Vorratsdatenspeicherung in Deutschland und in der Volksrepublik China

Eine Auseinandersetzung mit den einschlägigen Regelungen und den rechtlichen Anforderungen an die Speicherung von Vorratsdaten in Deutschland und China sowie Vorschläge für gesetzgeberische Anpassungen

Ruan Shuang。阮爽
Universität Münster

1. Februar 2019

Erster Berichterstatter: Prof. Dr. Bernd Holznagel

Zweiter Berichterstatter: Prof. Dr. Dirk Ehlers

Dekan/in: Prof. Dr. Klaus Boers

Tag der mündlichen Prüfung: 18.06.2019

INHALTSÜBERSICHT

INHALTSVERZEICHNIS

Kapitel 1: Gegenstand der Arbeit und Gang der Untersuchung

Unter der Vorratsdatenspeicherung versteht man eine Sicherheitsmaßnahme, nach der Telekommunikationsverkehrsdaten aller Bürger generell und verdachtsunabhängig auf Vorrat gespeichert werden müssen, um die Daten den befugten Behörden für eine zukünftige, anlassbezogene Abfrage und Auswertung zur Verfügung zu stellen. Durch die Vorratsdatenspeicherung soll eine effektive Strafverfolgung und Gefahrenabwehr gefördert werden.

Die Entstehung dieser Sicherheitsmaßnahme hängt eng mit der veränderten Bedrohungslage in der Informationsgesellschaft zusammen. Dank der rasanten Entwicklung und des unaufhaltsamen Fortschritts der Telekommunikations- und Informationstechnologie werden zahlreiche technische Errungenschaften in allen Lebensbereichen fruchtbar gemacht.[1] Jedoch sind gleichzeitig mit der Entwicklung neue Gefahren aufgetaucht. Vor allem werden völlig neue Formen von Cyber-Kriminalität[2] wegen der Unverzichtbarkeit der Nutzung von moderner Informations- und Kommunikationstechnologie ermöglicht.[3] Die zunehmende Häufigkeit der Begehung von Cybercrime hat schwere Schäden verursacht und das Schadenspotenzial ist absehbar noch höher.[4] Ferner werden die Vorbereitung sowie die Begehung herkömmlicher Straftaten mittels der neuesten Informations- und Kommunikationstechnologie auch in erheblicher Weise erleichtert.[5] Organisierte Kriminalität und internationaler Terrorismus haben eine weitere sichtbare Gefährdung der öf-

---

1 Aus zahlreichen Darstellungen der Vorteile bei Entstehung sowie Entwicklung neuer Informationstechnologie in verschiedenen Literatur siehe beispielhaft *Sieber*, in: *Hoeren/Sieber/Holznagel* (Hrsg.), 2014, Teil 1; *Roßnagel*, 2007; *Moser-Knierim*, S. 17 ff.; *Kutscha*, LKV 2008, 481 (481 ff.).

2 Gemäß Bundeskriminalamt umfasst Cybercrime die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen würden. Siehe Bundeskriminalamt, Cybercrime, Bundeslagebild 2015, S. 5, abrufbar unter: <https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2015.html?nn=28110> [Stand: 31.1.2019].

3 In der Literatur werden diese Formen der Kriminalität als Informations- und Kommunikationskriminalität (IuK-Kriminalität) bezeichnet, siehe zum Beispiel *Moser-Knierim*, S. 39; *Albrecht/Kilchling*, S. 9.

4 Nach dem Bundeskriminalamt betrugen die Schäden durch Cybercrime im Jahr 2015 40,5 Mio. Euro. Siehe Bundeskriminalamt, Cybercrime, Bundeslagebild 2015, S. 7 und 17-18, abrufbar unter: <https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2015.html?nn=28110> [Stand: 31.1.2019].

5 BVerfGE 120, 274 (319 f.); *Breyer*, S. 170; *Szuba*, S. 27; *Zimmer*, S. 46.

fentlichen Sicherheit hervorgebracht, die mit Hilfe der modernen Informations- und Kommunikationstechnologie in die Lage kommen, Maßnahmen zur Aufklärung und Vorbeugung mit Leichtigkeit zu unterlaufen.[6]

Seit dem Anschlag vom 11. September 2001 in den USA und nachfolgenden terroristischen Anschlägen in Europa hat sich die Bedrohungslage erheblich verschärft. Besonders beunruhigend ist eine seit den Terroranschlägen vom 11. September 2001 erkennbare Tendenz, dass Terrorismusaktivitäten öfter durch Selbstmordattentäter begangen werden, die sich durch repressive Sanktionen nicht abschrecken lassen.[7] Angesichts der veränderten Gefahren- und Bedrohungslage ist es notwendig, Sicherheitsstrategien unter den neuen technischen Bedingungen besser an die neue Bedrohungslage anzupassen.[8]

Den Behörden werden neue Befugnisse zur Strafverfolgung und Gefahrenabwehr durch Verabschiedung oder Änderung der Sicherheitsgesetze erteilt. Sie dürfen somit neue technische Ermittlungsmethoden wie Lauschangriffe, Rasterfahndung, Online-Durchsuchungen, automatische Kennzeichenerfassung bis hin zur Vorratsdatenspeicherung zum Zweck der Strafverfolgung und Gefahrenabwehr nutzen. Viele dieser Maßnahmen richten sich nicht mehr gegen eine konkrete Gefahr und gegen einen bestimmten Straftäter oder Verdächtigen, sondern allgemein und verdachtsunabhängig gegen alle Bürger, um Verbrechen vor ihrer Begehung aufzudecken und potenzielle Gefahren schon in ihrer Entstehung zu unterdrücken.[9] Die Anpassung der Sicherheitsstrategie ist also durch die Vorverlagerung von Sicherheitsmaßnahmen gekennzeichnet. Die Vorverlagerung von Maßnahmen tritt zunehmend in Form von umfangreicher Sammlung, Speicherung und Auswertung personenbezogener Daten vom Staat auf und werden ergriffen bevor eine tatsächliche Gefahr auftritt.[10]

In der Informationsgesellschaft ist das private und auch das soziale Leben zunehmend durch Nutzung der zahlreichen digitalen Instrumente im Telekommunikationsnetz und Internet gekennzeichnet. Immense digitale Daten-

---

6 Ausführlich dazu *Germann*, S. 40 ff.

7 Ausführlich zu diesen Besonderheit neuer Bedrohungslage siehe *Thiel*, S. 35 ff.; *Hoffmann-Riem*, ZRP 2002, 497 (499 ff.); *Krings*, ZRP 2015, 167 (167 ff.).

8 Zur Erforderlichkeit der Anpassung von Sicherheitspolitik siehe auch *Hoffmann-Riem*, ZRP 2002, 497 (497 ff.); *Calliess*, DVBI 2003, 1096 (1098 f.); *Moser-Knierim*, S. 10 und 50 ff.

9 *Hetzer*, ZRP 2005, 132 (134); *Hirsch*, ZRP 2008, 24 (25); Vgl. *Szuba*, S. 41.

10 *Hoffmann-Riem*, ZRP 2002, 497 (499), vgl. *Szuba*, S. 21 f., *Weidner-Braun*, S. 18.

berge sind damit entstanden,[11] aus denen der Nutzer identifiziert und umfassende persönliche Informationen in Bezug auf beispielweise Bewegungsprofile ermittelt werden können.[12] Dies hat neue Möglichkeiten der Strafverfolgung und Gefahrenabwehr durch Speicherung und Auswertung der Telekommunikationsdaten mit sich gebracht.

Vor allem können Telekommunikationsdaten als „Spuren" der Vorbereitung oder Durchführung von Straftaten genutzt und die Täter damit identifiziert und verfolgt werden.[13] Somit sind die Sicherheits- und Strafverfolgungsbehörden zur Erfüllung ihrer Aufgaben tendenziell immer mehr auf Speicherung, Zugriff und Auswertung der Telekommunikationsdaten angewiesen.[14]Ein großes Problem bei nachträglicher Erhebung der Daten wegen bestimmten Verdachts im Einzelfall liegt jedoch darin, dass viele nutzbare Telekommunikationsdaten nicht mehr vorhanden sind.[15]Eine Mindestspeicherungspflicht soll daher eine vorsorgliche umfassende Protokollierung der Telekommunikationsdaten von Bürgern schaffen und damit sicherstellen, dass die nutzbaren Telekommunikationsdaten bei Bedarf zur Verfügung stehen. Die Verkehrsdaten der Bürger werden also nicht aufgrund des konkreten und bewiesenen Verdachts gegen eine bestimmte Person, sondern unterschiedslos auf Vorrat gespeichert. Die anlasslose Speicherung dient dem zukünftigen Zugriff und der Verwendung der Daten.

Das Verhältnis zwischen Freiheit und Sicherheit ist immer mehr von den neuen technischen Bedingungen, insbesondere auch von der zunehmenden Verarbeitung personenbezogener Daten gekennzeichnet.[16] Dieser Wandel in Bezug auf die Fragen zur Sicherheitsstrategie bringt das Recht auf informationelle Selbstbestimmung in große Gefahr. Angesichts der Verbreitung von Telekommunikationstechnologie und der Unverzichtbarkeit der Telekommunikationsmittel in der heutigen Welt[17] birgt die Vorratsdatenspeicherung das große Risiko, dass eine Totalüberwachung der Bürger geschaffen und die Ausübung der Freiheitsrechte für das demokratische Gemeinwesen gehemmt

---

11 Ähnlich *Moser-Knierim*, S. 35.

12 Wie genau eine derartige Ermittlung funktioniert, siehe *Hammer/Knopp*, DuD 2015, 503 (504 f.).

13 *Roßnagel/Moser-Knierim/Schweda*, S. 17; *Breyer*, S.12 f.; *Albrecht/Kilchling*, S. 71 f.

14 Vgl. *Breyer*, S. 12 f.

15 Bundesministerium des Innern, Bundesministerium der Justiz: Erster Periodischer Sicherheitsbericht, Berlin, 2001, S. 200, abrufbar unter https://zh.scribd.com/doc/3993633/KRIM-BKA-PSB-I-2001.

16 Siehe auch *Kipker*, S. 2.

17 *Hoffmann-Riem*, JZ 2008, 1009 (1009 ff.); *Kutscha*, LKV 2008, 481 (481).

wird.[18] Darüber hinaus besteht eine erhebliche Enthüllungs- und Missbrauchsgefahr bei der flächendeckenden Speicherung riesiger Mengen von Telekommunikationsdaten.[19]

Zwar ist zutreffend, dass der Staat seine Politik der Strafverfolgung und Gefahrenabwehr an den technischen Fortschritt und die geänderte Bedrohungslage anpassen und deshalb durch Sicherheitsmaßnahmen das Recht auf Handlungsfreiheit und Privatsphäre beschränken darf oder auch muss. Aber die sicherheitsrechtliche Anpassung an die technischen Neuheiten muss im verfassungsrechtlichen Rahmen bleiben. Die Beschränkung muss also auf das absolut notwendige Maß begrenzt und das Risiko des Missbrauches möglichst minimalisiert werden.[20]

Das neu zu justierende Verhältnis zwischen Freiheit und Sicherheit stellt sich nicht nur Deutschland. Die anlasslose Speicherung von Telekommunikationsdaten auf Vorrat kommt auch in der Volksrepublik China (VR China) zur Anwendung. Aber bezüglich des Speicherungsumfangs, der Verpflichtungen und der Verwendungsvoraussetzungen unterscheidet sich die Ausgestaltung der Vorratsdatenspeicherung in der VR China sehr von der in Deutschland.

Auch für die VR China stellt international agierender Terrorismus und Cybercrime eine Bedrohung dar. Der Gesetzgeber ist also mit den gleichen Herausforderungen konfrontiert wie in Deutschland, um auf die neue Bedrohungslage und die technischen Bedingungen zum Zweck der Strafverfolgung und Gefahrenabwehr reagieren zu können. Kennzeichen dieser Anpassungsreaktion ist die stetige Erweiterung der staatlichen Kontrollbefugnisse auf Kosten der Freiheit und Privatsphäre der Bürger. Dazu zählen die immer umfassendere Erhebung von personenbezogenen Daten auf Vorrat und immer niedrigere Zugriffs- sowie Verwendungshürden. Dies führt zu einer erheblichen Gefahr für die Handlungsfreiheit und Privatsphäre der Bürger. Diese Gefahr droht sich insofern zu vergrößern, als ein strukturierter Rechtsrahmen für den wirksamen Grundrechtsschutz bisher noch nicht in der VR China umfassend aufgebaut wurde.

Im vorhandenen Rechtsrahmen ist das grundrechtliche Korrespondenzgeheimnis der chinesischen Verfassung (Verf VRC) relevant. Für den Schutz

---

18 Siehe auch *Puschke*/*Singelnstein*, NJW 2008, 113 (118).

19 Vgl. *Breyer*, S. 221 ff., S. 228 ff.; *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 92; *Szuba*, S. 104; *Moser-Knierim*, S. 184-185.

20 Siehe auch *Roßnagel*/*Moser-Knierim*/*Schweda*, S.12;

der personenbezogenen Daten kommt auch die „Würde der Persönlichkeit“ aus Art. 38 Verf VRC in Betracht. Ferner können grundlegende Prinzipien des Datenschutzes und allgemeine Anforderungen an die Datensicherheit in verschiedenen einzelnen Gesetzen sowie Regelungswerken gefunden werden. Mangels Konkretisierung der Grundsätze und Bestimmtheit der Rechtsvorschriften ist es jedoch sehr fraglich, ob das vorhandene grundrechtliche Schutzniveau dem Gewicht der Vorratsdatenspeicherung ausreichend Rechnung tragen kann.

Vor diesem Hintergrund ist es dringend geboten, dass der chinesische Gesetzgeber bei der Ausgestaltung der Vorratsdatenspeicherung die staatlichen Eingriffsbefugnisse durch genaue und bestimmte Regelung begrenzt. Anlässlich der grundrechtlichen Analyse der Vorratsdatenspeicherung in Deutschland ist es daher angezeigt, die Verfassungsmäßigkeit der chinesischen Vorratsdatenspeicherung zu eruieren und Vorschläge zur Ausfüllung der Schutzlücken der relevanten Grundrechte zu auszuarbeiten.

