Terrorismusbekämpfung als Waffe gegen Alltagskriminalität – Argumentation und Wirklichkeit der Vorratsdatenspeicherung in Deutschland*

Mathias Bug

> „Vorratsdatenspeicherung hat mit Terrorismusbekämpfung relativ wenig zu tun. Ich wäre für die Vorratsdatenspeicherung auch dann, wenn es überhaupt keinen Terrorismus gäbe."[1]

1. Die Vorratsdatenspeicherung in der Debatte um neue Sicherheitsmaßnahmen

In Reaktion auf die islamistischen Anschläge in den USA am 11. September 2001, in Madrid 2004 und London 2005 wurden Gesetze mit weitreichenden Kompetenzen für Sicherheitsbehörden in außergewöhnlichem Tempo verabschiedet.[2] Gerade durch die breite Nutzung von Informations- und Kommunikationstechnologien (IKT) bekommen die Maßnahmen einen umfassenden und in die Privatsphäre der Gesamtgesellschaft eingreifenden Charakter. Die verfassungsgerichtliche Prüfung stellt dabei nach 9/11 (wie auch bereits zuvor) immer wieder einen Schutzwall vor zu tiefen Eingriffen in die Persönlichkeitsrechte der Bürger dar.[3] Das wohl prominenteste Beispiel dafür ist die Vorratsdatenspeicherung (VDS).[4] Obwohl das Bundesverfassungsgericht die deutsche Umsetzung der VDS im März

* Dieser Beitrag entstand im Rahmen des Forschungsprojektes „Sicherheit im öffentlichen Raum" (SIRA) an der Universität der Bundeswehr München und wurde am DIW Berlin grundlegend überarbeitet. Das Forschungsprojekt wurde im Zuge der Bekanntmachung der Förderlinie „Gesellschaftliche Dimensionen der Sicherheitsforschung" im Rahmen des Programms „Forschung für die zivile Sicherheit" der Bundesregierung vom Bundesministerium für Bildung und Forschung (BMBF) gefördert.

1 *Dieter Wiefelspütz*, innenpolitischer Sprecher der SPD-Bundestagsfraktion. Eintrag auf abgeordnetenwatch.de vom 11. November 2007, http://www.abgeordnetenwatch.de/dr_dieter_wiefelspuetz-650-5785--f78879.html (Abruf am 21. Oktober 2013.)

2 Eine kritische Würdigung zur vermeintlichen Auslöserrolle von 9/11 und zur Dauer von Gesetzgebungsprozessen findet sich in *Jasmin Riedl*, Policy Timing nach 9/11. Die strategische Nutzung politischer Zeit, Baden-Baden 2015.

3 Vgl. *Viola Schmid*, 2. SIRA Conference Series: Innere Sicherheit – auf Vorrat gespeichert?, in: *Mathias Bug* / *Ursula Münch* / *Viola Schmid* (Hrsg.), Innere Sicherheit – auf Vorrat gespeichert?, München 2011, S. 2 – 11, S. 5, http://athene-forschung.unibw.de/doc/89818/89818.pdf (Abruf am 12. Oktober 2012); *Gerrit Hornung*, Datenschutz – nur solange der Vorrat reicht?, in: *Andreas Busch* / *Jeanette Hofmann* (Hrsg.), Politik und die Regulierung von Information, Baden-Baden 2012, S. 377 – 407, S. 377.

4 Richtlinie 2006/24/EG spezifiziert die Speicherung von Stamm- und Verkehrsdaten, die in der Kommunikation via Telefon und Internet anfallen und sechs bis 24 Monate lang zu speichern sind. Siehe dazu auch *Gerrit Hornung*, a.a.O. (Fn. 3), S. 378 f. Eine grundsätzliche juristische Einordnung der Vorratsdatenspeicherung aufbauend auf dem Urteil des BVerfG bieten *Alexander Roßnagel*, Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung", in: NJW, 63. Jg. (2010), H. 18, S. 1238 – 1242; *Viola Schmid*, a.a.O. (Fn. 3); *Alexander Roßnagel* / *Antonie Moser-Knierim* / *Sebastian Schweda*, Interessenausgleich im Rahmen der Vorratsdatenspeicherung, Baden-Baden 2013.

Zeitschrift für Parlamentsfragen (ZParl), Heft 3/2016, S. 670 – 692, DOI: 10.5771/0340-1758-2016-3-670

2010[5] außer Kraft setzte und der Europäische Gerichtshof (EuGH) die gesamte EG-Richtlinie im April 2014 für ungültig erklärte[6], führten diese Entscheidungen keineswegs zu einem Abebben der Auseinandersetzung. Spätestens seit ihrer deutschen Wiedereinführung im Dezember 2015[7] ist die VDS aufs Neue ein Stein des Anstoßes für verbraucher-, netz-, datenschutz-, urheberrechts- und insbesondere sicherheitspolitische Akteure wie auch Inhalt höchstrichterlicher Prüfung.[8]

Typisch in den Begründungen für die Maßnahme ist der Rückgriff auf vermeintlich klar umgrenzte Tatbestände der schweren Straftaten und Deliktbereiche wie Terrorismus, Kinderpornografie, Cyberkriminalität, Organisierte Kriminalität (OK) oder Korruption. Über die Jahre hinweg wurden diese Begründungsmuster aneinandergereiht, aber auch Argument nach Argument wissenschaftlich hinterfragt.[9] Die prominente Nennung der Terrorismusbekämpfung korreliert dabei zeitlich mit den Reaktionen auf 9/11 und dann insbesondere auf die Anschläge von Madrid und London – gemeinhin wird davon ausgegangen, dass die europäische Richtlinie aus dem Jahre 2006 und ihre deutsche Umsetzung ohne die beiden Anschläge in Europa kaum denkbar gewesen wäre.[10] Es lässt sich zeigen, dass die

5 Vgl. BVerfG, 1 BvR 256 vom 2. März 2010, Absatz Nr. (1-345).

6 Vgl. Gerichtshof der Europäischen Union, Der Gerichtshof erklärt die Richtlinie über die Vorratsdatenspeicherung von Daten für ungültig, Pressemitteilung Nr. 54/14 vom 8. April 2014, curia.europa.eu/jcms/jcms/P_125953/ (Abruf am 7. Februar 2015).

7 Vgl. Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdate vom 10. Dezember 2015, in: BGBL vom 17. Dezember 2015, S. 2215.

8 Vgl. *Sebastian Bukow*, Vorratsdatenspeicherung in Deutschland – Symbol des sicherheitspolitischen Wandels und des zivilgesellschaftlichen Protests?, in: *Mathias Bug* / *Ursula Münch* / *Viola Schmid* (Hrsg.), a.a.O. (Fn. 3), S. 22 – 55, S. 23; *Gerrit Hornung*, a.a.O. (Fn. 3), S. 377. Zur Einordnung der Vorratsdatenspeicherung als sicherheitspolitische Maßnahme: *Sebastian Bukow*, ebenda, S. 41 ff.; *Dorothee Szuba*, Vorratsdatenspeicherung. Der europäische und deutsche Gesetzgeber im Spannungsfeld zwischen Sicherheit und Freiheit, Baden-Baden 2011, S. 291. Zu gesellschaftlichen Wahrnehmungsmustern siehe *Christian Lüdemann* / *Christina Schlepper*, Angst im Überwachungsstaat, in: *Sandro Gaycken* (Hrsg.), Jenseits von 1984: Datenschutz und Überwachung in der fortgeschrittenen Informationsgesellschaft, Bielefeld 2013, S. 147 – 162, S. 155; *Mathias Bug* / *Ursula Münch*, Politik verändert Internet (und Medien) – Innere Sicherheit, Vorratsdatenspeicherung und die Wahrnehmung durch die Bevölkerung; in: *Michael Schröder* (Hrsg.), Die Web-Revolution, München 2012, S. 147 – 174, S. 164 – 171; *Mathias Bug*, Innere Sicherheit – digital und vernetzt, in: *Jasmin Röllgen* (Hrsg.), „Wie die Statistik belegt…". Zur Messbarkeit von Kriminalitätsfurcht und (Un-)Sicherheit, München 2014, S. 45 – 70, https://athene-forschung.unibw.de/doc/92194/92194.pdf (Abruf am 9. Februar 2015).

9 Vgl. *Bernd-Dieter Meier*, Kinderpornographie im Internet, in: *Dieter Dölling* / *Jörg-Martin Jehle* (Hrsg.), Taten – Täter – Opfer. Grundlagenfragen und aktuelle Probleme der Kriminalität und ihrer Kontrolle, Mönchengladbach 2013, S. 374 – 391; *Arnd Hüneke*, Das Internet – ein „Milliardenmarkt" für Kinderpornographie?, in: Unimagazin. Zeitschrift der Leibniz Universität Hannover, Nr. 1/2 (2012), S. 50 – 52, http://www.uni-hannover.de/imperia/md/content/alumni/unimagazin/2012_web/netz13__hueneke.pdf (Abruf am 1. Juni 2013); *Kay Hamacher* / *Stefan Katzenbeisser*, Public Security: Simulations Need to Replace Conventional Wisdom, in: Proceedings of the 2011 Workshop on New Security Paradigms Workshop 2011, http://www.nspw.org/papers/2011/nspw2011-hamacher.pdf (Abruf am 14. Februar 2013).

10 Vgl. *Sebastian Bukow*, a.a.O. (Fn. 8), S. 39; *Gabriel Brönnimann*, Die umkämpfte Einführung der Vorratsdatenspeicherung in der EU, in: *Sandro Gaycken* (Hrsg.), Jenseits von 1984: Datenschutz und Überwachung in der fortgeschrittenen Informationsgesellschaft, Bielefeld 2013, S. 43 – 62, S. 50; *Sabine Leutheusser-Schnarrenberger*, Vorratsdatenspeicherung – Ein vorprogrammierter Verfassungskonflikt, in: ZRP, 40. Jg. (2007), H. 1, S. 9 – 15, S. 10.

wichtigsten Akteure der Inneren Sicherheit in Aussagen für eine Wiedereinführung der VDS auf vormalige Begründungsmuster alternierend zurückgreifen.[11] Allgemein überlappen sich die Begründungsmuster dabei zeitlich und erfolgen regelmäßig in Reaktion auf medial bekannt gewordene Straftaten – ohne diese jedoch empirisch in das gesamte Aufkommen an Kriminalität einzuordnen oder Aussagen über die tatsächliche Bedrohungslage zu machen.[12]

Es liegt daher nahe, dass Bemühungen, solch umfassende Überwachungsmaßnahmen zu begründen, nicht zwangsläufig die tatsächlichen polizeilichen Nutzungsbereiche widerspiegeln. Diese Argumentationskulissen müssen im Falle von Maßnahmen wie der Vorratsdatenspeicherung (wegen der hohen Grundrechtsrelevanz) einem besonderen Legitimierungsdruck standhalten. Daher wird im Folgenden die diskursive Argumentationsentwicklung in den einschlägigen Parlamentsvorgängen auf Bundesebene am Beispiel der VDS nachgezeichnet. Mit der Maßnahmenauswahl wird gleichzeitig der Mehrebenencharakter des Politikfeldes der Inneren Sicherheit deutlich. Während die Hauptkompetenz für die Innere Sicherheit bei den Ländern liegt, handelt es sich mit der VDS um ein Bundesgesetz, das gleichzeitig eng mit der Genese auf europäischer Ebene verbunden war. Daher liegt das besondere Augenmerk der vorliegenden Studie auf der Rolle des Bundestages im Zusammenspiel mit der Exekutive und dem Bundesrat. Die Analyse setzt 1996 an und beleuchtet bewusst auch erfolglos gebliebene Einführungsversuche, um die Argumentationsentwicklung in ihrer Gesamtheit abbilden zu können. Der Abgleich mit den Anlässen der polizeilichen Nutzung von IKT-Überwachungsmaßnahmen zeigt große Diskrepanzen[13], die der Erklärung bedürfen.

