Stellungnahme zum Gesetzentwurf der Fraktionen der CDU/CSU und SPD für ein Gesetz "zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

Mit der vorliegenden Stellungnahme soll auf verfassungsrechtliche Bedenken gegen die Regelungen des Gesetzentwurfes in der Drucksache 18/5088 eingegangen werden, ohne in umfassender Weise alle Kritikpunkte an Einzelfragen des Gesetzes aufzugreifen. Dazu haben insbesondere die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und einzelne Verbände detailliert Stellung bezogen.

1. Die verfassungsrechtlichen Prüfungsmaßstäbe

1.1. Bundesrecht

Als Prüfungsmaßstab kommen das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm 1 Abs. 1 GG) und das Telekommunikationsgeheimnis aus Art. 10 Abs. 1 GG in Betracht. [1]

Hierbei ist in der Rechtsprechung des Bundesverfassungsgerichts geklärt, dass Verkehrsdaten in den Schutzbereich des Art. 10 Abs. 1 GG fallen, während Bestandsdaten vom Grundrecht auf informationelle Selbstbestimmung geschützt sind.

Eine Besonderheit gilt für die dynamischen IP-Adressen, da diese Auskunft über die Identität eines Nutzers geben, also mit anderen Bestandsdaten wie der Telefonnummer vergleichbar sind, aber nur vorübergehend vergeben werden, so dass ihr Rückbezug auf den Inhaber nur unter Verwendung von Verkehrsdaten ermittelt werden kann. Wegen dieses Rückbezuges ordnet das Bundesverfassungsgericht auch die dynamischen IP-Adressen dem Schutzbereich des Art. 10 Abs. 1 GG zu. [2]

Das zu beurteilende Gesetz betrifft ausschließlich die Speicherung und Beauskunftung von Verkehrsdaten und ist daher am Prüfungsmaßstab des Art. 10 Abs. 1 GG zu messen.

1.1.2 Schutzbereich des Art. 10 Abs. 1 GG

Art. 10 Abs. 1 GG schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs vor einer Kenntnisnahme durch die öffentliche Gewalt. Hiervon sind nicht nur der Inhalt der Kommunikation, sondern auch die äußeren Umstände derselben, wer hat wann, mit wem, von wo und unter Benutzung welcher Medien kommuniziert, betroffen. [3]

Der Schutzbereich "...erstreckt sich auch auf die Informations- und Datenverarbeitungsprozesse, die sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließen, und auf den Gebrauch, der von den erlangten Kenntnissen gemacht wird (vgl. BVerfGE 100, 313 <359>) " [4]

1.1.3. Schranken

Einschränkungen stehen gemäß Art. 10 Abs. 2 S. 1 GG unter Gesetzesvorbehalt und

1 BVerfG Beschl. v. 24.01.2012 - 1 BvR 1299/05 – Ls. 1; diese und alle weiteren Entscheidungen des Bundesverfassungsgerichts zitiert nach http://www.bundesverfassungsgericht.de
2 BVerfG aaO Ls. 1 und Rn. 116
3 BVerfG U. v. 02.03.2010 - 1 BvR 256/08 u.a. - Rn 189; st. Rspr., vgl. die dortigen Nachweise
4 BVerfG aaO Rn. 190

müssen darüberhinaus verhältnismäßig sein.

Bei der Verhältnismäßigkeitsprüfung ist das BVerfG in seinem Urteil vom 02.03.2010 von der grundsätzlichen Eignung und Erforderlichkeit der Vorratsdatenspeicherung für den angestrebten Zweck ausgegangen.[5]

Es hat den Eingriff, der in der Speicherung der Kommunikationsverbindungsdaten liegt, wegen der seiner Streubreite, des Fehlens jeglichen Bezuges der betroffenen Bürger zu einer Straftat und der Aussagekraft dieser Daten für besonders schwerwiegend gehalten.[6]

