Unterabteilung Europa
Fachbereich Europa

Deutscher Bundestag

Ausarbeitung

Zur Vereinbarkeit des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten mit dem EuGH-Urteil vom 21. Dezember 2016 zur Vorratsdatenspeicherung

Zur Vereinbarkeit des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten mit dem EuGH-Urteil vom 21. Dezember 2016 zur Vorratsdatenspeicherung

Aktenzeichen: PE 6 – 3000 – 167/16
Abschluss der Arbeit: 12.01.2017
Fachbereich: PE 6: Fachbereich Europa

Inhaltsverzeichnis

1.	**Die zu untersuchende Fragestellung**	**4**
2.	**Das Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten im Überblick**	**4**
3.	**Die Entscheidung des EuGH vom 21. Dezember 2016 zur VDS**	**6**
3.1.	Zum Verfahrensgegenstand und Entscheidungsverfahren	6
3.2.	Der Prüfungsmaßstab des EuGH	7
3.3.	Die daraus abgeleiteten Vorgaben für die VDS	7
4.	**Entspricht das Gesetz zur Einführung einer Speicherung und Höchstspeicherfrist für Verkehrsdaten den Vorgaben der Entscheidung des EuGH vom 21. Dezember 2016 zur VDS?**	**12**
4.1.	Zulässige Ziele der VDS	12
4.2.	Die für eine gerechtfertigte VDS erforderlichen Sachgründe und Beschränkungen	13
4.3.	Zugangsvoraussetzungen zu den auf Vorrat gespeicherten Daten	18
5.	**Ergebnis**	**23**

1. Die zu untersuchende Fragestellung

Der Fachbereich Europa wird um die Klärung folgender Fragestellung ersucht:

> *„Inwieweit ist das am 16.10.2015 vom Bundestag beschlossene Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten mit dem heutigen Urteil des EuGH in den verbundenen Rechtssachen C-203/15, Tele2 Sverige AB/Post-och telestryelsen, und C-698/15, Secretary of State fort he Home Department / Tom Watson u.a. […] vereinbar und welche Folgen würde eine vollständige oder teilweise Unvereinbarkeit jeweils nach sich ziehen?“*

Der Fachbereich Europa PE 6 untersucht die Vereinbarkeit des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten mit vorstehender Entscheidung. Es wird darauf hingewiesen, dass Gegenstand vorstehender Entscheidung des Gerichtshofes der Europäischen Union (EuGH) nur die anlasslose Speicherung von Verkehrsdaten ist und daher diese Ausarbeitung nur deren Ausgestaltung im Gesetz zur Einführung einer Speicher-pflicht und einer Höchstspeicherfrist für Verkehrsdaten untersucht und sich daher nicht mit der Frage befasst, ob die gezielte Erhebung von Verkehrsdaten von Tatverdächtigen nach § 100g Abs. 1 StPO mit dem Unionsrecht vereinbar ist.

Die Frage, welche Folgen eine vollständige oder teilweise Unvereinbarkeit jeweils nach sich ziehen würde, bearbeitet der Fachbereich Zivil-, Straf- und Verfahrensrecht, Umweltschutzrecht, Bau und Stadtentwicklung (WD 7).

2. Das Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten im Überblick

Dem Gesetz zur Einführung einer Speicherung und Höchstspeicherfrist für Verkehrsdaten lassen sich im Wesentlichen folgende Regelungen zur Ausgestaltung der Vorratsdatenspeicherung (VDS) entnehmen:

- Die Erbringer öffentlich zugänglicher Telefondienste sind hiernach verpflichtet, bei der Telekommunikation anfallende Verkehrsdaten zu speichern. Zu speichern sind 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[1], bei Mobilfunk auch die Standortdaten.[2] Die Erbringer öffentlich zugänglicher Internetzugangsdienste sollen zur Speicherung von IP-Adressen einschließlich Zeitpunkt und Dauer der Internetnutzung unter der zugewiesenen IP-Adresse verpflichtet sein.[3] Nicht (auf Grundlage dieses Geset-

---

1 § 113b Abs. 2 Nr. 1. bis 4. TKG.

2 § 113b Abs. 4 TKG. Zur näheren Bestimmung der zu speichernden Standortdaten vgl. die Begründung des Gesetzentwurfs BT-Drs. 18/5088, S. 39 zu Absatz 4.

3 § 113b Abs. 3 TKG.

zes) gespeichert werden dürfen der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post.[4] Die Speicherung der Daten muss im Inland erfolgen[5]; diese sind vor unbefugter Kenntnisnahme und Verwendung zu schützen.[6]

- Die Speicherfrist beträgt für Standortdaten vier Wochen[7], im Übrigen zehn Wochen.[8] Die Daten sind nach Ablauf der Speicherfrist (irreversibel) zu löschen.[9] Bewegungs- und Persönlichkeitsprofile sollen auf Grundlage des Gesetzes zur Einführung einer Speicherung und Höchstspeicherfrist für Verkehrsdaten nicht erstellt werden können, was durch die Präzisierung der Anforderungen an die Funkzellenabfrage sichergestellt werden soll.[10] Deshalb sollen im Grundsatz auch nur einzelne Standortdaten abgerufen werden dürfen.[11]

- Die Strafverfolgungsbehörden dürfen die gespeicherten Daten zur Verfolgung besonders schwerer Straftaten abrufen, die als solche in § 100g Abs. 2 StPO enumerativ abschließend definiert werden. Den Gefahrenabwehrbehörden der Länder dürfen Vorratsdaten übermittelt werden, wenn die jeweiligen Polizeigesetze einen Abruf der Verkehrsdaten zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit oder für den Bestand des Bundes oder eines Landes erlauben.[12]

- Verkehrsdaten zu nach § 53 StPO zeugnisverweigerungsberechtigten Personen dürfen nicht abgerufen werden und unterliegen im Übrigen einem Verwertungsverbot.[13] 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.[14]

---

4 § 113b Abs. 5 TKG.

5 § 113b Abs. 1 TKG.

6 §§ 113d, 113g TKG.

7 § 113b Abs. 1 Nr. 2. TKG

8 § 113b Abs. 1 Nr. 1. TKG.

9 § 113b Abs. 8 TKG.

10 § 100g Abs. 3 StPO; Begründung BT-Drs. 18/5088, S. 32 f.