2. Theoretische Überlegungen

Bei der Einführung einer staatlich verordneten Speicherpflicht für Kommunikationseckdaten handelt es sich zweifelsohne um einen gewichtigen Eingriff in bürgerliche Grundrechte – andernfalls ließen sich die sehr konsequenten Entscheidungen von BVerfG und EuGH (und weiteren höchsten Gerichten in der EU) auch nicht erklären. Ganz allgemein zeichnet sich die VDS trotz der emotional bestimmten Wahl der Argumentationsmuster[14] dadurch aus, dass durch sie die Nutzung von Sicherheitsmaßnahmen in das präventive, verdachtsunabhängige Feld erweitert wird – also eine tatsächliche Veränderung zum Ziel hat, die an den kulturbedingten Grenzen deutscher Sicherheitspolitik kratzt und nicht mit dem (viel-

11 Vgl. *Hans-Jörg Albrecht* (Gesamtverantwortung), Gutachten der kriminologischen Abteilung des Max-Planck-Instituts für ausländisches und internationales Strafrecht im Auftrag des Bundesamtes für Justiz zu möglichen Schutzlücken durch den Wegfall der Vorratsdatenspeicherung, Freiburg im Breisgau 2011, S. 85 – 86, http://vds.brauchts.net/MPI_VDS_Studie.pdf (Abruf am 3. März 2013).

12 Diese Kritik wird auch insgesamt zur EU-Agitation im Bereich Inneres und Justiz geteilt. Vgl. *Dominik Brodowski*, Innere Sicherheit in der Europäischen Union, in: JURA, 35. Jg. (2013), H. 5, S. 492 – 504, S. 494.

13 Die Daten veröffentlicht das Bundesministerium der Justiz für die Zeit ab 2000.

14 So auch verallgemeinernd zur Argumentation der EU im Bereich der Inneren Sicherheit *Dominik Brodowski*, a.a.O. (Fn. 12), S. 494.

leicht sogar beschwichtigenden) Vorwurf von Symbolpolitik belegt werden kann.[15] Dieser Umstand verdeutlicht gleichzeitig, dass es sich bei der Einführung einer Vorratsdatenspeicherung um einen signifikanten Schritt in Richtung einer „Versicherheitlichung" des Kommunikationsgebarens der Bevölkerung handelt. Im Laufe der letzten Jahre wurde bereits mehrfach dieser theoretische Ansatz der so genannten securitisation, auf den Bereich der Inneren Sicherheit[16] und insbesondere auf die Einführung solcher deutlich einschneidenden Maßnahmen angewandt.

Der Ansatz kommt ursprünglich aus dem Forschungsbereich der Internationalen Beziehungen Ende der 1990er Jahre[17] und gewann dort insbesondere nach den terroristischen Anschlägen 2001 an Bedeutung. Securitisation richtet den Blick auf so genannte securitising moves, sicherheitsbezogene Aktionen. Dabei bedarf es eines „securitising actors" (beispielsweise ein Innenminister), der eine Bedrohung als existenziell für eine bestimmte Gruppe oder auch Gesellschaft beschreibt (das so genannte referent object) und mit einer erweiterten Sicherheitsmaßnahme (so genannte extraordinary measures) zum Schutz dieses Referenzobjektes verbindet. Wird die „Existentialisierung" einer Bedrohung vom Publikum (zum Beispiel der Bevölkerung, den Medien oder auch dem Bundestag beziehungsweise den Koalitionsfraktionen) akzeptiert, kann die Maßnahme umgesetzt werden.[18]

Der Verlauf der Diskussion um die Vorratsdatenspeicherung weist mehrere Etappen an sicherheitsbezogenen Aktionen auf. Um deren Erfolgspotential analysieren zu können, werden in diesem Beitrag erfolgreiche und erfolglose Ansätze zur Einführung der VDS integriert. Damit wird das ursprüngliche Konzept, das sich eher auf erfolgreiche Schritte der Versicherheitlichung konzentriert, mit dem Ziel einer empirischen Offenheit für Argumentationsveränderungen ausgeweitet. Dabei stellt sich heraus, dass nicht nur der Argumentationsrahmen an den zeitlichen Kontext angepasst wird, sondern sich auch die Akteurskonstellationen unterscheiden. Es handelt sich dann wohl – wie in Abschnitt 3 zu zeigen sein wird – bei variierenden Einzelargumenten sozusagen um ein alternierendes Referenzobjekt. Das Ziel der Sprecher, vornehmlich Akteure aus dem Bereich der Inneren Sicherheit[19], ist eine enge diskursive Kopplung der Referenzobjekte mit der Maßnahme (VDS). Dabei stellt

15 Vgl. *Hendrik Hegemann* / *Martin Kahl*, Politische Entscheidungen und das Risiko Terrorismus, in: *Christopher Daase* / *Philipp Offermann* / *Valentin Rauer* (Hrsg.), Sicherheitskultur, Frankfurt am Main / New York 2013, S. 159 – 181, S. 163 ff., 174 f.

16 Vgl. *Bernhard Frevel* / *Christoph Riederer*, Abschlussbericht zur Medien- und Diskursanalyse im Rahmen des Arbeitspakets 02: Sozialwissenschaftliche Aspekte – Fankultur, Wahrnehmung und Diskurs des Forschungsprojekts SiKomFan. Mehr Sicherheit im Fußball – Verbessern der Kommunikationsstrukturen und Optimieren des Fandialogs, Münster 2014, https://www.fhoev.nrw.de/uploads/media/Frevel-Riederer_Abschlussbericht_SiKomFan_Medienanalyse.pdf (Abruf am 12. Mai 2015), S. 122 – 124.

17 Vgl. *Barry Buzan* / *Ole Wæver* / *Jaap de Wilde*, Security: A New Framework for Analysis, Boulder 1997.

18 Vgl. *Susanne Fischer* / *Carlo Masala* / *Philippp Klüfers* / *Katrin Wagner*, (Un-)Sicherheitswahrnehmung und Sicherheitsmaßnahmen im internationalen Vergleich, in: Schriftenreihe Forschungsforum öffentliche Sicherheit, Nr. 14 vom März 2014, http://www.sicherheit-forschung.de/publikationen/schriftenreihe_neu/sr_v_v/sr_14.pdf (Abruf am 9. Januar 2015), S. 15 ff.

19 Insbesondere durch den europäischen Charakter der VDS ließe sich die Gruppe an zentralen Akteuren freilich erweitern, ähnlich dem vielmehr professionellen als politischen Netzwerk wie *Diedier Bigo*, Delivering Liberty and Security?, in: *ders.* / *Sergio Carrera* / *Elspeth Guild* / *R.B.J. Walker* (Hrsg.), Europe's 21st Century Challenge. Delivering Liberty, London 2010, S. 388 – 420, S. 396 es für inter-/supranationale Zusammenarbeit in der Sicherheitspolitik konzeptualisiert.

die Maßnahme eine Konstante dar, zu deren Gunsten mit securitising moves (also dem Rückgriff auf die spezifischen Argumentationslinien) ein alltägliches Werkzeug der parlamentarischen, aber auch (insbesondere nach dem Urteil des BVerfG und des EuGH) gesellschaftlichen Mehrheitsbeschaffung verbunden wird. Durch die alternierende und kumulierte Policy-Begründung der letzten Jahre kann also nicht mehr von einem diskursiven Rückgriff auf Ausnahme- oder auch Notstandssituationen (was beispielsweise im Terrorkontext der Jahre 2005/2006 zur Verabschiedung der Richtlinie zur Vorratsdatenspeicherung nahe lag), wie sie der securitisation-Ansatz eigentlich vorsieht, gesprochen werden. Durch die hier vorgenommene Konzeptualisierung wird der analytische Blick des Ansatzes am Beispiel der VDS über die ausschließliche Anti-Terror-Begründung hinaus erweitert. So gerät zwangsläufig die gesamte Argumentationsgenese in das Blickfeld, was den singulären Einfluss des Terrorarguments erst messbar macht.[20]

Ausgehend von der Annahme, dass der VDS im Speziellen und der Telekommunikationsüberwachung im Allgemeinen für die Bekämpfung von spezifischen Kriminalitätsformen eine besondere Bedeutung zukommt, wird in einem zweiten Schritt die tatsächliche Nutzung von Kommunikationsdaten zwischen 2000 und 2014 den Begründungsmustern der offiziellen politischen Argumentationslinie gegenüber gestellt.

Empirisch ergibt sich dabei ein Problem. Die Nutzung der Vorratsdaten war über die Katalogstraftaten des §100 a StPO geregelt. Hier war entsprechend auch feingliedrig vorgeschrieben, unter welchen Umständen welche Vorratsdaten genutzt werden dürfen. Da die Eingriffstiefe in die Privatsphäre bei der Preisgabe so genannter Stammdaten (beispielsweise Inhaber eines Telefonanschlusses) weniger tief ist als die Nutzung von so genannten Verkehrsdaten (mit denen ganze Bewegungsprofile oder auch individuelle Netzwerke analysiert werden können), lagen auch die Hürden – oder die Schwere der Verdachtsmomente – unterschiedlich. Die verpflichtende Dokumentation der behördlichen Nutzung von Verkehrsdaten zu Ermittlungszwecken erfordert jedoch keine Auflistung nach den verschiedenen Katalogstraftaten des § 100a StPO, in dem die für diesen Beitrag zentralen Straftaten mit besonderer Schwere enthalten sind. Im Folgenden wird daher der Umweg über die detaillierte Dokumentation zur Telekommunikationsüberwachung (TKÜ) gewählt. Diese wird ebenfalls jährlich dokumentiert und listet die einzelnen Einsatzbereiche nach §100 a StPO auf. Der hier vorgenommene Analogieschluss ist also auf Nutzungstendenzen von IKT-Maßnahmen im Kontext von schweren Straftaten gerichtet. Die mit TKÜ und Verkehrsdatenabfrage verbundene signifikante Eingriffstiefe in Persönlichkeitsrechte verdeutlicht, dass es um die Überprüfung einer Argumentation aus dem Blickwinkel der securitisation geht, wo es ja gerade die schweren Anlässe sind, die das Existentielle an einer ins Feld geführten Bedrohung ausmachen. Eine 2008 veröffentlichte umfassende Studie im Auftrag der Bundesregierung zeigt zwar einerseits die Grenzen des formulierten Vorgehens auf, verdeutlicht aber andererseits ebenso, wie wichtig es ist, eine Analyse auf Grundlage statistischer Längsschnittdaten vorzunehmen. Ebendies ist bisher lediglich mittels der TKÜ-Daten möglich.[21]

Zusammenfassend wird argumentiert, dass eine Einführung der VDS einer securitisation-Logik insoweit folgt, als hauptsächlich moralisch-normativ nicht hinterfragbare Straftaten als Begründungsfolie herangezogen werden (und insoweit eine permanente Ausnahme-

20 Ganz allgemein zur Rolle der Terrorismusbegründung für Sicherheitsmaßnahmen nach 9/11 vgl. *Dorothee Szuba*, a.a.O. (Fn. 8), S. 28 f.

21 Vgl. BT-Drs. 16/8434 vom 28. Februar 2008.

situation behauptet wird). Eine deutliche Entkoppelung der politischen Begründung von der tatsächlichen Nutzung der Überwachung von Telekommunikation kann jedoch empirisch im vierten Kapitel nachgewiesen werden. Daraus entstehen delegitimierende Effekte für die Sicherheitsmaßnahme der Vorratsdatenspeicherung, da deren proklamierte Ziele mit der Nutzungsrealität nicht in Einklang stehen dürften. Das Ausmaß und die Dauer der Diskussion um die Vorratsdatenspeicherung machen diese Diskrepanz deutlich, was nur mit einer transparenteren Argumentation aufgedeckt werden kann.

