Verwaltungsgericht Köln, 9 L 1009/16

Datum:	25.01.2017
Gericht:	Verwaltungsgericht Köln
Spruchkörper:	9. Kammer
Entscheidungsart:	Beschluss
Aktenzeichen:	9 L 1009/16
ECLI:	ECLI:DE:VGK:2017:0125.9L1009.16.00

Nachinstanz:	Oberverwaltungsgericht NRW

Tenor:

1. Der Antrag wird abgelehnt.

Die Antragstellerin trägt die Kosten des Verfahrens.

2. Der Streitwert wird auf Euro 40.037,50 festgesetzt.

G r ü n d e:

Der Antrag der Antragstellerin,

im Wege der einstweiligen Anordnung im Sinne des § 123 Abs. 1 Satz 1 VwGO anzuordnen, dass die Antragstellerin bis 6 Monate nach rechtskräftigem Abschluss des Hauptsacheverfahrens nicht verpflichtet ist, die in § 113b Abs. 3 TKG aufgeführten Telekommunikations-Verkehrsdaten ihrer Kunden zu speichern, denen sie den Internet-Zugang vermittelt,

bleibt ohne Erfolg.

Nach § 123 Abs. 1 Satz 1 VwGO kann eine einstweilige Anordnung in Bezug auf den Streitgegenstand getroffen werden, wenn die Gefahr besteht, dass durch eine Veränderung des bestehenden Zustandes die Verwirklichung eines Rechts des Antragstellers/der Antragstellerin vereitelt oder wesentlich erschwert werden könnte (Sicherungsanordnung). Einstweilige Anordnungen sind nach § 123 Abs. 1 Satz 2 VwGO auch zur Regelung eines vorläufigen Zustandes in Bezug auf ein streitiges Rechtsverhältnis zulässig, wenn diese Regelung, vor allem bei dauernden Rechtsverhältnissen zur Abwendung wesentlicher Nachteile, zur Verhinderung drohender Gewalt oder aus anderen Gründen nötig erscheint

(Regelungsanordnung). Die Notwendigkeit der vorläufigen Regelung (Anordnungsgrund) und der geltend gemachte Anspruch (Anordnungsanspruch) sind glaubhaft zu machen (§ 123 VwGO i.V.m. §§ 920 Abs. 2, 294 Zivilprozessordnung – ZPO).

Diese Voraussetzungen für den Erlass einer einstweiligen Anordnung liegen nicht vor. 6

Der Antrag ist zulässig. 7

Dem Erlass der begehrten Regelungsanordnung steht nicht entgegen, dass es sich um vorbeugenden Rechtsschutz handelt. Die für die Antragstellerin (spätestens) ab dem 1. Juli 2017 (§ 113b Abs. 3 TKG i.V.m. § 150 Abs. 13 Satz 1 TKG in der Fassung des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015, BGBl I S. 2218) bestehende gesetzliche Verpflichtung, Einrichtungen zur Vorratsdatenspeicherung auf eigene Kosten vorzuhalten und zu betreiben (§§ 113a ff. TKG), kann von der Bundesnetzagentur durch entsprechende Anordnung sichergestellt und auch im Wege des Verwaltungszwangs durchgesetzt werden (§ 115 Abs. 1, Abs. 2 Nr. 1 TKG); gegen den gemäß § 137 Abs. 1 TKG vollziehbaren Verwaltungsakt kann die Antragstellerin dann zwar auch vorläufigen gerichtlichen Rechtsschutz nach § 80 Abs. 5 VwGO erhalten, in dessen Rahmen die Rechtmäßigkeit der ihr auferlegten Pflicht vom Gericht zu prüfen ist. Nur ausnahmsweise genügt die Möglichkeit, vorläufigen Rechtsschutz durch die Suspendierung eines die normative Verpflichtung umsetzenden Verwaltungsakts zu erlangen, zur Wahrung der Effektivität des Rechtsschutzes allerdings nicht, wenn bereits die Verletzung der normativen Pflicht, unabhängig vom Ergehen eines sie umsetzenden Verwaltungsakts, staatliche Sanktionen ermöglicht, 8

vgl. VG Berlin, Beschluss vom 16. Januar 2009 – 27 A 321.08 –, juris, Rn. 14. 9

Diese Ausnahmesituation ist vorliegend gegeben. Die Antragstellerin ist vor dem Hintergrund, dass in § 149 Abs. 1 Nr. 36 - 44 und Absatz 2 Satz 1 TKG eine Bußgeldandrohung bis zu 500.000 Euro bei einem Verstoß gegen die Vorschriften der § 113b - § 113g TKG vorgesehen ist, nicht gehalten, eine Anordnung bzw. (Zwangs)Maßnahmen der Antragsgegnerin gemäß § 115 Abs. 1 und Abs. 2 Nr. 1 TKG zur Umsetzung der Verpflichtungen aus § 110 Abs. 1 i.V.m. § 113b TKG abzuwarten und sich hiergegen nach § 80 Abs. 5 VwGO bzw. im Rahmen eines Ordnungswidrigkeitenverfahrens zu wenden, 10

vgl. BVerwG, Urteil vom 13. Januar 1969 – I C 86.64 -, BVerwGE 31, 177, juris, Rn. 19 ff.; in diesem Sinne auch BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08 u.a. – „Vorratsdatenspeicherung“, BVerfGE 125, 260 ff., juris, Rn. 179; VG Berlin, Beschluss vom 16. Januar 2009 – 27 A 321.08 -, juris, Rn. 14. 11

Ein Rechtsschutzbedürfnis der Antragstellerin für die begehrte Anordnung besteht bereits zum jetzigen Zeitpunkt, obwohl sie (erst) spätestens ab dem 1. Juli 2017 verpflichtet ist, die umstrittenen Regelungen zur Vorratsdatenspeicherung anzuwenden (§ 113b Abs. 3 TKG i.V.m. § 150 Abs. 13 Satz 1 TKG). Denn die Antragstellerin hat glaubhaft und nachvollziehbar dargelegt, dass eine Verpflichtung zur Vorratsdatenspeicherung einen gewissen Zeitablauf erfordert, um die notwendige Technik zu installieren und sonstige Organisationsmaßnahmen im sächlichen und personellen Bereich zu treffen. 12

Die vorläufige Entbindung der Antragstellerin von der gesetzlichen Verpflichtung zur Einrichtung und Bereithaltung der technischen Anlagen zur Vorratsdatenspeicherung stellt zudem keine unzulässige Vorwegnahme der Hauptsache dar. Denn hierunter ist nur eine endgültige – rechtliche oder zumindest faktische – Vorwegnahme der Hauptsache in dem 13

Sinne zu verstehen, dass die Entscheidung und ihre Folgen aus rechtlichen oder tatsächlichen Gründen auch nach der Hauptsacheentscheidung gänzlich nicht mehr rückgängig gemacht werden können. Die bloße Tatsache, dass die vorübergehende Aussetzung als solche nicht wieder rückgängig gemacht werden kann, macht die vorläufige Regelung in einem solchen Fall nicht zu einer faktisch endgültigen. Denn eine derartige zeitweise Vorwegnahme wohnt jeder vorläufigen Entscheidung inne, würde eine einstweilige Anordnung somit regelmäßig unzulässig machen,

vgl. BVerfG, Beschluss vom 31. März 2003 – 2 BvR 1779/02 -, NVwZ 2003, 1112, juris, Rn. 4 f.; Kopp, VwGO, 22. Auflage, § 123 Rn. 14. 14

Der Antrag ist jedoch nicht begründet. Die Antragstellerin hat weder einen Anordnungsanspruch noch einen Anordnungsgrund glaubhaft gemacht. 15

Der Grundsatz effektiven Rechtsschutzes aus Art. 19 Abs. 4 GG gebietet, vorläufigen Rechtsschutz zu gewähren, wenn ohne ihn schwere und unzumutbare, anders nicht abwendbare Nachteile entstünden, zu deren nachträglicher Beseitigung die Entscheidung in der Hauptsache nicht mehr in der Lage wäre. Dies gilt vor allem dann, wenn eine erhebliche Grundrechtsverletzung droht, es sei denn, dass ausnahmsweise überwiegende, besonders gewichtige Gründe entgegenstehen, 16

vgl. BVerfG, Beschluss vom 25. Oktober 1988 – 2 BvR 745/88 -, BVerfGE 79, 69 ff., juris, Rn. 17. 17

Hinzu kommt, dass nach bundesverfassungsgerichtlicher Rechtsprechung bei dem Begehren um Aussetzung des Vollzugs eines Gesetzes bei der Folgenabwägung ein besonders strenger Maßstab anzulegen ist und von einer Aussetzung nur mit größter Zurückhaltung Gebrauch zu machen ist, weil der Erlass einer solchen einstweiligen Anordnung stets einen erheblicher Eingriff in die Gestaltungsfreiheit des Gesetzgebers darstellt. Müssen die für eine vorläufige Regelung sprechenden Gründe schon im Regelfall so schwer wiegen, dass sie den Erlass einer einstweiligen Anordnung unabdingbar machen, so müssen sie im Fall der begehrten Außervollzugsetzung eines Gesetzes darüber hinaus besonderes Gewicht haben, 18

vgl. BVerfG, Beschluss vom 28. Oktober 2008 – 1 BvR 256/08 -, BVerfGE 122. 120 ff., juris, Rn. 72 und Beschluss vom 11. März 2008 – 1 BvR 256/08 -, juris, Rn. 141-145. 19

Insoweit ist von entscheidender Bedeutung, ob die Nachteile irreversibel oder nur erschwert revidierbar sind, um das Aussetzungsinteresse durchschlagen zu lassen, 20

vgl. BVerfG, Beschluss vom 8. Juni 2016 – 1 BvQ 42/15 -, juris, Rn. 13 mit zahlreichen Nachweisen. 21

Die Antragstellerin hat in diesem Sinne keine schweren und unzumutbaren Nachteile glaubhaft gemacht, die es rechtfertigen würden, schon jetzt gegen die gesetzliche Regelung vorläufigen Rechtsschutz zu gewähren. 22

Vorliegend hat die Antragstellerin nicht glaubhaft gemacht, dass ihr der von ihr geltend gemachte Anordnungsanspruch zusteht. Vielmehr ist dies offen. 23

Die Antragstellerin führt hierzu im Wesentlichen aus, die ihr zukünftig obliegende Speicherung von Internetzugangsdaten nach § 113b Abs. 3 TKG verstoße gegen Grundrechte, so dass sie deshalb ein entsprechendes Abwehrrecht habe, sie also den gesetzlichen Verpflichtungen aus den §§ 113a ff. TKG also nicht nachkommen müsse. Sie 24

beruft sich dabei auf ihre Berufsfreiheit nach Art. 12 Abs. 1 GG sowie die Grundrechte ihrer Kunden, Art. 10 Abs. 1 GG, zusätzlich Art. 5 Abs. 1 Satz 1 GG bzw. Art. 12 GG, soweit ihre Kunden Berufsgeheimnisträger sind. Darüber hinaus sieht sie einen Verstoß gegen Unionsgrundrechte in Form des Verstoßes gegen ihre Berufsfreiheit und unternehmerische Freiheit gemäß Art. 15 und 16 der Charta der Grundrechte der Europäischen Union (EuGRCh), einen Verstoß gegen Unionsgrundrechte ihrer Kunden in Form der Achtung des Privat- und Familienlebens sowie des Schutzes personenbezogener Daten, Art. 7 und 8 EuGRCh. Zudem stelle die Speicherpflicht eine Beschränkung der Dienstleistungsfreiheit der Antragstellerin im Sinne des Art. 56 des Vertrags über die Arbeitsweise der Europäischen Union in der konsolidierten Fassung (AEUV, ABl. EU C 202 vom 7. Juni 2016) dar, deren Rechtfertigung ebenfalls am Maßstab der Grundrechte aus der EuGRCh zu messen sei.