11 § 101a Abs. 2 StPO; Begründung BT-Drs. 18/5088, S. 35: *„Grundsätzlich sollen nur einzelne Standortdaten abgerufen werden, um keine überflüssigen Bewegungsprofile zu erstellen.“*

12 § 113c Abs. 1 Nr. 2. TKG.

13 § 100g Abs. 4 StPO.

14 § 113b Abs. 6 TKG; Begründung BT-Drs. 18/5088, S. 23 f., 40.

- Der Abruf von Verkehrsdaten soll neben weiteren Voraussetzungen nur zur Verfolgung von in einem Katalog als solche festgelegten schweren Straftaten zulässig sein[15] und unterliegt - ohne eine Eilkompetenz der Staatsanwaltschaft vorzusehen - uneingeschränkt einem Richtervorbehalt.[16]

3. Die Entscheidung des EuGH vom 21. Dezember 2016 zur VDS

3.1. Zum Verfahrensgegenstand und Entscheidungsverfahren

Der Gerichtshof der Europäischen Union (EuGH) hatte mit Urteil vom 21. Dezember 2016[17] im Wege eines Vorabentscheidungsverfahrens nach Art. 267 Vertrag über die Arbeitsweise der Europäischen Union (AEUV) in einem Streitverfahren, das eine auf Grundlage des schwedischen Gesetzes über die elektronische Kommunikation (*Lag om elektronisk kommunikation)* ergangene Anordnung der schwedischen Überwachungsbehörde für Post und Telekommunikation zur Vorratsspeicherung von Verkehrs- und Standortdaten ihrer Teilnehmer und registrierten Nutzer zum Gegenstand hat, und ein weiteres Streitverfahren, in dem über die Vereinbarkeit des Gesetzes von 2014 zur Vorratsdatenspeicherung und zu den Ermittlungsbefugnissen des Vereinigten Königreichs (*Data Retention and Investigatory Powers Act 2014*) mit dem Unionsrecht gestritten wird, über zahlreiche Detailfragen zur VDS entschieden.

Dem EuGH wurden dazu folgende Fragen zur Entscheidung vorgelegt:

> *„Ist eine generelle Verpflichtung zur Vorratsspeicherung von Verkehrsdaten, die sich (wie [im Vorabentscheidungsersuchen] beschrieben) auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten erstreckt, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung von Straftaten vorzusehen, mit Art. 15 Abs. 1 der Richtlinie 2002/58 (1) unter Berücksichtigung der Art. 7, 8 und 52 Abs. 1 der Charta vereinbar?*
> *Falls die erste Frage zu verneinen ist, kann die Vorratsspeicherung dennoch zulässig sein, wenn:*
> *a) der Zugang der nationalen Behörden zu den gespeicherten Daten wie [im Vorabentscheidungsersuchen] beschrieben festgelegt ist und*
> *b) die Sicherheitsanforderungen wie [im Vorabentscheidungsersuchen] beschrieben geregelt sind und*
> *c) sämtliche relevanten Daten wie [im Vorabentscheidungsersuchen] beschrieben für einen Zeitraum von sechs Monaten ab dem Tag, an dem die Kommunikation beendet wird, gespeichert und anschließend gelöscht werden müssen?“*

---

15 § 100g Abs. 1, 2 StPO.

16 § 101a Abs. 1 Satz 2 StPO, Begründung BT-Drs. 18/5088, S. 34.

17 Verbundene Rechtssachen C-203/15 und C-698/15, abrufbar unter: http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=192727.

3.2. Der Prüfungsmaßstab des EuGH

Prüfungsmaßstab zur Beantwortung der vorgelegten Rechtsfragen ist die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation, nachfolgend: RL 2002/58)[18], die im Lichte der Art. 7, 8, 11 und 52 Charta der Grundrechte der Europäischen Union (GRC) ausgelegt wird.

Regelungen der Mitgliedstaaten, mit denen diese den Betreibern elektronischer Kommunikationsdienste vorschreiben, den nationalen Behörden Zugang zu den von ihnen gespeicherten Daten zu gewähren, misst der Gerichtshof an Art. 15 Abs. 1 RL 2002/58, da dieser Norm ansonsten jede praktische Wirksamkeit genommen würde, wenn nicht auch mitgliedstaatliche Vorschriften über die Aufbewahrung von Daten zum Zwecke der Kriminalitätsbekämpfung dem Anwendungsbereich dieser Richtlinie unterlägen (dazu unten 3.3.). Er verweist zudem darauf, dass diese Richtlinie die Mitgliedstaaten zum Erlass entsprechender Vorschriften nur dann ermächtigt, wenn die in Art. 15 Abs. 1 RL 2002/58 vorgesehenen Voraussetzungen eingehalten werden.[19]

3.3. Die daraus abgeleiteten Vorgaben für die VDS

Der Gerichtshof misst gesetzliche Regelungen zur VDS der Mitgliedstaaten an Art. 15 Abs. 1 RL 2002/58 im Lichte der grundrechtlichen Verbürgungen der Art. 7, 8, 11 und 52 GRC.

Nach Art. 5 Abs. 1 RL 2002/58 müssen die Mitgliedstaaten die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicherstellen. Im Grundsatz ist es jeder anderen Person als dem Nutzer untersagt, ohne dessen Einwilligung die mit elektronischer Kommunikation verbundenen Verkehrsdaten zu speichern mit Ausnahme der in Art. 15 Abs. 1 RL 2002/58 dazu ermächtigten Personen sowie der für die Weiterleitung einer Nachricht erforderlichen technischen Speicherung.[20]

> *„Artikel 5*
> *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*

---

18 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, abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1483367910717&uri=CELEX:32002L0058

19 EuGH (Fußn. 17) Rn. 73, 81.

20 EuGH (Fußn. 17) Rn. 85.

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.“

Verkehrsdaten dürfen nach Art. 6 RL 2002/58 nur zur Gebührenabrechnung für die Dienste, zu deren Vermarktung und zur Bereitstellung von Diensten mit Zusatznutzern verarbeitet und gespeichert werden.

Art. 15 Abs. 1 RL 2002/58 erlaubt den Mitgliedstaaten, Ausnahmen von der in Art. 5 Abs. 1 RL 2002/58 normierten grundsätzlichen Pflicht zur Wahrung der Vertraulichkeit personenbezogener Daten bei der elektronischen Kommunikation und den weiteren, in dieser Richtlinie normierten Pflichten vorzusehen.