Kapitel 2: Die Vorratsdatenspeicherung in Deutschland und Europa

A. Rückblick auf die Entstehung und Entwicklung der Vorratsdatenspeicherung

I. Europäische Union als treibender Faktor

Auf europäischer Ebene wurde eine Vorratsdatenspeicherung bereits lange diskutiert. Kurz nach den Terroranschlägen vom 11. September 2001 in den USA wurde auf europäischer Ebene festgestellt, dass der Terrorismus eine weltweite Herausforderung und der Kampf gegen den Terrorismus ein vorrangiges Ziel der Europäischen Union darstelle. Dafür wurde Solidarität und Zusammenarbeit mit den Vereinigten Staaten gefordert.[21] In den Schlussfolgerungen des Rates für Inneres und Justiz vom 20. September 2001 wurde per Vorschlag von der Europäische Kommission gefordert, dass eine effektivere Aufklärung von Straftaten mittels elektronischer Kommunikationssysteme sichergestellt werden soll.[22] So haben Belgien[23] und Dänemark[24] nacheinander in ihrer Ratspräsidentschaft versucht, Vorgaben für die Mindestspeicherung der Telekommunikationsdaten festzulegen. Beide Vorstöße konnten sich allerdings nicht durchsetzen.

Die Terroranschläge vom 11. März 2004 in Madrid haben schnelle Reaktionen ausgelöst. Der Europäische Rat hat am 25. März 2004 die Erklärung zum Kampf gegen den Terrorismus angenommen, in der der Rat der EU beauftragt wurde, Vorschläge für Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch Diensteanbieter zu beraten.[25] Vor diesem Hintergrund haben die Regierungen von Frankreich, Irland, Schweden und dem Vereinigten Königreich am 28. April 2004 dem Rat den Entwurf eines Rahmenbeschlusses über eine einheitliche Vorratsdatenspeicherung der Telekommunikations-

---

21 Schlussfolgerungen und Aktionsplan anlässlich der außerordentlichen Tagung des Europäischen Rates am 21. September 2001 in Brüssel, SN 140/01, S. 1.

22 Schlussfolgerungen vom Rat der Europäischen Union für Inneres und Justiz, Brüssel, 20.9.2001, SN 3926/6/01, S. 3.

23 Entwurf eines Rahmenbeschlusses der dritten Säule, englische Fassung abrufbar unter http://www.statewatch.org/news/2002/aug/05datafd.htm.

24 Draft Council conclusions on information technology-related measures concerning the investigation and prosecution of organized crime, Brussels, 24 June 2002 (28.06), 10358/02.

25 Erklärung zum Kampf gegen den Terrorismus, Brüssel, den 25. März 2004, 7906/04, S. 4.

verkehrsdaten vorgelegt und ihn in das Europäische Parlament eingebracht.[26] Wegen der uneinheitlichen Stellungnahmen und starker Kritik wurde dieser Entwurf nicht weiter diskutiert und zuletzt nicht verwirklicht.

Einen weiteren Anstoß zur Vorratsdatenspeicherung gaben die Terroranschläge in London vom 7. Juli 2005. Die Angst vor neuen Terroranschlägen und der Handlungsdruck, den Terrorismus zu bekämpfen, beschleunigte die Reaktion der europäischen Gesetzgebung.[27] In den Schlussfolgerungen der Ratspräsidentschaft vom 15. Juli 2005 wurde zum Ausdruck gebracht, dass die Gesetzgebungsarbeiten zur Stärkung der polizeilichen und justiziellen Zusammenarbeit, insbesondere im Hinblick auf die Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten, vorrangig behandelt werde müssen.[28] Daraufhin hat die EU-Kommission den Entwurf für eine Richtlinie zur Vorratsdatenspeicherung am 21. September 2005 vorgelegt.[29] Trotz vorgebrachter Bedenken wurde der Entwurf in kurzer Zeit verabschiedet, vom Europäischen Parlament beschlossen und schließlich vom Ministerrat angenommen. Schließlich trat die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung am 3. Mai 2006 in Kraft.[30]

Sie hat heftige Kritik hervorgerufen. Vor allem wurde ihre kompetenzrechtliche Grundlage in Zweifel gestellt. Es wurde vorgetragen, dass es sich bei einer Vorratsdatenspeicherung auf europäischer Ebene nicht um die Errichtung und das Funktionieren des Binnenmarktes drehte.[31] Sie lege vielmehr den Mitgliedstaaten die Pflicht auf, alle Telekommunikationsdaten der Bürger auf Vorrat zur Strafverfolgung und Gefahrenabwehr zu speichern. Unter anderem habe sie den Mitgliedstaaten umfangreichen Umsetzungsspielraum

---

26 Entwurf eines Rahmenbeschluss über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus, Brüssel, den 28. April 2004 (06.05), 8958/04.

27 In der Literatur wird vielfach darauf hingewiesen, dass diese Gesetzgebung das schnellste Rechtssetzungsverfahren der EU ist. Beispielhaft siehe *Moser-Knierim*, S. 14; *Albrecht*, FoR 1/2007, S. 13; *Alvaro*, DANA 2006, 52 (52 f.).

28 Schlussfolgerungen des Vorsitzes von dem Europäischen Rat, Brüssel, den 15. Juli 2005 (22.07), 10255/1/05, S. 5.

29 Vorschlag für eine Richtlinie des europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, Brüssel, den 21. 9. 2005, KOM (2005) 438 endgültig, 2005/0182 (COD).

30 ABI. EG Nr. L 105, S. 54-60.

31 Kritik an der Rechtsetzungskompetenz der Richtlinie siehe beispielhaft *Breyer*, StV 2007,214 (215f.); *Braum*, ZRP 2009, 174 (175); *Ambos*, JZ 2009, 468 (469); *Simitis*, NJW 2006, 2011 (2013); *Terhechte*, EuZW 2009, 199 (201).

gelassen. Damit habe hier keine Harmonisierung der Vorschriften zur Vorratsdatenspeicherung im Rahmen des Funktionierens des Binnenmarktes vorgelegen.[32]

Irland hat in der Folge am 6. Juni 2006 eine Nichtigkeitsklage gegen die Richtlinie vor dem Europäischen Gerichtshof (EuGH) eingereicht.[33] Die Klage wurde aber vom EuGH am 10. Februar 2009 abgewiesen. Der EuGH war der Auffassung, dass die Richtlinie zur Vorratsdatenspeicherung die Tätigkeiten der Telekommunikationsdienstanbieter im Binnenmarkt betraf und damit in überwiegendem Maße das Ziel der Schaffung eines europäischen Binnenmarkts verfolge.[34] Der Streit um die Rechtssetzungskompetenz der Richtlinie sowie die allgemeine Frage, ob ein Rechtsakt innerhalb des Gemeinschaftsrechts oder innerhalb des Unionsrechts erlassen werden muss, wurde jedoch nach dem Inkrafttreten des Vertrags von Lissabon beendet.[35] Die zur damaligen dritten Säule, und zwar der „Polizeilichen und justiziellen Zusammenarbeit in Strafsachen", gehörenden Regelungsgegenstände können nach dem Inkrafttreten des Vertrags von Lissabon durch eine Richtlinie geregelt werden.[36]

Über die Kompetenzfrage hinaus gab es Bedenken im Hinblick auf die Konformität mit den Gemeinschaftsgrundrechten, vor allem mit dem Recht auf Achtung des Privat- und Familienlebens (Art. 7 GRCh), dem Schutz personenbezogener Daten in Art. 8 GRCh und auch Art. 8 EMRK.[37] Aber diese wesentliche Frage wurde vom EuGH in seinem Urteil vom 10. Februar 2009 nicht beantwortet. Angesichts der nationalen grundrechtlichen Bedenken erfolgte in vielen Mitgliedsstaaten nicht nur eine verzögerte Umsetzung,[38]

---

32 *Gitter*/*Schnabel*, MMR 2007, 411 (412); *Gietl*/*Tomasic*, DuD 2008, 795 (796 f.).

33 Az. C-301/06, abrufbar unter: http://curia.europa.eu/juris/document/document.jsf?docid=64262&doclang=de.

34 EuGH Urt. V. 10.2.2009, C-301/06, Rn. 83-84.

35 Siehe auch *Szuba*, S. 85; *Roßnagel*, DuD 2010, 544 (544); *Hornung*/*Schnabel*, DVBI 2010, 824 (825). Änderung bezüglich der Rechtsetzungskompetenz nach Inkrafttreten des Vertrags von Lissabon siehe *Mayer*, JuS 2010, 189 (193); *Leutheusser-Schnarrenberger*, DuD 2010, 519 (519 f.); *Kahler*, DuD 2008, 449 (454).

36 *Gundel*, in: *Ehlers* (Hrsg.), 2014, S. 839, Rn. 1, S. 862 Rn. 44; *Schwarze*, in: *Schwarze*/*Becker*/*Hatje*/*Schoo* (Hrsg.), 2012, Einführung, Rn. 48; *Hatje*/*Kindt*, NJW 2008, 1761 (1763); *Weber*, EuZW 2008, 7 (13), siehe auch *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 87; *Szuba*, S. 84.

37 Grundrechtliche Bedenken gegen die Richtlinie siehe beispielhaft in *Zöller*, GA 2007, 393 (411); *Gercke*, MMR 2008, 291 (293); *Westphal*, EuZW 2006, 555 (558); *Gola*/*Klug*/*Reif*, NJW 2007, 2599 (2599); *Leutheusser-Schnarrenberger*, ZPR 2007, 9 (10); *Bizer*, DuD 2007, 586 (587); *Petri*, DuD 2011, 607 (609 f.).

38 Der Zustand der Verzögerung der Umsetzung in den Mitgliedstaaten siehe in *Roßnagel*/*Moser-Knierim*/*Schweda*, S.36 ff.; *Forgó*/*Jlussi*/*Klügel*/*Krügel*, DuD 2008, 680 (681 f.).

sondern auch Nichtigkeitsurteile in Bezug auf die jeweiligen Umsetzungsgesetze von nationalen Verfassungsgerichten wie zum Beispiel in Rumänien am 8. Oktober 2009, in der Tschechischen Republik am 31. März 2011[39] und Deutschland am 2. März 2010.[40]

Der irische High Court hat in einem Beschwerdeverfahren der Bürgerrechtsorganisation Digital Rights Irland am 5. Mai 2010 eine Vorlage zum EuGH dahingehend eingereicht, die Vereinbarkeit der Richtlinie mit den europäischen Grundrechten vom EuGH überprüfen zu lassen.[41] Ein weiterer Anlass für den EuGH, die materielle Rechtmäßigkeit der Richtlinie zu beurteilen, wurde durch das vom österreichischen Verfassungsgericht initiierte Vorabentscheidungsverfahren gegeben.[42] Vor diesem Hintergrund stand der EuGH vor einer dringend gebotenen finalen Entscheidung über die materielle Rechtmäßigkeit der zu diesem Zeitpunkt höchst umstrittenen Richtlinie zur Vorratsdatenspeicherung.

II. Umsetzung der Richtlinie 2006/24/EG in Deutschland

Als Mitgliedstaat der Europäischen Union galt auch für Deutschland die Umsetzungspflicht in Bezug zur Richtlinie der Vorratsdatenspeicherung. Durch das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ vom 21.12.2007 wurde die Vorratsdatenspeicherung umgesetzt. Das Umsetzungsgesetz trat am 1.1.2008 in Kraft.[43]

Demgemäß wurden §§ 113a, 113b Telekommunikationsgesetz (TKG) neu eingeführt und § 100g Strafprozessordnung (StPO) neugestaltet.[44] Die Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sind nach diesen Vorschriften verpflichtet, die von ihnen beim Dienstanbieten erzeugten oder verarbeiteten Verkehrsdaten zum Zweck der Strafverfolgung sechs Monate zu speichern (§ 113a Abs. 1 TKG a.F.[45]). Werden die Voraussetzungen in

---

39 Vorstellung der nationalen Urteile in Rumänien und Tschechische Republik siehe *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 39-42; *Albrecht*/*Kilchling*, S. 6 ff.

40 BVerfG, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, vom 2.3.2010.

41 High Court of Ireland, Vorabentscheidungsersuchen v. 11.6.2012, beim EuGH anhängig als Rs. C-293/12.

42 Österreich Verfassungsgerichtshof, Vorabentscheidungsersuchen v. 19.12.2012, beim EuGH anhängig als Rs. C-594/12.

43 BGBI. I, 3198 vom 31.12.2007.

44 Im Jahr 2015 wurden die Normen abermals reformiert. Dies geschah als Reaktion auf die Urteile des Bundesverfassungsgerichts und des Europäischen Gerichtshofs; siehe hierzu. Die zitierten Normen des TKG wurden strukturell novelliert; deshalb werden die ursprünglichen Fassungen mit a.F. gekennzeichnet.

45 Die Speicherungspflicht ist nun in § 113b TKG geregelt, siehe hierzu Kapitel 2,

§ 100g Abs. 1 StPO erfüllt, dürfen die Vorratsdaten auch ohne Wissen des Betroffenen erhoben werden. Die Verpflichteten müssen die Qualität und den Schutz der gespeicherten Daten gemäß der im Bereich der Telekommunikation erforderlichen Sorgfalt beachten (§ 113a Abs. 10 S. 1 TKG a.F.) und die Vorratsdaten innerhalb eines Monats nach Ablauf des sechsten Monats löschen (§ 113a Abs. 11 TKG a.F.). Die Inhalte der Telekommunikation dürfen nicht gespeichert werden (§ 113a Abs. 8 TKG a.F.). Eine Entschädigung für die Anbieter wegen der Erfüllung der Speicherpflicht wurde nicht geregelt.