Das Bundesverfassungsgericht hat hieran anknüpfend die Vorratsdatenspeicherung nur als Ausnahmemaßnahme zugelassen, sie dürfe insbesondere nicht im Zusammenspiel mit anderen Dateien zu einer Rekonstruierbarkeit "...praktisch aller Aktivitäten der Bürger führen." [7]

Der Spielraum des Gesetzgebers für weitere Datenspeicherungspflichten sei daher und im Hinblick auf die schon bestehenden Datensammlungen erheblich eingeschränkt und auch nicht durch europäische Regelungen erweiterbar, da es zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehöre, die Freiheitswahrnehmungen der Bürger nicht total zu erfassen und zu registrieren.[8]

Die Verhältnismäßigkeit der Vorratsdatenspeicherung im TKG ist nach Auffassung des Bundesverfassungsgerichts nur zu wahren, wenn besonders strenge Sicherheitmaßnahmen für die Speicherung und Weiterverarbeitung der Daten Platz greifen, wobei dies vom Gesetzgeber hinreichend normenklar selbst angeordnet werden müsse.[9]

1.2. Europäische Grundrechte als Prüfungsmaßstab

1.2.1 Anwendbarkeit der Grundrechtecharta

Der Gesetzentwurf selbst geht von der Anwendbarkeit der Europäischen Grundrechte auf die Regelungsmaterie aus.

Lediglich klarstellend sei hervorgehoben dass die vorliegenden Regelungen zur Datenspeicherung und -verarbeitung unter den Anwendungsbereich der Richtlinie 95/46 EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sowie der Richtlinie 2002/58 EG (Datenschutzrichtlinie für elektronische Kommunikation) fallen.[10]

Nach der Entscheidung in der Rechtssache C-617/10 (Åkerberg Fransson) gilt die Grundrechtecharta der EU (EuGRCh) auch für das Verhältnis der EU-Bürger zu einem Mitgliedsstaat, wenn eine nationale Rechtsvorschrift in den Geltungsbereich des Unionsrechts fällt,[11] vgl. Art. 51 Abs. 1 EuGRCh.

---

5 BVerfG aaO Rn. 207f.
6 BVerfG aaO, Rn. 210f.
7 BVerfG aaO, Rn. 218
8 BVerfG ebenda
9 BVerfG aaO, Ls. 2, 4 und 5 und Rn. 220ff.
10 Vgl. EUGH, Urteil vom 08.04.2014, Rs. C-293/12 und C-594/12, Rn. 4-10 (diese und alle weiteren Entscheidungen des EUGH zitiert nach: http://eur-lex.europa.eu
11 EUGH, Urteil vom 26.02.2013, RS 617/10 Rn. 17-23; zur Abgrenzung vgl. BVerfG, Urteil vom

1.2.2 Art. 7 EuGRCh - Achtung des Privatlebens und Art. 8 EuGRCh – Schutz personenbezogener Daten

Der EUGH erklärte in seinem Urteil vom 08.04.2014 die Richtlinie 2006/24 (Vorratsdatenspeicherungsrichtlinie) für nichtig. Er bejaht sowohl einen Eingriff in das Grundrecht aus Art. 7 EuGRCh als auch aus Art. 8 EuGRCh, verneint trotz des besonders schwerwiegenden Charakters des Eingriffs eine Verletzung der Wesensgehaltsgarantie, bejaht das Vorliegen einer dem Gemeinwohl dienenden Zielsetzung und prüft sodann die Verhältnismäßigkeit des Eingriffs.[12] Für die Zwecke dieser Stellungnahme braucht zwischen den unterschiedlichen Schutzbereichen nicht differenziert zu werden.