3. Entwicklung der Argumentationsmuster für die Vorratsdatenspeicherung

Die Argumente für die VDS wurden seit 1996 einerseits kontinuierlich weiterentwickelt, andererseits finden sich zentrale Gefahrenszenarien regelmäßig wieder. Inspiziert man die verschiedenen Versuche politischer Akteure, Mindestspeicherfristen beziehungsweise VDS[22] einzuführen, zeigt sich, dass die Vorstellungen zu den Nutzungsmodalitäten auch die Argumentationslinien für die VDS vorstrukturierten und erweiterten. Versuche einer rechtlichen Verankerung beziehungsweise dessen Agenda-Setzung erfolgten 1996, 1999, 2000, 2001, 2002, 2003, 2006, 2007, 2010, 2012 und 2015. Die empirische Basis für diese Zusammenschau besteht hauptsächlich in Drucksachen von Bundesrat und Bundestag.[23] Ausgehend von einer Dokumentenanalyse im Rahmen der Umsetzungsgesetzgebung der EG-Richtlinie zur Vorratsdatenspeicherung im Jahr 2007 konnten Quellen zu vorangehenden Initiativen bis in das Jahr 1996 zu Zeiten der Deregulierung des deutschen Telekommunikationsmarktes zurückverfolgt werden. Bekanntlich war damals das Kommunikationsgebaren in der deutschen Bevölkerung ein anderes, die Abhängigkeit vom Internet war deutlich niedriger, Telekommunikation war weniger mobil und bot daher nur bedingt die Möglichkeit von Bewegungsprofilen. Entsprechend fiel die Eingriffstiefe einer Vorratsdatenspeicherung niedriger aus. Dennoch haben diese Vorgängermaßnahmen den oben genannten vorstrukturierenden Effekt für die neuere Diskussion rund um die Vorratsdatenspeicherung entfaltet.

1996: Telekommunikationsgesetz

Im Rahmen der Liberalisierung des Telekommunikationsmarktes entstand 1996 das Telekommunikationsgesetz (TKG)[24] – die endgültige Fassung geht in weiten Teilen auf den Gesetzentwurf der Regierung sowie wortgleich der Fraktionen CDU/CSU, FDP und SPD

22 Über den gesamten Beobachtungszeitraum hinweg verändert sich die konkrete Bezeichnung. Im Bundestagswahlkampf wurde diese Tatsache dann auch in der Breite thematisiert, als das Wort Vorratsdatenspeicherung im CDU/CSU-Wahlprogramm nicht mehr vorkam *Peter Müller*, Reaktion auf NSA-Skandal: Union rückt von Vorratsdatenspeicherung ab, in: Spiegel Online vom 5. Juli 2013, http://tinyurl.com/nf4h7pl (Abruf am 21. Oktober 2013).

23 Es wird hauptsächlich auf die online gestellten Dokumente zurückgegriffen. Insbesondere für den Bereich des Bundesrates sind damit jedoch Einschränkungen in der Analyse des Stimmverhaltens einzelner Länder verbunden. Eine detaillierte Analyse zur Agitation einzelner Länder im Politikfeld Innere Sicherheit findet sich bei *Jasmin Riedl*, a.a.O. (Fn. 2).

24 Vgl. Telekommunikationsgesetz vom 25. Juli 1996, BGBl. I vom 31. Juli 1996, S. 1120 – 1151, S. 1120.

zurück. Hier traf der Gesetzgeber in den §§ 86 und 87 TKG Regelungen zum Datenschutz und zur Datenweitergabe an Sicherheitsbehörden, die das TKG-Begleitgesetz 1998 weiter konkretisierte.[25] Der Bundesrat versuchte, mit der Argumentation sich ausbreitender Organisierter Kriminalität im wachsenden Telekommunikationssektor weit reichende Überwachungsmöglichkeiten wie Mindestspeicherfristen von Verkehrsdaten umzusetzen. Er begründete dies in seiner Vorab-Stellungnahme zum Gesetzentwurf (nach Art. 76 II GG) damit, dass sicherheitspolitische „Maßnahmen zur Überwachung privater Telekommunikationsnetze bisher unzulässig" seien und es daher anzunehmen sei, dass „die internationale Kriminalität, die Wirtschafts- sowie die Organisierte Kriminalität sich dieser Netze […] bedienen" würden.[26] Hinzu träte die Möglichkeit, dass der rasant wachsende Telekommunikationsmarkt für die Anlage kriminell erworbener Gelder genutzt werde. Die Bundesregierung lehnte das Ansinnen jedoch mit dem Verweis auf das Prinzip der Verhältnismäßigkeit in ihrer Entgegnung zur Stellungnahme des Bundesrats ab.[27] Der Bundesrat ließ schließlich an diesem Punkt von seinem Ansinnen ab, weshalb Mindestspeicherfristen auch nicht Inhalt im Vermittlungsausschuss waren.[28]

Das Thema Datenschutz spielte in den Lesungen zum TKG eine sehr geringe Rolle. Lediglich *Manuel Kieper* von den Grünen[29] und *Gerhard Jüttemann* von der PDS[30] bezogen sich in ihren Redebeiträgen kritisch auf die Paragraphen zum Datenschutz. *Jüttemann* führte sogar den Vergleich mit *George Orwell*s 1984 ins Feld. *Arne Börnsen* (SPD) hingegen sah in den Regelungen zum Datenschutz lediglich die Übertragung der Datenschutzvorkehrungen aus anderen Bereichen wie dem Straßenverkehr.[31] Im Gesetzgebungsprozess fielen die Länder durch ihre anfängliche Forderung nach Mindestspeicherfristen auf – ein Befund, der die Landeskompetenz in der Inneren Sicherheit unterstreicht und darüber hinaus auf eine Große Koalition der Inneren Sicherheit zwischen SPD- und CDU/CSU-Regierungen hinweist.[32]

Mit dem Verweis auf internationale und Organisierte Kriminalität sowie auf Wirtschaftskriminalität wird der Eindruck erweckt, dass es sich um klar abgegrenzte Deliktfelder handelt; diese greifen aber vielmehr ineinander.[33] Bereits die Definition der Organisier-

25 Vgl. *Fabian Schuster*, Beck'scher TKG-Kommentar, München 2006, Rn. 10.
26 BT-Drs. 13/4438 vom 23. April 1996, S. 6.
27 Vgl. ebenda, S. 39. Das Gegenargument der Verhältnismäßigkeit wird auch im weiteren Verlauf bis einschließlich 2005 als kritisches Hauptargument beibehalten.
28 Vgl. BR-Drs. 425/1/96 vom 12. Juni 1996 (keine Forderung zu § 86 TKG mehr enthalten) sowie BR-Drs. 13/4938 vom 17. Juni 1996.
29 Vgl. BT-PlPr. 13/110 vom 13. Juni 1996, S. 9794.
30 Vgl. ebenda, S. 9797.
31 Vgl. ebenda, S. 9800.
32 Vgl. *Martin Kutscha*, Große Koalition der Inneren Sicherheit, in: CILIP Bürgerrechte & Polizei, 59. Jg. (1998), H. 2, S. 57 – 69; *Sebastian Bukow*, a.a.O. (Fn. 8); *Mathias Bug* / *Jasmin Röllgen*, Internal Security Institutions Meeting Internet Governance – A Comparative View on the UK and Germany, in: JeDEM, 3. Jg. (2011), H. 3, S. 59 – 74.
33 Internationale Kriminalität sowie Wirtschaftskriminalität werden an und für sich unter die Organisierte Kriminalität (OK) subsumiert. Es ist daher davon auszugehen, dass durch die Aufzählung verschiedener Bereiche innerhalb der OK, dem Argument zusätzlich Gewicht verliehen werden soll. Der Begriff der OK ist auch bereits kein trennscharfer Begriff. Siehe hierzu *Klaus von Lampe*, Was ist „Organisierte Kriminalität"?, in: APuZ, 63. Jg. (2013), H. 38/39, S. 3 – 15.

ten Kriminalität bündelt eine Vielzahl an denkbaren Straftaten[34], deren Summe an Delikten im Gegensatz zur oben zitierten Prognose des Bundesrats in den letzten zwei Jahrzehnten recht konstant geblieben ist.[35]

1999: Gesetzentwurf zur Änderung des Gesetzes über Fernmeldeanlagen

In einem Entwurf für ein Gesetz zur Änderung des Gesetzes über Fernmeldeanlagen[36] forderten Abgeordnete der CDU/CSU-Fraktion die Bindung an den Straftatenkatalog von § 100a StPO aufzuweichen. Ihr Vorstoß ging auf die Aktivitäten des Bundesrates und aller Landesjustizminister zurück.[37] Ziel war es, die Abfragehürden von gespeicherten Kommunikationsdaten für Sicherheitsbehörden bei Delikten außerhalb des Straftatenkatalogs aus §100a StPO zu reduzieren. Als Begründung wurde dringender Handlungsbedarf (was im Duktus der Versicherheitlichung am ehesten der diskursiven Herbeiführung von „urgency" entspräche) ins Feld geführt: „Im Vordergrund stehen hier belästigende und beleidigende Anrufe, bei denen das Auskunftsersuchen ein wichtiges Instrument der Sachaufklärung und Beweissicherung ist. Zum Beispiel bei massiven Beleidigungen von Frauen am Telefon (kein Katalogdelikt des § 100a StPO) muss der Anrufer über § 12 FAG festgestellt werden können."[38]

In diesem Vorhaben ist zweifelsohne ein erster Versuch zu sehen, die Hürden für die Abfrage von Verkehrsdaten insbesondere im Falle von IKT-gestützten Straftaten zu senken. Dieses Ziel wurde jedoch erst mit der Richtlinienumsetzung zur VDS 2007 erreicht, denn der Gesetzentwurf erhielt 1999 im Bundestag keine Mehrheit. Im folgenden Jahr rückten wieder die Speicherzeiten ins Zentrum des Interesses.

2000: Telekommunikations-Datenschutzverordnung (TDSV)

Die Vorlage der Bundesregierung zur TDSV sah eine Höchstgrenze der Speicherung von Kommunikationsdaten von sechs Monaten vor. In seiner Stellungnahme wollte der federführende Wirtschaftsausschuss im Bundesrat die Speicherdauer grundsätzlich auf drei Monate verkürzen.[39] Das Plenum der Länderkammer folgte am 29. September 2000 jedoch dem abweichenden Votum des Innenausschusses, der durch die Empfehlung des Wirtschaftsausschusses „die Arbeit der Strafverfolgungsbehörden unangemessen beeinträchtigt"[40] sah.

34 Vgl. Bundeskriminalamt, Bundeslagebild Organisierte Kriminalität 2002, S. 6 ff.; dies., Bundeslagebild Organisierte Kriminalität 2011, S. 8, http://www.bka.de/nn_193314/DE/Publikationen/JahresberichteUndLagebilder/OrganisierteKriminalitaet/organisierteKriminalitaet__node.html?__nnn=true (Abruf jeweils am 9. Juni 2013); *Karlhans Liebl*, Organisierte Kriminalität, in: *Hans Jürgen Lange* / *Peter Ohly* / *Jo Reichertz* (Hrsg.), Auf der Suche nach neuer Sicherheit, Wiesbaden 2009, S. 63 – 74, S. 64.

35 Vgl. Bundeskriminalamt, Bundeslagebild Organisierte Kriminalität, a.a.O. (Fn. 34), S. 5; dies., Bundeslagebild Organisierte Kriminalität 2011, a.a.O. (Fn. 34), S. 9.

