Meinhard Starostik • Rechtsanwalt

RECHTSANWALTSKANZLEI
Wittestr. 30E • D- 13509 Berlin
+49 30 8800030 • Fax: +49 30 88000310
kanzlei@starostik.de
USt-ID-Nr.: DE165877648

KANZLEI VEREIDIGTER BUCHPRÜFER
Schwarzenberger Str. 7 • D-08280 Aue
+49 3771 564700 • Fax: +49 3771 5647025

RA Starostik • Wittestr. 30 E • D-13509 Berlin

Bundesverfassungsgericht
Schlossbezirk 3
76131 Karlsruhe

Mein Zeichen: 49/2015 Berlin, den 28.11.2016

Verfassungsbeschwerde

des Herrn Dr. Patrick Breyer, XXXXXXXX, XXXXXXX
- Beschwerdeführer zu 1 -

des Herrn Frank Bsirske, XXXXXXXX, XXXXXXX
- Beschwerdeführer zu 2 -

des Deutschen Journalistenverbandes e.V., XXXXXXXX, XXXXXXX
- Beschwerdeführer zu 3 -

des Herrn Dr. Rolf Gössner, XXXXXXXX, XXXXXXX
- Beschwerdeführer zu 4 -

des Herrn Wolfgang Grebenhof, XXXXXXXX, XXXXXXX
- Beschwerdeführer zu 5 -

des Herrn Peer Heinlein, XXXXXXXX, XXXXXXX
- Beschwerdeführer zu 6 -

der Firma Heinlein Support GmbH, XXXXXXXX, XXXXXXX
- Beschwerdeführerin zu 7 -

des Herrn Prof. em. Dr. Friedhelm Hengsbach SJ XXXXXXXX, XXXXXXX
- Beschwerdeführer zu 8 -

der Frau Julia Hesse, XXXXXXXX, XXXXXXX
- Beschwerdeführerin zu 9 -

des Herrn Peter Jebsen-Marwedel, XXXXXXXX, XXXXXXX
- Beschwerdeführer zu 10 -

des Herrn Michael Kellner, Die Grünen, XXXXXXXX, XXXXXXX
- Beschwerdeführer zu 11 -

des Herrn Marc-Uwe Kling, XXXXXXXX, XXXXXXX
- Beschwerdeführer zu 12 -

der Frau Dr. Silke Lüder, XXXXXXXX, XXXXXXX

- Beschwerdeführerin zu 13 -

der Frau Katharina Nocun, XXXXXXXX, XXXXXXX

- Beschwerdeführerin zu 14 -

des Herrn padeluun, Marktstr. XXXXXXXX, XXXXXXX

- Beschwerdeführer zu 15 -

der Frau Petra Pau, Platz der Republik 1, XXXXXXXX, XXXXXXX

- Beschwerdeführerin zu 16 -

des Herrn Heinz Raschdorf, XXXXXXXX, XXXXXXX

- Beschwerdeführer zu 17 -

des HerrnKai-Uwe Steffens, XXXXXXXX, XXXXXXX

- Beschwerdeführer zu 18 -

der Frau Rena Tangens, XXXXXXXX, XXXXXXX

- Beschwerdeführerin zu 19 -

des Herrn Albrecht Ude, XXXXXXXX, XXXXXXX

- Beschwerdeführer zu 20 -

des Herrn Prof. Dr. Frank Überall, XXXXXXXX, XXXXXXX

- Beschwerdeführer zu 21 -

der Frau Halina Wawzyniak, XXXXXXXX, XXXXXXX

- Beschwerdeführerin zu 22 -

der Frau Dr. Juli Zeh, XXXXXXXX, XXXXXXX

- Beschwerdeführerin zu 23 -

Prozessbevollmächtigter: Rechtsanwalt Meinhard Starostik, Wittestr. 30E, 13509 Berlin

Namens und Kraft anliegender Vollmachten der Beschwerdeführerinnen und Beschwerdeführer erhebe ich Verfassungsbeschwerde mit dem Antrag,

1. dem Europäischen Gerichtshof die Frage vorzulegen, ob die zu 2. benannten angefochtenen Vorschriften mit Art. 15 RiL 2002/58/EG sowie Art. 7 und 8 der Charta der Grundrechte der Europäischen Union vereinbar sind,

2. die §§ 113b Abs. 1-4 und 8 sowie 113c Abs. 1 des Telekommunikationsgesetzes in der Fassung, die sie durch das Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (Bundesgesetzblatt I Seite 2218 ff.) erhalten haben, für unvereinbar mit Artikel 10, Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1, und Artikel 5 Abs. 1 des Grundgesetzes zu erklären.

Die Beschwerde wird im Namen von 32.043 Grundrechtsträgern erhoben. Beschwerdeführer im prozessualen Sinne sind die vorstehend genannten 23 Personen.

1 Die Beschwerdeführerinnen und Beschwerdeführer

Die Beschwerdeführerinnen und Beschwerdeführer (künftig: Beschwerdeführer) nutzen alle gängigen Telekommunikationsmittel, insbesondere Mobilfunkanschluss, Festnetzanschluss, SMS-Nachrichten, Internet und mobiles Internet.

1.1. Der Beschwerdeführer zu 1 ist Mitglied des Schleswig-Holsteinischen Landtags. Er ist Inhaber und regelmäßiger Nutzer eines Festnetztelefonanschlusses, eines Mobiltelefonanschlusses, mehrerer E-Mail-Postfächer sowie eines Internetzugangs. Mitunter nutzt der Beschwerdeführer einen kostenfreien Internet-Telefoniedienst.

Als Landtagsabgeordneter erhält er Hinweise auf Rechtsverstöße, Dienstpflichtverletzungen oder sonstige Missstände im Verantwortungsbereich des

Landes, die teilweise unter Verletzung von Vertraulichkeitsvorschriften gegeben werden. Aus seinen Kommunikationsdaten lässt sich auf die Quellen schließen und auf dieser Grundlage Ermittlungen einleiten. Es ist zu befürchten, dass solche Hinweise mit Blick auf das Risiko von Nachteilen ausbleiben, wenn jeder Kontakt wochenlang gespeichert bleibt.

Der Beschwerdeführer zu 1 ist in der Bürgerrechtsorganisation „Arbeitskreis Vorratsdatenspeicherung“ aktiv. Es handelt sich um einen Zusammenschluss von Bürgerrechtlern, Datenschützern und Internet-Nutzern, mithin um eine Bürgerinitiative. Die Aktivitäten des Arbeitskreises werden ausschließlich per E-Mail koordiniert. Der Beschwerdeführer zu 1 hat mehrere Demonstrationen des Arbeitskreises maßgeblich mit organisiert und geleitet. Zur Vorbereitung der Demonstrationen sind elektronische Kontakte mit den zahlreichen Kooperationspartnern und Unterstützern erforderlich. Bei Vorbereitungstreffen mit der Polizei waren teilweise auch Beamte des Landesverfassungsschutzes anwesend, weswegen auch sonst mit einer nachrichtendienstlichen Beobachtung der – vollkommen legalen – Aktivitäten des Arbeitskreises gerechnet werden muss. Der Beschwerdeführer zu 1 fühlt sich in seinen regierungskritischen Aktivitäten beeinträchtigt, wenn künftig sein gesamtes Kommunikations-, Bewegungs- und Internetnutzungsverhalten über Monate hinweg für staatliche Stellen nachvollziehbar wird. In Anbetracht einer Reihe von Durchsuchungen und Festnahmen staatskritischer Personen in der Vergangenheit, deren Rechtswidrigkeit oder Unbegründetheit später festgestellt wurde, will sich der Beschwerdeführer zu 1 nicht darauf verlassen, dass ihn die legale Ausübung seiner Grundrechte vor Nachteilen bewahrt.

1.2. Der Beschwerdeführer zu 2 ist Vorsitzender der Vereinten Dienstleistungsgewerkschaft (ver.di). In dieser Eigenschaft steht er in ständigem Kontakt mit Gewerkschaftsfunktionären und Außenstehenden (z.B. bei Betriebsratsgründungen, Streiks, Tarifverhandlungen) sowie im Austausch mit Politikern und Journalisten. Viele dieser Kontakte sind streng vertraulich.

1.3. Der Beschwerdeführer zu 3 ist die Gewerkschaft der deutschen Journalistinnen und Journalisten in der Rechtsform eines eingetragenen Vereins. Die Vertraulichkeit der Kommunikation mit den Mitgliedern und Funktionsträgern des Vereins sowie mit Außenstehenden, die Kontakt zu den Mitgliedern des Beschwerdeführers suchen, ist Voraussetzung für die unbefangene Kommunikation mit den vorstehend erwähnten Personen. Der Beschwerdeführer ist im Vereinsregister des Amtsgerichts Berlin (Charlottenburg) unter VR 4777 eingetragen und hat seine Geschäftsstelle in Berlin.

1.4. Der Beschwerdeführer zu 4 ist als Rechtsanwalt und Publizist tätig und damit zweifacher Berufsgeheimnisträger. Er hat die gesetzlich geschützten Vertrauensverhältnisse zwischen Anwalt/Mandant sowie Journalist/Informant zu schützen und sichert in diesen Verhältnissen stets Vertraulichkeit zu. Dasselbe gilt auch für seine Tätigkeit als

parlamentarischer Berater im Verhältnis zu Abgeordneten sowie als Vorstandsmitglied einer Menschenrechtsorganisation.

1.5. Der Beschwerdeführer zu 5 ist Mitglied des Vorstandes des Beschwerdeführers zu 3. Der Beschwerdeführer zu 5 gibt zu seiner Betroffenheit folgendes an, das hier wörtlich wiedergegeben werden soll:

„Ich arbeite seit über 25 Jahren als Redakteur in der Lokalredaktion einer mittelständischen Regionalzeitung in Nordbayern. Über die Jahre habe ich mir im Verbreitungsgebiet einen Namen erarbeitet als verlässlicher Ansprechpartner, der Informationen ggf. auch vertraulich behandelt und seine Informanten keinesfalls ‚ans Messer liefert'. Wer sich mit einem Thema oder einem Hinweis an mich wendet, weiß, dass er dies gefahrlos tun kann - Informantenschutz steht bei meiner Arbeit an vorderster Stelle. Denn auf Informanten bin ich als Journalist angewiesen, wenn ich meiner Funktion gerecht werden möchte.

Vertrauen und Vertraulichkeit sind das Fundament meiner Arbeit. Die Vorratsspeicherung rüttelt an diesen Grundfesten. Wie sollen sich Informanten vertrauensvoll an mich wenden, wenn sie nicht sicher sein können, dass Kontakte nicht zurückzuverfolgen sind? Informantenschutz beginnt bereits bei einer simplen Terminabsprache. Aus gutem Grund ziehen es manche Informanten vor, niemals mit ‚der Presse' gesprochen zu haben. Dies gilt es zu akzeptieren. Vorratsdatenspeicherung wirkt sich negativ auf die Bereitschaft von ‚Whistleblowern' und Informanten aus, sich an Journalisten zu wenden. Das kann nicht im Sinne von Pressefreiheit, die im Grundgesetz einen hohen Stellenwert genießt, sein."

1.6. Der Beschwerdeführer zu 6 ist als Systemadministrator bei der Beschwerdeführerin zu 7 tätig. Er kommt in dieser Eigenschaft täglich mit besonders sensiblen Geschäftsgeheimnissen in Berührung, deren Bekanntwerden existenzielle Unternehmungsgefährdungen ermöglichen könnte.

1.7. Die Beschwerdeführerin zu 7 bietet das Hosting von Daten auf Linux-Servern und den Betrieb von Mailboxen sowie revisionssichere Mail-Archiv-Lösungen an. Vertraulichkeit der von ihr ermöglichten Kommunikation für ihre Kunden sowie der Kommunikation mit denselben ist Kernbestand ihres Geschäftsmodells. Die Beschwerdeführerin ist im Handelsregister des Amtsgerichts Berlin (Charlottenburg) zu HRB 93818 eingetragen und hat den Sitz Ihrer Geschäftstätigkeit in Berlin.

1.8. Der Beschwerdeführer zu 8 ist als Geistlicher tätig und eine Grundvoraussetzung für die persönliche, geistliche und pastorale Begleitung ist die Vertraulichkeit seiner Tätigkeit. Er nutzt elektronische Briefkontakte, steht zu öffentlichen und privaten Radio-und TV-Sendeanstalten in häufigem Kontakt und trifft bei Publikationen Absprachen mit

Medien und Verlagen. Auch hierbei setzt er besondere Vertraulichkeit voraus. Er benutzt kein Mobiltelefon zum Surfen im Internet.

1.9. Die Beschwerdeführerin zu 9 ist in ihrer beruflichen Tätigkeit als Rechtsanwältin Berufsgeheimnisträgern. Sowohl im Hinblick auf die allgemeine Kommunikationsfreiheit als auch im ständigen vertraulichen Kontakt mit Ihren Mandanten ist sie darauf angewiesen, dass diese Kontakte vertraulich bleiben. Sie legt Wert auf die Feststellung, dass der Kontakt mit verschiedenen Mandanten einer bestimmten Gruppe bereits ein „Bild" formen kann. Ferner kann die Kontaktaufnahme zu ihr dazu führen, dass Mandanten bereits unter einen bestimmten Verdacht fallen. Sie stellt fest, dass Mandanten zunehmend zögern, Daten und Schriftsätze durch Fernkommunikation zu übermitteln bzw. zu besprechen.

1.10. Der Beschwerdeführer zu 10 ist Vorstandsmitglied des Beschwerdeführers zu 3 und gibt zu seiner besonderen Betroffenheit folgendes an:

„Ich arbeite seit 37 Jahren als Journalist; mal festangestellt, mal frei – für Radio, Print, TV und Online-Medien. In dieser Zeit habe ich mir ein Netz an Informanten aus vielen verschiedenen Branchen und gesellschaftlichen Bereichen aufgebaut. Diese müssen sich darauf verlassen können, dass sämtliche Kontakte mit mir als Pressevertreter hundertprozentig vertraulich sind.

Die Medien erfüllen als ‚vierte Gewalt' eine wichtige gesellschaftliche Funktion. Die Kontaktaufnahme mit mir als Journalist muss daher einem besonderen Schutz unterliegen. Vor allem, wenn sie durch ‚Whistleblower' geschieht, die politische, wirtschaftliche oder andere gesellschaftliche Missstände aufdecken wollen. Wenn ihre Identität durch Kontakt zu Journalisten zurückverfolgt werden kann und sie deshalb das Risiko der Weitergabe relevanter vertraulicher Informationen scheuen, schadet das der grundgesetzlich garantierten Pressefreiheit.

Auch als Funktionär einer Journalistengewerkschaft, der früher u.a. als Betriebsrat eines Großkonzerns fungierte, muss ich in der Lage sein, Kommunikation jedweder Art mit Informanten in einem geschützten Raum zu betreiben."

1.11. Der Beschwerdeführer zu 11 ist politischer Bundesgeschäftsführer von Bündnis 90/die Grünen. Er ist bei seinen sämtlichen politischen Kontakten auf Vertraulichkeit der Kommunikation und der durch die Verbindungsdaten aufgedeckten Beziehungsgeflechte seiner Tätigkeit angewiesen.

1.12. Der Beschwerdeführer zu 12 ist Künstler. Ihm ist wichtig, dass eine offene Gesellschaft Raum für Widerstand lässt. Die Vorratsdatenspeicherung beschneidet diesen Raum. Wer sich überwacht fühlt, agiert

nicht mehr frei und zensiert sich selbst. Zudem kann niemand garantieren, dass die gespeicherten Daten nicht über Sicherheitslücken in die Hände Dritter gelangen und dabei jegliche Privatsphäre vernichten.

1.13. Die Beschwerdeführerinnen zu 13 ist niedergelassene Ärztin und stellvertretende Bundesvorsitzende der „Freie Ärzteschaft e. V.“. Die Vertraulichkeit ihrer Verbindungsdaten ist für sie als Ärztin besonders wichtig, weil nur so die ärztliche Schweigepflicht bewahrt werden kann, was die Grundvoraussetzung für ihre berufliche Tätigkeit ist.

1.14. Die Beschwerdeführerin zu 14 ist Mitglied des Beirats des Whistleblower Netzwerk e.V. und führt zu ihrer besonderen Betroffenheit folgendes aus:

„Als Mitglied im Beirat des vorbezeichneten Vereins fungiere ich als Anlaufstelle für journalistische Quellen und Hinweisgeber. Durch die Vorratsdatenspeicherung wird der Schutz von Whistleblowern, die im öffentlichen Interesse handeln, gefährdet. Als Journalistin verfasse ich regelmäßig Beiträge für große Tageszeitungen. Meine Kommunikation mit Quellen sowie die Recherche für Beiträge wird durch Vorratsdatenspeicherung massiver Überwachung ausgesetzt. Als Kampagnenleiterin für NGOs, gemeinnützige Vereine und politische Initiativen organisiere ich regelmäßig Demonstrationen und politische Protest-Aktionen. Durch die Vorratsdatenspeicherung lassen sich interne Strukturen politischer Bündnisse, wie etwa der Volksinitiative gegen CETA in Schleswig-Holstein, rekonstruieren. Die Vorratsdatenspeicherung schränkt die Wahrnehmung des politischen Engagements durch die Bevölkerung ein, wie Studien zur Selbstzensur und ‚Chilling-Effects‘ durch Überwachung zeigen.“

1.15. Der Beschwerdeführer zu 15 ist Mitglied im Vorstand des digitalcourage e.V. Er betreibt vertrauliche Recherchen mit Informanten, speziell für die Veranstaltung „BigBrotherAwards“. Er steht in laufendem Kontakt zu Bundes- und Europapolitikern und betreibt vertrauliche Recherchen im Internet.

1.16. Die Beschwerdeführerin zu 16 ist Vizepräsidentin des Deutschen Bundestages und Mitglied desselben. Bürgerinnen und Bürger vertrauen ihr oft sensible Daten und persönliche Informationen zwecks Interessenvertretung gegenüber Behörden und Institutionen an und erwarten zu Recht absolute Vertraulichkeit.

1.17. Der Beschwerdeführer zu 17 ist als Steuerberater und vereidigter Buchprüfer tätig und daher besonders um die Vertraulichkeit seiner Kontakte zu Mandanten, Banken und anderen Institutionen besorgt. Mandanten suchen ihn auch um Rat in steuerstrafrechtlichen Angelegenheiten auf. Der Beschwerdeführer sieht sich der Gefahr ausgesetzt, dass durch die Speicherung seiner Verbindungsdaten

ein aussagekräftiges Profil seines Mandanten- und Kontakte-Netzwerks gebildet werden kann.

1.18. Der Beschwerdeführer zu 18 ist politisch in Bürgerinitiativen aktiv und aus diesem Grunde besonders auf die Vertraulichkeit seiner Kommunikationsdaten angewiesen.

1.19. Die Beschwerdeführerin zu 19 ist Mitglied im Vorstand des digitalcourage e.V. In dieser Tätigkeit recherchiert sie sehr viel, sowohl telefonisch als auch persönlich und im Internet, unter anderem für den Datenschutz-Negativpreis „BigBrotherAwards“. Hierbei erhält sie Informationen aus Behörden, zivilgesellschaftlichen Organisationen und Unternehmen, bei denen es für sie essenziell ist, dass Ihre Informant.innen vertraulich bleiben. Dies ist bei Speicherung der Metadaten ihrer Kommunikation und ihrer Bewegungsdaten beim Mobilfunk nicht mehr gegeben. Da sie nicht ausschließen kann, dass die gesammelten Verbindungsdaten in unbefugte Hände geraten können, behindert die Vorratsdatenspeicherung ihrer Arbeit und ihre freie Kommunikation ganz erheblich. Deshalb ist auch bereits die Speicherung als solche für die Beschwerdeführerin ein Problem. Schon jetzt hört sie bei ihren Vorträgen, dass viele Bürgerinnen und Bürger sich nicht mehr trauen, Telefonnummern anzurufen, von denen sie befürchten, dass daraus Rückschlüsse auf sie, ihre Gesundheit, ihre politische Einstellung und ihren Freundeskreis gezogen werden. Wenn Menschen sich nicht mehr trauen ihre Organisation telefonisch oder per Internet zu kontaktieren, können wichtige Dinge möglicherweise nicht mehr ans Licht der Öffentlichkeit gelangen. Das schadet nicht nur der Beschwerdeführerin, sondern der Demokratie insgesamt.

1.20. Der Beschwerdeführer zu 20 ist Journalist und in seinem Beruf insbesondere investigativ tätig. Zur besonderen Bedeutung der Vertraulichkeit seiner Verbindungsdaten gibt er folgendes an:

„Aus den Verbindungsdaten können Rückschlüsse auf meine beruflichen Kontakte und auf meine Informanten gewonnen werden. Diese Kontakte muss ich aber schützen; die Vorratsdatenspeicherung wird (erneut) dazu führen, dass Informanten den Kontakt ablehnen. Aus den Metadaten der Kommunikation können Rückschlüsse über meine Recherchethemen gewonnen werden. Diese dürfen aber nicht bekannt werden, ehe die Recherchen abgeschlossen sind.“

1.21. Der Beschwerdeführer zu 21 ist der Vorsitzende der Beschwerdeführerin zu 3. Er macht zu seiner besonderen beruflichen Betroffenheit folgende Angaben:

„Ich recherchiere als freier Journalist (vor allem für WDR/ARD, aber auch für viele andere Medien) seit vielen Jahren investigativ vor allem in Korruptionsverfahren, in der (rechts-

)extremen Szene und bei Sicherheitsbehörden. Dass bei diesen Themen ein öffentliches Aufklärungsinteresse besteht, dürfte unbestritten sein. Die Kontaktaufnahme zu Informanten gestaltet sich in diesen Bereichen besonders schwierig. ‚Whistleblower', die auf problematische Zustände und Handlungen aufmerksam machen, sind in Deutschland gesetzlich nicht hinreichend geschützt. Aber selbst wenn sie das wären, besteht immer noch die Gefahr einer sozialen Ausgrenzung, wenn sie ihre Beobachtungen oder Erkenntnisse öffentlich machen. Hinzu kommt, dass sie zuweilen selbst gar nicht einordnen können, ob es sich um rechtlich zu beanstandende Vorgänge handelt oder nicht. Insofern ist die professionelle Recherche notwendig, um Hintergründe zu verstehen, um sie berichten zu können. Ein Vertrauensverhältnis kann da mit Hilfe von Telekommunikationsmitteln nur eingeschränkt aufgebaut werden. Trotzdem sind diese als erste Kontaktaufnahme unerlässlich. Die Kommunikation mit Informanten und deren Anwälten muss sich in einem geschützten Raum abspielen, da Medien(vertreter) sonst ihrer gesellschaftlichen Aufgabe als ‚vierte Gewalt' nicht mehr nachkommen können: Wer wendet sich schon an Journalistinnen oder Journalisten, wenn er Angst vor Verfolgung haben muss? So wie das Briefgeheimnis für postalische Kommunikation gilt, ist auch das gesprochene Wort zu schützen. Es muss einen Bereich geben, in dem auch womöglich falsche Vorwürfe geäußert werden können, ohne dass daraus der Vorwurf der Verleumdung abgeleitet werden kann. Die Kontaktaufnahme zu Medienvertretern ist keine Veröffentlichung! Die Betroffenen vertrauen sich dieser Berufsgruppe an, weil sie ihrer eigenen Organisation und auch Behörden nicht trauen. Neben dem Aspekt der psychischen Gewalt ist auch der der physischen Gewalt nicht zu unterschätzen: In extremistischen Szenen werden ‚Verräter' häufig verfolgt und eingeschüchtert. Wenn eine Vertraulichkeit der Kommunikation mit Medien nicht mehr gewährleistet ist, werden Menschen konkret gefährdet."

1.22. Die Beschwerdeführerin zu 23 ist Mitglied des Deutschen Bundestages der Fraktion DIE LINKE und zugleich Rechtsanwältin. Sie benutzt die Kommunikationsmöglichkeiten, insbesondere das Mobiltelefon sowohl in ihrer Eigenschaft als Abgeordnete als auch als Rechtsanwältin.

1.23. Die Beschwerdeführerin zu 23 ist Schriftstellerin. Sie führt zu Ihrer besonderen Betroffenheit aus:

„Für meinen Beruf als Schriftstellerin und Juristin ist die Vertraulichkeit der Kommunikation unerlässlich. Häufig recherchiere ich sensible Sachverhalte, die ich für meine Bücher brauche. Auch führe ich per Telefon oder E-Mail Gespräche mit Menschen, die sich als Quellen für meine Texte anbieten. Diesen muss ich Vertraulichkeit und Anonymität zusichern können; das ist, ähnlich wie bei einem Journalisten, Teil meines Berufs und meiner Berufsfreiheit. Schon die Tatsache, überhaupt mit mir in Kontakt zu stehen, ist in vielen Fällen ein sensibles Datum.

Hinzu kommt, dass ich mich durch anlasslose Vorratsdatenspeicherung in meinem Kommunikationsverhalten massiv gestört fühle und mich gezwungen sehe, in vielen Fällen auf andere Kommunikationswege auszuweichen, was ich als starken Eingriff in meine persönliche Freiheit empfinde."

2 Das Rechtsschutzbegehren der Beschwerdeführerinnen und Beschwerdeführer

2.1. Die angegriffenen Vorschriften

Die Beschwerdeführerinnen und Beschwerdeführer wenden sich mit der Verfassungsbeschwerde gegen die nachfolgend dargestellten Vorschriften des Telekommunikationsgesetzes – künftig: TKG –, in der Fassung, die sie durch das Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (Bundesgesetzblatt I Seite 2218 ff.) erhalten haben. Das Gesetz wurde im Bundesgesetzblatt Teil 1 Nr. 51 vom 17.12.2015 verkündet.

Es werden folgende Vorschriften angegriffen:

§ 113 Buchst. b Abs. 1-4 und 8 TKG

§ 113 Buchst. c Abs. 1 TKG.

Die angegriffenen Vorschriften haben folgenden Wortlaut:

§ 113b Pflichten zur Speicherung von Verkehrsdaten

(1) Die in § 113a Absatz 1 Genannten sind verpflichtet, Daten wie folgt im Inland zu speichern:

1.

Daten nach den Absätzen 2 und 3 für zehn Wochen,

2.

Standortdaten nach Absatz 4 für vier Wochen.

(2) Die Erbringer öffentlich zugänglicher Telefondienste speichern

1.

die Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,

2.

Datum und Uhrzeit von Beginn und Ende der Verbindung unter Angabe der zugrunde liegenden Zeitzone,

3.

Angaben zu dem genutzten Dienst, wenn im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können,

4.

im Fall mobiler Telefondienste ferner

a)

die internationale Kennung mobiler Teilnehmer für den anrufenden und den angerufenen Anschluss,

b)

die internationale Kennung des anrufenden und des angerufenen Endgerätes,

c)

Datum und Uhrzeit der ersten Aktivierung des Dienstes unter Angabe der zugrunde liegenden Zeitzone, wenn Dienste im Voraus bezahlt wurden,

5.

im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen.

Satz 1 gilt entsprechend

1.

bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei treten an die Stelle der Angaben nach Satz 1 Nummer 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht;

2.

für unbeantwortete oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe, soweit der Erbringer öffentlich zugänglicher Telefondienste die in Satz 1 genannten Verkehrsdaten für die in § 96 Absatz 1 Satz 2 genannten Zwecke speichert oder protokolliert.

(3) Die Erbringer öffentlich zugänglicher Internetzugangsdienste speichern

1.

die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,

2.

eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung,

3.

Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse unter Angabe der zugrunde liegenden Zeitzone.

(4) Im Fall der Nutzung mobiler Telefondienste sind die Bezeichnungen der Funkzellen zu speichern, die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt wurden. Bei öffentlich zugänglichen Internetzugangsdiensten ist im Fall der mobilen Nutzung die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle zu speichern. Zusätzlich sind die Daten vorzuhalten, aus denen sich die geografische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben.

...