„Art. 15
Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG

(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.“

Mit Blick auf die Tragweite der grundsätzlichen Verpflichtung, die Vertraulichkeit elektronischer Kommunikation und der damit verbundenen Verkehrsdaten zu gewährleisten, ist die aus Art. 15 Abs. 1 RL 2002/58 folgende Beschränkungsbefugnis der Mitgliedstaaten nach Ansicht des EuGH eng auszulegen.[21] Die in Art. 15 RL 2002/58 normierte Ausnahme von dem grundsätzlichen Verbot, Verkehrsdaten zu speichern, darf nach Ansicht des Gerichtshofs nicht in der Weise ausgelegt werden, dass diese zur Regel wird.[22] Regelungen zur VDS „*müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen*“ (Art. 15 Abs. 1 Satz 3 RL 2002/58), wovon auch die allgemeinen Grundsätze des Unionsrechts und die Grundrechte der GRC umfasst sind.[23] Demgemäß sind nach Ansicht des Gerichtshofs sowohl das in Art. 7 der Charta gewährleistete Grundrecht auf Achtung des Privatlebens als auch das in Art. 8 der Charta gewährleistete

21 EuGH (Fußn. 17), Rn. 89.

22 EuGH (Fußn. 17), Rn. 89.

23 EuGH (Fußn. 17), Rn. 91.

Grundrecht auf Schutz personenbezogener Daten bei der Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 zu berücksichtigen. Das Gleiche gilt in Anbetracht der besonderen Bedeutung, die der Freiheit der Meinungsäußerung in jeder demokratischen Gesellschaft zukommt, für das Recht auf freie Meinungsäußerung.[24]

Im Einzelnen lassen sich dieser Entscheidung folgende Leitlinien für mitgliedstaatliche Vorschriften zur VDS entnehmen:

Materiellrechtliche Anforderungen

- Die vom Grundsatz der Vertraulichkeit von Kommunikationen und der damit verbundenen Verkehrsdaten abweichenden Rechtsvorschriften müssen „*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*“ (Art. 15 Abs. 1 Satz 1 RL 2002/58) zum Ziel haben oder einen der anderen Zwecke des Art. 13 Abs. 1 RL 96/46[25] [26], auf den Art. 15 Abs. 1 Satz 1 RL 2002/58 verweist, verfolgen.[27] Die VDS darf nur zu einem dieser Zwecke erfolgen.[28]

- Die Vorratsspeicherung von Verkehrs- und Standortdaten darf nur während einer begrenzten Zeit erfolgen.[29]

---

[24] EuGH (Fußn. 17), Rn. 93.

[25] 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 281.

[26] *„Artikel 13 Ausnahmen und Einschränkungen*

(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Pflichten und Rechte gemäß Artikel 6 Absatz 1, Artikel 10, Artikel 11 Absatz 1, Artikel 12 und Artikel 21 beschränken, sofern eine solche Beschränkung notwendig ist für
a) die Sicherheit des Staates;
b) die Landesverteidigung;
c) die öffentliche Sicherheit;
d) die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen;
e) ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Union einschließlich Währungs-, Haushalts- und Steuerangelegenheiten;
f) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben c), d) und e) genannten Zwecke verbunden sind;
g) den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.“

[27] EuGH (Fußn. 17), Rn. 90.

[28] EuGH (Fußn. 17), Rn. 95.

[29] EuGH (Fußn. 17), Rn. 95.

- Die Vorratsspeicherung von Verkehrs- und Standortdaten ist nur zur Bekämpfung schwerer Kriminalität, insb. der organisierten Kriminalität und des Terrorismus, zulässig.[30]

- Offenbar fordert der EuGH, dass bei der VDS eine Differenzierung vorzunehmen ist, etwa danach, ob Personen hiervon betroffen sind, die Anlass zur Strafverfolgung geben oder deren Kommunikationsvorgänge nach den nationalen Vorschriften dem Berufsgeheimnis unterliegen.[31] Grundsätzlich soll der Zugang „*nur zu den Daten von Personen gewährt werden, die in Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein. Allerdings könnte in besonderen Situationen wie etwa solchen, in denen vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind, der Zugang zu Daten anderer Personen ebenfalls gewährt werden, wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung solcher Aktivitäten leisten könnten*."[32]

- Ein Kriterium für die Bewertung, ob eine nationale Regelung zur VDS europarechtkonform ist, soll nach Ansicht des Gerichtshofs auch sein, ob die VDS nur in einem begrenzten geografischen Gebiet oder ohne eine solche territoriale Beschränkung vorgenommen werden darf.[33]

- Gesetze zur VDS der Mitgliedstaaten müssen klare und präzise Regeln zur Tragweite und Anwendung der VDS aufstellen, so dass Personen, deren Daten auf Vorrat gespeichert werden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauch gewährleisten.[34] Deren materielle Voraussetzungen müssen die VDS auf das absolut Notwendige beschränken, wobei gewährleistet sein muss, dass „*die Vorratsspeicherung der Daten stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen.*"[35]

Zugang zu Vorratsdaten, Verfahrenserfordernisse

- Der Zugang zu den auf Vorrat gespeicherten Daten darf nur den in Art. 15 Abs. 1 Satz 1 RL 2002/58 genannten Zwecken dienen.[36]

- Unverzichtbar soll auch sein, *„dass der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten grundsätzlich – außer in hinreichend begründeten*

---

30 EuGH (Fußn. 17), Rn. 102 f., 115.

31 EuGH (Fußn. 17), Rn. 105.

32 EuGH (Fußn. 17), Rn. 119.

33 EuGH (Fußn. 17), Rn. 106, 111.

34 EuGH (Fußn. 17), Rn. 109.

35 EuGH (Fußn. 17), Rn. 110.

36 EuGH (Fußn. 17), Rn. 115.

Eilfällen – einer vorherigen Kontrolle entweder durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und deren Entscheidung auf einen mit Gründen versehenen Antrag ergeht, der von den zuständigen nationalen Behörden u. a. im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten gestellt wird.“[37]

- Die zuständigen nationalen Behörden, denen Zugang zu den Vorratsdaten gewährt wird, müssen die betroffenen Personen nach dem einschlägigen Recht der Mitgliedstaaten davon in Kenntnis setzen, sobald eine entsprechende Mitteilung die behördlichen Ermittlungen nicht mehr beeinträchtigen kann.[38]

