Unterabteilung Europa
Fachbereich Europa

Deutscher Bundestag

Ausarbeitung

Europarechtliche Spielräume zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten in den Mitgliedstaaten der Europäischen Union

PE 6 – 3000 – 53/15

Europarechtliche Spielräume zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten in den Mitgliedstaaten der Europäischen Union

Aktenzeichen: PE 6 – 3000 – 53/15
Abschluss der Arbeit: 04.06.2015
Fachbereich: PE 6: Fachbereich Europa

Inhaltsverzeichnis

1. Die zu untersuchende Fragestellung

Der Fachbereich Europa wird um die Klärung der Frage ersucht,

> *„ob der Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für den Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (Bearbeitungsstand: 15.05.2015 14:51 Uhr) […] die Vorgaben […] des EuGH zur Aufhebung der Vorratsdatenspeicherungs-Richtlinie (EuGH (Große Kammer), Urteil vom 8. April 2014, C-293/12 und C-594/12) richtig umsetzt."*

Da inzwischen der Gesetzentwurf der Bundesregierung *Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*[1] (RE) vorliegt, soll nachfolgend dieser nach Maßgabe vorstehender Fragestellung überprüft werden.

Die Frage, ob vorstehender RE die Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung (BVerfG, Urteil vom 2. März 2010, 1 BvR 256/08) richtig umsetzt, bearbeitet der Fachbereich Verfassung und Verwaltung (WD 3).

Der Gerichtshof der Europäischen Union (EuGH) hatte mit Urteil vom 8. April 2014[2] die *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*[3] (RL 2006/24) wegen Verstoßes gegen die in Art. 7 und Art. 8 der Charta der Grundrechte der Europäischen Union (GRCh) verankerten Grundrechte für ungültig erklärt. Bevor der Frage nachgegangen werden kann, ob der in Frage stehende RE der Entscheidung des EuGH vom 8. April 2014 hinreichend Rechnung trägt (3), bedarf es zunächst der Klärung, ob die dieser zugrundeliegende GRCh als Prüfungsmaßstab für dieses nationale Regelungsvorhaben Anwendung findet (2).

2. Zur Anwendbarkeit der Charta der Grundrechte der Europäischen Union

Der Anwendungsbereich der GRCh ist nur dann eröffnet, wenn Organe oder Einrichtungen der EU oder die Mitgliedstaaten EU-Recht, also Primär- und Sekundärrecht der EU, durchführen (Art. 51 Abs. 1 GRCh). Was darunter genau zu verstehen ist, ist umstritten.[4] Der Grundrechtekon-

---

1 Abrufbar unter: http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Gesetze/RegE_Hoechstspeicherfrist.pdf;jsessionid=AE9EF942BC29D6A7E0C36809A6AAA396.1_cid334?__blob=publicationFile.

2 EuGH, verb. Rs. C-293/12 u. C-594/12, Urt. v. 8.04.2014, online abrufbar unter: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=135421.

3 ABl L 105/54, online abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32006L0024&qid=1430730858712&from=DE.

4 Zum Meinungsstand vgl. Borowsky, in: Meyer (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Aufl. 2014, Art. 51 Rn. 24 ff.; Burgkardt, Grundrechtlicher Datenschutz zwischen Grundgesetz und Europarecht, 2013, S. 40 ff.

vent hatte sich gegen die Formulierung „*bei Anwendung des Gemeinschaftsrechts*" entschieden und stattdessen den Ausdruck „*bei der Durchführung des Rechts der Union*" bevorzugt.[5] Mit dieser Formulierung sollte die vom EuGH vorgenommene bisherige weite Anwendung der Unionsgrundrechte auf alle unionsrelevanten Sachverhalte, insbesondere auf Bereiche, die die Grundfreiheiten betreffen, eingeschränkt werden.[6]

Die Ausgangslage, dass der EuGH die Richtlinie 2006/24 für ungültig erklärt hatte, die Mitgliedstaaten mithin unionsrechtlich nicht mehr verpflichtet sind, eine Vorratsdatenspeicherung (VDS) in ihren nationalen Rechtsordnungen einzuführen, diese über die Einführung einer VDS auf nationaler Ebene, soweit EU-Recht dem nicht entgegensteht, demgemäß eigenständig entscheiden dürfen, könnte zunächst dagegen sprechen, dass sie in diesem Falle Unionsrecht durchführen. Die Einführung einer verpflichtenden VDS in einem Mitgliedstaat erfolgte allerdings nicht losgelöst vom Unionsrecht.

Nach ständiger Rechtsprechung des EuGH ist von einer gemäß Art. 51 GRCh die Anwendung der GRCh auslösenden „*Durchführung des Unionsrechts*" auszugehen, wenn die in Frage stehende Maßnahme in den Anwendungsbereich des Unionsrechts fällt.[7]

Während nach früherer europäischer Rechtsprechung die Unionsgrundrechte nur dann und nur soweit als Prüfungsmaßstab für nationales Recht zur Anwendung kamen, wenn dieses sich explizit aus europäischem Recht ableiten lässt[8], ließ der EuGH in seiner Entscheidung in der Rechtssache *Åkerberg Fransson* es für die Anwendbarkeit der GRCh genügen, dass eine mitgliedstaatliche Rechtsnorm in den Anwendungsbereich des Unionsrechts fällt.[9] Eine Bindung des nationalen Rechts an die Unionsgrundrechte erforderte nunmehr keine vollständige Determinierung des mitgliedstaatlichen Rechts durch Unionsrecht bzw. Ableitbarkeit hieraus.[10] Hierfür hinreichend ist nach der Åkerberg Fransson-Entscheidung bereits das Bestehen von dem Unionsrecht zu entnehmenden allgemein sachbezogenen Handlungspflichten,[11] da das nationale Recht so zu deren Erfüllung einen Beitrag leiste.[12]

---

5 Siehe hierzu die Zusammenfassung der Diskussion im Konvent bei Borowsky, in: Meyer (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Aufl. 2014, Art. 51, Rn. 2 ff.

6 Borowsky, in: Meyer (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Aufl. 2014, Art. 51, Rn. 24.

7 EuGH, R. C-617/10 (Åkerberg Fransson), Urt. v. 23.02.2013 ; Rs. C-418/11 (Texdata).

8 EuGH, Rs. C-2/92 Rn. 16; C-313/99.

9 EuGH, R. C-617/10 (Åkerberg Fransson), Urt. v. 23.02.2013 Rn. 17 ff.

10 EuGH, R. C-617/10 (Åkerberg Fransson), Urt. v. 23.02.2013 Rn. 29.

11 Vgl. Haratsch/Koenig/Pechtsein, Europarecht, 9. Aufl. 2014, Rn. 679.

12 Grimm, Der Datenschutz vor einer Neuorientierung, JZ 2013, S. 585 (590 ff.); Kubicki, Der Fall Åkerberg Fransson, DeLuxe 4/2013; Thym, Die Reichweite der EU-Grundrechte-Charta – Zu viel Grundrechtsschutz?, NVwZ 2013, S. 889. Zur grundsätzlichen Problematik der Geltung der GRCh bei nationalen Gestaltungsspielräumen bei der Durchführung von Unionsrecht vgl. Hufeld/Rathke, Der Grundrechtsschutz nach Lissabon im Wechselspiel zwischen der Charata der Grundrechte der Europäischen Union, Europäischer Menschenrechtskonvention und den nationalen Verfassungen, EuR Beiheft 3 2013, S. 7 (20 ff.).