Vorliegend kann bei der nur möglichen summarischen Überprüfung nicht festgestellt werden, dass die gesetzlichen Regelungen in den §§ 113a ff TKG gegen die von der Antragstellerin genannten Artikel des Grundgesetzes verstoßen. Vielmehr spricht Überwiegendes dafür, dass der Gesetzgeber bei der Neuregelung der sog. Vorratsdatenspeicherung die verfassungsrechtlichen Vorgaben hinreichend beachtet hat. Anders verhält es sich allerdings bei den geltend gemachten Verstößen gegen Unionsgrundrechte. Inwieweit die deutschen Regelungen über die Vorratsdatenspeicherung mit dem Unionsrecht, insbesondere mit der Rechtsprechung des Europäischen Gerichtshofs (EuGH), 25

Urteil vom 8. April 2014 – C-293/12, C-594/12 -, u.a. Vorlagebeschluss High Court Dublin „Digital Rights Ireland Ltd.“, juris; Urteil vom 21. Dezember 2016 – C-203/15 und C-698/15 -, verbundene Rechtssache Tele2 SverigeAB/Post- och telestyrelsen und Secretary of State for the Home Department/Tom Watson u.a. - , www.curia.europa.eu, 26

vereinbar sind, muss aufgrund der Komplexität der zu beantwortenden Fragen der Prüfung im Hauptsacheverfahren überlassen bleiben. Jedenfalls ist aber im Rahmen des vorliegenden Verfahrens nicht davon auszugehen, dass das Unionsrecht das Gericht dazu verpflichten könnte, die angegriffenen Vorschriften des TKG schon im Eilverfahren im Wege der einstweiligen Anordnung für nicht anwendbar zu erklären, 27

in diesem Sinne auch: BVerfG, Beschluss vom 8. Juni 2016 – 1 BvQ 42/15 -, juris, Rn. 26. 28

Ferner führen auch die von der Antragstellerin gegen die einzelnen gesetzlichen Vorschriften erhobenen Rügen nicht zu dem geltend gemachten Anordnungsanspruch. 29

Es spricht Überwiegendes dafür, dass die gesetzlichen Regelungen über die Vorratsdatenspeicherung verfassungsrechtlicher Überprüfung im Hauptsacheverfahren standhalten werden, so dass sich aus einer Verletzung der von der Antragstellerin gerügten (deutschen) Grundrechte kein Abwehrrecht ableiten lässt, um den geltend gemachten Anordnungsanspruch zu stützen. 30

Soweit die Antragstellerin rügt, die Vorratsdatenspeicherungspflicht stelle einen unzulässigen Eingriff in den in Art. 10 Abs. 1 GG verankerten Persönlichkeitsschutz der betroffenen Kunden dar, spricht im Rahmen des vorliegenden Eilverfahrens – jedenfalls nach der bisherigen bundesverfassungsrechtlichen Rechtsprechung - Überwiegendes dafür, dass dies für die im Rahmen des vorliegenden Eilverfahrens im Vordergrund stehende Frage, ob die Investitions- und Bereithaltungskosten für eine „Vorratsdatenspeicherung“ den Telekommunikationsunternehmen auferlegt werden können, unerheblich ist, da es der Antragstellerin mangels unmittelbarer Selbstbetroffenheit verwehrt ist, sich auf mögliche Grundrechtsverletzungen ihrer Kunden zu berufen. Insbesondere geht es nicht um die 31

informationelle Selbstbestimmung der Antragstellerin selbst. Zwar gewährleistet Art. 2 Abs. 1 GG in Verbindung mit Art. 19 Abs. 3 GG das Recht auf informationelle Selbstbestimmung auch juristischen Personen und können staatliche informationelle Maßnahmen auch deren Rechte gefährden. Datenabrufe bezogen auf ihre Kunden zwecks Tätigwerdens diesen gegenüber betreffen jedoch nicht die spezifische Freiheitsausübung der juristischen Person, d.h. ihre eigene wirtschaftliche Tätigkeit, und stellen deshalb keinen Eingriff in den Schutzbereich des der Antragstellerin auch als juristischer Person zustehenden Rechts auf informationelle Selbstbestimmung dar,

vgl. BVerfG, Beschluss vom 13. Juni 2007 – 1 BvR 1550/03, 2357/04, 605/05 -, BVerfGE 118, 168, 202 ff., juris, Rn. 149 ff. betreffend die Verfassungsbeschwerde eines Kreditinstituts gegen den Abruf von Kontostammdaten eines Kunden nach der AO; OVG Berlin-Brandenburg, Beschluss vom 2. Dezember 2009 – OVG 11 S 9.09 -, juris, Rn. 73. 32

Die Kammer verkennt allerdings nicht, dass die identifizierende Zuordnung dynamischer IP-Adressen eine besondere Nähe zu konkreten Telekommunikationsvorgängen aufweist und damit grundsätzlich in den Schutzbereich des Art. 10 Abs. 1 GG fallen kann, 33

vgl. BVerfG, Beschluss vom 24. Januar 2012 – 1 BvR 1299/05 -, juris, Rn- 116 ff. 34

Gleichwohl ändert dies nichts daran, dass es unter Zugrundelegen der bisherigen bundesdeutschen rechtlichen Grundsätze Sache der Kunden der Antragstellerin sein dürfte, sich auf diese mögliche Rechtsverletzung zu berufen. Daher wird die Antragstellerin nicht unter Berufung auf die Rechte ihrer Kunden die Übermittlung von Daten ihrer Kunden verweigern können, so dass sie auch nicht mit dieser Begründung im Vorfeld die Schaffung und Bereitstellung der technischen Voraussetzungen für die gesetzlich geregelte Vorratsdatenspeicherung ablehnen kann. Soweit hiergegen eingewandt werden könnte, dass dies anders zu sehen ist, weil schon die der Antragstellerin auferlegten Speicherungspflichten gegen Grundrechte ihrer Kunden verstoßen, steht dem entgegen, dass das Bundesverfassungsgericht Anträge auf Aussetzung der Neuregelung der Vorratsdatenspeicherung nach Maßgabe einer Folgenabwägung abgelehnt hat, da ein besonders schwerwiegender und irreparabler Nachteil, der es rechtfertigen könnte, den Vollzug der Norm ausnahmsweise im Wege der einstweilige Anordnung auszusetzen, nach Auffassung des Bundesverfassungsgerichts nicht allein in der Datenspeicherung liegt. Denn der in der Speicherung für einzelne liegende Nachteil für ihre Freiheit und Privatheit verdichte und konkretisiere sich erst durch einen Abruf der Daten zu einer möglicherweise irreparablen Beeinträchtigung, 35

vgl. BVerfG, Beschluss vom 8. Juni 2016 – 1 BvQ 42/15 -, juris, Rn. 14 ff. 36

Dies gilt nach den Ausführungen des Bundesverfassungsgerichts auch für die Speicherung der Daten von Berufsgeheimnisträgern, 37

vgl. BVerfG, Beschluss vom 8. Juni 2016 – 1 BvQ 42/15 -, juris, Rn,. 18. 38

Allerdings scheint der EuGH grundsätzlich davon auszugehen, dass mit Rechtsvorschriften, die den Betreibern elektronischer Kommunikationsdienste vorschreiben, die Verkehrs- und Standortdaten auf Vorrat zu speichern, zwangsläufig eine Verarbeitung personenbezogener Daten durch die Betreiber verbunden ist. Infolgedessen zieht er im Rahmen seiner rechtlichen Überprüfung, auch wenn Klagen von Betreibern elektronischer Kommunikationsdienste Grundlage für die von den nationalen Gerichten erfolgten Vorlagebeschlüsse sind, als Prüfungsmaßstab für die Auslegung von Art. 15 Abs. 1 der 39

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. 2002, L 201, S. 37) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. 2009, L 337, S. 11) geänderten Fassung (im Folgenden Richtlinie 2002/58) die Art. 7,8, 11 und 52 Abs. 1 EuGRCh heran,

vgl. EuGH, Urteil vom 21. Dezember 2016 – C-203/15 und C-698/15 -, Rn. 75. 40

Inwiefern hieraus jedoch der Schluss gezogen werden kann, dass in Abkehr von der bisherigen bundesverfassungsrechtlichen Rechtsprechung im Rahmen von Klagen der Betreiber elektronischer Kommunikationsdienste sich diese (auch) auf die grundsätzlich nur ihren Kunden zustehenden Grundrechte, insbesondere Art. 10 GG, berufen können, muss der vertieften Überprüfung im Hauptsacheverfahren überlassen bleiben. Die Frage, ob sich die Telekommunikationsunternehmen auf Art. 10 GG (erfolgreich) berufen können, ist jedenfalls, selbst wenn man die Rechtsprechung des EuGH zugrunde legt, nicht eindeutig zu bejahen. Denn es ist zu berücksichtigen, dass der Prüfungsgegenstand einer Verfassungsbeschwerde vor dem Bundesverfassungsgericht und in einem Vorabentscheidungsersuchen vor dem EuGH ein anderer ist. Während Streitgegenstand bei Verfassungsbeschwerden eine individuelle Rechtsverletzung durch einen Hoheitsakt ist, ist Streitgegenstand bei Vorlagen von nationalen Gerichten bei Vorabentscheidungsgesuchen die Vereinbarkeit nationalen Rechts mit europäischen Richtlinien. Eine Entscheidung in den vorgelegten Verfahren zu Gunsten des einen oder anderen Beteiligten wird gerade nicht getroffen, vielmehr ist dies den vorlegenden nationalen Gerichten vorbehalten, 41

vgl. EuGH, Urteil vom 21. Dezember 2016, a.a.O., Rn. 124. 42

Diese unterschiedlichen Streitgegenstände können daher auch unterschiedliche Prüfungsmaßstäbe bedingen. 43

Es ist nach summarischer Prüfung vorliegend nicht davon auszugehen, dass die Antragstellerin durch die gesetzlich geregelte Vorratsdatenspeicherung in dem ihr zustehenden Grundrecht aus Art. 12 GG verletzt ist. 44

Dabei spricht bereits im Rahmen der Prüfung, ob sich die Antragstellerin für den von ihr geltend gemachten Abwehranspruch auf eine Verletzung des Art. 12 Abs. 1 GG berufen kann, der Umstand gegen einen entsprechenden Abwehranspruch, dass das Bundesverfassungsgericht in seinem Urteil zur „Vorratsdatenspeicherung“ aus dem Jahre 2010 zu der Vorgängerregelung zum Ergebnis gekommen ist, dass die damals zur Überprüfung stehenden gesetzlichen Vorschriften aus dem TKG hinsichtlich Art. 12 Abs. 1 GG für Diensteanbieter, die, wie auch die Antragstellerin, öffentlich zugängliche Telekommunikationsdienste in der Regel gegen Entgelt für Endnutzer erbringen – anders als ein privater Teilnehmer am Telekommunikationsverkehr, dessen Verkehrsdaten gespeichert worden sind bzw. werden sollten -, keinen durchgreifenden verfassungsrechtlichen Bedenken ausgesetzt waren, 45

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 293 ff. 46

Dass eine Überprüfung der Neufassung der gesetzlichen Regelungen zur Vorratsdatenspeicherung einen anderen Schluss rechtfertigt, kann im Rahmen einer summarischen Prüfung nicht festgestellt werden. 47

48

Die Auferlegung von Speicherpflichten für Anbieter von Telekommunikationsdiensten mag zwar einen Eingriff in die von Art. 12 Abs. 1 GG geschützte Berufsfreiheit darstellen. Es ist aber davon auszugehen, dass dieser Eingriff durch Allgemeinwohlbelange verfassungsrechtlich gerechtfertigt ist.

Dabei ist zunächst davon auszugehen, dass es sich bei dem mit der gesetzlichen Regelung verbundenen Eingriff um keine Berufswahlregelung handelt, deren Rechtfertigung hohen Anforderungen genügen müsste, 49

vgl. ständige Rechtsprechung des BVerfG seit Urteil vom 11. Juni 1958 – 1 BvR 596/56 -, BVerfGE 7, 377 ff. „Apothekenurteil“, 50

sondern um eine (bloße) Berufsausübungsregelung. Denn Regelungsgegenstand der §§ 113a ff. TKG sind Speicherungs- und Übermittlungspflichten, die sich als technische Maßgaben für die Erbringung von Telekommunikationsdiensten darstellen, und es der Antragstellerin – wie bei einer unzulässigen Berufswahlregelung erforderlich – nicht (faktisch) unmöglich machen, ihren Beruf sinnvoll auszuüben, 51

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 295; BVerfG, Beschluss vom 16. März 1971 – 1 BvR 52/66, 1 BvR 665/66, 1 BvR 667/66, 1 BvR 754/66 -, juris, Rn. 57, jeweils mit weiteren Nachweisen. 52