(8) Der nach § 113a Absatz 1 Verpflichtete hat die auf Grund des Absatzes 1 gespeicherten Daten unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfristen nach Absatz 1, irreversibel zu löschen oder die irreversible Löschung sicherzustellen.

§ 113c Verwendung der Daten

(1) Die auf Grund des § 113b gespeicherten Daten dürfen

1.

an eine Strafverfolgungsbehörde übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b genannten Daten zur Verfolgung besonders schwerer Straftaten erlaubt, verlangt;

2.

an eine Gefahrenabwehrbehörde der Länder übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b genannten Daten zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes erlaubt, verlangt;

3.

durch den Erbringer öffentlich zugänglicher Telekommunikationsdienste für eine Auskunft nach § 113 Absatz 1 Satz 3 verwendet werden.

(2) Für andere Zwecke als die in Absatz 1 genannten dürfen die auf Grund des § 113b gespeicherten Daten von den nach § 113a Absatz 1 Verpflichteten nicht verwendet werden.

(3) Die Übermittlung der Daten erfolgt nach Maßgabe der Rechtsverordnung nach § 110 Absatz 2 und der Technischen Richtlinie nach § 110 Absatz 3. Die Daten sind so zu kennzeichnen, dass erkennbar ist, dass es sich um Daten handelt, die nach § 113b gespeichert waren. Nach Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten.

2.2. Die gerügten Grundrechtsverletzungen

Die Beschwerdeführer rügen in erster Linie

die Verletzung ihres Grundrechtes aus Art. 10 Abs. 1 GG (Telekommunikationsgeheimnis)

ferner

Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 (informationelle Selbstbestimmung)

Art. 5 Abs. 1 S. 1 HS 2 GG (Informationsfreiheit),

Art. 5 Abs. 1 S. 2 (Pressefreiheit),

vorsorglich auch Art. 3 Abs. 1 GG (allgemeiner Gleichheitssatz).

3 Zulässigkeit der Verfassungsbeschwerde

3.1. Die Grundrechtsträgereigenschaft der Beschwerdeführer

Bei den Grundrechten aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, 3 Abs. 1, 5 und 10 Abs. 1 GG handelt es sich um Jedermann-Rechte. Die Beschwerdeführer zu 1,2, 4 bis 6, 8 – 23 sind natürliche Personen

und können insofern die Verletzung dieser Grundrechte geltend machen.

Die Beschwerdeführer zu 3 und 7 sind inländische juristische Personen, deren Mitarbeiter alle angegebenen Formen der Telekommunikation nutzen. Diese Beschwerdeführer können sich gemäß Art. 19 Abs. 3 GG auf die Verletzung ihrer Grundrechte aus Art. 2 Abs. 1 i.V.m. 1 Abs. 1 und 10 Abs. 1 GG berufen.

Die besonderen Zulässigkeitsvoraussetzungen für eine unmittelbar gegen ein Gesetz gerichtete Verfassungsbeschwerde sind gleichfalls erfüllt. Die Beschwerdeführer sind unmittelbar, gegenwärtig und selbst betroffen.

3.2. Selbstbetroffenheit

Die Speicherverpflichtung, die aus § 113 Abs. 1 TKG folgt, und in § 113 Buchst. b TKG ausgestaltet ist, sowie die Verpflichtung zur Weitergabe der Daten durch die in § 113 Buchst. a TKG genannten, die in § 113 Buchst. c TKG geregelt ist, wendet sich nicht gegen die Beschwerdeführer. Das spricht jedoch nicht gegen die Selbstbetroffenheit der Beschwerdeführer, denn mit dem Rechtsbefehl an die in § 113 Buchst. a TKG genannten wird in der Ausgestaltung durch §§ 113 Buchst. b und c TKG die Speicherung und Weitergabe der Telekommunikationsdaten der Beschwerdeführer an staatliche Behörden geregelt. Dies ist nicht ein bloßer Reflex der Regelung, sondern der Kern ihres Gehaltes.[1]

3.3. Unmittelbarkeit der Selbstbetroffenheit

Gleichfalls keine Zweifel bestehen an der Unmittelbarkeit der Selbstbetroffenheit. Soweit es um die Speicherung von Daten nach § 113 Buchst. b TKG geht, sind die Beschwerdeführer direkt betroffen, denn es handelt sich um ihre Kommunikationsdaten.

Soweit es um die Verwendung der Daten gemäß § 113 Buchst. c TKG geht, steht der Unmittelbarkeit der Betroffenheit der Beschwerdeführer nicht entgegen, dass die Verwendung der Daten jeweils eines weiteren Vollzugsaktes bedarf. Insofern ist die Unmittelbarkeit schon deswegen gegeben, weil wegen der Streubreite der Speicherung und der damit verbundenen Möglichkeit der weiteren Verwendung der Daten der Beschwerdeführer eine hinreichende Wahrscheinlichkeit besteht, dass auch die Daten der Beschwerdeführer betroffen sein können. Die Darlegung, dass die Beschwerdeführer eine Straftat begangen haben, welche die in § 113 Buchst. c Abs. 1 Nr. 2 TKG genannten Rechtsgüter konkret gefährdet, ist nicht erforderlich[2].

---

[1] Insoweit bereits unproblematisch angenommen im Urteil vom 2. März 2010 1 BvR 256/08 u.a., Rn. 177

[2] BVerfG aaO, Rn. 178

3.4. Gegenwärtigkeit der Betroffenheit

Die Beschwerdeführer sind auch gegenwärtig betroffen. Die Speicherverpflichtung und die damit verbundenen Verpflichtungen nach §§ 113 Buchst. b und c TKG sind spätestens ab dem 1. Juli 2017 zu füllen, § 150 Abs. 13 S. 1 TKG.

Damit steht zwar im Zeitpunkt der Erhebung der Verfassungsbeschwerde noch nicht fest, dass die Telekommunikationsanbieter der Beschwerdeführer deren Telekommunikationsdaten speichern müssen, es ist aber innerhalb einer kurzen Frist sicher damit zu rechnen. In der Rechtsprechung des Bundesverfassungsgerichtes zur Gesetzesverfassungsbeschwerde ist geklärt, dass im Falle des alsbaldigen sicheren Eintretens einer möglichen Grundrechtsverletzung von deren Gegenwärtigkeit auszugehen ist. Die Rechtswirkungen des Gesetzes sind bereits jetzt klar abzusehen und für die Beschwerdeführer gewiss.[3.] Hinzu kommt, dass die Beschwerdeführer Dispositionen treffen müssen, wenn sie die Speicherung ihrer Telekommunikationsdaten vermeiden wollen, indem sie z.B. andere Kommunikationswege, die nicht erfasst werden, vorbereiten.[4]

Eine anderweitige Entscheidung, die dazu führte, dass die Verfassungsbeschwerde unzulässig wäre, führte auch zu einer unzumutbaren Verkürzung des Rechtsschutzes durch Erhebung einer Verfassungsbeschwerde. In zunehmendem Maße ist der Gesetzgeber gezwungen, gesetzliche Regelungen erst eingreifen zu lassen, wenn die einjährige Beschwerdefrist des §§ 93 Abs. 3 1. Alt. BVerfGG zur Erhebung einer Verfassungsbeschwerde unmittelbar gegen ein Gesetz bereits abgelaufen ist. Dies liegt häufig an der Erforderlichkeit, umfangreiche Voraussetzungen für die Anwendbarkeit eines Gesetzes zu regeln. So ist es auch hier. Die Speicherpflicht setzt so spät ein, weil zunächst die Bundesnetzagentur den nach § 113 Buchst. f Abs. 1 S. 2 TKG zu erstellenden Anforderungskatalog veröffentlichen muss. Danach brauchen die Telekommunikationsanbieter mehrere Monate, um ihre Systeme umzustellen. Sie müssen umfangreiche Investitionen in Speichermöglichkeiten und insbesondere in die dazugehörige Software sowie die Auswahl und Schulung ihre mit den Pflichten nach § 113 Buchst. b ff. TKG betrauten Mitarbeiter tätigen.

In einer solchen immer häufiger vorkommenden Konstellation entfiele der Grundrechtsschutz durch Erhebung einer Gesetzesverfassungsbeschwerde, wenn der Gesetzgeber aus jeweils nachvollziehbaren Gründen den Vollzug des Gesetzes jeweils in einen Zeitraum nach Ablauf der Beschwerdefrist legte. Auch unter dem

[3] BVerfG 14.07.1999 – 1 BvR 995/95 u.a. – Rn. 102 mwN = BverfGE 101,54

[4] BverfG 15.12.1983 -1 BvR 209/83 u.a. – Rn. 134 mwN = BverfGE 65,1

Gesichtspunkt des effektiven Rechtsschutzes ist daher hier davon auszugehen, dass die Beschwerdeführer gegenwärtig betroffen sind.[5]

3.5. Subsidiarität

Die hier eingereichte Verfassungsbeschwerde verstößt auch nicht gegen den Grundsatz der Subsidiarität, da der Sachverhalt allein spezifisch verfassungsrechtliche Fragen aufwirft. [6]

4 Die angefochtenen Regelungen

4.1. Zu erhebende Daten

Die §§ 113 Buchst. a und 113 Buchst. b TKG regeln die Speicherpflichten für die Verbindungs- und Standortdaten. Nach § 113 Abs. 1 S. 1 TKG bezieht sich die Speicherpflicht auf die Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer. Satz 2 der Vorschrift regelt sodann, dass der Anbieter öffentlich zugänglicher Telekommunikationsdienste für Endnutzer, der die zu speichernden Daten nicht selbst erzeugt oder verarbeitet, sicherstellen muss, dass die nicht von ihm selbst bei der Erbringung des Dienstes erzeugten oder verarbeiteten Daten nach § 113 Buchst. b Abs. 1 TKG gespeichert werden. Daraus folgt, dass der Gesetzgeber davon ausgeht, dass nicht alle nach § 113 Buchst. b Abs. 1 TKG zu speichernden Daten durch den Betrieb eines Telekommunikationsdienstes „einfach da sind“ sondern von unterschiedlichen Rechtspersonen erzeugt und verarbeitet werden können. Daraus folgt weiterhin, dass der Speicherung der Daten durch den zur Speicherung Verpflichteten deren Erhebung vorausgeht. Der erste grundrechtsrelevante Eingriff liegt demzufolge in der Erhebung der zu speichernden Daten.

Dies ergibt sich auch unter dem Gesichtspunkt, dass die vom Erbringer eines Telekommunikationsdienstes nach § 96 TKG zu speichernden Daten grundsätzlich von den nach § 113 Buchst. b TKG zu speichernden Daten zu trennen sind.[7] In beiden Fällen handelt es sich um Verkehrsdaten nach § 3 Nr. 30 TKG, ihre Erhebung und Verarbeitung erfolgt aber zu unterschiedlichen Zwecken. Geht man davon aus, dass die nach § 3 Nr. 30 TKG bei Erbringung eines Telekommunikationsdienstes vorhandenen Daten in einem technischen Prozess aufgrund der Prozessstruktur entstehen, so erfolgt ihre Erhebung jedenfalls für Zwecke der Speicherung und Verwendung nach §§ 113 Buchst. b ff. TKG erst durch

[5] So schon BverfG 07.10.2003 – 1 BvR 1712/01 - Rn. 65 = BverfGE 108, 370 <383>
6 vgl. BVerfG 12.05.2009, 2 BvR 890/06, BVerfGE 123, 148 <172 f>
[7] Vergleiche dazu Seite 16f. des Arbeitsentwurfs eines Anforderungskataloges nach § 113 Buchst. f TKG der Bundesnetzagentur – Stand Mai 2016

die Entnahme aus dieser Prozessstruktur für die Speicherung nach § 113 Buchst. b TKG.

4.2. Der Katalog des § 113b TKG

Erhoben werden nach dem Katalog des § 113 Buchst. b Abs. 2 bis 4 TKG insgesamt 25 unterschiedliche Daten:

1 Die Rufnummer oder Kennung des anrufenden Anschlusses, § 113b Abs. 2 S. 1 Nr. 1,

2 die Rufnummer oder Kennung des angerufenen Anschlusses, § 113b Abs. 2 S. 1 Nr. 1,

3 bei Um- und Weiterschaltungen die Rufnummer oder Kennung jedes weiteren beteiligten Anschlusses, § 113b Abs. 2 S. 1 Nr. 1,

4 Datum und Uhrzeit des Beginns der Verbindung unter Angabe der zu Grunde liegenden Zeitzone, § 113b Abs. 2 S. 1 Nr. 2,

5 Datum und Uhrzeit des Endes der Verbindung unter Angabe der zu Grunde liegenden Zeitzone, § 113b Abs. 2 S. 1 Nr. 2,

6 Angaben zu dem genutzten Dienst, falls die Nutzung unterschiedlicher Dienste möglich ist, § 113b Abs. 2 S. 1 Nr. 3

bei Nutzung von Diensten des Mobilfunks ferner:

7 die internationale Kennung des anrufenden Anschlusses (IMSI), § 113b Abs. 2 S. 1 Nr. 4 a)

8 die internationale Kennung des angerufenen Anschlusses (IMSI), § 113b Abs. 2 S. 1 Nr. 4 a)

9 die internationale Kennung des anrufenden Endgerätes (IMEI), § 113b Abs. 2 S. 1 Nr. 4 b)

10 die internationale Kennung des angerufenen Endgerätes (IMEI), § 113b Abs. 2 S. 1 Nr. 4 b)

11 bei Prepaid-Diensten Datum und Uhrzeit der ersten Aktivierung des Dienstes unter Angabe der zu Grunde liegenden Zeitzone, § 113b Abs. 2 S. 1 Nr. 4 c)

12 die Bezeichnung der Funkzelle, die durch den anrufenden Anschluss bei Beginn der Verbindung genutzt wird, § 113b Abs. 4 S. 1,

13 die Bezeichnung der Funkzelle, die durch den angerufenen Anschluss bei Beginn der Verbindung genutzt wird, § 113b Abs. 4 S. 1,

14 bei allen vorstehenden Telefondiensten ferner die vorstehenden Daten, soweit der Anruf unbeantwortet oder wegen eines Eingriffs des Netzwerkmanagements erfolglos geblieben ist, sofern die Daten für die in § 96 Abs. 1 S. 2 TKG genannten Zwecke gespeichert oder protokolliert werden. § 113b Abs. 2 S. 2 Nr. 2,

bei Nutzung von Internet Telefondiensten ferner:

15 Die IP-Adresse des anrufenden Anschlusses, § 113b Abs. 2 S. 1 Nr. 5,

16 die IP-Adresse des angerufenen Anschlusses, § 113b Abs. 2 S. 1 Nr. 5,

17 eine zugewiesene Benutzerkennung des anrufenden Anschlusses, § 113b Abs. 2 S. 1 Nr. 5

18 eine zugewiesene Benutzerkennung des angerufenen Anschlusses, § 113b Abs. 2 S. 1 Nr. 5,

bei Nutzung öffentlich zugänglicher Internet-Zugangsdienste ferner:

19 die dem Teilnehmer für die Internetnutzung zugewiesene IP-Adresse, § 113b Abs. 3 Nr. 1,

20 eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, § 113b Abs. 3 Nr. 2,

21 eine zugewiesene Benutzerkennung, § 113b Abs. 3 Nr. 2,

22 Datum und Uhrzeit des Beginns der Internetnutzung und der zugewiesenen IP-Adresse unter Angabe der zu Grunde liegenden Zeitzone, § 113b Abs. 3 Nr. 3,

23 Datum und Uhrzeit des Endes der Internetnutzung unter der zugewiesenen IP-Adresse unter Angabe der zu Grunde liegenden Zeitzone, § 113b Abs. 3 Nr. 3,

24 bei mobiler Nutzung des Internet-Zugangsdienstes die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle, § 113b Abs. 4 S. 2,

25 bei Nutzung von Kurz-, Multimedia- oder ähnlichen Nachrichten werden analog zu Nr. 1-18 die angefallenen Daten erhoben, wobei die unter Nr. 4 und 5 genannten Daten sich entsprechend auf den Zeitpunkt der Versendung und des Empfangs der Nachricht beziehen, § 113b Abs. 2 S. 2 Nr. 1.

Schließlich sind nach § 113 Buchst. b Abs. 4 S. 3 TKG zusätzlich die Daten vorzuhalten, aus denen sich die geographische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben.

Bei der Erhebung der Daten geht der Gesetzgeber davon aus, dass diese bereits vorhanden sind, ohne insofern auf eine Rechtsvorschrift Bezug zu nehmen, nach der diese Daten erhoben werden. Eine Ausnahme bildet die unter Nr. 14 genannte Erhebung der Daten erfolgloser Anrufe, denn diese hängt davon ab, dass der Anbieter sie nach der Vorschrift des § 96 Abs. 1 S. 2 TKG speichert oder protokolliert, also bereits erhoben hat. Hier wird eine Zweckänderung bereits vorhandener Daten gesetzlich festgelegt.

Bei der Bestimmung der Dienste, für die die Daten zu erheben sind, verwendet der Gesetzgeber bekannte Begriffe bis auf die unter Nr. 25 genannten „ähnlichen Nachrichten“ (§ 113 Buchst. b Abs. 2 S. 2 Nr. 1 TKG), sowie den unter Nr. 17, 18 und 21 benannten Begriff der „Benutzerkennung“, eine Neuschöpfung, die in § 113 Buchst. b Abs. 2 S. 1 Nr. 5 und Abs. 3 Nr. 2 TKG erstmalig im Gesetz verwendet wird.

4.3. Vergleich der nach dem neuen Gesetz zu erhebenden Daten mit der für nichtig erklärten Fassung des § 113 a TKG

An dieser Stelle ist es erforderlich, die nach geltender Rechtslage bestehenden Datenerhebungs- und Speicherpflichten mit der vom Bundesverfassungsgericht für nichtig erklärten Fassung des §§ 113 Buchst. a TKG zu vergleichen. Zunächst der Wortlaut der nichtigen Vorschrift:

(1) Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten nach Maßgabe der Absätze 2 bis 5 sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern. Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ohne selbst Verkehrsdaten zu erzeugen oder zu verarbeiten, hat sicherzustellen, dass die Daten gemäß Satz 1 gespeichert werden, und der Bundesnetzagentur auf deren Verlangen mitzuteilen, wer diese Daten speichert.

(2) Die Anbieter von öffentlich zugänglichen Telefondiensten speichern:

1.die Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,

2.den Beginn und das Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone,

3.in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst,

4.im Fall mobiler Telefondienste ferner:

a) die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss,

b) die internationale Kennung des anrufenden und des angerufenen Endgerätes,

c) die Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen,

d) im Fall im Voraus bezahlter anonymer Dienste auch die erste Aktivierung des Dienstes nach Datum, Uhrzeit und Bezeichnung der Funkzelle,

5.im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adresse des anrufenden und des angerufenen Anschlusses.

Satz 1 gilt entsprechend bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei sind anstelle der Angaben nach Satz 1 Nr. 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht zu speichern.

(3) Die Anbieter von Diensten der elektronischen Post speichern:

1. bei Versendung einer Nachricht die Kennung des elektronischen Postfachs und die Internetprotokoll-Adresse des Absenders sowie die Kennung des elektronischen Postfachs jedes Empfängers der Nachricht,

2. bei Eingang einer Nachricht in einem elektronischen Postfach die Kennung des elektronischen Postfachs des Absenders und des Empfängers der Nachricht sowie die Internetprotokoll-Adresse der absendenden Telekommunikationsanlage,

3. bei Zugriff auf das elektronische Postfach dessen Kennung und die Internetprotokoll-Adresse des Abrufenden,

4. die Zeitpunkte der in den Nummern 1 bis 3 genannten Nutzungen des Dienstes nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

(4) Die Anbieter von Internetzugangsdiensten speichern:

1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,

2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt,

3. den Beginn und das Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

(5) Soweit Anbieter von Telefondiensten die in dieser Vorschrift genannten Verkehrsdaten für die in § 96 Abs. 2 genannten Zwecke auch dann speichern oder protokollieren, wenn der Anruf unbeantwortet bleibt oder wegen eines Eingriffs des Netzwerkmanagements erfolglos ist, sind die Verkehrsdaten auch nach Maßgabe dieser Vorschrift zu speichern.

Nach der alten Vorschrift bestanden damit in Abs. 2 Nr. 1-4 d) Speicherpflichten, die in der obigen Liste den Nr. 1-13 entsprechen. Die Speicherpflicht nach Abs. 2 Nr. 5 entspricht in der obigen Liste den Nr. 15-16, die Speicherpflicht in Abs. 2 S. 2 entspricht der laufenden Nr. 25, die Speicherpflicht in Abs. 4 entspricht den obigen Nr. 19 und 20 sowie 22 und 23, die Verpflichtung in Abs. 5 entspricht der

laufenden Nr. 14. In der neuen Vorschrift sind die Dienste der elektronischen Post weggefallen, das war in der alten Vorschrift Abs. 3.

Damit sind die Erhebungs- und Speicherverpflichtungen neu hinzugekommen, die dargestellt wurden in Nr. 17, 18, 21 – das sind die Benutzerkennungen und 24 – das ist die Funkzelle bei Beginn einer Internetverbindung.

4.4. Die Bedeutung der zu erhebenden Daten im Hinblick auf das Grundrecht aus Art. 10 Abs. 1 GG

An dieser Stelle soll auf die Bedeutung der einzelnen zu erhebenden Daten eingegangen werden. Es ist dies erforderlich, um bei der Verhältnismäßigkeitsprüfung in Bezug auf die Erforderlichkeit für die Verfolgung des gesetzgeberischen Zweckes und die Verhältnismäßigkeit im engeren Sinne unter Abwägung der Tiefe des Grundrechtseingriffs eine genaue Feststellung der in jeder Datenerhebung, Speicherung und weiteren Verarbeitung liegenden Bedeutung für die Beschwerdeführer zu treffen.

Der Gesetzentwurf der Fraktion der CDU/CSU und SPD für den Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten begründet in der Einleitung die Erforderlichkeit des Grundrechtseingriffes wie folgt:

„*Bei der Aufklärung schwerer Straftaten und bei der Gefahrenabwehr sind Verkehrsdaten ein wichtiges Hilfsmittel für die staatlichen Behörden. Unter Verkehrsdaten im Sinne des § 96 des Telekommunikationsgesetzes (TKG) versteht man die Daten, die bei einer Telekommunikation anfallen, also zum Beispiel die Rufnummer der beteiligten Anschlüsse sowie Zeit und Ort eines Gesprächs. Es geht nicht um die Inhalte der Telekommunikation, sondern um die Frage, ob und wann Telekommunikation überhaupt stattgefunden hat*."[8]

Es geht also um die Frage, ob und wann Telekommunikation überhaupt stattgefunden hat.

Diese Frage lässt sich durch Erhebung der oben unter Ziffer 1-6 dargestellten Daten feststellen.

Nach den Ziffern 7 und 8 wird darüber hinaus die IMSI des anrufenden und angerufenen Anschlusses festgestellt, soweit Dienste des Mobilfunks genutzt werden. Die IMSI ist eine Kennung nach internationalem Standard, die sich auf der SIM-Karte befindet. Sie ist bei oberflächlicher Betrachtung nur eine andere Kennzeichnung der Rufnummer eines Mobilfunkanschlusses. Sie enthüllt damit zunächst keine weiteren Daten des Benutzers. Anders ist es aber, wenn ein

[8] BT Drs. 18/5088, S. 1

Benutzer unter einer Rufnummer seines Anschlusses mehrere SIM-Karten verwaltet, wie dies zumindest bei allen großen Anbietern von Mobilfunkdiensten möglich ist. Angenommen ein Benutzer hat drei SIM-Karten mit derselben Rufnummer. Die erste Karte dient der Benutzung des Smartphones, die zweite Karte wird im fest eingebauten Autotelefon benutzt und die dritte Karte wird im Tablet-Computer vorzugsweise für die Internetbenutzung, Internettelefonie aber auch Sprachtelefonie verwendet. Jede Karte hat ihre eigene IMSI, verwendet aber die dieselbe Rufnummer wie die beiden anderen Karten. Die Speicherung des Verkehrsdatums IMSI gibt damit über die bloße Tatsache, dass und mit wem zu welcher Zeit und wie lange und welchem Ort ein Telefonat stattgefunden hat, auch Auskunft darüber, welche SIM-Karte der Benutzer verwendet hat. Es handelt sich also um ein weiteres Datum betreffend das Kommunikationsverhalten des Benutzers, das über die nach der Gesetzesbegründung erforderlichen Daten hinausgeht.

Nach den Ziffern 9 und 10 wird die internationale Kennung der beteiligten Endgeräte, die IMEI, erhoben. Dieses Datum ist die eindeutige Kennung des beim Telefonat verwendeten Endgerätes. In dem vorangegangenen Beispiel ergibt sich aus diesem Datum, ob der Benutzer mit seinem Smartphone, seinem Autotelefon oder seinem Tablet-Computer telefoniert hat.

Bei Prepaid-Diensten sollen Datum und Uhrzeit der ersten Aktivierung des Dienstes unter Angabe der zu Grunde liegenden Zeitzone gespeichert werden. Dies Gesetzesbegründung zu § 113c Abs. 2 Nr. 4 Buchst. c bemerkt dazu:

„*Nach Buchstabe c ist bei der Inanspruchnahme im Voraus bezahlter anonymer Telefondienste der Zeitpunkt der ersten Aktivierung des Dienstes zu speichern. Sofern die Aktivierung einer solchen sogenannten Prepaidkarte mittels Anrufs beim Telekommunikationsdiensteerbringer erfolgt, werden diese Daten bereits durch die Nummern 1, 2 und 4 Buchstabe a und b erfasst, so dass auf der Grundlage dieses Aktivierungsverfahrens Buchstabe c zu keiner zusätzlichen Datenspeicherung führt. Soweit die Aktivierung des Dienstes auf eine Weise erfolgt, bei der Verkehrsdaten weder erzeugt noch verarbeitet werden, wie dies etwa der Fall sein kann, wenn die Freischaltung durch eine sofortige Onlineanmeldung bei Vertragsschluss von einem Mitarbeiter des Erbringers öffentlich zugänglicher Telekommunikationsdienste erfolgt, begründet dies nach Maßgabe von Absatz 1 Satz 1 keine Speicherpflicht*.“[9]

Mit Erhebung dieses Datums wird sichergestellt, dass der Zeitpunkt der Aktivierung einer Prepaidkarte auch in den Fällen festgestellt werden kann, in denen die Aktivierung nicht durch Erzeugung von Verkehrsdaten geschah. Der Zeitpunkt der Aktivierung einer Prepaidkarte ist ein für die Vertragsdauer

[9] BT Drs. 18/5088, S. 39

feststehendes Datum, also ein Bestandsdatum. Es kann erforderlichenfalls mit anderen Ermittlungsbefugnissen ermittelt werden. Es ist gerade nach der vorstehend wiedergegebenen Begründung des Gesetzesentwurfes in der zweiten dargestellten Fallgestaltung (sofortige Online-Freischaltung durch Mitarbeiter des Erbringers) kein Datum, das durch einen Telekommunikationsvorgang erzeugt wird. Eine Begründung für die Erforderlichkeit der Speicherung dieses Datums gibt der Gesetzesentwurf nicht.

Nach den Ziffern 12 und 13 werden die Standortdaten der Gesprächsteilnehmer bei Beginn des Gespräches erhoben. Das entspricht der Gesetzesbegründung.

Die Erfassung frustrierter Anrufe dient der Feststellung, wer versucht hat wen anzurufen und wo die Teilnehmer sich bei dem Anruf befanden. Jedenfalls geht die Erfassung dieser Daten bereits über das mit der Gesetzesbegründung verfolgte Ziel hinaus, indem auch die Nicht-Kommunikation festgestellt wird.

