

7. September 2015

Gemeinsame Stellungnahme

**zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen
CDU/CSU und SPD zur Einführung einer Speicherpflicht
und einer Höchstspeicherfrist für Verkehrsdaten
(BT-Drs. 18/5171; BT-Drs. 18/5088)**

von

Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten (ARD)

Bundesverband Deutscher Zeitungsverleger (BDZV)

Deutscher Journalisten-Verband (DJV)

Deutscher Presserat

Verband Deutscher Zeitschriftenverleger (VDZ)

Vereinte Dienstleistungsgewerkschaft (dju in ver.di)

Verband Privater Rundfunk und Telemedien (VPRT)

Zweites Deutsches Fernsehen (ZDF)

A.

1. Mit der Rechtsprechung des EuGH zum Verhältnis von Berufsgeheimnis und Vorratsdatenspeicherung sind die vorgeschlagenen Regelungen, insbesondere § 100g Abs. 4 StPO, nicht in Einklang zu bringen.
2. Beim Umgang mit personenbezogenen Daten sind - vor allem im Hinblick auf den Erhalt der journalistischen Berichterstattungsfreiheit - enge rechtliche Grenzen zu wahren. Sowohl das Bundesverfassungsgericht als auch der Europäische Gerichtshof haben diese Grenzen in Entscheidungen konkretisiert. Auch der vorliegende, vom Bundeskabinett am 27. Mai 2015 verabschiedete Gesetzentwurf zur Einführung der Speicherung, Erhebung und Verwendung

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

von Verkehrsdaten auf Vorrat zu Strafverfolgungszwecken und Zwecken der Gefahrenabwehr (Vorratsdatenspeicherung), muss den Anforderungen des Europäischen Gerichtshofs in seinem Urteil vom 8. April 2014 zur Richtlinie 2006/24/EG und denen des Bundesverfassungsgerichts in seinem Urteil vom 2. März 2010 (BVerfGE 125,260) genügen. Das ist nicht der Fall.

3. Die im Entwurf vorgesehene anlasslose Speicherung von u. a. Verkehrsdaten ist weder verfassungsrechtlich noch europarechtlich zu rechtfertigen, da danach deren Erforderlichkeit zu Zwecken der Gefahrenabwehr oder der Strafverfolgung nicht stets zweifelsfrei nachgewiesen werden muss. Die anlasslose Speicherung, Erhebung und sonstige Verwendung solcher Daten auf Vorrat ist mit dem national und auf europäischer Ebene garantierten Recht auf informationelle Selbstbestimmung und den hieraus erwachsenden datenschutzrechtlichen Grundsätzen der Erforderlichkeit und der Datensparsamkeit nicht zu vereinbaren und deswegen unzulässig und stellt in der vorgesehen Form auch einen massiven Eingriff in die Bürgerrechte dar.
4. Die Speicherung, Erhebung und sonstige Verwendung von Telekommunikationsdaten auf Vorrat für Zwecke der Gefahrenabwehr bzw. der Strafverfolgung greift überdies in besonderem Maße in die Vertrauensverhältnisse von Berufsheimnisträgern, hier: der Journalistinnen und Journalisten, ein. Bereits die Speicherung von Telekommunikationsdaten bei Verpflichteten nach dem TKG (§ 113a TKG) ermöglicht, diese vertrauliche Kommunikation nachzuvollziehen. Vorgesehen ist zudem die Erhebung von Standortdaten zum Zwecke der Anfertigung von Bewegungsprofilen. Jede Maßnahme für sich, aber auch deren Verknüpfung, ist geeignet, das Vertrauen in den Informantenschutz nachhaltig zu untergraben bzw. gar nicht erst aufkommen zu lassen. Das gefährdet die journalistische Berichterstattungsfreiheit in nicht hinnehmbarem Maße. Das Vorhaben der Bundesregierung bedarf unter diesem Gesichtspunkt einer besonders strengen Überprüfung. Erst recht ist die Erhebung der Daten für den späteren Zugriff durch Strafverfolgungsbehörden bzw. zur Gefahrenabwehr daraufhin zu untersuchen, ob der Informantenschutz noch effektiv gewährleistet wird. Das ist nach dem vorliegenden Entwurf nicht der Fall.
5. Unter den notwendigen Verfahrensgarantien einer Rechtsordnung ist nach der Rechtsprechung des Europäischen Menschenrechtsgerichtshofs (EGMR) zuerst und vor allem die Garantie notwendig, dass ein Gericht und nicht etwa die Staatsanwaltschaft über Ermittlungsmaßnahmen entscheidet, bevor die Ermittlungsbehörden sich Zugang zu dem Informantenschutz oder dem Redaktionsgeheimnis unterliegenden journalistischen Quellen verschaffen.

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

6. Art. 5 (§ 202d StGB-E) des geplanten Gesetzes ist trotz der vorgesehenen Regelung in § 202d Abs. 3 Nr. 2 StGB-E als eine Schwächung des Informantenschutzes und des Redaktionsgeheimnisses und damit als eine erhebliche Beeinträchtigung der Presse- und Rundfunkfreiheit anzusehen, insbesondere, weil die Ausnahmeregelung in § 202d Abs. 3 StGB-E lediglich journalistische Tätigkeiten in Vorbereitung einer konkreten Veröffentlichung umfasst.

B.

I. Vorhaben der Bundesregierung und der Fraktionen von CDU/CSU und SPD

Mit dem vorgelegten Gesetzentwurf beabsichtigen die Bundesregierung und die Fraktionen von CDU/CSU und SPD, eine Regelung zur zeitlich befristeten Speicherung von Verkehrsdaten und Standortdaten zur Gefahrenabwehr und zur Strafverfolgung zu schaffen. Die damit verbundenen Eingriffe in das Recht auf informelle Selbstbestimmung, die freie Entfaltung der Persönlichkeit, die Kommunikationsgrundrechte und das Fernmeldegeheimnis (Art. 2, 5, 10 GG; Art. 7, 8 und 11 der Grundrechtecharta der Europäischen Union) sollen sich dabei nach Ansicht der Bundesregierung noch in zulässigem Rahmen bewegen.

1) Im Einzelnen sieht der Gesetzentwurf vor:

- a) die Speicherung von Verkehrsdaten (§ 96 Abs. 1 TKG) bei Verdacht einer Straftat mittels Telekommunikation bzw. einer im Einzelfall erheblich bedeutenden Straftat,
- b) die Speicherung von Verkehrsdaten nach § 113b TKG bei auch im Einzelfall besonders schwerwiegenden, im Einzelnen aufgeführten Straftaten,
- c) die Speicherung aller in einer Funkzelle angefallenen Verkehrsdaten bei Verdacht einer Straftat auch im Einzelfall von erheblicher Bedeutung bzw. der nach § 113b TKG angefallenen Verkehrsdaten unter der Voraussetzung des Verdachts einer besonders schweren Straftat,
- d) die Erhebung (bzw. den Abruf) der Daten zu den genannten Zwecken durch die Strafverfolgungsbehörden und die Polizeibehörden sowie durch Telekommunikationsunternehmen für eine Bestandsdatenauskunft nach § 113 Abs. 1 Satz 3 TKG,
- e) einen Richtervorbehalt ohne Eilkompetenz der Staatsanwaltschaften, soweit nicht Verkehrsdaten nach § 96 TKG oder eine Funkzellenabfrage außerhalb des Anwendungsbereichs des § 113b TKG i.V.m. § 100g Abs. 2 StPO betroffen ist,
- f) eine qualifizierte Begründungspflicht für Maßnahmen zur Datenspeicherung hinsichtlich der Erforderlichkeit und Angemessenheit einer Maßnahme,