Die Vorratsdatenspeicherung ist kein neues Thema in Deutschland. Im Jahr 1996 wurde ein mit ihr vergleichbares Gesetzesvorhaben thematisiert. Der Bundesrat hat damals eine Mindestspeicherfrist der Telekommunikationsverkehrsdaten anlässlich der Einführung der Regulierungsbehörde für Telekommunikation und Post, die TKG-Novelle gefordert, aber diese wurde abgelehnt.

Danach kam die Vorratsdatenspeicherung mehrfach in Form von Gesetzes- und Regierungsentwürfen vor, scheiterte aber stets an der Zustimmung des Bundestags aufgrund verfassungsrechtlicher Bedenken.[46] Damit ist es nicht überraschend, dass das Umsetzungsgesetz der Richtlinie 2006/24/EG heftig kritisiert wurde. Es hat Proteste hervorgerufen hat.[47] Kurz vor dem Inkrafttreten des Umsetzungsgesetzes hat die Bürgerrechtsinitiative „Arbeitskreis Vorratsdatenspeicherung“[48] (AK VDS) Verfassungsbeschwerde eingelegt. Sie war der Meinung, dass das Umsetzungsgesetz das Fernmeldegeheimnis, das Recht auf informationelle Selbstbestimmung und die Berufsfreiheit verletze.[49] Am 2. März 2010 hat das Bundesverfassungsgericht die Regelungen

---

C.III.1.

46 Details der Geschichte der Gesetzgebungsvorhaben der Vorratsdatenspeicherung in Deutschland siehe in *Gausling*, S. 47 ff.; *Gietl*, DuD 2008, (317) 317; *Gietl*, K&R 2007, 545 (45 ff.).

47 Für Kritik und Proteste siehe beispielsweise folgende Meldungen: https://netzpolitik.org/2007/spd-medienkommission-gegen-vorratsdatenspeicherung/ [31.1.2019]; https://www.heise.de/newsticker/meldung/Land-Berlin-legt-Widerspruch-gegen-Gesetz-zur-TK-ueberwachung-ein-198919.html [31.1.2019]; https://netzpolitik.org/2007/vorratsdatenspeicherung-kommt-proteste-gehen-weiter/ [31.1.2019].

48 Der AK VDS ist ein bundesweiter Zusammenschluss von Bürgerrechtlern, Datenschützern und Internetnutzern, wurde im Dezember 2005 gegründet. Sein Ziel ist gegen die Überwachung im Allgemeinen und gegen die Totalprotokollierung der Telekommunikation und anderer Verhaltensdaten im Besonderen. Homepage: http://www.vorratsdatenspeicherung.de.

49 Beschwerdeführer sind auch Vertreter von FDP und Bündnis 90/Die Grünen (insgesamt über 34,000 Personen), Fassung der Verfassungsbeschwerde ist abrufbar unter http://wiki.vorratsdatenspeicherung.de/images/Verfassungsbeschwerde_Vorratsdaten

in TKG und StPO der Vorratsdatenspeicherung wegen Verstoßes gegen Art. 10 Abs. 1 des Grundgesetzes für nichtig erklärt und angeordnet, die nach diesen Regelungen bereits gespeicherten Vorratsdaten unverzüglich zu löschen.[50]

Trotz der Feststellung der Verfassungswidrigkeit des Umsetzungsgesetzes hat das BVerfG die Vorratsdatenspeicherung als *„nicht von vorneherein schlechthin verfassungswidrig"* angesehen.[51] Bei der Prüfung der Verhältnismäßigkeit der Vorratsdatenspeicherung hat das BVerfG ausgeführt, dass die Effektivierung der Strafverfolgung sowie die Gefahrenabwehr und die Erfüllung der Aufgaben der Nachrichtendienste legitime Zwecke seien und den Eingriff in das Fernmeldegeheimnis grundsätzlich rechtfertigen könnten.[52] Eine vorsorgliche Speicherung der Telekommunikationsdaten dürfe auch als ein geeignetes und erforderliches Mittel wegen ihrer Tauglichkeit zur Erreichung des Ziels qualifiziert werden.[53]

Nach Maßstab der Angemessenheit sei die Vorratsdatenspeicherung trotz des mit ihr verbundenen Eingriffsgewichts verfassungsrechtlich nicht schlechthin verboten.[54] Die Vorratsspeicherung werde einerseits nicht direkt durch den Staat, sondern durch die privaten Diensteanbieter verwirklicht, deswegen bleibe sie trotz der umfassenden Streubreite wirksam begrenzt.[55] Andererseits sei die Vorratsdatenspeicherung in noch begrenzt bleibender Weise für eine effektive Strafverfolgung und Gefahrenabwehr in der modernen Welt von besonderer Bedeutung.[56] Die verfassungsrechtliche Unbedenklichkeit der Vorratsdatenspeicherung setze jedoch voraus, dass ihre Ausgestaltung verfassungsrechtlichen Anforderungen insbesondere hinsichtlich der Datensicherheit, des Umfangs der Datenverwendung, der Transparenz und des Rechtsschutzes unterliege.[57] Das Umsetzungsgesetz habe nicht dem besonderen Gewicht einer solchen Speicherung angemessen Rechnung getragen und sei damit nicht angemessen.[58]

---

speicherung.pdf.

50 BVerfGE, 125, 260. Zu diesem Urteil siehe *Gietl*, DuD 2010, 398; *Roßnagel*, NJW 2010, 1238; *Hornung*/*Schnabel*, DVBI. 2010; *Petri*, in: *Roßnagel* (Hrsg.), S. 123; *Forgó*/*Krügel*, K&R 2010, 217.

51 BVerfGE, 125, 260 (316).

52 BVerfGE, 125, 260 (316 f.).

53 BVerfGE, 125, 260 (317 ff.).

54 BVerfGE, 125, 260 (318).

55 BVerfGE, 125, 260 (321).

56 BVerfGE, 125, 260 (322).

57 BVerfGE, 125, 260 (325).

58 BVerfGE, 125, 260 (325 ff.).

Nach dem Ablauf der Umsetzungsfrist hat die Europäische Kommission ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet, weil Deutschland die Richtlinie nicht rechtzeitig umgesetzt hat.[59] Nach dem Ungültigkeitsurteil des Umsetzungsgesetzes stand Deutschland unter dem Druck einer neuen Umsetzung und eines enormen Strafgeldes.[60]

III. Ungültigkeit der Richtlinie 2006/24/EG

In den Vorabentscheidungsersuchen des High Court Irland und vom Verfassungsgerichtshofs Österreich wurde vom EuGH erwartet, vor allem die Frage zu beantworten, ob und inwieweit die Richtlinie 2006/24/EG mit der Europäischen Charta der Grundrechte vereinbar sei. Am 8. April 2014 hat der EuGH die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung wegen Verstoßes gegen Art. 7 und 8 GRCh für ungültig erklärt.[61]

In diesem bedeutsamen Urteil hat der EuGH einen schwerwiegenden Eingriff der Richtlinie 2006/24/EG in das Recht auf Achtung des Privatlebens und auf Schutz der personenbezogenen Daten festgestellt.[62] Obwohl die Vorratsdatenspeicherung einem Gemeinwohlziel diene[63] und geeignet sei, dieses Ziel zu erreichen,[64] sei sie angemessen. Denn die Vorratsdatenspeicherung werde ohne Ausnahme insbesondere für Berufsgeheimnisträger, und zudem anlasslos durchgeführt.[65] Die Voraussetzungen des Eingriffs seien nicht klar bestimmt und mit differenzierten Regeln ausgestaltet. Dies führe dazu, dass die Beeinträchtigung der Vorratsdatenspeicherung nicht auf das absolut Notwendige beschränkt werde.[66] Damit sei die Richtlinie zur Vorratsdatenspeicherung unverhältnismäßig und grundrechtswidrig.

Der Streit über Rechtmäßigkeit der Richtlinie zur Vorratsdatenspeicherung wurde so schließlich zu einem Ende gebracht. Das Vertragsverletzungsverfahren gegen Deutschland, weil es die Richtlinie nicht rechtzeitig umgesetzt

---

59 Rechtssache C-329/12, 11.07.2012, abrufbar unter http://eur-lex.europa.eu/legal-content/de/TXT/PDF/?uri=uriserv%3AOJ.C_.2012.287.01.0023.01.DEU. Meldung dazu abrufbar unter https://www.heise.de/newsticker/meldung/Vorratsdatenspeicherung-Bruessel-klagt-gegen-Berlin-1587599.html.

60 Meldung dazu abrufbar unter http://www.faz.net/aktuell/politik/inland/vorratsdatenspeicherung-jeden-tag-315-036-54-euro-strafe-11769721.html.

61 EuGH, Urteil in Rechtssachen C-293/12 und C-594/12 v. 08.04.2014.

62 EuGH, Urteil in Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn 37.

63 EuGH, Urteil in Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn 41-44.

64 EuGH, Urteil in Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn 46.

65 EuGH, Urteil in Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn 57, 58.

66 EuGH, Urteil in den Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn 62 ff.

hat, wurde zurückgenommen. Deutschland musste damit keine neuen Umsetzungsregelungen der Vorratsdatenspeicherung ausarbeiten.

IV. Neue Auflage der Vorratsdatenspeicherung in Deutschland

Trotz des Ungültigkeitsurteils der Richtlinie 2006/24/EG vom EuGH war das Thema der Vorratsdatenspeicherung in Deutschland immer noch nicht beendet und wurde im Jahr 2015 wieder auf die Tagesordnung gesetzt. Das Bundesministerium der Justiz und des Verbraucherschutzes veröffentlichte eine Leitlinie[67] und einen Referentenentwurf zu einem Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten.[68] Der Gesetzentwurf wurde am 6. Juni 2015 von den Fraktionen der CDU/CSU und SPD im Bundestag eingebracht.[69] Die Bundesregierung hat den gleichen Gesetzentwurf am 15. Juni 2015 vorgelegt.[70]

Dieser Gesetzentwurf wurde am 16. Oktober 2015 vom Bundestag beschlossen. Der Bundesrat stimmte am 6. November 2015 zu. Nach einem sehr kurzen Gesetzgebungsverfahren wurde das „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ am 17. Dezember 2015 verkündet und es trat am 18. Dezember 2015 in Kraft.[71]

Nach den neuen Regeln der Vorratsdatenspeicherung wurden die §§ 100g, 100i und 101 StPO geändert, §§ 101a und 101b StPO neu eingeführt und §§ 113a bis 113g TKG überarbeitet. Dadurch wird die Vorratsdatenspeicherung nach den Ungültigkeitsurteilen zur Vorratsdatenspeicherung vom BVerfG und dem EuGH in veränderter Form eingeführt. Deren Vereinbarkeit mit den europäischen Grundrechten sowie den Anforderungen im Ungültigkeitsurteil der Richtlinie 2006/24/EG des EuGH werden stark bezweifelt.[72] Gegen das neue Gesetz werden beim BVerfG viele Verfassungsbeschwerden

---

67 Die Fassung der Leitlinie ist abrufbar unter http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/leitlinien-vorratsdatenspeicherung.html [31.1.2019].

68 Die Fassung des Entwurfs ist abrufbar unter http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Hoechstspeicher-frist.pdf;jsessionid=5C6B11AE53EF8291CBAF1A9B47C4618B.2_cid297?__blob=publicationFile&v=6 [31.1.2019].

69 BT-Drs. 18/5088.

70 BT-Drs. 18/5171.

71 BGBI. I 2015, 2218. Details des Gesetzgebungsverfahrens der neuen Regelungen zur Vorratsdatenspeicherung siehe *Roßnagel*, NJW, 2016, 533 (535).

72 Kritik siehe *Roßnagel*, NJW, 2016, 533 (538); *Dix*/*Kipker*/*Schaar*, ZD 2015, 300 (302 ff.); *Forgó*/ *Heermann*, K&R 2015, 753 (754 ff.); *Nachbaur*, ZRP 2015, 215 (217).

eingereicht, zwei davon auch mit Eilantrag.[73] Die Eilanträge wurden abgelehnt.[74] Somit ist die Beurteilung der Verfassungsmäßigkeit sowie die Vereinbarkeit mit den europäischen Grundrechten der neuen Vorratsdatenspeicherung vom Bundesverfassungsgericht im Hauptverfahren zu klären.

V. Das Verbot einer allgemeinen und unterschiedslosen Vorratsdatenspeicherung in den Mitgliedsstaaten des EuGH

Nach dem Ungültigkeitsurteil der Richtlinie 2006/24/EG hat der EuGH am 21. Dezember 2016 im Urteil in den verbundenen Rechtssachen C-698/15 und C-698/15 weiter festgestellt, dass die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG einer nationalen Regelung entgegenstehe, die zum Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierter Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsehe.[75] Geklagt hatte zum einen ein schwedischer Telekommunikationsanbieter, der sich gegen die behördliche Verfügung wehrte, die Vorratsdatenspeicherung vorzunehmen. Zum anderen hatten sich britische Staatsbürger gegen die nationale Regelung zur Vorratsdatenspeicherung gewandt.

Nach Ansicht des EuGH untersagt die Richtlinie 2002/58/EG den Mitgliedstaaten nicht, eine Regelung zu erlassen, die zur Bekämpfung schwerer Straftaten vorbeugend die gezielte Vorratsdatenspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern die Vorratsdatenspeicherung hinsichtlich Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsdatenspeicherung auf das absolut Notwendige beschränkt ist.[76] Durch dieses Urteil hat der EuGH eine unterschiedslose und anlasslose Speicherung aller Bürger in den Mitgliedstaaten verboten, jedoch wird eine

---

73 Meldung dazu ist abrufbar unter https://netzpolitik.org/2016/eilantraege-abgelehnt-vorratsdatenspeicherung-hat-erheblichen-einschuechterungseffekt-bleibt-aber-vorerst-in-kraft/ [31.1.2019].

74 BVerfG, Beschlüsse vom 8. Juni 2016 – 1 BvQ 42/15 und 1 BvR 229/16. ZD 2016, 433; NVwZ 2016, 1240;

75 Pressemitteilung Nr. 145/16, Luxemburg, den 21. Dezember 2016, die Übersetzung in deutscher Sprache des EuGH-Urteils ist abrufbar unter http://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=DE [31.1.2019].