Die nach den Ziffern 15 bis 18 zu erhebenden Daten dienen auf den ersten Blick auch lediglich der Feststellung der Teilnehmer von Telefonaten unter Zuhilfenahme von Internet-Telefondiensten. Dass hierzu die IP-Adresse nicht mehr ausreicht, sondern eine weitere Kennung erforderlich ist, vom Gesetz als „zugewiesene Benutzerkennung“ bezeichnet, liegt an der rasanten Entwicklung der Benutzerzahlen von Internet-Diensten. Die IP-Adressen sind knapp. Sie reichen nicht mehr aus, um alle Benutzer mit einer jeweils eindeutigen IP-Adresse zu versorgen. Demzufolge sind die Anbieter zunächst im Mobilfunkbereich, jetzt aber auch im Festnetzbereich, dazu übergegangen, dynamische IP-Adressen jeweils für mehrere Benutzer zu vergeben. Es werden einer IP-Adresse bis zu 200 Benutzer zugewiesen. Die Unterscheidung der Benutzer erfolgt durch die Feststellung, welche Ports den Benutzern durch den Anbieter zugewiesen wurden.[10] Die jeweils benutzten Ports könnten also die „zugewiesene Benutzerkennung“ sein. Mithilfe des Ports wird zugleich der von einem Benutzer verwendete „Dienst“ im Sinne der IPv4-Terminologie festgestellt. Hat er Port 25 benutzt, so hat er eine E-Mail-Nachricht verschickt, über Port 995 hat der eine Internet-Nachricht von einem POP3-Server unter Zuhilfenahme der TLS- oder SSL-Verschlüsselung benutzt, Port 1167 ist Telefonaten zugewiesen.[11] Mit der Einführung der „Benutzerkennung“ als zu erhebendes Datum hat der Gesetzgeber also nicht nur die eindeutige Feststellung des benutzten Anschlusses sichergestellt, sondern darüber hinaus die Feststellung des Nutzerverhaltens.

[10] Vgl. die Darstellung in dem ECO-Hintergrundpapier „zur Diskussion um ein neues Gesetz zur Vorratsdatenspeicherung“ , S. 9 https://www.eco.de/wp-content/blogs.dir/20150520_hintergrundpapier_vds.pdf

[11] Vgl. https://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports und http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?&page=9 (das Original-Dokument der IANA-Organisation.

4.5. Datenspeicherung

Die vorgenannten zu erhebenden Daten sind zu speichern, und zwar im Inland;

die Verbindungsdaten nach Nr. 1 bis 11 und 14-25 für zehn Wochen,

die Standortdaten nach Nr. 12 und 13 für vier Wochen.

Für die Angaben zur geographischen Lage und Hauptstrahlrichtung der die jeweilige Funkzelle versorgenden Funkantennen sind keine Speicherfristen angegeben, was sich aus der Natur der Sache ergibt. Sie sind neben der Erhebung der Verkehrsdaten vom Anbieter zu erheben und zu speichern, um sie zusammen mit der Verkehrsdaten– oder Standortdaten-Auskunft zu übermitteln.

5 Art. 10 Abs. 1 GG

5.1. Schutzbereich

Das Telekommunikationsgeheimnis schützt die Vertraulichkeit der Kommunikation zwischen nicht Anwesenden vor einer Kenntnisnahme durch die öffentliche Gewalt, soweit die Grundrechtsträger Telekommunikationseinrichtungen in Anspruch nehmen[12]. Das Grundrecht stellt damit die Vertraulichkeit der Fernkommunikation derjenigen unter Anwesenden im Wesentlichen gleich.

Hierzu gehört nicht nur der Schutz der Kommunikationsinhalte, sondern auch der näheren Umstände der Kommunikation, wer mit wem wann von wo aus unter Nutzung welcher Dienste kommuniziert oder zu kommunizieren versucht hat. Das Kommunikationsmedium soll insgesamt vertraulich genutzt werden können[13].

Daraus folgt nach der Rechtsprechung des Bundesverfassungsgerichts, dass der Schutzbereich des Grundrechts auch den die Erhebung der Daten über die Umstände der Kommunikation sich anschließenden Informations- und Datenverarbeitungsprozess und den Gebrauch, der von den erlangten Kenntnissen gemacht wird, umfasst[14].

5.2. Eingriffstatbestände

Die Erhebung der Daten, ihre Speicherung und die Erteilung von Auskünften an Dritte stellen jeweils einen eigenen Eingriffstatbestand dar.[15] Wegen des engen

---

[12] BVerfG 02.03.2010 – 1 BvR 256/08 – Rn. 189; st. Rspr, vgl. die dortigen Nachweise = BverfGE 125, 260
[13] BVerfG, 02.03.2010, 1 BvR 256/08, BVerfGE 125, 260 <309>, BVerfG 14.07.1999 – 1 BvR 2226/94 – Rn. 163
[14] BVerfG 14.07.1999 – 1 BvR 2226/94- Rn. 165
[15] BVerfG, 24.01.2012, 1 BvR 1299/05, BVerfGE 130, 151 Ls. 2b

Sachzusammenhangs dieser drei Eingriffe werden sie aus Gründen der Übersichtlichkeit künftig auch weiter im Zusammenhang behandelt.

5.3. Rechtfertigung

5.3.1. Formelles Gesetz

Das Grundrecht des Art. 10 Abs. 1 steht unter Gesetzesvorbehalt, Abs. 2. Da es sich bei §§ 113b und 113 c TKG um ein Parlamentsgesetz handelt, das formell ordnungsgemäß zustande gekommen ist, sind insofern keine verfassungsrechtlichen Bedenken gegeben.

Es ist weiter zu prüfen, ob die angegriffenen Vorschriften auch nach den sonstigen Maßstäben zur verfassungsmäßigen Ordnung gehören, also insbesondere bestimmt sind, verhältnismäßig und gegebenenfalls im Einklang mit dem höherrangigen europäischem Recht stehen. Gerade auch die besonderen Anforderungen an den Gesetzgeber, die die Verarbeitung personenbezogener Daten betreffen, die mittels Eingriffen in das Telekommunikationsgeheimnis erlangt worden sind, gehören zu den besonderen Schranken des Art. 10 Abs. 1 GG. Insofern hat das Bundesverfassungsgericht weitgehend auf die Maßgaben zurückgegriffen, die im Volkszählungsurteil aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG entwickelt wurden[16].

5.3.2. Bestimmtheit

5.3.2.1. Maßstab

Der zugrunde zu legende Bestimmtheitsmaßstab ist bereits unter Berücksichtigung der Grundsätze, die das Bundesverfassungsgericht im Volkszählungsurteil aufgestellt hat, streng[17] Er ergibt sich vorliegend ferner aus Art. 103 Abs. 2 GG. Die Verarbeitung der Daten nach § 113b TKG ist durch die Bußgeldtatbestände in § 149 Abs. 1 Nr. 36-38 TKG geschützt.

Nach § 149 Abs. 1 Nr. 36 TKG handelt ordnungswidrig, wer entgegen § 113b Abs. 1 TKG Daten nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise, nicht für die vorgeschriebene Dauer oder nicht rechtzeitig speichert. Um welche Daten es sich handelt, ergibt sich aus dem Verweis in § 113b Abs. 1 TKG auf die Daten nach den Abs. 2 und drei in Nr. 1 der Vorschrift und die Daten nach Abs. 4 in Nr. 2 der Vorschrift. Der Tatbestand der Bußgeldvorschrift bezieht sich also auf alle oben zu Gliederungspunkt 4.1.2. unter Nr. 1-25 dargestellten Daten.

---

[16] BVerfG 14.07.1999 – 1 BvR 2226/94- Rn.166 und BVerfGE 65,1 <44ff.>

[17] Vgl. BVerfGE 65,1 <44ff.>

Nach § 149 Abs. 1 Nr. 37 TKG handelt ordnungswidrig, wer der Sicherstellungspflicht aus § 113b Abs. 1 i.V.m. § 113a Abs. 1 S. 2 TKG nicht nachkommt. Die Sicherstellungspflicht bezieht sich wiederum auf die dort genannten Daten, also diejenigen aus § 113b Abs. 2-4 TKG.

Nach § 149 Abs. 1 Nr. 38 TKG handelt ordnungswidrig, wer entgegen § 113 b Daten nicht oder nicht rechtzeitig löscht oder nicht sicherstellt, dass die Daten rechtzeitig gelöscht werden. Betroffener ist der nach § 113 a Abs. 1 TKG Verpflichtete, Daten sind die nach § 113 b Abs. 1 TKG zu speichernden Daten. Das sind wiederum diejenigen aus § 113 b Abs. 2-4 TKG.

Durchgängig ist demzufolge der strenge Bestimmtheitsgrundsatz des Art. 103 Abs. 2 GG auf den Begriff „Daten“ in § 113 b TKG anzuwenden.

5.3.2.2. § 113b Abs. 2 S. 2 Nr. 1 ,TKG

Der Begriff der „ähnlichen Nachricht“ in § 113 b Abs. 2 S. 2 Nr. 1 TKG ist unbestimmt. Hierauf hat die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in ihrer im Gesetzgebungsverfahren über die Vorsitzende des Ausschusses für Recht und Verbraucherschutz abgegebenen Stellungnahme hingewiesen.[18] Die Übermittlung einer Kurz-Nachricht wird man wohl als Übermittlung einer SMS verstehen können. Die Übermittlung einer Multimedianachricht wird man gleichfalls als MMS verstehen können.[19]

Die Gesetzesbegründung erwähnt hier als Beispiel „EMS“ und bezieht sich ausdrücklich darauf, dass die Speicherpflicht für Erbringer öffentlich zugänglicher Telefondienste gilt.

Neben der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit hat auch der deutsche Anwaltsverein in seiner Stellungnahme zum Gesetzentwurf darauf hingewiesen, dass unklar sei, ob die aktuellen Kommunikationsformen wie die Nutzung von Instant Messengern auf Mobilgeräten, Skype, Chats, Foren, IRC von der Speicherpflicht erfasst sind.[20]

---

[18] Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (BT-Drucksache 18/5088), S. 21 - http://www.bfdi.bund.de/DE/Datenschutz/Themen/Telefon_Internet/TelefonArtikel/VoarratsdatenspeicherungReloaded.pdf?__blob=publicationFile&v=3

[19] BT Drs. 18/5088, S. 38 (in der Bemerkung zu Abs. 2)

[20] DAV Stellungnahme Nr.: 25-15, S. 21 - https://anwaltverein.de/de/newsroom/sn-25-15-referentenentwurf-des-bundesministeriums-der-justiz-und-fuer-verbraucherschutz-fuer-ein-gesetz-zur-einfuehrung-einer-sp

Der Begriff der „ähnlichen Dienste“ lässt sich nicht zweifelsfrei durch Auslegung ermitteln. Der Wortlaut als äußerste Grenze der Auslegung ergibt keinerlei klares Auslegungsergebnis.

Aus Sinn und Zweck der Vorschrift ergibt sich gleichfalls nicht, dass die ähnlichen Dienste auf Dienste von Erbringern öffentlich zugänglicher Telefondienste beschränkt sind. Insbesondere ergibt diese Beschränkung kein klares Ergebnis, denn die Erbringer öffentlich zugänglicher Telefondienste stellen diese zunehmend über IP-basierte Dienste zur Verfügung. Zunehmend verschmelzen die Grenzen zwischen Telefon-, sonstigen Telekommunikations- und Telemediendiensten. Aktuell wirbt die deutsche Telekom:

„Deine Telefon- und Nachrichten-Funktionen können jetzt noch mehr!

Entdecke die neue Art der mobilen Kommunikation. RCS ist ein neuer IP basierter Mobilfunkstandard, der sich jetzt nahtlos in die Telefon- und Nachrichten-Funktionen Deines Smartphone einfügt. Damit ergänzt er die klassische SMS und MMS um Einzel- und Gruppenchats, das Austauschen von Fotos, Videos und vieles mehr. Anrufen verleiht RCS noch mehr Bedeutung und Interaktion. Verfügt Dein Smartphone noch nicht über diesen Standard, kannst Du Dir die RCS-fähige Telekom App Message+ installieren.*“ [21]

Ohne Zweifel ist die deutsche Telekom ein Erbringer eines öffentlich zugänglichen Telefondienstes, wie dies in § 3 Nr. 17 TKG definiert ist. Sind die in dieser Werbung angepriesenen Chats, ist das Austauschen von Fotos und Videos unter den Begriff „ähnliche Nachricht“ zu subsumieren wie eine Kurznachricht oder eine MMS, mit der schließlich auch Fotos ausgetauscht werden können? Wenn Sinn und Zweck der Vorschrift ist, neben den Umständen klassischer Telefonate auch die neueren Formen der elektronischen Übermittlung von Nachrichten wie SMS und MMS zu erfassen, dann könnten diese vorstehend beispielhaft dargestellten neuen Möglichkeiten der Kommunikation über das Telefon unter das Tatbestandsmerkmal „ähnliche Nachricht“ fallen.

Bei systematischer Auslegung ist zu berücksichtigen, dass § 113 b S. 2 TKG an die Vorschrift des S. 1 anschließt, der sich ausschließlich auf Erbringer von Telefondiensten, seien es die klassischen öffentlichen Telefondienste oder die mobilen Telefondienste oder auch die Internet-Telefondienste, bezieht. Allerdings soll S. 1 lediglich entsprechend gelten. Das spricht dafür, dass S. 2 lediglich an die zu speichernden Daten anknüpfen will, nicht aber an den der Datenübermittlung zu Grunde liegenden Dienst. § 113 b Abs. 5 TKG verbietet aber ausdrücklich die Speicherung der Daten von Diensten der elektronischen Post. Der Katalog der

21 https://messageplus.telekom-dienste.de/

Definitionen in § 3 TKG enthält keinen Begriff der elektronischen Post. Es ist davon auszugehen, dass der Gesetzgeber den Begriff so verwendet, wie er in Art. 2 Buchst. h) der Richtlinie 2002/58/EG verwendet wird. Danach ist „elektronische Post“ „jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird.“ Enthält § 113 b Abs. 5 TKG ein generelles Verbot der Speicherung der Daten solcher Dienste, dann wäre § 113 b Abs. 2 S. 2 TKG die Ausnahme von diesem generellen Verbot und wäre eng auszulegen. Das Ergebnis der systematischen Auslegung spricht dagegen, die über Chat-Dienste ausgetauschten Nachrichten unter diese eng auszulegende Ausnahme zu subsumieren. Was aber ist mit Diensten wie „WhatsApp“ oder „Threema“? Beide bieten nicht nur die Übermittlung von Textnachrichten, sondern auch die Versendung von Bildern, Videos sowie Sprach-und Ton-Nachrichten an. Auch hier spricht die systematische Auslegung gegen die Anwendung der eng auszulegenden Ausnahme in § 113 b Abs. 2 S. 2 TKG. Dem steht wiederum Sinn und Zweck der Vorschrift entgegen, die äußeren Umstände einer solchen Kommunikation zu erfassen.

Die Entstehungsgeschichte der Norm gibt für eine Auslegung in die eine oder andere Richtung keine entscheidenden Anhaltspunkte. Wie oben bereits dargestellt, führt die Erläuterung zum Gesetzentwurf nicht weiter. Der Vergleich der Kurznachrichten und MMS mit EMS hilft nicht weiter. Die Gesetzesbegründung erklärt nicht, was eine EMS ist, und es handelt sich auch nicht um eine den Beschwerdeführern bekannte Form der elektronischen Kommunikation.

Auch eine verfassungskonforme Auslegung des Begriffs erscheint nicht möglich. Eine Reduzierung des Begriffsinhalts „ähnliche Nachricht“ auf null führte zu einem zwar unter dem Gesichtspunkt des Grundrechtsschutzes wünschenswerten Ergebnis, dürfte aber dem Willen des Gesetzgebers, auch andere Nachrichten als SMS und MMS zu erfassen, nicht mehr entsprechen. Bei einem durch Auslegung nicht zu ermittelnden Ergebnis bleibt nur die Feststellung der Unbestimmtheit des Tatbestandsmerkmals.[22]

5.3.2.3. Zeitliche Unbestimmtheit der Auskunftsbefugnis

Das Gesetz bestimmt nicht eindeutig, für welchen Zeitraum die Auskunftsbefugnis besteht.

[22] Vgl. auch die Stellungnahme Nr. 25-15 des DAV, die insbesondere darauf abhebt, dass Messenger-Dienste zur elektronischen Post gehören (mwN) und über das Gebot der Speicherung „ähnlicher Nachrichten“ die Ausnahme der Daten der elektronischen Post von den Speicherpflichten faktisch ins Leere läuft.

Dazu fehlt bereits das Datum des Beginns der Speicherpflicht für die Daten. Ist es der Beginn der Verbindung, das Ende der Verbindung oder ihres Versuchs, oder ist es das Datum der erstmaligen Speicherung?

Diese Unbestimmtheit rührt daher, dass der Gesetzgeber keine Regelung zur Erhebung der Daten getroffen hat. Diese liegen nicht bereits bei Ende einer Verbindung in speicherbarer Form vor. Vielmehr bedarf es zunächst einer Aufarbeitung der in dem Netzelement (der Funkzelle) anfallenden Rohdaten, bis diese eindeutig mit allen zur Auskunftserteilung erforderlichen anderen Daten kombiniert sind und aus den Verkehrsdaten des Telekommunikationsanbieters erhoben werden können. Die Bundesnetzagentur geht in ihrem Leitfaden davon aus, „*…dass die erhobenen Verkehrsdaten binnen 24 Stunden nach dem jeweiligen Ereignis dem Verkehrsdatenspeichersystem zugeführt werden. In begründeten Einzelfällen kann nach Absprache mit der Bundesnetzagentur von dieser abgewichen werden.*“[23] Demzufolge besteht eine Datumsverschiedenheit zwischen dem zu speichernden Ereignis und dem Beginn der Datenspeicherung von einem Tage. Dieser Datumsunterschied besteht aber nur im Regelfall, der Anforderungskatalog sieht Ausnahmenmöglichkeiten vor. Die Ausnahmemöglichkeiten sind dadurch zu rechtfertigen, dass im Netz des Telekommunikationsanbieters Fehler bei der Datenerhebung auftreten können und diese Fehler zunächst festgestellt und berichtigt werden müssen, ferner können Fehler bei den Verkehrsdaten entstehen, die von Interconnectionpartnern des Telekommunikationsanbieters übermittelt werden.[24] Demzufolge ist vorhersehbar, dass bei auftretenden fehlerhaften Daten die Datumsdifferenz zwischen dem zu speichernden Ereignis und dem Tage der Speicherung mehr als einen Kalendertag beträgt.

Neben dem Fehlen des Beginns der Auskunftsfrist für die gespeicherten Daten fehlt es an einer eindeutigen Bestimmung des Endes des Zeitraums. Die Speicherfrist nach § 113 b Abs. 1 beträgt zehn Wochen für Verkehrsdaten und vier Wochen für Standortdaten. Die nach Ablauf der Speicherfrist mögliche weitere Speicherung beträgt gemäß § 113 b Abs. 8 eine Woche, weil innerhalb eines Zeitraums von maximal einer Woche die Daten gelöscht werden müssen.

Die Auskunftsverpflichtung nach § 113 c Abs. 1 bezieht sich auf die aufgrund des § 113 b gespeicherten Daten. Solange die Daten noch nicht nach § 113 b Abs. 8 gelöscht sind, sind sie „aufgrund des § 113 b gespeichert“. Angenommen, der Beschwerdeführer zu 1 wird mit seinem Mobiltelefon am 1. Juli 2017 telefonieren. Das ist ein Samstag. Der Gesprächspartner befindet sich im Ausland und die

[23] Ziff. 5.1.3 des Entwurfs eines Anforderungskataloges der Bundesnetzagentur nach § 113f TKG
[24] Vgl. Ziff. 4.2.2., 4.2.3. und 5.1.1. des Anforderungskataloges der Bundesnetzagentur nach § 113f TKG

Verkehrsdaten des Gesprächspartners sind, wie der Erbringer des Telefondienstes des Beschwerdeführers zu 1 bei der Aufbereitung der Daten feststellt, fehlerhaft. Eine sofortige Korrektur ist am folgenden Tage, einem Sonntag, nicht möglich. Die fehlerfreien Verkehrs- und Standortdaten werden daher erst am 3. Juli 2017 gespeichert werden. Der Erbringer des Telefondienstes führt die Löschung der Daten nach § 113 b Abs. 8 einmal täglich durch, aufgrund seines Organisationsplan erfolgt das am fünften Arbeitstag nach Ablauf der Speicherfrist, die der Betreiber vom Beginn des Ereignisses rechnet. Arbeitstage sind von Montag bis Freitag. Am Wochenende hat der Betreiber lediglich einen Notdienst, um den ungestörten Netzbetrieb aufrechtzuerhalten. Demzufolge sind die Standortdaten betreffend das Telefonat des Beschwerdeführers zu 1 bei dem Betreiber mit Ablauf des 7. August 2017 zur Löschung vorgesehen. Hätte nun der Betreiber der am 4. August 2017 anfragenden Strafverfolgungsbehörde noch Auskunft zu erteilen, da die Daten noch vorhanden sind, oder ist die Pflicht zur Auskunftserteilung mit Ablauf des 29. Juli 2017 erloschen oder mit Ablauf des 31. Juli 2017? Bestünde die Auskunftspflicht des Betreibers sogar noch am 7. August 2017? Der Mangel an Bestimmtheit führt auf Seiten des Betreibers zu einem schwerwiegenden Konflikt; ist die Auskunftserteilung am 7. August 2017 rechtswidrig, so kann ein Verstoß gegen § 206 StGB vorliegen, wird sie dagegen rechtswidrig nicht erteilt, so kann sich der Betreiber dem Vorwurf der Beihilfe zu einer Straftat oder der Begünstigung ausgesetzt sehen.[25] Erteilt er die Auskunft nicht, läuft er zumindest Gefahr, eine Ordnungswidrigkeit nach § 149 Abs. 1 Nr. 37 zu begehen. Der Beschwerdeführer zu 1 ist dem Risiko ausgesetzt, dass über seine Standortdaten vom 1. Juli 2017 noch am 4. oder 7. August 2017 Auskunft erteilt wird.

§§ 113 b und c sind mangels Bestimmtheit des Zeitraums der Auskunftspflicht verfassungswidrig.

5.3.2.4. § 113c Abs. 1 Nr. 1 und 2 TKG – Unbestimmtheit des Auskunftsberechtigten

§ 113 c Abs. 1 eröffnet die Auskunftsbefugnis gegenüber Strafverfolgungs- und Gefahrenabwehrbehörden. Nach dem „Doppeltürenmodell“ des Bundesverfassungsgerichts[26] wird damit die Erlaubnis an die privaten Verpflichteten (Verwaltungshelfer) geregelt, Auskünfte zu erteilen. Auf Seiten der

[25] Vgl. die Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (BT Drucksache 18/5088), dort S. 23f.
http://www.bfdi.bund.de/DE/Datenschutz/Themen/Telefon_Internet/TelefonArtikel/VoarratsdatenspeicherungReloaded.pdf?__blob=publicationFile&v=3

[26] Vgl. BverfG v. 24.01.2012 – 1 BvR 1299/05 – Rn. 123 = BverfGE 130, 151

anfragenden Behörden bedarf es dazu ferner einer Befugnisnorm, die Auskunft zu begehren. Auf der Stufe des § 113c Abs. 1 geht es nur darum, ob überhaupt – vorausgesetzt, die Behörde fragt berechtigt an – eine Auskunft erteilt werden darf.

Dazu muss normenklar festgelegt werden, wem die Erlaubnis zur Auskunftserteilung übertragen wird. Ausdrücklich benennt das Gesetz in Nr. 1 und 2 der Vorschrift niemanden, in Nr. 3 dagegen den Erbringer öffentlich zugänglicher Telekommunikationsdienste. Aus dieser unterschiedlichen Begrifflichkeit folgt, dass das Gesetz in Nr. 1 und 2 der Vorschrift einen anderen Erlaubnisinhaber meint. Allerdings ist bei Verwendung des einzigen Anhaltspunktes für eine Auslegung, nämlich bei systematischer Betrachtung, unklar, wer dies sein soll. Die Erlaubniserteilung gilt für die aufgrund des § 113 b TKG gespeicherten Daten. § 113b TKG verweist in Abs. 1 zurück auf die Vorschrift des § 113a TKG. Diese Vorschrift benennt in Abs. 1 S. 1 die Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer als zur Speicherung Verpflichtete, um sodann in S. 2 Nr. 1 die Möglichkeit zu eröffnen, dass diejenigen Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer, die nicht alle der nach Maßgabe der §§ 113b bis 113g TKG zu speichernden Daten selbst erzeugen oder verarbeiteten, durch einen Dritten speichern lassen.

Gäbe es diese Ausnahmemöglichkeit nicht, so könnte aus der Rückbezüglichkeit des § 113c Abs. 1 TKG auf § 113a Abs. 1 TKG geschlossen werden, dass die Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer die Erlaubnis zur Auskunftserteilung haben. Anders sieht es aber aus, wenn von der Übertragung der Speicherpflicht auf Dritte Gebrauch gemacht wird. Ist dann sowohl der Dritte Erlaubnisinhaber als auch der Erbringer der öffentlich zugänglichen Telekommunikationsdienste oder ist es nur der Letztere oder ist es derjenige, der die Daten gespeichert hat? Angenommen ein Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer – nennen wir ihn A – erzeugt die Daten für die Internetnutzung selbst, während er für die Erbringung der Telefondienste einen anderen Erbringer solcher Dienste, sagen wir die Telekom, benutzt. A speichert die bei Benutzung seiner Internet-Zugangsdienste anfallenden Daten nach § 113 b Abs. 3 TKG selbst, die bei Nutzung der Telefondienste einschließlich mobiler Telefondienste anfallenden Daten, die wiederum auch Daten über die Internetnutzung enthalten, lässt A bei der Telekom speichern. Wer hat nun die Erlaubnis zur Auskunftserteilung? Hierbei ist zu berücksichtigen, dass auch die Telekom öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, damit auch zu den Pflichtigen nach § 113 a Abs. 1 TKG gehört.

Denkbar ist z.B. Variante eins:

> A ist zur Auskunftserteilung über die unmittelbar von ihm gespeicherten Daten befugt. Die Telekom ist zur Auskunftserteilung über die bei ihr gespeicherten Daten befugt.

Denkbar ist aber auch Variante zwei:

> A ist nach dem Gesetzeskonzept der zur Speicherung Verpflichtete, die Telekom ist bei der Speicherung nur sein Erfüllungsgehilfe, daher ist A insgesamt zur Auskunftserteilung befugt, die Telekom ist es nicht.

Drei weitere Varianten ergäben sich, wenn A alle Dienste ausschließlich über die Telekom abwickelte, diese also auch die Daten erzeugte und schließlich für A speicherte. Hier wäre

denkbar Variante drei:

> Zur Auskunft berechtigt sind sowohl A als der genuin Speicherpflichtige als auch die Telekom als die Auftragsverarbeiterin.

Denkbar ist ferner Variante vier:

> A als der genuin Speicherpflichtige ist alleine zur Auskunft berechtigt.

Denkbar ist schließlich Variante fünf:

> Die Telekom, die die Daten speichert und den unmittelbaren Zugang zu ihnen hat, ist die zur Auskunft Berechtigte.

Keine Variante ist die zwingend richtige oder unter verfassungsrechtlichen Gesichtspunkten alternativlos. Es ist daher dem Gesetzgeber zu überlassen, hier Klarheit zu schaffen. Die Norm ist hinsichtlich der Feststellung des Auskunftsberechtigten unklar.

Sie ist mangels Bestimmtheit verfassungswidrig.

5.3.2.5. § 113c Abs. 1 Nr. 3 TKG - Zweckbindung der Auskunftsbefugnis

Die Vorschrift ermöglicht die Verwendung der aufgrund des § 113 b TKG gespeicherten Daten für eine Auskunft nach § 113 Abs. 1 S. 3 TKG, ermöglicht also die Auskunft über den Inhaber eines Internetanschlusses der hinter einer IP-Adresse steht – Bestandsdaten-Auskunft. Der Zweck der Datenverarbeitung ist in § 113 c Abs. 1 Nr. 3 TKG nicht eingegrenzt. Es handelt sich insofern um eine Tatbestandsverweisung auf § 113 Abs. 1 S. 3 TKG. Zum Tatbestand dieser Vorschrift gehört auch die Schrankenregelung in Absatz 2, was aus dem Wortlaut

„Die Auskunft darf nur erteilt werden…“ folgt. Danach sind tatbestandliche Voraussetzungen:

- Abfrage in Textform
- durch folgende Berechtigte:
    - Strafverfolgungs- oder Ordnungswidrigkeitenbehörden,
    - Für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständige Behörden,
    - Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst
- zu folgenden (alternativen) Zwecken:
    - Straftatenverfolgung
    - Verfolgung von Ordnungswidrigkeiten
    - Zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung
    - Für die Aufgabenerfüllung der Nachrichtendienste.