Das wird von der Antragstellerin auch selbst nicht behauptet. 53

Die den Telekommunikationsdiensteanbietern auferlegten Verpflichtungen stellen auch keine verfassungsrechtlich unzulässige Berufsausübungsregelung dar, wobei es für die Verfassungsmäßigkeit der Regelung nicht auf die individuelle Interessenlage eines einzelnen Unternehmens ankommt. Vielmehr ist nach der Rechtsprechung des Bundesverfassungsgerichts erst dann ein Gesetz, das die Berufsausübung regelt, nicht mehr verfassungsgemäß, wenn es bei der betroffenen Berufsgruppe generell das Übermaßverbot verletzt, 54

vgl. BVerfG, Beschluss vom 16. März 1971, a.a.O., juris Rn. 61. 55

Für die Verfassungsmäßigkeit eines Gesetzes, das eine Berufsausübungsregelung zum Gegenstand hat, genügt es, dass der Gesetzgeber den Eingriff in das Grundrecht mit sachgerechten und vernünftigen Erwägungen des Gemeinwohls begründet und seine Rechtssetzungsmacht nicht zu sachfremden Zwecken missbraucht. Hinsichtlich der Zumutbarkeit bzw. der Verhältnismäßigkeit im engeren Sinne kommt es jedenfalls bei einer nicht schlechthin unternehmensfremden Tätigkeit und bei einer lediglich quantitativen Steigerung von Belastungen, die hinsichtlich der Kosten im Grundsatz abwälzbar sind, nur darauf an, ob die Verpflichtung für die Gesamtheit der betroffenen Berufsgruppe zu einer ernsthaften, nach der besonderen Ausgestaltung des Gesetzes auch nicht vermeidbaren, die wirtschaftliche Existenz dieser Berufsgruppe gefährdenden Beeinträchtigung der Unternehmensrentabilität führt, 56

vgl. BVerfG, Beschluss vom 16. März 1971, a.a.O., juris, Rn. 85 ff. 57

Nach Maßgabe dieser Voraussetzungen spricht Überwiegendes dafür, dass die den Anbietern von Telekommunikationsdienstleistungen auferlegten Speicherpflichten im Rahmen des Art. 12 GG grundsätzlich verfassungsrechtlich nicht zu beanstanden sind. Dabei ist zunächst zu berücksichtigen, dass die Speicherung von Verkehrsdaten keine 58

unternehmensfremde Tätigkeit ist, da viele Telekommunikationsunternehmen diese, wenn auch regelmäßig nicht für die im Gesetz vorgesehene Zeit, für eigene Abrechnungszwecke speichern. Die Datenübermittlung an die zuständigen behördlichen Stellen für Strafverfolgungszwecke, für deren Umsetzung kostenrelevante technische Vorkehrungen zu treffen sind, ist als technischer Vorgang ferner nichts Unternehmensfremdes. Somit handelt es sich bei den den Telekommunikationsunternehmen durch das Telekommunikations-Neuregelungsgesetz auferlegten Speicherungs- und Übermittlungspflichten letztlich nur um eine quantitative Steigerung von Belastungen, die zudem grundsätzlich auf die Kunden abwälzbar sein dürften. Ob die entstandenen Kosten im Einzelfall aufgrund der Wettbewerbslage tatsächlich nicht weitergegeben werden können, ist unerheblich. Für die Verfassungsmäßigkeit eines Gesetzes kommt es nicht auf die situationsbedingte und prinzipiell variable Marktlage an.

Vgl. BVerfG, Beschluss vom 16. März 1971, a.a.O., Rn. 87 mit weiteren Nachweisen. 59

Hinsichtlich des Eingriffs in die Berufsausübungsfreiheit legitimieren sich die den Telekommunikationsunternehmen auferlegten Speicherungs- und Übermittlungspflichten aus der Zielsetzung des Gesetzes zur Effektivierung der Strafverfolgung, 60

Vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 298. 61

Das Bundesverfassungsgericht hat zudem bereits vorher wiederholt das verfassungsrechtliche Gebot einer effektiven Strafverfolgung hervorgehoben, das Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren betont und die wirksame Aufklärung gerade schwerer Straftaten als einen wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet, 62

vgl. BVerfG, Beschluss vom 12. Oktober 2011 – 2 BvR 236/08 u.a., juris, Rn. 249 m.w.N.. 63

Der Gesetzgeber hat insoweit nachvollziehbar in der Begründung des neu gefassten Gesetzentwurfs ausgeführt, dass die – ohne entsprechende Vorratsdatenspeicherung – bestehende Gesetzeslage zu Unzulänglichkeiten bei der Strafverfolgungsvorsorge und bei der Gefahrenabwehr führt. Zwar können die Strafverfolgungsbehörden auf der Grundlage von § 100g Absatz 1 StPO bei Vorliegen eines Anfangsverdachts und entsprechender richterlicher Anordnung auf Verkehrsdaten Zugriff nehmen, die bei den Erbringern öffentlich zugänglicher Telekommunikationsdienste aus geschäftlichen Gründen im Sinne des § 96 TKG zum Zeitpunkt der Anfrage noch gespeichert sind. Da die Speicherpraxis der Erbringer öffentlich zugänglicher Telekommunikationsdienste sehr unterschiedlich sei, sei es jedoch „derzeit“ vom Zufall abhängig, welche Daten bei einer Abfrage nach § 100g StPO abgerufen werden könnten. Diese Unzulänglichkeiten würden durch den Gesetzentwurf im Wesentlichen behoben. Durch die Speicherung der Verkehrsdaten für eine begrenzte Zeit würden Aufklärungsmöglichkeiten geschaffen, die der zunehmenden Bedeutung der Telekommunikation für die Vorbereitung und Begehung von Straftaten Rechnung trügen, 64

vgl. BT-Drs. 18/5088 S. 21 f. 65

Auch nach der Rechtsprechung des EuGH stellt die Bekämpfung des internationalen Terrorismus zur Wahrung des Weltfriedens und der internationalen Sicherheit im Übrigen eine dem Gemeinwohl dienende Zielsetzung der Europäischen Union dar. Dasselbe gilt für die Bekämpfung schwerer Kriminalität, um die öffentliche Sicherheit zu gewährleisten. Im Übrigen ist insoweit festzustellen, dass nach Art. 6 EuGRCh jeder Mensch nicht nur das Recht auf Freiheit, sondern auch auf Sicherheit hat, 66

vgl. Schlussanträge des Generalanwalts am EuGH vom 19. Juli 2016 in den Verfahren C-203/15, C-698/15, juris, Rn. 163 mit weiteren Nachweisen zur Rechtsprechung des EuGH. 67

Die auch der Antragstellerin mit den gesetzlichen Regelungen auferlegten Speicherungs- und Übermittlungspflichten sind damit grundsätzlich durch vernünftige Gründe des Gemeinwohls gerechtfertigt. 68

Die streitgegenständlichen gesetzlichen Regelungen sind für die Erfüllung dieser Zwecke geeignet. 69

Dieses Erfordernis ist dann erfüllt, wenn eine generelle Verpflichtung zur Vorratsdatenspeicherung geeignet ist, zu der oben bezeichneten dem Gemeinwohl dienenden Zielsetzung beizutragen, d.h. zur Bekämpfung schwerer Kriminalität. Dies kann nicht in Abrede gestellt werden. Denn die auf Vorrat zu speichernden Daten bieten den für die Strafverfolgung zuständigen Behörden eine zusätzliche Ermittlungsmöglichkeit zur Verhütung oder Aufklärung schwerer Straftaten. Damit trägt die Vorratsdatenspeicherung zur Bekämpfung schwerer Kriminalität bei. Insbesondere ermöglicht diese Verpflichtung in gewissem Umfang den Strafverfolgungsbehörden – anders als bei gezielten Überwachungsmaßnahmen, für die zukünftig eine Datenspeicherung angeordnet wird -, durch Abfragen der auf Vorrat gespeicherten Daten die „Vergangenheit zu entschlüsseln“, 70

vgl. Schlussanträge des Generalanwalts am EuGH vom 19. Juli 2016 in den Verfahren C-203/15, C-698/15, juris, Rn. 178 ff. 71

Eine gezielte Überwachungsmaßnahme ist hingegen auf Personen gerichtet, bei denen zuvor festgestellt wurde, dass sie in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnten. Solche gezielten Maßnahmen erlauben es den Strafverfolgungsbehörden nur, auf Kommunikationsdaten dieser Personen zurückzugreifen, die von den betreffenden Personen nach ihrer Identifizierung abgewickelt wurden. Dagegen erfasst eine generelle Verpflichtung zur Vorratsdatenspeicherung alle Kommunikationsvorgänge sämtlicher Nutzer, ohne dass irgendein Bezug zu einer schweren Straftat erforderlich ist. Diese Verpflichtung ermöglicht es den Strafverfolgungsbehörden damit, auf alle zurückliegenden Kommunikationsvorgänge einer Person zuzugreifen, bevor bei ihr ein solcher Bezug festgestellt wurde. Insofern verleiht diese Verpflichtung den Strafverfolgungsbehörden die begrenzte Fähigkeit zur Entschlüsselung der Vergangenheit, indem sie ihnen Zugang zu den Kommunikationsvorgängen gewährt, die diese Personen vor ihrer Identifizierung abwickeln. 72

Im Rahmen des vorliegenden Verfahrens ist ferner davon auszugehen, dass die gesetzliche Regelung zur generellen Vorratsdatenspeicherung für die Bekämpfung schwerer Kriminalität erforderlich ist. 73

Eine Maßnahme kann grundsätzlich nur dann als erforderlich angesehen werden, wenn es keine andere Maßnahme gibt, die genauso geeignet, jedoch weniger belastend ist. Eine weniger eingreifende Regelung, die ebenso effektiv – insbesondere im Hinblick auf die „Entschlüsselung der Vergangenheit“ - ist, ist nicht ersichtlich, 74

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 298. 75

Es ist im Rahmen des vorliegenden Verfahrens auch nicht davon auszugehen, dass sich die Auferlegung der generellen Speicherungspflicht gegenüber den betroffenen Dienstanbietern als unverhältnismäßiger Eingriff darstellt. 76

Soweit die Antragstellerin die „anlasslose“ Speicherung von Internetzugangsdaten grundsätzlich wegen ihrer Reichweite als einen unverhältnismäßigen Eingriff in Art. 12 Abs. 1 GG ansieht, steht dem entgegen, dass das Bundesverfassungsgericht die Vorgängerregelungen für die Vorratsdatenspeicherung auf der Grundlage des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. I S. 3192) zwar wegen teilweiser unverhältnismäßiger Ausgestaltung der gesetzlichen Regelungen für verfassungswidrig erklärt hat, gleichwohl aber betont hat, dass eine „Vorratsdatenspeicherung“ grundsätzlich als zulässig, geeignet und erforderlich angesehen wird, um eine zeitgemäße Strafverfolgung und Gefahrenabwehr betreiben zu können. Die Datenspeicherung ist hiernach dann verhältnismäßig und zulässig, wenn sie bestimmte Zwecke verfolgt und in eine dem Eingriff adäquate gesetzliche Ausgestaltung eingebettet ist, 77

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Leitsatz 3a und Rn. 205 ff., 293 ff. 78

Im Übrigen setzt sich die Gesetzesbegründung mit diesem Aspekt ausdrücklich auseinander und kommt zu dem Schluss, dass der Gesetzentwurf den verfassungs- rechtlichen Vorgaben dadurch gerecht werde, dass er eine möglichst begrenzte Speicherpflicht mit strengen Abrufungsregelungen kombiniere, 79

vgl. BT-Drs. 18/5088, S. 23 ff. 80

Allerdings ist unter Berücksichtigung des Urteils des EuGH vom 21. Dezember 2016 – C-203/15 und C-698/15 – derzeit offen, ob davon auszugehen ist, dass die TKG-Vorschriften über die generellen Speicherungspflichten europarechtlicher Überprüfung standhalten werden. Denn den Ausführungen des EuGH, dass Art. 15 Abs. 1 der Richtlinie 2002/58 im Lichte der Art. 7,8 und 11 sowie des Art. 52 Abs. 1 EuGRCh dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsdatenspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht, könnte zu entnehmen sein, dass eine „anlasslose“, generelle Speicherung grundsätzlich europarechtswidrig ist. 81

Ob dies allerdings auch dann gilt, wenn die nationale „anlasslose“ Speicherungsverpflichtung mit gesetzlichen Garantien hinsichtlich des Datenzugangs, der Dauer der Vorratsdatenspeicherung sowie des Schutzes und der Sicherheit der Daten einhergeht, bedarf der vertieften Überprüfung im Hauptsacheverfahren. 82

Jedenfalls kann im Rahmen des vorliegenden Verfahrens nicht festgestellt werden, dass die gesetzlichen Regelungen des TKG über die Speicherpflichten als Verstoß gegen die Richtlinie 2002/58 offensichtlich europarechtswidrig sind, indem sie u.a. gegen Art. 15 Abs. 1 der Richtlinie 2002/58 verstoßen. Nach dieser Bestimmung können die Mitgliedstaaten u.a. durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Diese ausdrückliche Bezugnahme auf die Verpflichtung zur Vorratsdatenspeicherung bestätigt im Grunde, dass die Verpflichtung als solche mit der durch die Richtlinie 2002/58 geschaffenen Regelung grundsätzlich nicht unvereinbar ist. Die angeführte Formulierung sieht zwar nicht ausdrücklich vor, dass eine generelle Verpflichtung zur Vorratsdatenspeicherung eingeführt werden kann, doch ist festzustellen, dass sie ihr auch nicht entgegensteht, 83

84

so ausdrücklich: Schlussanträge des Generalanwalts am EuGH vom 19. Juli 2016 in den Verfahren C-203/15, C-698/15, juris, Rn. 106.