76 EuGH, Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 vom 21.12.2016, Nr. 108.

vorsorgliche gezielte Vorratsdatenspeicherung von Telekommunikationsdaten nur unter strengen Voraussetzungen für zulässig erklärt.[77]

Wegen dieses Urteils des EuGH steht die Vereinbarkeit der wieder eingeführten Vorratsdatenspeicherung in Deutschland mit der Grundrechtecharta noch einmal im Vordergrund. Das Oberverwaltungsgericht Nordrhein-Westfalen in Köln hat am 22. Juni 2017 in einem Beschluss klargestellt, dass die neue Regelung der Vorratsdatenspeicherung *„im Sinne des Unionsrechts nicht auf das absolut Notwendige beschränkt ist“* und der Eingriff in die unternehmerische Freiheit *„ist jedenfalls aus unionsrechtlicher Hinsicht nicht durch die Regelung des § 113a Abs. 1 i.V.m. § 113b Abs. 1 und 3 TKG als dem Grunde nach gerechtfertigt anzusehen, weil es insoweit an einer mit Art. 15 Abs. 1 der Richtlinie 2002/58/EG im Licht der Grundrechte aus Art. 7, 8, 11 und Art. 52 Abs. 1 der Charta zu vereinbarenden gesetzlichen Grundlage fehlt“*.[78] Die Bundesnetzagentur hat daraufhin die Anwendung der Vorschriften zur Vorratsdatenspeicherung ausgesetzt.

Zum gleichen Ergebnis kam auch der wissenschaftliche Dienst des Deutschen Bundestages im Gutachten zur Vereinbarkeit der neuen Regelung mit dem EuGH-Urteil zur Vorratsdatenspeicherung.[79] Den Antrag auf Erlass einer einstweiligen Anordnung gegen die neu ausgestalteten Regelungen zur Vorratsdatenspeicherung aufgrund dieses Urteils vom EuGH wurde vom Bundesverfassungsgericht im März 2017 abgelehnt.[80] Eine abschließende Beurteilung vom Bundesverfassungsgericht über die Vereinbarkeit neuer Vorratsdatenspeicherungen mit der Grundrechtecharta steht noch aus. In einem späteren Kapitel soll dieser Frage vertieft nachgegangen werden.[81]

---

77 Pressemitteilung Nr. 145/16, Luxemburg, den 21. Dezember 2016.

78 Beschluss des OVG NRW, 13 B 238/17, Rn 86 und 134.

79 Ausarbeitung des Fachbereichs Europa des Deutschen Bundestages zur Vereinbarkeit des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten mit dem EuGH-Urteil vom 21. Dezember 2016 zur Vorratsdatenspeicherung vom 12. Januar 2017, PE 6 – 3000 – 167/16, abrufbar unter https://www.bundestag.de/analysen.

80 BVerfG, Beschluss vom 26. März 2017 – 1 BvR 141/16.

81 Siehe Kapitel 2, C. IV.

B. Grundrechtliche Anforderungen an die Vorratsdatenspeicherung (Grundgesetz)

Seit dem Inkrafttreten der Richtlinie 2006/24/EG hat die Vorratsdatenspeicherung heftige Diskussionen ausgelöst. Dabei steht häufig die Vereinbarkeit der verdachtsunabhängigen Speicherung der Telekommunikationsdaten aller Bürger mit Grundrechten im Mittelpunkt. Die Vorratsdatenspeicherung könnte als taugliches Hilfsmittel zur Strafverfolgung und Gefahrenabwehr dienen. Jedoch ist ihre Verfassungsmäßigkeit wegen der großen Eingriffsintensität und des erheblichen Missbrauchspotenzials sehr sorgfältig zu überprüfen.

Relevante Grundrechte sind insbesondere das Recht auf das Fernmeldegeheimnis gemäß Art. 10 Abs. 1 GG und die Berufsfreiheit gemäß Art. 12 GG. Um die Vereinbarkeit der Vorratsdatenspeicherung mit den oben genannten Grundrechten zu überprüfen, sollen der Schutzbereich des jeweiligen einzelnen Grundrechts und der Eingriff durch die Durchführung der Vorratsdatenspeicherung erläutert werden. Danach wird im Rahmen der Überprüfung der verfassungsrechtlichen Rechtfertigung der Grundrechtseingriffe das Hauptaugenmerk auf die Verhältnismäßigkeit gelegt. Dafür wird der Grundrechtseingriff anhand der Kriterien des legitimen Zwecks, der Geeignetheit, der Erforderlichkeit sowie der Angemessenheit und anderer verfassungsrechtlicher Anforderungen überprüft. Bei dieser Überprüfung werden verschiedene Auffassungen aus der aktuellen Literatur und insbesondere die Argumentationslinien in den Urteilen des Bundesverfassungsgerichts über die Vorratsdatenspeicherung berücksichtigt.

I. Fernmeldegeheimnis (Art. 10 Abs. 1 GG)

1. Schutzbereich des Fernmeldegeheimnisses

In Art. 10 Abs. 1 GG wird die Unverletzlichkeit des Brief-, Post- und Fernmeldegeheimnisses festgeschrieben. Zwar werden drei unterschiedliche Kommunikationsmittel aufgelistet, aber Art. 10 Abs. 1 GG stellt ein einheitliches Grundrecht dar.[82] Dieses einheitliche Grundrecht gewährleistet *„die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Informationen und schützt damit zugleich die Würde des Menschen“*.[83] Im Vergleich zur direkten individuellen Kommu-

---

82 *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 10, Rn. 1; *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 10 Rn. 8.

83 BVerfGE 115, 166 (64).

nikation, die zwischen den Beteiligten zur gleichen Zeit am gleichen Ort stattfindet, ist die Fernkommunikation aufgrund der zeitlichen sowie räumlichen Distanz der Gefahr der staatlichen Kenntnisnahme besonders ausgesetzt.[84] Damit gewährleitstet Art. 10 Abs. 1 GG „eine Privatheit auf Distanz".[85]

Die Nutzung neuer Telekommunikationsmittel und die Entwicklung der Telekommunikationstechnologie stellen für den Schutz der Privatheit individueller Fernkommunikation neue Herausforderungen dar. Zwar ermöglicht die Telekommunikationstechnologie, individuelle Kommunikation ohne Beschränkung mehr von Zeit und Distanz bequem durchzuführen, aber die Telekommunikation ist deswegen auch anfälliger für den staatlichen Zugriff geworden. Denn eine staatliche heimliche Kenntnisnahme kann wegen der besonderen Funktionsweise der Telekommunikation mit Hilfe der Telekommunikations- sowie Informationstechnologie viel leichter erreicht werden.[86] Staatliche Stellen können durch Telekommunikationsdiensteanbieter, die die Kontrolle über technische Einrichtungen ausüben, die übermittelten Informationen der Beteiligten erheben und speichern können. Dafür ist der Beteiligte kaum in der Lage, die Privatheit des Telekommunikationsvorgangs zu kontrollieren. Deswegen schützt das Fernmeldegeheimnis die Vertraulichkeit der Telekommunikation, damit die Beteiligten so gestellt werden, „wie sie bei einer Kommunikation unter Anwesenden stünden".[87] In der Informationsgesellschaft, in der die Telekommunikation immer mehr Bedeutung gewinnt, kommt dem Fernmeldegeheimnis in Art. 10 Abs. 1 GG eine zentrale Bedeutung zu.[88]

Das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG gewährleistet die Vertraulichkeit von der unkörperlichen Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs.[89] Zu entsprechenden Medien gehören sowohl das traditionelle Telefon, Telegramm, der Funk, als auch die neuen Medien wie der Mobilfunk und das Internet.[90] Ge-

---

84 BVerfGE 85, 386 (396); 115, 166; *Hermes*, in: *Dreier* (Hrsg.), GG 2013, Art. 10 Rn. 15.

85 BVerfGE 115, 166.

86 *Hermes*, in: *Dreier* (Hrsg.), GG 2013, Art. 10 Rn. 20; *Pagenkopf*, in: *Sachs* (Hrsg.), GG 2014, Art. 10 Rn. 6; siehe auch *Breyer*, S. 73 f.

87 BVerfGE 115, 166 (66).

88 Siehe auch *Pagenkopf*, in: *Sachs* (Hrsg.), GG 2014, Art. 10 Rn. 14.

89 BVerfGE 115, 166 (182), 125, 260 (189) vgl. BVerfGE 106, 28 (35 f.); 120, 274 (306 f.); siehe auch *Durner*, in: *Maunz*/*Dürig* (Begr.), GG 2017, Art. 10 Rn. 81; *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 10 Rn 5; *Baldus*, in: *Epping*/*Hillgruber* (Hrsg.), GG 2017, Art. 10 Rn. 37.

90 BVerfGE 120, 274 (307); *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 10 Rn. 5; *Dur-*

schützt wird in erster Linie der Inhalt der Telekommunikation. Darunter fällt der Inhalt des Telekommunikationsverkehrs durch Telefon, Telegramm, Mobilfunk, E-Mail, elektronische Post (E-Post), Internettelefonie (VoIP) und so weiter.[91] Geschützt werden auch die näheren Umstände des Telekommunikationsvorgangs vor Kenntnisnahme durch staatliche Stellen. Zu den nähren Umständen gehört insbesondere die Frage, „ob, wann, und wie oft zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist."[92] Somit sind aus der Nutzung der Telekommunikationsdienste erzeugte Verbindungsdaten, Standortsdaten, Internetzugangsdaten in den Schutzbereich des Fernmeldegeheimnisses zu erfassen.

Sogenannte Kunden- und Bestandsdaten in § 3 Nr. 3 TKG wie Rufnummer, Anschlusskennungen, Name und Anschriften vom Teilnehmer unterfallen dem Recht auf informationelle Selbstbestimmung statt dem Fernmeldegeheimnis.[93] Denn bei Bestandsdaten handelt es sich nicht um die Bereitstellung und Erbringung von Telekommunikationsdiensten. Sie beziehen sich vielmehr nur auf den Abschluss des Vertrags der Telekommunikationsdienste.[94] Somit sind Bestandsdaten vom Schutzbereich des Art. 10 GG auszuschließen. Die Schutzwirkung des Art. 10 GG erstreckt sich auch auf die mit der Telekommunikation verbundene Verwendung und Weitergabe erlangter Kenntnisse.[95]

Mit Hilfe der neuen Technologien werden zahlreiche Nutzungsmöglichkeiten der Telekommunikations- und Informationsdienste angeboten. Dabei ist die Relevanz des Fernmeldegeheimnisses sowie die Abgrenzung zu anderen Grundrechten nicht immer leicht zu bestimmen.[96]

Besonders problematisch ist vor allem, ob das Internetsurfen für das Fernmeldegeheimnis relevant ist. Der Inhalt von den meisten Internetseiten stellt für jedermann öffentlich zugängliche Informationen dar. Beim Internetsurfen

---

ner, in: *Maunz*/*Dürig* (Begr.), GG 2017, Art. 10 Rn. 82; *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 10 Rn. 42-43.

91 Siehe auch *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 10 Rn. 5.

92 BVerfGE 125, 260 (309); *Durner*, in: *Maunz*/*Dürig* (Begr.), GG 2017, Art. 10 Rn. 60; *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 10 Rn. 9.

93 *Durner*, in: Maunz/Dürig (Begr.), GG 2017, Art. 10 Rn. 88.

94 OVG Münster, MMR 2009, 424 (424); siehe auch Durner, in: Maunz/Dürig (Begr.), GG 2017, Art. 10 Rn. 88.

95 BVerfGE 100, 313 (359); *Hermes*, in: *Dreier* (Hrsg.), GG 2013, Art. 10 Rn. 16; *Durner*, in: *Maunz*/*Dürig* (Begr.), GG 2017, Art. 10 Rn. 61.