An dieser Stelle wird an den Erhebungszweck laut Gesetzesbegründung erinnert:

„*Es wird eine Regelung zur zeitlich befristeten Speicherung von Verkehrsdaten zur Strafverfolgungsvorsorge und zur Gefahrenabwehr geschaffen. Diese soll die Eingriffe in das Fernmeldegeheimnis aus Artikel 10 GG und die Grundrechte auf Datenschutz nach Artikel 7 (Achtung der Privatsphäre) und Artikel 8 (Schutz personenbezogener Daten) der Grundrechtecharta der Europäischen Union aus Gründen der effektiven Strafverfolgung in zulässiger Weise gestalten.*[27]

Der erklärte Erhebungszweck der Verkehrsdaten ist die Abwehr von (schweren) Straftaten und die Abwehr (besonders gewichtiger) Gefahren. Der tatsächlich erlaubte Verwendungszweck nach § 113 Buchst. c Abs. 1 Nr. 3 TKG ist die Verfolgung jeglicher Straftat oder Ordnungswidrigkeit, die Abwehr jeglicher Gefahr für die öffentliche Sicherheit oder Ordnung und die Erfüllung sämtlicher gesetzlicher Aufgaben der in § 113 Abs. 3 Nr. 3 genannten Dienste. Insofern liegt eine vom Gesetz vorgesehene Zweckänderung vor. Abgesehen davon, ob diese Zweckänderung hier zulässig sein kann, ist jedenfalls nicht hinreichend normenklar die Datenverwendung geregelt. Indem die

[27] BT Drs. 18/5088 , S. 2

Identifizierung von dynamischen IP-Adressen eine Deanonymisierung der Kommunikationsvorgänge im Internet ermöglicht, hat sie eine erhebliche Persönlichkeitsrelevanz. Der Anwendungsbereich der Auskunftsberechtigung ist nach dem Vorstehenden so weit, dass seine Grenzen völlig unscharf werden.[28]

§ 113c Abs. 1 Nr. 3 TKG ist mangels Bestimmtheit der Zweckbindung der Auskunftsbefugnis verfassungswidrig[29].

5.3.3. Vereinbarkeit der Erhebung, Speicherung und Verarbeitung mit der Charta der Grundrechte der Europäischen Union

5.3.3.1. Die Anwendbarkeit der Charta der Grundrechte der Europäischen Union

Mit der vorliegenden Verfassungsbeschwerde wird die Verletzung deutschen Verfassungsrechts durch die angegriffenen Gesetze gerügt. Vor Prüfung der Verhältnismäßigkeit soll hier erwogen werden, inwieweit Art. 7 und 8 der Charta der Grundrechte der Europäischen Union Einfluss auf die Prüfung nach deutschem Verfassungsrecht haben können. Die Charta der Grundrechte der Europäischen Union ist im Verhältnis zum deutschen Verfassungsrecht die höherrangige Norm; ihre Vorschriften bedürfen daher, soweit sie anwendbar sind, der Berücksichtigung bei der verfassungsrechtlichen Prüfung. Somit ist zu klären, ob die Vorschriften der Charta der Grundrechte der Europäischen Union überhaupt anzuwenden sind, sollte dies der Fall sein, ob und gegebenenfalls wie sie bei der Prüfung der Verfassungswidrigkeit einer Bundesnorm durch das Bundesverfassungsgericht anwendbar sind.

Der Gesetzgeber selbst ging im Gesetzgebungsverfahren von der Anwendbarkeit der Charta der Grundrechte der Europäischen Union aus.[30] Auch die wissenschaftlichen Dienste des Deutschen Bundestages und des europäischen Parlaments teilten diese Ansicht.[31] Allerdings binden die Unionsgrundrechte nur die Organe der Union im Verhältnis zu den Unionsbürgern, Art. 51 Abs. 1 S. 1 Charta der Grundrechte der Europäischen Union. Für die Mitgliedstaaten sind die

[28] Zu den Bestimmtheitsanforderungen vgl. BVerfG 24.01.2012 – 1 BvR 1299/05 – Rn. 174

[29] Vgl. auch die Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, aaO S. 24f.

[30] Vgl. BT-Drucksache 18/4764, S. 3

[31] Vgl. das Rechtsgutachten des Juristischen Dienstes des Europäischen Parlaments v. 22.12.2014, LIEBE – Questions relating to the judgement of the court of justice of 8 April 2014 in joined cases C-293/12 and C-594/12, Digital Rights and Seitlinger and others – Directive 2006/24EC on data retention – Consequencies of the judgement, S. 15ff.; Roland Derksen, Europarechtliche Spielräume zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten in den Mitgliedstaaten der Europäischen Union, Deutscher Bundestag – Ausarbeitung PE6-3000-53/15, S. 4ff. mwN

europäischen Grundrechte dann bindend, wenn diese Unionsrecht durchführen, was die legislative Umsetzung von Unionsrecht einschließt.[32]

Nach der Rechtsprechung des EuGH in der Entscheidung Åkerberg-Fransson ist der Anwendungsbereich des Art. 51 Grundrechte-Charta dann eröffnet, wenn die nationale Gesetzgebung in den Anwendungsbereich des Unionsrechts fällt und das Unionsrecht das nationale Recht determiniert.[33]

Das Bundesverfassungsgericht hat in seinem Urteil zur „Antiterror-Datei“ die Anwendbarkeit der Charta der Grundrechte der Europäischen Union auf seine Entscheidung in jenem Falle mit dem Argument abgelehnt, dass das Antiterrordateigesetz zum Bereich der öffentlichen Sicherheit gehöre, der nach Art. 3 Abs. 2 der Richtlinie 95/46 EG aus dem Anwendungsbereich der Richtlinie ausgenommen sei.[34] Das Bundesverfassungsgericht begrenzt in Übereinstimmung mit dem europäischen Gerichtshof die Anwendbarkeit der europäischen Grundrechte auf die „unionsrechtlich geregelten Fallgestaltungen“.[35]

Der Gesetzgeber hat nach dem Doppeltür-Modell des Bundesverfassungsgerichts mit der Anordnung der Erhebung, Speicherung und weiteren Verarbeitung der Telekommunikationsdaten die 1. Tür, nämlich die Auskunftsberechtigung, eröffnet. Ermächtigungsgrundlage für den Bundesgesetzgeber ist hierzu die Gesetzgebungskompetenz im Telekommunikationsrecht, Artikel 73 Abs. 1 Nr. 7 GG. Die Gesetzgebungskompetenz dieser Vorschrift ermächtigt den Bund nicht nur zur Regelung der technischen Seite der Errichtung einer Telekommunikationsinfrastruktur, sondern auch kraft Sachzusammenhangs zu datenschutzrechtlichen Bestimmungen der Datenverarbeitung innerhalb dieser Infrastruktur. Die Grenze der Gesetzgebungskompetenz des Bundes ist hierbei die Erforderlichkeit nach datenschutzrechtlichen Gesichtspunkten und den damit verbundenen verfassungsrechtlichen Anforderungen. Ausgeschlossen ist die Ermächtigung zum Datenabruf, soweit der Bund hierzu nicht weitere Kompetenznormen hat, wie dies im Strafrecht der Fall ist.[36] Festzuhalten bleibt, dass der Bund mit den hier angegebenen Rechtsvorschriften die datenschutzrechtlichen Gesichtspunkte der Telekommunikation regelt.

Die Telekommunikation und die datenschutzrechtlichen Anforderungen hieran sind Gegenstand des sekundären Unionsrechts, Sie sind in der Richtlinie

[32] Vgl.Schiedermair/Mrozek, Vorratsdatenspeicherung im Zahnräderwerk des europäischen Mehrebenensystems, DÖV 2016,89 <91mwN>
[33] EUGH 26.2.2013 Rs C-617/10
[34] BVerfG 24.4.2013 – 1 BvR 1215/07 – Rn. 90
[35] BVerfG ebda. Rn. 91
[36] BVerfG 24.1.2012 Rn. 128 - 130

2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation geregelt. Anders als in Art. 3 Abs. 2 Richtlinie 95/46/EG ist die Bereichsausnahme für den Bereich der öffentlichen Sicherheit in Art. 15 Abs. 1 der Richtlinie 2002/58/EG dergestalt geregelt, dass Ausnahmen von den Datenschutzvorschriften der Art. 5, 6, 8 Abs. 1, 2, 3 und 4 sowie Art. 9 der Richtlinie zulässig sind. Diese Ausnahme stehen unter dem Vorbehalt der Notwendigkeit, Angemessenheit und Verhältnismäßigkeit in einer demokratischen Gesellschaft und der allgemeinen Grundsätze des Gemeinschaftsrechts einschließlich der in Art. 6 Abs. 1 und 2 des Vertrages über die Europäische Union niedergelegten Grundsätze.

Mit dieser Regelung ist die Determinierung des Telekommunikationsrechts durch Unionsrecht auch im Bereich der öffentlichen Sicherheit gegeben. Die Richtlinie lässt lediglich Ausnahmen unter dem Vorbehalt der Notwendigkeit, Angemessenheit und Verhältnismäßigkeit nach unionsrechtlichen Vorschriften und der grundsätzlichen Geltung der Grundrechte der Union zu.

Nicht zu überzeugen vermag in diesem Zusammenhang die Argumentation von Wollenschläger, Art. 15 Abs. 1 der Richtlinie 2002/58/EG stelle lediglich eine klarstellende Öffnungsklausel zu Gunsten der Mitgliedstaaten dar, trotz der den Telekommunikationsunternehmen aufzuerlegenden Datenschutzpflichten Regelungen der Verkehrsdatenspeicherung einzuführen.[37] Wollenschläger übersieht hierbei nicht nur die strenge Beschränkung der Ausnahmen auf einzelne Artikel der Richtlinie und die Verhältnismäßigkeit nach unionsrechtlichen Maßstäben, sondern auch den ausdrücklichen Bezug auf Art. 6 Abs. 1 und 2 des EUV. Der Gesetzgeber der Richtlinie hat die Anwendbarkeit der Ausnahmen ausdrücklich an die Beachtung der europäischen Grundrechtecharta geknüpft.

5.3.3.2. Verhältnis zu den Grundrechten des Grundgesetzes

Geht man von der grundsätzlichen Anwendbarkeit der Grundrechte der europäischen Grundrechtecharta aus, so ist damit noch nicht die Frage geklärt, ob und wie diese im vorliegenden Verfahren der Verfassungsbeschwerde zu beachten sind.

Anders als die Grundrechte der EGMRK, die durch einfaches Bundesgesetz im Range unter dem Grundgesetz stehen und vom Bundesverfassungsgericht bei der Auslegung der Grundrechte beachtet werden, sind die Grundrechte der Charta der Grundrechte der Europäischen Union übergeordnetes Unionsrecht. Nach hier

[37] Vgl. Wollenschläger, Schriftliche Stellungnahme zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, S. 28
http://www.bundestag.de/blob/388296/77e18af13306be0d15e1b9fe9c002d33/wollenschlaeger-data.pdf

vertretener Ansicht können Sie dennoch im Verfassungsbeschwerdeverfahren angewendet werden, zumindest soweit sie Schutzbereiche eröffnen, die mit denjenigen der Grundrechte übereinstimmen. Dies dürfte bei Art. 7 und 8 der europäischen Grundrechtecharta und Art. 10 Abs. 1 GG sowie Art. 2 Abs. 1 in Verbindung mit 1 Abs. 1 GG (informationelle Selbstbestimmung) der Fall sein.

Nach Art. 53 der Charta der Grundrechte der Europäischen Union schränken die Bestimmungen der Charta die durch die Verfassungen der Mitgliedstaaten gewährten Grundrechte nicht ein. Gleichzeitig kann das Recht der Union nach Art. 52 Abs. 3 S. 2 einen weitergehenden Schutz als die EMRK gewähren. Der eigenständige und weitergehende Schutzbereich der unionalen Grundrechte bleibt damit gegenüber dem nationalen Verfassungsrecht bestehen. Das heißt auch, dass der Anwendungsvorrang des Unionsrechtes in diesem Bereich erhalten bleibt. Für den umgekehrten Fall der Einschränkung der bundesrechtlichen Grundrechte durch Unionsrecht hat das Bundesverfassungsgericht die durch Art. 23 Abs. 1 S. 3 i.V.m. Art. 79 Abs. 3 GG ausgestaltete Verfassungsidentität des Grundgesetzes als Grenze festgestellt die anzuwenden alleine dem Bundesverfassungsgericht vorbehalten ist.[38]

Für den hier zu entscheidenden Fall, wie die Unionsgrundrechte bei der Anwendung des grundrechtlichen Verfassungsrechts zu berücksichtigen sind, ist deren Schutzbereich, so er weiter ist als derjenige der Grundrechte des Grundgesetzes, in Erweiterung derselben anzuwenden, vorausgesetzt, nach der acte-claire-Rechtsprechung lässt sich dies eindeutig feststellen. Art. 23 Abs. 1 GG enthält auch ein Wirksamkeits-und Durchsetzungsversprechen für das unionale Recht.[39] Demzufolge verschafft das Bundesverfassungsgericht bei der Auslegung der Grundrechte zugleich dem Schutzbereich der unionalen Grundrechte Geltung. Bestehen dagegen Zweifel über den Schutzbereich der Grundrechte der Grundrechtecharta, so ist das Bundesverfassungsgericht als vorliegendes Gericht im Sinne des Art. 267 Abs. 3 AEUV anzusehen.[40]

Dies vorausgeschickt, werden bei den nachfolgenden Prüfungsmaßstäben für die Verhältnismäßigkeit diejenigen des Europäischen Gerichtshofs aus dem Urteil vom 08.04.2014 in den verbundenen Rechtssachen C-293/12 C-594/12 mit angewandt.

5.3.4. Verhältnismäßigkeit

[38] BVerfG, 15.12.2015 – 2 BvR 2735/14 – Rn. 40ff.

[39] BVerfG aaO Rn. 23

[40] Vgl. im Ergebnis auch: Österreichischer Verfassungsgerichtshof, Vorlagebeschluss vom 28.11.2012Rn. 25ff. https://www.vfgh.gv.at/downloads/vorabentscheidungsvorlagen/vorratdatenspeicherung_vorlage_eugh_g47-12.pdf

5.3.4.1. Gemeinwohlzweck

Die Datenspeicherung dient

1 der Verfolgung von Straftaten und

2 der Abwehr von Gefahren, schließlich auch

3 der Verfolgung von Ordnungswidrigkeiten und

4 dem Schutze der öffentlichen Sicherheit und Ordnung.

Nach der Rechtsprechung sowohl des Bundesverfassungsgerichts als auch des Europäischen Gerichtshofs bestehen bei den Zwecken zu 1 und 2 keine Zweifel hinsichtlich der Verfolgung eines legitimen Gemeinwohlzweckes soweit es sich um schwere Straftaten und die Abwehr besonders schwerer Gefahren handelt. Bei der Verfolgung von Ordnungswidrigkeiten hat das Bundesverfassungsgericht die Zulässigkeit der Beauskunftung auf die Inhaber von IP-Adressen beschränkt und ein Mindestmaß an Schwere vorausgesetzt[41], bei dem Schutz der öffentlichen Sicherheit dürften die Grenzen für die Ziele 1-3 einzuhalten sein, diesem Gemeinwohlzweck käme also neben den Zielen 1-3 in deren zulässigen Grenzen keine gesonderte Bedeutung zu, beim Schutz der öffentlichen Ordnung dürfte ein anerkennenswerter Gemeinwohlzweck für einen solch tiefgreifenden Grundrechtseingriff nicht mehr gegeben sein. Bereits die angestrebten Gemeinwohlzwecke sind also zu weit und können insofern das Grundrecht aus Art. 10 Abs. 1 GG nicht wirksam einschränken.

5.3.4.2. Erforderlichkeit

Erhebliche Zweifel sind bereits an der Erforderlichkeit der Maßnahme angebracht. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit weist in ihrer Stellungnahme darauf hin, dass es sich bei den Vorratsdaten um solche handelt, die die Erbringer öffentlicher Telekommunikationsdienste für Abrechnungszwecke speichern, so dass diese Daten anderweitig ohnehin zur Verfügung stehen.

In der Begründung zum Gesetzentwurf wurde ausführlich dargelegt, dass nach jetziger Tatsachenlage eine Schutzlücke bestehe, wenn die Strafverfolgungsbehörden nur auf die bei den Erbringern öffentlicher Telekommunikationsdienste vorhandenen Daten zugreifen könnten:

„*Die jetzige Gesetzeslage führt jedoch zu Unzulänglichkeiten bei der Strafverfolgungsvorsorge und bei der Gefahrenabwehr. Zwar können die*

[41] Vgl. BverfG v. 02.03.2010 – 1 BvR 256/08 u.a. – Rn. 261f. = BverfGE 125, 260

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 zum Zeitpunkt der Anfrage noch gespeichert sind. Die Erbringer öffentlich zugänglicher Telekommunikationsdienste dürfen im Einzelnen im Telekommunikationsgesetz bezeichnete Verkehrsdaten nämlich auch nach Beendigung des einzelnen Kommunikationsvorgangs speichern, wenn sie diese für – im Einzelnen im TKG festgelegte – eigene Bedürfnisse benötigen (zum Beispiel Aufbau weiterer Verbindungen, Rechnungsstellung, Störungsbeseitigung oder Schutz vor belästigenden Anrufen, § 96 TKG). Da die Speicherpraxis der Erbringer öffentlich zugänglicher Telekommunikationsdienste sehr unterschiedlich ist, ist es jedoch derzeit vom Zufall abhängig, welche Daten bei einer Abfrage nach § 100g StPO abgerufen werden können.“ [42]

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit widerspricht der auf nachvollziehbare Tatsachendarstellungen nicht gegründeten Behauptung energisch. Sie bezeichnet in ihrer Stellungnahme diese Aussage als nicht nachvollziehbar und stützt ihre Argumentation insofern auf die umfangreichen jahrelangen Prüferfahrungen bei den TK-Anbietern. Sie führt aus, dass beispielsweise Verkehrsdaten von Telefonverbindungen zu betrieblichen Zwecken regelmäßig zwischen drei und sechs Monaten vorgehalten werden. Diese Notwendigkeit ergebe sich schon aus dem den Kunden zustehenden, in § 45 Buchst. i Abs. 1 TKG gesetzlich normierten Einspruchszeitraum von acht Wochen nach Rechnungsversand. Somit könne davon ausgegangen werden, dass der überwiegende Teil der zu speichernden Daten bei den TK-Anbietern – jedenfalls in dem vom Gesetzentwurf festgelegten Zeitraum von zehn Wochen – ohnehin vorhanden ist und somit auch nach Maßgabe des geltenden Rechts für Auskünfte an die Sicherheitsbehörden zur Verfügung steht.

Eine Ausnahme hiervon bildeten lediglich die den Teilnehmern zugewiesenen IP-Adressen – die grundsätzlich nur bis zu sieben Tagen gespeichert werden –, Standortdaten in Form der Funkzellen sowie unter eine so genannte Flatrate fallenden netzinterne Verbindungen, die jeweils nach System des TK-Anbieters üblicherweise zwischen sieben und 30 Tage abrufbar seien. Im Gesamtvolumen der zu speichernden Daten dürften diese aber einen eher geringen Anteil ausmachen. Im Ergebnis sei die hier angeordnete Doppelspeicherung von unzähligen Daten daher absolut unnötig.[43]

---

[42] BT Drs. 18/5088,S. 21

[43] Vgl. die Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, aaO S. 5f.des BT vom 25.02.2011, WD 11-3000-18/11

Allenfalls käme als milderes Mittel eine Beschränkung der Speicheranordnung auf die Daten der zugewiesenen IP- Adresse und der Standortdaten in Betracht. Der Gesetzentwurf mache keine weiteren Ausführungen zur Erforderlichkeit, was nicht nur wünschenswert, sondern verfassungsrechtlich geboten sei, da der Gesetzgeber die Erforderlichkeit eines massiven Grundrechtseingriffs belegen müsse. Dieser Darlegungslast könne vorliegend auch nicht mit dem Argument entgangen werden, das Gesetz sei noch nicht in Kraft, so dass dementsprechend auch noch keine Ergebnisse über die Auswirkungen der Vorratsdatenspeicherung vorlägen. Bei der durch das Gesetz angeordneten Speicherung von Verkehrsdaten handele es sich nicht um eine völlig neue Maßnahme, sondern um eine neu aufgelegte, für die es bereits aus der Vergangenheit einschlägige, wenn auch nicht unumstrittene Gutachten gebe[44], die im Ergebnis keine messbare Effektivitätssteigerung durch die damalige Vorratsdatenspeicherung festgestellt hätten.[45]

Eine ausdrückliche Betonung der Darlegungslast des Gesetzgebers nahm auch der Deutsche Anwaltverein in seiner Stellungnahme im Gesetzgebungsverfahren vor. Auch diese Stellungnahme vermisst die ausreichende Darlegung der Erforderlichkeit und verweist darauf, dass der Gesetzgeber im Rahmen seines ihm alleine zustehenden Gestaltungsspielraums verfahrensbezogene Anforderungen zu erfüllen habe, zu denen eine Prognose gehöre, die aus sich selbst heraus eine spätere und überprüfbare Begründung zu den Annahmen über ihre voraussichtliche Wirkung erkennen lasse.[46] Die hierfür zum Beleg herangezogene Rechtsprechung des Bundesverfassungsgerichts dürfte zutreffend zitiert sein. Es handelt sich bei der infrage stehenden Maßnahme um einen schwerwiegenden Grundrechtseingriff – im Urteil des Bundesverfassungsgerichts vom 2. März 2010[47] als gerade noch zulässig gekennzeichnet – den der Gesetzgeber nicht ins Blaue hinein vornehmen darf. Da die Begründung für die Wiedereinführung der Vorratsspeicherung von Telekommunikationsdaten alleine auf dem vorerwähnten Grunde beruht, anderenfalls seien ausreichende Daten nicht verfügbar, steht diese Begründung zur vollen gerichtlichen Überprüfung.

Die Erforderlichkeit der angegriffenen gesetzlichen Regelungen ist ferner unter der Prämisse fraglich, dass bei einem solch schwerwiegenden Grundrechtseingriff die Beschränkung desselben auf das absolut Notwendige zu fordern ist, wie dies der Europäische Gerichtshof in seinem Urteil vom 8. April zu den Vorabentscheidungsersuchen betreffend die Gültigkeit der Richtlinie 2006/24/EG

[44] Vgl. Gutachten des Max-Planck-Instituts (zweite erweiterte Fassung) Juli 2011, S. 218; Rechtsgutachten des WD des BT vom 25.02.2011, WD 11-3000-18/11

[45] BfDI aaO, S. 6f. mwN

[46] Vgl. DAV Stellungnahme 25-15 aaO S. 8f. und Fn. 4

[47] Vgl. BverfG 02.03.2010 – 1 BvR 256/08 – Rn. 218 = BverfGE 125, 260

des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentliche Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG getan hat. [48]

Wendet man diesen Maßstab im Lichte der oben erwähnten Ausführungen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit an, so lässt sich die Begrenzung der gesetzlichen Speicherverpflichtung für die insgesamt 25 Merkmale nicht mehr als absolut notwendig feststellen.

5.3.4.3 Geeignetheit

5.3.4.3.1. Fehlende faktische Eignung

Das Bundesverfassungsgericht hat in seinem Urteil vom 2. März 2010 zur damaligen Regelung der Vorratsdatenspeicherung die Eignung dieser Regelung zur Verfolgung des angestrebten Zweckes nicht in Zweifel gezogen. [49] Auch der Europäische Gerichtshof hat die Vorratsspeicherung von Kommunikationsdaten als zur Erreichung des mit der Richtlinie 2006/24/EG verfolgten Zweckes als geeignet angesehen. Zur Frage der Umgehungsmöglichkeiten der Vorratsspeicherung der Daten folgte der EuGH der Einschätzung des Generalanwaltes, dass solche Möglichkeiten zwar die Eignung der Maßnahme begrenzten, aber nicht grundsätzlich infrage stellten.[50] An dieser Stelle bleibt festzuhalten, dass die im Gesetzgebungsverfahren vom Deutschen Bundestag zurate gezogenen Sachverständigen weitere Gründe oder Hinweise für die Eignung der Maßnahme nicht gefunden haben. Die Sachverständigen führten lediglich immer wieder Einzelfälle auf, die die Eignung der Maßnahme belegen sollten. Der Richter am Bundesgerichtshof Dr. Berger wies darauf hin, dass die Telekommunikationsdaten in der Regel am Anfang der Ermittlungen Ermittlungshinweise lieferten.[51] Insgesamt gibt es bisher keine wissenschaftliche Untersuchung, die diese Einschätzung bestätigt, die Wissenschaft hat bisher nur die gegenteiligen Einschätzungen bestätigt.[52] Leider hat bei den Terroranschlägen des letzten Jahres auch die Erfahrung bestätigt, dass die in Frankreich umfänglich eingeführte Vorratsdatenspeicherung zur Verhinderung der Anschläge nichts beigetragen hat.

---

[48] EUGH 08.04.2014 Rn. 51ff.
[49] BverfG 02.03.2010 – 1 BvR 256/08 – Rn. 207 = BverfGE 125,260
[50] EUGH 08.04.2014, Rn 49f.
[51] Vgl. Stellungnahme Dr. Berger, S. 37 - http://www.bundestag.de/blob/387808/d6991ea70ad90bf15cceaec565c36b3b/berger-data.pdf
[52] Vgl. Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg, 2. Aufl. 2011, S. 218

5.3.4.3.2. Bedeutung von Umgehungsmaßnahmen

Wie vorstehend ausgeführt, hat die verfassungsgerichtliche Rechtsprechung den Umgehungsmaßnahmen für die auf der Richtlinie 2006/24/EG beruhende Vorratsspeicherung von Kommunikationsdaten nicht die Bedeutung beigemessen, dass diese die Vorratsspeicherung vollständig ungeeignet machen. Diese Einschätzung beruht auf einer anderen Sachlage als sie bei der neuen gesetzlichen Regelung gegeben ist. Die Daten betreffend die elektronische Post sind vom Gesetz ausdrücklich ausgenommen, § 113 b Abs. 5. Die elektronische Post in Form der E-Mail hat quantitativ eine hohe Bedeutung; es werden in Deutschland (ohne Spam) weit über 500 Milliarden E-Mails verschickt.[53] Damit besteht eine einfache Möglichkeit, ohne Aufdeckung der Verbindungsdaten zu kommunizieren. Hinzu kommt die wachsende Bedeutung von Telemedienanbietern wie WhatsApp, die nach dem oben unter 5.3.2.2. ausgeführten nicht unter die „ähnlichen Nachrichten“ fallen dürften und daher gleichfalls eine spurenlose Kommunikation ermöglichen. Damit sind die Umgehungsmaßnahmen von ihrer Bedeutung her anders zu bewerten als bei der Entscheidung des Bundesverfassungsgerichts im Jahre 2010 und auch derjenigen des EuGH im Jahre 2014.

