Hauke Gärtner, Dennis-Kenji Kipker

Die Neuauflage der Vorratsdatenspeicherung

Lösungsansätze für zentrale Kritikpunkte am aktuellen Gesetzentwurf

Seit der „Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten" des BMJV im Mai dieses Jahres öffentlich wurde, ist die seit Jahren schwelende Debatte um Sinn und Nutzen der Vorratsdatenspeicherung wieder voll entbrannt. Ob diese überhaupt einen den Grundrechtseingriff rechtfertigenden, maßgeblichen Vorteil für die Strafverfolgung mit sich bringt, ist höchst streitig und bereits Gegenstand einer Vielzahl von Publikationen gewesen. In diesem Beitrag hingegen soll es, ausgehend von der Annahme, dass die Regierungskoalition dieses Gesetzgebungsverfahren trotz aller Bedenken weiter vorantreiben wird, um einige ausgewählte, besonders kritische Punkte des Gesetzentwurfs gehen und es werden konkrete Vorschläge für die hier gebotenen Nachbesserungen skizziert.

1 Einleitung

Mittlerweile haben Politiker, Verbände und Publizisten eine Fülle von Beiträgen veröffentlicht, die in ganz überwiegender Zahl den neuerlichen Gesetzentwurf zur Wiedereinführung der Vorratsdatenspeicherung[1] scharf kritisieren.[2] Auch stellen sich wie schon bei der erstmaligen Einführung dieses Ermittlungsinstruments 2008 wieder grundsätzliche Fragen wie diejenige, ob auf diesem Wege eine Bekämpfung schwerer Kriminalität angesichts einfach zu bedienender und frei verfügbarer Anonymisierungsprogramme wie z.B. dem Tor-Netzwerk, bei dem der Datenverkehr verschlüsselt über wechselnde internationale Knotenpunkte gelenkt wird, überhaupt erreicht werden kann.

Sowohl das Bundesverfassungsgericht als auch der Europäische Gerichtshof haben in ihren einschlägigen Urteilen die Vorratsdatenspeicherung zwar nicht per se für unzulässig erklärt, für eine grundrechtskonforme Ausgestaltung aber recht hohe Hürden aufgestellt.[3] Wenngleich der Gesetzentwurf an vielen Stellen diese Maßgaben aufzugreifen versucht, so besteht an anderen Punkten noch erheblicher Nachbesserungsbedarf: Die Anforderungen an die Erhebung von Verkehrsdaten gem. § 96 TKG müs-

Hauke Gärtner

Studium der Rechtswissenschaft in Münster und Saragossa, derzeit Rechtsreferendar im OLG-Bezirk Düsseldorf

E-Mail: hauke.gaertner@gmx.de

Dr. Dennis-Kenji Kipker

Wissenschaftlicher Mitarbeiter am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) der Universität Bremen, Projektleitung und -durchführung des BMBF-geförderten Projekts VeSiKi – Vernetzte IT-Sicherheit für Kritische Infrastrukturen und Berater für das Human Brain Project der Europäischen Kommission
E-Mail: kipker@uni-bremen.de

1 BR-Drs. 249/15.

2 Vgl. Dix/Kipker/Schaar, ZD 2015, 300; Voßhoff, „Zweifel an einer verfassungsgemäßen Umsetzung der Vorratsdatenspeicherung mit dem heute vorgelegten Gesetzentwurf nicht ausgeräumt!", abrufbar unter: http://www.bfdi.bund.de/DE/Infothek/

Pressemitteilungen/2015/15_VDS.html?nn=5217040 (Stand: 10.07.2015). BITKOM, „BITKOM warnt vor Schnellschuss bei der Vorratsdatenspeicherung", abrufbar unter: http://www.bitkom.org/de/presse/8477_82314.aspx (Stand: 10.07.2015). Siehe für weitere Stellungnahmen zur Vorratsdatenspeicherung auch die Linkliste der EAID unter http://www.eaid-berlin.de/?page_id=684 (Stand: 10.07.2015).

3 BVerfG DuD 2010, 409 und EuGH, Rs. C-293/12 und C-594/12 (siehe auch DuD 2014, 488 ff.).

sen in restriktiver Weise konkretisiert werden, den Vorschriften zur Datensicherheit sind u.a. Regelungen zu effektiven Kontrollmechanismen an die Seite zu stellen und die statistische Erfassung der Erhebung von Vorratsdaten muss so ausgestaltet werden, dass sie tatsächlich eine Aussage über den Nutzen dieses Ermittlungsinstruments ermöglicht und damit eine fundierte Grundlage für die Entscheidung über dessen Zukunft sein kann. Zentrales Problem ist darüber hinaus, dass dem Gesetzentwurf eine befriedigende Antwort auf den insbesondere vom Europäischen Gerichtshof angemahnten besonderen Schutz der Daten von Berufsgeheimnisträgern vor der Vorratsspeicherung und deren Verwertung fehlt. Hierzu wird ein verfahrenstechnischer Lösungsansatz vorgestellt, der auch die Interessen dieser besonderen Personengruppen berücksichtigt.

2 Konkretere Anforderungen an die Erhebung von Daten gem. § 96 Abs. 1 TKG

Um den Anforderungen des rechtsstaatlichen Bestimmtheitsgrundsatzes gerecht zu werden, sind die in § 100g Abs. 1 StPO-E formulierten Voraussetzungen für die Erhebung von Verkehrsdaten nach § 96 Abs. 1 TKG deutlich zu konkretisieren, indem der Katalog von Anlassdelikten des § 100g Abs. 2 StPO-E auch für die Fälle des Abs. 1 übernommen wird.