96 Siehe auch *Pagenkopf*, in: *Sachs* (Hrsg.), GG 2014, Art. 10 Rn. 14.

kann es somit nicht um eine Telekommunikation *„zwischen individuellen Kommunikationspartnern“*[97], sondern nur um eine *„rein passive Informationsgewinnung“*[98] gehen, weshalb es vom Schutzbereich des Art. 10 GG auszuschließen ist. Nach dieser Ansicht wird die Funktionsweise des Telekommunikationsverkehrs nicht berücksichtigt. Zwar ist der Inhalt der Internetseite generell öffentlich und für jeden zugänglich, aber die Gewinnung des Inhalts der Internetseite findet immer noch zwischen zwei Telekommunikationsanschüssen statt[99] und ist nur durch telekommunikationstechnische Übermittlung möglich. Internetsurfen ist deswegen mit dem Lesen eines Plakats nicht vergleichbar, sondern ähnelt vielmehr einer Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs.[100]

Der Schutzzweck des Fernmeldegeheimnisses ist gerichtet auf die Vertraulichkeit individueller Telekommunikationsvorgänge. So führt das BVerfG aus:

„Für das Merkmal Telekommunikation kommt es im Rahmen des Art. 10 Abs. 1 GG weder auf die technische Umsetzung der Kommunikation noch auf deren Inhalt und Empfängerkreis an. Auch ist irrelevant, wer Betreiber der Übertragungs- und Vermittlungseinrichtungen ist.“[101] *„Die Nutzung eines Kommunikationsmediums soll in allem vertraulich möglich sein. ...Der Schutz der Vertraulichkeit knüpft dabei aber nicht an die Beteiligten der Kommunikation, sondern an den Übermittlungsvorgang und das dabei genutzte Medium an.“*[102] *„Ein empfängergesteuerter Abruf von Informationen aus dem Netz erfüllt zudem die Kriterien der köperlosen Übermittlung von Informationen an einen individuellen Rezipienten. Bei der Nutzung des Internets durch eine natürliche Person kommunizieren auch nicht ausschließlich technische Geräte miteinander. [...] Das Surfen im Internet ist unter das Fernmeldegeheimnis zu subsumieren.“*[103]

Mit diesen Ausführungen hat das BVerfG klargestellt, dass die Vertraulichkeit der Telekommunikationsvorgänge den zentralen Schutzzweck des Fernmeldegeheimnisses darstellt. Der Schutzbereich des Fernmeldegeheimnisses ist eröffnet, sobald es sich nicht um einen rein technischen Datenaustausch zwi-

---

97 *Hiéramente*, StraFo 2013, 96 (98 f.).
98 *Schmitt*, in: *Meyer-Goßner*/*Schmitt*, StPO 2016, § 100a Rn. 7d.
99 *Breyer*, S. 79f.
100 Vgl. BVerfG, Beschluss vom 6.7.2016 – 2 BvR 1454/113 – Rn. 38.
101 BVerfG, Beschluss vom 6.7.2016 – 2 BvR 1454/113 – Rn. 34.
102 BVerfG, Beschluss vom 6.7.2016 – 2 BvR 1454/113 – Rn. 36.
103 BVerfG, Beschluss vom 6.7.2016 – 2 BvR 1454/113 – Rn. 38, dagegen *Eidam*, NJW 2016, 3508 (3512).

schen zwei Geräten handelt.[104] Das Schutzbedürfnis des Fernmeldegeheimnisses liegt hauptsächlich in der Anfälligkeit des individuellen Informationsaustauschs für den Zugriff Dritter mittels telekommunikationstechnischer Übermittlung.[105] *„Das Fernmeldegeheimnis knüpft an das Kommunikationsmedium an.“*[106] Ob der Informationsaustausch zwischen natürlichen Personen stattfindet, ist dabei unerheblich. Denn Kernpunkt des Fernmeldegeheimnisses ist, dass man in der Informationsgesellschaft durch Nutzung des Telekommunikationsmediums Informationen vertraulich austauschen können soll. Der Schutzbereich des Fernmeldegeheimnisses soll nicht zu eng aufgefasst werden. Das BVerfG hat den Schutzbereich des Fernmeldegeheimnisses zurecht für neue Entwicklungen der Telekommunikations- sowie Informationstechnologie offengehalten.[107]

Weiterhin ist fraglich, ob eine dynamische IP-Adresse dem Telekommunikationsvorgang und damit dem Schutzbereich zuzuordnen ist. Eine IP-Adresse ist eine dem Nutzer zugeteilte Adresse des Internets, die aus einer Zahlenfolge einem Host zugeordnet wird und ihn identifiziert.[108] Bei der Vergabe der IP-Adressen sind statische und dynamische IP-Adressen zu unterscheiden, wobei erstere normalerweise fest auf dem Gerät eingetragen werden und für einen längeren Zeitraum mit einem bestimmten Rechner verknüpft sind, während letztere erst bei Bedarf für die Dauer der konkreten Nutzung zufällig und vorübergehend zugewiesen wird.[109] So sind grundrechtliche Zuordnungen der statischen und dynamischen IP-Adressen getrennt zu behandeln.

Vor allem ist der Personenbezug der statischen und dynamischen IP-Adresse zu bejahen. Bei statischen IP-Adressen ist ohnehin klar, dass sie personenbezogene Daten sind, weil sie fest mit einem bestimmten Rechner verknüpft sind und damit einer Person zugeordnet werden können, wenn auch die Zuordnung nicht immer direkt, sondern mit anderen Daten zusammen verwirklicht werden muss.[110] Bei dynamischen IP-Adressen ist die Zuordnung zu einer Person zwar schwieriger aber ebenfalls durchaus möglich.[111] Umstrit-

---

104 Siehe auch *Bär*, ZD 2017, 136 (132).

105 BVerfGE 67, 157 (171 f.), 106, 28 (36).

106 BVerfG, Beschluss vom 22.8.2006 – 2 BvR 1345/03, Rn. 54.

107 Siehe BVerfG, Beschluss vom 6.7.2016 – 2 BvR 1454/113 – Rn. 34; Beschluss vom 22.8.2006 – 2 BvR 1345/03, Rn. 51.

108 *Sieber*, in: *Hoeren*/*Sieber*/*Holznagel* (Hrsg.), 2014, Teil 1 Rn. 53.

109 *Sieber*, in: *Hoeren*/*Sieber*/*Holznagel* (Hrsg.), 2014, Teil 1 Rn. 55; siehe auch *Eckhardt*, in: *Geppert*/*Schütz* (Hrsg.), TKG 2013, § 113 Rn. 28; *Zimmer*, S. 32 f.

110 *Roßnagel*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, S. 1299 Rn. 56.

111 *Roßnagel*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, S. 1299 Rn. 56; Zum Personenbezug der dynamischen IP-Adresse siehe auch *Gundermann*, K&R 2000, 225 (225 ff.); *Meyerdierks*, MMR 2009, 8 (8 ff.); *Karg*, MMR-Aktuell 2011, 315811,

ten ist, ob eine IP-Adresse zum Telekommunikationsvorgang gehört. Wenn man eine IP-Adresse nur als „Adresse im Internet" versteht, erscheint sie ähnlich wie eine Anschrift der Nutzer und kann als Bestandsdatum angesehen werden.[112] Aber diese Auffassung ist nur zutreffend bei einer statischen IP-Adresse, da diese allein trotz der Zuordnung zu einem bestimmten Anschlussinhaber auf die abstrakte Zuordnung von Nummer und Anschlussinhaber beschränkt ist. Damit stellt sie die bloße Zuordnung einer Telekommunikationsnummer zu einem Anschlussinhaber dar und bezieht sich nicht auf die Vertraulichkeit des konkreten Kommunikationsvorgangs.[113]

Dynamische IP-Adressen dürfen jedoch nicht mit der Anschrift oder der Telefonnummer der Nutzer gleichgesetzt werden.[114] Beim Besuchen der Internetseite werden dynamische IP-Adressen generiert. Wegen der Verknüpfung mit der konkreten Nutzung kann eine Erhebung der dynamischen IP-Adresse Kenntnis vom Inhalt der Internetseite ermöglichen.[115] Bei einer dynamischen IP-Adresse, die aus anderen Nutzungen der Telekommunikationsdienste hergestellt wird, kann eine Speicherung zumindest eine grobe geographische Nachverfolgung und so eine Erstellung von Aufenthaltsprofilen ermöglichen.[116] Damit bezieht sich die dynamische IP-Adresse unmittelbarer als eine Anschrift oder eine Telefonnummer auf den Telekommunikationsvorgang.

Zwar hat das BVerfG im Urteil zur Vorratsdatenspeicherung den Unterschied der dynamischen IP-Adresse zu den Bestandsdaten betont und ihre Aussagekraft sowie das damit verbundene Gewicht für den Betroffenen hervorgehoben, aber es hat die grundrechtliche Zuordnung der dynamischen IP-Adresse immer noch nicht klargestellt. Mit diesem Punkt hat es sich endlich im Urteil zur Zuordnung dynamischer IP-Adressen im Jahr 2012 ausführlich auseinandergesetzt.[117] Das Telekommunikationsgeheimnis aus Art. 10 GG schützt allein die Vertraulichkeit konkreter Telekommunikationsvorgänge, es schützt nicht *„die Vertraulichkeit der jeweiligen Umstände der Bereitstellung von Telekommunikationsdienstleistungen wie etwa die Zuordnung der von den*

MMR 2011, 341 (345 ff.); *Specht/Müller-Riemenschneider*, ZD 2014, 71 (71 ff.); *Breyer*, ZD 2014, 400 (400 ff.).

112 So fand zum Beispiel das BGH im Urteil vom 12.5.2010, siehe NJW 2010, 2061; MMR 2010, 565.

113 BVerfGE 130, 151 (180 f.).

114 BVerfGE 120, 265 (342).

115 BVerfGE 120, 265 (342).

116 *Roßnagel/Moser-Knierim/Schweda*, S. 171.

117 BVerfGE 130, 151 (179 ff.), siehe auch MMR 2012, 410; NJW 2012, 1419; ZD 2012, 220.

Diensteanbietern vergebenen Telekommunikationsnummern zu bestimmten Anschlussinhabern".[118] Bei Bestandsdaten sowie statischen IP-Adressen ist dies der Fall. Dynamische IP-Adressen weisen demgegenüber *„eine besondere Nähe zu konkreten Telekommunikationsvorgängen"* auf und *„fallen in den Schutzbereich des Art. 10 Abs.1 GG"*.[119] Deswegen betrifft die Zuordnung von statischen IP-Adressen zu ihren Anschlussinhabern das Recht auf informationelle Selbstbestimmung, während die Zuordnung dynamischer IP-Adressen das Fernmeldegeheimnis berührt.

2. Eingriff in den Schutzbereich

Als Eingriff in das Fernmeldegeheimnis wird jede Aufzeichnung, Verarbeitung, Verwertung sowie Änderung oder Übermittlung von Kommunikationsdaten durch die öffentliche Gewalt verstanden.[120] Eine Speicherung der Inhalte oder Umstände der Telekommunikationsvorgänge stellt somit einen eigenständigen Eingriff dar.[121] Hiernach wird bzw. wurde in das Fernmeldegeheimnis vor allem von der in § 113b TKG und § 113a Abs. 1 TKG a.F.[122] vorgesehenen Speicherungspflicht der Dienstanbieter eingegriffen. Die gemäß § 113a Abs. 2 bis 5 i.V.m. Abs. 6 und 7 TKG a.F. zu speichernden Telekommunikationsdaten umfassten alle Verbindungsdaten mit traditionellem Telefon, Online-Telefon und der E-Mail sowie Zugangsdaten. Aus solchen Daten können Informationen über das Ob, Wann und Wo der Kommunikation hergestellt werden. Entsprechendes gilt auch für die nunmehr geltenden Speicherungspflichten des § 113b TKG.

In das Fernmeldegeheimnis wird weiterhin durch die Übermittlung und Verwendung gespeicherter Vorratsdaten eingegriffen.[123] Obwohl die Übermittlung und Verwendung nur nach weiteren gesetzlichen Voraussetzungen geschehen dürfen, beinhaltet diese Abrufnorm aber schon die Verwendungszwecke und Erlaubnis zur Übermittlung und Verwendung gespeicherter Da-

---

118 BVerfGE 130, 151 (179 f.).

119 BVerfGE 130, 151 (181).

120 BVerfGE 100, 313 (366 f.); 125, 260 (310); *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 10 Rn 11; *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 10 Rn.61; *Hermes*, in: *Dreier* (Hrsg.), GG 2013, Art. 10 Rn. 16.

121 *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 10 Rn. 61, vgl. *Hermes*, in: *Dreier* (Hrsg.), GG 2013, Art. 10 Rn. 16; BVerfGE 100, 313 (366); so auch *Breyer*, S. 89.

122 Mit a.F. ist hier und im Folgenden die Fassung der betreffenden TKG-Normen gemeint, die dem BVerfG in seinem Vorratsdatenspeicherungsurteil vorlag, siehe hierzu speziell Kapitel 2, C.II.4.a).

123 Vgl. hierzu § 113b S. 1 Hs. 1 TKG a.F.; aktuell § 113c TKG.

ten, damit ist sie für eine Verwendungsregelung und insoweit als Eingriff in das Fernmeldegeheimnis qualifiziert.[124]

Gegen den Charakter des staatlichen Eingriffs der Vorratsspeicherung spricht, dass die Telekommunikationsdaten nicht durch den Staat, sondern durch die privaten Diensteanbieter gespeichert werden, die in aller Regel nicht der öffentlichen Gewalt zuzurechnen sind.[125] Allerdings ist die Verpflichtung zur Speicherung für die Diensteanbieter nicht freiwillig, weder bei Speicherung noch bei Abrufung der Telekommunikationsdaten haben die Dienstanbieter eigenständigen Handlungsspielraum. Infolgedessen werden sie nur als Hilfspersonen der öffentlichen Stellen für die Aufgabenerfüllung angesehen.[126] Die Speicherungspflichten aus § 113b TKG und § 113a TKG a.F. bedeuten damit einen unmittelbaren Eingriff des Staates in das Fernmeldegeheimnis. Schließlich greift § 100g StPO in das Fernmeldegeheimnis ein, denn den Strafverfolgungsbehörden wird die Befugnis erteilt, die nach § 113b TKG[127] gespeicherten Vorratsdaten der Dienstanbieter abzurufen und zu verwenden.

3. Anforderungen an die verfassungsrechtliche Rechtfertigung

Das Fernmeldegeheimnis ist nicht schrankenlos gewährleistet. Ein Eingriff in das Fernmeldegeheimnis ist zulässig, wenn er aufgrund eines Gesetzes erfolgt[128] und den Rechtfertigungsanforderungen wie dem Bestimmtheitsgebot, der Wesensgehaltsgarantie, dem Verhältnismäßigkeitsprinzip und der Gewährleistung wirksamen Rechtsschutzes genügt.[129]

a) Das Bestimmtheitsgebot

Die das Fernmeldegeheimnis einschränkenden Normen müssen die Anforderungen des Bestimmtheitsgebots einhalten. Das Bestimmtheitsgebot fordert, dass der Zweck und die Voraussetzungen des Eingriffs hinreichend klar und bestimmt formuliert werden müssen. Unter anderem muss der Wortlaut der Normen für den Bürger klar und verständlich sein, sodass der Bürger die

---

124 Siehe auch BVerfGE 125, 260 (312 f.).

125 Abweichende Meinung vom Richter *Schluckebier* zum Urteil der Vorratsdatenspeicherung, BVerfGE, 125 260 (365 f.).

126 Vgl. BVerfGE 125, 260 (311); *Gola*/*Klug*/*Reiff* NJW 2007, 2599 (2599); *Albers*/*Reinhardt*, ZJS 2010, 767 (770); *Moser-Knierim*, S. 269.

127 In der alten Fassung verwies § 100g StPO auf § 113a TKG.

128 Der Eingriff müsse nicht durch ein förmliches Gesetz erfolgen, sondern auf Grund eines Gesetzes angeordnet werden dürfen, siehe *Pagenkopf*, in: *Sachs* (Hrsg.), GG 2014, Art. 10 Rn. 31.

