistung der öffentlichen Sicherheit sei und dass ihre Wirksamkeit in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen könne. Eine solche dem Gemeinwohl dienende Zielsetzung könne jedoch, so grundlegend sie auch sein möge, für sich genommen die Erforderlichkeit einer Speicherungsmaßnahme - wie sie die Richtlinie

2006/24/EG vorsah - für die Kriminalitätsbekämpfung nicht rechtfertigen (EuGH, Urteile vom 8. April 2014 - C-293/12 und C-594/12 - Rn. 51, 60 und vom 21. Dezember 2016 - C-203/15 und C-698/15 - Rn. 102 f.).

33 Der beschließende Senat hat im Hinblick auf die sich aus Art. 6 GRC ergebende Handlungspflicht der Mitgliedstaaten Zweifel, ob diese Aussage des Gerichtshofs so verstanden werden muss, dass eine anlasslose Vorratsdatenspeicherung nicht nur in der konkreten Ausgestaltung, die sie in der Richtlinie 2006/24/EG und den hierauf gestützten schwedischen und britischen Regelungen gefunden hat, sondern generell nicht auf Art. 15 Abs. 1 der Richtlinie 2002/58/EG gestützt werden kann. Denn das Grundkonzept der Vorratsdatenspeicherung ist mit der einschränkungslos formulierten Forderung des Gerichtshofs, bei den zu speichernden Daten nach Personen, Zeiträumen und geografischen Gebieten zu differenzieren, kaum in Einklang zu bringen (vgl. in diesem Sinne auch bereits die Schlussanträge des Generalanwalts Saugmandsgaard Øe vom 19. Juli 2016 in den verb. Rs. C-203/15 und C-698/15 [ECLI:EU:C:2016:572] - Rn. 213 ff.). Eine solche Differenzierung kann naturgemäß nur zukunftsgerichtet erfolgen, soweit bereits Erkenntnisse vorliegen. Zweck der Vorratsdatenspeicherung ist jedoch gerade die Rekonstruktion zurückliegender Vorgänge auf der Grundlage solcher Telekommunikations-Verkehrsdaten, die zum Zeitpunkt des Anlasses bereits vorhanden sind. Dieser Zweck dürfte nicht erreicht werden können, wenn etwa danach differenziert werden muss, welchen Personen - z.B. aufgrund der Beobachtung des Kommunikationsverhaltens in sozialen Netzwerken - schwere Straftaten zugetraut werden, oder in geografischer Hinsicht lediglich solche Funkzellen erfasst werden dürfen, in denen Einrichtungen liegen, bei denen aufgrund konkreter Erkenntnisse eine erhöhte Anschlagsgefahr oder ein hohes Schadenspotenzial gegeben ist. So ist eine geografische Einschränkung gerade bei Straftaten, die mittels elektronischer Telekommunikationsdienste begangen werden, kaum geeignet.

34 Gegen die Annahme, eine anlasslose Speicherung von Verkehrsdaten sei per se mit der Grundrechtecharta unvereinbar, spricht aus Sicht des Senats zudem das Erfordernis, ein Gleichgewicht herzustellen zwischen einerseits der Pflicht der Mitgliedstaaten, die Sicherheit der sich in ihrem Hoheitsgebiet aufhaltenden Personen zu gewährleisten, und andererseits der Wahrung der in den Art. 7

und 8 GRC verankerten Grundrechte auf Achtung der Privatsphäre und auf Schutz personenbezogener Daten (vgl. Schlussanträge des Generalanwalts Saugmandsgaard Øe vom 19. Juli 2016 in den verb. Rs. C-203/15 und C-698/15 - Rn. 5, 163). Der Senat vermag der Rechtsprechung des Gerichtshofs daher nicht eindeutig zu entnehmen, dass die nationalen Gesetzgeber keine Möglichkeit mehr haben sollen, aufgrund einer Gesamtabwägung eine - ggf. durch strenge Zugangsregelungen ergänzte - anlasslose Vorratsdatenspeicherung einzuführen, um dem spezifischen Gefahrenpotenzial, das sich mit den neuen Telekommunikationsmitteln verbindet (vgl. hierzu BVerfG, Urteil vom 2. März 2010 - 1 BvR 256, 263, 586/08 - BVerfGE 125, 260 <322 f.>), Rechnung zu tragen.

35 (5) Wäre die erwähnte Rechtsprechung des Gerichtshofs so zu verstehen, dass eine anlasslose Vorratsdatenspeicherung generell nicht auf Art. 15 Abs. 1 der Richtlinie 2002/58/EG gestützt werden kann und es auf die konkreten Regelungen zu den erfassten Kommunikationsmitteln, zu den Kategorien der zu speichernden Daten, zur Speicherdauer, zu den Voraussetzungen für den Zugang zu den gespeicherten Daten und zum Schutz vor Missbrauchsrisiken folglich nicht ankommt, wäre zudem der Handlungsspielraum der nationalen Gesetzgeber in einem Bereich der Strafverfolgung und der öffentlichen Sicherheit, der nach Art. 4 Abs. 2 Satz 3 EUV jedenfalls grundsätzlich weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt, erheblich eingeschränkt. In diesem Bereich haben die nationalen Gesetzgeber die Aufgabe, - wie ausgeführt - ein Gleichgewicht zwischen den Grundrechten auf Achtung der Privatsphäre und auf Schutz personenbezogener Daten einerseits und der Pflicht der Mitgliedstaaten, die Sicherheit der Bevölkerung zu gewährleisten, andererseits herzustellen. Dass den demokratisch legitimierten Gesetzgebern der Mitgliedstaaten die Möglichkeit, im Bereich der Strafverfolgung und der öffentlichen Sicherheit auf der Grundlage des Art. 15 Abs. 1 der Richtlinie 2002/58/EG eine für erforderlich gehaltene Ermittlungstechnik wie die anlasslose Vorratsdatenspeicherung einzuführen, unabhängig von der Art der Gefahrenlage und der konkreten Ausgestaltung der Regelungen vollständig verwehrt sein soll, vermag der beschließende Senat der Entscheidung des Gerichtshofs vom 21. Dezember 2016 nicht hinreichend sicher zu entnehmen.