Nach § 100g Abs. 1 S. 1 Nr. 1 StPO-E soll die Erhebung von Daten gem. § 96 Abs. 1 TKG schon zulässig sein, sofern der Verdacht einer Straftat von auch im Einzelfall erheblicher Bedeutung besteht, wobei „insbesondere" auf den in § 100a Abs. 2 StPO-E aufgeführten Katalog verwiesen wird. Die einschlägigen Delikte sind also nicht abschließend definiert. Ähnlich problematisch ist die Formulierung in § 100g Abs. 1 S. 1 Nr. 2 StPO-E, der zufolge schon der begründete Verdacht irgendeiner Straftat mittels Telekommunikation für die Datenerhebung ausreichen soll. Auch die vorgesehene Erforderlichkeits- und Angemessenheitsklausel trägt hier wenig zur Präzision bei.

Angesichts des Umstands, dass die Verkehrsdaten die Identität des Endgerätnutzers wie auch die hergestellten Verbindungen und damit Teile seines Soziallebens offenbaren, wiegt der Eingriff in das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung so schwer, dass der rechtsstaatliche Bestimmtheitsgrundsatz eine Konkretisierung des Normwortlautes erfordert. Zwar genießen die gem. § 96 Abs. 1 TKG ohnehin aus geschäftlichen Gründen bei den Telekommunikationsunternehmen gespeicherten Verkehrsdaten einen geringeren Grundrechtsschutz als solche nach § 113b TKG-E, die anlasslos systematisch gesammelt werden[4] und auf die der Zugriff gem. § 100g Abs. 2 StPO-E nur zur Verfolgung im Einzelnen benannter besonders schwerer Straftaten gestattet ist. Das bedeutet indes nicht, dass der Gesetzgeber die Anforderungen an eine Erhebung von Daten gem. § 96 Abs. 1 TKG beliebig herabsetzen kann; auch hier muss dem Bestimmtheitsgebot in ausreichender Weise Rechnung getragen werden.

Eine solche Konkretisierung ist auch ohne Weiteres möglich, enthält doch § 100g Abs. 2 StPO-E bereits einen ausführlichen Katalog besonders schwerer Straftatbestände, der als Voraussetzung für die Verkehrsdatenerhebung nach Abs. 1 übernommen werden könnte. So geht zwar die im Entwurf angestrebte Differenzierung zwischen der Erhebung von Daten nach § 96 TKG und nach § 113b TKG-E teilweise verloren, allerdings wird dies im Interesse einer verfassungskonform bestimmten und ausreichend restriktiven Zugriffsregelung auf Verkehrsdaten i.S.v. § 96 TKG kaum vermeidbar sein. Befürchtungen, dass durch die höheren Hürden für eine Erhebung dieser Daten eine effektive Strafverfolgung in Fällen schwerer Kriminalität behindert würde, müssen dabei angesichts der Länge des Straftatenkatalogs nicht aufkommen. Vielmehr würde die Verkehrsdatenerhebung insgesamt auf Fälle besonders schwerer Kriminalität beschränkt und wäre damit aus verfassungsrechtlicher Sicht eher zu rechtfertigen.

3 Umsetzung der Datensicherheitsbestimmungen

Schon das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung 2010 hervorgehoben, dass es bezüglich der Datensicherheit klarer Regelungen bedarf, die einen besonders hohen Sicherheitsstandard unmissverständlich und verbindlich festlegen.[5] Ebenso wies der Europäische Gerichtshof in seinem Urteil von 2014 auf die Erforderlichkeit von Regelungen zum effektiven Schutz der auf Vorrat gespeicherten Daten vor Missbrauchsrisiken, unberechtigtem Zugang und unberechtigter Nutzung hin.[6] Die Gewährleistung wirksamer Datensicherheit stellt also eine der zentralen Maßgaben der Rechtsprechung an den Gesetzgeber dar.

Verkehrs- und Standortdaten erlauben laut Europäischem Gerichtshof „sehr genaue Schlüsse auf das Privatleben der Personen […], etwa auf Gewohnheiten des täglichen Lebens […] und das soziale Umfeld, in dem sie verkehren."[7] Dem Risiko des Missbrauchs dieser bei den TK-Unternehmen gespeicherten Daten versucht die Bundesregierung in den §§ 113d und 113f TKG-E mit einer Reihe von – für sich genommen durchaus sinnvollen – Vorgaben zur Datensicherheit zu begegnen.

3.1 Regelmäßige und unabhängige Kontrollen

Die Wirksamkeit der gesetzlichen Anforderungen an die Datensicherheit wird jedoch dadurch erheblich geschmälert, dass keine ausreichend effektive Überprüfung des normativ bestimmten Datensicherheitsstandards durch externe fachkundige Stellen vorgeschrieben wird. Einer fortlaufenden Überprüfung durch die Bundesnetzagentur in Zusammenarbeit mit dem BSI und dem Bundesdatenschutzbeauftragten unterliegt gem. § 113f TKG-E nur der Katalog der technischen Anforderungen, nicht aber dessen tatsächliche Einhaltung durch die Telekommunikationsanbieter. Hierfür sind nur gem. § 113f Abs. 3 S. 2 TKG-E i.V.m. § 109 Abs. 7 TKG in das Ermessen der Bundesnetzagentur gestellte Einzelfallprüfungen vorgesehen. Angesichts der Vielzahl von Unternehmen, die gesetzlich zur Vorratsdatenspeicherung verpflichtet werden sollen,[8] sowie der bei ihnen jeweils anfallenden enormen Datenmengen kann durch solche punktuellen Stichproben kein ausreichend wirksamer Schutz durch staatliche Kontrollmechanismen garantiert werden. Sofern der Staat eine derartige Akkumulation personenbezogener Daten in den Händen

4 Vgl. BVerfG DuD 2010, 409, 413.

5 BVerfG DuD 2010, 409, 412.

6 EuGH, Rs. C-293/12 und C-594/12, Rz. 66 f.

7 EuGH, Rs. C-293/12 und C-594/12, Rz. 27.

8 Vgl. BR-Drs. 249/15, S. 4.

Privater vorschreibt, steht er auch in der Pflicht, effektive Sicherheitsvorkehrungen zum Schutz vor missbräuchlichen Handlungen innerhalb des Unternehmens oder gegen Hacker-Angriffe von außen zu treffen. Nötig wären hier flächendeckende Überprüfungen, die ohne spezifischen Anlass regelmäßig von einer fachkundigen Stelle durchgeführt werden müssen, sodass Lücken in der Datensicherheit zeitnah entdeckt und Gegenmaßnahmen ergriffen werden können.