129 Vgl. *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 10 Rn. 16-25; *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 10 Rn. 70; *Hermes*, in: *Dreier* (Hrsg.), GG 2013, Art. 10 Rn. 65-74.

Rechtsfolgen seiner Handlungen voraussehen kann.[130] Ebenfalls müssen die Gerichte eine wirksame Rechtskontrolle durchführen können.[131] Das Bestimmtheitsgebot ist besonders dann zu beachten, wenn sich die Eingriffsintensität wegen der Art und Schwere des Eingriffs als schwerwiegend darstellt.[132] Demgemäß müssen der Umfang der Vorratsdatenspeicherung, der Zweck und die konkreten Voraussetzungen der Speicherung sowie die Weitergabe der Vorratsdaten bereichsspezifisch und präzise festgelegt werden.[133]

In § 113c TKG werden die Verwendungszwecke der Vorratsdaten als Verfolgung von Straftaten, Abwehr von erheblichen Gefahren für die öffentliche Sicherheit und Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes festgelegt. Vormals wurde dies in § 113b TKG geregelt. Die dort, in § 113b TKG a.F., abstrakt genannten Zwecke genügten einem bereichsspezifischen und präzisen Zweck nicht. Es fehlte eine nähere Begrenzung der Straftaten sowie der erheblichen Gefahr.[134] Als ebenso wenig bestimmt wird der Begriff der Straftat mit „auch im Einzelfall erheblicher Bedeutung“ in § 100g Abs. 1 Nr. 1 StPO angesehen.[135] Zwar wird auf die Aufzählung der Straftatbestände in § 100a StPO verwiesen. Diese ist jedoch nicht abschließend („insbesondere“). Mangels Einhaltung des Bestimmtheitsgebots kann die Beurteilung der Verhältnismäßigkeit der Vorratsdatenspeicherung schwerlich durchgeführt werden, weil ein genauer Vergleich zwischen konkretem Nutzen und Schaden der fraglichen Eingriffe von einer bestimmten und klaren Fassung der Normen abhängt.[136]

Problematisch ist auch, dass sich der Zweck der Vorratsspeicherung aus der Regelung selbst nicht erkennbar ergibt. Die Bereitstellung der Vorratsdaten für eine spätere eventuelle Verwendung kann mangels des Zusammenhangs zwischen den Vorratsdaten und den künftigen Strafverfolgungen nicht einem

---

130 BVerfGE 65, 1 (44); 100, 313 (359 f.); 103, 21 (33); *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 10 Rn. 17;

131 BVerfGE 110, 33 (54 f.); 120, 378 (407); *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 10 Rn. 72; *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 20 Rn. 83; *Baldus*, in: *Epping*/*Hillgruber* (Hrsg.), GG 2017, Art. 10 Rn. 36.

132 BVerfGE 41, 251 (264); 110, 33 (55); 130, 372 (388 ff.); *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 10 Rn. 73; dazu siehe auch *Puschke*/*Singelnstein*, NJW 2008, 113 (118); *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 105.

133 BVerfGE 110, 33 (53); 125, 260 (315).

134 Vgl. *Gola*/*Klug*/*Reif*, NJW 2007, 2599 (2599); *Gitter*/*Schnabel*, MMR 2007, 411 (414); *Gausling*, S. 169.

135 Siehe auch *Gola*/*Klug*/*Reif*, NJW 2007, 2599 (2599); *Gausling*, S. 188.

136 BVerfGE 65, 1 (44); 120, 274 (321); Vgl. *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 105; *Breyer*, S. 126.

hinreichend bestimmten Zweck zugeordnet werden.[137] Der Zweck der Vorratsspeicherung darf nicht durch den Zweck der Vorratsverwendung als ein pauschaler Zweck ersetzt werden. Die Speicherung selbst stellt schon einen eigenständigen Eingriff dar und benötigt eine eigenständige gesetzliche Grundlage, die ebenfalls hinreichend bestimmt festgestellt werden muss.[138]

Insofern müssen Regelungen zur Vorratsdatenspeicherung hinsichtlich des Zwecks und der Voraussetzung strengen Anforderungen des Bestimmtheitsgebots gerecht werden, insbesondere wenn der schwere Eingriffscharakter berücksichtigt wird.

b) Wesensgehaltsgarantie

Nach Art. 19 Abs. 2 GG ist es verboten, mit grundrechtseinschränkenden Gesetzen den Wesensgehalt eines Grundrechts anzutasten. Dem Bundesverfassungsgericht zufolge ist der Wesensgehalt eines Grundrechtes für jedes Grundrecht aus seiner besonderen Bedeutung im Gesamtsystem der Grundrechte zu ermitteln.[139]

Das Fernmeldegeheimnis schützt die Vertraulichkeit individueller Telekommunikation. Die Vertraulichkeit würde beeinträchtigt und das Fernmeldegeheimnis somit faktisch leer laufen, wenn die Inhalte der Telekommunikation aller Bürger gespeichert würden und den staatlichen Behörden zugänglich wären.[140] Angesichts der Aussparung der Inhaltsdaten bleibe der Eingriff der Vorratsdatenspeicherung trotz seiner umfassenden Streubreite und langen Speicherungsdauer noch wirksam begrenzt.[141]

Zwar müssen Inhalte der Telekommunikation nicht gespeichert werden, aber wegen der allumfassenden Datenkategorie und der Sensibilität der Verkehrsdaten können mittels heutiger Informationstechnologie zahlreiche genaue persönliche Informationen einschließlich Inhalte der Telekommunikation aus den Vorratsdaten gezogen werden.[142] Allerdings schafft die Vorratsdaten-

---

137 Vgl. BVerfGE 113, 348 (377); *Gola*/*Klug*/*Reif*, NJW 2007, 2599; *Puschke*/*Singelnstein*, NJW 2008, 113 (118); *Gausling*, S. 169 f.; *Bizer*, DuD 2007, 586 (587); *Gitter*/*Schnabel*, MMR 2007, 411 (414); *Graulich*, NVwZ 2008, 485 (490).

138 Vgl. *Hermes*, in: *Dreier* (Hrsg.), GG 2013, Art. 10 Rn. 67; *Durner*, in: *Maunz*/*Dürig* (Begr.), GG 2017, Art. 10 Rn. 138.

139 BVerfGE 22, 180 (219); BVerfGE 109, 133 (156).

140 Vgl. *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 99.

141 BVerfGE 125, 260 (322), dagegen *Dix*/*Petri*, DuD 2009, 531 (533).

142 Vgl. BVerfGE 125, 260 (319, 328), siehe auch *Hermes*, in: *Dreier* (Hrsg.), GG 2013, Rn. 21; *Szuba*, S. 177; *Breyer*, S. 212 f.

speicherung immerhin keine *„globale und pauschale Überwachung“*[143] der Telekommunikation aller Bürger, die vom Bundesverfassungsgericht ausdrücklich verboten ist.

Somit wird der Wesensgehalt des Fernmeldegeheimnisses nicht von der Vorratsdatenspeicherung antastet, wenngleich er von der Maßnahme schon sehr bedroht wird.[144]

c) Wahrung des Verhältnismäßigkeitsprinzips

Das Verhältnismäßigkeitsprinzip ist auf das Rechtsstaatsprinzip zurückzuführen.[145] Jede staatliche Maßnahme ist materiell verfassungsmäßig, wenn sie dem Verhältnismäßigkeitsprinzip entspricht, also einem legitimen Zweck dient und zur Erreichung dieses Zwecks geeignet, erforderlich und angemessen ist.[146] Angesichts des sehr schweren Eingriffsgewichts ist die Vorratsdatenspeicherung an besonders strengen Verhältnismäßigkeitsanforderungen zu messen.[147]

aa) Legitimer Zweck

Eine staatliche Maßnahme, die Grundrechte der Bürger beschränkt, muss einen legitimen öffentlichen Zweck verfolgen, der das Gemeinwohl gewährleistet oder verbessern wird.[148] Die Vorratsdatenspeicherung dient dem Zweck der Effektivierung der Strafverfolgung, Gefahrenabwehr und der Aufgabenerfüllung zuständiger Behörden darstellen. Der Gesetzgeber zielt damit auf eine Erhöhung der Sicherheit der Bürger ab. Dies stellt problemlos ein Allgemeininteresse dar. Die erhöhte Sicherheit ist ein legitimer Zweck und dieser Zweck kann einen Eingriff in das Fernmeldegeheimnis grundsätzlich rechtfertigen.[149]

---

143 BVerfGE 67, 157 (174); 100, 313 (376).

144 Siehe auch *Breyer*, S. 152.

145 *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 20, Rn.112.

146 BVerfGE 65, 1 (54); 100, 313 (375 f.); 115, 320 (345); 120, 274 (318 f.); 125, 260 (Nr. 204); *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 20, Rn. 116.

147 Siehe auch *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 10 Rn. 77; Art. 2 Rn. 106.

148 BVerfGE 100, 313 (373); *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Ar. 10 Rn. 78.

149 Vgl. BVerfGE 100, 313 (373, 383 f.); 107, 299 (316); 109, 279 (336); 115, 320 (345); 125, 260 (316).

Allerdings wird die Verhältnismäßigkeit der Vorratsdatenspeicherung wegen der Verdachtsunabhängigkeit und der Anlasslosigkeit bezweifelt. Eine derartig umfangreiche verdachtsunabhängige Vorratsdatenspeicherung, die sich auf alle Bürger ausrichtet, gab es bisher noch nicht. Der Zweifel ist zutreffend vor dem Hintergrund einer Tendenz, dass Sicherheitsmaßnahmen im Namen der Strafverfolgung und Gefahrenabwehr ohne Bedenken vorgelagert werden. Es ist fragwürdig, ob die Effektivität der Strafverfolgung allein immer noch problemlos einen legitimen Zweck darstellt, der die Vorratsdatenspeicherung rechtfertigen kann.[150] Die effektivere Strafverfolgung selbst kann kein allgemeiner und pauschaler Zweck sein, ansonsten müssten alle personenbezogenen Daten den staatlichen Stellen schrankenlos zugänglich sein.[151]

Nach der Ansicht des BVerfG verbietet Art. 10 Abs. 1 GG *„nicht jede vorsorgliche Erhebung und Speicherung von Daten überhaupt, sondern schützt vor einer unverhältnismäßigen Gestaltung solcher Datensammlungen und hierbei insbesondere vor entgrenzenden Zwecksetzungen“*.[152] Strikt verboten sei lediglich die Speicherung von personenbezogenen Daten auf Vorrat zu unbestimmten und noch nicht bestimmbaren Zwecken.[153] Zwar wird das Fehlen der näheren Anknüpfungs- und Verbindungspunkte zwischen den als Vorrat gespeicherten Daten und den späteren Straftaten zu Recht kritisiert, gleichwohl richtet sich der genannte Zweck doch auf die bessere öffentliche Sicherheit und die Vorratsdaten werden nur bei konkreten anlassbezogenen Fällen verwendet.

Deswegen hat sich der vom Gesetzgeber formulierte Zweck für einen legitimen Zweck qualifiziert. Das Fehlen näherer Anknüpfungspunkte ist erst bei der Beurteilung der Angemessenheit zu bewerten.

bb) Geeignetheit

Die Vorratsdatenspeicherung muss geeignet sein, den angestrebten Zweck zumindest zu fördern. Nicht erforderlich ist, dass der legitime Zweck in jedem Einzelfall tatsächlich erreicht wird. Es reicht aus, wenn die abstrakte Möglichkeit der Zweckerreichung besteht, die zugelassene Maßnahme also nicht von vornherein untauglich ist, sondern dem gewünschten Erfolg förderlich sein könnte.[154]

---

150 Vgl. *Simitis*, RDV 2007, 143 (145); *Kunnert*, DuD 2014, 103 (107).
151 Siehe auch *Simitis*, RDV 2007, 143 (145).
152 BVerfGE 125, 260, (317).
153 BVerfGE 125, 260, (317).
154 BVerfGE 63, 88 (115); 67, 157 (175); 100, 313 (373); 125, 260 (317 f.); *Jarass*, in:

In der sogenannten Informationsgesellschaft hinterlässt man mit jeder Nutzung des Telekommunikationsnetzes und auch des Internets *„Spuren"*.[155] So können Verkehrsdaten bei der Vorbereitung und Durchführung von Straftaten hinterlassen werden und sie gelten als nützliche Ressource für die Identifizierung der Straftäter und zur Rekonstruierung der Telekommunikationsverbindung, damit sind Erhebung und Verwendung der Verkehrsdaten für Strafverfolgung und Gefahrenabwehr von erheblicher Bedeutung.[156]

Die Vorratsdatenspeicherung garantiert die Verfügbarkeit der Telekommunikationsdaten während eines Mindestzeitraums und sichert damit die Aufklärungsmöglichkeit mittels späterer Abrufung und Auswertung von den zuständigen Behörden.[157] Es ist zwar zu bezweifeln, ob die Vorratsdatenspeicherung tatsächlich zu einer Steigerung der Aufklärungsquote führt. Bei der Prüfung der abstrakten Geeignetheit reicht aber nur eine theoretisch höhere Aufklärungsquote durch die Einführung der Vorratsdatenspeicherung aus. Damit wird die Geeignetheit der Vorratsdatenspeicherung bejaht.[158]

cc) Erforderlichkeit

Eine Maßnahme ist erforderlich, wenn keine gleich geeigneten, milderen Mittel zur Verfügung stehen, die mit einem nicht unvertretbaren Aufwand durchgeführt werden könnten.[159] Der Eingriff der Vorratsdatenspeicherung in das Fernmeldegeheimnis muss sich demgemäß auf das zur Zweckerreichung Unerlässliche beschränken. Ein milderes Mittel ist denkbar, wenn die Vorratsdatenspeicherung im Einzelfall vorgenommen wird und auf einer konkreten Gefahr basiert.