So vertritt der Generalanwalt am EuGH in seinen Schlussanträgen zu den Vorgaben des Unionsrechts für im nationalen Recht vorgesehene Vorratsdatenspeicherung ausdrücklich die Auffassung, dass eine generelle Verpflichtung zur Vorratsdatenspeicherung mit der durch die Richtlinie 2002/58 geschaffenen Regelung vereinbar ist, und dass ein Mitgliedstaat von der durch Art. 15 Abs. 1 der Richtlinie eingeräumten Befugnis Gebrauch machen kann, um eine solche Verpflichtung aufzuerlegen, wenn die Inanspruchnahme dieser Befugnis von der Einhaltung strenger Voraussetzungen abhängig gemacht wird, die sich nicht nur aus der genannten Bestimmung, sondern auch aus den einschlägigen Bestimmungen der EuGRCh im Lichte des Urteils des EuGH vom 8. April 2014 - C-293/12, C-594/12 - ergeben, 85

vgl. Schlussanträge des Generalanwalts am EuGH vom 19. Juli 2016 in den Verfahren C-203/15, C-698/15, juris, Rn. 116. 86

Ferner spricht auch Vieles dafür, dass dem Urteil des EuGH vom 8. April 2014 – C-293/12, C-594/12 -, mit dem dieser die Richtlinie 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 (RL 24/2006) für ungültig erklärt hat, nicht zwingend entnommen werden kann, dass eine anlasslose (generelle) Speicherungspflicht grundsätzlich nicht mit Europarecht vereinbar ist. Denn der EuGH hat in dem genannten Urteil im Grunde nur festgestellt, dass eine generelle Verpflichtung zur Vorratsdatenspeicherung über das absolut Notwendige (nur) dann hinausgeht, wenn sie nicht mit strengen Garantien bezüglich des Datenzugangs, der Dauer der Vorratsspeicherung sowie des Schutzes und der Sicherheit der Daten einhergeht, 87

vgl. EuGH, Urteil vom 8. April 2014, a.a.O., juris, Rn. 56-69 88

Hingegen dürfte den Ausführungen des EuGH nicht zu entnehmen sein, dass der EuGH in seinem Urteil vom 8. April 2014 darüber befunden hat, ob eine generelle Verpflichtung zur Vorratsdatenspeicherung, die mit diesen Garantien einhergeht, mit dem Unionsrecht vereinbar ist, da eine solche Regelung nicht Gegenstand der dem EuGH in jener Rechtssache vorgelegten Fragen war, 89

in diesem Sinne: Schlussanträge des Generalanwalts am EuGH vom 19. Juli 2016 in den Verfahren C-203/15, C-594/12, juris, Rn. 195 f.; so auch Begründung des Entwurfs eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, BT-Drs. 18/5088, S. 23 (Mitte). 90

Mit der Argumentation des Generalanwalts in seinen Schlussanträgen zu der Frage einer generellen Speicherungsverpflichtung, die weitgehend der Interpretation des deutschen Gesetzgebers entspricht, und die der Generalanwalt selbst aus dem Urteil des EuGH vom 8. April 2014 ableitet, setzt sich der EuGH in seinem Urteil vom 21. Dezember 2016 nicht explizit auseinander, so dass offen bleibt, inwiefern der EuGH in seinem Urteil vom 21. Dezember 2016 von seiner im Urteil vom 8. April 2014 geäußerten Rechtsauffassung abweichen will. Zur Begründung der Auffassung des EuGH im Urteil vom 21. Dezember 2016 wird ferner häufig auf Ausführungen in seinem Urteil vom 8. April 2014 Bezug genommen, die jedoch, wie oben ausgeführt, nicht eindeutig sind, sondern sich auch dahingehend interpretieren lassen, dass eine generelle Vorratsdatenspeicherung mit Art. 15 Abs. 1 der Richtlinie 2002/58 unter bestimmten, eingeschränkten Voraussetzungen vereinbar sein kann. 91

Darüber hinaus wird im Rahmen der Entscheidung des EuGH vom 21. Dezember 2016 an mehreren Stellen auf die nationalen Regelungen, die Gegenstand der Vorlagebeschlüsse sind, Bezug genommen. Diese nationalen Regelungen unterscheiden sich aber in wesentlichen Punkten – wie Speicherungsdauer und –umfang, den Zugangsregelungen zu den gespeicherten Daten sowie den Maßnahmen zur Datensicherung - deutlich von der deutschen Regelung. So sind nach den für Schweden geltenden gesetzlichen Regelungen unterschiedslos alle Daten für sechs Monate zu speichern, die bei Telefoniediensten, bei der Mobilfunktelefonie, bei der elektronischen Nachrichtenübermittlung, beim Internetzugang und bei der Bereitstellung von Kapazitäten für den Internetzugang (Art der Verbindung) erzeugt oder verarbeitet werden. Ausgeschlossen sind hingegen die übermittelten Inhalte,

vgl. EuGH vom 21. Dezember 2016, a.a.O., Rn. 17-19. 92

Bei der Beschaffung von Informationen dürfen die nationale Polizeibehörde, die Sicherheitspolizei und die Zollbehörde unter den im Gesetz festgelegten Voraussetzungen bei einem Betreiber elektronischer Kommunikationsnetze oder – dienste (sogar) ohne dessen Wissen Daten über in einem elektronischen Kommunikationsnetz übermittelte Nachrichten, in einem bestimmten geografischen Gebiet befindliche elektronische Kommunikationsgeräte sowie das oder die geografischen Gebiete, in dem oder denen sich ein elektronisches Kommunikationsgerät befindet oder befunden hat, erfassen, 93

vgl. EuGH, Urteil vom 21. Dezember 2016, a.a.O., Rn. 21. 94

Die Daten dürfen grundsätzlich erfasst werden, wenn die Maßnahme nach den Umständen von besonderer Bedeutung ist für die Verhütung, Abwendung oder Feststellung krimineller Handlungen, bei denen es sich entweder um eine oder mehrere Straftaten handelt, die mit mindestens zweijährigem Freiheitsentzug geahndet werden, oder um eine der in § 3 des Gesetzes aufgeführten Taten, auch wenn die Strafandrohung unter zwei Jahre Freiheitsentzug beträgt. Die Entscheidung über die Vornahme dieser Maßnahme wird von dem Leiter der betreffenden Behörde oder einer hierzu beauftragten Person getroffen und unterliegt keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsbehörde, 95

vgl. EuGH, Urteil vom 21. Dezember 2016, a.a.O., Rn. 22,23. 96

Darüber hinaus haben die Betreiber elektronischer Kommunikationsdienste der Staatsanwaltschaft, der nationalen Polizeibehörde, der Sicherheitspolizei oder sonstigen mit der Kriminalitätsbekämpfung betrauten Behörden auf Verlangen Teilnehmeranschlussdaten zu übergeben, falls sich die Daten auf eine mutmaßliche Straftat beziehen, wobei es sich nicht um eine schwere Straftat handeln muss, 97

vgl. EuGH, Urteil vom 21. Dezember 2016, a.a.O., Rn. 25 ff. 98

Die Sicherheitsmaßnahmen zum Schutz der auf Vorrat gespeicherten Daten beschränken sich auf die Vorgabe, geeignete technische und organisatorische Maßnahmen hierfür zu treffen, 99

vgl. EuGH, Urteil vom 21. Dezember 2016, a.a.O., Rn. 28. 100

Das Recht des Vereinigten Königreichs bleibt noch weit hinter diesen Anforderungen zurück. Hier kann der Minister durch Anordnung (ohne gesetzliche Grundlage) von einem Betreiber eines öffentlichen Telekommunikationsdienstes verlangen, relevante Kommunikationsdienste 101

auf Vorrat zu speichern, wenn er dies für einen oder mehrere Zwecke, die im Gesetz von 2000 zur Regelung von Ermittlungsbefugnissen aufgeführt sind, für erforderlich und verhältnismäßig hält, wobei die dort genannten Zwecke sehr weitreichend sind und u.a. auch rein wirtschaftlichen Interessen des Staates dienen können. Hervorzuheben ist insbesondere, dass eine Datenerhebung auch zu jedem Zweck möglich ist, der „in einer Verordnung des Ministers des Innern eigens aufgeführt wird“. Die Höchstdauer einer solchen Maßnahme darf zwölf Monate nicht übersteigen. Die Ausgestaltung der Datenweitergabe und die Sicherheitsstandards bleiben weit hinter der deutschen Regelung zurück,

vgl. im Einzelnen die Darstellung im Urteil des EuGH vom 21. Dezember 2016, a.a.O., Rn. 29-43. 102

Es kann daher nicht ausgeschlossen werden, dass diese (anderen) nationalen Regelungen das Ergebnis der Rechtsprüfung des EuGH nicht unwesentlich beeinflusst haben. 103

Darüber hinaus kann vorliegend bei summarischer Prüfung auch nicht festgestellt werden, dass die streitgegenständlichen gesetzlichen Regelungen des TKG nicht den im Urteil des EuGH vom 8. April 2014 geforderten Anforderungen entsprechen. So kann der Begründung des Gesetzes entnommen werden, dass der Gesetzgeber die Vorgaben der Grundrechtscharta, wie sie der EuGH in seinem Urteil vom 8. April 2014 zur Richtlinie 2006/24/EG präzisiert hat, beachtet hat. Zur Begründung wird insoweit im Wesentlichen ausgeführt, dass der Gesetzentwurf den vom EuGH genannten verfassungs- und europarechtlichen Vorgaben dadurch Rechnung trage, dass er eine möglichst begrenzte Speicherpflicht mit strengen Abrufregelungen kombiniere. Er sehe einerseits eine (nur) zehnwöchige Speicherung von genau bezeichneten Verkehrsdaten - bei Standortdaten sogar nur eine vierwöchige Speicherung - bei den Erbringern öffentlich zugänglicher Telekommunikationsdienste zu Zwecken der Strafverfolgungsvorsorge und zur Gefahrenabwehr vor und ermögliche den Abruf der Daten durch staatliche Stellen andererseits nur unter sehr engen Voraussetzungen. Schon die Verpflichtung zur Speicherung werde – entsprechend den Anforderungen des EuGH – auf das absolut Notwendige beschränkt. Daten von Diensten der elektronischen Post seien vollständig von der Speicherpflicht ausgenommen. Zum Schutz des besonderen Vertrauensverhältnisses seien Verkehrsdaten, die sich auf Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen bezögen, grundsätzlich von der Speicherpflicht ausgenommen. Detaillierte und normenklare Regeln begrenzten die Verwendung der Daten und gewährleisteten ihre Sicherheit, 104

vgl. BT-Drs. 18/5088, S. 23 f. 105

Inwiefern insbesondere nach diesen Ausführungen zum nur begrenzten Umfang der Speicherungspflicht, die auch in den gesetzlichen Regelungen des TKG ihrer Niederschlag gefunden haben, überhaupt bei der deutschen Regelung von einer allgemeinen und unterschiedslosen Vorratsdatenspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel gesprochen werden kann, die der EuGH in seiner Entscheidung vom 21. Dezember 2016 als mit Art. 15 Abs. 1 der Richtline 2006/24 unvereinbar beanstandet, 106

EuGH, Urteil vom 21. Dezember 2016, a.a.O., juris, Rn. 97, 107

ist daher offen. 108

109

Ob damit die deutsche Regelung mit den Vorgaben des EuGH in beiden genannten Urteilen übereinstimmt, bedarf wegen der Komplexität und des Umfangs der zu beantwortenden Fragen einer vertieften Überprüfung im Hauptsacheverfahren.