Schutzniveau der gespeicherten Vorratsdaten

- Die Betreiber elektronischer Kommunikationsdienste müssen geeignete technische und organisatorische Vorkehrungen treffen, die sicherstellen, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsrisiken und jedem unberechtigten Zugang geschützt sind. Die Daten sind im Unionsgebiet zu speichern und nach Ablauf der Speicherfrist unwiderruflich zu vernichten.[39]

- Die Einhaltung des Schutzniveaus muss von einer unabhängigen Stelle überwacht werden.[40]

Der Entscheidung des EuGH lässt sich nicht entnehmen, dass mitgliedstaatliche Regelungen zur VDS bereits dann unionsrechtswidrig sind, wenn diese eine der genannten Anforderungen nicht erfüllen, noch lässt sich zweifelsfrei hieraus generell ableiten, welches Maß fehlender Übereinstimmung hiermit zur Unionsrechtswidrigkeit führt. Aus dieser Entscheidung lassen sich allerdings Schlussfolgerungen für andere Vorschriften zur VDS als die verfahrensgegenständlichen ziehen, soweit diese mit den zur Entscheidung vorgelegten Vorschriften zur VDS übereinstimmen: Zu diesen traf der Gerichtshof folgende Feststellungen:

„Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 sowie des Art. 52 Abs. 1 der Charta [ist] 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“,*

- *„die den Schutz und die Sicherheit der Verkehrs- und Standortdaten, insbesondere den Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten zum Gegenstand hat, ohne im Rahmen der Bekämpfung von Straftaten diesen Zugang ausschließlich auf die Zwecke einer Bekämpfung schwerer Straftaten zu beschränken, ohne*

---

37 EuGH (Fußn. 17), Rn. 120.

38 EuGH (Fußn. 17), Rn. 121.

39 EuGH (Fußn. 17), Rn. 122.

40 EuGH (Fußn. 17), Rn. 123.

den Zugang einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen und ohne vorzusehen, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind."

4. Entspricht das Gesetz zur Einführung einer Speicherung und Höchstspeicherfrist für Verkehrsdaten den Vorgaben der Entscheidung des EuGH vom 21. Dezember 2016 zur VDS?

Zunächst ist darauf hinzuweisen, dass sich der Entscheidung des EuGH vom 21.12.2016 nur Gründe dafür entnehmen lassen, weshalb aus Sicht des Gerichtshofs die konkrete Ausgestaltung der VDS durch das schwedische Gesetz über die elektronische Kommunikation (*Lag om elektronisk kommunikation*) und das Gesetz von 2014 zur Vorratsdatenspeicherung und zu den Ermittlungsbefugnissen des Vereinigten Königreichs (*Data Retention and Investigatory Powers Act 2014*) mit dem Unionsrecht unvereinbar sein soll. Offen muss daher bleiben, ob die vom Gericht dazu getroffenen Erwägungen (uneingeschränkt) auch für das deutsche Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten Geltung beanspruchen. An dieser Stelle kann daher nur überprüft werden, inwieweit diese Regelung den Vorgaben des EuGH entspricht, nicht aber, welche Folgerungen der Gerichtshof hierfür aus den nachfolgend zu treffenden Feststellungen ziehen würde.

Bereits die Speicherung von Vorratsdaten ist ein Eingriff in die Grundrechte des Art. 7, 8, 11 und 52 GRC, der nicht allein mit dem damit verfolgten Ziel der Bekämpfung der schweren Kriminalität gerechtfertigt werden kann (4.1.), und Differenzierungen bzw. Einschränkungen erfordert hinsichtlich Teilnehmer, registrierter Nutzer, sowie Verkehrsdaten in Abhängigkeit von dem verfolgten Ziel (4.2.). In einem weiteren Schritt ist zu prüfen, ob die vom Gerichtshof dargelegten Voraussetzungen für den Zugang zu Vorratsdaten eingehalten sind (4.3.).

4.1. Zulässige Ziele der VDS

Nach Art. 15 Abs. 1 Satz 1 RL 2002/58 müssen Vorschriften wie solche zur VDS, die die Vertraulichkeit von Kommunikationen und der damit verbundenen Verkehrsdaten einschränken, eines oder mehrere der in dieser Vorschrift genannten Ziele verfolgen.[41] Sie müssen das Ziel des Schutzes der nationalen Sicherheit, d. h. der Sicherheit des Staates, der Landesverteidigung, der öffentliche Sicherheit, der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder einen der Zwecke des Art. 13 Abs. 1 Richtlinie 95/46 verfolgen.

Im Telekommunikationsgesetz (TKG) müssen genau definierte Verkehrsdaten, bei Mobilfunk auch Standortdaten sowie IP-Adressen einschließlich Zeitpunkt und Dauer der Vergabe einer IP-Adresse gespeichert werden, ohne dafür das Vorliegen einer schweren Straftat vorauszusetzen. Eine entsprechende Einschränkung besteht erst beim Abruf der Daten. Das Gesetz zur Einführung einer Speicherung und Höchstspeicherfrist für Verkehrsdaten dient allerdings als einheitliches Regelwerk zur anlasslosen Speicherung von Verkehrsdaten und zum Informationszugang hierzu ausweislich der Gesetzesbegründung der Strafverfolgung und Gefahrenabwehr und erfüllt demgemäß diese Anforderung des Gerichtshofs.

---

41 EuGH (Fußn. 17), Rn. 90.

4.2. Die für eine gerechtfertigte VDS erforderlichen Sachgründe und Beschränkungen

Die für die Speicherung von Vorratsdaten tragenden Gründe

Nach Ansicht des Gerichtshofs könne wegen der Schwere des mit einer VDS verbundenen Eingriffs in die Grundrechte der davon Betroffenen eine nationale Regelung, die für Zwecke der Kriminalitätsbekämpfung die Vorratsspeicherung von Verkehrs- und Standortdaten vorsieht, nicht allein die damit verfolgte Bekämpfung der schweren Kriminalität rechtfertigen.[42]

Die im Gesetz zur Einführung einer Speicherung und Höchstspeicherfrist für Verkehrsdaten ausgestaltete VDS setzt für die Speicherung nicht das Vorliegen einer schweren Straftat voraus. Eine entsprechende Einschränkung gilt erst beim Abruf der Daten. Der Datenabruf soll nur bei schwersten Straftaten zulässig sein, die in § 100g Abs. 2 Satz 2 StPO abschließend legaldefiniert sind. Die nach § 113b TKG gespeicherten Verkehrsdaten dürfen nach § 100g Abs. 2 StPO nur erhoben werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Katalogtat nach § 100g Abs. 2 StPO 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.