36 Vgl. BT-Drs. 14/1315 vom 29. Juni 1999.

37 Vgl. ebenda, S. 2.

38 Ebenda.

39 Vgl. BR-Drs. 300/2/00 vom 19. September 2000, S. 3; *Matthias Spittmann*, Sind wir nicht alle Cyber-Kriminelle?, in: TAZ vom 29. September 2000, S. 8.

40 BR-Drs. 300/2/00, a.a.O. (Fn. 39), S. 4.

In der Verordnungsbegründung selbst wurden keine Interessen der Strafverfolgungsbehörden vermerkt, sondern lediglich abstrakt mit den neuartigen Erfordernissen im Telekommunikationsmarkt argumentiert.[41] Dass die Höchstgrenze der Speicherungsfristen bei sechs Monaten verblieb, sah der hessische Datenschutzbeauftragte bereits als Problem und befürchtete, dass sich daraus eine Regelfrist entwickeln würde – eine durchaus begründete Furcht, wie sich zeigen sollte.[42]

2001: Ministerrat der Europäischen Union für Justiz und Inneres – Reaktionen auf 9/11

In den Fokus der europäischen Ebene geriet die elektronische Kommunikation in einer ersten Reaktion auf die Terroranschläge des 11. September 2001. In den Schlussfolgerungen des Rates für Justiz und Inneres wurde die Kommission aufgefordert, Vorschläge zu entwickeln, wie Straftaten mittels Telekommunikation besser geahndet werden können. Eine Konkretisierung auf die Verkehrsdaten erfolgte aber erst im Jahr darauf.[43] Die 2001 gesetzten Grundlagen führten in unmittelbarer Folge der Anschläge von Madrid 2004 erstmals zur konkreten Forderung des Europäischen Rats nach einer VDS.[44] Dieser deutliche Terrorismusbezug blieb in der folgenden breiten (wissenschaftlichen) Diskussion rund um die VDS prominent bestehen. Dies erklärt sich insbesondere durch die Verabschiedung der Richtlinie 2006/24/EG, die unter britischer Ratspräsidentschaft nach den Anschlägen von London 2005 verwirklicht wurde. Interessanterweise hatte der Bundestag sich im Zusammenhang mit den Tätigkeitsberichten des Bundesbeauftragten für den Datenschutz (BfD) für die Jahre 2001 und 2002 einstimmig auf eine Resolution geeinigt, der zufolge sich die Bundesregierung auf europäischer Ebene gegen eine VDS stellen sollte. Diesen Auftrag wiederholte der Bundestag 2005[45], als sich die europäische Harmonisierung – unterstützt durch das Bundesjustizministerium – bereits abzeichnete.[46]

2002: Gesetzentwurf zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Maßnahmen

Die nach 9/11 alles überschattende Terrorismusargumentation zur VDS wurde durch einen Gesetzentwurf des Bundesrates eingeschränkt, der auf einen Antrag der rot-grünen Landesregierung Niedersachsens zurückging.[47] Darin forderte der Bundesrat explizit, eine Vorrats-

41 Vgl. BR-Drs. 300/00 vom 19. Mai 2000, S. 16 ff.
42 Vgl. *Friedrich von Zezschwitz,* Neunundzwanzigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten vorgelegt zum 31. Dezember 2000, http://www.datenschutz.hessen.de/_old_content/tb29/inhalt.htm (Abruf am 5. Juli 2013).
43 Vgl. *Sabine Leutheusser-Schnarrenberger*, a.a.O. (Fn. 10), S. 10.
44 European Council, Declaration on Combatting Terrorism vom 25. März 2004, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/79637.pdf (Abruf am 9. Juni 2013), S. 4.
45 Vgl. *Stefan Krempl* / *Jürgen Kuri*, Bundestag bleibt bei Nein zur Vorratsspeicherung von Verbindungsdaten, in: heise-online vom 25. Januar 2005, http://tinyurl.com/q6bjsbb (Abruf am 9. Juni 2013).
46 Vgl. *Gerrit Hornung*, a.a.O. (Fn. 3), S. 382.
47 Vgl. BR-Drs. 275/02 vom 27. März 2002.

datenspeicherung einzuführen, wenngleich dies etwas versteckt nicht bereits im Problemaufriss und den Lösungsansätzen des Gesetzentwurfes genannt wurde.

Der eigentliche Gegenstand – sexueller Missbrauch von Kindern – geriet dabei bereits aus den Augen, da für Zwecke der Strafverfolgung und Gefahrenabwehr bei diversen Sicherheitsbehörden Mindestspeicherfristen in das Telekommunikationsgesetz (§ 86 I 3, wie es der Bundesrat bereits 1996 im Rahmen der Erstellung des TKG gefordert hatte) aufzunehmen seien.[48] Die Problematik des Kindesmissbrauchs fungiert also als mittelbares Referenzobjekt, das mit dem securitising move (der Einführung einer Vorratsdatenspeicherung) nicht explizit verbunden wird. Die Einführung von Mindestspeicherfristen fand jedoch nicht die Zustimmung der Koalition im Bundestag, was vor allem an den sehr weitreichenden Eingriffsbefugnissen lag.[49]

Trotz des zeitlichen Zusammenhangs der Gesetzesinitiative mit den Anschlägen von 9/11 und den europäischen Forderungen nach einer VDS wurde hier auf die Begründungsfolie des Kampfes gegen Terrorismus an keiner Stelle zurückgegriffen. Es gab zwar zeitgleich weitere Gesetzesinitiativen mit klarem Terrorismusbezug, jedoch stand der Gesetzentwurf des Bundesrates quer zur allgemeinen Auffassung, nach 9/11 sei der Kampf gegen den Terrorismus zur übermächtigen Handlungsmaxime in der Inneren Sicherheit allgemein und insbesondere bei Forderungen nach weitreichenden Überwachungsmaßnahmen geworden.

2003: Neuauflage des TKG

Auch 2003 verlangte der Bundesrat – wie bereits 1996 – eine Mindestspeicherung von anfallenden Verkehrsdaten für sechs Monate.[50] In der Begründung wurde zwar auf die vorangegangen Bestrebungen hingewiesen, dabei jedoch nur auf „die Bedürfnisse einer effektiven Strafverfolgung und wirksamen Gefahrenabwehr“[51] abgestellt. Die Forderung konnte sich im weiteren Verfahren jedoch nicht durchsetzen. Interessanterweise fand 2003 das Argument einer verbesserten Terrorismusbekämpfung wie bereits im Vorjahr keine gesonderte Erwähnung in der Beschlussfassung mehr. In dieser Phase scheint das Konzept der securitisation also gänzlich für die Erklärung eines securitising moves (oder besser: eines Versuchs dazu) zu versagen.

2006: Bundestagsresolution

Ein Jahr nach der oben genannten deutlich einschränkenden Bundestagsresolution gegen eine europaweite Einführung der VDS arbeitete die nunmehr schwarz-rote Bundesregierung unter Federführung des Bundesjustizministeriums dennoch auf eine europäische Eini-

48 Vgl. BT-Drs. 14/9801 vom 17. Juli 2002, S. 8.
49 Vgl. ebenda, S. 15 f.
50 Vgl. BR-Drs. 755/03 vom 17. Oktober 2003, S. 33. In den Empfehlungen der Ausschüsse war alternativ auch die Möglichkeit einer zwölfmonatigen Speicherfrist vorgesehen. Vgl. BR-Drs. 755/2/03 vom 19. Dezember 2003, S. 35 f.
51 BR-Drs. 755/03, a.a.O. (Fn. 50), S. 34. Lediglich in den vorangegangenen Ausschussempfehlungen fand eine umfassendere Begründung unter Rückgriff auf die Themen Terrorismusbekämpfung und Kindesmissbrauch (in Zusammenhang mit der oben genannten Gesetzesinitiative aus dem Jahr 2002) statt. BR-Drs. 755/2/03, a.a.O. (Fn. 50), S. 36.

gung hin.[52] Der Problemaufriss der Beschlussempfehlung, die die Bundesregierung für die weitere Aushandlung einer Richtlinie zur VDS anleiten sollte, schrieb die europäische Regelung dem „Ziel der Erleichterung der Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten wie Terrorismus und organisierter Kriminalität“[53] zu. Der angenommene Antrag der Regierungsfraktionen hingegen sah die Argumentationszusammenhänge etwas breiter und berücksichtigte zusätzlich allgemeine Straftaten mittels Telekommunikation: „Zur Aufklärung von Straftaten mit komplexen Täterstrukturen, wie sie für den internationalen Terrorismus und die Organisierte Kriminalität kennzeichnend sind, und von mittels Telekommunikation begangenen Straftaten ist dieses Ermittlungsinstrument unverzichtbar.“[54]

Es kam 2006 also zu einem erfolgreichen Schritt in Richtung VDS, bei dem mit der Aufzählung mehrerer zu versicherheitlichender Objekte argumentiert wurde.

2007: Umsetzung der Richtlinie 2006/24/EG

Angesichts der Fülle an Veränderungen im Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG ist es schwierig, einen Argumentationsfaden zur VDS gesondert herauszuarbeiten. Der Gesetzentwurf der Bundesregierung wiederholte im Begründungsteil die Erwägungen der europäischen Ebene und blieb recht allgemein bei den Zwecken der Strafverfolgung.[55] Letztlich wurden lediglich die Ermittlungserkenntnisse und -erfolge in den Bereichen internationaler Terrorismus, Organisierte Kriminalität und Straftaten mittels Telekommunikation, wie sie in der Bundestagsresolution 2006 (ohne weitere Quellenangabe) bereits beschrieben worden waren, wieder aufgezählt. Demnach hielt die Bundesregierung die „Kenntnis von Verkehrsdaten weithin [für] unverzichtbar“[56], was wiederum an die diskursive Untermauerung einer – nunmehr allerdings sehr weit gefassten – Dringlichkeitssituation (urgency) des securitisation-Ansatzes erinnert.

Da in der Umsetzungsgesetzgebung jedoch der Grundstein einerseits für das Verfassungsgerichtsurteil lag und andererseits damit die VDS erst zu einem großen Zankapfel werden konnte, sollen hier einige Argumente aus dem parlamentarischen Prozess wiedergegeben werden: In den Debatten und auch in der gesonderten Expertenanhörung im Rechtsausschuss zur VDS wurde der Terrorbezug immer wieder hergestellt, zum Beispiel von *Jürgen Gehb* (CDU/CSU) in der ersten Lesung:

> „Verabredungen zu Verbrechen und Terror setzen Kommunikation voraus. […] Die Fortschritte der Technik sind der Grund dafür, dass die Polizei dem Verbrecher eigentlich immer hinterher hechelt. […]Man wird auch darüber nachdenken müssen […], ob Online-Überwachungen sinnvoll sind; schließlich bedienen sich Kriminelle und insbesondere Terroristen des Internets.“[57]

52 Vgl. BT-Drs. 16/690 vom 15. Februar 2006, S. 5; kritisch dazu *Gerrit Hornung*, a.a.O. (Fn. 3), S. 382.
53 BT-Drs. 16/690, a.a.O. (Fn. 52), S. 1.
54 BT-Drs. 16/545 vom 7. Februar 2006, S. 2.
55 Vgl. BT-Drs. 16/5846 vom 27. Juni 2007, S. 28 ff.
56 Ebenda, S. 31.
57 BT-PlPr. 16/109 vom 6. Juli 2007, S. 11350 f.