Soweit die Antragstellerin darauf verweist, dass selbst dann, wenn eine anlasslose Bevorratung von Telekommunikations-Verkehrsdaten mit den Grundrechten der Betroffenen vereinbar wäre, die anlasslose Speicherung bei den von ihr zu speichernden Daten wegen der besonders hohen Sensibilität von Internetzugangsdaten auf der Grundlage des § 113b Abs. 3 TKG über das grundrechtlich hinnehmbare Maß hinausgehe, ist dem – jedenfalls im Rahmen des vorliegenden Eilverfahrens - entgegen zu setzen, dass das Bundesverfassungsgericht in seinem Urteil zur „Vorratsdatenspeicherung“ zu dem Ergebnis kommt, dass weniger strenge verfassungsrechtliche Maßgaben gelten für eine nur mittelbare Verwendung der vorsorglich gespeicherten Daten in Form von behördlichen Auskunftsansprüchen gegenüber den Diensteanbietern hinsichtlich der Anschlussinhaber bestimmter IP-Adressen, die diese unter Nutzung der vorgehaltenen Daten zu ermitteln haben. Die Schaffung von solchen Auskunftsansprüchen ist nach dieser Entscheidung unabhängig von begrenzenden Rechtsgüter- oder Straftatenkatalogen insgesamt weitergehend zulässig als die Abfrage und Verwendung der Telekommunikationsverkehrsdaten selbst, 110

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 254 ff.. 111

Zwar verweist die Antragstellerin in diesem Zusammenhang darauf, dass die Ausführungen des Bundesverfassungsgerichts zur Bevorratung von Internetzugangsdaten mittlerweile überholt seien, geht dabei aber von einer fehlerhaften Vorstellung hinsichtlich des notwendigen Umfangs der von ihr zu speichernden Daten aus, wie unten noch auszuführen sein wird. 112

Die Speicherungspflichten überschreiten die Grenze der Verhältnismäßigkeit auch nicht durch den technischen Aufwand, den sie den Diensteanbietern abverlangen. Hierbei ist insbesondere zu berücksichtigen, dass jedenfalls ein Großteil der nach § 113b TKG zu speichernden Daten ohnehin von den meisten betroffenen Telekommunikationsunternehmen vorübergehend für eigene Zwecke gespeichert wird. 113

Es ist im vorliegenden Verfahren auch nicht davon auszugehen, dass die Speicherungspflicht in Bezug auf die finanziellen Lasten, die den Unternehmen durch die Speicherungspflicht nach § 113b TKG und die hieran knüpfenden Folgeverpflichtungen wie die Gewährleistung von Datensicherheit erwachsen, unverhältnismäßig ist. Dabei ist zu beachten, dass der Gesetzgeber einen weiten Gestaltungsspielraum dahingehend hat, welche Pflichten zur Sicherstellung von Gemeinwohlbelangen er Privaten im Rahmen ihrer Berufstätigkeit auferlegt, 114

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O, juris, Rn. 301. 115

Grundsätzlich kann er Lasten und Maßnahmen zur Wahrung von Gemeinwohlbelangen, die als Folge kommerzieller Aktivitäten regelungsbedürftig sind, den entsprechenden Marktakteuren auferlegen, um die damit verbundenen Kosten auf diese Weise in den Markt und den Marktpreis zu integrieren. Dabei ist der Gesetzgeber nicht darauf beschränkt, Private nur dann in Dienst zu nehmen, wenn ihre berufliche Tätigkeit unmittelbar Gefahren auslösen kann oder sie hinsichtlich dieser Gefahren unmittelbar ein Verschulden trifft. Vielmehr reicht insoweit eine hinreichende Sach- und Verantwortungsnähe zwischen der beruflichen Tätigkeit und der auferlegten Verpflichtung, 116

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 301. 117

Eine solche hinreichende Sach- und Verantwortungsnähe besteht entgegen der von der Antragstellerin geäußerten Rechtsauffassung „zwischen“ der Vorratsdatenspeicherung und den durch die gesetzlichen Regelungen zur Datenspeicherung in Pflicht genommenen Telekommunikationsunternehmen. Deshalb geht die bundesverfassungsgerichtliche Rechtsprechung auch davon aus, dass gegen die den Speicherungspflichtigen erwachsenen Kostenlasten grundsätzlich keine Bedenken bestehen. Der Gesetzgeber verlagert auf diese Weise die mit der Speicherung verbundenen Kosten entsprechend der Privatisierung des Telekommunikationssektors insgesamt in den Markt. Auch werden hierbei nicht einzelnen Diensteanbietern einzelfallbezogene Sonderopfer auferlegt, sondern in allgemeiner Form die Rahmenbedingungen für die Erbringung von Telekommunikationsdiensten ausgestaltet. Allein die gemeinwohlbezogene Zielsetzung gebietet es nicht, hierfür einen Kostenersatz vorzusehen. Ein Gesetz, das die Berufsausübung in der Weise regelt, dass es Privaten bei der Ausübung ihres Berufs Pflichten auferlegt und dabei regelmäßig eine Vielzahl von Personen betrifft, ist nicht bereits dann unverhältnismäßig, wenn es einzelne Betroffene unzumutbar belastet, sondern erst dann, wenn es bei einer größeren Betroffenengruppe das Übermaßverbot verletzt, 118

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 302. 119

Soweit die Antragstellerin einwendet, eine „hinreichende Sach- und Verantwortungsnähe“, welche die entschädigungslose Indienstnahme eines Unternehmens für einen hoheitlichen Zweck rechtfertigen könnte, bestehe nicht, stehen dieser Annahme die insoweit eindeutigen Ausführungen des Bundesverfassungsgerichts entgegen, dass der Gesetzgeber mit der Verlagerung der aus den Speicherungspflichten erwachsenden Kostenlasten auf die im Markt tätigen Unternehmen den Umstand berücksichtige, dass die Telekommunikationsunternehmen die neuen Chancen der Telekommunikationstechnik, die mit Sicherheitsrisiken verbunden sind, zur Gewinnerzielung nutzen könnten. Damit stünden die den Unternehmen auferlegten Pflichten in engem Zusammenhang mit den von ihnen erbrachten Dienstleistungen und könnten als solche nur von ihnen erbracht werden, 120

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 302. 121

Umso weniger bestehen verfassungsrechtliche Bedenken gegen die durch die heutige gesetzliche Regelung auferlegte Kostenlast der betroffenen Unternehmen vor dem Hintergrund, dass nach § 113a Abs. 2 TKG – anders als noch nach der Vorläufervorschrift – für notwendige Aufwendungen, die den Verpflichteten durch die Umsetzung der Vorgaben aus den §§ 113b, 113d bis 113g TKG entstehen, eine angemessene Entschädigung zu zahlen ist, soweit dies zur Abwendung oder zum Ausgleich unbilliger Härten geboten erscheint. Für die Bemessung der Entschädigung sind die tatsächlich entstandenen Kosten maßgebend, wobei über Anträge auf Entschädigung die Bundesnetzagentur zu entscheiden hat. Es sind im Rahmen des vorliegenden Verfahrens keine Gründe dafür ersichtlich, dass diese Entschädigungsregelung auf die Antragstellerin, wenn in ihrem Fall tatsächlich eine unbillige Härte vorliegen sollte, keine Anwendung finden könnte. 122

Die Entschädigungsregelung ist entgegen der Auffassung der Antragstellerin auch hinreichend bestimmt. Soweit die Antragstellerin ausführt, um die grundrechtlichen Anforderungen an die gebotene Entschädigungsregelung zu konkretisieren, könne die zu Art. 14 Abs. 1 Satz 2 GG ergangene Rechtsprechung zu der sogenannten ausgleichspflichtigen Inhaltsbestimmung des Eigentums herangezogen werden, steht dem entgegen, dass die Rechtsprechung zur ausgleichspflichtigen Inhaltsbestimmung auf Eingriffe in die 123

Berufsfreiheit – und nur ein solcher steht vorliegend in Rede – nicht übertragen werden kann. Das Konzept der Entschädigung ist auf solche Rechtspositionen ausgerichtet und beschränkt, die dem Schutz der Eigentumsgarantie aus Art. 14 GG unterstehen,

vgl. BGH, Urteil vom 14. März 1996 – III ZR 224/94, juris, Rn. 19, 20; Beschluss vom 27. Mai 1993 – III ZR 142/92 -, juris, Rn. 3. 124

Im Übrigen handelt es sich bei dem in § 113a Abs. 2 TKG verwandten Begriff der „unbilligen Härte“ zwar um einen unbestimmten, aber auslegungsfähigen Rechtsbegriff, der in vielen Gesetzen u.a. im Rahmen von Entschädigungsregelungen Verwendung findet, und von dem grundsätzlich nicht angenommen wird, er sei inhaltlich zu „unbestimmt“. Eine „unbillige Härte“ ist hiernach in der Regel dann anzunehmen, wenn ohne die Gewährung einer teilweisen Entschädigung dem Betroffenen Nachteile entstehen, die über die Ziele des jeweiligen Gesetzes hinaus gehen und die nicht oder nur schwer wieder gut zu machen sind. Dies trifft z.B. bei drohender Insolvenz oder Existenzgefährdung zu, 125

vgl. z.B. VG Potsdam, Urteil vom 20. Juni 2003 – 3 K 3663/02 - zu § 70 TierSG, juris, Rn. 20; Kopp, VwGO, 22. Auflage, § 80 Rn. 116. 126

Das Bundesverfassungsgericht sah zudem keine Verletzung des Übermaßverbotes bei der gesetzlichen Vorgängerregelung, die keine ausdrückliche Entschädigungsregelung für betroffene Unternehmen vorsah, weil nicht erkennbar war, dass die mit den auferlegten Speicherungspflichten bestehenden Kostenlasten erdrosselnde Wirkung hatten, 127

BVerfG, Beschluss vom 2. März 2010, a.a.O., juris, Rn. 302 am Ende. 128

Berücksichtigt man, dass in § 113a Abs. 2 TKG eine Entschädigungsregelung vorgesehen ist, liegt es daher fern, unter diesem Aspekt einen unverhältnismäßigen Eingriff in die Berufsausübungsfreiheit anzunehmen. Der Gesetzgeber war damit nicht nur bemüht, die durch die Neuregelung entstehenden finanziellen und sonstigen Belastungen für die Telekommunikationsunternehmen durch Entlastungsregelungen zu begrenzen und besondere Härten für kleinere Anbieter abzufedern, sondern auch die Belange der Telekommunikationsunternehmen mit den öffentlichen Interessen in sachgerechter Weise auszugleichen. 129

Sind damit die Regelungen über die Speicherungs- und Übermittlungspflichten betroffener Telekommunikationsunternehmen grundsätzlich als verfassungsgemäßer Eingriff in die durch Art. 12 Abs. 1 GG geschützte Berufsausübungsfreiheit zu werten, hat die Antragstellerin darüber hinaus gehend nicht glaubhaft gemacht, dass – gerade im Falle von Telekommunikationsunternehmen, die, wie sie, „nur“ Internet-Dienstleistungen ausschließlich für Geschäftskunden anbieten – aus dem Gesichtspunkt der Verhältnismäßigkeit zusätzliche Härte- oder Ausnahmeregelungen geboten gewesen wären, 130

vgl. zu diesem Aspekt: BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 303. 131

Die seitens der Antragstellerin beanstandete Reichweite der Speicherpflicht als zu weitgehend einerseits, andererseits aber auch die gleichzeitig beanstandete Lückenhaftigkeit der Telekommunikationsüberwachung rechtfertigen nicht den Schluss, die Verpflichtung zur generellen Speicherung für ihren Gesetzeszweck (Sicherung der Strafverfolgung und Gefahrenabwehr) als unverhältnismäßig bzw. als generell ungeeignet anzusehen. 132

133

Die von der Antragstellerin befürchtete zu weitgehende Reichweite der Speicherpflicht besteht nach der gesetzlichen Regelung nicht. So trägt die Antragstellerin vor, dass die Mehrfachvergabe dynamischer IP-Adressen dazu führe, dass zu einer eindeutigen Identifizierung des einzelnen Nutzers eine Vielzahl weiterer Daten erforderlich sei. Die eindeutige Zuordnung einer dynamischen IP-Adresse zu einem Nutzer erfordere nach heutigem Stand der Technik (Version 4 des Internetprotokolls) bzw. aufgrund der Mehrfachvergabe externer IP-Adressen (nach der derzeitigen Form des Carrier-Grade Network Address Translation-Verfahrens-CNAT -) zusätzliche Kenntnis über die interne IP-Adresse und interne Port-Nummer, die zugeordnete externe IP-Adresse und externe Port-Nummer, die jeweilige Ziel-IP-Adresse und Ziel-Port-Nummer sowie den präzisen Zeitstempel der Zuordnung. Würden alle diese Daten erhoben, würden lückenlos Rückschlüsse auf die genutzten Dienste möglich sowie Erkenntnisse darüber, wer, wann auf welches Ziel zugegriffen habe, so dass ein umfassendes Nutzerprofil erstellt werden könne. Diese Gefahr besteht allerdings schon deshalb nicht, da die gesetzliche Speicherverpflichtung keineswegs eine derart umfassende Speicherung verlangt. § 113b Abs. 3 TKG verpflichtet die Antragstellerin als Erbringerin öffentlich zugänglicher Internetzugangsdienste (lediglich) dazu, die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse (Ziffer 1), eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung (Ziffer 2) als auch Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse unter Angabe der zugrunde liegenden Zeitzone (Ziffer 3) zu speichern. Die weiteren von der Antragstellerin genannten Speichererfordernisse finden sich nicht in der Norm. Dies hat die Antragsgegnerin im Schriftsatz vom 13. September 2016, der im Verfahren 9 K 3859/16 vorgelegt worden ist, auch nochmals nachvollziehbar bestätigt.