Diese Regelung dürfte, ausgehend von den Vorgaben des Gerichtshofs in seiner Entscheidung vom 21. Dezember 2016, nicht mehr als erforderlicher Grundrechtseingriff anzusehen sein. Tragender Grund hierfür dürfte sein, dass diese – abgesehen von den im Regelfall nicht zu speichernden 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 – eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vorsieht.

Der EuGH fordert Einschränkungen hinsichtlich des Sachgrundes für die VDS und des davon betroffenen Personenkreises bereits für die Speicherung von Vorratsdaten und nicht erst für den Zugang hierzu. Da die Speicherpflicht nach Ansicht des Gerichtshofs, wie er ausführlich bereits zuvor in seiner Entscheidung vom 8. April 2014 verdeutlicht hat, eine Bedrohung der öffentlichen Sicherheit voraussetzt[43], 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.[44] Bereits die Speicherung von Daten ist im europäischen Da-

---

42 EuGH (Fußn. 17) Rn. 105.

43 EuGH, Verb. Rs. C-293/12 und C-594/12, Rn. 59.

44 So die Schlussfolgerungen aus der Entscheidung des EuGH vom 8. April 2014 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

tenschutzrecht ein der Rechtfertigung bedürftiger Eingriff.[45] Nach Art. 8 Abs. 1 Satz 2 GRC 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) RL 95/46/EG[46] näher definierte Begriff *Verarbeitung* ist als Oberbegriff aller datenbezogenen Prozesse zu verstehen.[47] 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.*“

Zulässige Höchstdauer der Vorratsspeicherung von Verkehrs- und Standortdaten

Der Gerichtshof verweist lediglich darauf, dass nach Art. 15 Abs. 1 Satz 2 RL 2002/58 die Vorratsspeicherung von Daten nur „*während einer begrenzten Zeit*“ erfolgen dürfe, ohne dies in zeitlich Hinsicht zu präzisieren.[48] In seiner Entscheidung 8. April 2014[49] zur Richtlinie 2006/24[50] hob

---

2014, S. 300 (301) und Roßnagel, Neue Maßstäbe für den Datenschutz in Europa, MMR 2014, S. 372 (375) und ders.: Der nächste Schritt im Ringen um Sicherheit und Grundrechtsschutz, NJW 2016, S. 533 (538 f.); Koshan, Vorratsdatenspeicherung – verfassungsrechtliche Rahmenbedingungen und rechtspolitische Verortung, DuD 2016, S. 167 (169 f.); Boehm/Andrees, Zur Vereinbarkeit der Vorratsdatenspeicherung mit europäischem Recht, CR 2016, S. 146 (152); 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. 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.).

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

46 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.

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

48 EuGH (Fußn. 17), Rn. 95.

49 EuGH (Fußn. 43), Rn. 63 f.

50 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, Abl L 105/54, abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1483538372774&uri=CELEX:32006L0024

der Gerichtshof hervor, dass es keine objektiven Kriterien gebe, 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 höchstens 24 Monaten auf das absolut Notwendige beschränke.[51]

Dieser Anforderung will das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten in der Weise entsprechen, dass die Speicherfrist für Standortdaten vier Wochen[52], im Übrigen zehn Wochen betragen soll[53] und die Daten nach Ablauf der Speicherfrist zu löschen sind.[54] Sie sehen mithin erheblich kürzere Speicherfristen vor als noch seinerzeit die Richtlinie 2006/24; außerdem differenziert diese Vorschrift hinsichtlich der Speicherfrist zwischen Standortdaten und (sonstigen) Verkehrsdaten. Eine Unvereinbarkeit des zu überprüfenden Gesetzes hinsichtlich der zulässigen Speicherfrist zu den Vorgaben des EuGH ist insoweit nicht auszumachen.

Beschränkung der VDS auf bestimmte geografische Gebiete

Ein Kriterium für die Bewertung, ob eine nationale Regelung zur VDS europarechtkonform ist, soll nach Ansicht des Gerichtshofs auch sein, ob die VDS in einem begrenzten geografischen Gebiet vorzunehmen ist oder ohne eine solche Beschränkung vorgenommen werden darf.[55] Eine solche Beschränkung ist in § 113b TKG, wo die Adressaten und die Grundvoraussetzungen der Speicherpflichten bestimmt werden, nicht vorgesehen.

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

Die Entscheidung des EuGH vom 21. Dezember 2016 verdeutlicht, dass sowohl die Vorratsspeicherung von Verkehrsdaten wie die Gewährung des Zugangs hierzu rechtfertigungsbedürftige Grundrechtseingriffe sind, die grundrechtswahrenden Anforderungen hinsichtlich der von der VDS erfassten Verkehrsdaten, Kommunikationsmittel und des davon betroffenen Personenkreises unterliegen.

Offenbar fordert der EuGH, dass bereits die Speicherung von Vorratsdaten von einschränkenden Zulässigkeitskriterien, insb. davon abhängig sein soll, ob Personen hiervon betroffen sind, die Anlass zur Strafverfolgung geben, und meint, dass die Hürden für die Speicherung von Vorratsdaten besonders hoch sein sollen, soweit dies Kommunikationsvorgänge betrifft, die nach den nationalen Vorschriften dem Berufsgeheimnis unterliegen.[56]

---

51 EuGH (Fußn. 43) Rn. 64.

52 § 113b Abs. 1 Satz 1 Nr. 2. TKG.

53 § 113b Abs. 1 Satz 1 Nr. 1 TKG.

54 § 113b Abs. 8 TKG.

55 EuGH (Fußn. 17), Rn. 106, 111.

56 EuGH (Fußn. 17), Rn. 105.

Grundsätzlich soll der Zugang „*nur zu den Daten von Personen gewährt werden, die in Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein. Allerdings könnte in besonderen Situationen wie etwa solchen, in denen vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind, der Zugang zu Daten anderer Personen ebenfalls gewährt werden, wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung solcher Aktivitäten leisten könnten.*“[57]

Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten sieht – soweit ersichtlich – im Grundsatz keine diesen Anforderungen genügende 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 zwar (grundsätzlich) von der Speicherpflicht ausgenommen sein.[58] Davon abgesehen müssen die im TKG genau definierten Verkehrsdaten, bei Mobilfunk auch Standortdaten sowie IP-Adressen einschließlich Zeitpunkt und Dauer der Vergabe einer IP-Adresse, gespeichert werden. Die im Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vorgesehene VDS sieht – mit Ausnahme der zuvor genannten Personengruppen – keine Beschränkungen hinsichtlich des von einer Speicherung betroffenen Personenkreises vor.