> *„Da folglich die durch die Charta garantierten Grundrechte zu beachten sind, wenn eine nationale Rechtsvorschrift in den Geltungsbereich des Unionsrechts fällt, sind keine Fallgestaltungen denkbar, die vom Unionsrecht erfasst würden, ohne dass diese Grundrechte anwendbar wären. Die Anwendbarkeit des Unionsrechts umfasst die Anwendbarkeit der durch die Charta garantierten Grundrechte."*[13] *„Die Tatsache, dass die nationalen Rechtsvorschriften [....] nicht zur Umsetzung der Richtlinie 2006/112 erlassen wurden, vermag dieses Ergebnis nicht in Frage zu stellen."*[14]

In einer späteren Entscheidung präzisierte der EuGH die Anwendbarkeit der GRCh auf nationale Maßnahmen dahin, dass das zur Anwendung der GRCh führende Merkmal der „Durchführung" (Art. 51 Abs. 1 GRCh) *„einen hinreichenden Zusammenhang von einem gewissen Grad verlangt, der darüber hinausgeht, dass die fraglichen Sachbereiche benachbart sind oder der eine von ihnen mittelbare Auswirkungen auf den anderen hat."*[15] Durchführung nach Art. 51 Abs. 1 GRCh setze einen *„hinreichenden Zusammenhang von einem gewissen Grad"* zwischen Unionsrecht und der in Frage stehenden mitgliedstaatlichen Maßnahme voraus.[16]

Die Einführung einer VDS im nationalen Recht der Mitgliedstaaten ist mithin an der GRCh zu messen, soweit dieses Vorhaben *„in den Geltungsbereich des Unionsrechts fällt"* bzw. einen *„hinreichenden Zusammenhang von einem gewissen Grad"* zum Unionsrecht aufweist. Dieser Zusammenhang zwischen einer mitgliedstaatlichen Regelung einer VDS und europäischem Recht könnte aufgrund des geltenden sekundärrechtlichen Datenschutzrechts insb. für den Bereich der elektronischen Kommunikation bestehen.

Die VDS fällt in den Anwendungsbereich der Datenschutzrichtlinie für elektronische Kommunikation[17] (RL 2002/58), da es sich hierbei i.S.d. Art. 1 Abs. RL 2002/58 um eine Regelung *„in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und –diensten"* handelt. Die Richtlinie 2002/58 *„gilt für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft"* (Art. 3 RL 2002/58).

---

13 EuGH, R. C-617/10 (Åkerberg Fransson), Urt. v. 23.02.2013 Rn. 21.

14 EuGH, R. C-617/10 (Åkerberg Fransson), Urt. v. 23.02.2013 Rn. 28.

15 EuGH, Rs. C-206/13 (Siragusa), Urt. v. 6.03.2014, Rn. 24.

16 EuGH, Rs. C-206/13 (Siragusa), Urt. v. 6.03.2014, Rn. 25; dazu vertiefend Terhechte, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 7. Aufl. 2015, Art. 51 GRCh, Rn. 11 ff.

17 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 201/37, online abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32002L0058&qid=1430738429270&from=DE.

Den Vorschriften in Art. 5, 6 und 9 RL 2002/58 lassen sich zudem das (grds.) Verbot anlassloser Speicherung – insb. auch von „Verkehrsdaten“[18] und „Standortdaten“[19] – entnehmen.

Art. 5 Abs. 1 RL 2002/58 definiert das Speichern von Verkehrsdaten als Eingriff in die Vertraulichkeit der Kommunikation.

> *„(1) Die Mitgliedstaaten stellen die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind. Diese Bestimmung steht — unbeschadet des Grundsatzes der Vertraulichkeit — der für die Weiterleitung einer Nachricht erforderlichen technischen Speicherung nicht entgegen.“*

Art. 6 Abs. 1 RL 2002/58 normiert Vorgaben für die Löschung bzw. Anonymisierung von Verkehrsdaten.

> *„(1) Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes verarbeitet und gespeichert werden, sind unbeschadet der Absätze 2, 3 und 5 des vorliegenden Artikels und des Artikels 15 Absatz 1 zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden.“*

Art. 9 Abs.1 RL 2002/58 normiert die Verwendung von anderen Standortdaten als Verkehrsdaten.

> *„(1) Können andere Standortdaten als Verkehrsdaten in Bezug auf die Nutzer oder Teilnehmer von öffentlichen Kommunikationsnetzen oder öffentlich zugänglichen Kommunikationsdiensten verarbeitet werden, so dürfen diese Daten nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben. Der Diensteanbieter muss den Nutzern oder Teilnehmern vor Einholung ihrer Einwilligung mitteilen, welche Arten anderer Standortdaten als Verkehrsdaten verarbeitet werden, für welche Zwecke und wie lange das geschieht, und ob die Daten zum Zwecke der Bereitstellung des Dienstes mit Zusatznutzen an einen Dritten weitergegeben werden. Die Nutzer oder Teilnehmer können ihre Einwilligung zur Verarbeitung anderer Standortdaten als Verkehrsdaten jederzeit zurückziehen.“*

---

[18] Verkehrsdaten werden in Art. 2 Buchst. b) RL 2002/58 als „*Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden*“ definiert.

[19] Standortdaten werden in Art. 2 Buchst. c) RL 2002/58 als Daten, „*die in einem elektronischen Kommunikationsnetz verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben*“ definiert.

Art. 15 Abs. 1 RL 2002/58 normiert eine Öffnungsklausel der Mitgliedstaaten, diese Rechte zu beschränken.

> *„(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, 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 Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen."*

Nationale Regelungen zur VDS können das sekundärrechtlich bestehende Verbot anlassloser Speicherung von Daten im Bereich der elektronischen Kommunikation nur umgehen, wenn die Mitgliedstaaten dabei von der durch die Öffnungsklausel des Art. 15 Abs. 1 RL 2002/58 eröffneten Option zur Beschränkung der Verbürgungen der Vertraulichkeit öffentlich zugänglicher Kommunikationsdienste dieser Richtlinie Gebrauch machen. Es dürfte daher viel dafür sprechen, dass Mitgliedstaaten bei Einführung nationaler Regelungen zur VDS (auch) Unionsrecht i.S.d. Art. 51 Abs. 1 GRCh ausführen, wenn sie die von der Öffnungsklausel des Art. 15 Abs. 1 Satz 2 RL 2002/58 dafür eröffneten Spielräume nutzen.[20]

Eine argumentative Stütze hierfür bietet auch der Erwägungsgrund 2 der Richtlinie 2002/58, der dieser Richtlinie den Status einer sekundärrechtlichen Konkretisierung der in Art. 7 und 8 GRCh verbürgten Grundrechte verleiht.

> *„Ziel dieser Richtlinie ist die Achtung der Grundrechte; sie steht insbesondere im Einklang mit den durch die Charta der Grundrechte der Europäischen Union anerkannten Grundsätzen. Insbesondere soll mit dieser Richtlinie gewährleistet werden, dass die in den Artikeln 7 und 8 jener Charta niedergelegten Rechte uneingeschränkt geachtet werden."*

Das in Frage stehende Vorhaben zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten unterliegt mithin dem Anwendungsbereich und den Vorgaben der RL 2002/58 und dürfte daher Unionsrecht nach Art. 51 Abs. 1 GRCh durchführen. Diese Auffassung vertreten auch ein niederländisches Gericht, die Rechtbank Den Haag, und der Verfassungsgerichtshof Wien. Die Rechtsbank Den Haag überprüfte das niederländische Gesetz zur Vorratsspeicherung von Telekommunikations-Verkehrs- und Standortdaten (auch) anhand der in Art. 7 und 8 GRCh verbürgten Grundrechte, nachdem das Gericht die Anwendbarkeit der GRCh hierfür nach Art. 51

---

[20] Bäcker, Das Vorratsdatenurteil des EuGH: Ein Meilenstein des europäischen Grundrechtsschutzes, in: JA 2014, S. 1263 (1272); Priebe, Reform der Vorratsdatenspeicherung – strenge Maßstäbe des EuGH, EuZW 2014, S. 456 (458).

GRCh bejaht hatte.[21] In ähnlicher Weise überprüfte der Verfassungsgerichtshof Wien die für Österreich eingeführte VDS am Maßstab der Art. 7 und 8 GRCh, nachdem auch dieses Gericht zuvor die Anwendbarkeit der GRCh festgestellt hatte.[22]

Nach Art. 15 Abs. 1 Satz 3 RL 2002/58 müssen zudem alle „*in diesem Absatz genannten Maßnahmen [...] den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.*" Diese Norm kann zwar als sekundärrechtliche Regelung nicht den Anwendungsbereich des Art. 51 Abs. 1 GRCh erweitern, lässt sich allerdings als durch die Richtlinie 2002/58 statuierte Verpflichtung deuten, dass die Mitgliedstaaten die Unionsgrundrechte unabhängig davon beachten, ob die GRCh gemäß Art. 51 Abs. 1 GRCh Anwendung findet.[23]

Es dürfte mithin viel dafür sprechen, dass eine im mitgliedstaatlichen Recht vorgesehene Speicherpflicht von Verkehrsdaten auf Vorrat dem Anwendungsbereich des EU-Rechts unterliegt.[24]

Da nach ständiger Rechtsprechung des EuGH Unionsrecht Vorrang vor einzelstaatlichem Recht hat[25] und wegen dieses Anwendungsvorrangs des EU-Rechts damit in Widerspruch stehendes mitgliedstaatliches Recht unanwendbar ist,[26] müssen auch mitgliedstaatliche Regelungen, die zur Bevorratung von Daten verpflichten, den Vorgaben der Entscheidung des EuGH vom 8. April 2014 entsprechen.[27]

---

21 Vgl. Rechtbank Den Haag, C/09/480009 / KG ZA 14/1575, Urt. v. 11.03.2015, online abrufbar unter: http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2015:2498.