3.2 Angemessene Kostenverteilung für Datensicherheitsmaßnahmen

Zwar dürfte es bei den TK-Unternehmen angesichts der verheerenden Image-Wirkung von Datenskandalen grundsätzlich kaum an der nötigen Motivation zur Einrichtung der erforderlichen technischen und organisatorischen Sicherheitsvorkehrungen fehlen,[9] jedoch scheint es fragwürdig, allein der Telekommunikationswirtschaft die insgesamt wohl im Bereich dreistelliger Millionenbeträge liegenden Lasten[10] der Einführung und Unterhaltung der Vorratsdatenspeicherung zu überantworten. Dies gilt umso mehr angesichts des Risikos verfehlter Investitionen, sofern ein Urteil des Bundesverfassungsgerichts oder des Europäischen Gerichtshofes die neuen gesetzlichen Regelungen im Nachhinein wieder hinfällig werden lässt. Eine Entschädigungsregelung sieht § 113a Abs. 2 TKG-E bisher nur für den Fall vor, dass wegen erdrosselnder Wirkung der mit der Speicherung einhergehenden Pflichten eine unbillige Härte anzunehmen ist. Das Bundesverfassungsgericht hatte 2010 zwar festgestellt, dass schon die „Sach- und Verantwortungsnähe" der TK-Betreiber grundsätzlich ausreichen würde, um ihnen die Kosten der Vorratsdatenspeicherung einschließlich der Datensicherheitsmaßnahmen aufzubürden.[11]

Diese Argumentation ist auf das vorliegende Gesetzeskonzept indes nicht übertragbar, stellt der Gesetzentwurf der Bundesregierung doch deutlich höhere und damit kostenintensivere Anforderungen an die Datensicherheit als es noch der 2010 für nichtig erklärte § 113a Abs. 10 TKG tat. Wenn der Gesetzgeber trotz des hohen Aufwands für die Privatwirtschaft und der zweifelhaften Nützlichkeit des Instruments die Vorratsdatenspeicherung wiedereinführen will, so kann sich die staatliche Kostentragung nicht nur, wie zurzeit im Gesetzentwurf vorgesehen,[12] auf die durch Behörden angeforderten Auskünfte erstrecken, sondern muss auch die in den TK-Unternehmen zu schaffende Sicherheitsinfrastruktur abdecken.

9 Insoweit noch skeptisch: BVerfG DuD 2010, 409, 413.

10 Vgl. die Kostenschätzungen der Branchenverbände BITKOM und eco in BR-Drs. 249/15, Anlage mit Stellungnahme des Nationalen Normenkontrollrates, S. 4. Laut eco drohen insb. dem Mittelstand erhebliche Kosten, vgl. Greis, „Kritik an Gesetzentwurf – Eco hält Vorratsdatenspeicherung für nicht umsetzbar", abrufbar unter: http://www.golem.de/news/eco-kritik-an-gesetzentwurf-vorratsdatenspeicherung-ist-technisch-nicht-umsetzbar-1505-114166.html (Stand 10.07.2015).

11 BVerfG, U. v. 2.3.2010 – 1 BvR 256/08, 1 BvR 263/08 u. 1 BvR 586/08, Rz. 301, Volltext abrufbar unter http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html (Stand 10.07.2015).

12 Siehe die in Art. 4 des Gesetzentwurfs (BR-Drs. 249/15) vorgesehenen Änderungen des Justizvergütungs- und -entschädigungsgesetzes (JVEG), v.a. der Anlage 3.

3.3 Längere Speicherung der Zugriffsprotokolle

Grundsätzlich begrüßenswert ist die in § 113e TKG-E vorgeschriebene Protokollierungspflicht für Zugriffe auf die gespeicherten Daten. Als möglicher Beleg für Datenmanipulationen durch unbefugte Dritte und andere Verletzungen der Datenintegrität ist eine solche Dokumentation von hoher Relevanz. Vor diesem Hintergrund allerdings ist die vorgesehene Speicherfrist für die Protokolle von nur einem Jahr zu kurz angesetzt. Missbräuchlicher Umgang mit Datensätzen wird oft erst geraume Zeit später publik,[13] so dass – um die betreffenden Vorgänge im Nachhinein besser nachvollziehen und auch im Rahmen gerichtlicher Auseinandersetzungen belegen zu können – der Zeitraum auf drei Jahre auszudehnen ist. Dies gilt umso mehr angesichts der immensen Menge der bei den großen Diensteanbietern gespeicherten Datensätze, bei der einzelne Verletzungen der Datenintegrität oft nicht sofort auffallen dürften. Der effektive Rechtsschutz für Betroffene kann hier durch längere Protokollspeicherfristen deutlich erleichtert werden.

Das Erfordernis einer längeren Speicherung der Protokolle besteht umso mehr, solange im Gesetzentwurf keine regelmäßigen externen Datenschutzkontrollen vorgeschrieben sind und damit nicht gesichert ist, dass Protokolle auch tatsächlich vor ihrer Löschung zumindest einmal von einer außerhalb des TK-Betreibers stehenden Überprüfungsstelle eingesehen werden.