1.2.3 Verhältnismäßigkeit des Eingriffs

Der EUGH bejaht die Eignung der Vorratsdatenspeicherung zur Bekämpfung schwerer Kriminalität,[13] verneint dagegen die Erforderlichkeit.[14]

Hierzu führt der EUGH aus, dass selbst die Bekämpfung schwerer Kriminalität für sich genommen die Erforderlichkeit einer Speicherungsmaßnahme, wie sie die Richtlinie zur Vorratsdatenspeicherung vorsah, nicht rechtfertigen kann.[15]

Der Schutz personenbezogener Daten verlangt nach ständiger Rechtsprechung des EUGH, dass sich die Ausnahmen auf das absolut Notwendige beschränken.[16]

Dies verneint der EUGH zum einen, weil die Richtlinie sich auf sämtliche Kommunikationsdaten erstreckte, ohne anhand des Zieles der Bekämpfung schwerer Straftaten eine Differenzierung, Einschränkung oder Ausnahmen vorzunehmen. Insbesondere könnten die gespeicherten Daten sich auf Personen beziehen, die in keinerlei Zusammenhang mit schweren Straftaten stünden. Ferner nehme die Richtlinie die Berufsgeheimnisträger nicht von ihrem Anwendungsbereich aus.[17]

Zum anderen lege die Richtlinie keinen Zusammenhang zwischen den zu speichernden Daten und einer Bedrohung der öffentlichen Sicherheit fest. Insbesondere enthalte die Richtlinie keine Beschränkung auf die Daten eines bestimmten Zeitraumes, eines bestimmten geografischen Gebietes und/oder von Personen, die in eine schwere Straftat verwickelt sein, bzw. deren Daten zur Aufklärung von Straftaten beitragen könnten.[18]

Weitere vom EUGH aufgeführten Unwirksamkeitsgründe betreffen fehlende Einschränkungen der Richtlinie betreffend die Zugangsberechtigung zu den Daten in materieller und personeller Hinsicht und die Unverhätnismäßigkeit der Speicherfrist.[19]

Hinsichtlich der Datensicherheit rügt der EUGH das Fehlen klarer und strikter Vorkehrungen für den Schutz und die Sicherheit der Daten zur Gewährleistung von

---

24.04.2013, 1 BvR 1215/07, Rn. 88-91

12 Vgl. EUGH, Urteil vom 08.04.2014, Rs. C-293/12 und C-594/12, Rn. 32-43

13 EUGH aaO, Rn. 59f.

14 EUGH aaO, Rn. 51-59

15 EUGH aaO, Rn. 51

16 EUGH aaO, Rn. 52 mit weiteren Nachweisen

17 EUGH aaO, Rn. 57f.

18 EUGH aaO, Rn.

19 EUGH aaO, Rn. 60-65

deren Unversehrtheit und Vertraulichkeit.[20]

Schließlich gewährleiste die Richtlinie nicht, dass die Telekommunikationsanbieter ein besonders hohes Sicherheitsniveau für die Speicherung und Verarbeitung der Daten ohne Kostenerwägungen realisieren müssten. Auch die unwiderrufliche Datenvernichtung nach Ablauf der Spericherungsfrist sei nicht gewährleistet und der Schutz der Daten durch Speicherung auf dem Unionsgebiet einschließlich der Überwachung durch eine unabhängige Stelle seien nicht vorgesehen.[21]

2. Anwendung der Prüfungsmaßstäbe der vorerwähnten Rechtsprechung auf den Gesetzentwurf

2.1 Speicherpflichten - §§ 113 a und b TKG

Die verfassungsrechtlichen Bedenken meinerseits richten zunächst sich gegen die uneingeschränkte Anordnung der Speicherpflicht.