Soweit die Antragstellerin meint, im Falle der bloßen Speicherung der in § 113b Abs. 3 Ziffern 1- 3 TKG ausdrücklich genannten Daten sei die Regelung ungeeignet, weil auf Basis dieser Daten immer nur ein kleiner Kreis von Anschlüssen identifiziert werden könne, und es den Anbietern von Internetzugangsdiensten vor dem Hintergrund, dass eine umfassende Einführung von CNAT in allen Netzen in den nächsten Jahren zu erwarten sei, nicht zuzumuten sei, lediglich für die Zwischenzeit bis zu einer flächendeckenden Umstellung auf CNAT eine sehr kostenaufwändige Bevorratungsinfrastruktur aufzubauen, ist darauf hinzuweisen, dass der Gesetzgeber verfassungsrechtlich nicht gehalten ist, ein lückenloses Überwachungssystem zu garantieren. Er hat vielmehr gerade auch die Gesichtspunkte der Erforderlichkeit und Angemessenheit eines Eingriffs zu beachten und Schutzgüter abzuwägen. Ferner darf er auch aus Praktikabilitätsgründen generalisieren, typisieren und pauschalieren und hat hierbei generell einen verhältnismäßig weiten Gestaltungsspielraum, 134

vgl. BVerfG, Beschluss vom 4. April 2001 – 1 BvL 7/98 -, Juris, Rn. 42 f. m.w.N.. 135

Auch wenn eine Datenspeicherung nicht sicherstellen kann, dass alle Telekommunikationsverbindungen verlässlich bestimmten Anschlussnehmern zugeordnet werden können, kann dies der Geeignetheit einer solchen Regelung nicht entgegengehalten werden. Diese erfordert nicht, dass das Regelungsziel in jedem Einzelfall tatsächlich erreicht wird, sondern verlangt lediglich, dass die Zweckerreichung gefördert wird, 136

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 207. 137

Dass eine Förderung des Gesetzeszwecks aufgrund der in § 113b Abs. 3 TKG begrenzten Datenspeicherung ausgeschlossen ist, lässt sich im vorliegenden Verfahren nicht feststellen. Zwar mag aufgrund der nur begrenzten Speicherungsverpflichtung möglicherweise nicht jedes berechtigte Auskunftsverlangen zu einem unmittelbaren Erfolg bei der Strafverfolgung 138

führen. Es ist aber nicht von der Hand zu weisen, dass es ohne die Speicherung von Internetzugangsdaten in vielen Deliktsbereichen bereits an einem ersten Ermittlungsansatz fehlte. Selbst wenn bei Einsatz des CNAT-Verfahrens ohne die Speicherung der Portadresse nur ein Kreis von Personen und nicht eine Einzelperson ermittelt werden kann, kann diese Information Ausgangspunkt weiterer Ermittlungen sein.

Der von der Antragstellerin weiter hervorgehobene Umstand, dass die Erhebung der von ihr zu speichernden Internetzugangsdaten wegen ihres Kundenkreises im Wesentlichen nicht der Bekämpfung schwerer Kriminalität dienen können, sondern im Wesentlichen „nur“ die Aufklärung von Betrugsstraftaten, Cyber-Kriminalität, Straftaten gegen die Integrität und Vertraulichkeit von Daten ermöglichen dürfte, ein Auskunftsverlangen der Strafverfolgungsbehörden auf der Grundlage des § 100g Abs. 2 StPO auf diese Straftaten aber nicht gestützt werden könne, führt ebenfalls nicht zur Annahme der Unverhältnismäßigkeit der gesetzlichen Regelung. Denn selbst wenn dem so wäre, wäre die Inanspruchnahme der Antragstellerin zur Datenspeicherung vom weiten Gestaltungsspielraum des Gesetzgebers umfasst und überschritte die verfassungsrechtlich zulässige Grenze schon deshalb nicht, weil verfassungsrechtlich nicht zu fordern ist, dass das Regelungsziel des Gesetzes in jedem Einzelfall tatsächlich erreicht wird. Verlangt wird lediglich, dass die Zweckerreichung gefördert wird, 139

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 207. 140

Dass kein Fall denkbar ist, in dem die von der Antragstellerin zu speichernden Daten zur Bekämpfung schwerer Kriminalität dienlich sein können, wird von ihr selbst nicht behauptet. 141

Soweit die Antragstellerin darauf hinweist, bei den von ihr angegriffenen gesetzlichen Regelungen sei nach dem Bundeverfassungsgericht im Rahmen der Verhältnismäßigkeit einer Regelung auch die „Überwachungs-Gesamtrechnung“ zu überprüfen, dürfte dieses Vorbringen auf Ausführungen des Bundesverfassungsgerichts in seinem Urteil zur Vorratsdatenspeicherung vom 2. März 2010 abzielen, nach denen auszuschließen ist, dass die zulässige Speicherung von Telekommunikationsverkehrsdaten als Vorbild für weitere anlasslose Datensammlungen dient. Der Gesetzgeber sei bei der Einführung neuer Speicherpflichten gezwungen, die Gesamtheit der schon vorhandenen Datensammlungen in den Blick zu nehmen. Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung von Telekommunikationsverkehrsdaten setze vielmehr voraus, dass diese eine Ausnahme bleibe. Sie dürfe auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen, 142

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 218. 143

Vorliegend ist nicht erkennbar, dass die konkrete Ausgestaltung der Speicherpflichten diese Grenze überschreitet. Denn gemäß § 113b Abs. 5 TKG dürfen die dort genannten Daten nicht gespeichert werden. Hinsichtlich der zu speichernden Daten ist die Speicherfrist im Vergleich zur Vorgängerregelung deutlich verkürzt und auf vier bzw. zehn Wochen beschränkt, vgl. § 113b Abs. 1 TKG, wobei selbst die undifferenzierten längeren Speicherfristen der Vorgängerregelung als verfassungsrechtlich zulässig erachtet worden sind, 144

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 216 f. 145

Nach Ablauf der Speicherfrist müssen die Daten irreversibel gelöscht werden und sind somit nicht mehr rekonstruierbar, vgl. § 113b Abs. 8 TKG. Flankiert werden diese Vorschriften 146

zudem von den Zugriffsschranken des § 100g StPO.

Der Antragstellerin ist auch nicht darin zu folgen, dass zumindest die konkrete Ausgestaltung der Vorratsdatenspeicherung von Internetzugangsdaten durch das von ihr angegriffene Gesetz grundrechtliche Defizite aufweise, die zu einer Verfassungswidrigkeit führten. Diese Defizite beträfen sowohl die Regelungen über die Datenspeicherung selbst als auch die Regelungen über die Auswertung und Übermittlung der gespeicherten Daten durch die Anbieter von Internetzugangsdiensten. 147

Soweit die Antragstellerin sich im Rahmen ihres diesbezüglichen Vortrags darauf bezieht, dass auf der Ebene der Datenspeicherung insbesondere zu bemängeln sei, dass das Gesetz in §§ 113a ff. TKG keine hinreichenden Vorkehrungen zum Schutz von Berufsgeheimnissen vorsehe, ist darauf zu verweisen, dass im Rahmen des vorliegenden Verfahrens Überwiegendes dafür spricht, dass sie, selbst wenn dies der Fall wäre, nicht in eigenen Rechten verletzt wäre, da der Schutz von Berufsgeheimnissen von den betroffenen Kunden geltend zu machen wäre. Unabhängig hiervon ist im Rahmen des vorliegenden Verfahrens aufgrund der durchzuführenden summarischen Überprüfung aber auch nicht erkennbar, dass der Schutz der Berufsgeheimnisträger nicht ausreichend und entsprechend den verfassungsgerichtlichen Vorgaben ausgestaltet wäre. So dürfen Daten, die den in § 99 Abs. 2 TKG genannten Verbindungen zugrunde liegen, ausdrücklich nicht gespeichert werden. Für andere Berufsgruppen trifft § 100g Abs. 4 StPO die Regelung, dass die Erhebung von Verkehrsdaten nach Absatz 2, auch in Verbindung mit Absatz 3 Satz 2, die sich gegen eine der in § 53 Abs. 1 Satz 1 Nummer 1 bis 5 StPO genannten Personen richtet und die voraussichtlich Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte, unzulässig ist. Dennoch erlangte Erkenntnisse dürfen nicht verwendet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und der Löschung der Aufzeichnungen ist aktenkundig zu machen (Sätze 1-4). Die Sätze 2 bis 4 gelten nach Satz 5 entsprechend, wenn durch eine Ermittlungsmaßnahme, die sich nicht gegen eine in § 53 Abs. 1 Satz 1 Nummer 1-5 StPO genannte Person richtet, von dieser Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte. Die Antragstellerin übersieht damit, dass die Speicherregelungen durch strenge Verwendungsregelungen - § 100g Abs. 4 StPO - flankiert werden, die im Strafverfahren ein absolutes Verwertungsverbot zur Folge haben, wenn Daten versehentlich erhoben werden. Insoweit spricht vorliegend Überwiegendes dafür, dass die Vorgaben des Bundesverfassungsgerichts in seiner Entscheidung zur „Vorratsdatenspeicherung“, dass es verfassungsrechtlich als Ausfluss des Verhältnismäßigkeitsgrundsatzes (nur) geboten ist, für einen engen Kreis von auf besondere Vertraulichkeit angewiesene Telekommunikationsverbindungen ein grundsätzliches Übermittlungsverbot vorzusehen, 148

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 238; Beschluss vom 8. Juni 2016 – 1 BvQ 42/15 -, 149

eingehalten worden sind. 150

Darüber hinaus trägt die Antragstellerin vor, die in § 113d TKG enthaltenen Vorgaben zur Datensicherheit verletzten die Grundrechte und Grundfreiheiten der Anbieter von Internetzugangsdiensten, da sie teilweise unklar beziehungsweise faktisch nicht umsetzbar seien. Zudem würden diese Unklarheiten noch durch § 113f TKG verstärkt, der eine Konkretisierung der Vorgaben zur Datensicherheit regeln solle. 151

Auch diese Überlegungen können im Rahmen des vorliegenden Verfahrens zu keinem Erfolg führen. 152

Sowohl das Bundesverfassungsgericht als auch der Gerichtshof der Europäischen Union leiten in ihren Urteilen zur Vorratsdatenspeicherung aus Art. 10 GG und Art. 7 EuGRCh hohe Anforderungen an die technische und organisatorische Sicherung bevorrateter Telekommunikations-Verkehrsdaten her, 153

vgl. BVerfG, Beschluss vom 2. März 2010, a.a.O., juris Rn. 220 ff.; EuGH, Urteil vom 8. April 2014, a.a.O., juris, Rn. 66 f. 154

Nach den Darlegungen des Bundesverfassungsgerichts muss der Gesetzgeber ein besonders hohes Maß an Datensicherheit gewährleisten, das sich fortlaufend dem Entwicklungsstand der Fachdiskussion anpasst. Hierzu muss er den gebotenen Sicherheitsstandard im Gesetz zumindest dem Grunde nach normenklar und verbindlich vorgeben, darf die technische Konkretisierung des vorgegebenen Maßstabs jedoch auch delegieren. Das Bundesverfassungsgericht bezieht sich in diesem Zusammenhang zudem auf schriftliche und mündliche Stellungnahmen von Sachverständigen, die im Rahmen des Vorratsdatenverfahrens eingeholt worden sind, 155

vgl. BVerfG. Beschluss vom 2. März 2010, a.a.O., juris, Rn 223 ff. 156

Hervorzuheben ist, dass sich der Gesetzgeber bei der Konzeption von § 113d TKG die vom Bundesverfassungsgericht im Vorratsdatenurteil konkret genannten Maßnahmen im Wesentlichen zu eigen macht. Das Bundesverfassungsgericht hat diese Maßnahmen nach den Stellungnahmen von sachverständiger Seite für geeignet gehalten, einen besonders hohen Standard der Datensicherheit gesetzlich zu gewährleisten, 157

BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 224 ff. 158

Die Antragstellerin meint zwar, § 113d Nr. 3 TKG, der eine Speicherung der Vorratsdaten „auf vom Internet entkoppelten Datenverarbeitungssystemen“ verlangt, sei technisch nicht umsetzbar. Ob diese Ansicht zutreffend ist, ist jedoch zweifelhaft, da der Anforderungskataloges zu § 113f TKG aufzeigt, wie ein vom Internet entkoppeltes Datensystem ausgestaltet werden kann, 159

vgl. Anforderungskatalog zu § 113f TKG, S. 13 ff., abrufbar auf der Internetseite der BNetzA. 160

Insbesondere wird aber durch die Regelung in § 113f TKG die Vorgabe des Bundesverfassungsgerichts umgesetzt, 161

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, LS 4, 162

dass die zu fordernden hohen Sicherheitsstandards dem Stand der Technik entsprechen und fortlaufend aktualisiert werden müssen. § 113f Satz 1 TKG verpflichtet die Dienstanbieter, bei der Umsetzung der Verpflichtungen der §§ 113b bis 113e TKG einen besonders hohen Standard der Datensicherheit und Datenqualität zu gewährleisten. Satz 2 bestimmt, dass die Antragsgegnerin unter Beteiligung des Bundesamtes für Sicherheit in der Informationstechnik und der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit einen Katalog von Anforderungen für die technischen Vorkehrungen und sonstigen Maßnahmen zur Erfüllung der Verpflichtungen aus den §§ 113b bis 113e TKG erstellt. Durch den Anforderungskatalog wird für die Verpflichteten erkennbar, welche technischen Vorkehrungen und sonstigen Maßnahmen sie zur Erfüllung ihrer Verpflichtungen mindestens einrichten müssen. Dieser Anforderungskatalog, der zum 1. Januar 2017 in Kraft getreten ist, bietet somit auch die von der Antragstellerin vermisste Rechtssicherheit. Denn die Einhaltung der 163

darin geregelten Anforderungen schafft eine gesetzliche Vermutung zugunsten des verpflichteten Unternehmens, dass der nach § 113f TKG geforderte besonders hohe Standard der Datensicherheit und Datenqualität eingehalten wird.