Für die Frage, ob der mit der Speicherung von Vorratsdaten verbundene Grundrechtseingriff gerechtfertigt werden kann, weisen die Gründe der Entscheidung vom 21. Dezember 2016 auch auf die Bedeutung einer Ausnahmeregelung für Personen hin, deren Kommunikationsvorgänge nach den nationalen Vorschriften der Mitgliedstaaten dem Berufsgeheimnis unterliegen.[59] Dort wird auf die Entscheidung des Gerichtshofs vom 8. April 2014 verwiesen, wo die Große Kammer gegen die Richtlinie 2006/24 kritisch anmerkte, dass diese keine Ausnahmeregelung für Personen vorsehe, „*deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen*“[60].

Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten trägt dieser Anforderung insoweit Rechnung, als 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

---

57 EuGH (Fußn. 17), Rn. 119.

58 § 113b Abs. 6; Begründung S. 25, 46.

59 EuGH (Fußn. 17), Rn. 105.

60 EuGH (Fußn. 43) Rn. 58.

§ 53 StPO zeugnisverweigerungsberechtigten Personen[61], sollen *grundsätzlich* bereits von der Speicherpflicht ausgenommen sein.[62]

Es wurde aber schon mehrfach darauf hingewiesen, dass bereits die Speicherung von Vorratsdaten ein legitimationsbedürftiger Grundrechtseingriff ist. Da das TKG auch die Speicherung der Daten von anderen Berufsgeheimnisträgern als den ausgenommen Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen vorsieht, trägt diese Regelung der Vorgabe des EuGH, die eine Ausnahmeregelung bereits von der Speicherung von Verkehrsdaten für Personen fordert, *„deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen“*, nicht Rechnung. [63]

Für die Frage, ob der mit der Speicherung von Vorratsdaten verbundene Grundrechtseingriff gerechtfertigt werden kann, soll es ausweislich der Gründe der Entscheidung vom 21. Dezember 2016 auch von Bedeutung sein, ob eine Regelung zur VDS der Mitgliedstaaten einen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit fordert. Dabei soll von Bedeutung sein, ob diese die Vorratsspeicherung auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises beschränkt, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, oder deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung von Straftaten beitragen können.[64] Eine zur Bekämpfung schwerer Straftaten vorbeugende gezielte Vorratsspeicherung von Verkehrs- und Standortdaten soll grundrechtskonform sein, sofern die VDS „*hinsichtlich Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist*.“[65] Diese müsse sich „*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*.“[66]

Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten lässt auf der Stufe der Datenspeicherung nicht erkennen, dass es diese an derartige Be-

---

61 Der Deutsche Anwaltsverein fordert in seiner Stellungnahme zum Referentenentwurf vom 15.05.2015 S. 13 f. den Verzicht auf die VDS zum Schutze der Berufsgeheimnisträger bzw. die Gewährleistung des Schutzes von Berufsgeheimnissen durch einen Datenabgleich.

62 § 113b Abs. 6; Begründung S. 25, 46

63 Kunnert, DuD 2014, S. 774 (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.

64 EuGH (Fußn. 17), Rn. 106.

65 EuGH (Fußn. 17), Rn. 108.

66 EuGH (Fußn. 17), Rn. 111.

schränkungen bindet. Dieses Gesetz dürfte insb. nicht hinreichend sicherstellen, dass die Vorratsdaten nur solcher Personen gespeichert und abgerufen werden können, die der Beteiligung an einer nach § 100g StPO 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[67] in diesem Zusammenhang darauf hin, dass auf Grundlage des dem vorliegend untersuchten Gesetz vorangegangenen Referentenentwurfs nicht zwangsläufig die Daten derer erfasst würden, die kommunizieren, sondern die Daten der Personen, die die technische Infrastruktur vorhalten. Damit dürfte der Anforderung des EuGH nicht umfassend entsprochen sein, dass nur Daten auf Vorrat zu solchen Personen gespeichert werden dürfen, die Anlass zur Strafverfolgung gegeben haben. Bereits 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.*“[68]

4.3. Zugangsvoraussetzungen zu den auf Vorrat gespeicherten Daten

Verwendung von Vorratsdaten nur zu den in Art. 15 Abs. 1 Satz 1 RL 2002/58 genannten Zwecken auf präziser gesetzlicher Grundlage

Auch der Zugang zu den auf Vorrat gespeicherten Daten darf nach Ansicht des Gerichtshofs nur den in Art. 15 Abs. 1 Satz 1 RL 2002/58 genannten Zwecken dienen.[69] Zu dem Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten könne nur die Bekämpfung schwerer Straftaten einen solchen Zugang auf Grundlage einer die Voraussetzungen hierfür anhand objektiver Kriterien klaren und präzisen gesetzlichen Regelung zu den auf Vorrat gespeicherten Daten rechtfertigen.[70]

§ 113c Abs. 1 Nr. 1. TKG dürfte dieser Anforderung genügen, da hiernach die Strafverfolgungsbehörden die gespeicherten Daten insb. zur Verfolgung gesetzlich definierter schwerer (Katalog-) Straftaten abrufen dürfen. Den Gefahrenabwehrbehörden der Länder dürfen die gespeicherten

---

67 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.

68 EuGH (Fußn. 43) Rn. 58.

69 EuGH (Fußn. 17), Rn. 115.

70 EuGH (Fußn. 17), Rn. 116 f.

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 Nr. 2 TKG).

Diese Zweckbindung erhobener Vorratsdaten genügt nach hiesiger Einschätzung der Forderung des EuGH, Vorratsdaten nur zur Verhütung und Feststellung genau definierter schwerer Straftaten den zuständigen Stellen zugänglich zu machen. Der Gerichtshof deutet in seiner Entscheidung vom 8. April 2014 auch die Option an, Vorratsdaten mit Blick auf eine Bedrohung der öffentlichen Sicherheit zu speichern.[71]

Grundsätzlicher Zugang nur zu den Daten von Personen, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein

Nach Ansicht des Gerichtshofs dürfe mit Blick auf die Zweckbindung des Datenzugangs, der Bekämpfung von Straftaten, „*Zugang grundsätzlich nur zu den Daten von Personen gewährt werden, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein*.“[72] In besonderen Situationen, in denen vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind, dürfe „*auch Zugang zu Daten anderer Personen gewährt werden, wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung solcher Aktivitäten leisten könnten.*“

Die Anforderung, dass im Grundsatz nur Zugang zu den Daten von Personen gewährt werden darf, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein, erfüllt die Zugangsregelung des § 113c TKG nicht.