Auch Bundesjustizministerin *Brigitte Zypries* brachte die Sache auf den Punkt, zeigte aber gleichzeitig mit dem Finger gen Europa, woher die Aufforderung zur VDS stamme, ohne auf ihre eigene Rolle im bisherigen Prozess einzugehen:

> „Das Gesetz zur Vorratsdatenspeicherung dient der Umsetzung einer europäischen Richtlinie. Wie kam es zu dieser europäischen Richtlinie? Nach den Attentaten von Madrid wurde anhand von Handys, die man gefunden hatte, festgestellt, mit wem die Attentäter zuvor telefoniert hatten. Auf diese Weise konnte man andere aus dem terroristischen Umfeld fangen, die an den Attentaten beteiligt waren."[58]

Jörg van Essen (FDP) ging auf *Zypries'* Argumentation ein und kritisierte sie hinsichtlich ihrer Untätigkeit. Sie hätte die Richtlinie deutlich entschärfen können, dann wäre es auch bei den Minimalforderungen der Richtlinie geblieben. Stattdessen habe aber gerade sie den Umfang der Regelung nochmals erweitert.[59]

Dem entgegen stehen exemplarisch die Positionen von *Siegfried Kauder* (CDU/CSU), *Klaus Uwe Benneter* (SPD) und *Joachim Stünker* (SPD). Ihres Erachtens handelte es sich hier legitimerweise um „schwere und schwer zu ermittelnde Straftaten"[60]. *Stünker* konkretisierte und koppelte die VDS im Grunde an fast alle aufkommenden Argumentationslinien. Er erwähnte dabei als erster die Thematik Betäubungsmittel, eine Straftatengruppe, die selten angesprochen wird, aber (siehe unten Abschnitt 4) Anlass für einen Großteil der IKT-Maßnahmen ist:

> „Zur wirksamen Kriminalitätsbekämpfung und zur Aufklärung von Straftaten sind Methoden der verdeckten Ermittlung unerlässlich […]. Das gilt insbesondere für die Bekämpfung der organisierten Kriminalität weltweit, für die Bekämpfung von Wirtschaftsstraftaten und für die Bekämpfung von Betäubungsmittelstraftaten. All dies sind Delikte schwerer Kriminalität, häufig mit erheblichen Verletzungen von Opfern und hohem wirtschaftlichen Schaden. Die VDS dient auch der Abwehr terroristischer Angriffe auf die Sicherheit dieses Landes. Darum geht es und um nichts anderes."[61]

Komplettiert wurde das Feld der Argumente durch *Beate Merk* (CSU, bayerische Justizministerin). In ihrem Redebeitrag im Bundesrat fügte sie der Diskussion um VDS die Problematik der Kinderpornographie hinzu.[62]

Interessanterweise gaben 26 SPD-Abgeordnete eine Zusatzerklärung zu ihrer Zustimmung zum Gesetz ab und stellten so nochmals den Terrorismus ins Zentrum ihrer Erwägungen – obwohl zeitgleich bereits das Potential der VDS zur Terrorismusbekämpfung in Frage stand:

> „[…] Grundsätzlich stimmen wir mit dem Ansatz der Bundesregierung und der Mehrheit unserer Fraktion dahingehend überein, dass die insbesondere durch den internationalen Terrorismus und dessen Folgeerscheinungen entstandene labile Sicherheitslage auch in Deutschland neue Antworten benötigt."[63]

58 BT-PlPr. 16/124 vom 9. November 2007, S. 12994.
59 Vgl. ebenda, S. 12996. In der gleichen Logik zu den erweiterten Möglichkeiten der Geheimdienste *Sabine Leutheusser-Schnarrenberger*, ebenda, S. 12998.
60 Ebenda, S. 12999.
61 Ebenda, S. 13004.
62 BR-PlPr. 834 vom 8. Juni 2007, S. 187.
63 Vgl. BT-PlPr. 16/124, a.a.O. (Fn. 58), S. 13031 f.

In der abschließenden Debatte des Bundesrats am 30. November 2007 führte der Parlamentarische Staatssekretär des Bundejustizministeriums, *Alfred Hartenbach* (SPD), ein weiteres Argument ein: So fordere der Bundesrat eine Nutzung der Vorratsdaten im Kontext von Urheberrechtsverstößen, was die Bundesregierung aber ablehne.[64] Gleichwohl ist nicht zu leugnen, dass die Rechteverwertungsindustrie durchaus hartnäckig ihre Interessen in die Ausschussarbeit des Bundestages einzubringen suchte.[65] Deren Forderungen erhörte der Gesetzgeber allerdings erst 2008 mit einer Öffnung der Weitergabe von Verkehrsdaten auch im Fall von Urheberrechtsverstößen.

2010: Das Bundesverfassungsgerichtsurteil

Einige der Argumentationsmuster, beispielsweise die Herabstufung auf erhebliche Gefahren zog auch die Kritik des Bundesverfassungsgerichts nach sich (das die Nutzung der Vorratsdaten in einstweiligen Verfügungen schon vor 2010 stark eingegrenzt hatte). In der bis dato größten Sammelklage in der Geschichte des Gerichts setzte es insbesondere für Entwicklungspotentiale von Überwachungsmaßnahmen im Gesamten ein deutliches Zeichen. In seinem umfangreichen Urteil geht das BVerfG auch auf die unterschiedlichen Argumentationsmuster ein – exemplarisch soll hier der Leitsatz 5 zitiert werden:

> „Der Abruf und die unmittelbare Nutzung der Daten sind nur verhältnismäßig, wenn sie überragend wichtigen Aufgaben des Rechtsgüterschutzes dienen. Im Bereich der Strafverfolgung setzt dies einen durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraus."[66]

In Folge des Urteils gerät – wie oben bereits erwähnt – die VDS in die Mühlen zwischen europäischen Harmonisierungsforderungen, grundrechtlich argumentierenden Bedenkenträgern und Akteuren der Inneren Sicherheit.

2012: Referentenentwurf des Bundesministeriums der Justiz

Im Frühjahr 2012 wurde deutlich, dass in der 17. Wahlperiode nicht mehr mit einer Einigung in Sachen VDS gerechnet werden konnte, obwohl die EU-Kommission und die Sicherheitsbehörden massiv Druck (bis hin zur Klage vor dem EuGH auf Richtlinienumsetzung) aufbauten. Die Harmonisierungsanforderungen von Seiten der EU lockerten sich

64 Vgl. BR-PlPr. 839 vom 30. November 2007, S. 399.

65 Die Rechteverwertungsindustrie war beim Bundesrat erfolgreicher als im Bundestag. (Forum der Rechteinhaber, Stellungnahme zum Regierungsentwurf vom 18. April 2007; nicht veröffentlichte Eingabe in die Ausschussarbeit des Bundestages. Börsenverein des Deutschen Buchhandels, Schreiben an *Andreas Schmidt* (MdB) vom 9. Oktober 2007; nicht veröffentlichte Eingabe in die Ausschussarbeit des Bundestages. Spitzenorganisation der Filmwirtschaft e.V., Stellungnahme der Filmwirtschaft vom 20. September 2007; nicht veröffentlichte Eingabe in die Ausschussarbeit des Bundestages. *Gerrit Hornung*, a.a.O. (Fn. 3), S. 382. Ob hierin ein so genannter Spill-Over Effekt bei Sicherheitsmaßnahmen oder eine eigenständige politische Handlungsmotivation zu sehen ist, muss in diesem Rahmen dahingestellt bleiben. Im Diskurs des Internets als ‚rechtsfreier Raum' taucht die Argumentation nach dem Urteil des BVerfG von Seiten derselben Akteure als eigenständige auf.

66 BVerfG, a.a.O. (Fn. 5), Rn. 228, 231.

erst 2014 in Folge der umgehenden Außer-Kraft-Setzung der EG-Richtlinie zur Vorratsdatenspeicherung durch den EuGH.[67]

Der Referentenentwurf des federführenden BMJ differenziert sich in seinen Umsetzungsvorschlägen und den Argumentationsmustern nach in zwei Bereiche. Es wurde ein Quick-Freeze-Verfahren für bereits vorhandene Fälle im Bereich der Telekommunikationsunternehmen vorgesehen und allgemein mit den Interessen der Strafverfolgungsbehörden begründet.[68] Bei Internetzugangsdiensten sollte es jedoch eine „eng befristete Speicherung von Verkehrsdaten zu dem Zweck [geben], Bestandsdatenauskünfte […] insbesondere zur Bekämpfung von Kinderpornografie im Internet zu ermöglichen"[69]. Explizit ausgeschlossen wurde eine Verwendung in Zusammenhang mit Ordnungswidrigkeiten.[70] Hier schieden sich – neben der Ausgestaltung der Speicherfristen und Nutzungsmöglichkeiten für die Geheimdienste – wohl auch grundlegend die Geister zwischen Justiz- und Innenministerium.[71] Diese Konfrontationslinie bestand auch zu Beginn der Großen Koalition der 18. Wahlperiode fort.

2015: Wiedereinführung der VDS

Erst im April 2015 wurde diese Konfrontation mit einem neuen Referentenentwurf des Justizministeriums – allerdings diesmal mit dem Bundesinnenministerium abgestimmt – beendet.[72] Dieser erneute Schritt zur Einführung einer Vorratsdatenspeicherung – nunmehr ohne Rückgriff auf eine europäische Richtlinie – stellte nur noch abstrakt darauf ab, die Aufklärung schwerer Straftaten und die Gefahrenabwehr durch das Mittel der Vorratsdatenspeicherung zu ermöglichen. Diese Argumentationslinie behielt die Beschlussfassung der Regelung vom 16. Oktober 2015 bei.[73] Ein weiterer Aspekt – die Einführung des Straftatbestands der Datenhehlerei – wurde dabei erstmalig in die Diskussion eingeführt, was gleichzeitig neues Konfliktpotential eröffnete, da dies direkt den Bereich journalistischer Recherchetätigkeiten oder auch des Whistleblowing traf. Gerade im seit gut zwei Jahren diskutierten Kontext rund um die Enthüllungen von *Edward Snowden* war zu erwarten, dass die Einführung eines Straftatbestands der Datenhehlerei im Zusammenhang mit der Vorratsdatenspeicherung medial besondere Beachtung finden würde.[74] Allerdings

67 Vgl. EuGH, a.a.O. (Fn. 6).

68 Beim Quick-Freeze-Verfahren können Strafverfolgungsbehörden die Speicherung der Kommunikationsdaten veranlassen. Die richterliche Entscheidung kann im Nachhinein eingeholt werden.

69 Bundesministerium der Justiz, Eckpunktepapier zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet, Berlin 2011, http://rsw.beck.de/docs/librariesprovider5/rsw-dokumente/eckpunktepapier_zur_sicherung_vorhandener_verkehrsdaten (Abruf am 26. Juli 2016), S. 2.

70 Vgl. ebenda, S. 5.

71 Vgl. *Kai Biermann*, Wie umfangreich wird die Vorratsdatenspeicherung?, in: Zeit Online vom 29. April 2012, http://www.zeit.de/digital/datenschutz/2012-04/vorratsdaten-gesetzentwurf/komplettansicht (Abruf am 9. Juni 2013).

72 Vgl. Bundesministerium der Justiz und für Verbraucherschutz, Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 15. Mai 2015, https://netzpolitik.org/wp-upload/2015-05-15_BMJV-Referentenentwurf-Vorratsdatenspeicherung.pdf (Abruf am 18. Mai 2015), S. 1 f.

73 BT-Drs. 18/5088 vom 9. Juni 2015, S. 1.

74 Hinweise darauf bestehen bereits. So zum Beispiel *Svenja Bergt*, Überwachung im Schnelldurchlauf, in: taz.de vom 18. Mai 2015, http://www.taz.de/!160057/ (Abruf am 19. Mai 2015).

war die Gesetzgebungsphase insbesondere im Sommer/Herbst 2015 von den erheblich gestiegenen Flüchtlingszahlen geprägt, was wohl eine breite Debatte um die VDS verhinderte.

Zusammenschau der Gesetzesinitiativen in Zusammenhang mit einer Vorratsdatenspeicherung

Die Frage von Mindestspeicherfristen für Eckdaten des Kommunikationsgebarens der Bevölkerung ist seit 1996 auf der Agenda. Zunächst verwiesen politische Akteure in ihren Begründungen auf die Entwicklung der Organisierten Kriminalität (im Telekommunikationsbereich). Im Verlauf der gesamten Diskussion tat sich der Bundesrat als besonders aktiv hervor.