3.4 Datensicherheit innerhalb der Behörden

Im Übrigen stellen sich nicht nur bei den TK-Anbietern erhöhte Anforderungen an die Datensicherheit, auch für die Behörden müssen spezifisch auf den Umgang mit den durch die Vorratsdatenspeicherung erlangten Verkehrsdaten zugeschnittene Vorgaben getroffen werden. Solche sind im Gesetzentwurf bisher nur unzureichend vorhanden. So trifft § 101a StPO-E zwar Regelungen zu Kennzeichnung, Auswertung, Löschung und Weitergabe der erhobenen Verkehrsdaten, nicht aber beispielsweise zur sicheren Aufbewahrung und Abwehr von Zugriffen Unberechtigter. Dabei zeigten sich bereits etwa im Staatstrojaner-Skandal von 2011 eklatante Mängel u.a. bei der Dokumentation und den Zugriffsmöglichkeiten Dritter.[14] Mit anderen Worten: Der Umgang staatlicher Behörden mit den technischen Herausforderungen neuartiger Ermittlungsinstrumente weist teilweise noch erhebliche Schwächen auf. Klarere Maßgaben würden hier auf beiden Seiten – bei Behörde und Betroffenem – für größere Rechtssicherheit sorgen und sollten deshalb in den Gesetzentwurf aufgenommen werden.

4 Weitreichendere statistische Erfassung des Nutzens der Vorratsdatenspeicherung

Ob die Vorratsdatenspeicherung ein geeignetes und erforderliches Mittel darstellt, um sicherheitsbehördliche Ermittlungen zum Erfolg zu führen, ist seit Jahren Gegenstand einer hoch emotional geführten Debatte, die durch die Ergebnisse verschiedener, sich teils widersprechender Gutachten mehr angeheizt als versachlicht wurde.[15] Um diese Diskussion in Zukunft auf einer objektiveren Grundlage führen zu können, sollte die Wiedereinführung der Vorratsdatenspeicherung dazu genutzt werden, deren tatsächlichen Wert für Ermittlungsarbeiten gründlich zu evaluieren. Regelungen zur aussagekräftigen statistischen Erfassung der Vorratsdatenspeicherung müssen daher Bestandteil des neuen Gesetzes werden.

Nach dem jetzigen § 101b StPO-E soll lediglich eine jährliche Übersicht über die Anzahl der Verfahren, in denen auf Vorrat gespeicherte Verkehrsdaten von Behörden erhoben wurden, sowie die Anzahl und Art der Anordnungen erstellt werden. Die Häufigkeit solcher Maßnahmen besagt aber inhaltlich wenig über deren tatsächlichen Nutzen für die Ermittlung. Vielmehr bedarf es einer Verpflichtung der Ermittlungsbehörden zur Dokumentation darüber, welchen konkreten Vorteil die Datenerhebung für das Verfahren gebracht hat und ob dieser Nutzen nicht auf anderem Wege auch erzielbar gewesen wäre. Es muss folglich ein Kausalitätsnachweis erbracht werden, welcher objektiv einen Bedarf für die Vorratsdatenspeicherung belegt.

Hieran anknüpfend sollte zudem festgehalten werden, wie lange die erhobenen Daten bereits gespeichert waren. So könnte geklärt werden, ob es für Ermittlungserfolge tatsächlich notwendig ist, die allgemeinen Verkehrsdaten für zehn Wochen und Standortdaten für vier Wochen zu speichern. Diese in § 113b TKG-E vorgesehenen Speicherfristen werden in der Begründung des Gesetzentwurfs als „ausreichend, um in der weitaus überwiegenden Anzahl von Ersuchen eine Verfügbarkeit der maßgeblichen Daten sicherzustellen", bezeichnet. Warum nicht auch eine kürzere Speicherdauer denselben Erfolg haben könnte, bleibt unbeantwortet. Am Beispiel dieser letztlich willkürlich gewählten Zeiträume wird erneut deutlich, dass es dem Gesetzgeber an aussagekräftigen Daten fehlt, die Erkenntnisse über den tatsächlich nötigen Umfang einer Vorratsdatenspeicherung zulassen.

Wenn der Gesetzgeber trotz unsicherer Faktenlage dieses Instrument wiedereinführt, so ist er zumindest in der Pflicht, die sich nunmehr bietende Gelegenheit zur Effektivitätsüberprüfung mittels der dargelegten Dokumentation durch die Ermittlungsbehörden zu ergreifen. Der in ein elementares Grundrecht seiner Bürger eingreifende Staat steht hier unter Rechtfertigungszwang. Die Evaluierung der gesammelten statistischen Daten sollte dabei nicht von den Ermittlungsbehörden selbst, sondern einer unabhängigen fachkundigen Stelle vorgenommen werden, um so dem Vorwurf der Parteilichkeit von Anfang an vorzubeugen.

Da erst auf Basis der so gewonnenen Erkenntnisse eine endgültige Entscheidung darüber getroffen werden kann, ob der Nutzen der Vorratsdatenspeicherung den Eingriff in das Fernmelde-

13 Beispielhaft sei hier an die diversen Datenskandale der Deutschen Telekom erinnert, vgl. etwa Spiegel-Online, „Mangelnder Datenschutz: Telekom schludert mit Daten von 120.000 Beschäftigten", abrufbar unter: http://www.spiegel.de/wirtschaft/unternehmen/datenpanne-telekom-schludert-mit-daten-von-120-000-beschaeftigten-a-919143.html (Stand 10.07.2015).

14 BfDI, Bericht gemäß § 26 Abs. 2 Bundesdatenschutzgesetz über Maßnahmen der Quellen-Telekommunikationsüberwachung bei den Sicherheitsbehörden des Bundes, Bonn 2012, S. 47 f.