Nach § 113c TKG dürfen die nach § 113b TKG gespeicherten Verkehrsdaten an die Strafverfolgungsbehörde übermittelt werden, soweit diese entsprechende Daten nach § 100g Abs. 2 StPO zu Strafverfolgungszwecken erhoben werden. Dies wiederum erfordert, dass ein durch bestimmte Tatsachen begründeter Verdacht einer schweren Straftat i.S.d. § 100g Abs. 2 StPO besteht und dass jemand diese als Täter oder Teilnehmer begangen oder – soweit der Versuch einer Katalogtat des § 100g Abs. 2 StPO strafbar ist – versucht hat, eine solche zu begehen.[73] Diese Vorschrift setzt allerdings nicht voraus, dass nur solche Verkehrsdaten der in vorstehender Weise in Verdacht stehenden Personen übermittelt werden. Vielmehr ermöglicht sie auch – liegen vorstehende Voraussetzungen vor – die Übermittlung von Verkehrsdaten tatunbeteiligter Personen, ohne dafür einen erhöhten Schwellenwert für den Informationszugang zu normieren, so wie dies der Gerichtshof verlangt. Dieser fordert, dass dafür eine Situation vorliegen müsse, in denen vitale Inte-

---

71 EuGH (Fußn. 43) Rn. 59.

72 EuGH (Fußn. 17), Rn. 119.

73 Vgl. dazu auch die Begründung zu § 100g Abs. 2 StPO des Gesetzentwurfs BT-Drs. 18/5088, S. 32.

ressen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind.

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

Der EuGH fordert, dass der Datenzugang zu den zuständigen nationalen Behörden – außer in hinreichend begründeten Eilfällen – erst nach Entscheidung auf einen mit Gründen versehenen Antrag eines Gerichts oder einer unabhängigen Verwaltungsstelle erfolgen dürfe, der von den zuständigen nationalen Behörden u. a. im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten gestellt wird.[74]

Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten sieht einen Richtervorhalt für die Erhebung von Verkehrsdaten durch die Strafverfolgungsbehörden vor (§ 101a Abs. 1 Satz 2 StPO i.V.m. § 100b StPO). Während die Eilkompetenz der Staatsanwaltschaft für die personenbezogene Anordnung der Erhebung von Verkehrsdaten nach § 100g Abs. 1, 3 StPO besteht, ist die Möglichkeit der Eilanordnung durch die Staatsanwaltschaft für die nach § 100g Abs. 2 StPO verpflichtend zu speichernden Verkehrsdaten ausgeschlossen.[75]

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

Diese 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 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.*

Mitteilung der Zugangsgewährung von auf Vorrat gespeicherten Daten an die betroffenen Personen

Der EuGH erachtet es als wichtig, „*dass die zuständigen nationalen Behörden, denen Zugang zu den auf Vorrat gespeicherten Daten gewährt worden ist, die betroffenen Personen im Rahmen der einschlägigen nationalen Verfahren davon in Kenntnis setzen, sobald die Mitteilung die behördlichen Ermittlungen nicht mehr beeinträchtigen kann*.“[76]

---

74 EuGH (Fußn. 17), Rn. 120.

75 Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten will dies in der Weise sicherstellen, dass für die Fälle des § 100g Abs. 2 StPO 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 ausgeschlossen wird. Vgl. dazu auch die Begründung des Gesetzentwurfs BT-Drs. 18/5088, S. 34 f.

76 EuGH (Fußn. 17), Rn. 121.

Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten trägt diesem Erfordernis mit der Benachrichtigungspflicht nach § 101a Abs. 6 StPO Rechnung.

> *„Die Beteiligten der betroffenen Telekommunikation sind von der Erhebung der Verkehrsdaten nach § 100g zu benachrichtigen. 2§ 101 Absatz 4 Satz 2 bis 5 und Absatz 5 bis 7 gilt entsprechend mit der Maßgabe, dass*
> *1. das Unterbleiben der Benachrichtigung nach § 101 Absatz 4 Satz 3 der Anordnung des zuständigen Gerichts bedarf;*
> *2. abweichend von § 101 Absatz 6 Satz 1 die Zurückstellung der Benachrichtigung nach § 101 Absatz 5 Satz 1 stets der Anordnung des zuständigen Gerichts bedarf und eine erstmalige Zurückstellung auf höchstens zwölf Monate zu befristen ist.“*

Die Betroffenen sind hiernach von der Erhebung der Verkehrsdaten nach § 100g StPO zu benachrichtigen und dabei auf die Möglichkeit des nachträglichen Rechtsschutzes hinzuweisen (§ 101 Abs. 4 Satz 2 StPO). Diese Benachrichtigung darf nur mit Blick auf die Gefährdung des Untersuchungszwecks oder anderer schutzwürdiger Belange nach § 101 Abs. 5 StPO auf Anordnung des zuständigen Gerichts unterbleiben (§ 101 Abs. 6 StPO).

Schutz der erhobenen Vorratsdaten vor unberechtigtem Zugang und unberechtigter Nutzung

Der Gerichtshof betont, dass Art. 15 Abs. 1 RL 2002/58 den Mitgliedstaaten nicht erlaube, von den in Art. 4 Abs. 1 und Abs. 1a RL 2002/58 abzuweichen. „*Nach diesen Bestimmungen haben die Betreiber geeignete technische und organisatorische Maßnahmen zu ergreifen, um zu gewährleisten, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang geschützt sind. Unter Berücksichtigung der Menge an gespeicherten Daten, ihres sensiblen Charakters und der Gefahr eines unberechtigten Zugangs zu ihnen müssen die Betreiber elektronischer Kommunikationsdienste, um die Unversehrtheit und Vertraulichkeit der Daten in vollem Umfang zu sichern, durch geeignete technische und organisatorische Maßnahmen ein besonders hohes Schutz- und Sicherheitsniveau gewährleisten. Die nationale Regelung muss insbesondere vorsehen, dass die Daten im Unionsgebiet zu speichern und nach Ablauf ihrer Speicherungsfrist unwiderruflich zu vernichten sind.*“

Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten normiert in § 113d TKG eine Reihe von Vorgaben zur Gewährleistung der Sicherheit der nach § 113b TKG gespeicherten Daten.