2.1.1 Überwachungsgesamtrechnung

Das Bundesverfassungsgericht hat bereits im Jahre 2010 die Anordnung einer Vorratsdatenspeicherung als nur ausnahmsweise zulässig bezeichnet und den Gesetzgeber verpflichtet bei der Anordnung weiterer Speicherpflichten äußerste Zurückhaltung zu üben. Heute, mehr als fünf Jahre später, ist die Situation umgekehrt. Es ist zu überprüfen, ob die Anordnung der umfassenden Kommunikations- und Bewegungsüberwachung angesichts der bereits vorhandenen Datensammlungen gegen das Übermaßverbot verstößt. Hierbei sind insbesondere die tatsächlichen Entwicklungen neben der Fortschreibung der durch Gesetz angeordneten Datensammlungen zu berücksichtigen. Allgemein wird dies unter dem Stichwort “Überwachungsgesamtrechnung" behandelt.[22]

Hierzu würde eine Überprüfung der vorhandenen Anfragen – etwa im Bereich der Bestandsdatenabfragen, der Kontenabfragen, der Funkzellenabfragen- als auch die grundsätzlich angeordneten Kombinationsdateien – vergleiche "Anti-Terrordatei“ – gehören. Zu so einer Bestandsaufnahme gehört auch die Betrachtung erweiterter polizeilicher Überwachungsbefugnisse. In eine Überwachungsgesamtrechnung gehören auch die außerhalb öffentlich-rechtlicher Anordnung vorhandenen privaten Datensammlungen, die im Wege der allgemeinen Ermittlungsbefugnisse der Strafverfolgungsbehörden grundsätzlich der Beschlagnahme unterliegen.

Der Gesetzentwurf hat im bisherigen Verfahren die Überwachungsgesamtrechnung nicht thematisiert. Hält man aber, wie das Bundesverfassungsgericht, die Gesamtheit der vorhandenen Datensammlungen für eine verfassungsrechtlich zu beachtende Gefahr, weil die unbeobachtete Ausübung der Freiheitsrechte zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört und die Möglichkeiten der Erzeugung von Persönlichkeitsprofilen bereits anhand der vorhandenen Datensammlungen nicht mehr fern liegt, so steht die Einbindung der geplanten Speicherung von Kommunikationsdaten gerade unter dem aufgezeigten Gesichtspunkt der Verhältnismäßigkeit auf dem Prüfstand.

---

20 EUGH aaO, Rn. 66

21 EUGH aaO, Rn. 67f.

22 Vgl. Roßnagel, die “Überwachungs-Gesamtrechnung” - Das BVerfG und die Vorratsdatenspeicherung, in: NJW 2010, 1238

Meines Erachtens führt eine solche Prüfung bereits zu dem Ergebnis, dass die geplante Speicherung von Kommunikationsdaten bei einer Gesamtbetrachtung der vorhandenen Datensammlungen in tatsächlicher und rechtlicher Hinsicht, unverhältnismäßig ist. Der Gesetzgeber muss sich mit diesem Bedenken auseinandersetzen und einen entsprechenden Abwägungsprozess einleiten. Hierbei sind auch die weiteren Planungen, wie das geplante Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes, sowie sämtliche Ansammlungen von Passagierdaten in die Erwägung mit einzubeziehen.

Entsprechend hat die EU-Kommission in ihrem Schreiben an die Bundesregierung gerügt: "Die faktischen Elemente und Nachweise (d. h. statistische Daten oder Studien), die der Bewertung zugrunde liegen, dass eine Speicherfrist von 4 bzw. 10 Wochen unbedingt notwendig ist, um das verfolgte Ziel des Allgemeininteresses zu erreichen, sollten bereitgestellt und erläutert werden."

2.1.2 Ausnahmen für Berufsgeheimnisträger

Die Überwachung der Kommunikation eines Strafverteidigers mit seinem Mandanten ist bereits von Verfassungs wegen unstatthaft.[23]

Entsprechend gilt dies für sämtliche Berufsgeheimnisträger. Hierbei genügt das in § 100g Absatz 4 StPO-E angeordnete Verwertungsverbot der Daten von Berufsgeheimnisträgern bereits deshalb nicht, weil es die Übermittlung dieser Daten im Strafverfahren zulässt und die Übermittlung und Verwertung für Zwecke der Gefahrenabwehr nicht sperrt, obwohl die Anordnung der Speicherung und Auskunftsberechtigung der Telekommunikationsanbieter Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG darstellen und zur Gesetzgebungskompetenz des Bundes gehören.[24]