Neben dem Ob einer VDS stand auch das Wie der Nutzung im Mittelpunkt. So versuchte 1999 die CDU/CSU-Fraktion im Bundestag, die Nutzung von gespeicherten Verkehrsdaten über den Straftatenkatalog aus § 100a StPO auszuweiten. Darauf aufbauend wurden im Jahre 2000 – wiederum mit Zutun des Bundesrates – die Regelungen zur sechsmonatigen Höchstspeicherdauer aufrecht erhalten.

Argumentativ trat 2002 Kindesmissbrauch und Kinderpornographie – mittelbar – hinzu. Unter Bezugnahme auf den technologischen Wandel und das entsprechend veränderte Kriminalitätsverhalten stand die VDS 2003 im Zeichen einer effektiveren Strafverfolgung, und wiederum übernahm der Bundesrat die Rolle des Vorreiters bei der Forderung nach einer Mindestspeicherfrist von sechs Monaten.

Während sich im Jahre 2005 der Bundestag nochmals deutlich gegen die Einführung von Vorratsdatenspeicherungspflichten über den europäischen Umweg aussprach, war dieser Widerstand ein Jahr später gebrochen, und die Bundesregierung stimmte der Richtlinie 2006/24/EG – nicht zuletzt unter dem Eindruck der terroristischen Anschläge von Madrid und London – zu. 2007 erfolgte dann die deutsche Umsetzung der EG-Richtlinie unter der Hauptargumentation des Kampfes gegen Schwerkriminalität und Terrorismus. Nach dem einschneidenden Verfassungsgerichtsurteil von 2010 reaktivierten (und kumulierten) politische Akteure – vornehmlich aus den Reihen von CDU/CSU und SPD – die einzelnen Argumentationsmuster zu geeignet erscheinenden Zeitpunkten.

Seither wurde der Nutzen der VDS für die Aufklärung von Straftaten sowohl auf EU-Ebene als auch für die deutschen Sicherheitsbehörden verschiedentlich evaluiert. Dabei basieren diese Evaluationen anekdotisch auf dem Erfahrungsschatz der Sicherheitsbehörden[75], ohne jedoch auf die tatsächliche Rolle dieser Straftaten für den Polizeialltag einzugehen. Allerdings stellt sich dabei das Problem, dass die zu Grunde liegenden Sachverhalte für eine Abfrage von Vorratsdaten nach §100 g StGB überhaupt nicht dokumentiert werden. Die methodischen Zugänge der Evaluationen – soweit sie über die Anekdotenhaftigkeit hinausgingen – gerieten daher selbst in die (mediale) Kritik.[76]

Der aktuelle Rückgriff zur Begründung der VDS-Einführung auf die Unterstützung beziehungsweise Ermöglichung der Verfolgung schwerer Straftaten und der Gefahrenab-

75 Vgl. *Dominik Brodowski*, a.a.O. (Fn. 12), S. 498.

76 So bei der Veröffentlichung der MPI-Studie zum Nutzen der Vorratsdatenspeicherung von *Hans-Jörg Albrecht*, a.a.O. (Fn. 11).

wehr[77] ist das Produkt einer zwanzigjährigen Argumentationsentwicklung. Es werden keine skandalträchtigen Einzeldelikte (wie Terrorismus oder Kindesmissbrauch), die sich als Referenzobjekte in den ursprünglichen securitisation-Ansätzen besonders gut eignen, herangezogen, sondern die polizeiliche Alltagsarbeit – und damit die Gesamtgesellschaft als potentielles Opfer von Straftaten – wird nunmehr zum Referenzobjekt. Argumentiert wird also nicht mehr über die einschneidende Ausnahmesituation; vielmehr geraten nun gefährdete Möglichkeiten der Kriminalitätsbekämpfung in der digitalisierten Gesellschaft zum Dreh- und Angelpunkt der Argumentation – ohne dabei konkrete Deliktgruppen oder Ähnliches mehr zu nennen.

4. Nutzung der Kommunikationsüberwachung: Die Anwendung der §§ 100a und 100g StPO

Der vorliegende Beitrag muss daher für den folgenden Abgleich von kommunizierten Argumenten mit tatsächlichen Einsatzfeldern auf die Nutzungsmodalitäten der Telekommunikationsüberwachung (TKÜ) zurückgreifen. Dies erfolgt in dem Bewusstsein, dass die Übertragung mit Einschränkungen verbunden ist. Es wird jedoch davon ausgegangen, dass der methodische Bogen von der TKÜ zur VDS zulässig ist, da Vorratsdaten zumindest wohl in ähnlichen Deliktbereichen wie die TKÜ zur Aufklärung beitragen können.[78] Die Daten des Bundesjustizministeriums zur TKÜ erlauben einen aktuellen Längsschnitt, wodurch Trends der Zugriffsgründe ablesbar werden.

Ein älterer Forschungsbericht des MPI Freiburg[79] bemühte sich zwar um eine Aufschlüsselung der Deliktbereiche bei Verkehrsdatenabfragen, ist aber für die vorliegenden Zwecke nicht nutzbar, da die Erhebung 2003 und 2004 erfolgte, also vor Einführung der VDS. Zudem liegen methodische Spezifika vor, die zu einer nicht kontrollierbaren Verzerrung im Vergleich zur hier gewählten Datenbasis des Justizministeriums führen würde.[80]

Die TKÜ gibt es bereits seit dem 7. April 1987 (BGBl. I, S. 1319). Seither erfolgten zahlreiche Novellierungen, wobei zum 1. Januar 2008 eine völlige Neuregelung des § 100a StPO in Kraft trat. Die Nutzung von Verkehrsdaten, also solche, die beispielsweise im Rahmen der VDS anfallen, normiert § 100g StPO. Die Rechtsgrundlage schuf der Gesetzgeber zunächst mit Wirkung zum 20. Dezember 2001. Es handelt sich dabei um die Nachfolgeregelung des Fernmeldeanlagengesetzes (FAG).[81] Wie für § 100a StPO erfolgte zum 1. Januar 2008 mit demselben Gesetz auch für § 100g StPO eine Überarbeitung mit dem Ziel, die VDS laut EG-Richtlinie unter den Paragraphen subsumieren zu können. Der Zugriff auf Verkehrsdaten ist dabei ebenfalls an die Katalogstraftaten nach § 100a StPO gebunden,

77 Bundesministerium der Justiz und für Verbraucherschutz, a.a.O. (Fn. 72).

78 Eine aktuelle Studie zur Schweiz geht ähnlich vor und betrachtet die Begründungshäufigkeiten von Überwachungsmaßnahmen im Gesamten. Die Grundstrukturen der Ergebnisse stellen sich ähnlich dar, wie im Folgenden für den deutschen Fall gezeigt wird. Vgl. Digitale Gesellschaft, Swiss Lawful Interception Report 2016, https://www.digitale-gesellschaft.ch/uploads/2016/03/SLIR_2016.pdf (Abruf am 10. März 2016).

79 *Hans-Jörg Albrecht / Andina Grafe / Michael Kilchling*, Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h der Strafprozessordnung, in: BT-Drs. 16/8434 vom 28. Februar 2008.

80 Vgl. ebenda, S. 57 ff.

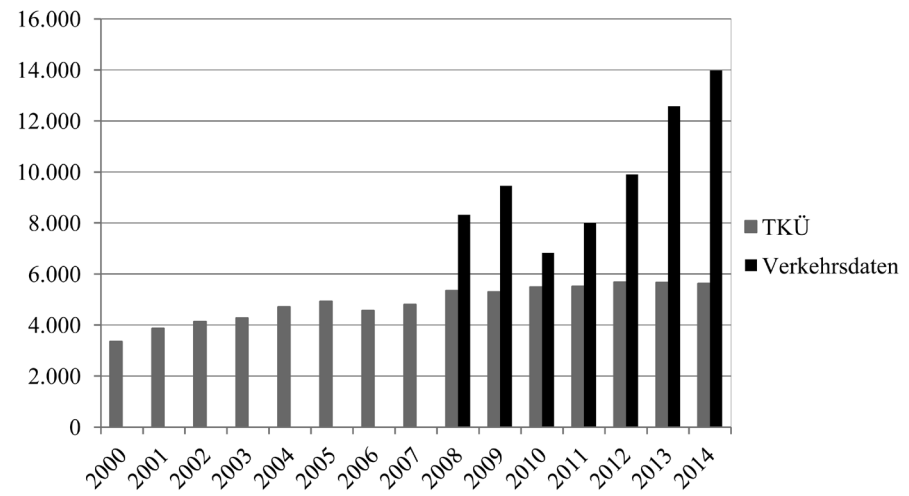
81 Dazu ausführlicher *Jasmin Riedl*, a.a.O. (Fn. 2).

seit 2008 aber darüber hinaus auch für weitere schwerwiegende Straftaten zulässig. Grundsätzlich gilt dabei die Hürde einer richterlichen Genehmigung, obwohl Zweifel an ihrer Effektivität bestehen.[82]

Diese Aspekte sind zentral, um die Zugriffe auf die Kommunikationsdaten und -inhalte, die vor allem seit Mitte der neunziger Jahre einen deutlichen Aufschwung erlebt haben, einordnen zu können. Die Anordnungen beziehen sich auf die konkreten Anschlüsse. Die Entwicklung ist daher auch im Zusammenhang mit der seit Mitte der neunziger Jahre deutlich zunehmenden Nutzung von Mobiltelefonen zu sehen.

Aber auch davon unabhängig betrachtet hat – wie Abbildung 1 zeigt – die Anzahl der Ermittlungsverfahren, in denen TKÜ-Maßnahmen zum Einsatz kamen, seit Beginn des Beobachtungszeitraums zwischen 2000 und 2014 zugenommen.[83] Sie verhält sich aber in den vergangenen Jahren relativ konstant.

Abbildung 1: Anzahl der TKÜ-Verfahren mit Verkehrsdatenabfrage, absolute Zahlen nach Jahren



Quelle: Eigene Darstellung. Die Datenbasis bilden die Übersichten zur Telekommunikations- und Verkehrsdatenüberwachung des Bundesjustizamtes 2001 bis 2015, https://bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html (Abruf am 10. Mai 2016).

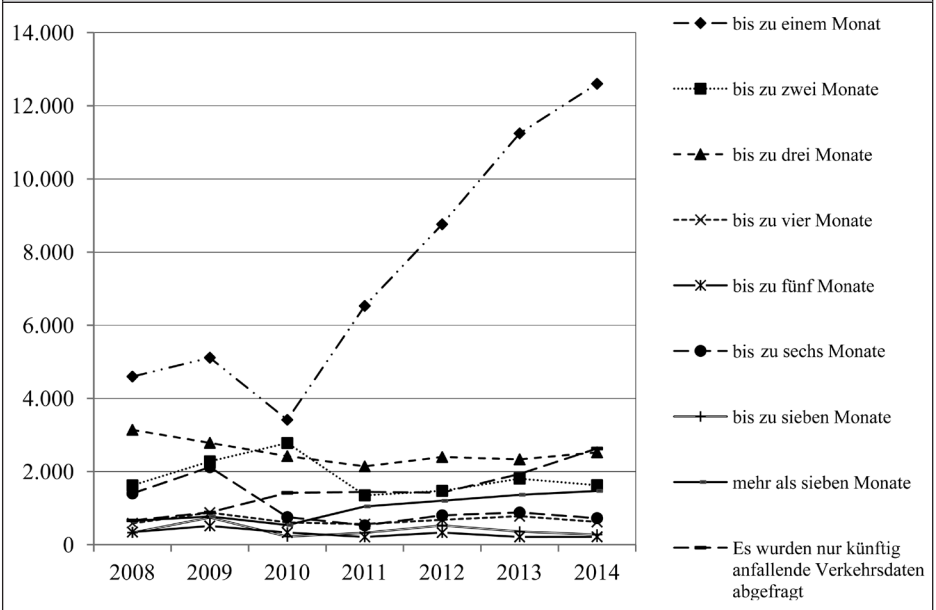
Die Nutzung von Verkehrsdaten – wie in Abbildung 1 dargestellt – muss seit 2008 dokumentiert werden und bewegt sich in den Jahren 2008 bis 2014 zwischen 6.828 und 13.979 Verfahren. Damit ist eine steigende Tendenz zu erkennen.