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

Die erforderlichen technischen und organisatorischen Maßnahmen zum Schutze der nach § 113b Abs. 1 TKG zu speichernden Daten sollen nach § 113d Satz 2 TKG 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.

Dem vom EuGH in seiner Entscheidung vom 8. April 2014 durch die Ausgestaltung der VDS nach Maßgabe der vom Gerichtshof für europarechtswidrig befundenen 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, trägt das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten neben stringenteren Anforderungen an den Schutz der erhobenen Daten, deren Verletzung mit Sanktionen[77] bedroht sind, auch insoweit Rechnung, als hiernach Unternehmen für die durch Speicherung und Abruf von Vorratsdaten entstehenden Kosten entschädigt werden können sollen (§ 113a Abs. 2 TKG). Diese setzt allerdings voraus, dass die den Telekommunikationsunternehmen entstehenden Kosten damit abgegolten werden.[78] Eine Kostendeckung dieser Investitionen scheint mit dieser Regelung offenbar nicht angestrebt worden zu sein, wenn eine Entschädigungsmöglichkeit nur solchen Unterneh-

---

77 Diese Regelung sieht eine Verschärfung der bereits bestehenden Sanktionsregelung im TKG vor. Verstöße gegen die Verpflichtungen, die sich hinsichtlich der nach § 113b TKG zu speichernden Daten ergeben, sollen nach § 149 Abs. 2 TKG einheitlich mit einer Geldbuße geahndet werden können. Vgl. dazu auch die Begründung des Gesetzentwurf BT-Drs. 18/5088, S. 44.

78 Das wird in Zweifel gezogen. Der Deutsche Anwaltsverein äußert in seiner Stellungnahme Strafrechts zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (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.) 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

men gewährt werden soll, „*die eine unbillige Härte bei der Durchführung der Speicherverpflichtung nachweisen können*.“[79]

Ob dem EuGH die im Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten 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 dürfte § 113b Abs. 8 TKG entsprechen, wonach die speicherpflichtigen Unternehmen die auf Grund des TKG gespeicherten Daten unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfristen, irreversibel löschen müssen oder die irreversible Löschung sicherzustellen haben.

Dem Erfordernis, dass die Daten im Unionsgebiet zu speichern sind, wird in der Weise Rechnung getragen, dass § 113b Abs. 1 TKG die Speicherung der Vorratsdaten im Inland anordnet. Die Vorgabe, Daten auf Vorrat im Unionsgebiet zu speichern, wird 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[80], ist eine Unvereinbarkeit des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten mit der entsprechenden des EuGH insoweit nicht auszumachen.

Überwachung der Einhaltung des durch EU-Recht gebotenen Schutzniveaus durch eine unabhängige Stelle

Der Gerichtshof verlangt von den Mitgliedstaaten, „*dass die Einhaltung des Schutzniveaus, das das Unionsrecht im Rahmen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten garantiert, durch eine unabhängige Stelle überwacht wird*.“

Dieses Erfordernis wird dadurch erfüllt, dass nach § 113f Abs. 2 TGK die Bundesnetzagentur verpflichtet ist, fortlaufend zu überprüfen, ob alle Anforderungen des Katalogs der technischen Vorkehrungen und sonstigen Maßnahmen erfüllt werden, den die Bundesnetzagentur im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erstellt.

5. Ergebnis

Die Entscheidung des EuGH vom 21. Dezember 2016 misst Regelungen der Mitgliedstaaten zur VDS an Art. 15 Abs. 1 RL 2002/58 und an den Grundrechten der Art. 7, 8, 11 und 52 GRC. Eine von den Mitgliedstaaten eingeführte rechtskonforme VDS muss mithin hiermit vereinbar sein.

---

79 Vgl. dazu die Begründung BT-Drs. 18/5088, S. 37 zu 113a TKG.

80 EuGH (Fußn. 43), Rn. 68.

Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten erfüllt die Vorgaben dieser Entscheidung nicht im vollen Umfang.

Dieses Gesetz erfüllt nicht die Vorgabe des EuGH, dass

- bereits die Speicherung von Vorratsdaten nur bei Vorliegen des Verdachts einer schweren Straftat zulässig ist,
- nur Vorratsdaten solcher Personen gespeichert werden, die Anlass zur Strafverfolgung geben,
- die Vorratsdatenspeicherung sich nicht auf geografisch eingegrenzte Gebiete beschränkt,
- die Vorratsdaten solcher Personen nicht gespeichert werden dürfen, deren davon betroffene Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen,
- grundsätzlich nur Zugang zu den Daten von Personen gewährt wird, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein oder dass in besonderen Situationen, in denen vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind, Zugang zu Daten anderer Personen nur gewährt wird, wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung solcher Aktivitäten leisten können.

Der Entscheidung des EuGH vom 21.12.2016 in den verbundenen Rechtssachen C-203/15 *(Tele2 Sverige AB/Post-och telestryelsen, und C-698/15, Secretary of State fort he Home Department / Tom Watson* u.a) lassen sich letztlich aber nur Gründe dafür entnehmen, weshalb aus Sicht des Gerichtshofs die konkrete Ausgestaltung der VDS durch die verfahrensgegenständlichen Regelungen zweier Mitgliedstaaten, des schwedischen Gesetzes über die elektronische Kommunikation (Lag om elektronisk kommunikation) und des Gesetzes von 2014 zur Vorratsdatenspeicherung und zu den Ermittlungsbefugnissen des Vereinigten Königreichs (Data Retention and Investigatory Powers Act 2014), mit dem Unionsrecht unvereinbar sein sollen. Da diese Wertung Ergebnis einer auf den Detailregelungen vorstehender Vorschriften beruhenden komplexen Abwägung der mit der VDS verfolgten Zielsetzungen und Vorgaben des Art. 15 Abs. 1 RL 2002/58 und der davon betroffenen Grundrechte ist, mit der sicherzustellen ist, dass eine VDS hinsichtlich der Kategorien der zu speichernden Daten, der erfassten Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer auf das absolut Notwendige beschränkt ist und diese daher jeweils nur Geltung für eine konkrete gesetzliche Regelung beanspruchen kann, muss es deshalb der Entscheidung des EuGH vorbehalten bleiben, ob und in welchem Umfang das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten mit dem Unionsrecht vereinbar ist.

- Fachbereich Europa -