15 Vgl. einerseits Abschlussbericht des BKA von 2011, abrufbar unter: https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/Mindestspeicherfrist/studie.pdf?__blob=publicationFile (Stand 10.07.2015), und andererseits Gutachten des Max-Planck-Institutes „Schutzlücken durch Wegfall der Vorratsdatenspeicherung?", insbes. S. 218 ff., Freiburg 2011, abrufbar unter: http://vds.brauchts.net/MPI_VDS_Studie.pdf (Stand 10.07.2015).

geheimnis und das Recht auf informationelle Selbstbestimmung überwiegt, müsste das vorliegende Gesetz konsequenterweise von vorneherein auf einen Zeitraum befristet sein, bei dessen Ablauf ausreichend Daten für eine aussagekräftige Analyse vorliegen. Einem solchen Vorgehen dürften sich bei nüchterner Herangehensweise selbst die Befürworter der Vorratsdatenspeicherung nicht verschließen, denn sofern ihre Behauptung des erheblichen sicherheitspolitischen Mehrwerts dieser Maßnahmen zutreffen sollte, würde dieser durch die Effektivitätsanalyse belegt werden und eines der zentralen Argumente ihrer Gegner wäre hinfällig. Sollte hingegen kein wesentlicher Nutzen der Vorratsdatenspeicherung erkennbar sein, dürfte angesichts dieser fehlenden empirischen Belege eine Nichtverlängerung der Regelungen weitgehend akzeptiert werden.

5 Aufrechterhaltung des Schutzes der Berufsgeheimnisträger

5.1 Auffassungen von EuGH und BVerfG

Ein besonders umstrittener Aspekt bei der Wiedereinführung der Vorratsdatenspeicherung ist die Frage, wie mit den Verkehrsdaten von Berufsgeheimnisträgern umgegangen werden soll. Bereits der Europäische Gerichtshof kritisierte an der bisherigen Richtlinie zur Vorratsdatenspeicherung 2006/24/EG die fehlenden Ausnahmen für die Speicherung der Daten, die dem Berufsgeheimnis unterliegen.[16] Eng damit verknüpft ist die Problematik, dass die EU-Richtlinie keine verfahrensrechtlichen Voraussetzungen enthielt, um den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung zu begrenzen.[17] So war folglich nicht nur die Speicherung der Daten in einem nahezu unbegrenzten Ausmaß möglich, sondern auch der Zugang zu den einmal gespeicherten Daten unterlag keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, die Anträge auf den Zugang zu den gespeicherten Daten überprüft und das Maß von deren Nutzung auf das absolut Notwendige beschränkt.[18] Fraglich dürfte in Bezug auf die Berufsgeheimnisträger aber sein, ob bloße Zugangsbeschränkungen für schon gespeicherte Daten ausreichend sind, um der besonderen Gefährdungslage für diese Personengruppen gerecht zu werden. Die Begrenzung der Datennutzung auf das „absolut Notwendige" könnte vielmehr nur darin zu sehen sein, von Beginn an sicherzustellen, dass die Speicherung der Verkehrsdaten von Berufsgeheimnisträgern so weit wie möglich technisch ausgeschlossen ist.

Das Bundesverfassungsgericht hat in seinem damaligen Urteil zur Nichtigkeitserklärung der Vorratsdatenspeicherung in Deutschland zwar keine ausdrücklichen Ausführungen zum Schutz der Berufsgeheimnisträger vorgenommen. Es hat aber schon in seinen Leitsätzen festgestellt, dass es einer Ausgestaltung der Vorratsdatenspeicherung bedarf, die dem besonderen Gewicht des hierin liegenden Eingriffs hinreichend Rechnung trägt und deshalb besonders strengen Anforderungen genügen muss.[19] Die Schwere des Eingriffs hat das Bundesverfassungsgericht vor allem auch damit begründet, dass die Verarbeitung der Verkehrsdaten einerseits von den Betroffenen nicht bemerkt wird, zugleich aber auch Verbindungen umfassen kann, die unter „Vertraulichkeitserwartungen" aufgenommen wurden.[20] Beispielhaft wird dabei die in § 99 Abs. 2 S. 1 TKG genannte Notlagen-Beratung von anonymen Anrufern bei Mitarbeitern genannt, die einer besonderen Verschwiegenheitsverpflichtung im sozialen und kirchlichen Bereich unterliegen.[21]

Speziell für solche Vertraulichkeitsverbindungen macht das Bundesverfassungsgericht den Vorschlag, das Eingriffsgewicht zu reduzieren, indem bei der Datenübermittlung zwischen TK-Unternehmen und Ermittlungsbehörde technische Filter zwischengeschaltet werden, um besonders schützenswerte TK-Verbindungen vor einem Zugriff durch den Staat auszublenden.[22] Nicht zuletzt wurde die Regelung des § 113a TKG durch das Bundesverfassungsgericht auch deshalb für nichtig erklärt, weil sie keine Vorkehrungen zum Schutz von solchen Vertrauensbeziehungen vorsah.[23]

5.2 Erweiterung der Vorgaben des BVerfG

Fraglich ist indes, warum das Bundesverfassungsgericht seine Argumentation zum Schutze der besonderen Vertrauensbeziehungen im Bereich der TK-Dienste ausschließlich auf die Definition des § 99 Abs. 2 S. 1 TKG stützte. Nicht nur für Personen und Organisationen in sozialen oder kirchlichen Bereichen, sondern für sämtliche in § 53 Abs. 1 StPO genannten Personengruppen gilt, dass ihre vertrauliche Kommunikation besonders schutzbedürftig ist, was im Gesetzgebungsverfahren explizit und umfassend berücksichtigt werden muss. Doch selbst wenn man die Anforderungen, die das Gericht in seinem Urteil aufstellt, über den in § 99 Abs. 2 S. 1 TKG genannten Personenkreis hinaus auf sämtliche Berufsgeheimnisträger ausdehnt, sind die Vorgaben noch unzureichend: So wird für den Schutz der Vertrauensverhältnisse lediglich ein Übermittlungsverbot angeordnet, nicht aber die Speicherung der Verkehrsdaten von Berufsgeheimnisträgern von vornherein untersagt.[24] Eine solche Regelung verkennt, dass bereits mit der Speicherung der Vorratsdaten das Risiko einer Ausspähung der Berufsgeheimnisträger geschaffen wird.