5.3.5. Verhältnismäßigkeit im engeren Sinne

Die stärksten Bedenken gegen das Gesetz ergeben sich unter dem Gesichtspunkt der Verhältnismäßigkeit im engeren Sinne. Diese Bedenken bestehen sowohl bei der isolierten Prüfung der Schwere des Eingriffs und dessen Folgen im Verhältnis zu dem erreichten Gemeinwohlziel als auch bei Einordnung der gesetzlichen Maßnahme in weitere Überwachungsmaßnahmen im Sinne einer gesamtgesellschaftlichen Überprüfung von additiven Grundrechtseingriffen, die von Rossnagel Überwachungsgesamtrechnung genannt wurde.[54]

5.3.5.1. Der Maßstab der strikten Erforderlichkeit

Die Schwere des Eingriffs eine - Überwachung nahezu des gesamten Telekommunikationsverhaltens der Bevölkerung - ist vom Bundesverfassungsgericht im Urteil vom 2. März 2010 ausführlich gewürdigt worden.[55] Nach dem vorstehend geschilderten Verhältnis der europäischen Grundfreiheiten und der bundesgesetzlichen Grundrechte dürfte aus heutiger Sicht bereits bei isolierter Betrachtung des Eingriffs dieser als verfassungsrechtlich unzulässig betrachtet werden. Der Europäische Gerichtshof hat für die in Betracht kommenden Grundrechte aus Art. 7 und 8 der Charta der

[53] BfDI aaO, S. 4 mit Nachweis in FN 6
[54] Roßnagel, Die „Überwachungs-Gesamtrechnung” – Das BVerfG und die Vorratsdatenspeicherung, NJW 2010, 1240
[55] BVerfG 02.03.2010 – 1 BvR 256/08 – Orientierungssatz 3c) aa) u. Rn 209

Grundrechte der Europäischen Union die Erforderlichkeit der Beschränkung des massiven Eingriffs der Vorratsspeicherung von Telekommunikationsdaten auf das absolut Notwendige verlangt.[56] Dabei ging der EuGH davon aus, dass die Richtlinie 2006/24 alle Verkehrsdaten betreffend Telefon, Festnetz, Mobilfunk, Internet-Zugang, E-Mail und Internet-Telefonie erfasste, also für alle elektronischen Kommunikationsmittel galt, deren Nutzung stark verbreitet und im täglichen Leben jedes einzelnen von wachsender Bedeutung ist. Zudem erfasste die Richtlinie alle Teilnehmer und registrierten Benutzer. Sie führte daher zu einem Eingriff in die Grundrechte fast der gesamten europäischen Bevölkerung.

Hierzu ist festzustellen, dass die angegriffene gesetzliche Regelung das Kommunikationsmittel E-Mail nicht mehr erfasst und daher die Kommunikation nicht mehr in dem Maße überwacht, wie es noch von der Richtlinie 2006/24 angeordnet war. Weiterhin bleibt es aber bei der vollständigen Überwachung des Telefonverhaltens und der Internetnutzung. In der Bedeutung stärker geworden ist auch die Möglichkeit der Erstellung von Bewegungsprofilen infolge der Nutzung von Mobiltelefonen.

5.3.5.2. Die verstärkte Überwachung der Internetnutzung und CNAT.

Die gesetzliche Anordnung der Erfassung der Internetprotokoll-Adresse zusammen mit einer eindeutigen Anschlusskennung, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung, § 113 b Abs. 3 Nr. 1 und 2 führt zu einer wesentlich genaueren Erfassung des Internetnutzungsverhaltens als man ohne Kenntnis der zu Grunde liegenden technischen Vorgänge aus der Vorschrift alleine erschließen könnte. Liest man die Vorschrift im Zusammenhang mit Nr. 3, dann würde lediglich Anfang und Ende der Internetnutzung von einem individuell eindeutig identifizierbaren Anschluss erhoben und gespeichert.

Wie oben unter 4.4 ausgeführt, hat die Knappheit der IP-Adressen im IPv4-Adressraum dazu geführt, dass die Anbieter von Telekommunikationsdiensten für Endnutzer einen Weg finden mussten, um durch Vergabe von Unterkennungen mehreren Nutzern den Internetzugang unter einer einzigen IP-Adresse zu ermöglichen. Das technische Verfahren hierzu ist das CNAT (Carrier Grade Network Address Translation, auch CGN abgekürzt).

Die Knappheit der IP-Adressen beruht darauf, dass sie aus vier Zahlenblöcken mit 256 Werten – einem Wert zwischen null und 255 - bestehen. Damit können in einem Netz maximal 4.294.967.296 Adressen (256^4) vergeben werden.[57] das reicht

[56] EUGH v. 08.04.2014 Rn. 52

[57] Vgl. https://de.wikipedia.org/wiki/IPv4#ICMP

bei weitem nicht mehr aus, um allen Internetnutzern jeweils eine einzige IP-Adresse zuzuweisen. Hintergrund ist zum einen die dauerhafte Nutzung von Internetzugängen infolge von Flatrates, zum anderen die insgesamt gestiegene Zahl von Internetzugängen, insbesondere durch Smartphones, Tablets und weitere technische Geräte, die einen Internetzugang haben. Die Zuweisung von dynamischen IP-Adressen beruhte darauf, dass nicht alle Nutzer gleichzeitig im Internet waren und deshalb die dynamische IP-Adresse mehreren Nutzen dienen konnte. Gerade durch die dauerhafte Nutzung von Anschlüssen infolge von Flatrates ist die Nutzung einer IP-Adresse durch aufeinander folgende Nutzungsvorgänge weitgehend entfallen.

Der technische Trick von CNAT besteht nun darin, dass der Telekommunikationsdiensteerbringer eine IP-Adresse ins Internet benutzt, intern aber diese IP-Adresse auf mehrere Nutzer aufteilt. Das geschieht dergestalt, dass jeder Nutzer eine interne IP-Adresse bekommt, für seine Nutzung intern einen jeweils benötigten Port nutzt, was an der Schnittstelle des Übergangs zum Internet dann in einen externen Port und eine externe IP-Adresse umgesetzt wird.

Aber auch das reicht nicht aus, wenn man bedenkt, dass 65.536 Ports vorhanden sind, bei Nutzung einzelner Kommunikationsdienste aber mehr als 1000 Ports gleichzeitig belegt werden, die nicht nur für die internen Ports, sondern hinter der Schnittstelle auch für die externen Ports benötigt werden. Um Überschneidungen zu vermeiden können daher nur 10-20 Kunden von ihren internen IP-Adressen ausgehend eine externe IP-Adresse gemeinsam benutzen.

Die Weiterentwicklung von CNAT besteht darin, dass nicht nur die interne IP-Adresse und der interne Port erfasst werden, sondern auch die IP-Adresse der Gegenstelle, deren Port und ggfls. die aufgerufene URL. So können mehrere Nutzer ein- und denselben externen Port nutzen, denn ihre abgehenden und ankommenden Datenpakete können über denselben externen Port an unterschiedliche Gegenstellen weitergeleitet werden. Der Erbringer eines Telekommunikationsdienstes muss also folgende Merkmale erfassen:

Interne IP-Adresse + genutzter Port -> externe IP-Adresse + genutzter externer Port <> IP-Adresse des Kommunikationspartners + dessen Port + ggfls. aufgesuchte URL. Damit können dreistellige Nutzerzahlen einer externen IP-Adresse zugewiesen werden. Dieses Verfahren wird in zunehmendem Maße von den Erbringern von Telekommunikationsdiensten genutzt. Es ist davon auszugehen, dass es in den nächsten drei Jahren flächendeckend in allen Netzen eingeführt wird.

Bei dieser Variante von CNAT muss der Diensteanbieter eine Übersetzungstabelle erzeugen, um die einzelnen Datenpakete jeweils intern und extern richtig

versenden zu können. Da die Anzahl dieser Daten sehr groß ist, werden sie lediglich vorübergehend – im Arbeitsspeicher – gespeichert. Für diese Tabelle werden mindestens benötigt:

Interne IP-Adresse und die von dieser benutzten Ports,

externe IP-Adresse für das vorstehende Datenpaar und externer Port,

IP-Adresse der Gegenstelle und deren Port sowie ggfls. die aufgerufene URL,

millisekundengenauer Zeitstempel zur Bestimmung von Status und Gültigkeit der Zuordnung.

Die Erhebungs- und Speicherpflicht nach § 113 b Abs. 3 führt dazu, dass diese große Datenmenge aus dem flüchtigen Speicher in einen permanenten Speicher übertragen werden muss und zu riesigen Datenbergen führen wird. Aus diesen Datenbergen lässt sich eine lückenlose Aufzeichnung des Verhaltens aller Nutzer im Netz rekonstruieren. Hiermit kann ein vollständiges Nutzerprofil des Einzelnen erstellt werden. Hierauf hat im Gesetzgebungsverfahren der ECO-Verband in seiner Stellungnahme vom 08.06.2016 hingewiesen.[58]

Wenn das Gesetz neben der IP-Adresse“ eine zugewiesene Benutzerkennung“ zu erheben und speichern verlangt, so kann die interne IP-Adresse diese Benutzerkennung nicht sein.

Das ergibt sich aus der nachstehenden Überlegung. Angenommen, ein nach § 113 Abs. 3 TKG Berechtigter fragt nach § 113 Abs.1 S. 3 i.V.m. § 113c Abs. 1 Nr. 3 TKG an:

„Wer ist Anschlussinhaber der um 0:00 Uhr genutzten IP-Adresse 160.20.20.183?“ Wären Anschlusskennung, interne IP-Adresse, externe IP-Adresse und Zeit gespeichert, so ergäbe die Ermittlung in der Datenbank des Providers, dass zum angegebenen Zeitpunkt unter der externen IP-Adresse die Benutzer mit der Anschlusskennung XYZ1, XYZ2, XYZ3, bis XYZn aktiv waren. Die IP-Adresse 160.20.0.183 ließe sich also nicht eindeutig einem einzigen Anschlussinhaber zuweisen.

Anschlusskennung	interne IP-Adresse	Schnittstelle	externe IP-Adresse	Zeit
XYZ1	10.0.0.20	|	160.20.20.183	00:00
XYZ2	10.0.0.21	|	160.20.20.183	00:00

[58] ECO Stellungnahme zum Gesetzentwurf der Bundesregierung für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, S 3 - https://www.eco.de/wp-content/blogs.dir/20150608-vds-stellungnahme-eco.pdf

XYZ3	10.0.0.22	|	160.20.20.183	00:00
…XYZn	10.0.0.n	|	160.20.20.183	00:00

Erst und allein die Kenntnis aller weiteren gespeicherten Verkehrsdaten, nämlich:

genutzter interner Port,

übersetzter externer Port,

IP Adresse des Zielsystems und dessen URL,

genutzter Port des Zielsystems,

ermöglicht zuverlässig die Kenntnis eines einzelnen Anschlussinhabers, der zum Zeitpunkt 0:00 Uhr die externe IP-Adresse 160.20.20.183 genutzt hat. Wegen der Möglichkeit der mehrfachen Nutzung von internen und externen Ports und auch der gleichzeitigen Nutzung der IP-Adresse des Zielsystems durch mehrere interne Nutzer darf keines der vorstehenden Merkmale wegfallen. Die Gesamtheit dieser Daten nenne ich künftig Nutzungsdaten.

Das Problem ist nun, dass über die Port-Adresse bereits festgestellt werden kann, welcher Art die Anfrage beim Zielsystem war. Die Ports 25, 143, 220 und 993 werden z.B. für die Versendung oder das Abrufen von E-Mails benutzt, über Port 80 wird das Protokoll HTTP benutzt, also Webseiten abgerufen. Damit ist bereits eine sehr genaue Feststellung des Nutzerverhaltens möglich. Wird zugleich beim Zielsystem ermittelt, lässt sich über die aufgezeichneten Daten feststellen, welche Webseiten benutzt wurden oder welche Mailbox angesprochen wurde.

Es ist also festzuhalten, dass das Tatbestandsmerkmal „eine zugewiesene Benutzerkennung“ und die Erforderlichkeit der Nutzung des CNAT-Verfahrens dazu führt, dass das gesamte Verhalten der Internetnutzung protokolliert werden muss. Das führt dazu, Rückschlüsse auf die Inhalte der Kommunikation zuzulassen, insbesondere auf die besuchten Webseiten, da auch die URL des Zielsystems gespeichert werden muss. Das gibt Aufschluss über die Inhalte der Internetkommunikation. Das wiederum soll nach der Regelung des § 113b Abs. 5 TKG nicht zulässig sein. Insofern ist das Gesetz also perplex. Kommt man dagegen zu dem Ergebnis, dass die Ermittlung einer Benutzerkennung Vorrang vor dem Verbot der Erhebung von Inhaltsdaten hat, dann müssten alle oben bezeichneten Daten gespeichert und beauskunftet werden, was in jedem Falle unverhältnismäßig wäre. Eine Generierung der Benutzerkennung aus den vorbezeichneten Nutzungsdaten führt nicht zu der vom Gesetz gewollten Nutzeridentifizierung, weil die Anfrage an den Telekommunikationsanbieter

lautet: „Wer ist Anschlussinhaber der um 0:00 Uhr genutzten IP-Adresse 160.20.20.183?“ Erst mit der Übergabe der gesamten Nutzungsdaten kann die Frage sinnvoll beantwortet werden.

Das ergibt sich auch aus folgender Kontrollüberlegung. Würde aus den Nutzungsdaten eines jeden Nutzers eine neue Benutzerkennung generiert, dann könnte die Antwort auf die Auskunftsfrage lauten:

Die IP-Adresse 160.20.20.83 wurde um 0:00 Uhr von folgenden Kunden genutzt:

Anschlusskennung	Benutzerkennung	Name
XYZ1	ABC1	A
XYZ2	ABC2	B
XYZ3	ABC3	C
…XYZn	ABCn	…N

Damit wäre die Anfrage beantwortet, ohne dass geklärt wäre, wer hinter der IP-Adresse 160.20.20.183 zum Zeitpunkt 0:00 Uhr stand. Hierbei ist insbesondere zu berücksichtigen, dass die Auskunft ca. 200 Benutzer umfassen kann.

Versteht man dagegen die Nutzungsdaten als Benutzerkennung, dann wäre bei der Modifikation der Anfrage: „Wer ist Anschlussinhaber der um 0:00 Uhr genutzten IP-Adresse 160.20.20.183 – wobei die IP-Adresse 80.245.153.130 und die URL: https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/PolizeilicherStaatsschutz/polizeilicherstaatsschutz_node.html. aufgerufen wurde?“ Dann wäre eine eindeutige Auskunft z.B. der Art: „ Anschlusskennung XYZ1, Benutzerkennung ABC1, Name A“ möglich, wobei die Benutzerkennung den Nutzungsdaten entspricht.

Im ersten Falle wäre die Auskunft unpräzise und führte zur Gefahr falscher Inanspruchnahme von Nicht-Verdächtigen/Nicht-Störern und die Benutzerkennung wäre überflüssig, da sie keinen anderen Aussagewert hätte als die Anschlusskennung. Im zweiten Falle wäre unter Verstoß gegen § 113b Abs. 5 TKG eine präzise Auskunft erteilt.

Denkbar wäre noch folgender Fall. Die Auskunftsfrage lautet wie am Anfang angegeben, es wird also nur nach dem Nutzer der externen IP 160.20.20.183 zum Zeitpunkt 0:00 Uhr gefragt und es werden alle dahinterstehenden Nutzer unter Angabe der Nutzungsdaten (=Benutzerkennung) angegeben. Das Ergebnis wird auch nicht durch die in § 113 Abs. 1 S. 3 Hs. 2 TKG vorgesehene automatisierte

Auswertung der Verkehrsdaten entschärft, denn im Ergebnis liefert auch die automatisierte Auswertung nur dann ein eindeutiges Ergebnis, wenn die Nutzungsdaten in die Auskunft mit einbezogen werden.

Ergebnis: Das Tatbestandsmerkmal „Benutzerkennung“ in § 113b Abs. 1 und 2 TKG führt zu einer verfassungswidrigen lückenlosen Aufzeichnung des Nutzungsverhaltens aller Internetnutzer. Insofern verstoßen die Vorschriften gegen Art. 10 Abs. 1 GG.

5.3.5.3 Die lückenlose Aufzeichnung der räumlichen Bewegung

Nach § 113 b Abs. 4 S. 2 TKG ist bei der mobilen Nutzung von Internet-Zugangsdiensten die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle zu speichern. Der Standardfall der mobilen Nutzung eines öffentlich zugänglichen Internet-Zugangsdienstes besteht in der Benutzung eines Smartphones. Dieses baut immer wieder neu eine Internet-Verbindung auf. Da jeder neue Verbindungsaufbau gespeichert wird, lässt sich damit sehr eindeutig die räumliche Bewegung des Trägers des Smartphones nachvollziehen.[59]

Die mobile Nutzung von Internet-Zugangsdiensten führt also dazu, dass die Bewegungen des Einzelnen sehr genau nachvollzogen werden können, wann hat jemand sich zu Hause aufgehalten, wann hat er seinen Arbeitsplatz aufgesucht, wie lange blieb er dort, wohin ging er danach, wann ist er wieder nach Hause zurückgekehrt? Die Eingriffsmöglichkeit ist tiefer als dies in dem Verfahren 1 BvR 256/08, das mit zum Urteil des Bundesverfassungsgerichts vom 2. März 2010 führte, nach dem damaligen Stand der Technik erkennbar war. Zu diesem Zeitpunkt waren die Möglichkeiten der Auswertung von Standortdaten zwar bereits bekannt, sie brauchten in der Entscheidung aber noch nicht weiter thematisiert werden. Lediglich in Rn. 237 der Entscheidung wird bei den Möglichkeiten der verfassungsrechtlichen Grenzen hinsichtlich des Umfangs der abzurufenden Daten auch die Möglichkeit des Ausschlusses der Auskunft über Standortdaten erwähnt.[60] Die systematische Nutzung der Standortdaten zur Entwicklung eines Persönlichkeitsprofils wurde zwar bereits als Möglichkeit gesehen, die Eingriffstiefe und Aussagekraft der Daten war zum damaligen Zeitpunkt aber noch nicht hinreichend deutlich. Für eine weitergehende Erörterung fehlte daher zum damaligen Zeitpunkt bereits die Notwendigkeit.

Ä[59] Vgl. DAV-Stellungnahme 25-15 aaO, S. 22

[60] BVerfG 02.03.2010 Rn. 237

Hierzu wurden inzwischen mehrere Studien gefertigt, die verdeutlichen, dass die Aufzeichnung von Standortdaten einen detaillierten Einblick in das Alltagsleben eines Grundrechtsträgers gibt.

Der Netzpolitiker der GRÜNEN, Malte Spitz, forderte von seinem Telekommunikationsanbieter die dort gespeicherten Standortdaten heraus und legt in ZEIT ONLINE mit einer interaktiven Grafik dar, dass anhand des Bewegungsprofils sein ganzer Tagesablauf transparent wurde. Die Grafik zeigt die Aufenthaltsorte des Politikers vom 01.09.2009 bis 31.03.2010. Sie verbindet die Aufenthaltsorte mit der Zahl und Dauer der getätigten Anrufe, ein- und ausgehender SMS als auch der Dauer der Internetverbindungen.[61]

Aufgrund der gewählten Darstellungstechnik, lässt sich der gesamte Aufenthaltsverlauf auch dynamisch, also in der Abfolge der Bewegungen, darstellen. Es ist ein Profil des Lebens des Herrn Spitz.

Ein ebenso eindrucksvolles Bewegungsprofil erstellte der Schweizer Nationalrat Balthasar Glättli aufgrund seiner in der Schweiz gesetzlich erhobenen Standortdaten für den Zeitraum 14.01. bis 14.07.2013. Bei den Kommunikationsdaten werden neben den vorerwähnten Daten auch die Tweets, Facebook-Posts und die Kommunikationspartner angezeigt. Zugleich zeigt die Liste das Netzwerk der Kommunikationspartner von Herrn Glättli.[62]

Aufgrund dieser Beispiele ist die Aufzeichnung der Standortdaten, verbunden mit den anderen Kommunikationsdaten, mit einer ständigen Observation des betreffenden Telekommunikationsnutzers nicht nur vergleichbar, sondern dürfte deren Eingriffsintensität noch übertreffen, denn es lässt sich, anders als bei einer Observation, auch der jeweilige Telekommunikationspartner feststellen.

Die lückenlose Aufzeichnung der Bewegungen aller Nutzer von mobilen Telekommunikationsgeräten ist unverhältnismäßig.

5.3.5.4. Der Maßstab der gebotenen Einschränkungen des betroffenen Personenkreises

Der europäische Gerichtshof hat in seinem Urteil vom 8. April 2014 bei der Verhältnismäßigkeitsprüfung der Speicherung von Telekommunikationsdaten insbesondere darauf abgestellt, dass der betroffene Personenkreis nicht eingegrenzt ist, zumal die betroffenen Personen in der Regel nicht einmal eine mittelbare Beziehung zu strafbaren Handlungen haben.[63] So ist es auch bei der hier angegriffenen Regelung, indem die Daten aller Nutzer von

[61] http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten
[62] https://www.digitale-gesellschaft.ch/vds.html
[63] EUGH 08.04.2014, Rn. 58

Kommunikationsmitteln erhoben und gespeichert werden, ohne dass irgend ein Bezug dieser Personen zu Straftaten besteht.

An der Richtlinie 2006/24 kritisiert der EuGH, sie betreffe „in umfassender Weise alle Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich jedoch die Personen, deren Daten auf Vorrat gespeichert werden, auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte.[64]

§ 113b TKG gewährleistet nicht, dass die Vorratsdaten nur solcher Personen gespeichert und abgerufen werden können, die der Beteiligung an einer Straftat verdächtig sind oder damit in sonstiger Weise in Verbindung gebracht werden können. Vielmehr sieht er eine massenhafte Erfassung sämtlicher Nutzer der entsprechenden Telekommunikationsdienste und damit nahezu der gesamten Bevölkerung vor. Fast alle betroffenen Nutzer haben keinerlei Anlass für eine vorsorgliche Aufzeichnung ihrer Kommunikationsdaten gegeben. Eine so umfassende Vorratsdatenspeicherung ist ein Fremdkörper in unserer freiheitlichen Rechtsordnung, die einen Grundrechtseingriff in dieser Streubreite nie gekannt hat. Eine derart flächendeckende Sammlung von Daten über das alltägliche Verhalten und Leben von Millionen von Bürgern greift unverhältnismäßig tief in die Grundrechte der unterschiedslos betroffenen Bürger ein.

Das Bundesjustizministerium hat das Urteil ursprünglich in diesem Sinne verstanden. Der Bundesjustizminister erklärte öffentlich: „Eine solche Speicherung verstößt gegen die Grundrechte. Das hat der Europäische Gerichtshof eindeutig festgestellt.“[65] Weiter erklärte er: „Der Europäische Gerichtshof hat gesagt, dass die Vorratsdatenspeicherung gegen die Grundrechte verstößt.“[66] Im weiteren Verlauf prüfte die Bundesregierung mit Blick auf das Urteil eine Datenspeicherung nur aus konkretem Anlass, beispielsweise bei zeitlich eingrenzbaren Großereignissen mit Gefahrenpotenzial, Hinweisen auf regional besonders auffällige Gefährdungslagen oder von Islamisten bevorzugte Kommunikationskanäle.[67]

---

[64] EUGH 08.04.2014, Rn. 58

[65] ZEIT vom 12.01.2015, http://www.zeit.de/politik/deutschland/2015-01/maas-anti-terror-gesetze.

[66] Deutschlandfunk vom 12.01.2015, http://www.deutschlandfunk.de/bundesjustizminister-maas-vorratsdatenspeicherung.694.de.html?dram:article_id=308417 .

[67] Rheinische Post, Koalition lotet "kleine" Vorratsdatenspeicherung aus (15.03.2015), http://www.rp-online.de/politik/deutschland/eugh-urteil-koalition-lotet-kleine-vorratsdatenspeicherung-aus-aid-1.4940505 .

Auch der Wissenschaftliche Dienst des Bundestags geht davon aus, dass der EuGH Einschränkungen hinsichtlich des von der Speicherung betroffenen Personenkreises fordert.[68]

5.3.5.5. Der Maßstab der raum- und zeitbezogenen Einschränkungen

Der europäische Gerichtshof hat in seinem Urteil vom 8. April 2014 bei der Verhältnismäßigkeitsprüfung ferner darauf abgestellt, dass die von der Richtlinie 2006/24 vorgesehene Vorratsspeicherung keine räumliche und keine zeitliche Beschränkung vorsieht. Dasselbe gilt für die hier angegriffene Regelung. Auch sie sieht, da bei Erhebung und Speicherung der Daten noch gar nicht feststeht, welche Straftaten ermittelt werden sollen, keine räumliche und keine zeitliche Beschränkung der Vorratsspeicherung vor.

An der Richtlinie 2006/24 kritisiert der EuGH, sie solle „zwar zur Bekämpfung schwerer Kriminalität beitragen, verlangt aber keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit; insbesondere beschränkt sie die Vorratsspeicherung weder auf die Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets und/oder eines bestimmten Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten.[69]

Die Speicherung nur solcher Telekommunikationsdaten kann also verhältnismäßig sein, die einen hinreichenden zeitlichen, örtlichen oder personellen Zusammenhang mit einer Gefährdung der öffentlichen Sicherheit aufweisen. Dies schließt eine anlasslose Vorratsdatenspeicherung aus.

Bei Zugrundelegung des vorstehenden Maßstabes ist die Regelung auch aus diesem Grunde unverhältnismäßig.

5.3.5.6. Der Schutz der Vertrauensberufe

Der EUGH stellt bei der Prüfung, ob die Richtlinie 2006/24/EG die Vorratsdatenspeicherung auf das absolut Notwendige beschränkt, als Kritik fest, dass keinerlei Ausnahme für diejenigen Personen vorgesehen ist, deren

[68] Derksen, aaO, S. 14

[69] EUGH 8.4.2014, Rn. 57ff.

Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen.

Auch das angegriffene Gesetz sieht auf der Ebene der Datenerhebung eine solche Ausnahme nicht vor. Eine solche wäre technisch möglich, denn für die Verbindungen gem. § 99 Abs. 2 TKG ist diese Ausnahme in § 113b Abs. 6 TKG vorgesehen. Für die einem besonderen Berufsgeheimnis unterliegenden Berufe kann als Schutz nur ein Beweisverwertungsverbot greifen, was zunächst zur Auswertung der Verbindungsdaten führt.[70] Auch diese Zugriffsmöglichkeit ist in der derzeit bekannten Regelung des § 100g Abs. 4 StPO noch gestuft: Ist bekannt, dass der Anschlussinhaber ein Berufsgeheimnisträger ist, so dürfen die (zunächst auf Vorrat gespeicherten) Daten nicht erhoben werden, wenn die Erhebung voraussichtlich Erkenntnisse erbringen würde, über die der Berufsgeheimnisträger das Zeugnis verweigern darf. Ist die Ermittlungsmaßnahme gegen eine nicht zur Zeugnisverweigerung berechtigte Person gerichtet und werden dadurch von dem Zeugnisverweigerungsberechtigten Erkenntnisse erlangt, über die dieser das Zeugnis verweigern darf, so sind die Daten zu löschen und dürfen nicht verwertet werden. In beiden Fällen wird zunächst erhoben, solange nicht bekannt ist, ob einer der beteiligten Kommunikationsteilnehmer zur Zeugnisverweigerung berechtigt ist. Völlig zu Recht weist der Deutsche Anwaltsverein in seiner Stellungnahme darauf hin, dass einmal erhobenen Daten zwar wieder gelöscht werden können, die Gefahr aber nicht zu leugnen ist, dass sie auf die ein oder andere Art ihren Eingang ins Verfahren finden.[71] So weist die Wirtschaftsprüferkammer in ihrer Stellungnahme zum Gesetzentwurf darauf hin, dass auch bei Beweisverwertungsverboten Folge -Erkenntnisse der Ermittler in einem nachfolgenden Strafverfahren häufig verwertbar seien, was aus der eingeschränkten Geltung der „Fruit of the poisonous tree doctrine“ im deutschen Strafprozessrecht folge.[72] Die Bundesrechtsanwaltskammer verschärft diese Kritik indem sie ausführt, dass die Verletzung der grundsätzlich geschützten Kommunikationssphäre zwischen Arzt/Rechtsanwalt einerseits und Patient/Mandant andererseits eine entscheidende Ursache dafür setzen könne, dass es zu staatlichen Sanktionen gegenüber demjenigen, „der im Vertrauen auf die absolut geschützte Kommunikation mit seinem Arzt oder Rechtsanwalt elektronisch kommuniziert habe.“ Das Bewusstsein von dieser nicht auszuschließenden Möglichkeit stelle eine die Kommunikation behindernde Tatsache und damit eine – gravierende – Verletzung des Schutzbereichs aus Art.