Verfassungsrechtlich kann dieser Mangel nur durch ein Speicherungsverbot, wie es in § 99 Abs. 6 TKG-E für die anonymen Beratungsstellen geregelt ist, behoben werden. Dem stehen insbesondere keine unüberwindbaren technischen Hürden entgegen, weil die Berufsgeheimnisträger verkammert sind und die Berufskammern bereits elektronische Verzeichnisse der Kommunikationsanschlüsse der Berufsgeheimnisträger führen. Für die nicht verkammerten Personen wäre ein entsprechendes Verzeichnis einzurichten.

Europarechtlich verstößt die Speicherung der Daten der Berufsgeheimnisträger gegen das Gebot der Eingriffsbeschränkung auf das absolut Notwendige, wie oben dargestellt.[25]

2.1.3 Beschränkung auf das absolut Notwendige

Schärfer als das Bundesverfassungsgericht hat der EUGH bereits bei der Datenspeicherungsanordnung der nichtigen Richtlinie 24/2006 gerügt, dass sie sich nicht auf das absolut Notwendige beschränke.[26]

---

23 Vgl. im Einzelnen BVerfG, 3. Kammer des Zweiten Senats, NJW 2007, 2749 ff.
24 Vgl. BVerfG aaO, Rn. 194 und 201f.
25 Vgl. FN 17 und Punkt 1.2.3
26 ebenda

Dieser Mangel besteht auch bei der Speicherungsanordnung nach §§ 113a und 113b TKG-E.

Es werden keine anlaß-, gebiets, zeitraum- oder personenbezogenen Einschränkungen vorgesehen. Damit dürfte aus europarechtlicher Sicht ein Verstoß gegen das Verbot der Beschränkung von Grundrechtseingriffen auf das absolut Notwendige vorliegen.

2.2 Übermittlung von Internet-Protokolladressen (IP-Adressen)

Wegen der Knappheit von Adressen im IP-IV-Adressbereich gehen die Provider zunehmend dazu über, eine IP-Adresse für mehrere Nutzer zu vergeben. Dies erfolgt durch die Zuweisung eines Ports für eine bestimmte Internetanwendung des Nutzers. Der Port hat die Funktion einer Sub-Adresse.

Diesen Sachverhalt hat das Gesetz nicht erfasst, wenn es anordnet, dass die dem Teilnehmer zugeordnete Internetadresse, eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt und die dem Teilnehmer zugewiesene IP-Adresse sowie Beginn und Ende von deren Nutzung zu speichern seien, § 113b Abs. 3 TKG-E.

Die vom Gesetzgeber gewollte Identifizierung des Internetnutzers ist nur unter gleichzeitiger Speicherung der genutzten Ports und der millisekundengenauen Aufzeichnung der Nutzung derselben technisch möglich. Angesichts der Zuweisung einer Internetadresse an bis zu 200 Nutzer dürfte ein außerordentlich erheblicher technischer Aufwand für die Speicherpflichtigen anfallen.

Das Gesetz ist jedenfalls insofern uneindeutig und damit unbestimmt. Die Verlagerung der Verpflichtung zur Datenspeicherung auf eine technische Umsetzungsrichtlinie dürfte verfassungsrechtlich nicht zulässig sein.

Hinzu kommt, dass der Port auch Details zum genutzten Dienst verrät, so gibt der Port z.B. Auskunft darüber, was der Nutzer „von der anderen Seite will“ - konkret ist so z.B. in der Regel die Nutzung verschiedener Dienste an der Port-Nummern erkennbar und in Folge, mit wem kommuniziert wurde.

Berlin, den 21.09.2015
Meinhard Starostik - Rechtsanwalt