36 (6) Ob die Ausführungen des Gerichtshofs in dem Urteil vom 21. Dezember 2016 als an die Mitgliedstaaten gerichtetes Verbot zu verstehen sind, die Einführung einer Pflicht zur anlasslosen Vorratsdatenspeicherung von Telekommunikations-Verkehrsdaten auf Art. 15 Abs. 1 der Richtlinie 2002/58/EG zu stützen, erscheint dem Senat auch vor dem Hintergrund der neueren Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte nicht abschließend geklärt. Denn der Europäische Gerichtshof für Menschenrechte hat zuletzt in einem Urteil vom 19. Juni 2018 entschieden, dass die schwedischen Rechtsvorschriften über die Massenüberwachung des grenzüberschreitenden Datenverkehrs mit Art. 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) in Einklang stehen. Angesichts der Bedrohungen, denen Staaten zur Zeit ausgesetzt seien einschließlich der Geißel des globalen Terrorismus und anderer schwerer Verbrechen, wie Drogenhandel, Menschenhandel, sexuelle Ausbeutung von Kindern und Internetkriminalität, sowie wegen des technischen Fortschritts, der es Terroristen und Kriminellen erleichtere, ihre Entdeckung im Internet zu vermeiden, und der Unvorhersehbarkeit der Übertragungswege elektronischer Daten, falle die Entscheidung, ein System der Massenüberwachung einzurichten, um bisher unbekannte Bedrohungen der nationalen Sicherheit zu erkennen, weiterhin in den Ermessensspielraum des Staates (EGMR, Urteil vom 19. Juni 2018 - Nr. 35252/08 [ECLI:CE:ECHR:2018:0619JUD003525208], Centrum för Rättvisa/Schweden - Rn. 112). Soweit der Europäische Gerichtshof für Menschenrechte auf die Unvorhersehbarkeit der Übertragungswege elektronischer Daten sowie den technischen Fortschritt verweist, der es Terroristen und Kriminellen erleichtere, ihre Entdeckung im Internet zu vermeiden, betont er stärker als der Gerichtshof der Europäischen Union das spezifische Gefahrenpotenzial, das sich mit den neuen Telekommunikationsmitteln verbindet.

37 Die anders akzentuierte Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte kann nach Ansicht des beschließenden Senats hier nicht außer Betracht bleiben. Denn zum einen wird in Erwägungsgrund 11 der Richtlinie 2002/58/EG hervorgehoben, dass Maßnahmen nach Art. 15 Abs. 1 der Richtlinie im Einklang mit der EMRK in ihrer Auslegung durch die Urteile des Europäischen Gerichtshofs für Menschenrechte zu erfolgen haben. Zum anderen hat der Gerichtshof der Europäischen Union wiederholt darauf hingewiesen, dass

mit Art. 52 Abs. 3 der Charta der Grundrechte der Europäischen Union, soweit diese Rechte enthält, die den durch die EMRK garantierten Rechten entsprechen, die notwendige Kohärenz zwischen den in der Charta verankerten Rechten und den entsprechenden durch die EMRK garantierten Rechten geschaffen werden soll, ohne dass dadurch die Eigenständigkeit des Unionsrechts und des Gerichtshofs der Europäischen Union berührt wird (vgl. EuGH, Urteil vom 29. Juli 2019 - C-469/17 [ECLI:EU:C:2019:623], Funke Medien NRW GmbH - Rn. 73 und die dort angeführte Rechtsprechung).

38 (7) Schließlich geht aus verschiedenen beim Gerichtshof bereits anhängigen Vorabentscheidungsersuchen aus anderen Mitgliedstaaten hervor, dass die vorlegenden Gerichte insbesondere im Hinblick auf Art. 6 GRC und Art. 4 EUV Zweifel daran haben, ob die Ausführungen des Gerichtshofs im Urteil vom 21. Dezember 2016 als generelles Verbot einer anlasslosen Vorratsdatenspeicherung zu verstehen sind, das weder im Hinblick auf die Erheblichkeit der zu bekämpfenden Gefahren für die öffentliche Sicherheit noch im Rahmen einer "Kompensation" durch restriktive Zugriffsregelungen und hohe Sicherheitsanforderungen überwunden werden kann. Der beschließende Senat nimmt insoweit Bezug auf das Vorabentscheidungsersuchen des Investigatory Powers Tribunal - London (Vereinigtes Königreich), das als Rechtssache C-623/17 beim Gerichtshof anhängig ist (ABl. C 22 vom 22. Januar 2018, S. 29), die beiden Vorabentscheidungsersuchen des Conseil d'État (Frankreich), die als Rechtssachen C-511/18 und C-512/18 anhängig sind (ABl. C 392 vom 29. Oktober 2018, S. 7 f.) sowie das Vorabentscheidungsersuchen des Belgischen Verfassungsgerichtshofs, das als Rechtssache C-520/18 anhängig ist (ABl. C 408 vom 12. November 2018, S. 39).

Prof. Dr. Kraft Dr. Heitz Dr. Möller

Hahn Steiner