[70] Vgl. zur Kritik statt vieler: Umlaufentschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9. Juni 2015, https://www.datenschutz-mv.de/datenschutz/themen/beschlue/ent_vorrat.html, DAV Stellungnahme, aaO, S. 12ff.

[71] DAV, Stellungnahme, aaO, S. 14

[72] Wirtschaftsprüferkammer, Stellungnahme v. 26.06.2015, S. 6 http://www.wpk.de/uploads/tx_news/WPK-Stellungnahme_26-06-2015.pdf

10 Abs. 1 GG dar. Bei den betroffenen Kommunikationspartnern (Patienten/Mandanten, Informanten) entstehe nicht nur – wie bei der Allgemeinheit – das Gefühl, dass ihr Privatleben Gegenstand einer ständigen Überwachung sei. Vielmehr gelte dies auch für einen besonders sensiblen und folglich besonders schutzwürdigen Bereich des Privatlebens (Gesundheit bzw. Verhältnis Anwalt/Mandant).[73]

Ein überzeugender Grund für die unterschiedliche Behandlung von Kommunikationsverbindungen im Sinne von § 99 Abs. 2 TKG und solchen zwischen Mandanten und den klassischen Berufsgeheimnisträgern wie Ärzten, Rechtsanwälten, Steuerberatern, Wirtschaftsprüfern u.a. ist nicht vorhanden. Der Regierungsentwurf führt dazu aus, es sei nicht möglich, die Berufsgeheimnisträger in ihrer Gesamtheit schon von der Speicherung ihrer Verkehrsdaten auszunehmen. Dazu müssten sämtlichen Telekommunikationsanbietern, von denen es in Deutschland ca. 1000 gebe, mitgeteilt werden, wer Berufsgeheimnisträger im Sinne des §§ 53 StPO sei; diese Liste müsse dauernd aktualisiert werden. Ihre Erstellung, Übermittlung und Aktualisierung berge auch im Falle des Einverständnisses der Betroffenen ein erhebliches Missbrauchsrisiko. Hinzu komme, dass Berufsgeheimnisträger in vielen Fällen nicht über statische, sondern über dynamische IP-Adressen verfügten, so dass eine Liste der verwendeten Adressen gar nicht erstellt werden könne. Der bessere Schutz ergebe sich daher bei einer Regelung, die die Verwendung der gespeicherten Daten ausschließe. Dieser Schutzmechanismus habe sich in der StPO auch an anderer Stelle bewährt.[74]

Das kann beim Vergleich der ansonsten infrage stehenden Datenmengen nicht überzeugen. Wenn schon ca. 40 Millionen Bankkonten von den mehr als 1000 deutschen Bank- und Finanzinstituten in einer Schattendatei für Abfragen durch die BaFin und das Bundeszentralamt für Steuern ohne Probleme vorgehalten werden können[75], wenn millionen- und milliardenfach Verbindungs- und Standortdaten gespeichert werden können[76], dann soll dies plötzlich bei den Telekommunikationsbestandsdaten der Berufsgeheimnisträger nicht möglich sein? Selbstverständlich ist es technisch ohne großen Aufwand möglich, eine Sperrdatei mit den Kommunikationsnummern der Berufsgeheimnisträger bei den Telekommunikationsanbietern vorrätig zu halten und diese täglich zu aktualisieren. Dies gilt im Übrigen auch für dynamische IP-Adressen der

[73] Vgl. Bundesrechtsanwaltskammer Stellungnahme Nr. 32/2015, Seite 13, http://www.brak.de/zur-rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2015/september/stellungnahme-der-brak-2015-32.pdf mwN

[74] Gesetzentwurf der Bundesregierung, S. 37

[75] Vgl. unten 5.3.5.7.4

[76] Vgl. oben 5.3.5.2.

Berufsgeheimnisträger, denn deren Anschlüsse können durch Ihren Provider selbst von der Erhebungspflicht für die Vorratsdatenspeicherung unmittelbar ausgenommen werden.

Die in der Begründung des Regierungsentwurfs angegebene hohe Zahl der Berufsgeheimnisträger im Vergleich zu den Stellen nach § 99 Abs. 2 TKG ist kein überzeugendes Vergleichskriterium. Zu Recht weist die Wirtschaftsprüferkammer in ihrer Stellungnahme darauf hin, dass auch ein Steuerstraftäter, der sich vertrauensvoll an einen Berufsgeheimnisträger als seinen Berater wende, um seine steuerrechtlichen Handlungsoptionen in Erfahrung zu bringen, seine Situation als persönliche Notlage empfinden könne.[77] Wenn aber die Notlage des Betroffenen das Vergleichskriterium für den Vertraulichkeitsschutz darstellt, dann ist die Unterscheidung zwischen den Stellen nach § 99 Abs. 2 TKG und den Berufsgeheimnisträgern sachlich nicht gerechtfertigt.

Inzwischen hat der Bundesgesetzgeber das Argument mangelnder Praktikabilität bei der Nicht-Erfassung von Personen, die zur Zeugnisverweigerung nach § 53 StPO berechtigt sind – oder zumindest der klassischen Berufsgeheimnisträger – widerlegt. Mit dem Art. 1 des Gesetzes zur Modernisierung des Besteuerungsverfahrens vom 18. Juli 2016 (BGBl. I 2016, S. 1679ff.) wurde die neue Vorschrift des § 80 a in die Abgabenordnung eingefügt. Die Vorschrift regelt, dass steuerlich Bevollmächtigte ihre Vollmachtsdaten unter Beachtung bestimmter Formvorschriften an die Landesfinanzbehörden übermitteln können. Die Regelung der Überprüfung, ob der Bevollmächtigte zum Personenkreis des § 3 Steuerberatungsgesetz gehört, hat der Gesetzgeber in Abs. 2 der Vorschrift geregelt.

Abs. 2 der Vorschrift hat folgenden Wortlaut:

„*Werden die Vollmachtsdaten von einem Bevollmächtigten, der nach § 3 des Steuerberatungsgesetzes zur geschäftsmäßigen Hilfeleistung in Steuersachen befugt ist, nach Maßgabe des Absatzes 1 übermittelt, so wird eine Bevollmächtigung im mitgeteilten Umfang vermutet, wenn die zuständige Kammer sicherstellt, dass Vollmachtsdaten nur von den Bevollmächtigten übermittelt werden, die zur geschäftsmäßigen Hilfeleistung in Steuersachen befugt sind. Die für den Bevollmächtigten zuständige Kammer hat den Landesfinanzbehörden in diesem Fall auch den Wegfall einer Zulassung unverzüglich nach amtlich vorgeschriebenem Datensatz mitzuteilen.*“

[77] WPK, Stellungnahme, aaO, S. 5

Hier ist also ist ein elektronisches Kontrollverfahren möglich, das die Mitgliedschaft zu einem regulierten (und zur Zeugnisverweigerung berechtigten) Beruf nachweist.

Der Gesetzgeber hat mit dieser Vorschrift also ein praktikables Verfahren eröffnet, um auf elektronischem Wege die Zugehörigkeit zum Personenkreis des § 3 des Steuerberatungsgesetzes festzustellen. Zu diesem Personenkreis gehören:

> Steuerberater, Steuerbevollmächtigte, Rechtsanwälte, niedergelassene europäische Rechtsanwälte, Wirtschaftsprüfer und vereidigte Buchprüfer,
>
> Partnerschaftsgesellschaften, deren Partner ausschließlich die in Nummer 1 genannten Personen sind,
>
> Steuerberatungsgesellschaften, Rechtsanwaltsgesellschaften, Wirtschaftsprüfungsgesellschaften und Buchprüfungsgesellschaften.

Der Nachweis der Zugehörigkeit zu diesem Personenkreis wird durch deren Berufskammern sichergestellt. Bei den Rechtsanwälten, niedergelassenen europäischen Rechtsanwälten, Steuerberatern und Steuerbevollmächtigten sind das lokale Berufskammern, bei den Wirtschaftsprüfern und vereidigten Buchprüfern ist es die Wirtschaftsprüferkammer als Bundeskammer. Diese Berufsangehörigen stellen bereits zahlenmäßig einen großen Teil der gemäß § 53 Abs. 1 Nr. 3 StPO zur Zeugnisverweigerung Berechtigten dar. Das vom Gesetzgeber in § 80 a AO eingeführte Verfahren zur Gewährleistung der Berechtigung der Bevollmächtigten ließe sich auch auf die gemäß § 53 StPO zur Zeugnisverweigerung berechtigten Personen, die in nicht verkammerten Berufen tätig sind, übertragen. Bei Journalisten ist etwa an den Presseausweis zu denken, bei den Mitgliedern der Gesetzgebungsorgane ist ebenfalls eine ausreichende Verwaltungsstruktur vorhanden, mit der festgestellt werden kann, wer zu diesem Personenkreis gehört.

Es bleibt festzuhalten, dass die im Gesetzgebungsverfahren geltend gemachten Schwierigkeiten bei der Erfassung der Zeugnisverweigerungsberechtigten offenbar überwindbar sind. Der Ausschluss der nach § 53 StPO zur Zeugnisverweigerung berechtigten Personen ist unverhältnismäßig und durch in der Sache liegende Gründe nicht gerechtfertigt. Höchst vorsorglich wird in diesem Zusammenhang gerügt, dass der allgemeine Gleichheitssatz verletzt ist, weil der angegebene sachliche Grund für die unterschiedliche Behandlung der nach § 53 StPO zur Zeugnisverweigerung Berechtigten und der Stellen nach § 99 Abs. 2 TKG offensichtlich nicht vorhanden ist.

5.3.5.7. Additive Grundrechtseingriffe (Überwachungsgesamtrechnung)

Neben der Überprüfung der Regelung am Maßstab der Verhältnismäßigkeit im Einzelnen ist wegen der Schwere des Eingriffs auch zu überprüfen, ob die Gesamtheit der staatlichen Überwachungsmaßnahmen ein Maß erreicht hat, das verfassungsrechtlich nicht mehr erträglich ist. Das Bundesverfassungsgericht hat die Freiheit des Bürgers von totaler Überwachung bei der Ausübung seiner Freiheitsrechte zur Verfassungsidentität der Bundesrepublik gezählt.[78]

Diese vielbeachtete und zitierte Äußerung des Gerichts ist der Obersatz für die nachstehenden Überlegungen:

„*Umgekehrt darf die Speicherung der Telekommunikationsverkehrsdaten nicht als Schritt hin zu einer Gesetzgebung verstanden werden, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte. Eine solche Gesetzgebung wäre, unabhängig von der Gestaltung der Verwendungsregelungen, von vornherein mit der Verfassung unvereinbar. Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt vielmehr voraus, dass diese eine Ausnahme bleibt. Sie darf auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen. Maßgeblich für die Rechtfertigungsfähigkeit einer solchen Speicherung ist deshalb insbesondere, dass sie nicht direkt durch staatliche Stellen erfolgt, dass sie nicht auch die Kommunikationsinhalte erfasst und dass auch die Speicherung der von ihren Kunden aufgerufenen Internetseiten durch kommerzielle Diensteanbieter grundsätzlich untersagt ist. Die Einführung der Telekommunikationsverkehrsdatenspeicherung kann damit nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen, sondern zwingt den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung. Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland (vgl. zum grundgesetzlichen Identitätsvorbehalt* BVerfG, Urteil des Zweiten Senats vom 30. Juni 2009 - 2 BvE 2/08 u.a. -, juris, Rn. 240), *für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss. Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer.*“

[78] BVerfG 02.03.2010, Rn. 218;

Demzufolge ist zunächst festzustellen, dass die Rechtfertigungsvoraussetzung „Nichterfassung der Kommunikationsinhalte und der aufgerufenen Internetseiten“ nicht erfüllt ist, wie oben unter 5.3.5.2 für den Fall der Nutzung des CNAT-Verfahrens dargelegt wurde.

5.3.5.7.1. Gesetzliche Neuregelungen nach dem Urteil des Bundesverfassungsgerichts vom 2. März 2010

Der Gesetzgeber hat eine irgendwie geartete Bestandsaufnahme der vorhandenen Gesetze, die zu Datenerhebungen, -Speicherungen und -Verarbeitungen führen, nicht vorgenommen. Auch von wissenschaftlicher Seite hat es keine weitere Bestandsaufnahme der vorhandenen Überwachungsgesetze bzw. -maßnahmen gegeben. Seit dem Urteil des Bundesverfassungsgerichts vom 2. März 2010 sind nach Auskunft des wissenschaftlichen Dienstes des Deutschen Bundestages die nachfolgenden Gesetze, die auch Datenerhebungen vorsehen, beschlossen worden:

- Gesetz zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatenangehörige (12. April 2011)
- Gesetz zur Verbesserung des Austauschs von strafregisterrechtlichen Daten zwischen den Mitgliedstaaten der Europäischen Union und zur Änderung registerrechtlicher Vorschriften (15. Dezember 2011)
- Gesetz zur Errichtung eines Nationalen Waffenregisters (25. Juni 2012)
- Gesetz zur Verbesserung der Bekämpfung des Rechtsextremismus (20. August 2012)
- Gesetz zur Änderung des AZR-Gesetzes (20. Dezember 2012)
- Gesetz zur Regelung des Assistenzpflegebedarfs in stationären Vorsorge- oder Rehabilitationseinrichtungen (20. Dezember 2012)
- Gesetz zum Schutz des Erbrechts und der Verfahrensbeteiligungsrechte nichtehelicher und einzeladoptierter Kinder im Nachlassverfahren (21. März 2013)
- Gesetz zur Fortentwicklung des Meldewesens (3. Mai 2013)
- Gesetz zur Änderung des Güterkraftverkehrsgesetzes und anderer Gesetze vom (17. Juni 2013)
- Gesetz zur Errichtung einer Schiffsunfalldatenbank und zur Änderung des Seefischereigesetzes (7. August 2013)
- Gesetz zur Anpassung des Luftverkehrsrechts (7. August 2013)
- Gesetz zum Ausbau der Hilfen für Schwangere und zur Regelung der vertraulichen Geburt (28. August 2013)
- Viertes Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze (28. August 2013)

- Gesetz zur Verbesserung der Rechte von international Schutzberechtigten und ausländischen Arbeitnehmern (14. Oktober 2013)

- Gesetz zur Änderung des Straßenverkehrsgesetzes, der Gewerbeordnung und des Bundeszentralregistergesetzes (28. November 2014)

- Gesetz zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch (21. Januar 2015)

- Gesetz zur Einführung einer Infrastrukturabgabe für die Benutzung von Bundesfernstraßen (8. Juni 2015)

- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (12.06.2015)

- Asylverfahrensbeschleunigungsgesetz (20. Oktober 2015)

- Steueränderungsgesetz 2015 (2. November 2015)

- Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (10. Dezember 2015)

- Gesetz zur Bekämpfung von Doping im Sport (10. Dezember 2015)

- Gesetz zum automatischen Austausch von Informationen über Finanzkonten in Steuersachen und zur Änderung weiterer Gesetze vom 21. Dezember 2015

- Gesetz zur Verbesserung der Registrierung und des Datenaustausches zu aufenthalts- und asylrechtlichen Zwecken (2. Februar 2016)

- Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts (17. Februar 2016)

- Gesetz zur Änderung des Hochschulstatistikgesetzes (2. März 2016)

- Gesetz zur Einführung beschleunigter Asylverfahren (11. März 2016)

Die Aufstellung des Wissenschaftlichen Dienstes des Deutschen Bundestages endet mit dem Gesetzgebungsstand vom 15.03.2016. Danach, und in der Aufstellung ausgelassen, sind folgende Gesetze hervorzuheben:

- Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes (17.11.2015

- Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus (26.07.2016)

- Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BT-Drucksache 18/9041)

Diejenigen Gesetzen, die nicht unmittelbar Überwachungscharakter haben, ordnen erweiterte Datenerhebungsbefugnisse und vor allem die Einrichtung von zentralen, bundeseinheitlichen Datenbanken an, deren Daten in der Regel auch für Ermittlungszwecke in Strafverfahren oder Zwecke der Gefahrenabwehr zur Verfügung stehen.

Das Gesetz zur Verbesserung der Bekämpfung des Rechtsextremismus führt die Errichtung einer zentralen Datei der Polizeibehörden des Bundes und der Länder sowie der Verfassungsschutzbehörden und des Militärischen Abschirmdienstes mit einem weitgehenden Katalog von personenbezogenen Daten bis hin zur Berufsausbildung ein, vgl. § 3 Rechtsextremismus-Datei-Gesetz.

Die Neufassung des Meldegesetzes führt eine regelmäßige Übermittlung der Meldedaten an Religionsgemeinschaften und die öffentlich-rechtlichen Sendeanstalten ein.

Das Gesetz zur Anpassung des Luftverkehrsrechts führt eine zentrale Flugbegleiterdatenbank ein.

Das Gesetz zur Einführung einer Infrastrukturabgabe ermöglicht die Vor-Ort-Überwachung des Straßenverkehrs auf den mautpflichtigen Straßen u.a. durch Fertigung eines Fotos des überwachten Fahrzeuges.

Das Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus v. 26.07.2016 ermöglicht die Errichtung gemeinsamer Datenbanken mit Nachrichtendiensten fremder Staaten, den Einsatz verdeckter Ermittler durch die Bundespolizei, § 28 Abs. 2 Nr. 4 BPolG, und die Identifikationspflicht bei Besitz einer Prepaid-Telefonkarte oder Einrichtung eines Postfaches der elektronischen Post, vgl. § 111 TKG.

Das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl. I 2015, S. 1938) schreibt die Einrichtung zentraler Datenbanken der Verfassungsschutzämter des Bundes und der Länder vor und ermöglicht den automatisierten Datenabruf durch diese Ämter und den Militärischen Abschirmdienst. Im Aufgabenbereich des Bundesnachrichtendienstes wurde § 5 Abs. 1 Satz 3 G 10 um Nr. 8 ergänzt, die als weiteres Überwachungsziel die rechtzeitige Erkennung der Gefahr „des internationalen kriminellen, terroristischen oder staatlichen Angriffs mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland“ definiert .

Rechtsfolge dieser Ausweitung ist die Möglichkeit, anlasslos den deutsch-internationalen Telekommunikationsverkehr nach Suchbegriffen zu filtern. Für die Zwecke dieser Verfassungsbeschwerde wird dabei außer Acht gelassen, dass für die Datenströme im Internet technisch nicht mehr erkennbar ist, ob es sich um Inlands- oder Auslandsdaten handelt.

Mit der Änderung des BND-Gesetzes durch das Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes, hier noch zitiert nach der BT-Drucksache 18/9041, darf der Dienst im Inland (Auslands-)Telekommunikation überwachen, wobei diese Befugnis ausgeweitet wird auf den Zweck,

„*frühzeitig Gefahren für die innere oder äußere Sicherheit der Bundesrepublik Deutschland erkennen und diesen begegnen zu können*“, vgl. § 6 Abs. 1 BND-Gesetz;

ferner darf der BND Verbindungsdaten sechs Monate lang speichern und sie mit ausländischen Diensten teilen, §§ 6 Abs. 6 und 13f. BND-Gesetz, wobei nach § 14 der Vorschrift auch der automatisierte Abruf durch ausländische Dienste möglich ist.

Die Beschränkung auf 20% der Leitungskapazität ist entfallen.

Der Sonderberichterstatter der UN in Bezug auf das Recht auf Privatheit kritisierte in seinem aktuellen Jahresbericht [79]

die Überwachungsgründe als zu unbestimmt,

die Differenzierung zwischen Auslands- und Inlandsüberwachung als verfassungs- und völkerrechtswidrig,

die Überwachung selbst als Massenüberwachung[80].

Festzuhalten bleibt, dass neben der Unbestimmtheit der Eingriffsgrundlage jegliche mengenmäßige Beschränkung der überwachten Verbindungen entfallen ist und eine Kombination von Zugriff auf Kommunikationsinhalte und Verbindungsdatenerhebung vorliegt, eine Kombination also, die das Bundesverfassungsgericht als nicht rechtfertigungsfähig bezeichnet hat.[81]

Zu erwähnen sind ferner die Änderungen der Polizeigesetze und der Versammlungsgesetze der Bundesländer, die vielfältige neue Datenerhebungsermächtigungen einschließlich der Ermächtigung zur Fertigung von Videoaufzeichnungen bei Versammlungen unter freiem Himmel enthalten.

5.3.5.7.2. Tatsächliche Ausweitung von Überwachungsmaßnahmen

in tatsächlicher Hinsicht ist in vielen Feldern festzustellen, dass elektronische Beauskunftungen und Überwachungsmaßnahmen in erheblichem Rahmen zugenommen haben

[79] http://www.un.org/ga/search/view_doc.asp?symbol=A/71/368
[80] vgl. S. 21 des Berichts, aaO
[81] FN 78

5.3.5.7.3. Funkzellenabfragen nach § 100g Abs. 3 StPO (Abs. 2 S. 2 a.F.)

Es gibt keine bundeseinheitliche Statistik über die Funkzellenabfragen sowohl betreffend die Anzahl der Abfragen selbst als auch die Anzahl der bei jeder Abfrage gewonnenen Daten. Aus parlamentarischen Anfragen im Landtag von Schleswig-Holstein, im Berliner Abgeordnetenhaus und im Landtag von Nordrhein-Westfalen sowie aus den Berichten von Datenschutzbeauftragten geht hervor, dass mit den Funkzellenabfragen immense Datenmengen bewegt werden. Der Berliner Landesbeauftragte für den Datenschutz und Informationsfreiheit stellt bereits im Jahresbericht 2012 fest:

„*Offensichtlich sind Funkzellenabfragen in vielen Deliktsbereichen entgegen der gesetzlichen Vorgabe zum alltäglichen Ermittlungsinstrument geworden. Aufgrund der Eingriffstiefe und Streubreite darf ihr Einsatz jedoch nicht zur Regel werden. Die stärkere Begrenzung der Durchführung solcher Maßnahmen ist durch den Gesetzgeber und die Strafverfolgungsbehörden sicherzustellen. Die Staatsanwaltschaft unterliegt auch dann der Kontrolle durch den Berliner Beauftragten für Datenschutz und Informationsfreiheit, wenn die von ihr beantragten Maßnahmen unter Richtervorbehalt stehen.*“ [82]

Im Jahre 2013 wurden in Berlin nach Auskunft des Senates an das Abgeordnetenhaus in 305 Verfahren Funkzellenabfragen durchgeführt, bei denen knapp 50 Millionen Datensätze anfielen. [83]

Nach Auskunft der nordrhein-westfälischen Landesregierung betrug die Anzahl der Funkzellenabfrage dort:

2011: 2674

2012: 3545

2013: 4145 . [84]

Für Mecklenburg-Vorpommern teilte die Landesregierung folgende Zahlen für nicht individualisierte Funkzellenabfragen mit:

2011: 62

2012: 89

[82] Berliner Beauftragter für Datenschutz und Informationsfreiheit, Bericht 2012, S. 27
https://datenschutz-berlin.de/content/veroeffentlichungen/jahresberichte/bericht-12
[83] https://netzpolitik.org/2015/funkzellenabfrage-in-berlin-vielleicht-werden-sie-gerade-ueberwacht/
[84] Landtag Nordrhein-Westfalen – Drucksache 16/6051, Seite 7
https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMD16-6051.pdf

2013: 209

2014: 260

2015 568 .[85]

Die sächsische Landesregierung berichtete auf eine kleine Anfrage, dass im Zeitraum vom 1. Januar 2013 bis 12. Januar 2015 654 Funkzellenabfragen realisiert wurden.

Für das Saarland gab die Landesregierung an, dass dort Im Zeitraum vom 01.09.2013 bis 31.08.2014 in insgesamt 175 Verfahren nicht individualisierte Funkzellenabfrage vorgenommen worden. Hierbei wurden 7.459.326 Datensätze über Verbindungsdaten erhoben, durchschnittlich also 42.624 Datensätze pro Verfahren. Dabei entspricht ein Datensatz einem Kommunikationsvorgang.[86]

Dabei wurden Verkehrsdaten aus 21.000 Funkzellen und von etwa 500 Tatorten erhoben. Die Anzahl der ermittelten Datensätze wurde nicht angegeben, es wurde lediglich angegeben, dass 23.000 Dateien mit Verkehrsdaten durch die Netzbetreiber übermittelt wurden.[87]

Für Schleswig-Holstein gab die Landesregierung folgende Zahlen über vorgenommene nicht-individualisierte Funkzellenabfragen an:

2013: 441

2014: 569 .[88]

andere Landesregierungen haben mangels vorhandener Erhebungen keine quantitativen Auskünfte geben können.[89]

5.3.5.7.4. Finanzdaten

Geldinstitute haben bestimmte Kontenbestandsdaten, die bei Ihnen bereits vorhanden sind, separat zu speichern und für ein automatisiertes Abrufverfahren durch die BaFin und das Bundeszentralamt für Steuern zum Abruf bereitzuhalten. Es werden also die Daten aller in Deutschland geführten Konten auf Vorrat

[85] Landtag Mecklenburg-Vorpommern – Drucksache 6/5468, Seite 2
https://kleineanfragen.de/mecklenburg-vorpommern/6/5468-funkzellenabfragen
[86] Vgl. Landtag des Saarlandes Drucksache 15/1197 (15/623), S. 2 und die Tabelle in der Anlage
https://www.landtag-saar.de/Drucksache/Aw15_1197.pdf
[87] Antwort der sächsischen Landesregierung zur Drucksache 6/772, S 3
https://kleineanfragen.de/sachsen/6/772-funkzellenabfragen-in-sachsen-2013-2015 geh schlafen
[88] Schleswig-Holsteinische Landtag – Drucksache 18/2838, S. 1
http://www.landtag.ltsh.de/infothek/wahl18/drucks/2800/drucksache-18-2838.pdf ; vgl. auch: Constanze Kurtz, erneut steigende Zahl von Funkzellenabfragen
https://netzpolitik.org/2015/erneut-steigende-zahl-von-funkzellenabfragen/
[89] vergleiche die Anfragen bei: https://kleineanfragen.de/search?page=2&q=funkzellenabfrag

gespeichert und für einen Abruf bereitgehalten, von dem die Bank nichts erfährt, im Einzelfall auch nicht der Kontoinhaber. Nach Auffassung des Bundeszentralamtes für Steuern ist der Kontenabruf kein Verwaltungsakt, sondern ein Realakt. Nach dieser Auffassung entspricht der Kontenabruf einer elektronischen Einnahme des Augenscheins und bedarf für seine Wirksamkeit nicht der Bekanntgabe. Er ist auch nicht selbständig anfechtbar. Seine Rechtmäßigkeit kann lediglich im Rahmen der Überprüfung des Steuerbescheides oder eines anderen Verwaltungsaktes, zu dessen Vorbereitung der Kontenabruf vorgenommen wurde oder isoliert im Wege der Leistungs- oder (Fortsetzungs-) Feststellungsklage überprüft werden.[90]

Die Bestandsdaten von Konten bei Geldinstituten können nach der Vorschrift der §§ 24 c KWG und 93 Abs. 7 und 8 AO abgefragt werden.

Nach § 24 c KWG sind Kreditinstitute, Kapitalanlagegesellschaften und Zahlungs-Institute verpflichtet, Kontostammdaten aller Kunden in einer Datei zu erfassen. Hierzu gehören Kontonummer, Name und Geburtsdatum der Kontoinhaber und Verfügungsberechtigten sowie das Errichtungs- und Schließungsdatum. Abrufberechtigt ist die BaFin im Rahmen ihrer Aufsichtsaufgaben. Die BaFin erteilt über diese Daten auf Ersuchen Auskunft gegenüber den Aufsichtsbehörden gemäß § 9 Abs. 1 S. 4 Nr. 2 KWG, den für die Leistung der internationalen Rechtshilfe in Strafsachen zuständigen Behörden, den für die Verfolgung und Ahndung von Straftaten zuständigen Behörden oder Gerichten sowie der für die Beschränkungen des Kapital-und Zahlungsverkehrs nach dem AWG zuständigen Behörde.