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

- g) eine Regelung zur Weitergabe der erhobenen Daten an andere Stellen nur unter Einhaltung der o. a. Verwendungszwecke,
 - h) eine Benachrichtigungs- und Anhörungspflicht vor der Entscheidung über die Zulässigkeit einer Anordnung des Abrufs der erhobenen Daten, es sei denn, der Zweck der Anordnung würde gefährdet,
 - i) eine Speicherpflicht, die sich auf die Pflicht zur Speicherung der Daten im Inland bezieht,
 - j) Regelungen zur Datensicherheit,
 - k) Lösungsregelungen entsprechend § 101 Abs. 8 StPO bzw. eine Vorschrift zur irreversiblen Löschung der gespeicherten Daten nach Ablauf der Speicherfristen (10 Wochen bzw. 4 Wochen bei Standortdaten),
 - l) die Speicherungspflicht von Verkehrsdaten auch von Berufsgeheimnisträgern, während die Erhebung dieser Daten durch die genannten Behörden unzulässig sein soll, soweit sie sich gegen eine zeugnisverweigerungsberechtigte Person richtet und die Erhebung voraussichtliche Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte.
- 2) Für die Speicherung in Frage kommende Verkehrsdaten nach § 96 TKG sind:
- a) Nummern oder Kennungen beteiligter Anschlüsse oder Endeinrichtungen, personenbezogene Berechtigungskennungen, Nummern von Kundenkarten sowie Standortdaten mobiler Anschlüsse,
 - b) der Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und Übermittelte Datenmengen,
 - c) der Name des in Anspruch genommenen Telekommunikationsdienstes
 - d) sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.
- 3) Verkehrsdaten nach § 113b TKG sind:
- a) Rufnummern oder Kennungen der beteiligten Anschlüsse,
 - b) Datum und Uhrzeit von Beginn und Ende der Verbindung (inkl. Zeitzone),
 - c) Angaben zur den genutzten Diensten,

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

- d) im Falle mobiler Telefondienste die internationale Kennung der beteiligten Anschlüsse bzw. Geräte sowie das Datum und die Uhrzeit der ersten Aktivierung des Dienstes (inkl. Zeitzone), wenn Dienste im Voraus gezahlt wurden,
 - e) im Fall von Internet-Telefondiensten die Internetprotokolladressen der beteiligten Anschlüsse sowie die zugewiesenen Benutzerkennungen,
 - f) bei der Inanspruchnahme öffentlich zugänglicher Internetzugangsdienste die dem Teilnehmer zugewiesene Internetprotokolladresse, die Kennung des Anschlusses, über die die Internetnutzung erfolgt sowie die zugewiesene Benutzerkennung und Datum und Uhrzeit von Beginn und Ende der Internetnutzung (inkl. der Zeitzone). Bei Inanspruchnahme von Funkzellen sind die zu Beginn der Verbindung genutzten Zellen zu speichern sowie die geografische Lage und die Hauptstrahlrichtung der die jeweilige Funkzelle versorgenden Funkantennen.
- 4) Nicht gespeichert werden dürfen der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post (nach § 113b TKG) sowie Daten von Verbindungen zum Zweck der Beratung in seelischen oder sozialen Notlagen, soweit Personen oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen.

II. Allgemeine Bewertung des Gesetzentwurfs

1) Anwendung europäischen Rechts

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 8. April 2014¹ die Richtlinie zur Vorratsdatenspeicherung in der EU (2006/24/EG) für ungültig erklärt, weil die Richtlinie gegen die Grundrechtecharta der EU, insbesondere gegen Art. 7 und 8 verstieß. Die nach der Richtlinie für eine Dauer von mindestens sechs Monaten zu speichernden Daten entsprachen den Daten, die nunmehr nach der Absicht der Bundesregierung für die Dauer von zehn bzw. vier Wochen zu speichern, zu erheben und unter den vorgesehenen Voraussetzungen zu nutzen sind.

Nachdem die Richtlinie 2006/24/EG als Rechtsgrundlage für die Vorratsdatenspeicherung aufgrund des Urteils des EuGH weggefallen ist, bleibt als europarechtliche Grundlage noch Art. 15

¹ vgl. EuGH, Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom High Court (Irland) und vom Verfassungsgerichtshof (Österreich), Az.: C-293/12 und C-594/12, ZUM-RD 2014,333

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

Abs. 1 der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation), die die Datenspeicherung zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten grundsätzlich zulässt, da durch Verweis auf Art. 6 Abs. 1 und Abs. 2 des Vertrages über die Europäische Union die Mitgliedsstaaten verpflichtet sind, die Charta der Grundrechte der EU zu beachten. Die Gesetzgebung zur Vorratsdatenspeicherung unterliegt damit der Bindung an die Charta².

2) Urteil des EuGH

Der EuGH hat sich bei der Ungültigkeitserklärung der Richtlinie 2006/24/EG vor allem auf die Achtung des Privat- und Familienlebens (Artikel 7 der Grundrechtecharta) und den Schutz personenbezogener Daten (Artikel 8), daneben aber auch auf die Freiheit der Meinungsäußerung und Informationsfreiheit (Artikel 11) gestützt.

Zwar ist nach dem Urteil des EuGH die Speicherung von Verkehrsdaten auf Vorrat zur Bekämpfung von Kriminalität nicht gänzlich ausgeschlossen, weil angesichts der wachsenden Bedeutung elektronischer Kommunikationsmittel die gespeicherten Daten den für die Strafverfolgung zuständigen nationalen Behörden zusätzliche Möglichkeiten zur Aufklärung schwerer Straftaten bieten und daher ein nützliches, geeignetes Mittel für strafrechtliche Ermittlungen darstellen³. Die Bekämpfung schwerer Kriminalität, z. B. des internationalen Terrorismus zur Gewährleistung der öffentlichen Sicherheit sei eine dem Gemeinwohl dienende Zielsetzung⁴.

Der Wesensgehalt der Achtung der Privatsphäre, des Schutzes personenbezogener Daten und der Meinungsfreiheit wird durch eine Vorratsdatenspeicherung nach Ansicht des EuGH nicht zwingend angetastet, solange sie den Inhalt der elektronischen Kommunikation nicht zur Kenntnis gibt, die Grundsätze des Datenschutzes und der Datensicherheit eingehalten werden sowie die Inhalte von Nachrichten und der mit Hilfe eines elektronischen Kommunikationsnetzes abgerufenen Informationen nicht offen gelegt werden⁵.

Dies sei jedoch bei der Vorratsdatenspeicherung, wie sie der EuGH zu beurteilen hatte, nicht der Fall gewesen. Diese beinhalte einen Eingriff in die genannten Grundrechte von großem

² so auch Gesetzentwurf der Bundesregierung, S. 24

³ vgl. Urteil des EuGH, aaO, Rdnr. 49

⁴ vgl. Urteil des EuGH, aaO, Rdnr. 42 ff., 44

⁵ vgl. Urteil des EuGH, aaO, Rdnr. 28, 39 und 40

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

Ausmaß, der als besonders schwerwiegend anzusehen sei⁶. Dieser Eingriff müsse, um rechtmäßig zu sein, nicht nur geeignet sein, die verfolgte Zielsetzung zu erreichen. Er müsse auch erforderlich und verhältnismäßig sein, dürfe also die Grenzen dessen nicht überschreiten, was zur Erreichung des Ziels geeignet und erforderlich sei⁷. Der Gestaltungspielraum des Unionsgesetzgebers, aber auch des nationalen Gesetzgebers, soweit er wie hier an das Unionsrecht gebunden ist, sei, soweit es sich um Grundrechtseingriffe handelt, durch Gesichtspunkte wie den des betroffenen Bereichs, des Wesens des durch die Charta gewährleisteten Rechts, der Art und Schwere des Eingriffs sowie des Zwecks des Eingriffs begrenzt⁸.

Die Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, ist zwar nach der Rechtsprechung des EuGH von größter Bedeutung für die Gewährleistung der öffentlichen Sicherheit und deren Effektivität kann in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen. Der EuGH unterstreicht jedoch, dass diese dem Gemeinwohl dienende Zielsetzung die Erforderlichkeit einer Speicherungsmaßnahme für die Kriminalitätsbekämpfung für sich genommen aber nicht rechtfertigen kann, soweit die Speicherung auf Vorrat, also anlasslos und ohne jede Differenzierung vorgenommen wird⁹.

Nach der Rechtsprechung des EuGH muss eine Regelung zur Vorratsdatenspeicherung klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahme vorsehen sowie Mindestanforderungen, die einen wirksamen Schutz der personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen¹⁰. Dieses Erfordernis gilt insbesondere dann, wenn personenbezogene Daten automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs zu diesen Daten besteht¹¹.