Wenig überzeugend ist es auch, wenn das Bundverfassungsgericht für die Verhältnismäßigkeit der Vorratsdatenspeicherung darauf abstellt, dass die Speicherung der TK-Verkehrsdaten nicht durch den Staat, sondern vorgelagert durch die privaten Diensteanbieter erfolgt. Das Gericht sieht in einem derartigen Verfahren vor allem deshalb einen Vorteil, weil die Daten im Zuge der Speicherung noch nicht zusammengeführt werden, sondern auf viele Einzelunternehmen verteilt sind, wodurch sie dem Staat in unmittelbarer Gesamtheit nicht zur Verfügung stehen, sondern anlassbezogen erst in einem zweiten Schritt der Abruf stattfindet.[25] Zunächst einmal mag dieser Ansatz angesichts von bundesweit fast 3.600 gewerblichen Betreibern öffentlicher Telekommunikationsnetze und Erbringern öffentlich zugänglicher Telekommunikationsdienste[26] zwar schlüssig klingen, der Großteil der anfal-

16 Siehe EuGH, Rs. C-293/12 und C-594/12, Rz. 58.
17 EuGH, Rs. C-293/12 und C-594/12, Rz. 61.
18 EuGH, Rs. C-293/12 und C-594/12, Rz. 62.
19 BVerfG DuD 2010, 409, 409.
20 BVerfG DuD 2010, 409, 411.
21 BVerfG DuD 2010, 409, 415.
22 BVerfG DuD 2010, 409, 415.
23 Vgl. BVerfG DuD 2010, 409, 421.
24 Vgl. BVerfG DuD 2010, 409, 415.
25 BVerfG DuD 2010, 409, 411.
26 Siehe die entsprechende Aufstellung der BNetzA, abrufbar unter: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Tele-

lenden TK-Daten wird jedoch von nur zwanzig Großunternehmen erhoben, die 98% des Marktes abdecken.[27] Allein aufgrund dieser wirtschaftlichen Konstellation ergibt sich eine Datenakkumulation, die von der Argumentation des Bundesverfassungsgerichts nicht berücksichtigt wird.

5.3 Keine technische Unmöglichkeit des Berufsgeheimnisträgerschutzes

Alles in allem sind somit die Vorgaben, die der Europäische Gerichtshof sowie das Bundesverfassungsgericht an den Schutz für die Berufsgeheimnisträger stellen, schon deshalb unzureichend, weil sie zu unbestimmt sind. Vor diesem Hintergrund wundert es nicht, dass der Gesetzentwurf der Bundesregierung zur Wiedereinführung der Vorratsdatenspeicherung nur einen einzelnen Absatz vorsieht, um besondere Vertrauensverhältnisse auch im TK-Bereich zu schützen: § 100g Abs. 4 StPO-E. Hierin wird lediglich bestimmt, dass die Erhebung von Verkehrsdaten, die sich gegen einen Berufsgeheimnisträger richtet und die voraussichtlich Erkenntnisse erbringen würde, über die dieser das Zeugnis verweigern dürfte, unzulässig ist. Dennoch erlangte Erkenntnisse dürfen nicht verwendet werden. Diese Vorgaben entsprechen inhaltlich im Wesentlichen dem § 160a Abs. 1 StPO.

Warum sich die Bundesregierung in ihrer Neuregelung ausschließlich auf ein solches Verwendungs- und Verwertungsverbot beschränkt, ergibt sich bereits aus der Gesetzesbegründung: Die vorgeschlagene Regelungsalternative, die Berufsgeheimnisträger in ihrer Gesamtheit von der Speicherung der TK-Verkehrsdaten auszunehmen, sei unmöglich, denn hierzu müsse eine Liste aller Berufsgeheimnisträger in Deutschland geführt werden, die regelmäßig aktualisiert wird. Die Erstellung, Übermittlung und Aktualisierung dieser Liste berge nicht nur ein erhebliches Missbrauchsrisiko, sondern sei auch technisch bereits nicht realisierbar, weil in den meisten Fällen dynamische IP-Adressen genutzt würden.[28] Obgleich die Bundesregierung diesen Lösungsansatz zum Schutz der Berufsgeheimnisträger als die bessere Alternative anpreist,[29] ist die Kritik an diesem Konzept schon jetzt erheblich. Von verschiedenen Stellen wird gefordert, dass der Schutz des Berufsgeheimnisses nicht erst im Anschluss an die Speicherung, sondern bereits bei der Erhebung durch technische Maßnahmen stattfinden muss.[30] Dass die Umsetzung technischer Schutzmaßnahmen dabei – wie von der Bundesregierung vertreten – unmöglich ist, wird angezweifelt.[31] Im Ergebnis kann und muss der Schutz der Berufsgeheimnisträger deshalb schon „by design" in die technische Einrichtung der Vorratsdatenspeicherung integriert werden. Auch unter diesem Gesichtspunkt sollte deutlich mehr Zeit in das Gesetzgebungsverfahren investiert werden.

kommunikation/Unternehmen_Institutionen/Anbieterpflichten/Meldepflicht/TKDiensteanbieterPDF.pdf?__blob=publicationFile&v=33 (Stand: 10.07.2015).

27 BR-Drs. 249/15, S. 4.

28 Siehe BR-Drs. 249/15, S. 33.

29 Vgl. BR-Drs. 249/15, S. 33.

30 Siehe nur die Stellungnahme des Deutschen Anwaltvereins (DAV) zum Referentenentwurf des BMJV für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, S. 13 ff.