Niedrig ist hingegen das Alter der verwendeten Daten. So bezogen sich die Erstanordnungen, wie Abbildung 2 zeigt, vorwiegend auf gespeicherte Informationen, die nicht älter

82 Vgl. *Richard Gutjahr*, Bestandsdaten außer Kontrolle, http://gutjahr.biz/2013/04/bestandsdatenauskunft/ (Abruf am 10. Juni 2013).

83 Der Beobachtungszeitraum folgt der Dokumentation von TKÜ-Maßnahmen seit 2001 durch das BMJ. Für die Verkehrsdaten erfolgt eine Dokumentation seit 2008. Für beide Bereiche liegen bisher noch keine Zahlen für 2012 vor.

Abbildung 2: Alter der abgefragten Verkehrsdaten

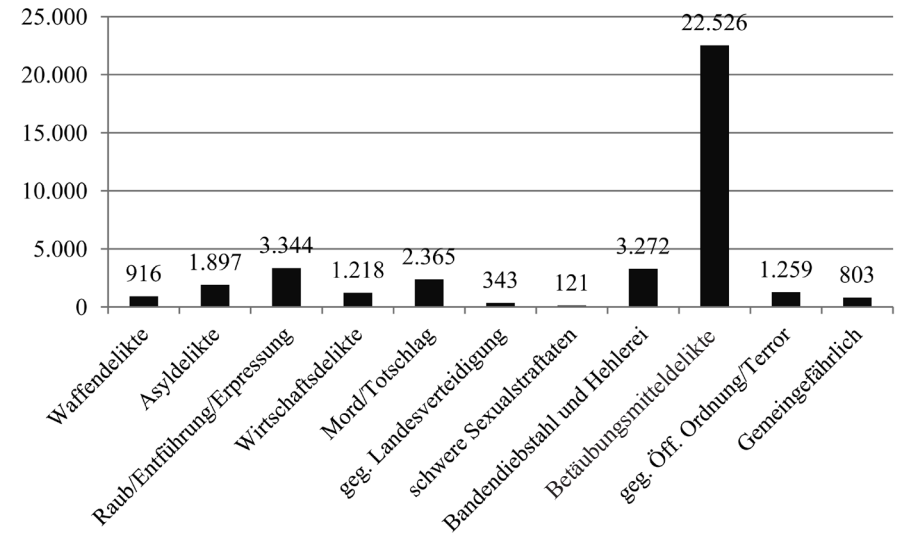


Quelle: Eigene Darstellung auf Grundlage des Bundesjustizamtes 2009 bis 2015, vgl. Abbildung 1.

als einen Monat sind. Dieser Trend verstärkt sich in den letzten Jahren. Entsprechend sind Forderungen aus Politik und Wissenschaft nach kurzen Mindestspeicherfristen durchaus mit den polizeilichen Nutzungstrends konform. So hielt beispielsweise die damalige Bundesministerin der Justiz, *Sabine Leutheusser-Schnarrenberger*, eine Speicherung der Verkehrsdaten von sieben Tagen für ausreichend. Von Bedeutung sind die Zeiträume auch hinsichtlich der Argumentation bei der versuchten Legitimierung von Mindestspeicherfristen im Rahmen der Telekommunikations-Datenschutzverordnung (TDSV) im Jahr 2000. Hier hatte, wie bereits dargelegt, der Innenausschuss des Bundesrates eine Speicherfrist von drei Monaten zurückgewiesen, da dies die Ermittlungsmöglichkeiten unangemessen einschränke. Wenngleich hier der Begriff der Angemessenheit nicht abschließend diskutiert werden kann, ist offensichtlich, dass mit steigender Speicherfrist die informationelle Selbstbestimmung der Gesamtbevölkerung stärker beeinträchtigt wird. Abbildung 2 verdeutlicht, dass um die 80 Prozent der abgerufenen Daten im dokumentierten Zeitraum nicht älter als drei Monate waren, was die Eingriffsschwere der VDS zumindest in Bezug auf ihre tatsächlichen Abfragemodalitäten etwas abmildert.

Wie gezeigt argumentieren politische Akteure vornehmlich mit stark emotional und normativ assoziierten Begriffen: Cyberkriminalität, Terrorismus, Missbrauch von Kindern. Hinzu tritt der diffuse Begriff der Organisierten Kriminalität. Diese ist in der Darstellung des Bundeskriminalamtes (BKA) ein Deliktfeld, das auf die meisten Katalogstraftaten des § 100a StPO angewandt werden kann. Folglich stellt das Argument, dass IKT-Maßnahmen allgemein und insbesondere TKÜ und VDS vornehmlich gegen die Organisierte Kriminalität angewandt werden sollen, eher einen Allgemeinplatz denn eine spezifische Begründung dar.

Abbildung 3: Anzahl der Anlassstraftaten der TKÜ 2000 bis 2007



Quelle: Eigene Darstellung auf Grundlage des Bundesjustizamtes 2001 bis 2008, vgl. Abbildung 1.

Die mit Organisierter Kriminalität assoziierten Deliktbereiche variieren im Detail stark.[84] Betrachtet man insgesamt die Einsatzfelder von TKÜ (wie sie entsprechend der Katalogstraftaten kumuliert wurden), ergibt sich ein Bild, das nicht den holzschnittartigen Bedrohungsszenarien entspricht, das die politischen Akteure als Begründung anführen. Abbildung 3 zeigt, dass TKÜ-Maßnahmen am weitaus häufigsten bei Betäubungsmitteldelikten (BTM) zum Einsatz kommen. Diese umfassen mehr als 50 Prozent aller Verfahren zwischen 2000 und 2007.

Dieses Bild verändert sich nur wenig nach der großen Reform des § 100a zum 1. Januar 2008. Der Gesetzgeber nahm zu diesem Datum beispielsweise erstmals den Straftatbestand des Cyberbetrugs auf, der klar in der Argumentationslinie von Cyberkriminalität liegt. Aber auch seit 2008 entfallen auf Verfahren nach dem Betäubungsmittelgesetz immer noch knapp 50 Prozent der TKÜ-Anordnungen (siehe Abbildung 4).

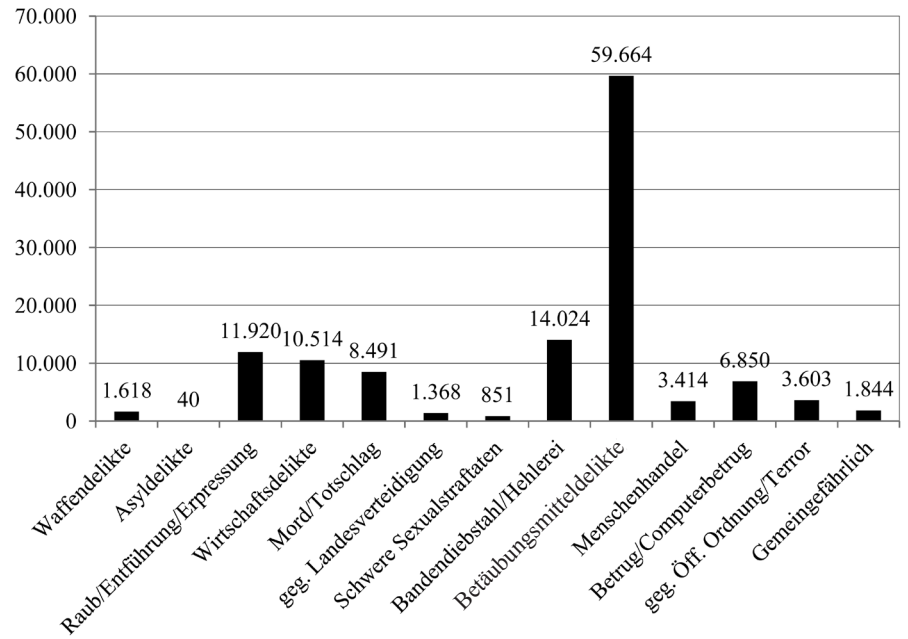
Seit 2000 finden TKÜ-Maßnahmen mit großem Abstand am häufigsten ihren Einsatz bei Betäubungsmitteldelikten. Diese Beobachtung kann nur in Einklang mit der Argumentation für die VDS gebracht werden, wenn ein großer Teil der seitens politischer Akteure formulierten Gefahr durch die Organisierte Kriminalität im Bereich der Rauschgift-Delikte liegt.

Diese Sichtweise wird einerseits unterstützt vom jährlichen Lagebild des BKA.[85] Danach hatten 2011 drei Deliktbereiche mehr als zehn Prozent Anteil an der Organisierten Krimi-

84 In einer internen Abfrage gab es keinen mit Organisierter Kriminalität bevorzugt assoziierten Deliktbereich. Spontane Nennungen waren Zwangsprostitution, Schutzgelderpressung, Drogenhandel und Autodiebstahl.

85 Vgl. Bundeskriminalamt, Bundeslagebild Organisierte Kriminalität 2011, Wiesbaden 2012, S. 30, https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/OrganisierteKriminalitaet/organisierteKriminalitaetBundeslagebild2011.pdf?__blob=publicationFile&v=3 (Abruf am 9. Juni 2013).

Abbildung 4: Anzahl der Anlassstraftaten der TKÜ 2008 bis 2014



Quelle: Eigene Darstellung auf Grundlage des Bundesjustizamtes 2009 bis 2015, vgl. Abbildung 1.

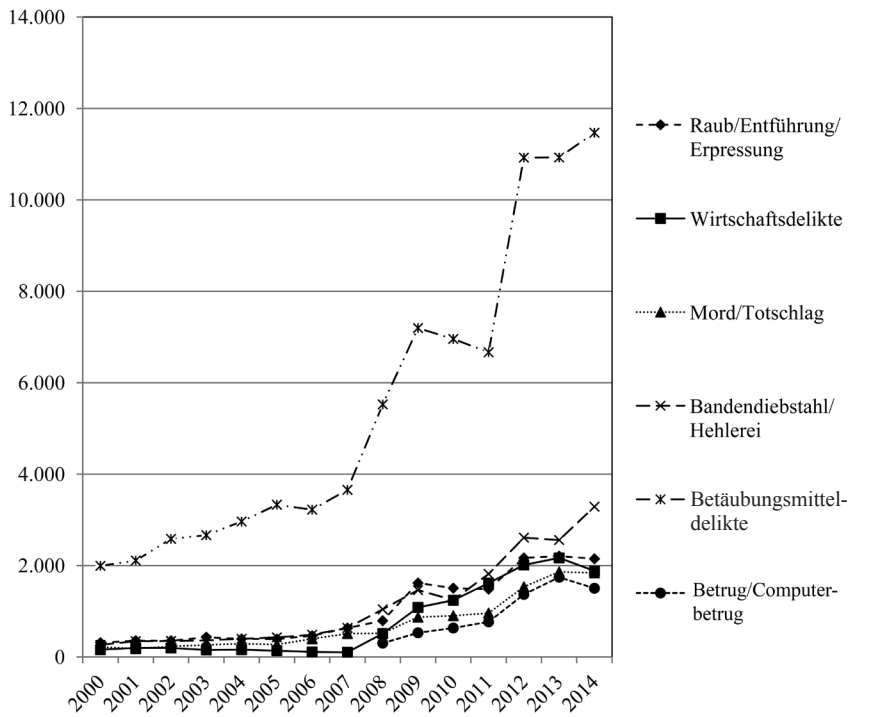
nalität: Rauschgifthandel (36,7 Prozent), Kriminalität im Wirtschaftsleben (14,8) und Eigentumskriminalität (13,1). Andererseits gibt es Hinweise zur Betäubungsmittelkriminalität und deren Verfolgung, die in der Mehrheit der Strafverfahren ein Vorgehen gegen Konsumenten und nicht gegen (organisierte) Händler sehen.[86] Insofern vermag die Argumentation, die hohe Zahl an Betäubungsmitteldelikten entspringe dem Feld der Organisierten Kriminalität, nicht zu überzeugen.