22 VerfGH Wien, Entscheidung vom 27.06.2014 – G 47/2012, Anm. 2.2.7., online abrufbar unter: https://beck-online.beck.de/?vpath=bibdata/ents/beckrs/2014/cont/beckrs.2014.81762.htm&pos=18&hlwords=.

23 Bäcker, Das Vorratsdatenurteil des EuGH: Ein Meilenstein des europäischen Grundrechtsschutzes, in: JA 2014, S. 1263 (1272); Spiecker gen. Döhmann, Anmerkung EuGH, verb. Rs. C-293/12 u. C-594/12, Urt. v. 8.04.2014, JZ 2014, S. 1109 (1112).

24 So auch das Rechtsgutachten des Juristischen Dienstes des Europäischen Parlaments vom 22.12.2014, LIBE – Questions relating to the judgment of the court of Justice of 8 April 2014 in Joined Cases C-293/12 und C-594/12, Digital Rights Ireland and Seitlinger and others – Directive 2006/24/EC on data retention – Consequences of the judgment, S. 15 ff.; online abrufbar unter: https://netzpolitik.org/wp-upload/2014-12-22_SJ-0890-14_Legal_opinion.pdf ; Boehm/Cole, Data Retention after the Judgement of the Court of Justice of the European Union, Gutachten vom 30.06.2014, S. 43 ff.; Hötzendorfer/Tschohl, Die Vorratsdatenspeicherung als Herausforderung der EU-Grundrechtscharta, in: Schweighofer u.a. (Hrsg.): Transparenz 2014, S. 597 (605), Kunnert, EuGH zur Vorratsdatenspeicherung: Außer Spesen nichts gewesen?, in: EuGH (Fußn. 2) Rn. 82); i.E. ist dies offenbar auch die Auffassung der Bundesregierung, wenn sie es für erforderlich hält, dass eine „*nationale Gesetzgebung, die Telekommunikationsanbieter zur Speicherung von Verkehrsdaten verpflichtet, [...] sowohl den Vorgaben des Bundesverfassungsgerichts als auch den Vorgaben des Gerichtshofs der Europäischen Union entsprechen*" muss (BT-Drs. 18/4764, S. 3).

25 EuGH, Rs. 106/77, Urt. v. 9.3.1978, Rn. 17/18 ff, ; verb. Rs. C 10 – 22/97, Urt. v. 22.10.1998, Rn. 20 ff.

26 Std. Rechtsprechung; vgl. EuGH, Rs. 6/64 (Costa/ENEL), Urt. v. 15.07.1964.

27 Rechtsgutachten des Juristischen Dienstes des Europäischen Parlaments vom 22.12.2014 (Fußn. 25, S. 17): „*...Member States must ensure that the national measures dealing with data retention in the electronic communications sector are compatible with the Charter, and in particular with Articles 7, 8 and 52(1) thereof, as interpreted by the court of Justice in the DRI judgment.*"

3. Entspricht der Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten den Vorgaben der Entscheidung des EuGH vom 8. April 2014?

3.1. Der Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten im Überblick

Dem Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Einführung einer Speicherung und Höchstspeicherfrist für Verkehrsdaten" (RE) lassen sich im Wesentlichen folgende Regelungen zur Ausgestaltung der VDS entnehmen:

- Die Erbringer öffentlich zugänglicher Telefondienste sollen verpflichtet sein, bei der Telekommunikation anfallende Verkehrsdaten (Rufnummern oder eine andere Kennung der beteiligten Anschlüsse, Zeitpunkt und Dauer des Anrufs, Angaben zu dem genutzten Dienst, wenn im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden, für den Bereich der Mobiltelefonie die internationalen Kennungen der beteiligten mobilen Teilnehmer und der beteiligten Endgeräte, im Bereich der Internettelefonie die Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses sowie die zugewiesenen Benutzerkennungen[28]), bei Mobilfunk auch die Standortdaten[29] zu speichern. Die Erbringer öffentlich zugänglicher Internetzugangsdienste sollen zur Speicherung von IP-Adressen einschließlich Zeitpunkt und Dauer der Vergabe einer IP-Adresse verpflichtet sein.[30] Nicht (auf Grundlage des RE) gespeichert werden dürfen der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post.[31] Die Speicherung der Daten muss im Inland erfolgen[32]; diese sind vor unbefugter Kenntnisnahme und Verwendung zu schützen.[33]

- Die Speicherfrist beträgt für Standortdaten vier Wochen, im Übrigen zehn Wochen.[34] Die Daten sind nach Ablauf der Speicherfrist (irreversibel) zu löschen.[35] Bewegungs- und Persönlichkeitsprofile sollen auf Grundlage des RE nicht erstellt werden können, was durch

---

28 RE § 113b Abs. 2 Nr. 1. bis 4. TKG-E.

29 RE § 113b Abs. 4 TKG-E. Zur näheren Bestimmung der zu speichernden Standortdaten vgl. die Begründung des RE S. 45 zu Absatz 4.

30 RE § 113b Abs. 3 TKG-E.

31 RE § 113b Abs. 5 TKG-E.

32 RE § 113b Abs. 1 TKG-E.

33 RE §§ 113d, 113g TKG-E.

34 RE § 113b Abs. 1 TKG-E.

35 RE § 113b Abs. 8 TKG-E.

die Präzisierung der Anforderungen an die Funkzellenabfrage sichergestellt werden soll.[36] Deshalb sollen im Grundsatz auch nur einzelne Standortdaten abgerufen werden dürfen.[37]

- Die Strafverfolgungsbehörden dürfen die gespeicherten Daten zur Verfolgung besonders schwerer Straftaten abrufen, die als solche im RE enumerativ abschließend definiert werden.[38] Den Gefahrenabwehrbehörden der Länder dürfen Vorratsdaten übermittelt werden, wenn die jeweiligen Polizeigesetze einen Abruf der Verkehrsdaten für den Fall zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit oder für den Bestand des Bundes oder eines Landes erlauben.[39]

- Verkehrsdaten zu nach § 53 StPO zeugnisverweigerungsberechtigten Personen dürfen nicht abgerufen werden und unterliegen im Übrigen einem Verwertungsverbot.[40] Verkehrsdaten, die sich auf Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen beziehen, 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, nicht aber die Verkehrsdaten der nach § 53 StPO zeugnisverweigerungsberechtigten Personen, sind (grundsätzlich) von der Speicherpflicht ausgenommen.[41]

- Der Abruf von Verkehrsdaten soll neben weiteren Voraussetzungen nur zur Verfolgung von in einem Katalog als solche festgelegten schweren Straftaten zulässig sein[42] und unterliegt einem Richtervorbehalt ohne eine Eilkompetenz der Staatsanwaltschaft.[43]

3.2. Vorgaben der Entscheidung des EuGH vom 8. April 2014 zur VDS

Der EuGH wertet die Verpflichtung zur VDS und die Verwendung der dabei erhobenen Daten als einen Eingriff sowohl in das Recht auf Achtung des Privatlebens (Art. 7 GRCh) als auch in das Recht auf Schutz personenbezogener Daten (Art. 8 GRCh) „von großem Ausmaß und als besonders schwerwiegend".[44] Der „*Umstand, dass die Vorratsdatenspeicherung der Daten und ihre*

---

36 RE § 100g Abs. 3 StPO-E; Begründung GE S. 36 f.

37 RE § 101a Abs. 2 StPO-E; Begründung GE S. 39: „*Grundsätzlich sollen nur einzelne Standortdaten abgerufen werden, um keine überflüssigen Bewegungsprofile zu erstellen.*"