31 Vgl. Spiecker/Simitis, „A Never-Ending Story: Die Vorratsdatenspeicherung", abrufbar unter: http://www.verfassungsblog.de/a-never-ending-story-die-vorratsdatenspeicherung/ (Stand: 10.07.2015).

5.4 Verfahrenstechnische Ansätze für den Berufsgeheimnisträgerschutz

Schon 1983 wurde im Volkszählungsurteil festgestellt, dass es unter den Bedingungen der automatischen Datenverarbeitung kein belangloses Datum gibt.[32] Für den speziellen Fall der Vorratsdatenspeicherung in Bezug auf die Berufsgeheimnisträger muss dies erst recht gelten. Deshalb ist es für den effektiven Schutz dieser besonderen Personengruppen notwendig, bereits die Datenspeicherung zu vermeiden: Wo keine Daten vorhanden sind, können diese auch nicht missbraucht werden. Unabhängig davon, ob die Aufstellung einer zentralen Liste sämtlicher Berufsgeheimnisträger in Deutschland technisch für realisierbar gehalten wird oder nicht, sollte es daher zumindest möglich sein, den Schutz besonderer Vertrauensverhältnisse um eine Stufe vorzuverlagern und bereits unmittelbar bei der organisatorischen Infrastruktur der TK-Unternehmen anzusetzen, um eine Speicherung der Vorratsdaten für die Berufsgeheimnisträger von Anfang an zu vermeiden. Ein alternativer verfahrenstechnischer Lösungsansatz könnte sich dabei in folgende Schritte gliedern:

1. **Ermittlung und Einmeldung der Berufsgeheimnisträger:** Zuvorderst ist sicherzustellen, dass bereits den TK-Dienstleistern diejenigen Personen unmittelbar bekannt sind, deren Kommunikation besonders schutzwürdig ist. Hierzu müssen für Bestands- und für Neukunden folgende Maßnahmen getroffen werden: Für Bestandskunden gilt, dass nach einer möglichen Wiedereinführung der Vorratsdatenspeicherung den TK-Unternehmen die einmalige Verpflichtung zugewiesen werden muss, sämtliche Anschlussinhaber auf die Speicherpflicht hinzuweisen und in diesem Zuge die Kunden zu befragen, ob sie den gesetzlich festgeschriebenen Kategorien besonders schutzbedürftiger Personen unterfallen. Diese können gegen einen gültigen Nachweis, beispielsweise einer beglaubigten Kopie des Arztausweises, ihre Einmeldung als Berufsgeheimnisträger unmittelbar bei dem jeweiligen TK-Unternehmen vornehmen. Die Rückmeldefrist für die Berufsgeheimnisträger sollte ein halbes Jahr betragen. In dieser Phase ist nach Inkrafttreten der neuen Regelungen zur Vorratsdatenspeicherung vorzusehen, dass noch keinerlei Speicherung der Verkehrsdaten stattfindet. Die durch das Einmeldeverfahren seitens der Betreiber entstehenden finanziellen Belastungen sind durch den Staat auszugleichen; entsprechende Ausschüttungen zugunsten der TK-Dienstleister müssen bereits im Vorfeld gesetzlich vorgesehen werden. Nach Ablauf der halbjährigen Privilegierungsfrist findet die Speicherung der Vorratsdaten gemäß dem Gesetzentwurf statt, zugleich aber ist die Einmeldung als Berufsgeheimnisträger für Bestandskunden weiterhin möglich. Für Neukunden gilt, dass die Einmeldung als Berufsgeheimnisträger bei Abschluss des TK-Dienstvertrags unmittelbar beim Netzbetreiber erfolgen muss. Entsprechende Vertragsformulare sind daher vorzusehen. Nach Nachweiserbringung und Überprüfung durch das TK-Unternehmen sind die Neukunden ebenso als Berufsgeheimnisträger eingemeldet.
2. **Privilegierung der Berufsgeheimnisträger unmittelbar durch den TK-Dienstleister:** Diejenigen Personen, die überprüft und eingemeldet sind, werden als Berufsgeheimnisträger in dem Sinne privilegiert, dass für ihren Anschluss die Verkehrsdaten nach § 113a TKG nicht gespeichert werden. Einge-

32 BVerfG NJW 1984, 419, 422.

meldete Berufsgeheimnisträger müssen in regelmäßigen Zeitabständen Nachweise über die Aktualität ihres Status erbringen, anzudenken wäre hier ein Halbjahresrhythmus. Dabei ist es nicht notwendig, dass jeweils spezifische Informationen über den tatsächlich ausgeübten Beruf gespeichert werden, vielmehr ist es ausreichend, dass alle eingemeldeten Personen ohne nähere Angaben in einer gemeinsamen Kategorie geführt werden. Ein solches Verfahren bietet gegenüber einer zentral geführten, bundesweiten Liste nicht nur den Vorteil, dass eine deutlich leichtere Aktualisierung stattfinden kann, indem der Kontakt zum Berufsgeheimnisträger unmittelbar über den jeweiligen Diensteanbieter vorgenommen wird, der stets über aktuelle Kundendaten verfügt. Darüber hinaus besteht auch ein geringeres Missbrauchsrisiko, indem eine Übermittlung der Liste mit der Gefahr der Erstellung unbefugter Kopien nicht stattfindet. Freilich sind die TK-Dienstleister für den Aufwand, jeweils eine eigene Kategorisierung der Berufsgeheimnisträger führen zu müssen, aus staatlichen Mitteln finanziell zu entlasten.