Zudem verlangt der Schutz des Grundrechts auf Achtung des Privatlebens nach der Rechtsprechung des EuGH, dass sich Ausnahmen vom Schutz personenbezogener Daten und die Einschränkungen dieses Schutzes auf das absolut Notwendige beschränken müssen¹². Der Eingriff in das Grundrecht auf Privatsphäre und andere Grundrechte könne nicht als absolut notwendig bezeichnet werden, wenn alle Verkehrsdaten des Telefonfestnetzes, des Mobilfunks, des Internetzugangs und der Internettelefonie gespeichert werden, ohne einen Zusammenhang zwischen

⁶ vgl. Urteil des EuGH, aaO, Rdnr. 37

⁷ vgl. Urteil des EuGH, aaO, Rdnr. 46

⁸ vgl. Urteil des EuGH, aaO, Rdnr. 47

⁹ vgl. Urteil des EuGH, aaO, Rdnr. 51

¹⁰ vgl. Urteil des EuGH, aaO, Rdnr. 54

¹¹ vgl. Urteil des EuGH, aaO, Rdnr. 55

¹² vgl. Urteil des EuGH, aaO, Rdnr. 52

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

den auf Vorrat gespeicherten Daten und einer Bedrohung der öffentlichen Sicherheit zu verlangen¹³ und ohne Ausnahmen vorzunehmen, die für Personen gelten, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen¹⁴.

3) Urteil des Bundesverfassungsgerichts

Das Bundesverfassungsgericht kommt in seinem Urteil vom 2. März 2010¹⁵ zu dem Schluss, dass eine anlasslose Speicherung von Verkehrsdaten für qualifizierte Verwendungen im Rahmen der Strafverfolgung, der Gefahrenabwehr und der Aufgaben der Nachrichtendienste nicht per se und schlechthin mit dem Grundgesetz, insbesondere dem durch Art. 10 GG gewährleisteten Brief- und Fernmeldegeheimnis, unvereinbar ist¹⁶. Das Bundesverfassungsgericht lässt sich dabei, anders als der EuGH, von der Überlegung leiten, dass durch die anlasslose Vorratsdatenspeicherung „Aufklärungsmöglichkeiten geschaffen (werden), die sonst nicht bestünden und angesichts der zunehmenden Bedeutung der Telekommunikation auch für die Vorbereitung und Begehung von Straftaten in vielen Fällen erfolgversprechend sind.“¹⁷ Diese Speicherung von Verkehrsdaten zu Zwecken der Kriminalitätsbekämpfung sei nicht nur geeignet, sondern auch erforderlich¹⁸ und unter genau bestimmten Voraussetzungen¹⁹ auch verhältnismäßig²⁰.

Das Bundesverfassungsgericht hat allerdings empirische Befunde zur Vorratsdatenspeicherung nicht berücksichtigen können, da diese erst nach der Entscheidung veröffentlicht wurden. Es hat jedoch darauf hingewiesen, dass eine Gesetzgebung zur Vorratsdatenspeicherung zwar nicht berücksichtigen müsse, dass das Regelungsziel in jedem Einzelfall tatsächlich erreicht wird. Wohl aber werde von der Gesetzgebung verlangt, dass durch sie die Zweckerreichung zumindest gefördert wird²¹.

Ebenso wie der EuGH geht das BVerfG daher von der Nützlichkeit der Vorratsdatenspeicherung für die Bekämpfung von Kriminalität aus, anders als der EuGH bejaht es aber auch deren Erforderlichkeit per se. Beide Gerichte sind sich jedoch einig darin, dass ein Zusammenhang

¹³ vgl. Urteil des EuGH, aaO, Rdnr. 56 und 59

¹⁴ vgl. Urteil des EuGH, aaO, Rdnr. 58

¹⁵ vgl. BVerfGE 125, 260 ff

¹⁶ vgl. BVerfGE, aaO, S. 316 ff

¹⁷ vgl. BVerfGE, aaO, S. 317

¹⁸ vgl. BVerfGE, aaO, S. 318

¹⁹ vgl. dazu im Einzelnen BVerfGE, aaO, S. 325 ff

²⁰ vgl. BVerfGE, aaO, S. 321

²¹ vgl. BVerfGE, aaO, S. 317f mit Hinweis auf BVerfGE 63, 88[115]; 67, 157[175]; 96, 10[23]; 103, 293[307]

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit bestehen muss²², bzw. dieser Zusammenhang mindestens durch die Förderung der Zweckerreichung²³ hergestellt wird.

4) Anlasslose Speicherung zulässig?

Einen Nachweis über einen Zusammenhang zwischen der anlasslosen Vorratsdatenspeicherung und der Bekämpfung von Kriminalität enthält der vorliegende Gesetzesentwurf nicht. Er nimmt auch nicht substantiiert dazu Stellung, ob und inwiefern der verfolgte Zweck durch das Gesetz gefördert wird.

Der Entwurf äußert sich zudem nur an wenigen Stellen und sehr allgemein zur Erforderlichkeit der Gesetzgebung. So wird nur abstrakt ausgeführt, dass die Einführung einer gesetzlichen Pflicht zur Speicherung von Verkehrsdaten durch die Erbringer öffentlich zugänglicher Telekommunikationsdienste erforderlich sei, um Lücken der Strafverfolgung und der Gefahrenabwehr im Einzelfall zu schließen und damit dem verfassungsrechtlichen Gebot einer effektiven Strafverfolgung zu genügen²⁴. Zudem werden „Unzulänglichkeiten bei der Strafverfolgung und der Gefahrenabwehr“²⁵ sowie Urteile des EGMR²⁶ und des EuGH²⁷ zur Begründung der Notwendigkeit des Gesetzes angeführt.

Diese undifferenzierte und damit pauschale Begründung vermag die Erforderlichkeit der Vorratsdatenspeicherung nicht zu rechtfertigen. Der Gesetzgeber muss auf der Grundlage ihm vorliegender Daten nachvollziehbar darlegen, aus welchen Gründen und in welcher Weise er Maßnahmen trifft, wenn er - wie vorliegend - einen Einschätzungs- und Beurteilungsspielraum in Anspruch nimmt²⁸.

²² vgl. EuGH, aaO, Rdnr. 59

²³ vgl. die Rspr. bei Fn 21

²⁴ vgl. Regierungsentwurf, S. 1

²⁵ vgl. Regierungsentwurf, S. 22

²⁶ vgl. Regierungsentwurf, aaO, Urteil des EGMR, Nr. 2872/02 vom 2. Dezember 2008 (- K.U. v. Finnland), wonach positive Pflichten für die Staaten bestehen, das materielle Strafrecht in der Praxis durch effektive Ermittlung und Verfolgung anzuwenden

²⁷ vgl. aaO, Urteil des EuGH in Sachen Digital Rights, Az: C-293/12 und C-564/12, Rdnr. 42, allerdings unterlässt es die Begründung im Regierungsentwurf, darauf hinzuweisen, dass der EuGH an anderer Stelle sehr deutlich die Erforderlichkeit von Speicherungsmaßnahmen für die Kriminalitätsbekämpfung verneint, siehe Rdnr. 51

²⁸ vgl. BVerfGE 79, 311 (344)

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

Das Max-Planck-Institut für ausländisches und internationales Strafrecht (MPI) hat in einem 2011 veröffentlichtem Gutachten zu „Schutzlücken durch Wegfall der Vorratsdatenspeicherung?“²⁹ dargelegt, dass „die Aufklärungsquote in Deutschland in keinem Fall unter den für die Schweiz mitgeteilten Aufklärungsquoten liegt. Vielmehr liegen die Aufklärungsquoten teilweise deutlich höher. Dies gilt auch für solche Delikte, für die die besondere Bedeutung des Zugriffs auf Telekommunikationsverkehrsdaten hervorgehoben wird (also Computerbetrug, Verbreitung von Pornografie (einschließlich Kinderpornografie) oder Drohung).“³⁰ Relevant ist dieses Ergebnis deswegen, weil in der Schweiz seit 2001 so genannte Randdaten der Telekommunikation auf Vorrat gespeichert werden, wobei diese Daten die Obergruppe zu den Verkehrsdaten darstellen, die hier in Rede stehen.³¹

In dem Gutachten, dem außer eigenen Erhebungen auch Interviews mit Praktikern aus der Strafverfolgung zu Grunde liegen, kommt das MPI im Übrigen zu dem Ergebnis, dass geeignete, belastbare Daten, die zu einer quantitativen Überprüfung der Auswirkungen der Vorratsdatenspeicherung auf die Aufklärungsquote führen könnten, bislang nicht erfasst werden und auch nicht systematisch erfasst werden sollen. Die auf Einzelfälle gegründete Argumentation zugunsten der Vorratsdatenspeicherung weise den Einzelfall als „typisch“ aus, ohne dass diese Einordnung empirisch belegt oder belegbar wäre³².