Das Ausmaß der Kontenabfragen nach § 24c KWG nimmt stetig zu. Im Jahr 2010 gab es bundesweit 105.615 Abfragen, bis zum Jahr 2015 stieg diese Zahl auf 137.779 Abfragen an.[91]

Die überwiegende Anzahl der Abfragen entfiel auf Finanzbehörden, Polizeibehörden, Staatsanwaltschaften und Zollbehörden. Auf die Finanzbehörden entfielen 2010 13.673 Anfragen, auf Finanz– Polizei – Zollbehörden und Staatsanwaltschaften 90.296 Anfragen. Diese Zahl stieg 2015 auf 123.087 an, während 14.020 Anfragen auf die Finanzbehörden entfielen.[92] Hinter der Anzahl der Anfragen verbirgt sich allerdings eine wesentlich größere Zahl von Kontendaten. Nach Auskunft der Bundesregierung auf eine Kleine Anfrage wurden im Jahr 2011 durch die BaFin 116.908 Abrufe getätigt. Im

[90] http://www.bzst.de/DE/Steuern_National/Kontenabrufverfahren/FAQ/faq_node.html
[91] Vgl. die Jahresberichte 2011, S. 252 und 2015, S 160 der Bundesanstalt für Finanzdienstleistungen https://www.bafin.de/DE/Publikationen/Jahresbericht/jahresbericht_node.html
[92] ebda.

Ergebnis wurden die Daten von 1.050.726 Konten abgerufen (Vorjahr: 105.615/990.995).[93]

Neben der Abfrage nach § 24 c KWG haben die Finanzämter nach § 93 Abs. 7 AO die Möglichkeit, über das Bundeszentralamt für Steuern eine Abfrage auf die Kontenstammdaten der Banken zu tätigen.

Hier zeigt sich sogar noch eine größere Steigerungsdynamik. Aus dem soeben zitierten und einer weiteren kleinen Anfrage im Bundestag sind folgende Zahlen bekannt:

2010: 56.696

2011: 62.333[94]

2012: 72.578[95]

2013: 141.640 (davon durch Gerichtsvollzieher: 61.760)[96] Die Abfragemöglichkeit für Gerichtsvollzieher war im Jahre 2013 neu eingeführt worden, zieht man deren Abfragen ab, so ergibt sich immer noch eine Gesamtzahl von 79.880 Abfragen.

Zu dem Kreis der Berechtigten für eine Anfrage über das Bundeszentralamt für Steuern gehören neben den Finanzbehörden die Sozialleistungsträger, die für Grundsicherung für Arbeitsuchende nach dem SGB 2, für Sozialhilfe nach dem SGB 12, für Ausbildungsförderung nach dem Bundesausbildungsförderungsgesetz, für Aufstiegsfortbildungsförderung nach dem Aufstiegsfortbildungsförderungsgesetz und für Wohngeld nach dem Wohngeldgesetz zuständig sind. Durch Änderung des § 802 Abs. 1 ZPO kamen 2013 noch die Gerichtsvollzieher als Abfrageberechtigte hinzu. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit fasst ihre Kritik hieran wie folgt zusammen:

„*Diese Ausdehnung ist schon deswegen kritisch zu sehen, weil die Zugriffsmöglichkeiten ursprünglich für die BaFin und die Strafverfolgungsbehörden vor dem Hintergrund der Bekämpfung der Terrorismusfinanzierung geschaffen worden sind. Ursprünglich verfolgtes Ziel war die Austrocknung der Finanzströme des Terrorismus. Die nunmehr verfolgten Zwecke stehen hiermit in keiner Verbindung und sind in ihrer Wertigkeit auch nicht mit der Terrorismusbekämpfung gleichzusetzen. Wenn bereits zum Zeitpunkt der Kontoeröffnung die Kontostammdaten automatisch als Datensatz gespeichert und dieser durch das*

[93] BT Drs. 17/8715, S. 3 - http://dipbt.bundestag.de/dip21/btd/17/087/1708715.pdf
[94] Ebda. S. 4
[95] http://www.bfdi.bund.de/DE/Datenschutz/Themen/Finanzen_Versicherungen/FinanzenArtikel/KontenabrufverfahrenVonPrivatenKonten.html;jsessionid=09DB486636FC268
[96] BT Drs. 18/2866, S. 6 http://dipbt.bundestag.de/dip21/btd/18/028/1802888.pdf

Kontenabrufverfahren verfügbar gemacht werden kann, erfolgt letztlich eine anlasslose Erfassung grundsätzlich aller Kontoinhaber in Deutschland. Da somit der Datensatz bereits vorliegt, obwohl noch keine Erklärungspflicht des Steuerpflichtigen besteht, ist von einer erheblichen Eingriffsintensität auszugehen, die weit über die ursprünglichen Absichten des Gesetzgebers hinaus das Recht auf informationelle Selbstbestimmung tangiert.

Zudem bestehen durchaus Bedenken, ob bei der praktischen Durchführung des Kontenabrufverfahrens durch die die BaFin und das BZSt um Auskunft ersuchenden Behörden die gesetzlichen Vorgaben eingehalten werden. Erfahrungen von Landesdatenschutzbeauftragten haben unter anderem gezeigt, dass eine fehlende Begründung für das konkrete Kontenabrufverfahren sowie eine fehlende Benachrichtigung des Betroffenen in der Praxis keine Seltenheit darstellen. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit setzt sich daher für eine strikte Eingrenzung des Kontenabrufverfahrens auf das unbedingt erforderliche Maß ein. Hierzu gehört insbesondere auch eine datenschutzkonforme Anwendung durch die zuständigen Behörden.“ [97]

Für diesen Bereich bleibt also festzuhalten, dass seit dem Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung die Kontenabfrage sowohl durch gesetzliche Erweiterungen als auch durch tatsächlich häufigeren Gebrauch erheblich zugenommen hat. Hinzu kommt offenbar ein erhebliches Risiko in Bezug auf die datenschutzkonforme Anwendung durch die zuständigen Behörden.

5.3.5.7.5. Totalspeicherung bei der Deutschen Post

Einen wenig beachteten Bereich der Vorratsdatenspeicherung von Daten bildet die vollständige Erfassung der Adressen auf allen Sendungen der Deutschen Post. Wie die Zeit und „Die Welt“ berichtete, fotografiert die Deutsche Post jede Adresse auf ihren Briefsendungen, das waren im Jahr 2012 66 Millionen Sendungen pro Tag.

Nach den Angaben der Post geschieht dies nur für betriebsinterne Zwecke wie die Qualitätskontrolle. Allerdings werden bei Auslandssendungen in die USA auch Angaben gegenüber den dortigen Behörden gemacht.[98]

97

http://www.bfdi.bund.de/DE/Datenschutz/Themen/Finanzen_Versicherungen/FinanzenArtikel/KontenabrufverfahrenVonPrivatenKonten.html;jsessionid=09DB486636FC2689D206513E47554741.1_cid329?nn=5217370

98 https://www.welt.de/wirtschaft/article117787481/Deutsche-Post-fotografiert-Briefe-fuer-interne-Zwecke.html# http://www.gulli.com/news/21979-datenueberwachung-deutsche-post-fotografiert-ohne-anlass-alle-postsendungen-2013-07-06

Bleibt festzuhalten, dass die gespeicherten Daten keinem Beweiserhebungsverbot in Strafsachen unterliegen.

5.3.5.7.6. Kameraüberwachung

Große öffentliche Beachtung findet stets das Thema der Kameraüberwachung des öffentlichen Raums und des Kameraeinsatzes durch Polizeibehörden.

Bodycams werden unter anderem in den Bundesländern Hamburg, Rheinland-Pfalz, Baden-Württemberg, Hessen, Nordrhein Westfalen, Bayern, der Bundespolizei und auch von der Deutschen Bahn getestet. Es ist den Kameras nicht eindeutig anzusehen, ob sie in Betrieb sind, außerdem ist eine „Pre-Recording-Funktion“ möglich, so dass bei Einschalten der Aufnahme auch die letzten 30 Sekunden vor Start der Aufnahme aufgezeichnet werden.[99] Anders ausgedrückt: Diese Bodycams nehmen ständig die Situation auf, mit Auslösung der Aufnahmetaste bleiben auch die letzten 30 Sekunden vor Drücken der Taste gespeichert. Von polizeilicher Seite wird den Bodycams vor allem eine Abschreckungsfunktion gegenüber Gewalttätern zugemessen. Dies bedeutet zugleich, dass Sie auch gegenüber Nicht-Gewalttätern eine Abschreckungsfunktion entfalten. So gilt die Befürchtung: Dort wo ein Polizist ist, existiert künftig keine Privatsphäre mehr.

Wesentlich stärker im öffentlichen Raum sichtbar sind in stets steigender Zahl Überwachungskameras. Auch hier ist die Datenlage unübersichtlich und lückenhaft, dennoch zeigen die vorhandenen Informationen den starken Anstieg der Kameraüberwachung.

Schätzungsweise 500.000 Kameras befinden sich in Deutschland auf öffentlichen und privaten Grundstücken und in Zügen im Einsatz.[100]

Nach einem Bericht der Süddeutschen Zeitung waren im Jahr 2015 alleine in München 9200 Kameras im öffentlichen Raum installiert, davon 4400 in Fahrzeugen und auf Bahnhöfen der Münchner Verkehrsgesellschaft und der Deutschen Bahn. [101] Nach einem Bericht der „Tageszeitung“ vom 28.05.2015

---

[99] Vgl.: https://www.land.nrw/de/pressemitteilung/nrw-polizei-will-bodycams-fuenf-behoerden-testen http://www.polizei-dein-partner.de/themen/gewalt/gesellschaft/detailansicht-gesellschaft/artikel/bodycams-bei-der-polizei-hessen.html http://www.rp-online.de/nrw/staedte/duesseldorf/polizei-bodycams-fragen-und-antworten-zum-einsatz-in-duesseldorf-und-koeln-aid-1.5733416 http://www.sueddeutsche.de/bayern/sicherheit-bayerische-polizei-testet-bodycams-1.3231348

[100] http://www.fr-online.de/recht/private-kameras-ueberwachung-ueberwachungskameras-haus-erlaubt,21157310,28482130.html

[101] http://www.sueddeutsche.de/muenchen/videoueberwachung-in-muenchen-stadt-der-augen-1.2316618

setzte die Deutsche Bahn damals an rund 640 Bahnhöfen 4800 Kameras ein, ferner 18.000 Videokameras in Regionalzügen und S-Bahnen.[102] In Berlin werden alle U-Bahn-Züge, 86 % der Busse und 64 % der Straßenbahnen sowie 173 Bahnhöfe mit Kameras überwacht.[103]

Der Datenschutzbeauftragte Nordrhein-Westfalens wies insbesondere darauf hin, dass die Technik immer billiger geworden sei[104], was zu einer weiteren Zunahme des Einsatzes von Überwachungskameras auch durch private Unternehmen geführt habe. Dem ist hinzuzufügen, dass durch den Einsatz digitaler Technik die Bildqualität auch erheblich besser geworden ist und damit vor allem die Möglichkeit des heimlichen Einsatzes von Programmen zur Gesichtserkennung zunimmt. Nach Feststellungen des Datenschutzbeauftragten von Niedersachsen im Jahre 2010 wurden 99 % aller Videokameras im öffentlichen Raum rechtswidrig betrieben. So habe er 3345 Kameras überprüft, von denen nur 23 korrekt betrieben worden seien.[105]

An dieser Stelle bleibt festzuhalten, dass in weiten Bereichen die Nutzung öffentlicher Plätze oder Einrichtungen nicht möglich ist, ohne durch Kameras überwacht zu werden.

5.3.5.8. Bedeutung von Telekommunikationsprofilen

Oben wurde bereits zwei Studien zur Standortdatenspeicherung betreffend deren Eingriffstiefe am Beispiel einzelner Personen dargestellt. Eine Studie der Stanford University aus dem Jahre 2014 hat unter Mitarbeit von 564 freiwilligen Teilnehmern deren Telefon-Verbindungsdaten ausgewertet.[106]

Die Forscher benutzten die Daten einer in Deutschland nicht erhältlichen Google-App mit Namen Metaphone. Dieses Programm speichert Log-Daten des Telefons und Daten über die Aktivitäten in sozialen Netzwerken.

Mithilfe dieser gespeicherten Daten identifizierten die Forscher zunächst die Kontakte der Versuchsteilnehmer aufgrund der öffentlichen Verzeichnisse von Yelp und Google Places. Insgesamt kontaktierten die 546 Versuchsteilnehmer 33.688 verschiedene Telefonnummern, von denen 6107 (18 %) einem bestimmten Teilnehmer zugewiesen werden konnten. Im nächsten Schritt kennzeichneten die Forscher die Kontakte, die nach ihrer Auffassung mit einer besonders sensiblen Aktivität verbunden waren. Meistens konnte dies aufgrund der geschäftlichen Angaben einer Organisation herausgefunden werden. Wo es

[102] http://www.taz.de/!5201371
[103] http://www.n-tv.de/panorama/Deutschland-wird-Land-der-Videoueberwachung-article15185831.html
[104] ebenda
[105] http://www.taz.de/!5143976/
[106] http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/

noch Zweifel gab, nuttzen die Forscher Google-Anfragen, um mehr Informationen zu erlangen.

Es wurden 2 Auswertungen gefertigt.

> Die Auswertung der Ergebnisse der einzelnen Anrufe ergab folgende statistische Verteilung der Anrufe:

Gesundheitsdienste	57%
Finanzdienste	40%
Apotheken	30%
Veterinäre	18%
Rechtsdienstleistungen	10%
Arbeitsvermittlung	10%
Religiöse Organisationen	8%
Waffenverkauf und-Reparatur	7%
Politiker und Kampagne	4%
Erotische Etablissements	2%
Marihuana Verkäufer	0.4%

> Bei den religiösen Organisationen überprüften die Forscher die Treffgenauigkeit ihrer Hypothesen. Die Google App MetaPhone extrahiert die Religionsangaben des Benutzers aus seinem Facebook-Profil. 15 Benutzer hatten ein klar definiertes religiöses Profil bei Facebook. Unterstellt, dass ein Benutzer am häufigsten eine Institution seiner eigenen Religion kontaktiert, wurde aus den Telefon-Metadaten bei 11 Benutzern die Religion in Übereinstimmung mit dem Facebook-Profil festgestellt. Die Trefferquote lag also bei 73%.

Eine noch höhere Aussagekraft hatten die Ergebnisse der Untersuchung der Kommunikationsmuster. Die Forscher stellten bei 5 Teilnehmern in anonymisierter Form diese Ergebnisse vor:

> Teilnehmer A kommunizierte mit verschiedenen örtlichen Neurologie-Gruppen, einer spezialisierten Apotheke, einem Gesundheitsdienst für seltene Krankheiten und einer Hotline für ein Medikament, das ausschließlich zur Behandlung von multipler Sklerose benutzt wird.
>
> Patient B führte sehr lange Gespräche mit Kardiologen in einem großen medizinischen Zentrum, sprach kurz mit einem medizinischen Labor, erhielt Anrufe von einer Apotheke und führte kurze Gespräche mit einer Hotline für ein medizinisches Gerät, das zur Beobachtung von Herzrhythmusstörungen benutzt wird
>
> Teilnehmer C führte eine Anzahl von Gesprächen mit einem Waffengeschäft, das auf bestimmte halbautomatische Gewehre spezialisiert war. Er führte außerdem lange Gespräche mit dem Kundendienst eines Gewehr-Herstellers, der auf diese bestimmten Waffen spezialisiert war.
>
> Im Verlauf von 3 Wochen kontaktierte Teilnehmer D ein Geschäft für Haus- und Wohnungsrenovierung, einen Schlosser, ein Geschäft für Hydrokultur und ein Geschäft für Raucherbedarf.
>
> Die Teilnehmerin E hatte ein langes Telefonat mit ihrer Schwester am frühen Morgen. Zwei Tage später führte sie eine Serie von Gesprächen mit einer lokalen Beratungsorganisation für Familienplanung. 2 Wochen später führte sie weitere kurze Gespräche sowie ein abschließendes Telefonat einen Monat später.

Bei den Ergebnissen dieser Studie ist zu berücksichtigen, dass die Forscher nicht die Telefonverzeichnisse zur Verfügung hatten, die den deutschen zur Auskunft berechtigten Behörden zur Verfügung stehen. Sind die vorstehend dargestellten Daten schon ausgesprochen aussagekräftig, so darf dabei nicht vergessen werden, dass die Forscher aufgrund der öffentlich zugänglichen Informationen lediglich 18 % der von den Versuchsteilnehmern angerufenen Nummern überhaupt identifizieren konnten.

Diese Ausführungen werden gemacht, weil sowohl das angerufene Bundesverfassungsgericht als auch der Europäische Gerichtshof die hohe Aussagekraft der Telekommunikationsverbindungsdaten zwar anerkennen, diese in ihrer Bedeutung aber den Gesprächsinhalten nicht gleichstellen. So hat insbesondere der europäische Gerichtshof eine Verletzung des Kernbereichs des Art. 7 der Charta durch die Erhebung der Telekommunikationsverbindungsdaten verneint.[107] Der EUGH führt an dieser Stelle aus, die Vorratsdatenspeicherung von

[107] Vgl. EUGH 08.04.2014, Rn. 39

Daten stelle zwar einen besonders schwerwiegenden Eingriff in die in Art. 7 der Charta verankerten Rechte dar, sei jedoch nicht geeignet, ihren Wesensgehalt anzutasten, da die Richtlinie (2006/24/EG) die Kenntnisnahme des Inhalts der Kommunikation als solchen nicht gestatte.[108]

Das Bundesverfassungsgericht sah den Wesensgehalt des Art. 10 Abs. 1 GG durch die Speicherung von Verbindungsdaten nicht als verletzt an.[109]

Berücksichtigt man die oben beispielhaft erwähnte Stanford-Studie und die Selbstversuchs-Studien von Herrn Spitz und Herrn Glättli, so besteht Anlass, diese Bewertung erneut zu überprüfen. Die Analyse von Telekommunikationsverbindungsdaten und Standortdaten ist aussagekräftiger als die bloßen Inhalte von Telefonaten. Auch ist das Abhören der Letzteren ausgesprochen personal-und zeitintensiv und ihre Ergebnisse sind häufig nicht zielführend, weil kriminelle Gesprächspartner sich unterschiedlicher Codes bedienen.

Die Eingriffstiefe der Erhebung, Speicherung und Beauskunftung von Telekommunikationsverbindungsdaten ist nach heutigem Stand der Technik mindestens so intensiv wie die Überwachung der Gesprächsinhalte von Telefonaten. Insbesondere i.V.m. Standortdaten sind die gewonnenen Erkenntnisse aussagekräftiger als die bloße Telefonüberwachung. Dies gesagt, erschließt sich unmittelbar, dass der Grundrechtseingriff durch die Erhebung und Verarbeitung dieser Daten bei praktisch allen Bürgern ohne konkreten Anlass für diesen Eingriff bereits isoliert nicht mehr rechtfertigungsfähig ist.

Der Anfall von Verkehrsdaten ist unvermeidbar, während Kommunikationsinhalte Ende-zu-Ende verschlüsselt werden können. Während man sich bei der Kommunikation – oder auch beim Verfassen eines Tagebuchs – bewusst entscheiden kann, bestimmte Tatsachen nicht offenzulegen, ist in Verkehrsdaten alles nachzulesen – ob man will oder nicht. Heutzutage wird es wenige persönliche Geheimnisse des täglichen Lebens geben, die sich nicht durch genaue Analyse von Verkehrsdaten aufdecken ließen.

Verkehrsdaten geben, wie am Beispiel der Stanford-Studie gezeigt, oftmals selbst Aufschluss über den Inhalt der Telekommunikation, beispielsweise Verbindungen mit bestimmten Beratungsstellen, spezialisierten Ärzten (z.B. Psychotherapeuten) oder Spenden per SMS.

Die von der EU finanzierte SURVEILLE-Studie kommt zu dem Ergebnis: „Eine Unterscheidung zwischen ‚Inhalt' (der vertraulichen Botschaft des Absenders an

[108] EUGH ebda.

[109] BverfG 02.03.2010 – 1 BvR 256/08 – Rn. 213 = BverfGE 125, 260

den Empfänger) und ‚Metadaten' (Informationen über die Beteiligten und über eine von ihnen versandte und empfangene Botschaft) ist kein entscheidender Faktor mehr für die Beurteilung des ethischen Risikos von Grundrechtseingriffen durch Überwachung. Die Kombination verschiedener Arten von Metadaten kann vertraulichere und sensiblere persönliche Daten offenlegen als der eigentliche Inhalt der Nachricht. Rechtfertigungen von Überwachung auf der Grundlage der Idee, sie betreffe nur Metadaten, sollten abgelehnt werden. Das Augenmerk sollte auf die Prüfung der Einzelheiten gelegt werden, beispielsweise um welche Arten von Metadaten es geht und worin ihre Gesamtwirkung auf die Grundrechte liegt."[110]

Über 100 zivilgesellschaftliche Organisationen betonen in „Internationalen Grundsätzen für die Anwendung der Menschenrechte in der Kommunikationsüberwachung":[111]

> *Traditionell wurde die Invasivität der Kommunikationsüberwachung auf Basis von künstlichen und formalen Kategorien bewertet. Bestehende rechtliche Rahmenbedingungen unterscheiden zwischen „Inhalt" oder „Nicht-Inhalt", „Teilnehmerinformation" oder „Metadaten", gespeicherten Daten oder Übertragungsdaten, Daten, die zuhause gespeichert werden oder die im Besitz eines dritten Diensteanbieters sind. Allerdings sind diese Unterscheidungen nicht mehr geeignet, den Grad des Eindringens der Kommunikationsüberwachung in das Privatleben von Einzelpersonen und Verbänden zu messen. Während seit Langem Einigkeit darin besteht, dass Kommunikationsinhalte per Gesetz signifikanten Schutz verdienen wegen ihrer Fähigkeit, sensible Informationen zu offenbaren, ist es nun klar, dass andere Informationen aus der Kommunikation - Metadaten und andere Formen der nicht-inhaltlichen Daten - vielleicht sogar mehr über eine Einzelperson enthüllen können als der Inhalt selbst und verdienen daher einen gleichwertigen Schutz. Heute könnte jede dieser Informationsarten für sich allein oder gemeinsam analysiert die Identität einer Person, deren Verhalten, Verbindungen, physischen oder gesundheitlichen Zustand, Rasse, Hautfarbe, sexuelle Orientierung, nationale Herkunft oder Meinungen enthüllen, oder die Abbildung einer Person mithilfe der Standortbestimmung, ihrer Bewegungen oder Interaktionen über einen Zeitraum ermöglichen oder auch von allen Menschen an einem bestimmten Ort, zum Beispiel bei einer öffentlichen*

[110] https://surveille.eui.eu

[111] Hier zitiert nach: http://www.humanistische-union.de/nc/publikationen/vorgaenge/online_artikel/online_artikel_detail/back/vorgaenge-203/article/internationale-grundsaetze-fuer-die-anwendung-der-menschenrechte-in-der-kommunikationsueberwachung-1/

> *Demonstration oder anderen politischen Veranstaltung. Als Ergebnis sollten alle Informationen, welche sich aus der Kommunikation einer Person ergeben, diese beinhalten, reflektieren, oder über diese Person stattfinden, und welche nicht öffentlich verfügbar und leicht zugänglich für die allgemeine Öffentlichkeit sind, als „geschützte Informationen" angesehen werden. Ihnen sollte dementsprechend der höchste gesetzliche Schutz gewährt werden.*

Nach dem EuGH hat sich auch der UN-Menschenrechtsbeauftragte der Auffassung angeschlossen, dass eine anlasslose Vorratsdatenspeicherung „weder notwendig noch verhältnismäßig erscheint".[112] Auch der UN-Sonderberichterstatter zu Menschenrechten bei der Bekämpfung von Terrorismus hält eine Vorratsdatenspeicherung für unvereinbar mit dem Schutz der Privatsphäre. „Der Wesensgehalt des Rechts auf vertrauliche Kommunikation liegt darin, dass Eingriffe die Ausnahme bleiben und fallweise gerechtfertigt werden müssen".

5.3.5.9 Das Urteil des Bundesverfassungsgerichts vom 02.03.2010

Vor dem Hintergrund des EuGH-Urteils, aber auch mit Blick auf die technische und rechtliche Entwicklung ist es erforderlich, die 2010 zur Vorratsdatenspeicherung aufgestellten oder auch bewusst unterlassenen Bewertungen neu zu treffen.

Da das Urteil die Vorschriften der damaligen §§ 113a und b TKG für nichtig erklärte, brauchte es sich nicht näher mit den empirischen Nachweisen des eklatanten Missverhältnisses zwischen Tragweite der Vorratsdatenspeicherung auf der einen und ihrem Ertrag auf der anderen Seite auseinander zu setzen. Gleichfalls brauchte es nicht weiter auf die Belege für die ebenso hohe Aufklärungsrate ohne Vorratsdatenspeicherung einzugehen. Das Freiburger Max-Planck-Institut für ausländisches und internationales Strafrecht kommt in einer umfassenden Studie zu dem Ergebnis: „Auch nach der Beiziehung anderer Informationsquellen ergeben sich keine belastbaren Hinweise darauf, dass die Schutzmöglichkeiten durch den Wegfall der Vorratsdatenspeicherung reduziert worden wären." [113]

Das Urteil bedurfte auch keiner Auseinandersetzung mit den kontraproduktiven Wirkungen einer Vorratsdatenspeicherung. Das Max-Planck-Institut verweist darauf, dass die Orientierung an Verkehrsdaten teilweise „nicht nur zur Aufklärung nichts beitragen kann, sondern teilweise wohl auch dazu geeignet ist,

---

[112] http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[113] Max-Planck-Institut, aaO

die Ermittlungsressourcen in eine wenig ertragreiche Richtung zu lenken.“ Hinzu kommt: Entfällt infolge einer Vorratsdatenspeicherung die Möglichkeit zur nicht rückverfolgbaren Erstattung von Strafanzeigen per Telefon, Fax, Internet oder E-Mail, so werden manche Straftaten schlicht nicht mehr angezeigt und können deswegen nicht mehr verfolgt werden. Beispielsweise dürften Strafanzeigen wegen Straftaten im eigenen Unternehmen oder auch wegen Kinderpornografie im Internet aus Furcht vor Nachteilen oftmals nur im Schutz der Anonymität erstattet werden. Drittens gilt: Wenn Straftäter wegen eines Gesetzes zur Vorratsdatenspeicherung mit einer jederzeitigen Rückverfolgbarkeit rechnen müssen, weichen sie verstärkt auf andere Kommunikationskanäle aus (z.B. persönliche Kommunikation, wechselnde Telefonzellen, wechselnde unregistrierte SIM-Handykarten, wechselnde öffentliche WLAN-Internetzugänge, ausländische Anonymisierungsdienste). Weil solche anonymen Kommunikationskanäle selbst bei dringendem Verdacht einer schweren Straftat auf besondere Anordnung nicht mehr überwachbar sind, führt eine Vorratsdatenspeicherung letztlich zur Unaufklärbarkeit schwerer Straftaten. Nach Inkrafttreten des Gesetzes zur Vorratsdatenspeicherung im Jahr 2008 erklärten 46% der in einer Umfrage Befragten, sie wollten einen Anonymisierungsdienst einsetzen oder täten dies bereits. 25% wollten Internet-Cafés nutzen oder taten dies bereits. Vor diesem Hintergrund erklärt sich, dass unter dem Strich ein messbarer Nutzen einer Vorratsdatenspeicherung nicht nachzuweisen ist.