So wurde das Quick-Freeze-Verfahren als eine bürgerfreundlichere Alternative zu der generellen verdachtsunabhängigen Vorratsspeicherung aller Bürger im Januar 2011 vorgeschlagen.[160] Nach dem Quick-Freeze-Verfahren

---

Jarass/*Pieroth*, GG 2016, Art. 20, Rn. 118; *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 10 Rn. 79.

155 *Simitis*, NJW 1997, 1902 (1903).

156 BVerfGE 125, 260 (317); *Albrecht*/*Kilchling*, S. 71; *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 18; *Breyer*, S.12 f.; *Münch*, ZRP 2015, 130 (131 f.).

157 Vgl. BVerfGE 125, 260 (317).

158 So auch BVerfGE 125, 260 (317); *Breyer*, S. 135.

159 BVerfGE 65, 1 (44); 79, 179 (198); 100, 226 (241); *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 20, Rn.119; *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 10 Rn. 80.

160 BMJ, Eckpunktepapier zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet, Stand Jan. 2011, 3. Meldung dazu ist

haben die Anbieter der Telekommunikationsdienste nach Anordnung der Behörden zur Strafverfolgung und Gefahrenabwehr, basiert auf begründeten Verdacht auf bestimmte schwere Straftaten, bestimmte Verbindungsdaten mit Personenbezug für einen bestimmten Zeitraum zu sichern („einfrieren"). Die gesicherten Daten dürfen erst dann mit Zustimmung eines Richters verwendet werden („aufgetaut").[161] Mittels des Quick-Freeze-Verfahrens soll bei den Strafverfolgungsbehörden eine hohe Erfolgswahrscheinlichkeit ohne die Notwendigkeit einer Vorratsdatenspeicherung verwirklicht werden.[162]

Im Vergleich zur Vorratsdatenspeicherung wird vor allem die förderliche Wirkung des Quick-Freeze-Verfahrens für Strafverfolgung und Gefahrenabwehr bezweifelt. Statt der Telekommunikationsdaten aller Teilnehmer werden nur die Telekommunikationsdaten nach bestimmten Kriterien gesichert. Die Tragweite der Maßnahme wird dadurch verringert und die Voraussetzungen für die Verwendung werden auch dementsprechend enger gesetzt. Ohne alle Telekommunikationsdaten auf Vorrat zu sichern, können die Strafverfolgungsbehörden nur die noch vorhandenen Daten abrufen, was die eigentliche Zweckerreichung der Vorratsdatenspeicherung abschwächen könnte.[163] Allerdings ist das Quick-Freeze-Verfahren trotz der geringeren gespeicherten Datenmengen wegen der geringeren Eingriffsschwere als eine mildere Alternative überlegenswert; insbesondere wenn man berücksichtigt, dass die Verkehrsdaten ohnehin auch zu Abrechnungszwecken von den Dienstanbietern für bis zu sechs Monate gespeichert werden.[164] Nach der Statistik werden Verkehrsdaten vor allem in den ersten drei Monaten abgefragt. Die Verkehrsdaten, die sechs Monate oder gar zwei Jahre alt sind, werden hingegen eher selten abgefragt.[165] Das bedeutet, dass der sogenannte Nachteil des Quick-Freeze-Verfahrens nur dann zählt, wenn die abgefragten Verkehrsdaten

---

abrufbar unter http://www.sueddeutsche.de/politik/eckpunktepapier-zur-datenspeicherung-anlassbezogene-speicherungspflicht-1.1047402 [31.1.2019].

161 Eckpunkte zur Verbesserung der Kriminalitätsbekämpfung im Internet von der FDP-Bundestagsfraktion, Stand: 9. November 2010, S. 7, nähere Auseinandersetzung der Funktionsweise des Quick-Freeze-Verfahren sowie Vergleich zwischen diesem und der Vorratsdatenspeicherung siehe in *Albrecht*/*Kilchling*, S. 38-42.

162 Eckpunkte zur Verbesserung der Kriminalitätsbekämpfung im Internet von der FDP-Bundestagsfraktion, Stand: 9. November 2010, S. 7; *Gitter*/*Schnabel*, MMR 2007, 411 (414); *Bizer*, DuD 2007, 586 (588).

163 Siehe auch BVerfGE, 125, 260 (318); *Albrecht*/*Kilchling*, S. 41; *Mahnken*, S. 18; *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 180; *Kühling*, NVwZ 2014, 681 (683).

164 *Moser-Knierim*, S. 273; *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 181.

165 *Moser-Knierim*, S. 273; *Bug*, ZParl 2016, 670 (685 f.). Eine Statistik dagegen, die darauf hinweist, dass die Speicherdauer von sechs Monaten erforderlich sei, siehe in *Münch*, ZRP 2015, 130 (130).

für Abrechnungszwecke nicht mehr vorgehalten werden, was jedoch nach der Statistik selten passiert.

Eine verdachtsabhängige Speicherung stellt ohne Zweifel ein milderes Mittel im Vergleich zu der anlasslosen Vorratsspeicherung dar. Wird jedoch auf die Anlasslosigkeit verzichtet, weicht die Maßnahme auch von ihrem eigentlichen Charakter ab. Der grundlegende Unterschied zwischen der Vorratsdatenspeicherung und dem Quick-Freeze-Verfahren liegt nun gerade darin, dass die Telekommunikationsdaten der Bürger im Einzelfall wegen des begründeten Verdachts gespeichert werden. Wegen des umfassenderen Speicherungsumfangs würden mehr verfügbare Daten bei der Vorratsdatenspeicherung gespeichert und theoretisch eine bessere Effektivität für Strafverfolgung und Gefahrenabwehr ermöglicht. Zwar stellt das Quick-Freeze-Verfahren wegen der Verdachtsabhängigkeit und der kürzeren Speicherungsdauer einen geringeren Eingriff in das Fernmeldegeheimnis dar, aber dessen Wirksamkeit bei der Strafverfolgung und Gefahrenabwehr bleibt immerhin nicht unhinterfragt im Vergleich mit der Vorratsdatenspeicherung.

Andere grundrechtsschonende und gleich effektive Ausgestaltungen der Vorratsdatenspeicherung sind zurzeit nicht ersichtlich. Deswegen wird die Vorratsdatenspeicherung für die Zweckerreichung als erforderlich angesehen.

dd) Angemessenheit

Ferner muss die Vorratsdatenspeicherung nach dem Verhältnismäßigkeitsprinzip angemessen sein. Nach der ständigen Rechtsprechung des BVerfG verlangt das Verhältnismäßigkeitsprinzip im engeren Sinn, dass die Schwere des eingesetzten Schutzmittels nicht außer Verhältnis zu den der Grundrechtsbeschränkung dienenden Gemeinwohlzwecken stehen dürfe.[166] Bei der diesbezüglichen Abwägung ist vor allem eine abstrakte Betrachtung derart erforderlich, das beeinträchtigte Interesse und die der Grundrechtsbeschränkung dienenden Interessen zu vergleichen.[167]

Die vorliegenden kollidierenden Interessen sind das Fernmeldegeheimnis einerseits und die öffentliche Sicherheit andererseits. Das BVerfG hat festgestellt:

---

166 BVerfGE 90, 145 (173); 92, 277 (327); 100, 313 (375 f.); 109, 279 (349 ff.); 115, 320 (345 f.); *Horn*, in: *Stern*/*Becker* (Hrsg.), GG, Art.2 Rn. 104.

167 Vgl. BVerfGE 109, 279 (350); 115, 320 (346), siehe auch *Breyer*, S. 138 f.

„Das Fernmeldegeheimnis gewährleistet die freie Entfaltung der Persönlichkeit durch einen privaten, vor den Augen der Öffentlichkeit verborgenen Austausch von Nachrichten, Gedanken und Meinungen (Informationen) und wahrt damit die Würde des denkenden und freiheitlich handelnden Menschen.“[168]

Das Fernmeldegeheimnis wird also als Konkretisierung der freien Entfaltung der Persönlichkeit vom Grundgesetz ein sehr hoher Rang zugewiesen. Diese Bedeutung ist umso erheblicher in der Informationsgesellschaft, als sich Telekommunikation wegen ihrer Unverzichtbarkeit im privaten und sozialen Leben heute schon als eine grundlegende Voraussetzung für die Wahrnehmung anderer Grundrechte erweist.[169] In diesem Zusammenhang sei das Recht auf das Telekommunikationsgeheimnis als ein zentrales Menschenrecht der Informationsgesellschaft anzuerkennen.[170]

Im Rahmen der abstrakten Abwägung kommt der öffentlichen Sicherheit jedoch keine geringere Bedeutung zu.[171] Wie das BVerfG im Urteil zur Online-Durchsuchung festgestellt hat, sind *„die Sicherheit des Staates als verfasster Friedens und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit Verfassungswerte, die mit anderen hochwertigen Gütern im gleichen Rang stehen.“*[172] Die Sicherheit stellt somit auch ein sehr hochrangiges Schutzgut dar und deren Gewährleistung wird als zentrale Aufgabe des Staates festgestellt.[173] Aus einer abstrakten Abwägung der kollidierenden Interessen kann sich deswegen nicht ergeben, dass einem Interesse davon grundsätzlich ein Vorrang eingeräumt wird. Bei der Überprüfung der Angemessenheit kommt es vielmehr auf eine Abwägung zwischen der konkreten Auswirkung des Eingriffs auf das Fernmeldegeheimnis der Bürger und der Bedeutung des Eingriffs für die öffentliche Sicherheit an.[174]

---

168 BVerfGE 67, 157 (171).

169 *Hoffmann-Riem*, JZ 2008, 1009, siehe auch *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 98; *Moser-Knierim*, S. 101 f.

170 *Dix*, in: Bundeskriminalamt (Hg.), S. 159; siehe auch *Moser-Knierim*, S. 101; *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 98.

171 Aus zahlreichen Untersuchungen über Begriff sowie Ausgleich der Freiheit und Sicherheit insbesondere in der Informationsgesellschaft siehe *Thiel*, S. 140 ff.; *Kipker*, S. 5 ff.; *Moser-Knierim*, S. 7 ff.; *Hoffmann-Riem*, ZRP 2002, 497 (497 ff.); *Di Fabio*, NJW 2008, 421 (422); *Krings*, ZRP 2015, 167 (168); *Trimbach*/*Dietrich*, NJ 2015, 461 (462 f.).

172 BVerfGE 120, 274 (319); 49, 24 (56 f.); 115, 320 (346).

173 Siehe *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 96; *Thiel*, S. 149.

174 *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 20, Rn. 121; *Sachs*. in: *Sachs* (Hrsg.), GG 2014, Art. 20 Rn.154; *Grzeszick*, in: *Maunz*/*Dürig* (Begr.), GG 2017, Art. 20 Rn. 117, vgl. *Breyer*, S. 140.

(1) Auswirkung der Vorratsdatenspeicherung auf das Fernmeldegeheimnis

Bei einer konkreten Ermittlung der Auswirkung der Vorratsdatenspeicherung auf das Fernmeldegeheimnis ist vor allem ihre besonders schwere Eingriffsintensität darzustellen.[175] In Betracht kommen der Umfang der Betroffenheit, die Intensität der Beeinträchtigungen und die Voraussetzungen der Datenverwendung, insbesondere ob die Betroffenen hierfür einen Anlass gegeben hätten.[176] Unter anderem ist erheblich, *„ob die Betroffenen als Personen anonym bleiben, welche persönlichkeitsbezogenen Informationen erfasst werden und welche Nachteile den Grundrechtsträgern aufgrund der Maßnahmen drohen oder von ihnen nicht ohne Grund befürchtet werden“*.[177] Im Ungültigkeitsurteil zur Umsetzungsregelung der Vorratsdatenspeicherung hat das BVerfG diese Kriterien wieder betont. Es hat dargelegt, dass die Eingriffsqualität der Vorratsdatenspeicherung durch die Streubreite der Vorratsspeicherung, anhand der Aussagekraft der gespeicherten Daten und der Frage, ob die Speicherung anlasslos durchgeführt wird, zu beurteilen ist.[178]

(a)Umfassende Streubreite

Die Schwere des Eingriffs durch die Vorratsdatenspeicherung lässt sich durch ihre umfassende Streubreite, *„wie sie die Rechtsordnung bisher nicht kennt“*[179] bestimmen. Zu speichern sind nämlich alle Telekommunikationsverkehrsdaten, welche zur Rückverfolgung und Identifizierung der Quelle und des Adressaten einer Nachricht sowie zur Bestimmung von Datum, Uhrzeit, Dauer und Art einer Nachrichtenübermittlung, der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern und des Standorts mobiler Geräte benötigt werden. Umfasst würden prinzipiell alle Telekommunikationsmittel wie zum Beispiel Telefon, Mobiltelefon, elektronisches Postfach sowie Internet, deren Nutzung im heutigen Leben nicht mehr wegzudenken sei und die Bürger auch nicht auf reguläre Weise ausweichen können.[180] Bei der Vorratsdatenspeicherung werden nämlich sämtliche bei der Bereitstellung

---

175 *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 20, Rn. 121.

176 BVerfGE 115, 320 (347); 100, 313 (376); 107, 299 (318 ff.); 109, 279 (353); *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 10 Rn. 81; *Baldus*, in: *Epping*/*Hillgruber* (Hrsg.), GG 2017, Art. 10 Rn. 46

177 BVerfGE 115, 320 (347); 100, 313 (376); 109, 279 (353).

178 BVerfGE 125, 260 (318 ff.), so auch *Hornung*/*Schnabel*, DVBI 2010, 824 (825).

179 BVerfGE 125, 260 (318), dagegen siehe *Bull*, in: *van Ooyen*/*Möllers* (Hrsg.), S. 640.

180 BVerfGE 125, 260 (318 ff.).

von Kommunikationsdiensten erzeugte Daten aller Bürger erfasst im Zeitraum von mindestens sechs Monaten.