38 RE § 100g Abs. 2 StPO-E.

39 RE § 113c Abs. 1 Buchst. 2. TKG-E.

40 RE § 100g Abs. 4 StPO-E.

41 RE § 113b Abs. 6; Begründung S. 25, 46.

42 RE § 100g Abs. 1, 2 StPO-E.

43 RE § 101a Abs. 1 Satz 2 StPO-E, Begründung S. 26, 38.

44 EuGH (Fußn. 2) Rn. 37.

spätere Nutzung vorgenommen werden, ohne dass der Teilnehmer oder der registrierte Benutzer darüber informiert wird", sei geeignet, „*bei den Betroffenen [...] das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist.*"[45] Da die von der Richtlinie 2006/24 vorgeschriebene Speicherung von Daten auf Vorrat nicht die Kenntnisnahme des Inhalts elektronischer Kommunikation gestatte, würde diese – trotz der Schwere dieses Eingriffs – nicht den Wesensgehalt der Grundrechte aus Art. 7 und 8 GRCh antasten.[46] Eine VDS kann mithin zur Verfolgung von dem Gemeinwohl dienenden Zielen Eingriffe in vorstehende Grundrechte rechtfertigen. Das materielle Regelungsziel der in der Richtlinie 2006/24 vorgesehenen VDS, „*zur Bekämpfung schwerer Kriminalität und somit letztlich zur öffentlichen Sicherheit beizutragen*", wertete der Gerichtshof „*als eine dem Gemeinwohl dienende Zielsetzung*"[47], das grds. Eingriffe in das Recht auf Achtung des Privatlebens und des Rechts auf Schutz personenbezogener Daten rechtfertigen könnte. Eingriffe in diese Grundrechte müssten sich aber auf das „absolut Notwendige" beschränken. Dies ließe sich nach Ansicht des Gerichtshofs bei der Richtlinie 2006/24 aufgrund folgender Ausgestaltungsbesonderheiten der VDS darin nicht feststellen.

- Die Speicherpflicht erfasse alle elektronischen Kommunikationsmittel und alle ihre Nutzer. Diese führe „*daher zu einem Eingriff in die Grundrechte fast der gesamten europäischen Bevölkerung*,[48] *ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen.*"[49] Es werde weder vorausgesetzt, dass das Verhalten der von der Speicherung ihrer Daten auf Vorrat betroffenen Personen auch nur im „*mittelbaren und entfernten Zusammenhang mit schweren Straftaten stehen könnte(n)*"[50], noch müssten die erhobenen Daten in einem Zusammenhang stehen mit einer Bedrohung der öffentlichen Sicherheit.[51]

- Die Richtlinie 2006/24 sehe keine Ausnahmeregelung für Personen vor, „*deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen.*"[52]

- Anders als noch der Generalanwalt[53] legt der EuGH keine exakte Höchstgrenze für die VDS fest, weist aber darauf hin, dass die Richtlinie 2006/24 keine Unterscheidung zwischen Datenkategorien „*nach Maßgabe ihres etwaigen Nutzens für das verfolgte Ziel oder*

---

45 EuGH (Fußn. 2) Rn. 37.

46 EuGH (Fußn. 2) Rn. 39.

47 EuGH (Fußn. 2) Rn. 41.

48 EuGH (Fußn. 2) Rn. 56.

49 EuGH (Fußn. 2) Rn. 57.

50 EuGH (Fußn. 2) Rn. 58.

51 EuGH (Fußn. 2) Rn. 59.

52 EuGH (Fußn. 2) Rn. 58.

53 Schlussanträge des Generalanwalts Pedro Cruz Villalón vom 12. Dezember 2013, Rn. 152.

anhand der betroffenen Personen" vornehme.[54] Es gebe keine objektiven Kriterien, die sicherstellten, dass die Speicherfrist von den Mitgliedstaaten so festgelegt werde, dass sie sich innerhalb des von der Richtlinie festgelegten Spielraums zwischen mindestens sechs Monaten und höchsten 24 Monaten auf das absolut Notwendige beschränke.[55]

- Der Gerichtshof moniert das Fehlen von materiell- und verfahrensrechtlichen Regelungen für den Zugang der zuständigen nationalen Behörden zu den Daten und deren Nutzung in der Richtlinie 2006/24. Dort sei nicht ausdrücklich geregelt, *„dass der Zugang zu diesen Daten und deren spätere Nutzung strikt auf Zwecke der Verhütung und Feststellung genau abgegrenzter schwerer Straftaten oder der sie betreffenden Strafverfolgung zu beschränken sind."*[56] Die Richtlinie normiere *„kein objektives Kriterium […], das es erlaubt, die Zahl der Personen, die zum Zugang zu den auf Vorrat gespeicherten Daten und zu deren späterer Nutzung befugt sind, auf das angesichts des verfolgten Ziels absolut Notwendige zu beschränken. Vor allem unterliegt der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung den Zugang zu den Daten und ihre Nutzung auf das zur Erreichung des verfolgten Ziels absolut Notwendige beschränken soll und im Anschluss an einen mit Gründen versehenen Antrag der genannten Behörden im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten ergeht. Auch sieht die Richtlinie keine präzise Verpflichtung der Mitgliedstaaten vor, solche Beschränkungen zu schaffen."*[57]

- Die Richtlinie sehe keinen hinreichenden Schutz der erhobenen Vorratsdaten vor unberechtigtem Zugang und unberechtigter Nutzung vor.[58] Art. 7 Richtlinie 2006/24 gewährleiste kein hohes Schutz- und Sicherheitsniveau, erlaube es den zur Speicherung verpflichteten Unternehmen, bei der Bestimmung ihres praktizierten Sicherheitsstandards auch wirtschaftliche Erwägungen zu treffen.[59] Die Richtlinie gewährleiste keine unwiderrufliche Vernichtung der Daten nach Ablauf ihrer Speicherfrist.[60] Sie gewährleiste auch nicht die Überwachung der Einhaltung der Erfordernisse des Datenschutzes und der Datensicherung, wie dies Art. 8 Abs. 3 GRCh ausdrücklich fordert, durch eine unabhängige Stelle, weil die Richtlinie 2006/24 nicht vorschreibe, dass die Vorratsdaten auf Unionsgebiet gespeichert werden.[61]

---

54 EuGH (Fußn. 2) Rn. 63.

55 EuGH (Fußn. 2) Rn. 64.

56 EuGH (Fußn. 2) Rn. 61.

57 EuGH (Fußn. 2) Rn. 62.

58 EuGH (Fußn. 2) Rn. 66.

59 EuGH (Fußn. 2) Rn. 67.

60 EuGH (Fußn. 2) Rn. 67.

61 EuGH (Fußn. 2) Rn. 68.

Das Ergebnis, dass die VDS in ihrer Ausgestaltung durch die Richtlinie 2006/24 als ein unverhältnismäßiger Eingriff in die durch Art. 7 und 8 GRCH gewährleisteten Grundrechte anzusehen ist und diese Richtlinie daher ungültig sei, stützt der Gerichtshof auf eine Gesamtbetrachtung vorstehender Erwägungen.[62]

3.3. Entspricht das Vorhaben der Bundesregierung zur „Einführung einer Speicherung und Höchstspeicherfrist für Verkehrsdaten" den Vorgaben der Entscheidung des EuGH vom 8. April 2014 zur VDS?

Zunächst bedarf es des Hinweises, dass sich der Entscheidung des EuGH vom 8. April 2014 nur Gründe dafür entnehmen lassen, weshalb aus Sicht des Gerichtshofs die konkrete Ausgestaltung der VDS durch die Richtlinie 2006/24 mit den Gewährleistungen der Art. 7 und 8 GRCh unvereinbar ist. Ein Verstoß gegen diese Grundrechte folgerte dieser aus einer Gesamtbetrachtung aller seiner Erwägungen. Offen muss daher bleiben, ob auch einzelne der in der Entscheidung getroffenen Feststellungen zur Eingriffsqualität und –intensität der Regelungen der Richtlinie 2006/24 die Annahme des Vorliegens eines unverhältnismäßiges Eingriffs in die durch Art. 7 und 8 GRCh geschützten Grundrechte rechtfertigen, da die Entscheidungsgründe dazu nichts ausführen. Naturgemäß könnte eine andere gesetzliche Regelung der VDS als die der Entscheidung des EuGH verfahrensgegenständlich zugrundliegende Richtlinie 2006/24 auch weitere, von dieser Entscheidung nicht behandelte Anknüpfungspunkte für die Frage der Grundrechtskonformität bieten. Eine gutachtliche Klärung der Frage, ob der RE den in der Entscheidung des EuGH vom 8. April 2014 dargelegten Anforderungen an eine grundrechtskonforme VDS entspricht, lässt vor diesem Hintergrund mithin keine zwingenden Schlussfolgerungen zu, ob die im RE entworfene VDS letztlich mit der GRCh vereinbar ist.