Zu einem vergleichbaren Ergebnis kommt der wissenschaftliche Dienst des Bundestages in einem Rechtsgutachten aus dem Jahr 2011. Darin wird auf der Grundlage von Zahlen des BKA eine Steigerung der Aufklärungsquote um sechs/Tausendstel Prozent angegeben, wenn die Vorratsdatenspeicherung angewandt wird³³.

Die polizeiliche Kriminalitätsstatistik zeigt zudem auf, dass in den Deliktgruppen, in denen die Relevanz der Telekommunikationsverkehrsdaten bzw. der Zugriff auf diese besonders betont wird, in den letzten Jahren 2014 und 2013 keine signifikant schlechteren Aufklärungsquoten ausgewiesen werden³⁴.

²⁹ vgl. <https://www.mpg.de/5000721/vorratsdatenspeicherung.pdf>; vgl. dazu auch BT-Drs. 18/4971

³⁰ vgl. Fn. 29, aaO, S. 123

³¹ vgl. dazu https://de.wikipedia.org/wiki/Randdaten_%28bei_der_Nutzung_elektronischer_Infrastruktur%29

³² vgl. Gutachten MPI, S. 218 (219)

³³ vgl. Rechtsgutachten des wissenschaftlichen Dienstes des Deutschen Bundestages vom 25.02.2011, S.20 WD 11-3000-18/11, mit Berufung auf: Gietl, Die Einführung der Vorratsdatenspeicherung, K&R 2007, S. 545-550 (552)

³⁴ vgl. www.bka.de, Publikationen/Polizeiliche Kriminalstatistik

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

Nach alledem besteht erheblicher Zweifel daran, dass die vorgesehene Gesetzgebung zur Einführung der Vorratsdatenspeicherung auch nur die Möglichkeit bietet, die verfolgte Zielsetzung der effektiven Bekämpfung der Kriminalität zu fördern. Jedenfalls aber ist ein Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit nicht erkennbar. Es ist daher auch nicht verwunderlich, dass sich die Bundesregierung in ihrem Gesetzentwurf nicht mit den (wenigen) vorliegenden Daten auseinandersetzt, sondern sich in allgemeine Aussagen über angebliche Strafbarkeits- und Gefahrenabwehrlücken flüchtet.

III. Zu einzelnen Regelungen des Gesetzentwurfs

1) Schutz der Berufsgeheimnisse, § 100g Abs. 4 StPO-E

Der Gesetzentwurf will durch § 100g Abs. 4 StPO ein grundsätzliches Verbot der Erhebung von Verkehrsdaten regeln, die sich gegen die in § 53 Abs. 1 Nr. 1 bis 5 StPO genannten Personen richtet. Da es nicht möglich sei, die Berufsgeheimnisträger in ihrer Gesamtheit schon von der Speicherung ihrer Verkehrsdaten auszunehmen, zumal diese „in vielen Fällen nicht über statische, sondern über dynamische IP-Adressen“ verfügten, ergebe sich der „bessere Schutz“ durch eine Regelung, die die Verwendung der gespeicherten Daten ausschließe. Dieser Schutzmechanismus habe sich in der StPO auch an anderer Stelle bewährt³⁵.

Mit der Vorschrift des § 100g Abs. 4 StPO knüpft der Entwurf an die Regelung des § 160a StPO an. Anders als § 160a StPO unterscheidet § 100g Abs. 4 StPO-E jedoch nicht zwischen den verschiedenen Gruppen der Berufsgeheimnisträger nach § 53 StPO³⁶. Das ist zu begrüßen, ändert jedoch nichts an der grundsätzlichen Kritik der hier Stellung nehmenden Organisationen³⁷ auch an dieser Vorschrift, insbesondere an § 160a Abs. 2 StPO. Die Norm bietet nämlich entgegen der Annahme der Bundesregierung³⁸ keinen ausreichenden Schutz davor, mit Hilfe staatlicher Maßnahmen die Person des Informanten zu ermitteln.

Verkehrsdaten haben nach der Rechtsprechung des Bundesverfassungsgerichts³⁹ einen besonders schutzwürdigen Aussagegehalt, weil sie im Einzelfall erhebliche Rückschlüsse auf das Kommunikations- und Bewegungsverhalten der Telekommunikationsnutzer zulassen. Deren

³⁵ vgl. Regierungsentwurf, S. 37

³⁶ vgl. Regierungsentwurf, aaO

³⁷ vgl. Rechtsausschuss des Deutschen Bundestages, öffentliche Anhörung am 26.01.2011: Stellungnahme von ARD, BDZV, DJV, Deutscher Presserat, VDZ, Ver.di, VPRT und ZDF vom 19.01.2011, S. 23ff

³⁸ vgl. BT-Drs. 16/11170, S. 5

³⁹ BVerfG AfP 2003, 138 (143); BVerfG NJW 2006, 976 (980 f.); BVerfGE 125, 260 (319)

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

Speicherung für Strafverfolgungszwecke und der staatliche Zugriff können in der Folge die Unbefangenheit des Kommunikationsaustausches und das Vertrauen in den Schutz der Unzugänglichkeit der Telekommunikationsanlagen zunehmend gefährden⁴⁰ bzw. ein Gefühl der Überwachung erzeugen, das mit dem Menschenwürdebild des Grundgesetzes unvereinbar ist.

Der den Verkehrsdaten der Telekommunikation zugeschriebene Aussagegehalt trifft alle Telekommunikationsvorgänge, insbesondere auch die Telekommunikation zwischen Journalistinnen und Journalisten und ihren Informantinnen und Informanten bzw. die berufliche Telekommunikation untereinander. Die berufliche Kommunikation von Journalistinnen und Journalisten wird im Hinblick auf Telekommunikationsvorgänge nicht nur durch Art. 5 Abs. 1 S. 2 GG, sondern auch durch Art. 10 Abs. 1 GG geschützt⁴¹.

Nach der ständigen Rechtsprechung sowohl des Bundesverfassungsgerichts, wie auch des Bundesgerichtshofs ist die Ausforschung der die Informanten schützenden Daten⁴² nicht zulässig⁴³. Der Schutz der Informanten umfasst nach dieser Rechtsprechung nicht nur den Inhalt der Mitteilung und den Namen des Informanten, sondern auch alle Umstände, aus denen sich eine Identifikation von Informanten ergeben könnte. Ausdrücklich wird dies in § 53 Abs. 2 S. 3 StPO seit 2002 gesetzlich geregelt. Danach kann der Zeuge auch in ansonsten der Zeugnispflicht unterliegenden Fällen die Aussage verweigern, soweit sie „zur Offenbarung der Person des Verfassers oder Einsenders (...) oder des sonstigen Informanten“ führen würde. Sowohl die Rechtsprechung wie auch die zitierte gesetzliche Regelung wird damit begründet, dass es mit Art. 5 Abs. 1 S. 2 GG nicht vereinbar sei, wenn der Schutz journalistischer Quellen sich lediglich auf den Inhalt der gemachten Mitteilung beziehe, nicht aber auf die Umstände, die zur Identifikation des Informanten führen. Müssten solche Umstände offenbart werden, würde die Presse- und Rundfunkfreiheit bei nicht öffentlich zugänglichen sensiblen Materien leer laufen, denn kaum ein Informant würde sich ohne Wahrung der Vertraulichkeit dem Risiko seiner Identifikation und eventuellen Maßregelung aussetzen. Die Pressefreiheit als Institution würde Schaden nehmen.⁴⁴ Dies widerspricht der ständigen Rechtsprechung des Bundesverfassungsgerichtes.