Betrachtet man demgegenüber im direkten Vergleich die Nutzungshäufigkeit der sechs wichtigsten Deliktgruppen im Zeitverlauf, wird die Diskrepanz nochmals deutlicher. Betäubungsmitteldelikte liegen hier im hohen vierstelligen Bereich. Zu den häufigsten Straftaten zählen des Weiteren (a) Bandendiebstahl und Hehlerei, (b) Raub, Entführung, Erpressung, (c) Mord, (d) Wirtschaftsdelikte und (e) der erst ab 2008 abbildbare Betrug/Computerbetrug.

Drei der in Abschnitt 2 dargestellten Argumentationslinien lassen sich den in Abbildung 4 verwandten Delikten relativ trennscharf zuordnen. Abbildung 6 gibt – kontrastierend zu Abbildung 5 – die argumentativen Schwerpunkte der TKÜ-Nutzung wieder – also im securitisation-Jargon die referent objects. Dass die Zahl der Verfahren weder bei schweren Sexualstraftaten (worunter Kindesmissbrauch und -pornographie fällt) noch für Deliktgruppen des Terrorismus den dreistelligen Bereich überschreitet, verwundert insbesondere vor dem Hintergrund, dass mit beiden seit vielen Jahren immer wiederkehrende und emo-

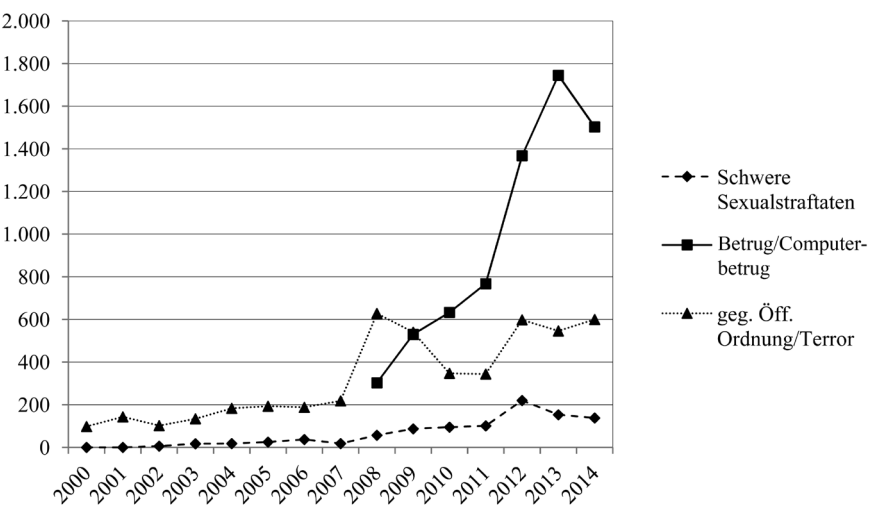
86 Vgl. *Hans Cousto*, Polizei intensiviert Kifferjagd, in: taz.de vom 22. Mai 2013, https://blogs.taz.de/drogerie/2013/05/22/polizei-intensiviert-kifferjagd/ (Abruf am 10. Juni 2013).

Abbildung 5: Die sechs häufigsten Deliktbereiche 2000 bis 2014 nach Anzahl der Anlassstraftaten



Quelle: Eigene Darstellung auf Grundlage des Bundesjustizamtes 2001 bis 2015, vgl. Abbildung 1.

Abbildung 6: Die prominent argumentierten Deliktbereiche 2000 bis 2014 nach Anzahl der Anlassstraftaten



Quelle: Eigene Darstellung auf Grundlage des Bundesjustizamtes 2001 bis 2015, vgl. Abbildung 1.

tional stark aufgeladene Gefahrenbilder gezeichnet werden. Lediglich bei Computerbetrug und Betrug entwickelte sich bis 2013 ein wachsender Trend in der Nutzung der TKÜ.

5. Fazit: Bekämpfung von Drogenkriminalität – der ignorierte Elefant im Raum der VDS-Argumente

Die Argumente für die Vorratsdatenspeicherung wandelten sich im Verlauf der bundesdeutschen Debatte seit Mitte der neunziger Jahre. Seit das BVerfG 2010 die Maßnahme außer Kraft setzte, wurden zudem die unterschiedlichen, zuvor bereits bekannten Argumentationsmuster kumuliert. Die Umsetzungsverpflichtung der Richtlinie 2006/24/EG findet als eigenständiges Argument Eingang in die Begründung einer deutschen Regelung, was dann jedoch mit der Gerichtsentscheidung des EuGH im Jahre 2014 gegen die VDS-Richtlinie wegfällt. Nachdem die kumulierten Einzelargumente in (wissenschaftlichen) Evaluationen wenig Unterstützung fanden, stellte die aktuellste Gesetzesbegründung von Ende 2015 nur noch abstrakt auf Kriminalitätsbekämpfung und Gefahrenabwehr ab. Im Gegensatz zur im ursprünglichen securitisation-Ansatz erwarteten diskursiven Herbeiführung der Dringlichkeits-Situation unter Bezug auf eine außerordentliche (terroristische) Gefahr, ist mit dem hier gewählten breiteren securitisation-Ansatz eine Ent-Emotionalisierung durch den diskursiven Verweis auf die Ermöglichung der alltäglichen Polizeiarbeit festzustellen. Die Wahrnehmung der Bedrohungssituation als existentiell wird also eher über die maximale Breite des Argumentes als über die Außerordentlichkeit des Anlasses erreicht.

Den Begründungen politischer Akteure für die Notwendigkeit von IKT-Maßnahmen, insbesondere der VDS, stehen jedoch auch mit dieser maximalen Breite des Arguments die deutlichen Eigenheiten der analysierten Nutzungsfelder von IKT-Maßnahmen gegenüber. Insbesondere der Bereich der Drogenkriminalität erscheint hier als besonders relevant. Es drängen sich daher zwei Fragen auf: (1) Wie sind die vornehmlichen Argumentationslinien zu erklären? (2) Warum tauchen Rauschmitteldelikte fast nie explizit in der Argumentation für Maßnahmen aus dem IKT-Bereich auf?

(1) Politische Akteure stellen ihre Argumente für die VDS zumeist in den größeren Kontext von IKT-Maßnahmen insgesamt. In weiten Teilen beziehen sie sich nicht bloß auf Vorratsdaten, sondern auf die Überwachung von (elektronischer) Kommunikation.

Die dominierenden Argumentationslinien scheinen unstreitige, gesellschaftlich geteilte normative Prinzipien zu sein, deren Gefährdung zwingend eine Dringlichkeitssituation herbeiführt. Dies entspricht auch ganz dem Blickwinkel des securitisation-Ansatzes. Die Verknüpfung der VDS mit den Kriminalitätsfeldern Kindesmissbrauch und -pornographie sowie Terrorismus – aber letztlich auch mit der grundsätzlichen Unterstützung der Verfolgung von Straftaten als breitest mögliches Argument – versucht, einen als gesellschaftlich erwartbaren Grundkonsens zu bedienen und darüber zugleich einen Konsens für entsprechende Forderungen nach verbesserten Überwachungsmöglichkeiten der Kommunikation zu schaffen. Der Argumentation wurde jedoch der Wind aus den Segeln genommen, weil der Vorratsdatenspeicherung wissenschaftlich fundiert nur eingeschränktes Aufklärungspotential für Schwerkriminalität bescheinigt wurde.

Des Weiteren erklärt sich die Argumentation zur Cyberkriminalität aus drei Gründen: Einerseits liegt eine subjektiv empfundene hohe Betroffenheit von derartigen Straftaten in

der Bevölkerung vor (23 Prozent mit in-/direkter Opfererfahrung[87]), und andererseits löst die Fremdheit des Themas insbesondere in höheren Altersklassen und die damit einhergehende Verunsicherung ein hohes Unterstützungspotential aus. Drittens steigt die Nutzung von TKÜ-Maßnahmen zur Bekämpfung dieses Kriminalitätsbereichs tatsächlich.

(2) Betäubungsmitteldelikte bilden gut die Hälfte aller Verfahren, in denen die Sicherheitsbehörden auf TKÜ zurückgreifen – kaum verwunderlich, da es sich hier um so genannte Transaktionskriminalität handelt, die eben typischerweise unter Zuhilfenahme von Telekommunikation geschieht. Trotz der sich daraus ergebenden augenscheinlichen Bedeutung für die Strafverfolgung kommt das Argument in der Diskussion um die VDS kaum vor. Eine Erklärung ist hierbei, dass Akteure der Inneren Sicherheit und insbesondere Repräsentanten von Sicherheitsbehörden die Drogenvergehen tendenziell unter dem Etikett der Organisierten Kriminalität führen (wie es das BKA-Lagebild von 2011 nahe legt). Dennoch verwundert, dass die Wichtigkeit des Betäubungsmittelbereichs nicht thematisiert wird. Dies könnte daran liegen, dass eine explizite Nennung dieser Problematik die gesellschaftlich normative Schlagkraft der Argumentation Organisierte Kriminalität abschwächt. Der Kontext Drogenkriminalität bedient nicht durchgehend einen normativ-kritischen Grundkonsens – zu denken ist hier etwa an die Cannabis-Diskussion. Ob der Rückgriff auf die nicht klar definierte Figur der Organisierten Kriminalität als normativ geladene Worthülse legitim ist, wenn eine relevante Untergruppe an Delikten klar benennbar wäre, scheint fragwürdig – zu Transparenz in Entscheidungsprozessen bezüglich grundrechtseinschränkender Sicherheitsmaßnahmen tragen die analysierten Begründungmuster jedenfalls nicht bei.

Der hier gewählte doppelte Ansatz einer breiten Analyse der Maßnahmengenese und der Maßnahmennutzung verdeutlicht den Vorteil des erweiterten securitisation-Konzeptes. Der Fokus auf einzelne Sprecher im Nachgang zu Terroranschlägen und auf ähnliche außerordentliche Ereignisse würde die Rolle dieser Ereignisse und den einzelnen subjektiven Akteur überinterpretieren. Durch das hier vorgestellte Vorgehen eröffnet sich die Chance, Terroranschläge in ihrer Katalysatorfunktion für die Durchsetzung bestimmter Maßnahmen durch den Abgleich mit nicht erfolgreich stattgefundenen Versuchen ihrer Einführung zu analysieren. Darüber hinaus eröffnet der empirische Abgleich der Nutzungsmodalitäten einer Sicherheitsmaßnahme mit ihrem offiziellen Gesetzesziel den Blick auf die Legitimität der einzelnen Maßnahme aber auch ganz allgemein auf Versicherheitlichung im Schatten von normativ-skandalisierenden Bedrohungsszenarien.

87 Vgl *Mathias Bug* / *Ursula Münch*, a.a.O. (Fn. 8), S. 155. Eine ähnliche Einschätzung ergibt sich für die Folgejahre: *Johannes Rieckmann* / *Martina Kraus*, Tatort Internet, in: DIW-Wochenbericht Nr. 12/2015, S. 295 – 301, S. 297.