Hinreichende Beschränkung der von der VDS erfassten Kommunikationsmittel und des davon betroffenen Personenkreises

Der EuGH wertete es als kritisch, dass die in der Richtlinie 2006/24 vorgesehene Speicherpflicht alle elektronischen Kommunikationsmittel und alle ihre Nutzer umfasst ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen.

Der RE sieht – soweit ersichtlich – im Grundsatz keine Beschränkung der auf Vorrat zu speichernden Daten vor. Verkehrsdaten, die sich auf Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen beziehen, 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, sollen allerdings (grundsätzlich) von der Speicherpflicht ausgenommen sein.[63] Gespeichert

---

62 EuGH (Fußn. 2) Rn. 69.

63 RE § 113b Abs. 6; Begründung S. 25, 46.

werden müssen im Telekommunikationsgesetz (TKG) genau definierte Verkehrsdaten, bei Mobilfunk auch Standortdaten sowie IP-Adressen einschließlich Zeitpunkt und Dauer der Vergabe einer IP-Adresse. Eine Speicherung von Dateninhalten war bereits in der Richtlinie 2006/24 nicht vorgesehen.

Die im RE ausgestaltete VDS sieht – mit Ausnahme der zuvor genannten Personengruppen – keine Beschränkungen hinsichtlich des von einer Speicherung betroffenen Personenkreises vor und setzt für die Speicherung auch nicht das Vorliegen einer schweren Straftat voraus. Eine entsprechende Einschränkung soll erst beim Abruf der Daten vorgenommen werden.

Der Datenabruf soll nur bei schwersten Straftaten zulässig sein, die in § 100g Abs. 2 Satz 2 StPO-E abschließend legaldefiniert sind. Die nach § 113b TKG-E gespeicherten Verkehrsdaten dürfen nach § 100g Abs. 2 StPO-E nur erhoben werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Katalogtat nach § 100g Abs. 2 StPO-E begangen oder in Fällen, in denen der Versuch strafbar ist, eine solche Straftat zu begehen versucht hat, soweit weitere Erfordernisse hinsichtlich der Schwere der Tat im Einzelfall und hinsichtlich der Erforderlichkeit der Erhebung von Vorratsdaten zur Erforschung des Sachverhalts erfüllt sind.

Der RE trägt daher dem vom Gerichtshof in seiner Entscheidung vom 8. April 2014 gegen die Richtlinie 2006/24 erhobenen Einwand, keine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten hinsichtlich der Speicherung von Vorratsdaten vorzusehen, nicht hinreichend Rechnung.

Der RE sieht Beschränkungen dieser Art nicht für die VDS selbst, sondern erst für den Datenabruf vor, indem dieser dafür den begründeten Verdacht, dass „jemand" an einer als schwere Straftat definierten Katalogtat beteiligt ist, voraussetzen will.[64] Der EuGH fordert Einschränkungen hinsichtlich des Sachgrundes für die VDS und des davon betroffenen Personenkreises aber bereits für die Speicherung von Vorratsdaten und nicht erst für den Zugang hierzu. Da die Speicherpflicht nach Ansicht des Gerichtshofs eine Bedrohung der öffentlichen Sicherheit voraussetzt[65], sind die Entscheidungsgründe offenbar so zu verstehen, dass eine VDS von der Kenntnis vom Vorliegen eines Verdachts einer Bedrohung der öffentlichen Sicherheit abhängen soll, was, wenn man diese Anforderung für sich betrachtet, für eine anlasslose VDS kaum einen Spielraum ließe.[66] Bereits die Speicherung von Daten ist im europäischen Datenschutzrecht ein der Recht-

---

64 Einzelfallbezogen sieht der RE in § 100g Abs. 1 StPO-E – außerhalb der VDS – auch die Erhebung von Verkehrsdaten für Vorfeldtaten und für mittels Telekommunikation verübte Straftaten vor.

65 EuGH (Fußn. 2) Rn. 59.

66 So die Schlussfolgerungen aus der Entscheidung des EuGH vom 8. April 2004 in den Urteilsanmerkungen von Kunnert, EuGH zur Vorratsdatenspeicherung: Außer Spesen nichts gewesen?, in: DuD 2014, S. 774 (777); Leutheuser-Schnarrenberger, Die Beerdigung 1. Klasse der anlasslosen Vorratsdatenspeicherung in Europa, DuD 2014, S. 589 (592); Otto/Seitlinger, MMR 2014, S. 9 (23); Moos, Die Entwicklung des Datenschutzrechts im Jahr 2014, K&R 2015, S. 158 (164); Petri, Anmerkung zu einer Entscheidung des EuGH (Urteil vom 08.04.2014 – C-293/12, C-594/12), ZD 2014, 296 - Zur Ungültigkeit der EU-Richtlinie über die Vorratsdatenspeicherung, ZD 2014, S. 300 (301) und Roßnagel, Neue Maßstäbe für den Datenschutz in Europa, MMR 2014, S. 372 (375); so i.E. auch die Stellungnahme der Europäischen Akademie für Informationsfreiheit und Datenschutz vom 25.05.2015 zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 15. Mai 2015.

fertigung bedürftiger Eingriff.[67] Nach Art. 8 Abs. 1 Satz 2 GRCh dürfen personenbezogene Daten *„nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden."* Der in Art. 2 Buchst. b) Richtlinie 95/46/EG[68] näher definierte Begriff *Verarbeitung* ist als Oberbegriff aller datenbezogenen Prozesse zu verstehen.[69] Er umfasst *„jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten."*

Für die VDS bedeutsam dürfte auch die vom Bundesgerichtshof (BGH) dem EuGH vorgelegten Fragen sein, ob eine IP-Adresse, die ein Diensteanbieter im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für den Diensteanbieter schon dann ein personenbezogenes Datum darstellt, wenn lediglich ein Dritter das nötige Zusatzwissen besitzt, um einen Personenbezug herzustellen, und ob die Speicherung von IP-Adressen durch Diensteanbieter, soweit dies über den Vorgang der Nutzung der bereitgestellten Dienste hinausgeht, mit der Richtlinie 95/46/EG vereinbar ist.[70] Aus der Qualität der IP-Adressen als personenbezogene Daten folgte die datenschutzrechtlich gebotene Zweckbindung auch von IP-Adressen. Die Zweckbindung für Vorratsdaten insgesamt dürfte der EuGH in seiner Entscheidung vom 8. April 2014 grundrechtlich für geboten halten, wenn er bei der Richtlinie 2006/24 zum Fehlen des Konnexes zwischen dem Ziel der Bekämpfung schwerer Kriminalität und des von der VDS betroffenen Personenkreises kritisch anmerkt:

> *„Zum anderen soll die Richtlinie zwar zur Bekämpfung schwerer Kriminalität beitragen, verlangt aber keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit; insbesondere beschränkt sie*

Skeptisch auch Bäcker, Das Vorratsdatenurteil des EuGH: Ein Meilenstein des europäischen Grundrechtsschutzes, in: JA 2014, S. 1263 (1273); Kühling, Der Fall der Vorratsdatenspeicherrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht, NVwZ 2014, S. 681 (683); Spiecker gen. Döhmann, Anmerkung zum Urteil des Europäischen Gerichtshofs vom 8.4.2014 zur Vorratsdatenspeicherung, JZ 2014, S. 1109 (1112) und Wolff, Anmerkung zum Urteil des Europäischen Gerichtshofs vom 8.4.2014 zur Vorratsdatenspeicherung, DÖV 2014, S. 608 (610); a.A. Gercke, Die Entwicklung des Internetstrafrechts 2013/2014, ZUM 2014, S. 641 (646); Orantek, Der lange Weg der Vorratsdatenspeicherung, NJ 2014, S. 326 (331); Priebe, Reform der Vorratsdatenspeicherung – strenge Maßstäbe des EuGH, EuZW 2014, S. 456 (459); Westphal, Kommentar zur Entscheidung vom 8.4.2014, KR 2014 S. 410 (411 f.).