Nichts anderes kann gelten, wenn mit Hilfe von Verkehrsdaten das Kommunikations- und Bewegungsverhalten von Journalistinnen und Journalisten und ihrer potenziellen Informanten auf

⁴⁰ BVerfGE 100, 313 (381); BVerfGE 125, 260 (310); EuGH, aaO (Fn. 1), Rdnr. 66

⁴¹ BVerfGE 107, 299; OLG Dresden AfP, 2007, 577 (578)

⁴² z.B. Umstände von Treffen mit Informanten, ggf. Zahlungsbeträge, Örtlichkeiten, Zeiten usw.

⁴³ vgl. BVerfG, NStZ 1982, 253 (254); BGH NJW 1990, 525 (526) m.w.N.

⁴⁴ vgl. Achenbach, in: Löffler, Presserecht, 5. Aufl. 2006, § 23 LPG, Rdnr. 25.

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

Vorrat gespeichert werden soll, um bei Bedarf auf diese Daten zugreifen zu können. Über Abgleiche von Bewegungsverhalten könnten zudem auch persönliche Treffen nachvollzogen werden.

Eine grundrechtlich geschützte Presse- und Rundfunkfreiheit kann nicht verwirklicht werden, wenn die ungehinderte Informationsbeschaffung und eine vertrauliche Kommunikation der Medien insbesondere mit den Informanten nicht mehr möglich sind. Potenzielle Informanten würden ihre Kenntnisse nicht weiter geben, wenn sie sich nicht darauf verlassen könnten, dass die Journalistinnen und Journalisten ihre Quellen nicht preisgeben. Es geht dabei nicht ausschließlich um den Schutz der Quellen, sondern auch um den Schutz des Redaktionsgeheimnisses, dem das BVerfG in ständiger Rechtsprechung eigenständige Bedeutung zumisst und in das eingegriffen würde, wenn die im Bereich journalistischer Recherche hergestellten Kontakte staatlich ausgeforscht würden⁴⁵ oder nachvollzogen werden können.

Die für den öffentlichen Meinungsbildungsprozess wichtige Aufgabe der Journalistinnen und Journalisten, Missstände an die Öffentlichkeit zu bringen, ist massiv gefährdet, wenn Informanten befürchten müssen, dass ihre Informationen nicht vertraulich bleiben, sondern z.B. durch die Herausgabe von Verkehrsdaten etc. personalisiert werden können. Dasselbe gilt, wenn Journalistinnen und Journalisten zudem damit rechnen müssten, dass ihre Kontakte staatlicherseits ausgeforscht werden können.

Das Bundesverfassungsgericht hat es in seinem Urteil zur Vorratsdatenspeicherung verfassungsrechtlich für geboten erachtet, zumindest für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen ein grundsätzliches Übermittlungsverbot vorzusehen⁴⁶. Begründet hat es diese Rechtsprechung mit der notwendigen Einhaltung des Verhältnismäßigkeitsgrundsatzes. Es hat dabei nicht ausdrücklich alle Gruppen von Berufsheimnisträger(innen) im Sinne des § 53 StPO erwähnt, sondern als Beispiel für auf besondere Vertraulichkeit Angewiesene auf seelsorgerische Tätigkeiten im Hinblick auf die Regelung in § 99 Abs. 2 TKG abgestellt. Deren Daten dürfen jedenfalls an staatliche Stellen nicht übermittelt werden, wenn sie sich bei der Bundesnetz-Agentur haben registrieren lassen, § 113b Abs. 6 TKG-E. Eine solche Registrierung kommt jedoch für Journalistinnen und Journalisten nicht in Betracht, sie würde ihrerseits gegen Art. 5 Abs. 1 S. 2 GG verstoßen⁴⁷. Aus diesem Umstand kann allerdings nicht der Schluss gezogen werden, dann komme nur noch ein

⁴⁵ vgl. BVerfGE 117, 244 (259) mit Hinweis auf BVerfGE 66, 116 (133 ff); 107, 299 (331)

⁴⁶ vgl. BVerfGE 125, 260 (334)

⁴⁷ Die Ausübung des journalistischen Berufs kann von einer „wie immer gearteten Berufszulassung“ nicht abhängig gemacht werden, Degenhart, Bonner Kommentar GG, Rdnr. 441, 122. Aktualisierung, 2006

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

Verwertungsverbot in Betracht, wie es grundsätzlich in § 100g Abs. 4 StPO-E vorgesehen⁴⁸ ist, denn bereits die Erhebung und Speicherung ist geeignet, Vertrauensverhältnisse zu unterbinden. Die Bereichsausnahme für den journalistischen Bereich muss daher bereits bei der Datenspeicherung ansetzen.

Wenn das BVerfG mindestens ein Übermittlungsverbot für auf besondere Vertraulichkeit angewiesene Telekommunikationsverbindungen als verfassungsrechtlich geboten erachtet, kann ein Verwertungsverbot allein diesen Anforderungen nicht genügen, denn es setzt die Übermittlung voraus. Genügt daher ein Verwertungsverbot den Anforderungen nicht und kommt ein Übermittlungsverbot rechtlich und tatsächlich nicht in Betracht, muss schon die Speicherung der besonders zu schützenden Telekommunikationsverbindungen unterbleiben. Diese Konsequenz hat der EuGH⁴⁹ ebenfalls aufgezeigt.

Die Notwendigkeit des Schutzes der Berufsgeheimnisträger wird vom EuGH in der Entscheidung zur Richtlinie 2006/24/EG generell höher eingestuft, als nach dem Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung. Hinsichtlich der Frage, ob der mit einer Vorratsdatenspeicherung verbundene Eingriff in die Rechte aus Artikel 7 und Artikel 8 der Charta auf das absolut Notwendige beschränkt ist, hat der EuGH nicht nur moniert, dass die anlasslose Vorratsdatenspeicherung unterschiedslos alle Personen betrifft, die elektronische Kommunikationsmittel benutzen. Er hat vor allem auch kritisch angemerkt, dass nach der Richtlinie 2006/24/EG keinerlei Ausnahme für Personen vorgesehen war, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen⁵⁰.

Die Notwendigkeit des Schutzes gerade der journalistischen Arbeit und des dafür essentiellen Quellenschutzes wird auch durch die Rechtsprechung des EGMR unterstrichen. Der Schutz der journalistischen Quellen ist danach von vitaler Bedeutung für die Pressefreiheit⁵¹. Er wird als eine der Grundvoraussetzungen der Pressefreiheit angesehen. Potenzielle Quellen ohne diesen Schutz könnten davon abgehalten werden, die Presse dabei zu unterstützen, die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren. Der Gerichtshof betont, dass ohne den Schutz der Quellen eines Journalisten die wichtige öffentliche Kontrollfunktion der Presse untergraben werden könnte und die Fähigkeit der Presse, genaue und verlässliche Informationen zu liefern, negativ beeinflusst werden könnte⁵². Eine Anordnung zur Preisgabe von Quellen könne nicht nur eine nachteilige Wirkung auf die Quelle selbst haben, sondern auch

⁴⁸ vgl. die Position der Bundesregierung, Fn. 35

⁴⁹ vgl. EuGH, Fn. 1, Rdnr. 59

⁵⁰ vgl. EuGH, aaO, Rdnr. 58

⁵¹ vgl. EGMR, Case of Sanoma Uitgevers B.V. v. The Netherlands, no. 38224/04, judgment. 14/09/2010, Rdnr. 88

⁵² vgl. EGMR, Case of Goodwin v. The United Kingdom, no. 17488/90, judgment 27/03/1996, Rdnr. 39

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

z. B. auf die Zeitung oder den Sender, deren Glaubwürdigkeit dadurch in Gefahr gerate, und auf die Öffentlichkeit, die ein Interesse daran habe, Informationen zu erhalten, die (auch) aus anonymen Quellen stammten⁵³. Das gilt auch dann, wenn eine Information öffentlich eingeholt wurde und keine besondere Geheimhaltungspflicht besteht. Ein Eingriff in den Informantenschutz sei bereits in der Aufforderung einer Behörde zu sehen, die Quelle preis zu geben⁵⁴. Auch wenn eine Anordnung nicht vollstreckt wird, ist sie als Verstoß gegen den durch Art. 10 EMRK geschützten Quellenschutz zu qualifizieren, wenn damit bezweckt werden soll, dass die Identität einer anonymen Quelle offen zu legen ist⁵⁵.