Das Urteil aus dem Jahr 2010 brauchte sich auch nicht mit der Europäischen Menschenrechtskonvention und der diesbezüglichen Rechtsprechung des EGMR[114] und des Verfassungsgerichtshofs Rumäniens[115] auseinanderzusetzen. Bei der gegenwärtigen Sachlage wäre auch eine konventionskonforme Auslegung des Grundgesetzes zugrunde zu legen.[116]

Das Urteil enthielt auch keine Auseinandersetzung mit der früheren Rechtsprechung des Bundesverfassungsgerichts, mit welcher eine allumfassende, permanente Vorratsdatenspeicherung nicht in Einklang zu bringen ist.[117] Die Entscheidung ist unter diesem Gesichtspunkt sowohl vom Bundesdatenschutzbeauftragten[118] als auch in der Literatur[119] kritisiert worden.

---

[114] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, NJOZ 2010, 696

[115] Verfassungsgerichtshof Rumäniens, 1258 vom 08.10.2009, http://www.vorratsdatenspeicherung.de/content/view/342/79/lang,de

[116] BverfG 14.10.2004 - 2 BvR 1481/04 -Rn. 32

[117] Näher Schriftsatz vom 13.08.2008 im Verfahren 1 BvR 256/08, http://www.vorratsdatenspeicherung.de/images/schriftsatz_2008-08-13.pdf, 33

[118] http://www.daten-speicherung.de/index.php/ziercke-greift-ak-vorrat-an/., dort Abschnitt: Peter Schaar: IP-Adressen „höchst sensibel“

[119] Forgó/Grügel, K&R 2010, 218 ff.

Auf dem Prüfstand steht aufgrund der veränderten Sachlage auch das Argument, dass eine Vorratsdatenspeicherung deshalb verhältnismäßig sei, weil der Staat ihre Durchführung Privatunternehmen übertrage[120]. Dann könnte der Staat auch in anderen Fällen die bisher geltenden verfassungsrechtlichen Grenzen durch Outsourcing sprengen. Die engen Voraussetzungen, die das Hohe Gericht etwa für Rasterfahndung oder Kfz-Massenabgleich aufgestellt hat,[121] wären nicht mehr bindend, wenn der Staat Private mit der Durchführung betraute. Es ist offensichtlich, dass dies nicht richtig sein kann. Es führte zu einer massiven Absenkung der rechtstaatlichen Anforderungen an die staatliche Datenverarbeitung, insbesondere im sensiblen Bereich der präventiven und repressiven Ermittlungstätigkeit staatlicher Behörden. Die Betrauung Privater kann eine Vorratsdatenspeicherung daher nicht rechtfertigen. Dass das Urteil für andere Vorhaben „größere Zurückhaltung" fordert,[122] ist leider durch die tatsächliche Entwicklung nicht mehr gegeben. Es kann daher ein Übergreifen des Prinzips einer permanenten, flächendeckenden Datensammlung ins Blaue hinein auf immer weitere Lebensbereiche nicht mehr verhindern.

Das Bundesverfassungsgericht argumentierte 2010 weiter, die Telekommunikation weise ein spezifisches Gefahrenpotential auf. Sie erleichtere die Begehung klassischer Straftaten und habe neue Formen von Straftaten hervorgebracht, deren Begehung sich „weithin der Beobachtung" entziehe. Eine Rekonstruktion gerade der Telekommunikationsverbindungen sei daher für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung[123]. All dies als richtig unterstellt, rechtfertigt es gleichwohl nicht eine generelle und undifferenzierte, globale und pauschale Erfassung von Informationen über nahezu jegliche Telekommunikation der gesamten Bevölkerung. Spezifischen Gefahren und damit einhergehend einem besonderen Aufklärungsinteresse kann nämlich schon ohne Vorratsdatenspeicherung Rechnung getragen werden. Auch ohne Vorratsdatenspeicherung waren ausweislich einer repräsentativen Aktenanalyse des Max-Planck-Instituts 96% aller Auskunftsersuchen nach § 100g StPO erfolgreich.[124] Zudem ist die Rekonstruktion und Überwachung der Telekommunikation technikbedingt ohnehin sehr viel leichter, geheimer und kostengünstiger zu bewerkstelligen als die Rekonstruktion und Überwachung unmittelbarer oder postalischer Kommunikation. Dementsprechend liegt die polizeiliche Aufklärungsquote im Bereich der Straftaten mit Tatmittel Internet aktuell bei 67% der bekannt gewordenen Internetkriminalität (2005: 84,9%, 2006: 84%, 2007: 82,9%, 2008: 79,8%, 2009: 75,7%, 2010: 72,3%; 2011: 65,1%; 2012:

[120] BverfG 02.03.2010 – 1 BvR 256/08 u.a. – Rn. 214
[121] BVerfGE 115, 320; BVerfGE 120, 378
[122] BverfG 02.03.2010 – 1 BvR 256/08 u.a. – Rn.218
[123] BverfG 02.03.2010 – 1 BvR 256/08 u.a. – Rn. 216
[124] MPI-Forschungsbericht, S. 253

60,1%; 2013: 61,6%; 2014: 66,4%) und übersteigt damit deutlich die durchschnittliche Aufklärungsquote von Straftaten (2015: 56,3%). Sind Telekommunikationsverbindungen schon ohne Vorratsdatenspeicherung überdurchschnittlich häufig rekonstruierbar, können die Eigenarten der Telekommunikation nicht auch noch eine verdachtslose Vorratsdatenspeicherung rechtfertigen. Die Vorratsdatenspeicherung hat die Aufklärungsrate im Übrigen nicht weiter gesteigert; vielmehr ist sie nach Inkrafttreten des letzten Gesetzes – wie auch nach seinem Außerkrafttreten – zurückgegangen. Demgegenüber ist seit 2014 auch ohne Vorratsdatenspeicherung eine Steigerung der Aufklärungsquote gelungen.

Richtig ist, dass Telekommunikation die Begehung klassischer Straftaten erleichtern kann. Auf der anderen Seite erleichtert sie aber die Aufklärung klassischer Straftaten enorm. Immer häufiger nutzen Ermittler Telekommunikationsdaten zur Aufklärung von Straftaten (z.B. Bewegungsdaten) – Informationen, die ohne Telekommunikation und Internet nicht für die Ermittlungsarbeit zur Verfügung stünden. So ist die Zahl der Verkehrsdatenzugriffe von ca. 5.000 im Jahr 2000[125] auf 27.167 im Jahr 2015angestiegen (Anzahl der Verfahren: 16.117). [126]

Richtig ist, dass die Telekommunikation neue Formen von Straftaten hervorgebracht hat, nämlich Angriffe auf die Vertraulichkeit, Integrität oder Verfügbarkeit von Computersystemen unter Verwendung von Telekommunikationsnetzen (beispielsweise durch „Hacking“). Dass sich die Begehung dieser Straftaten „weithin der Beobachtung“ entziehe, mag zutreffen. Vergleichbare Straftaten außerhalb der Telekommunikationsnetze entziehen sich jedoch ebenfalls „weithin der Beobachtung“. Datenveränderung und Computersabotage (§§ 303a, 303b StGB) sind eine moderne Form der Sachbeschädigung (§ 303 StGB). Im Jahr 2011 sind knapp 700.000 Fälle von Sachbeschädigung bei einer Aufklärungsquote von 25% verzeichnet worden.[127] Demgegenüber sind im gleichen Jahr knapp 5.000 Fälle von Datenveränderung und Computersabotage bei einer Aufklärungsquote von 41% verzeichnet worden.[128] Der unerwünschte Zugriff auf fremde Sachen und Anlagen entzieht sich somit stets „weithin der Beobachtung“. Im Bereich der Kommunikationsnetze ist eher eine höhere Aufklärbarkeit gegeben.

---

[125] Max-Planck-Institut, BT-Drs. 16/7434, S. 50

[126] Bundesamt für Justiz, Übersicht Telekommunikationsüberwachung, Stand 22.07.2016 https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_Verkehrsdaten_2015.pdf?__blob=publicationFile&v=2.

[127] Bundeskriminalamt, Kriminalstatistik 2011 Kurzbericht, 5

[128] Bundeskriminalamt, Kriminalstatistik 2011 Kurzbericht, 56

Spezifischen Gefahren der Telekommunikation und damit einhergehend einem besonderen Aufklärungsinteresse kann auch ohne generelle und undifferenzierte Datensammlung Rechnung getragen werden, wie die Vergangenheit zeigt. Die Rekonstruktion und Überwachung der Telekommunikation ist technikbedingt ohnehin sehr viel leichter, geheimer und kostengünstiger zu bewerkstelligen als die Rekonstruktion und Überwachung unmittelbarer oder postalischer Kommunikation.

Selbst die (unterstellte) Verurteilung einzelner sonst nicht überführbarer Straftäter infolge der Vorratsdatenspeicherung rechtfertigte in einem demokratischen Staat nicht die unterschiedslose Erfassung des Telekommunikations- und Bewegungsverhaltens der gesamten Bevölkerung. In Deutschland werden jährlich ca. 6 Mio. Straftaten registriert, von denen ca. 3,3 Mio. Taten aufgeklärt werden und ca. 2,7 Mio. Straftaten nicht. In einer demokratischen Gesellschaft ist nie jede Straftat aufklärbar und darf dies auch nicht um jeden Preis angestrebt werden.

Das Bundesverfassungsgericht argumentierte 2010 weiter, hinsichtlich der Telekommunikationsdaten existiere mangels öffentlicher Wahrnehmbarkeit kein gesellschaftliches Gedächtnis, das es wie in anderen Bereichen erlaubte, zurückliegende Vorgänge auf der Grundlage zufälliger Erinnerung zu rekonstruieren.[129] Dieser Unterschied besteht jedoch auch in anderen Bereichen nicht und rechtfertigt andernteils keine Identifizierungspflicht: Bei öffentlichen Veranstaltungen und sonst in der Öffentlichkeit bleibt man regelmäßig in der Menschenmenge anonym. Man behält weitgehend die Kontrolle darüber, ob und gegenüber wem man seine Identität offenlegt. Wenn man seine Identität nicht offenlegt, wird ein Gespräch auf einem Marktplatz, in einer Kneipe, auf einem Bahnhof usw. in aller Regel nicht zur nachträglichen Identifizierbarkeit führen. Auch hinsichtlich der Briefkommunikation existiert kein „gesellschaftliches Gedächtnis“. Hinzu kommt, dass die Ermittler im Fall öffentlich wahrnehmbarer Vorgänge regelmäßig nicht wissen, wer sie beobachtet hat, während die Telekommunikationsanbieter stets bekannt und auskunftsfähig sind. Wer sich der Fernkommunikationsmittel bedient, ist technisch bedingt typischerweise sehr viel leichter zu identifizieren als wer unmittelbar kommuniziert. Die Einschaltung eines Mittlers macht die Fernkommunikation ausforschungsanfälliger als wenn nur der Gesprächspartner als Informationsquelle zur Verfügung stünde. Im Übrigen trifft das Argument, es fehle im Telekommunikationsbereich an einem „gesellschaftlichen Gedächtnis“, gleichermaßen auf Kommunikationsinhalte zu. Gleichwohl würde niemand daraus folgern, Art. 10 GG sei überflüssig. Denn die Fernkommunikation ermöglicht einen heimlichen, zentralen, beweiskräftigen,

[129] BverfG 02.03.2010 – 1 BvR 256/08 u.a. – Rn. 217

kooperationsbereiten und kostengünstigen Zugriff auf Kommunikationsbeziehungen, wie ihn andere Ermittlungsmethoden niemals möglich machen können. Auch ohne Identifizierungspflicht sind telekommunizierende Straftäter leichter zu identifizieren als anders kommunizierende Straftäter, was die überdurchschnittliche Aufklärungsquote bei Straftaten mit Tatmittel Internet belegt.

Die Vorratsdatenspeicherung ist 2010 auch damit gerechtfertigt worden, dass die Verbreitung bestimmter Vertragsgestaltungen der Telekommunikationsdiensteanbieter die Verfügbarkeit von Daten reduziere.[130] Die verfassungsrechtliche Würdigung einer Vorratsdatenspeicherung im Telekommunikationsbereich kann sich indes nicht an überkommenen Vertragsgestaltungen der Telekommunikationsdiensteanbieter orientieren, sondern nur an nicht elektronisch vermittelter Kommunikation, bei der keinerlei Erfassung menschlicher Kontakte oder Identitäten bei einem Kommunikationsmittler erfolgt.

Das Bundesverfassungsgericht hat ferner argumentiert, elektronische Kommunikationsspuren seien besonders flüchtig.[131] Ebenso einfach wie elektronische Daten gelöscht werden können, können sie aber auch gespeichert werden. Schon aus der hohen Aufklärungsquote im Internetbereich ohne Vorratsdatenspeicherung ergibt sich, dass im Bereich der elektronischen Kommunikation ohnehin weitaus mehr Kommunikationsspuren anfallen als im Bereich der menschlichen oder schriftlichen Kommunikation. Gleiches gilt für das Bewegungsverhalten.

Nach dem Willen des Bundesverfassungsgerichts sollte seine Entscheidung zur Vorratsspeicherung von Verkehrsdaten auf andere Datensammlungen nicht übertragen werden. Die Verkehrsdatenspeicherung sollte eine „Ausnahme“ bleiben.[132] Die spätere Entscheidung zu § 111 TKG gibt diese Absicht aber bereits wieder auf und hält fest, „vorsorgliche Datensammlungen [könnten] als Grundlagen vielfältiger staatlicher Aufgabenwahrnehmung ihre Berechtigung“ haben.[133] Hier wird der drohende Dammbruch offenbar. Hielte man eine Vorratsdatenspeicherung im Telekommunikationsbereich für gerechtfertigt, dann würde es schrittweise dazu kommen, dass alle für die Strafverfolgung oder Gefahrenprävention nützlichen Daten vorsorglich erfasst werden.[134]

---

[130] BverfG 02.03.2010 – 1 BvR 256/08 u.a. – Rn. 217

[131] BverfG 02.03.2010 – 1 BvR 256/08 u.a. – Rn. 260

[132] BverfG 02.03.2010 – 1 BvR 256/08 u.a. – Rn.218

[133] BverfG 24.01.2012 – 1 BvR 1299/05 – Rn. 138

[134] BverfG 02.03.2010 – 1 BvR 256/08 u.a. – Rn.218

5.4. Ergebnis zu Art. 10 Abs. 1 GG

§§ 113 b Abs. 1 – 4 und 8, 113 c Abs. 1 greifen rechtswidrig in das Telekommunikationsgeheimnis ein. Sie sind unbestimmt und unverhältnismäßig.

6 Eingriff in das Grundrecht der Pressefreiheit aus Art. 5 Abs. 1 S. 2 GG

6.1. Eingriffstatbestand

Die Beschwerdeführer zu 1, 4, 5, 10, 14, 20 und 21 können sich hinsichtlich der Erhebung und Speicherung ihrer Telekommunikations- und Standortdaten auch auf das Grundrecht der Pressefreiheit aus Art. 5 Abs. 1 S. 2 GG berufen.

Die Erhebung von Verbindungsdaten der Telekommunikation ist ein Eingriff in das Grundrecht aus Art. 5 Abs. 1 S. 2 GG. Dem Staat werden hierdurch Informationen verfügbar gemacht, die die Beschwerdeführer geheim halten und auch gegenüber dem Staat nicht herausgeben wollen. Der Eingriff in die Pressefreiheit besteht auch immer dann, wenn durch die erhobenen Daten lediglich der Aufenthaltsort eines Informanten ermittelt werden soll. Der freie Informationsfluss zwischen den Medien und deren Informanten wird bereits dann gefährdet, wenn der Informant durch die Mitteilung an den Journalisten Schwierigkeiten zu befürchten hat. Dies kann nicht nur durch die Preisgabe der Identität des Informanten, sondern auch dadurch entstehen, dass Strafverfolgung und andere staatliche Organe durch Ziel Zugriff auf die Medien wichtige Informationen wie den Aufenthaltsort eines Informanten oder seine Kommunikation mit den Medien, obwohl dem Informanten an der Geheimhaltung dieser Informationen gelegen ist. Bereits durch die befürchtete Offenlegung könnte der Informant sich von der Mitteilung an die Presse abschrecken lassen.[135] Der Schutzbereich des Art. 5 Abs. 1 S. 2 GG ist vorliegend auch neben demjenigen des Art. 10 Abs. 1 GG eröffnet. Für die freiheitliche demokratische Grundordnung ist die Freiheit der Medien konstituierend. Für den freiheitlichen Staat sind die freie Presse und die freie Kommunikation durch neuere öffentliche Medien wie Internet-Blogs von besonderer Bedeutung. Der Schutzbereich des Grundrechts in seiner objektivrechtlichen Bedeutung als institutionelle Garantie der freien Presse und des Rundfunks umfasst die gesamte Tätigkeit von der Beschaffung der Information bis zur Verbreitung der Nachrichten und Meinungen; in seiner subjektivrechtlichen Bedeutung gewährt er dem tätigen Journalisten ein subjektives Freiheitsrecht, zu dem auch die Voraussetzungen und Hilfstätigkeiten gehören. Deshalb ist es nach der Rechtsprechung des Bundesverfassungsgerichts den staatlichen Stellen grundsätzlich verwehrt, sich Einblicke in die Vorgänge zu verschaffen, die zur

[135] So: BverfG 12.03.2003- 1 BvR 348/99 –Rn. 110= BverfGE 107, 299

Entstehung von Nachrichten oder Beiträgen führen, die in der Presse gedruckt oder im Rundfunk gesendet werden. Die Medien haben grundsätzlich ein schutzwürdiges Interesse an der Geheimhaltung solcher Unterlagen, die das Ergebnis eigener Beobachtungen und Ermittlungen sind und am Schutz des Kontaktes zu Personen, die selbst Gegenstand der Berichterstattung sind.[136]

6.2. Rechtfertigung

Die Pressefreiheit steht unter allgemeinem Gesetzesvorbehalt, Art. 5 Abs. 2 GG. Der vorliegende Eingriff ist in Bezug auf seine Rechtfertigung abzuwägen gegen das staatliche Schutzinteresse, das mit der Erhebung der Verbindungsdaten verfolgt wird. Dabei hat die Abwägung in besonderem Maße der hohen Bedeutung der Pressefreiheit Rechnung zu tragen.[137] Das Bundesverfassungsgericht hat in der vorerwähnten Entscheidung eine Abwägung für den Fall vorgenommen, dass konkret auf vertragliche Verbindungsdaten beim Telekommunikationsprovider im Rahmen eines Strafverfahrens zugegriffen werden sollte. Obwohl das Bundesverfassungsgericht in dieser Entscheidung die Verbindungsdaten aufgrund der Tatsache, dass sie bei Dritten gespeichert waren, weniger schützt als Unterlagen, die sich im Besitz eines Journalisten befinden[138] hat es auch in dieser Entscheidung Abwägungsüberlegungen getroffen, die für den vorliegenden Fall einer anlasslosen vorsorglichen Speicherung von Verbindungsdaten das Grundrecht der Pressefreiheit stärker bewerten lassen als die mit der Erhebung und Speicherung verfolgten Interessen der öffentlichen Sicherheit.

Das Bundesverfassungsgericht hat in seiner Abwägung dabei berücksichtigt, dass es bei der getroffenen Maßnahme nicht um die Aufdeckung der Identität eines typischen Informanten, sondern um die Ermittlung des Aufenthaltsortes eines Beschuldigten ging. Es hat offengelassen, wie weit das Interesse von Journalisten, unbehelligt telefonischen Kontakt zu gesuchten Straftätern haben zu können, verfassungsrechtlichen Schutz genießen kann. Nach Auffassung des Bundesverfassungsgerichtes hat dieses Interesse grundsätzlich ein geringeres Gewicht als das Interesse an der Kommunikation mit Personen, die als Informanten den Medien für die Öffentlichkeit wichtige Informationen zukommen lassen, etwa zur Aufdeckung und Aufklärung von Missständen ständen.[139] Das generelle Interesse des Vertrauensschutzes von Journalisten im Verhältnis zu ihren Informanten ist also höher zu bewerten, als der vom Bundesverfassungsgericht konkret entschiedene Fall des Kontaktes mit einem

[136] BverfG ebda. Rn 105 – 107 mwN
[137] BverfG ebda. 115ff. mwN
[138] BverfG ebda. Rn 122 – 124, zur Kritik vgl. Pöppelmann/Jehmlich, AfP 2003, 218
[139] BverfG ebda. Rn. 130

bereits namentlich bekannten Verdächtigen, dessen Aufenthaltsort ermittelt werden sollte. Bei Einführung der Vorratsdatenspeicherung ist die Vertrauensbeziehung aller Journalisten zu ihren Informanten und anderen Kontakten betroffen. Es liegt also ein ungleich schwererer Eingriff vor, der zugleich die institutionelle Funktion der Presse berührt. Dem steht gegenüber eine beabsichtigte Erhöhung der Aufklärung schwerster Straftaten und der Abwehr der von dieser Berufsgruppe ausgehenden Gefahren für höchste Rechtsgüter, wobei zumindest davon auszugehen ist, dass Journalisten als Berufsgruppe nicht überdurchschnittlich zu den genannten Straftaten/Gefahren beitragen. Nach der Lebenserfahrung ist das genaue Gegenteil der Fall. Damit steht der verfassungsrechtlich besonders hoch einzustufenden Pressefreiheit die zweifelhafte und quantitativ vernachlässigenswerte Erhöhung der Aufklärung von Straftaten und Abwehr von besonders schwerwiegenden Gefahren durch Mitglieder dieser Berufsgruppe gegenüber. Legt man diese Abwägungskriterien zugrunde, so ergibt sich zwingend, dass die erheblichen Beeinträchtigungen des Vertrauensverhältnisses der Presse gegenüber ihren Informanten das vom Staat verfolgte Sicherheitsinteresse nicht mehr zu rechtfertigen vermag.

6.3. Ergebnis zu Art. 5 Abs., 1 S. 2 GG

§ 113 Buchst. b Abs. 1-4 und 8 TKG und § 113 Buchst. c Abs. 1 TKG verletzen das Grundrecht der Beschwerdeführer zu 1, 4, 5, 10, 14, 20 und 21 aus Art. 5 Abs. 1 Satz 2 GG

7 Verletzung der Informationsfreiheit, Art. 5 Abs. 1 S. 1 GG

7.1. Eingriffstatbestand

Art. 5 Abs. 1 S. 1 GG erfasst von seinem Schutzbereich her nicht nur die Meinungsäußerungsfreiheit, sondern als deren Gegenstück auch die Informationsfreiheit als einander ergänzende Elemente eines Kommunikationsprozesses. Objektivrechtlich ist der Prozess der Kommunikation, subjektivrechtlich die Freiheit, daran teilzunehmen, geschützt.[140] Zum Schutzbereich gehört auch die freie, unbefangene und eigenverantwortliche Möglichkeit der Bildung einer Meinung.[141]

7.2. Rechtfertigung

Art. 5 Abs. 1 S. 1 GG steht unter Gesetzesvorbehalt, Art. 5 Abs. 2 GG. Vorliegend ist wiederum abzuwägen, ob das mit der Vorratsdatenspeicherung verfolgte

---

[140] BverfG 15.12.2004 – 2 BvR 2219/01 –Orientierungssatz 2a. mwN

[141] Zum Abschreckungseffekt bei der Güterabwägung: BverfG 09.10.1991 – 1 BvR 1555/88 – Rn. 59 = BverfGE 85,1 BverfG 09.10.1991 – 1 BvR 221/90 – Rn 53; BverfG 25.06.2009 – 1 BvR 134/03 – Rn. 62 mwN

staatliche Sicherheitsinteresse stärker wiegt, als die Bedeutung der Information- und Meinungsbildungsfreiheit.

Wem bewusst ist, dass er bei der Suche nach Informationen im Internet seine Identität preisgibt, indem sein Suchverhalten aufgezeichnet wird, der kann sich nicht mehr frei und unbefangen eine Meinung bilden, er wird durch dieses Bewusstsein davon abgeschreckt, „gefährliche" Informationen aufzusuchen. Wie oben zum CNAT-Verfahren ausgeführt wurde[142], befindet sich der Internetnutzer in der Situation ständigen Überwachtseins – wie in einem Panoptikum. Die für die Speicherung erforderliche „zugewiesene Benutzerkennung", § 113b Abs. 3 Nr. 2 TKG zu erzeugen, muss der Telekommunikationsanbieter millisekundengenau das Internetverhalten eines Nutzers speichern, insbesondere auch die aufgerufenen Webseiten.

Es liegt auf der Hand, dass das Bewusstsein von dieser Protokollierung einen erheblichen Einschüchterungs- und Abschreckungseffekt bei der Benutzung des Internets erzeugt. Wie schon zuvor bei der Pressefreiheit, ist auch hier zu bedenken, dass grundsätzlich das Verhalten eines jeden Internetnutzers, ohne dass dieser dazu einen rechtlichen Anlass gegeben hätte, vorsorglich protokolliert wird. Der so erzeugte Eingriff in die Informations- und Meinungsbildungsfreiheit lässt sich durch das Ziel, gegebenenfalls Informationen in Bezug auf besonders schwerer Straftaten zu gewinnen, nicht mehr rechtfertigen, weil der Grundrechtseingriff praktisch jeden Bürger treffen kann

7.3. Ergebnis zu Art. 5 Abs. 1 S. 1 GG

§ 113 b Abs. 3 TKG verletzt das Grundrecht der Beschwerdeführer aus Art. 5 Abs. 1 S. 1 in Gestalt der Informations-und Meinungsbildungsfreiheit.

8 Verletzung des Grundrechts auf informationelle Selbstbestimmung

Soweit die Erhebung der Standortdaten gemäß § 113b Abs. 4 TKG nicht zu einer Verletzung des Schutzbereiches des Art. 10 Abs. 1 GG führt, wird höchst vorsorglich die Verletzung von Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG in der Gestalt des Grundrechts auf informationelle Selbstbestimmung gerügt. Es wird grundsätzlich davon ausgegangen, dass die Erhebung der Bezeichnungen der Funkzellen die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt wurden, sowie derjenigen, die bei Beginn der Internetverbindung genutzt wurden, zu denjenigen Daten eines konkreten Telekommunikationsvorganges gehören, die in den Schutzbereich des Art. 10 Abs. 1 GG fallen. Sollte dies nicht der Fall sein, so greift wegen des Spezialitätsverhältnisses des Art. 10 Abs. 1 GG zu Art. 2 Abs. 1 GG das Grundrecht aus letzterer Vorschrift. Hinsichtlich der

[142] Oben S. 44ff. – 5.3.5.2

Rechtfertigung des Eingriffs wird auf die Ausführungen zu Art. 10 Abs. 1 GG verwiesen.

9 Begründung des Antrages auf Vorlage an den Europäischen Gerichtshof.

Nach Art. 15 Abs. 1 der Richtlinie 2002/58/EG hat der nationale Gesetzgeber einen Umsetzungsspielraum bei der Einführung von Maßnahmen der Strafverfolgung und Gefahrenabwehr. In diesem Rahmen kann das Bundesverfassungsgericht unmittelbar die Verletzung von deutschem Verfassungsrecht prüfen.[143] Nach hier vertretener Auffassung ist das Ergebnis der Prüfung der angegriffenen Vorschriften am Maßstab der Grundrechte des Grundgesetzes bereits negativ. Folgte das Bundesverfassungsgericht diesem Ergebnis, so bedürfte es keinerlei Überprüfung an den Maßstäben der europäischen Grundrechte-Charta.

Sollte das Bundesverfassungsgericht zu diesem Ergebnis nicht gelangen, so käme es für seine Entscheidung darauf an, ob die Grundrechte der Grundrechte Charta zur Unwirksamkeit der angegriffenen Vorschriften führen.

Als Gericht, gegen dessen Entscheidung Rechtsmittel nicht mehr möglich sind, ergäbe sich in diesem Falle die Vorlagepflicht des Gerichtes aus Art. 267 AEUV.

Starostik

- Rechtsanwalt –

Anlage: Schriftliche Vollmachten für dieses Verfahren

[143] BverfG 02.03.2010 – 1BvR 256/08 u.a. – Orientierungssatz 1b. und Rn 181f. mwN