67 Vgl. Augsburg, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 7. Aufl. 2015, Art. 8 GRCh, Rn. 11.

68 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 280/50.

69 Dazu und zu der Konturierung des Schutzbereichs von Art. 8 GRCh durch Sekundärrecht vgl. Augsburg, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 7. Aufl. 2015, Art. 8 GRCh, Rn. 11.

70 BGH, 28.10.2014, VI ZR 135/13.

die Vorratsspeicherung weder auf die Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets und/oder eines bestimmten Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten."[71]

Daran müsste sich auch der RE messen lassen, der nicht hinreichend sicherstellen dürfte, dass die Vorratsdaten nur solcher Personen gespeichert und abgerufen werden können, die der Beteiligung an einer nach dem RE einschlägigen Straftat verdächtig sind oder damit in sonstiger Weise in Verbindung gebracht werden können, da IP-Adressen Anschlussinhabern zugeordnet sind, die mit den tatsächlichen Nutzern elektronischer Kommunikationsmittel nicht identisch sein müssen. Der Deutsche Anwaltsverein weist in seiner Stellungnahme vom 15. Mai 2015[72] in diesem Zusammenhang darauf hin, dass auf Grundlage des RE nicht zwangsläufig die Daten derer erfasst würden, die kommunizieren, sondern die Daten der Personen, die die technische Infrastruktur vorhalten. Damit dürfte aber einer Anforderung des EuGH nicht umfassend entsprochen sein, dass nur Daten auf Vorrat zu solchen Personen gespeichert werden dürfen, die Anlass zur Strafverfolgung gegeben haben. Gegen die Richtlinie 2006/24 wandte der Gerichtshof ein, dass diese in umfassender Weise alle Personen betreffe, *„die elektronische Kommunikationsdienste nutzen, ohne dass sich jedoch die Personen, deren Daten auf Vorrat gespeichert werden, auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte."*[73]

Aus der Entscheidung des EuGH vom 8. April 2014 ließe sich allerdings nicht auf ein europarechtliches (generelles) Verbot der anlasslosen VDS schließen, weil der Gerichtshof die Ungültigkeit der Richtlinie 2006/24 aus der Gesamtheit der von ihm getroffenen Erwägungen folgerte, die Entscheidungsgründe aber nicht zu erkennen geben, ob einzelne darin getroffene Feststellungen zu der konkreten Ausgestaltung der VDS in dieser Richtlinie bereits eine Qualität und Intensität des Grundrechtseingriffs erreichen, dass auch mit diesen bereits die Grenzen überschritten werden, die, folgt man den Prüfungsmaßstab des EuGH, zur Wahrung des Grundsatzes der Verhältnismäßigkeit mit Blick auf Art. 7, 8 und 52 GRCh einzuhalten sind.[74]

---

71 EuGH (Fußn. 2) Rn. 59.

72 Deutscher Anwaltsverein, Stellungnahme des Deutschen Anwaltsvereins durch die Ausschüsse Gefahrenabwehrrecht, Informationsrecht und Strafrechts zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten S. 19, online abrufbar unter: http://www.google.de/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&ved=0CCgQFjAB&url=http%3A%2F%2Fanwaltverein.de%2Fde%2Fnewsroom%2Fsn-25-15-referentenentwurf-des-bundesministeriums-der-justiz-und-fuer-verbraucherschutz-fuer-ein-gesetz-zur-einfuehrung-einer-sp%3Ffile%3Dfiles%252Fanwaltverein.de%252Fdownloads%252Fnewsroom%252Fstellungnahmen%252F2015%252FDAV-SN-25-15.pdf&ei=9FlkVavtD8KLsgGmxYLICg&usg=AFQjCNE-hfiGPmjYHVh1HhDnI28lYguhcw&bvm=bv.93990622,d.bGQ.

73 EuGH (Fußn. 2) Rn. 58.

74 Dazu nochmals EuGH (Fußn. 2) Rn. 69.

Festzustellen ist aber, dass der RE nicht (im vollen Umfang) den Vorgaben des EuGH hinsichtlich der Beschränkung des von der VDS betroffenen Personenkreises entsprechen dürfte.

Zu dem Erfordernis einer Ausnahmeregelung zur Wahrung des Berufsgeheimnisses

Dem vom EuGH gegen die Richtlinie 2006/24 erhobenen Einwand, keine Ausnahmeregelung für Personen vorzusehen, *„deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen"*[75], will der RE damit Rechnung tragen, dass Berufsgeheimnisträger beim Abruf von Daten durch Verwendungs- und Verwertungsverbote geschützt werden sollen. Verkehrsdaten, die sich auf Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen beziehen, 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, nicht jedoch die nach § 53 StPO zeugnisverweigerungsberechtigten Personen[76], sollen *grundsätzlich* bereits von der Speicherpflicht ausgenommen sein.[77]

Bereits die Speicherung von Vorratsdaten ist ein legitimationsbedürftiger Grundrechtseingriff. Der EuGH monierte in seiner Entscheidung vom 8. April 2014, dass die Richtlinie 2006/24 keinerlei Ausnahme vorsehe, *„so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen."*[78] Da der RE die Speicherung auch der Daten von Berufsgeheimnisträgern vorsieht, trägt er dieser Vorgabe, die eine Ausnahmeregelung bereits von der Speicherung von Verkehrsdaten für Personen fordert, *„deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen"*, nicht Rechnung.[79]

Angemessene Dauer der VDS

Ohne eine exakte Höchstgrenze für die VDS anzugeben, hebt der EuGH kritisch hervor, dass die Richtlinie 2006/24 hinsichtlich der Speicherfrist keine Unterscheidung zwischen Datenkategorien *„nach Maßgabe ihres etwaigen Nutzens für das verfolgte Ziel oder anhand der betroffenen Personen"* vornehme.[80] Es gebe keine objektiven Kriterien, die sicherstellten, dass die Speicher-

---

75 EuGH (Fußn. 2) Rn. 58.

76 Der Deutsche Anwaltsverein fordert in seiner Stellungnahme zum RE vom 15.05.2015 S. 13 f. (Fußn. 72) den Verzicht auf die VDS zum Schutze der Berufsgeheimnisträger bzw. die Gewährleistung des Schutzes von Berufsgeheimnissen durch einen Datenabgleich.

77 RE § 113b Abs. 6; Begründung S. 25, 46

78 EuGH (Fußn. 2) Rn. 58.

79 Kunnert (Fußn. 24) S. 777 ist der Ansicht, dass der vom EuGH bereits bei der Speicherung geforderte Schutz von Trägern gesetzlich geschützter Berufsgeheimnisse bei einer VDS nicht einzuhalten ist.