Die überragende Bedeutung, die der Presse- und Rundfunkfreiheit für das Gemeinwesen und die Demokratie zukommt und die ohne Quellenschutz und den Schutz des Redaktionsgeheimnisses nicht auskommen, sowie die Anforderung des EuGH, Telekommunikationsverbindungen der Berufsgeheimnisträger bereits aus der Speicherpflicht herauszunehmen und schließlich der Hinweis des BVerfG, die Daten von besonders auf Vertraulichkeit angewiesene Telekommunikationsverbindungen mindestens nicht zu übermitteln, lassen nach Ansicht der Stellungnehmenden Organisationen nur den Schluss zu, dass die Erhebung und Speicherung insgesamt zu unterbleiben hat. Jedenfalls dürfte die vorgeschlagene Regelung zu § 100g Abs. 4 StPO, die lediglich ein Verwertungsverbot vorsieht, mit der Rechtsprechung des EuGH wie dargestellt, nicht vereinbar sein.

§ 100g Abs. 4 StPO stellt hinsichtlich des Schutzes der Berufsgeheimnisträger vor einer Verwertung ihrer Verkehrsdaten darauf ab, dass die Erhebung von Verkehrsdaten nach Absatz 2 unzulässig ist, wenn sie sich gegen eine der in § 53 Abs. 1 S. 1 Nr. 1 bis 5 StPO genannten Personen richtet und sie voraussichtlich Erkenntnisse erbringen würde, über die diese Personen das Zeugnis verweigern dürften. Die Formulierungen „die voraussichtlich Erkenntnisse erbringen würde“ sowie „diese das Zeugnis verweigern dürfte“ sind ersichtlich aus § 160a StPO übernommen worden. Dafür spricht auch, dass nach § 100g Abs. 4 S. 6, § 160a Abs. 3 und 4 entsprechend gelten sollen.

Damit kommt die Bundesregierung den Anforderungen des BVerfG⁵⁶ scheinbar nach, besonders auf Vertraulichkeit angewiesene Telekommunikationsverbindungen weitergehend zu schützen. Jedoch ist dieser Schutz bei näherer Betrachtung als Einzelfallregelung ausgestaltet und führt somit keineswegs zu einem generellen Schutz vor der Auswertung und Verwendung

⁵³ vgl. EGMR, Case of Sanoma Uitgevers B.V. v. The Netherlands, no. 38224/04, aaO, Rdnr. 89

⁵⁴ vgl. EGMR, British Broadcasting Corporation v. The United Kingdom, no. 25798/94, judgment 18/01/1996, 4

⁵⁵ vgl. EGMR, Financial Times Ltd. v. The United Kingdom, no. 821/03, judgment 15/12/2009, Rdnr. 70

⁵⁶ vgl. BVerfGE 125, 260 (334)

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

der gespeicherten Daten. Die Unzulässigkeit der Erhebung bzw. des Abrufes durch die berechnigte Behörde nach § 100g Abs. 4 StPO setzt nämlich voraus, dass die Maßnahme sich gegen eine zeugnisverweigerungsrechtliche Person richtet **und** voraussichtlich Erkenntnisse erbringen würde, über die eine Journalistin oder ein Journalist das Zeugnis verweigern dürfte, oder dass sie sich zwar nicht gegen eine solche Person richtet, gleichwohl aber Erkenntnisse erlangt werden, über die eine zeugnisverweigerungsrechtliche Person keine Aussage machen bräuchte.

Diese Regelung ist im Hinblick auf die Tragweite und die Anwendung der Übermittlung bzw. des Abrufs der damit zusammenhängenden Verkehrsdaten weder klar noch präzise im Sinne des Urteils des EuGH⁵⁷. Einen wirksamen Schutz vor der Übermittlung bzw. dem Abruf von Verkehrsdaten von Journalistinnen und Journalisten bietet die Regelung jedenfalls nicht.

Mit den gewählten Formulierungen sind zudem Prognoseentscheidungen verbunden, nämlich die, ob der Adressat des Verkehrsdatenabrufs ein Berufsgeheimnisträger ist bzw. ein solcher in die Ermittlungsmaßnahme involviert ist und ob der Abruf der Verkehrsdaten voraussichtlich Erkenntnisse zu Tage fördern würde oder erbringt, die in den Schutzbereich des Berufsgeheimnisses fallen würden. Mag die Identifizierung einer Person als Berufsgeheimnisträger in vielen oder sogar den meisten Fällen noch ohne großen Aufwand möglich sein, ist die Prognose, ob zur Verweigerung des Zeugnis berechtigende Erkenntnisse erlangt würden, ohne Kenntnis der Verkehrsdaten kaum möglich. Oder anders gewendet: beantragende Behörden müssten im Regelfall davon ausgehen, dass die Verkehrsdaten, die sie erheben wollen, keine die Zeugnisverweigerung betreffenden Erkenntnisse erbringen.

Mit den gleichen Prognosevoraussetzungen haben es Behörden und Gerichte bei der Anwendung des § 160a StPO zu tun. Zu dieser Vorschrift wird davon ausgegangen, dass „nur dann ex ante von der Unzulässigkeit der Maßnahme auszugehen (ist), wenn ausreichende äußere Anzeichen, also konkrete tatsächliche Anhaltspunkte, vorliegen, dass (...) geschützte Erkenntnisse zu erwarten sind.“⁵⁸ M.a.W. liegen solche Anhaltspunkte nicht vor, ist von der Zulässigkeit der Maßnahme auszugehen, denn die Erhebung ist danach nur unzulässig, wenn „zweifelsfrei erkannt wird, dass schutzrelevante Inhalte Gegenstand der Erhebung sind.“⁵⁹

Angesichts der mit den in § 100g Abs. 4 StPO-E verwendeten Formulierungen und den damit verbundenen Schwierigkeiten, zweifelsfrei zu erkennen, ob schutzrelevante Erkenntnisse mit

⁵⁷ vgl. Urteil des EuGH, aaO, Rdnr. 54

⁵⁸ vgl. KK-StPO/Griesbaum, StPO, § 160a Rdnr. 6, 7. Auflage 2013

⁵⁹ vgl. KK-StPO, aaO, Rdnr. 6

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

dem Abruf der Verkehrsdaten verbunden sein würden oder auch, ob der Adressat eine Journalistin oder ein Journalist ist, muss davon ausgegangen werden, dass Strafverfolgungsbehörden auch bei § 100g Abs. 4 StPO-E - bei Vorliegen der übrigen Voraussetzungen der Erhebung - grundsätzlich die Zulässigkeit des Abrufs von Verkehrsdaten bei Berufsheimnisträgern annehmen würden.

Auch hinsichtlich des der unzulässigen Erhebung nachgelagerten Verwendungs- bzw. Verwertungsverbots muss angenommen werden, dass dieses wie bei § 160a StPO nur dann zum Zuge kommen soll, wenn sich „zweifelsfreie Hinweise ergeben, dass geschützte Erkenntnisse anfallen oder angefallen sind.“⁶⁰

Der vermeintliche Schutz der Berufsheimnisträger nach § 100g Abs. 4 erweist sich damit im Hinblick auf den Abruf der Verkehrsdaten und möglicherweise ihre weitere Verwendung als weitgehend wirkungslos. Berufsheimnisträger sind dem Entwurf nach vor der Speicherung der Verkehrsdaten nicht und vor deren Erhebung nur dann geschützt, wenn und solange Strafverfolgungsbehörden und Ermittlungsgerichte nicht aufgrund fehlender zweifelsfreier Erkenntnisse von der grundsätzlichen Zulässigkeit des Abrufs der Verkehrsdaten ausgehen können. Dabei tritt der Umstand hinzu, dass Strafverfolgungsbehörden nicht verpflichtet sind, für die zu erstellende Prognose besondere Ermittlungen durchzuführen⁶¹.