Darüber hinaus bemängelt die Antragstellerin, dass es für kleine und mittlere Unternehmen finanziell unzumutbar sei, die Vorgabe in § 113d Nr. 5 TKG, nach der an jedem Zugriff auf die Vorratsdaten zwei besonders ermächtigte Personen beteiligt sein müssen, umzusetzen. Dies umso mehr, als sie ohnehin schon verpflichtet sei, die notwendige Technik zur Datenspeicherung und –sicherung auf eigene Kosten einzurichten und vorzuhalten. Der Verhältnismäßigkeitsgrundsatz gebiete es daher, kleine und mittlere Unternehmen von dem Vier-Augen-Prinzip freizustellen. 164

Dem ist zum einen entgegen zu halten, dass in § 113a Abs. 2 TKG eine Entschädigungsregelung für Härtefälle vorgesehen ist, zum anderen, dass das Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung eine entschädigungslose Indienstnahme von Unternehmen zur Datenbevorratung verfassungsrechtlich nicht beanstandet hat, 165

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 302 ff. 166

Auch hier gilt – wie bereits ausgeführt -, dass ein Gesetz, das Privaten bei der Ausübung ihres Berufs Pflichten auferlegt und dabei regelmäßig eine Vielzahl von Personen betrifft, nicht bereits dann unverhältnismäßig ist, wenn es einzelne Betroffene unzumutbar belastet, sondern erst dann, wenn es bei einer größeren Betroffenengruppe das Übermaßverbot verletzt, 167

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 302. 168

Es ist nicht erkennbar, dass eine solche generelle Wirkung von den gesetzlich festgelegten Speicherpflichten ausgeht. Eine eventuell erdrosselnde Belastung für kleinere und mittlere Unternehmen wird durch die – hinreichend bestimmte – Entschädigungsregelung in § 113a Abs. 2 TKG aufgefangen. 169

Ferner ist die Antragstellerin der Ansicht, dass auch die gesetzlichen Regelungen über die Auswertung und Übermittlung der bevorrateten Internetzugangsdaten durch die Dienstanbieter die grundrechtlichen Anforderungen verfehlten. So würden die gemäß § 113b TKG zu speichernden Daten in zu weitem Umfang für Bestandsdatenauskünfte im Sinne des § 113 TKG zur Verfügung gestellt. § 113c Abs. 1 Nr. 3 TKG erlaube es den Anbietern von Internetzugangsdiensten, die auf der Grundlage des § 113b Abs. 3 TKG bevorrateten Internetzugangsdaten zu verwenden, um eine IP-Adresse zuzuordnen. Diese Erlaubnis gehe zu weit und verletze darum Art. 10 GG sowie Art. 7 und 8 EuGRCh. Zudem erlaube § 113 Abs. 1 Sätze 1 und 3, Abs. 2 Satz 1 TKG in Verbindung mit § 113c Abs. 1 Nr. 3 TKG im repressiven Bereich die Verwendung von Vorratsdaten nicht nur zur Verfolgung von Straftaten, sondern auch zur Verfolgung von Ordnungswidrigkeiten. Ein abschließender Katalog besonders gewichtiger Ordnungswidrigkeiten, wie ihn das Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung fordere, fehle. Schließlich erlaube § 113 Abs. 1 Sätze 1 und 3, Abs. 2 Satz 1, Abs. 3 Nr. 3 TKG in Verbindung mit § 113c Abs. 1 Nr. 3 TKG die Datenverwendung allgemein zur Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste. Damit würden die Vorratsdaten hinsichtlich dieser Behörden für Auskunftszwecke geöffnet, die weit im Vorfeld konkreter Gefahren liegen können. 170

171

Unabhängig davon, ob die Antragstellerin, die ihre diesbezüglichen Einwände (wiederum) an Grundrechtsverletzungen ihrer Kunden anknüpft, aus diesem Grunde hiermit im vorliegenden Verfahren gehört werden kann, ist hervorzuheben, dass die genannten Regelungen den Dienstanbietern zwar erlauben, zur Beantwortung einer Bestandsdatenabfrage auf die verpflichtend zu speichernden Daten zurückzugreifen, um dann auf dieser Basis das Auskunftsersuchen zu beantworten. Es findet aber – anders als bei einem Ersuchen auf der Grundlage des § 100g StPO - keine direkte Übermittlung von Daten an die ersuchende Behörde statt, vielmehr ist der Dienstanbieter „nur“ zur Auskunft verpflichtet. Nach der Rechtsprechung des Bundesverfassungsgerichts sind für solche Auskünfte weniger strenge Anforderungen zu stellen. Insbesondere sah es den Rückgriff auf die nach der Vorgängerregelung auf der Grundlage des § 113a TKG a.F. gespeicherten Daten für Bestandsdatenauskünfte ohne vorherige richterliche Anordnung für die Verfolgung von Straftaten aller Art und allgemein auch für die Aufgaben der Gefahrenabwehr und der Nachrichtendienste als verfassungsrechtlich zulässig an,

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 289. 172

Für die Frage der erforderlichen Eingriffsermächtigung bei entsprechenden Auskunftsersuchen kam es in verfassungskonformer Auslegung zu dem Ergebnis, dass auf die jeweiligen fachgesetzlichen Eingriffsunterlagen zu verweisen war, 173

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 289. 174

Auch einem Missbrauch dieser allgemeinen Eingriffsermächtigungen zur Umgehung der strengen Voraussetzungen des § 100g StPO konnte nach den Ausführungen des Bundesverfassungsgerichts durch eine verfassungskonforme Auslegung begegnet werden, 175

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O.. juris, Rn. 290. 176

Dass sich an dieser Beurteilung heute etwas geändert haben könnte, ist bei summarischer Prüfung nicht ersichtlich. Darüber hinaus dürfte eine Bestandsdatenauskunft für die Verfolgung und Verhinderung von Ordnungswidrigkeiten bereits schon deshalb unzulässig sein, weil eine solche Auskunftsverpflichtung gegen § 46 Abs. 2 des Gesetzes über Ordnungswidrigkeiten – OWiG – verstoßen dürfte. Die Verwendung der auf der Grundlage des § 113b Abs. 3 TKG gespeicherten Daten durch die Erbringer öffentlich zugänglicher Telekommunikationsdienste für eine Bestandsdatenauskunft ist zwar grundsätzlich zulässig, wenn die Auskunft der Verfolgung von Ordnungswidrigkeiten dient (§ 113 Abs. 2 Satz 1 TKG). Es spricht Vieles dafür, dass aus § 46 Abs. 2 OWiG, nach dem die Verfolgungsbehörde im Sinne des OWiG im Bußgeldverfahren dieselben Rechte und Pflichten wie die Staatsanwaltschaft bei der Verfolgung von Straftaten hat, zu folgern ist, dass Auskunftsersuchen der Ordnungswidrigkeitenbehörden über Umstände, die dem Post- und Fernmeldegeheimnis unterliegen, unzulässig sind. Das Bundesverfassungsgericht hat in seinem Beschluss vom 24. Januar 2012 – 1 BvR 1299/05 – festgestellt, dass die identifizierende Zuordnung dynamischer Internetprotokoll-Adressen eine besondere Nähe zu konkreten Telekommunikationsvorgängen aufweist und damit in den Schutzbereich des Art. 10 Abs. 1 GG fällt, 177

vgl. BVerfGE 110, 151 (181 f.); juris, Rn. 116 ff. 178

Die Zuordnung von dynamischen IP-Adressen im Rahmen einer Bestandsdatenauskunft für die Verfolgung von Ordnungswidrigkeiten dürfte daher unzulässig sein, 179

180

vgl. BT-Drs. 18/5088, S. 40 zu § 113c Abs. 1 TKG.

Soweit die Antragstellerin darüber hinaus Mängel in den Datenverwendungsregeln gemäß § 113c TKG rügt, sind solche im Rahmen der hier nur möglichen summarischen Überprüfung nicht erkennbar. Die Antragstellerin begründet ihre Auffassung, dass die Datenverwendungsregeln in § 113c TKG ebenfalls die Grundrechte der verpflichteten Dienstanbieter aus Art. 12 GG, Art. 15,16 EuGRCh und die Dienstleistungsfreiheit aus Art. 56 AEUV verletzen, im Wesentlichen mit unzumutbaren Rechtsunsicherheiten, die dadurch entstünden, dass unklar sei, inwieweit die Dienstanbieter prüfen dürfen und müssen, ob sie einem behördlichen Auskunftsersuchen nachkommen dürfen. Unklar sei auch, ob ein Dienstanbieter seine Kunden über das Auskunftsverlangen benachrichtigen dürfe. Die von der Antragstellerin befürchteten Unklarheiten bestehen nicht. Das Gesetz regelt in § 113c TKG ausreichend und normenklar die Prüfungsrechte und –pflichten der Anbieter. Die Vorschriften machen hinreichend deutlich, dass den Dienstanbietern weder eine Prüfungspflicht noch eine Prüfungsbefugnis hinsichtlich der Legitimität eines Auskunftsersuchens zukommt. Die auskunftsersuchenden Behörden haben vielmehr in eigener Verantwortung zu prüfen, ob die Voraussetzungen für ein Übermittlungsverlangen vorliegen. In den Fällen des § 100g StPO ist zudem grundsätzlich eine entsprechende gerichtliche Anordnung erforderlich und einzuholen, 181

vgl. BT-Drs. 18/5088, S. 40 f.; BGH, Beschluss vom 23. September 2014 – 1 BGs 210/14 -, juris, Rn. 7. 182

Ein Abwehranspruch der Antragstellerin, der durch eine einstweilige Anordnung zu sichern wäre, folgt schließlich auch nicht aus dem Unionsrecht, soweit dieses die Berufsfreiheit (Art. 15 EuGRCh) oder die unternehmerischen Freiheit (Art. 16 EuGrCH) schützt. Ein Eingriff in diese Rechte wäre jedenfalls durch überragende Allgemeinwohlbelange gerechtfertigt. Insoweit gelten hier keine anderen Grundsätze als die, die für Art. 12 GG gelten. Die angegriffenen Regelungen zur Datenspeicherung sind im Sinne des Art. 52 Abs. 1 Satz 2 EuGRCh zur Erreichung des vorgesehenen legitimen Ziels geeignet, erforderlich und verhältnismäßig. 183

Schließlich steht der Antragstellerin auch kein Abwehranspruch aus Art. 56 AEUV zu. Selbst wenn man davon ausgeht, dass die Antragstellerin durch die Speicherverpflichtung in ihrer Dienstleistungsfreiheit aus Art. 56 AEUV beschränkt wird, wäre diese Beschränkung jedenfalls gerechtfertigt. Da die Speicherverpflichtung nicht diskriminierend wirkt, sondern unterschiedslos für in- und ausländische Diensteanbieter gilt, kann eine solche nichtdiskriminierende Allgemeinbeschränkung der Dienstleistungsfreiheit nach der Rechtsprechung des EuGH durch Gründe des Allgemeinwohls gerechtfertigt werden, 184

vgl. OVG Saarland, Beschluss vom 26. Mai 2010 – 3 B 122/10 -, juris, Rn. 54 mit zahlreichen Nachweisen aus der Rechtsprechung des EuGH. 185

Aus den obigen Ausführungen ergibt sich, dass eine solche Rechtfertigung vorliegt. 186

Zusammenfassend lässt sich damit feststellen, dass die gesetzlichen Regelungen über die Vorratsdatenspeicherung den verfassungsrechtlichen Vorgaben genügen, so dass aus einer Verletzung der der Antragstellerin in diesem Sinne zustehenden Rechte kein Abwehranspruch folgt, der durch eine einstweilige Anordnung zu sichern ist. Offen ist hingegen, ob ein entsprechender Abwehranspruch aus dem Verstoß der streitgegenständlichen gesetzlichen Regelungen gegen Art. 10 GG, Art. 7 und 8 EuGRCh folgen könnte, was allerdings voraussetzen würde, dass sich die Antragstellerin als 187

Telekommunikationsunternehmen überhaupt auf diese Rechtsverletzungen berufen kann. Dies bedarf wegen der Komplexität der sich stellenden Fragen vertiefter Überprüfung im Hauptsacheverfahren.