80 EuGH (Fußn. 2) Rn. 63.

frist von den Mitgliedstaaten so festgelegt werde, dass sie sich innerhalb des von der Richtlinie festgelegten Spielraums zwischen mindestens sechs Monaten und höchstens 24 Monaten auf das absolut Notwendige beschränke.[81]

Dem will der RE damit entsprechen, dass die Speicherfrist für Standortdaten vier Wochen[82], im Übrigen zehn Wochen betragen soll[83] und die Daten nach Ablauf der Speicherfrist zu löschen sind.[84] Sie sehen mithin erheblich kürzere Speicherfristen vor als noch die Richtlinie 2006/24 und differenziert hinsichtlich der Speicherfrist zwischen Standortdaten und (sonstigen) Verkehrsdaten. Der EuGH fordert hinsichtlich der Speicherfrist von Vorratsdaten eine differenzierte Regelung, wobei die von ihm genannten Differenzierungskriterien alternativ, nicht aber kumulativ erfüllt sein müssen. Eine Unvereinbarkeit des RE hinsichtlich der grundrechtlich gebotenen Speicherfrist zu den Vorgaben des EuGH ist insoweit nicht auszumachen. Mangels entsprechender Vorgabe durch den Gerichtshof muss offen bleiben, ob mit der im RE vorgesehenen Sanktionsandrohung bei Verletzung der Speicherfristen und der damit verbundenen Verpflichtungen den grundrechtlichen Anforderungen an den Datenschutz Genüge getan ist oder ob es danach erforderlich ist, dass bei Überschreitung der Höchstspeicherfrist Daten nicht mehr abgerufen werden können und ein Erhebungs- und Verwertungsverbot bestehen muss.[85]

Beschränkung des Zugangs zu Vorratsdaten und deren Nutzung zu Strafverfolgungszwecken

Der EuGH wertet es als ein die Schwere des Eingriffs in die durch Art. 7 und 8 GRCh geschützten Grundrechte kennzeichnendes Moment, dass die Richtlinie 2006/24 nicht sicherstelle, dass der Zugang zu Vorratsdaten und deren spätere Nutzung *„strikt auf Zwecke der Verhütung und Feststellung genau abgegrenzter schwerer Straftaten oder der sie betreffenden Strafverfolgung zu beschränken sind."*[86]

Der RE sieht vor, dass die Strafverfolgungsbehörden die gespeicherten Daten insb. zur Verfolgung gesetzlich definierter schwerer (Katalog-) Straftaten abrufen dürfen. Den Gefahrenabwehrbehörden der Länder sollen gespeicherte Verkehrsdaten 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 wird"* (§ 113c Abs. 1 Buchst. 2 TKG-E).

---

81 EuGH (Fußn. 2) Rn. 64.

82 RE § 113b Abs. 1 Satz 1 Nr. 2. TKG-E.

83 RE § 113b Abs. 1 Satz 1 Nr. 1 TKG-E.

84 RE § 113b Abs. 8 TKG-E.

85 Darauf verweist der Deutsche Anwaltsverein in seiner Stellungnahme (Fußn. 72) S. 25.

86 EuGH (Fußn. 2) Rn. 61.

Diese Zweckbindung erhobener Vorratsdaten genügt nach hiesiger Einschätzung der Forderung des EuGH, Vorratsdaten nur zur Verhütung und Feststellung genau definierter Straftaten den zuständigen Stellen zugänglich zu machen. Der Gerichtshof deutet auch die Option an, Vorratsdaten mit Blick auf eine Bedrohung der öffentlichen Sicherheit zu speichern.[87]

Beschränkung der Zahl zugangsberechtigter Personen auf das absolut Notwendige

Der EuGH erachtet die Normierung eines objektiven Kriteriums für erforderlich, mit dessen Hilfe die Zahl der Personen, die zum Zugang zu den auf Vorrat gespeicherten Daten und zu deren späteren Nutzung befugt sind, auf das angesichts des verfolgten Ziels absolut Notwendige beschränkt bleibt.

Dieser Anforderung dürfte der RE durch die Festlegung der Zwecke genügen, für die die gespeicherten Verkehrsdaten (ausschließlich) genutzt werden dürfen. Damit dürfte sichergestellt sein, dass nur Amtspersonen, die im Rahmen der im RE definierten Strafverfolgung und Gefahrenabwehr zuständig sind, auch zugangsberechtigt sind.

Kontrolle des Zugangs von Vorratsdaten durch ein Gericht oder eine unabhängige Behörde

Der EuGH fordert, dass der Datenzugang zu den zuständigen nationalen Behörden erst nach Entscheidung eines Gerichts oder einer unabhängigen Verwaltungsstelle erfolgen dürfe. Diese sollen den Datenzugang und die Nutzung dieser Daten auf das zur Erreichung des verfolgten Ziels absolut Notwendige beschränken und über den Antrag der zugangsberechtigten Behörden unter Angabe von Gründen bescheiden.

Der RE sieht einen Richtervorhalt für die Erhebung von Verkehrsdaten durch die Strafverfolgungsbehörden vor (§ 101a Abs. 1 Satz 2 StPO-E i.V.m. § 100b StPO). Während die Eilkompetenz der Staatsanwaltschaft für die personenbezogene Anordnung der Erhebung von Verkehrsdaten nach § 100g Abs. 1, 3 StPO-E besteht, soll die Möglichkeit der Eilanordnung durch die Staatsanwaltschaft für die nach § 100g Abs. 2 StPO-E verpflichtend zu speichernden Verkehrsdaten ausgeschlossen sein.[88]

Da der RE die Eilkompetenz der Staatsanwaltschaft in den Fällen der anlasslosen Speicherung von Verkehrsdaten nach § 100g Abs. 2 StPO-E generell ausschließt, entspricht dieser Regelungsvorschlag insoweit der Vorgabe des EuGH, den Zugang zu Vorratsdaten der Kontrolle durch ein Gericht oder eine unabhängige Behörde zu unterstellen.

---

87 EuGH (Fußn. 2) Rn. 59.

88 Der RE will dies in der Weise sicherstellen, dass für die Fälle des § 100g Abs. 2 StPO-E die durch § 100b Abs. 1 Satz 2 und 3 StPO eröffnete Anordnungskompetenz der Staatsanwaltschaft bei Gefahr in Verzug gem. § 101a Abs. 1 Satz 2 StPO-E ausgeschlossen wird. Vgl. dazu auch die Begründung des RE S. 38 f.

Mit dem im RE normierten Erfordernis, Verkehrsdaten nach § 100g Abs. 2 StPO-E nur auf Grundlage eines durch bestimmte Tatsachen gestützten Tatverdachts der Begehung einer schweren Straftat zu erheben, *„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“* dürfte dem von EuGH aufgestellten ultima-ratio-Erfordernis der Vorratsdatenspeicherung Genüge getan sein.

Der RE sieht auch, wie vom EuGH gefordert, vor, dass das Gericht über den Antrag der zugangsberechtigten Behörden unter Angabe von Gründen bescheidet. In § 101a Abs. 2 StPO-E ist vorgesehen, dass das Gericht bei der Anordnung oder Verlängerung einer Speicherung von Verkehrsdaten *„in der Begründung einzelfallbezogen insbesondere die wesentlichen Erwägungen zur Erforderlichkeit und Angemessenheit der Maßnahme, auch hinsichtlich des Umfangs der zu erhebenden Daten und des Zeitraums, für den sie erhoben werden sollen, darzulegen“ hat.*

Schutz der erhobenen Vorratsdaten vor unberechtigtem Zugang und unberechtigter Nutzung und Verpflichtung, diese nach Ablauf der Speicherfrist unwiderruflich zu löschen

Der EuGH macht einen unverhältnismäßigen Eingriff in die Grundrechte aus Art. 7 und 8 GRCh auch daran fest, dass die Richtlinie 2006/24

- keinen hinreichenden Schutz der erhobenen Vorratsdaten vor unberechtigten Zugang und unberechtigter Nutzung vorsehe[89],
- mit ihrer Regelung in Art. 7 kein hohes Schutz- und Sicherheitsniveau gewährleiste und sie es den zu Speicherung verpflichteten Unternehmen erlaube, bei der Bestimmung ihres praktizierten Sicherheitsstandards auch wirtschaftliche Erwägungen zu treffen,[90]
- keine unwiderrufliche Vernichtung der Daten nach Ablauf ihrer Speicherfrist gewährleiste[91] und
- auch nicht die Überwachung der Einhaltung der Erfordernisse des Datenschutzes und der Datensicherung, wie Art. 8 Abs. 3 GRCh dies ausdrücklich fordert, durch eine unabhängige Stelle gewährleiste.

Der RE normiert in § 113d TKG-E eine Reihe von Vorgaben zur Gewährleistung der Sicherheit der nach § 113b TKG-E gespeicherten Daten.

---

89 EuGH (Fußn. 2) Rn. 66.

90 EuGH (Fußn. 2) Rn. 67.

91 EuGH (Fußn. 2) Rn. 67.

Die nach § 113b Abs. 1 TKG-E gespeicherten Daten sind durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung zu schützen (§ 113d Satz 1 TKG-E).