Es ist für die an dieser Stellungnahme beteiligten Medienunternehmen und -verbände unverständlich, warum der Gesetzesentwurf auf jegliche Anstrengung verzichtet, den Schutz der Berufsheimnisträger - wie rechtlich geboten - bereits auf der Ebene der Speicherung vorzunehmen. Dies alleine, wie der Gesetzesgründung zu entnehmen ist, mit der Feststellung abzutun „Die Berufsheimnisträger in ihrer Gesamtheit schon von der Speicherung ihrer Verkehrsdaten auszunehmen, ist nicht möglich.“⁶² geht sowohl an den praktischen Gegebenheiten als auch an der rechtlichen Ausgangslage, nämlich der Pflicht des Gesetzgebers zu genau solchen Anstrengungen, vorbei.

Für die Sendeanstalten und -unternehmen, die Verlagshäuser und andere Institutionen des Medienbereichs und damit für deren Beschäftigte stehen sowohl die IP-Nummernkreise als auch die Festnetztelefonnummern und in vielen Fällen auch die dienstlichen Mobilfunknummern fest. Sie sind bereits heute den TK-Providern als Bestandsdaten speziell von Medienunternehmen und Journalistinnen und Journalisten bekannt. Aus diesem Grunde wäre eine Regelung

⁶⁰ vgl. KK-StPO, aaO, Rdnr. 7

⁶¹ vgl. KK-StPO, aaO, Rdnr. 6

⁶² vgl. Regierungsentwurf, S. 37

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

geboten, für diese Anschlüsse auf die Speicherung der Verkehrsdaten zu verzichten. Eine Registrierung bei der Bundesnetzagentur, wie sie § 99 Abs. 2 des Telekommunikationsgesetzes (TKG) für die Seelsorge und die Beratungsstellen vorsieht, wäre, da es hier nur auf die Kenntnis der TK-Provider ankommt, entbehrlich. Diese Registrierung wäre (s.o.) als Verstoß gegen Art. 5 Abs. 1 S. 2 GG auch unzulässig.

Insgesamt ist es höchst zweifelhaft, ob die bislang vorgesehene Regelung mit der vom Bundesverfassungsgericht festgestellten Ausprägung des Verhältnismäßigkeitsgrundsatzes vereinbar ist, wonach bereits ein Übermittlungsverbot von durch die Vorratsdatenspeicherung gewonnenen Daten für einen engen Kreis von auf besondere Vertraulichkeit angewiesene Berufsgeheimnisträger gilt. Mit der Rechtsprechung des EuGH zum Verhältnis von Berufsgeheimnis und Vorratsdatenspeicherung ist die vorgeschlagene Schutzregelung nicht in Einklang zu bringen.

Problematisch ist die Regelung vor allem aber auch hinsichtlich der Personen, um deren Willen Journalistinnen und Journalisten ein Zeugnisverweigerungsrecht haben. Das Verbot der Erhebung der Verkehrsdaten bzw. das Verbot des Abrufs geht ins Leere, wenn Adressat dieser Maßnahme nicht die Journalistin oder der Journalist ist, sondern die potenzielle Informantin bzw. der potenzielle Informant. Staatliche Stellen können sich insoweit trotz der Regelung in § 100g Abs. 4 StPO dann Einblick in die journalistische Arbeit verschaffen, wenn der Abruf beim vermuteten Informanten erfolgt.

2) Zu § 101a StPO-E

In § 101a Abs. 1 wird der für Verkehrsdaterhebungen nach § 100g wesentliche Richtervorbehalt geregelt. Hierbei wird nach der Art der gespeicherten Daten differenziert. Durch die Vorschrift des Abs. 1 S. 2 werden für die Fälle des § 100g Abs. 2, auch in Verbindung mit § 100g Abs. 3 S. 2, die § 100b Abs. 1 S. 2 und 3 von der Anwendung ausgenommen. Damit ist zwar sichergestellt, dass für die Erhebung der auf Vorrat zu speichernden Daten die Möglichkeit einer Eilanordnung durch die Staatsanwaltschaft bei Gefahr im Verzug nicht gegeben ist; aber es bleibt hinsichtlich des Richtervorbehalts bei der Regelung in Absatz 1 Satz 1. Danach ist eine Eilanordnung im Falle des § 100g Abs. 1 nach wie vor zulässig, weil wie bisher auf § 100a Abs. 3 und § 100b Abs. 1 bis 4 StPO verwiesen wird.

Auch insoweit ist zu konstatieren, dass der Schutz der Berufsgeheimnisträger und Berufsgeheimnisträgerinnen höchst unvollkommen ausgestaltet wird. Nicht nur unterliegen sie hinsichtlich der von ihnen geheim zuhaltenden Tatsachen nur dem Schutz einer Verhältnismäßigkeitsprüfung, auch der Richtervorbehalt ist nicht so konstruiert, dass er nicht umgegangen werden

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

könnte. So ist es für die Strafverfolgungsbehörden über den Weg des § 100g Abs. 1 ohne weiteres möglich, Verkehrsdaten nach § 96 TKG zu erheben. Diese sind denen durchaus vergleichbar, die nach § 113b Abs. 2 TKG-E gespeichert werden müssen. Der Schutz der Berufsgeheimnisse, vor allem aber der Informantenschutz und das Redaktionsgeheimnis erfordern es jedoch, den Richtervorbehalt ohne Ausnahme zu gewährleisten.

Unter den notwendigen Verfahrensgarantien einer Rechtsordnung ist zuerst und vor allem die Garantie notwendig, dass ein Richter oder eine unabhängige und unparteiische Stelle angerufen werden kann, bevor die Polizei oder der Staatsanwalt Zugang zu den (journalistischen) Quellen erhält⁶³. Obwohl auch die Staatsanwaltschaft an Recht und Gesetz gebunden ist⁶⁴, stellt sie doch, was das Ermittlungsverfahren anbelangt, eine „Partei“ dar, die Interessen vertritt, die möglicherweise nicht mit dem journalistischen Quellenschutz vereinbar sind⁶⁵. Sie kann daher wohl kaum als objektive und unparteiische Partei angesehen werden, von der erwartet werden kann, dass sie die angemessene Bewertung der konkurrierenden Interessen vornimmt.

3) Zu Art. 5, § 202d StGB

Nach der geplanten neuen Vorschrift des § 202d StGB soll strafbar handeln, wer Daten, die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen.

Der Straftatbestand soll nicht öffentlich zugängliche, elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeicherte Daten erfassen. Er soll das formelle Datengeheimnis schützen. Als Vortat einer Datenhehlerei sollen alle Taten in Betracht kommen, die ein Strafgesetz verwirklichen, unabhängig von der Schuld des Täters oder vom Vorliegen eines Strafantrages, z.B. das Abfangen und Ausspähen von Daten (§§ 202a, 202b StGB), Diebstahl (§ 242

⁶³ vgl. EGMR (Fn.51); Case of Sanoma Uitgevers B.V. v. The Netherlands, Rdnr. 90: "First and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial decision-making body."

⁶⁴ vgl. EGMR, Case of Sanoma Uitgevers B.V. v. The Netherlands, Rz. 93: "Although the public prosecutor, like any public official, is bound by requirements of basic integrity, in terms of procedure he or she is a "party" defending interests potentially incompatible with journalistic source protection and can hardly be seen as objective and impartial so as to make the necessary assessment of the various competing interests."

⁶⁵ vgl. Fn 63. Der entsprechende Ermittlungseifer der Staatsanwaltschaft war jüngst bei den unbegründeten Ermittlungen wegen angeblichen Landesverrats gegen netzpolitik.org und Journalisten dieses Mediums zu besichtigen.

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

StGB), Betrug (§ 263 StGB), Computerbetrug (§ 263a StGB), Nötigung (§ 240 StGB), Fälschung technischer Aufzeichnungen (§ 269 StGB) etc.⁶⁶

§ 202d Abs. 3 StGB sieht einen Tatbestandsausschluss für Handlungen vor, die ausschließlich zu dem Zwecke der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu sollen, als von beruflichen Pflichten umfasst, auch journalistische Tätigkeiten in Vorbereitung einer konkreten Veröffentlichung gehören⁶⁷. Durch das Ausschließlichkeitskriterium soll entsprechend der Regelung des § 184b Abs. 5 StGB sichergestellt werden, dass die konkrete Aufgabenerfüllung einziger Grund für die Verwendung der Daten ist⁶⁸.