Ist damit offen, ob der Antragstellerin ein Anordnungsanspruch zusteht, hat der Antrag deshalb keinen Erfolg, weil die Antragstellerin keinen Anordnungsgrund glaubhaft gemacht hat. Die in diesem Falle vorzunehmende Folgenabwägung geht zu Lasten der Antragstellerin aus. 188

Wie bereits eingangs erwähnt, gebietet der Grundsatz effektiven Rechtsschutzes aus Art. 19 Abs. 4 GG, vorläufigen Rechtsschutz zu gewähren, wenn ohne ihn schwere und unzumutbare, anders nicht abwendbare Nachteile entstünden, zu deren nachträglicher Beseitigung die Entscheidung in der Hauptsache nicht mehr in der Lage wäre. Dies gilt vor allem dann, wenn eine erhebliche Grundrechtsverletzung droht, es sei denn, dass ausnahmsweise überwiegende, besonders gewichtige Gründe entgegenstehen, 189

vgl. BVerfG, Beschluss vom 25. Oktober 1988 – 2 BvR 745/88 -, BVerfGE 79, 69 ff., juris, Rn. 17. 190

Müssen die für eine vorläufige Regelung sprechenden Gründe schon im Regelfall so schwer wiegen, dass sie den Erlass einer einstweiligen Anordnung unabdingbar machen, so müssen sie im Fall der begehrten Außervollzugsetzung bzw. Nichtanwendung eines Gesetzes, wie vorliegend von der Antragstellerin begehrt, darüber hinaus besonders Gewicht haben, 191

vgl. BVerfG, Beschluss vom 28. Oktober 2008 – 1 BvR 256/08 -, BVerfGE 122. 120 ff., juris, Rn. 72 und Beschluss vom 11. März 2008 – 1 BvR 256/08 -, juris, Rn. 141-145. 192

Insoweit ist von entscheidender Bedeutung, ob die Nachteile irreversibel oder nur erschwert revidierbar sind, um das Aussetzungsinteresse durchschlagen zu lassen, 193

vgl. BVerfG, Beschluss vom 8. Juni 2016 – 1 BvQ 42/15 -, juris, Rn. 13 mit zahlreichen Nachweisen. 194

Solche irreversiblen Nachteile hat die Antragstellerin nicht glaubhaft gemacht. 195

Soweit die Antragstellerin darauf verweist, ohne die beantragte einstweilige Anordnung würde die Verwirklichung ihres Abwehranspruches, den sie aus Grundrechtsverletzungen und Verletzungen des Unionsrechts ableitet, vereitelt werden, steht dem zum jetzigen Zeitpunkt entgegen, dass die gesetzliche Verpflichtung zur Vorratsdatenspeicherung erst zum 1. Juli 2017 in Kraft treten wird. Soweit die Kammer bis zu diesem Zeitpunkt des Inkrafttretens eine Entscheidung in der Hauptsache herbeiführen kann, ist die Gefahr der Beeinträchtigung des von der Antragstellerin geltend gemachten grundrechtlichen Abwehranspruchs durch (rechtswidrige) Verpflichtung zur Vorratsdatenspeicherung nur gering. Selbst wenn eine in diesem Sinne rechtzeitige Entscheidung nicht möglich sein würde, wäre die von der Antragstellerin geltend gemachte Grundrechtsverletzung nur vorübergehend, da sie nach einem Obsiegen in der Hauptsache die Datenspeicherung beenden könnte. Dieser potentiellen, vorübergehenden Grundrechtsverletzung stehen aber gewichtige, und in der Sache überwiegende Gemeinwohlinteressen in Form einer Gefahr für eine effektive Strafverfolgung gegenüber. Denn erwiesen sich die zur rechtlichen Überprüfung gestellten gesetzlichen Regelungen zur Vorratsdatenspeicherung im Hauptsacheverfahren als rechtmäßig, so könnten die Strafverfolgungsbehörden für den Zeitraum der Nichtanwendung der Verpflichtung zur Datenspeicherung im Falle der Antragstellerin aufgrund des Ergehens 196

einer einstweiligen Anordnung im Falle eines berechtigten Auskunftsersuchens nicht auf Daten bei der Antragstellerin zurückgreifen. Damit wäre die gesetzlich bezweckte Gewährleistung effektiver Strafverfolgung und Gefahrenabwehr nicht zu erreichen. Dabei ist im Übrigen auch die Pflicht des Staates zum Schutz der Bürger vor Übergriffen zu berücksichtigen. Strafverfolgung und Gefahrenabwehr sind im Rahmen des Angemessenen und Zumutbaren geboten, um die Inanspruchnahme der Grundrechte abzusichern und Rechtsgüter im Einzelnen zu schützen,

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 315. 197

Somit verbleibt für die Antragstellerin als Anordnungsgrund der Umstand, dass sie bis zu einer Entscheidung in der Hauptsache und auch schon vor Inkrafttreten der gesetzlichen Regelung zum 1. Juli 2017, verpflichtet ist, sollte sie es nicht auf eine Anordnung der Antragsgegnerin auf der Grundlage des § 115 TKG ankommen lassen, die für die gesetzliche Datenspeicherung erforderliche Infrastruktur zu schaffen und vorzuhalten. Insofern fürchtet sie, für den Fall, dass sich ihre Datenspeicherungspflicht im Hauptsacheverfahren als rechtswidrig erweisen wird, die für die Einrichtung und das Vorhalten der Infrastruktur entstehenden Kosten nicht ersetzt zu bekommen, so dass ihr ein irreparabler Vermögensschaden entstünde. Dem steht allerdings vorliegend schon entgegen, dass die Antragstellerin die Unzumutbarkeit des Tragens des ihr (angeblich) entstehenden Vermögensschadens nicht hinreichend glaubhaft gemacht hat. Zwar beruft sich die Antragstellerin auf ein von ihr eingeholtes Gutachten von K. L. vom 17. Oktober 2016, nach dessen Ergebnis für die Einrichtung und Installation der für die geforderte Datenspeicherung erforderlichen Infrastruktur auf der Grundlage der Sicherheitsanforderungen für eine Datenspeicherung im Sinne der § 113d - § 113f TKG, insbesondere auch unter Berücksichtigung des Anforderungskatalogs im Sinne des § 113f TKG, für den Erwerb der notwendigen Hardware im Falle der Antragstellerin ein Betrag von 41.100 Euro anfallen wird. Hinzu kommen für den Einbau/Grundeinrichtung dieser Hardware 725 Euro. Für die (erstmalige) Programmierung/Konfiguration der notwendigen Software für die Verschlüsselung, das Schlüsselmanagement, Verwaltung und Löschung der Daten auf der gesetzlichen Grundlage werden zusätzlich 38.250,00 Euro veranschlagt, so dass für die erstmalige Einrichtung insgesamt ein Betrag von 80.075 Euro erforderlich wird. Hinzukommen werden nach dem vorgelegten Gutachten ab der gesetzlichen Speicherungspflicht zusätzliche Betriebs- und Personalkosten in Höhe von 9.778 Euro monatlich. Selbst wenn die Antragstellerin dieser Kostenlast ausgesetzt ist, vermag diese allein keine grundrechtsrelevante Unzumutbarkeit der Kostentragungspflicht zu begründen. Denn hierfür ist die Kostenhöhe in Relation zu den wirtschaftlichen Daten des Unternehmens, d.h. zu seiner Größe, den Umsatz und Gewinn zu stellen, 198

vgl. OVG Berlin-Brandenburg, Beschluss vom 2. Dezember 2009 – OVG 11 S 9.09 -, NVwZ 2010, 328 ff,.= juris, Rn. 75. 199

Die damit erforderlichen Unternehmensdaten sind vorliegend nicht ausreichend belegt und die durch die Vorlage des Gutachtens behauptete Kostenhöhe kann damit keine hinreichende Grundlage für eine den Erlass einer einstweiligen Anordnung rechtfertigende Geschäftsgefährdung bieten. Maßstab für eine unzumutbare Belastung kann zudem auch nicht allein die momentane wirtschaftliche und finanzielle Situation eines Unternehmens sein, da diese üblicherweise Veränderungen unterworfen ist, 200

vgl. OVG Berlin-Brandenburg, Beschluss vom 2. Dezember 2009, a.a.O., juris, Rn. 76. 201

202

Die Grenze einer zumutbaren Belastung würde zudem nach bundesverfassungsgerichtlicher Rechtsprechung in diesem Sinne nur dann überschritten, wenn der zu tragende Aufwand die Leistungsfähigkeit des Unternehmens übersteigen würde und sie deshalb zur Einstellung ihrer Dienstleistung gezwungen wäre,

vgl. BVerfG, Beschluss vom 28. Oktober 2008, a.a.O., juris, Rn. 80. 203

Die Antragstellerin trägt indessen nicht vor, dass bei dem geltend gemachten Kostenaufwand eine Fortsetzung ihrer wirtschaftlichen Betätigung ernstlich gefährdet wäre. Angesichts der Höhe der geltend gemachten Kosten ist dies auch nicht zu vermuten. 204

Zu berücksichtigen ist zudem, dass die Antragstellerin nicht dargelegt hat, dass die geltend gemachten zusätzlichen Kosten bei Installation und Vollzug der notwendigen Infrastruktur der Vorratsdatenspeicherung nicht ganz oder zum Teil auf ihre Endkunden abgewälzt werden könnten, um ihre wirtschaftliche Belastung zu minimieren, 205

vgl. zu diesem Aspekt: BVerfG, Beschluss vom 28. Oktober 2008, a.a.O., juris, Rn. 80. 206

Darüber hinaus ist, wie bereits oben dargelegt, zu beachten, dass das Bundesverfassungsgericht in seinem Urteil vom 2. März 2010 zur Vorgängerregelung vor dem Hintergrund, dass in der Vorgängerregelung keinerlei Entschädigungsregelung vorgesehen war, ausgeführt hat, dass die dort gesetzlich verankerte Speicherungspflicht nicht als unverhältnismäßig in Bezug auf die finanziellen Lasten, die den Unternehmen durch die (damalige) Speicherungspflicht auf der Grundlage des § 113a TKG a.F. und die hieran knüpfenden Folgeverpflichtungen wie die Gewährleistung von Datensicherheit erwachsen, anzusehen war, 207

vgl. BVerfG, Urteil vom 2. März 2010, a.a.O., juris, Rn. 301 ff. 208

Diesen Ausführungen ist im Rahmen des vorliegenden Verfahrens zu folgen. Die Einwendung der Antragstellerin, dass eine „hinreichende Sach- und Verantwortungsnähe“, welche die entschädigungslose Indienstnahme eines Unternehmens für einen hoheitlichen Zweck rechtfertigen könnte, fehle, führt genau so wenig zum Erfolg, wie ihre Rüge, die Entschädigungsregelung sei nicht hinreichend bestimmt, wie oben bereits ausgeführt wurde. 209

Selbst wenn die Antragstellerin aber bei einem Abwarten der Entscheidung der Hauptsache Schäden in Form überflüssiger Investitionen ausgesetzt wäre, stünden diesen Nachteilen gewichtige öffentliche Interessen an der Sicherstellung der mit der Einführung der Speicherpflicht bezweckten effektiven Strafverfolgung und Gefahrenabwehr gegenüber. 210

Darüber hinaus würde eine einstweilige Anordnung zu einer Benachteiligung derjenigen Dienstanbieter führen, denen gegenüber sie keine Wirkung entfalten würde und die daher nach Veröffentlichung des Anforderungskatalogs gemäß § 113f Abs. 1 Satz 2 TKG mit der Einrichtung der erforderlichen technischen Vorkehrungen beginnen. Dies könnte letztlich Wettbewerbsverzerrungen zur Folge haben, 211

vgl. BVerfG, Beschluss vom 28. Oktober 2008, a.a.O., juris, Rn. 82. 212

Zu Gunsten der Antragstellerin streitet auch nicht der von ihr geltend gemachte Umstand, dass ihren nicht unerheblichen Aufwendungen nur ein sehr begrenzter Ertrag gegenüber stünde. Denn aufgrund ihres Kundenstammes sei es in den vergangenen Jahren nur sehr vereinzelt zu Ermittlungsanfragen gekommen. Ob dies auch in Zukunft der Fall ist, lässt sich zum einen derzeit nicht absehen. Zum anderen bestünde aber auch die Gefahr, dass im Falle 213

der alleinigen (vorläufigen) Freistellung der Antragstellerin von Datenspeicherungspflichten gerade Personen, denen nicht an einer Speicherung ihrer Daten gelegen ist, sich um vertragliche Beziehungen zur Antragstellerin bemühen würden.

Die Kostenentscheidung beruht auf § 154 Abs. 1 VwGO. 214

Die Streitwertfestsetzung beruht auf §§ 53 Abs. 2 Nr. 1, 52 Abs. 1, GKG und entspricht der Hälfte des geltend gemachten Kostenaufwandes der Antragstellerin für die Einrichtung und Sicherung der ihr gesetzlich auferlegten Speicherverpflichtung. 215