Die erforderlichen technischen und organisatorischen Maßnahmen zum Schutze der nach § 113b Abs. 1 TKG-E zu speichernden Daten sollen nach § 113d Satz 2 TKG-E insbesondere folgende Vorkehrungen umfassen:

- den Einsatz eines als besonders sicher geltenden Verschlüsselungsverfahrens,
- die Speicherung in gesonderten, von den für die üblichen betrieblichen Aufgaben getrennten Speichereinrichtungen,
- die Speicherung mit einem hohen Schutz vor dem Zugriff aus dem Internet auf vom Internet entkoppelten Datenverarbeitungssystemen,
- die Beschränkung des Zutritts zu den Datenverarbeitungsanlagen auf besonders ermächtigte Personen sowie
- die Gewährleistung des Vier-Augen-Prinzips für den Zugriff auf die Daten.

Diese Anforderungen an den Schutz der erhobenen Vorratsdaten gehen deutlich über das hinaus, was die Richtlinie 2006/24 in Art. 7 dafür an Vorkehrungen vorsah. Hiernach sollen

- die auf Vorrat gespeicherten Daten von der gleichen Qualität sein, der gleichen Sicherheit unterliegen und dem gleichen Schutz wie die im Netz vorhandenen Daten,
- in Bezug auf die Daten geeignete technische und organisatorische Maßnahmen getroffen werden müssen, um die Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust oder zufällige Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung zu schützen und
- in Bezug auf die Daten geeignete technische und organisatorische Maßnahmen getroffen werden müssen, um sicherzustellen, dass der Zugang zu den Daten ausschließlich besonders ermächtigten Personen vorbehalten ist.

Der vom EuGH durch die Ausgestaltung der VDS durch die Richtlinie 2006/24 ausgemachte Anreiz für die zur VDS verpflichteten Unternehmen, bei der Bereitstellung des Schutz- und Sicherheitsniveaus des Datenschutzes und der Datensicherung die Kosten für die Durchführung von Sicherheitsmaßnahmen zu berücksichtigen, könnte der RE neben stringenteren Anforderungen an den Schutz der erhobenen Daten, deren Verletzung mit Sanktionen[92] bedroht sind, auch insoweit begegnen, als hiernach Unternehmen für die durch Speicherung und Abruf von Vorratsda-

---

92 Der RE sieht eine Verschärfung der bereits bestehenden Sanktionsregelung im TKG vor. Verstöße gegen die Verpflichtungen, die sich hinsichtlich der nach § 113b TKG-E zu speichernden Daten ergeben, sollen nach § 149 Abs. 2 TKG-E einheitlich mit einer Geldbuße geahndet werden können. Vgl. dazu auch die Begründung des RE S. 51.

ten entstehenden Kosten entschädigt werden können sollen (RE § 113a Abs. 2 TKG-E), was allerdings voraussetzte, dass die den Telekommunikationsunternehmen entstehenden Kosten damit abgegolten werden.[93] Eine Kostendeckung dieser Investitionen scheint der RE offenbar nicht anzustreben, wenn er eine Entschädigungsmöglichkeit nur solchen Unternehmen gewährt, *„die eine unbillige Härte bei der Durchführung der Speicherverpflichtung nachweisen können."*[94]

Ob dem EuGH die im RE vorgesehenen Vorkehrungen zur Gewährleistung von Datenschutz und Datensicherheit genügen, lässt sich nicht feststellen, da der Gerichtshof die zur Gewährleistung des grundrechtlich gebotenen Datenschutzes und der grundrechtlich gebotenen Datensicherheit im Rahmen einer VDS zu treffenden Maßnahmen letztlich nicht explizit benennt.

Der vom EuGH geforderten unwiderruflichen Vernichtung der Daten nach Ablauf ihrer Speicherfrist entspricht der RE mit der hierin in § 113b Abs. 8 TKG-E vorgesehenen Regelung, nach der die speicherpflichtigen Unternehmen die auf Grund des TKG-E gespeicherten Daten unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfristen, irreversibel löschen müssen oder die irreversible Löschung sicherzustellen haben.

Vorratsdatenspeicherung auf Unionsgebiet

Der EuGH hebt schließlich kritisch hervor, dass die Richtlinie 2006/24 nicht vorschreibe, dass die Vorratsdaten auf Unionsgebiet gespeichert werden.[95]

Dem will der RE Rechnung tragen, indem er die Speicherung der Vorratsdaten im Inland anordnet (§ 113b Abs. 1 TKG-E). Die Vorgabe, Daten auf Vorrat im Unionsgebiet zu speichern, wird

---

93 Das wird in Zweifel gezogen. Der Deutsche Anwaltsverein äußert in seiner Stellungnahme (Fußn. 72) S. 27 f. die Befürchtung, dass die Auswahl der Sicherheitstechnologie anhand der Kosten erfolgen werde. Der Normenkontrollrat hebt dazu in seiner zusammenfassenden Stellungnahme zum RE (abrufbar unter http://www.bundesrat.de/SharedDocs/drucksachen/2015/0201-0300/249-15.pdf?__blob=publicationFile&v=1) folgendes hervor: *„In der vorliegenden Fassung entspricht der Entwurf nicht den Anforderungen der GGO einer Gesetzesvorlage an die Bundesregierung: Die Darstellung des Erfüllungsaufwandes fehlt für die Wirtschaft völlig und für die Verwaltung in wesentlichen Teilen. Dieser Mangel ist umso gravierender, als der NKR durch eigene Erhebungen Anhaltspunkte für Kosten der Telekommunikationswirtschaft von bis zu rd. 600 Mio. Euro gefunden hat; ferner deshalb, weil das Regelungsvorhaben Entschädigung für den Fall vorsieht, dass Investitionen und ggf. gesteigerte Betriebskosten „für einzelne Unternehmen erdrosselnde Wirkung haben könnten". Nicht nachzuvollziehen ist auch, weshalb das BMJV eine Evaluierung ausschließt, ohne diese Abweichung von dem Konzept des St-Ausschusses zu begründen. Der NKR hat gegen die Gesetzesvorlage erhebliche Bedenken, weil sie den Erfüllungsaufwand des Regelungsvorhabens nicht darstellt, obwohl zumindest eine Schätzung möglich wäre."* Der Verband der deutschen Internetwirtschaft (eco) erwartet Kosten von ca. 600 Mio. Euro für die betroffenen Telekommunikationsunternehmen; vgl. Stellungnahme des eco vom 20.05.2015 S. 3, online abrufbar unter: https://www.eco.de/wp-content/blogs.dir/analysepapier_eco-vds-gesetzesentwurf-auf-dem-pruefstand.pdf

94 Begründung RE S. 43 zu 113a TKG-E

95 EuGH (Fußn. 2) Rn. 68.

damit restriktiver als vom EuGH gefordert umgesetzt. Da der Gerichtshof mit dem Erfordernis der Speicherung der fraglichen Daten auf Unionsgebiet sicherstellen will, dass die Einhaltung des europäischen Datenschutzes und der Datensicherheit durch eine unabhängige Stelle überwacht wird[96], ist eine Unvereinbarkeit der RE mit der Entscheidung des EuGH vom 8. April 2014 insoweit nicht auszumachen.

4. Ergebnis

Eine von den Mitgliedstaaten eingeführte rechtskonforme VDS muss (auch) mit europäischen Grundrechten vereinbar sein. Mitgliedstaatliche Regelungen, die zur Bevorratung von Daten verpflichten, müssen mithin den Vorgaben der Entscheidung des EuGH vom 8. April 2014 entsprechen.

Der Entscheidung des EuGH vom 8. April 2014 lässt sich nicht entnehmen, dass eine (anlasslose) VDS europarechtlich von vornherein ausgeschlossen ist. Gegenteiliges ließe sich hieraus allerdings auch nicht folgern. Davon abgesehen lassen sich den Urteilsgründen nicht die Grenzen einer grundrechtskonformen VDS trennscharf entnehmen,[97] so dass letztlich nicht abschließend festgestellt werden kann, ob die im RE ausformulierte VDS den dieser Entscheidung zu entnehmenden Anforderungen an einer mit europäischen Grundrechten konformen Ausgestaltung einer VDS in dem Maße übereinstimmt, dass diese sich noch innerhalb der Grenzen bewegt, die nach Ansicht des Gerichtshofs zur Wahrung des Grundsatzes der Verhältnismäßigkeit mit Blick auf Art. 7, 8 und 52 Abs. 1 GRCh einzuhalten sind.

---

96 EuGH (Fußn. 2) Rn. 68.

97 So auch Bäcker (Fußn. 20) S. 1273.