Im Einzelnen sollen nach § 202d Abs. 3 S. 2 StGB-E solche beruflichen Handlungen der in § 53 Abs. 1 S. 1 Nr. 5 der Strafprozessordnung genannten Personen von der Anwendung des Tatbestandes ausgeschlossen sein, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden. Dabei soll § 202d Abs. 3 S. 2 StGB-E einen Unterfall des § 202d Abs. 3 S. 1 StGB-E darstellen⁶⁹. § 202d Abs. 3 Satz 2 StGB-E ist im Wortlaut an § 353b Abs. 3a StGB angelehnt.

Gegenüber der Fassung des Referentenentwurfs wird nun bereits im Wortlaut des § 202d klar gestellt, dass journalistische Tätigkeiten, die im Zusammenhang mit einer Datenhehlerei stehen könnten, nicht strafbar sind, wenn sie sich darin erschöpfen, Daten entgegenzunehmen, auszuwerten oder zu veröffentlichen. In der Begründung des Regierungsentwurfs wird allerdings auch darauf hingewiesen, dass wegen des gewählten Wortlautes die Auslegungsgrundsätze zu § 353b Abs. 3a StGB anzuwenden sind.

Demzufolge sollen auch bei § 202d StGB-E diejenigen Handlungen strafbar bleiben, die sich auf den Zeitraum beziehen, der vor der Vortat einer Datenhehlerei liegt oder in Zusammenhang mit der Vortat steht⁷⁰. Es ist daher auch nach dem Wortlaut des Regierungsentwurfs nicht ausgeschlossen, dass eine Strafbarkeit wegen der journalistischen Tätigkeit angenommen wird, weil etwa vermutet wird, dass ein Journalist oder eine Journalistin durch seine bzw. ihre Tätigkeit nicht nur passiv die Vortat ermöglicht hat, sondern (z.B. durch eine vorherige Erklärung zur Entgegennahme oder zu einem Angebot einer Geldzahlung für die Daten) den Entschluss des Vortäters zur Tatbegehung auch aktiv gefördert oder vielleicht sogar hervorgerufen hat⁷¹.

⁶⁶ vgl. Regierungsentwurf, S. 54

⁶⁷ vgl. zu der ähnlichen Formulierung in § 184b Abs. 5 StGB: MüKO/Hörnle, Rdnr. 41, 12. Auflage

⁶⁸ vgl. Regierungsentwurf, S. 57; BT-Drs 12/4883, S. 8 f.

⁶⁹ vgl. Regierungsentwurf, S. 57

⁷⁰ vgl. zu § 353b Abs. 3a StGB: MüKo/Graf, § 353b, Rdnr. 58, 12. Aufl.

⁷¹ vgl. zu § 353b Abs. 3a StGB: Schönke/Schröder (Perron), § 353b, Rdnr. 21d, 29. Aufl.

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

Die Beschränkung des Schutzes der Journalistinnen und Journalisten auf in unmittelbarem Zusammenhang mit der (konkreten) Veröffentlichung stehenden Handlungen im Rahmen des § 202d StGB-E ist aber auch sachlich nicht gerechtfertigt. In solchen Handlungen erschöpft sich journalistische Tätigkeit nicht. Sollen tatsächlich nur solche journalistischen Tätigkeiten straffrei bleiben, die in „Vorbereitung einer **konkreten Veröffentlichung**“ erfolgen⁷²? Unklar ist schon, ob aus der ex-post-Betrachtung die Veröffentlichung konkret erfolgt sein muss oder ob von diesem Blickwinkel die Veröffentlichung konkret geplant sein muss. Und sollen umgekehrt z.B. vorgelagerte journalistische Tätigkeiten, vor allem Recherchen, die noch nicht mit geplanten konkreten Veröffentlichungen in Verbindung zu bringen sind, oder der Austausch von Rechercheergebnissen⁷³, der zwar auf Veröffentlichung gerichtet ist, zu dem aber eine konkrete Veröffentlichung noch nicht geplant ist, nach § 202d StGB-E ohne Ausnahme strafbar sein?

Das Ergebnis der geplanten Normen wäre eine Schwächung des Informantenschutzes und des Redaktionsgeheimnisses und damit eine erhebliche Beeinträchtigung der Presse- und Rundfunkfreiheit. Hinzu kommt, dass gerade im Ermittlungsverfahren die Strafverfolgungsbehörden etwa zum Zeitpunkt des Antrags auf Durchsuchung und Beschlagnahme - außer der Tatsache der Veröffentlichung - in aller Regel nicht mehr wissen, als dass ein Journalist oder eine Journalistin in die Datenhehlerei verwickelt sein könnte⁷⁴.

Es ist gerade eine Aufgabe der Medien und der Schutz des Art. 5 Abs. 1 S. 2 GG erstreckt sich deshalb darauf, Informationen zu beschaffen und Nachrichten und Meinungen zu verbreiten⁷⁵. Allerdings gehören die Vorschriften des Strafgesetzbuches als allgemeine Gesetze zu den Schranken der Pressefreiheit des Art. 5 Abs. 2 GG. Die allgemeinen Gesetze sind ihrerseits im Licht der Pressefreiheit auszulegen und anzuwenden⁷⁶. Die Einschränkung der Pressefreiheit muss geeignet und erforderlich sein, um den angestrebten Erfolg zu erreichen; dieser muss in

⁷² So die Begründung, S. 57 mit Hinweis auf MüKo/Hörnle, aaO, der ebenso wenig wie der Regierungsentwurf erklärt, unter welchen Umständen eine „konkrete“ Veröffentlichung anzunehmen ist.

⁷³ Man denke etwa an gemeinsame Recherchen verschiedener Medien.

⁷⁴ vgl. zu dem vergleichbaren Fall des Besitzes des gesuchten Materials: BVerfGE 117, 244 (246); auf dieses Problem hatten die Stellung nehmenden Organisationen schon im Gesetzgebungsverfahren zu § 353b StGB hingewiesen

⁷⁵ vgl. BVerfGE 10, 118 (121); 66, 116 (133); 77, 65 (74);
http://www.bverfg.de/entscheidungen/rk20101210_1bvr173904.html , Rz. 14

⁷⁶ vgl. BVerfGE 77, 65 (81ff); 107, 299 (329ff); BVerfG NJW 2001, 507; BVerfGE 117, 244 (261)

Gemeinsame Stellungnahme
zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD
zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

*ARD • BDZV • DJV • Deutscher Presserat
VDZ • ver.di • VPRT • ZDF*

angemessenem Verhältnis zu den Einbußen stehen, welche die Beschränkung für die Pressefreiheit mit sich bringt⁷⁷. Geboten ist insofern eine Abwägung zwischen dem sich auf die konkret zu verfolgenden Taten beziehenden Strafverfolgungsinteresse und der Pressefreiheit⁷⁸.

Gemessen daran stellt sich der Straftatbestand der Datenhehlerei als eine Störung dar, die das Potenzial einer einschüchternden Wirkung auf journalistische Quellen in sich trägt und damit als Beeinträchtigung der Presse- und Rundfunkfreiheit anzusehen ist⁷⁹.

Falls daher der Straftatbestand der Datenhehlerei eingeführt werden sollte, muss zweifelsfrei geregelt werden, dass journalistische Tätigkeiten vom Tatbestand generell nicht umfasst werden. § 202d Abs. 3 könnte demnach wie folgt formuliert werden:

„(3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere

1.

2. berufliche Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen.“



Benno H. Pöppelmann
– DJV-Justiziar –

⁷⁷ vgl. BVerfGE 59, 231 (265); 71, 206 (214); 77, 65 (75)

⁷⁸ vgl. BVerfG NJW 2001, 507 (508)

⁷⁹ vgl. zu den Auswirkungen z.B. einer Durchsuchung: BVerfG NJW 2005, 965; BGH NJW 1999, 2052 (2053); BVerfGE 117, 244 (259)