3. **Ergänzung der Einmeldungen durch manuelle Prüfverfahren:** Grundsätzlich wird davon auszugehen sein, dass die Berufsgeheimnisträger sich selbstständig einmelden, um in den Genuss der Privilegierung von der Vorratsdatenspeicherung zu gelangen. Dies kann jedoch nicht ausreichend sein, um einen möglichst umfassenden Schutz vor unberechtigten Datenerhebungen seitens der Ermittlungsbehörden zu gewährleisten, denn immer noch besteht das Risiko, dass einzelne Berufsgeheimnisträger keine Einmeldung nach vorgenanntem Verfahren durchführen. Für diesen Fall ist ein weiterer Verfahrensschritt vorzusehen: Soweit eine Person nicht eingemeldet ist, werden ihre Verkehrsdaten unabhängig von ihrem beruflichen Status zunächst beim TK-Diensteanbieter gespeichert. Falls dann ein behördlicher Abruf dieser Daten über das Instrument der Vorratsdatenspeicherung erfolgt, ist in einem doppelt gestuften Verfahren das behördliche Informationsrecht zunächst auf die Identifikationsmerkmale des Berufsgeheimnisträgers zu beschränken. Die Ermittlungsbehörde wäre dann verpflichtet, zunächst die fehlende Eigenschaft als Berufsgeheimnisträger festzustellen, bevor der Abruf der eigentlichen Vorratsdaten vom TK-Unternehmen stattfindet. Falls sich im Rahmen der Ermittlungen hingegen ergibt, dass es sich bei der betroffenen Person tatsächlich um einen Berufsgeheimnisträger handelt, der jedoch beim Diensteanbieter nicht eingemeldet ist, so dürfen die Vorratsdaten trotz Speicherung nicht abgerufen werden. Vielmehr ist das TK-Unternehmen durch die Behörde von der Eigenschaft als Berufsgeheimnisträger in Kenntnis zu setzen und die schon gespeicherten Verkehrsdaten sind zu löschen. Der TK-Diensteanbieter muss den Kunden darüber hinaus über seine von nun an folgende, halbjährliche Nachweispflicht unterrichten. Abschließend ist zu gewährleisten, dass die Einhaltung des gesamten, behördlich vorzunehmenden manuellen Prüfverfahrens durch regelmäßige Kontrollen zumindest der Fach- und Dienstaufsichtsbehörden sichergestellt wird. Ebenso muss eine regelmäßige, externe Überprüfung der für den TK-Diensteanbieter vorgesehenen Verfahrensbestimmungen stattfinden.[33]

Durch das vorgenannte Verfahren ist es nicht nur möglich, der Tatsache Rechnung zu tragen, dass die Kommunikation bestimmter Berufsgruppen besonders vertraulich ist und deshalb auch eines besonderen Schutzes bedarf. Ebenso kann hierdurch die beispielsweise in § 100g Abs. 4 S. 1 StPO-E bzw. in § 160a Abs. 1 S. 1 StPO vorgesehene unsichere Prognoseentscheidung[34] vermieden werden, welche das Bestehen des Erhebungsverbots davon abhängig macht, ob voraussichtlich Erkenntnisse erbracht würden, bezüglich derer ein Zeugnisverweigerungsrecht besteht. Zwar hat eine verfahrenstechnische Begrenzung der Vorratsdatenspeicherung auch zur Folge, dass hierdurch die Verstrickungsregelungen des § 160a Abs. 4 StPO, die über § 100g Abs. 4 S. 6 StPO-E ebenso für anwendbar erklärt werden, leerlaufen, da die Verkehrsdaten im Sinne des § 113b TKG schon nicht gespeichert sind. Für das Bestehen eines wirklichen und nicht nur auf dem Papier stehenden Schutzes der Berufsgeheimnisträger ist das aber wohl hinzunehmen, da die Vorratsdatenspeicherung letzten Endes nicht das einzige Ermittlungsinstrument ist, welches den Behörden zur Verfügung steht. In diesem Sinne sollte auch die Vorratsdatenspeicherung nur als eine weitere Ermittlungsmöglichkeit unter vielen gesehen werden, die herkömmliche Methoden zwar ergänzt, nicht aber ersetzt.

6 Fazit

Ob die Wiedereinführung der Vorratsdatenspeicherung noch vor Einigung über eine Neuregelung auf europäischer Ebene tatsächlich so sinnvoll ist, wie vonseiten der Bundesregierung behauptet wird, muss sich erst noch zeigen. Zurzeit vermittelt das Gesetzgebungsverfahren einen Eindruck, wie er sich in der Debatte um Freiheit und Sicherheit seit den Anschlägen des 11. September 2001 schon häufig eingestellt hat: Es ist vor allem die Sicherheit, die im Vordergrund steht, nicht die Freiheit. Dass aber die Sicherheit kein Selbstzweck sein kann, sondern letztlich dem Schutz der Freiheit zu dienen bestimmt ist, gerät dabei schnell aus dem Fokus. Deshalb sind bei der Wiedereinführung der Vorratsdatenspeicherung in Deutschland dem Eingriff in die Grundrechte der Bürger klare Grenzen zu setzen. Eine verfassungskonforme Lösung kann nur unter strengen verfahrensrechtlichen Voraussetzungen möglich sein. Dabei muss allen Kritikern derartiger Verfahrensregelungen bewusst sein, dass es für die Vorratsdatenspeicherung als technisch äußerst anspruchsvollem Ermittlungsinstrument keine simple, allen Interessen gleichermaßen gerecht werdende Lösung auf Knopfdruck gibt, sondern umfassende Detailregelungen erforderlich sind, die einen breiten Abstimmungsprozess erfordern.

33 Siehe hierzu bereits den Aspekt der Kontrolle der Einhaltung von Datensicherheitsbestimmungen unter 3.

34 Kritisch zur hierbei stattfindenden Interessenabwägung auch Griesbaum, in: Karlsruher Kommentar zur Strafprozessordnung, § 160a, Rn. 6.