Angesichts der weiten Verbreitung der Telekommunikationsmittel und der Unverzichtbarkeit der Nutzung von Telekommunikationsdiensten ist festzustellen, dass nahezu alle Bürger von der Vorratsdatenspeicherung betroffen sind. Somit ist die Streubreite der Maßnahme außerordentlich umfassend.

(b)Aussagekräftige Verkehrsdaten

Der Eingriff der Vorratsdatenspeicherung ist umso schwerwiegender, je höher die der Aussagekraft und der damit verbundenen Sensibilität der Verkehrsdaten ist. Aus den zu speichernden Verkehrsdaten können genaue Informationen der Umstände des Telekommunikationsverkehrs sowie der Internetverbindungen aller Bürger entnommen werden. Angesichts der großen Verbreitung der Telekommunikationsmittel und der engen Verbindung zwischen der Telekommunikationstechnologie und dem Alltagsleben beziehen sich die gespeicherten Verkehrsdaten unter Umständen auf vielfältige Alltagshandlungen, Bewegungen und private sowie soziale Beziehungen der Bürger.[181] Durch eine dauerhafte Speicherung der Telekommunikationsdaten können Persönlichkeits- sowie Bewegungsprofile der Bürger leicht erstellt werden.[182]

Die Eingriffsintensität hinsichtlich der Aussagekraft der *Verkehrs*daten wird als geringer erachtet als die Speicherung der Telekommunikationsinhalte.[183] Diese Ansicht ist nur insoweit zutreffend, als die Speicherung sich auf traditionelle Telekommunikationsmittel und noch begrenzte Informationstechnologien bezieht.[184] Schon im Volkszählungsurteil wurde betont, dass bei der Festlegung der Eingriffsintensität staatlicher Maßnahmen zur Erhebung personenbezogener Daten die Nutzbarkeit und Verwendungsmöglichkeit der Angaben entscheidend sind und dies hänge von den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten ab.[185] Somit darf die Schutzwürdigkeit der Verkehrsdaten nicht wegen begrifflicher sowie technischer Unterschiede zwischen Verkehrsdaten und Inhaltsdaten als geringer angesehen werden.[186]

---

181 BVerfGE 125, 260 (318); *Puschke*, DANA 2006, 65 (66 f.); *Hensel*, DuD 2009, 527 (528 f.); *Pfitzmann*/*Köpsell*, DuD 2009, 542 (543 f.).

182 BVerfGE 125, 260 (319);

183 Hierzu eingehend die abweichende Meinung zum Urteil der Vorratsdatenspeicherung von Richter *Schluckebier* BVerfGE 125, 260 (310 f.).

184 Vgl. *Puschke*, DANA 2006, 65 (71).

185 BVerfGE 65, 1 (45).

186 *Breyer*, StV 2007, 214 (218), vgl. *Simon*, S. 227.

Unter heutigen informationstechnischen Bedingungen hinsichtlich der Datenanalyse sowie der Datenauswertung können nicht nur Daten der Umstände des Telekommunikationsverkehrs für einen inhaltlichen Rückschluss ausreichen.[187] Verkehrsdaten sind nicht weniger aussagekräftig als Inhaltsdaten. Wegen der von vornherein digitalen Eigenschaft der Verkehrsdaten und des noch nicht abzusehenden Potenzials neuer Informationstechnologien sind die Verarbeitungsmöglichkeiten sowie die Verwendbarkeit der Verkehrsdaten im Vergleich mit den Inhaltsdaten womöglich sogar größer.[188] Im Vergleich zu traditionellen Verkehrsdaten aus Telefonie, die nur grobe Persönlichkeits- sowie Bewegungsprofile erstellen können, können weitaus detailliertere persönliche Informationen wie zum Beispiel *„gesellschaftliche oder politische Zugehörigkeiten, persönliche Vorlieben, Neigungen und Schwächen“*,[189] *„Gewohnheiten, soziale Verflechtungen, Netzwerkstrukturen und Verhaltensauffälligkeiten“*[190] durch die Analyse der Verkehrsdaten – erzeugt von Empfang und Versand der Nachrichten in verschiedener Form und vom Internetzugang – gewonnen werden.[191]

Hinzu kommt, dass Verkehrsdaten selbst in vielen Fällen von hoher Sensibilität sein können, unabhängig davon, ob der Telekommunikationsinhalt zur Kenntnis genommen wird oder nicht.[192] Beispielweise sind die von den Kontakten mit spezialisierten Beratern über Gesundheit oder Geisteszustand erzeugten Verkehrsdaten selbst schon hochsensibel. Die Speicherung der Verkehrsdaten in diesem Fall kann *„die Gefahr der sozialen Abstempelung für den Betroffenen hervorrufen“*[193] und diese Gefahr stellt eine ebenso große wie die Speicherung der Telekommunikationsinhalte dar. Wegen der wachsenden Abhängigkeit der Bürger von den Telekommunikationsnetzen werden immer mehr besonders sensible Verkehrsdaten anfallen. Die unterschiedslose Vorratsspeicherung der Verkehrsdaten bedroht somit gravierend die Privatsphäre der Bürger. Deswegen wird der Eingriff der Vorratsdatenspeicherung angesichts der Aussagekraft der Verkehrsdaten als besonders schwerwiegend qualifiziert.

---

187 Vgl. BVerfGE 125, 260 (319); *Dix*/*Petri*, DuD 2009, 531 (531); *Breyer*, StV 2007, 214 (218).
188 *Breyer*, S. 212 f.; *Moser-Knierim*, S. 182-183; *Szuba*, S. 177 f.
189 BVerfGE 125, 260 (319).
190 *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 132.
191 *Breyer*, S. 215.
192 Siehe auch *Breyer*, S. 218; *Hensel*, DuD 2009, 527 (530).
193 BVerfGE 65, 1 (48).

(c) Die Verdachtsunabhängigkeit und die Anlasslosigkeit

Zu den Zugriffen auf Verkehrsdaten im Rahmen der Strafverfolgung, die für Abrechnungszwecke bereits vorhandenen sind, hat das BVerfG schon gefordert:

„Derartige Eingriffe sind nur gerechtfertigt, wenn sie zur Verfolgung einer Straftat von erheblicher Bedeutung erforderlich sind, hinsichtlich der ein konkreter Tatverdacht besteht und wenn eine hinreichend sichere Tatsachenbasis für die Annahme vorliegt, dass der durch die Anordnung Betroffene mit dem Beschuldigten über Telekommunikationsanlagen in Verbindung steht.“[194]

Statt Telekommunikationsdaten bestimmter Personen verdachtsabhängig punktuell bei konkreten Gefahrensituationen zu erfassen, werden gemäß der Vorratsdatenspeicherung Telekommunikationsdaten verdachtsunabhängig für spätere mögliche Verwendungen protokolliert. Das heißt, dass bei der Vorratsdatenspeicherung weder eine konkrete Gefahr noch ein Tatverdacht gegen bestimmte Personen auftreten muss. Es handelt sich somit um eine anlasslose und verdachtsunabhängige Erfassung der Telekommunikationsdaten.[195]

Zwar hat sich das BVerfG in früheren Entscheidungen nicht unmittelbar zu der Frage verhalten, ob eine vorsorgliche verdachtsunabhängige und anlasslose Speicherung aller Telekommunikationsverkehrsdaten verfassungsmäßig ist. Aber es hat sich schon mit vergleichbaren Maßnahmen, vor allem in den Urteilen zur Telekommunikationsüberwachung,[196] Großer Lauschangriff,[197] Rasterfahndung[198] und automatisierte Kennzeichenerfassung[199] auseinandergesetzt und verfassungsrechtliche Anforderungen für diese Maßnahme aufgestellt.

Im Hinblick auf das Verhältnismäßigkeitsprinzip sind intensive Grundrechtseingriffe erst von bestimmten Verdachts- oder Gefahrenstufen an zulässig.[200] Bei der Verfassungsmäßigkeit vorsorglicher Maßnahmen zur Gefahrenabwehr im Vorfeld komme des Weiteren nicht nur die Erfolgseignung dieser

---

194 BVerfGE 107, 299 (322).

195 Nach der Ansicht von *Moser-Knierim* ist zwischen den Begriffen von „verdachtsunabhängig“ und „anlasslos“ zu differenzieren und angesichts der frühen Entscheidung vom Bundesverfassungsgericht ist „anlasslos“ noch stärker als den Begriff „verdachtsunabhängig“, siehe in *Moser-Knierim*, S. 233.

196 BVerfGE 100, 313 (392).

197 BVerfGE 109, 279 (353).

198 BVerfGE 115, 320 (354).

199 BVerfGE 120, 378 (401 f., 428 f.).

200 BVerfGE 115, 320 (361).

Maßnahme in Betracht, sondern auch, ob begrenzende Anforderungen an die Wahrscheinlichkeit des Gefahreneintritts und an die Nähe der betroffenen Personen zur fraglichen Rechtsgutbedrohung vorgesehen werden.[201] Demgemäß muss die Durchführung einer vorsorglichen Maßnahme nicht nur auf einem konkreten Anlass basieren, sondern ihre Verfassungsmäßigkeit hängt auch von den strengen Begrenzungen des konkreten Anlasses ab. Als Beispiel verlange die Durchführung präventiver Rasterfahndungen nicht nur eine konkrete Gefahr, sondern die Feststellung der Wahrscheinlichkeitsprognose dieser Gefahr müsse sich auch noch auf Tatsachen beziehen.[202] Der gleiche Bemessungsstandard galt und wurde insbesondere in der Entscheidung zur automatisierten Kennzeichenerfassung betont. Die Maßnahme dürfe nicht durchgeführt werden, ohne dass konkrete Gefahrenlagen oder allgemein gesteigerte Risiken von Rechtsgutgefährdungen oder -verletzungen einen Anlass geben würden.[203]

Daraus kann sich ergeben, dass verdachtsunabhängige informationsbezogene Sicherheitsmaßnahmen nicht schon wegen des Fehlens einer näheren Beziehung zwischen dem gefährdeten Rechtsgut und dem Betroffenen unverhältnismäßig ist, aber sie darf auf keinen Fall ohne Anlass durchgeführt werden.[204] Bei Durchführung der Vorratsdatenspeicherung werden alle Bürger verdachtsunabhängig in den Wirkungsbereich einbezogen. Der Eingriff knüpft auch nicht an das Vorliegen einer konkreten Gefahr für die bedrohten Rechtsgüter an. Eine schwerwiegende Eingriffsintensität der Vorratsdatenspeicherung wegen ihrer Verdachtsunabhängigkeit und Anlasslosigkeit ist somit ohne Zweifel festzustellen.[205]

(2) Die Bedeutung der Vorratsdatenspeicherung für die öffentliche Sicherheit

Im Hinblick auf das Verhältnismäßigkeitsprinzip im engeren Sinn darf die oben erwähnte schwerwiegende Grundrechtsbeeinträchtigung den Nutzen der Vorratsdatenspeicherung nicht überwiegen. Dafür ist einerseits die positive Bedeutung der Vorratsdatenspeicherung zu untersuchen, und zwar wie sehr die Effektivierung der Strafverfolgung und Gefahrenabwehr in der Praxis mit Hilfe der Vorratsdatenspeicherung wirklich verbessert und die öffentliche Sicherheit damit gefördert wird.

---

201 BVerfGE 115, 320 (361 f.).
202 BVerfGE 115, 320 (364).
203 BVerfGE 120, 378 (378).
204 So auch *Moser-Knierim*, S. 233.
205 Vgl. *Puschke*, DANA 2006, 65 (68).

Andererseits kann in Anlehnung an ein Gutachten des Max-Planck-Instituts 2011[206] die Frage gestellt werden, ob ohne die Vorratsdatenspeicherung ersichtlich Schutzlücken auftreten würden. Diese Sicht ist besonders beachtenswert. Denn sie ist nicht nur wesentlich für die Abwägung der Angemessenheit der Vorratsdatenspeicherung. Dadurch lässt sich auch deduzieren, dass die Ursachen des Terrorismus und der schweren Kriminalität nicht im Mangel an strengen Sicherheitsmaßnahmen liegen.[207] Die Prävention und Bekämpfung des Terrorismus und die schwere Kriminalität kann auch nicht hauptsächlich von den strengen Sicherheitsmaßnahmen abhängen.[208]

Werden die Grundrechtsbeeinträchtigungen der Vorratsdatenspeicherung berücksichtigt, ist diese unangemessen, wenn keine oder nur eine geringfügige Förderung für die Effektivierung der Strafverfolgung und Gefahrenabwehr geschaffen wird. Hauptsächlich begründen die Befürworter der Vorratsdatenspeicherung, dass die Strafverfolgung wegen der knapp vorhandenen Telekommunikationsdaten erheblich erschwert worden sei.[209] So werden große Schutzlücken der Sicherheit durch Wegfall der Vorratsspeicherungspflicht behauptet.[210] Allerdings hat eine Untersuchung, basierend auf einer Studie des Bundeskriminalamts im Jahr 2005, also vor dem Umsetzungsgesetz, dargestellt, dass die wegen fehlender Kommunikationsdaten nicht aufgeklärten Straftaten nur einen Anteil von 0,01% aller nicht aufgeklärten Straftaten ausmache, was bedeute, dass sich die Aufklärungsquote nach Durchführung der Vorratsdatenspeicherung von 55 auf 55,006% steigern könne.[211] Daraus kann sich die Notwendigkeit der Vorratsdatenspeicherung nicht ergeben.

Hinzu kommt, dass die Vorratsdatenspeicherung so umfassend wie möglich Telekommunikationsdaten und deshalb eine große Verfügbarkeit für spätere Abrufe und Verwendungen von zuständigen Behörden sichern soll, wodurch eine verstärkte Strafverfolgung und effektivere Gefahrenprävention erwartet wird. Den vorhandenen Statistiken gemäß ist dies in der Praxis aber nicht der

---

206 *Albrecht/Kilchling*.

207 Siehe auch *Hoffmann-Riem*, ZRP 2002, 497 (500 ff.).

208 Vgl. *Breyer*, S. 179 f.

209 *Beukelmann*, NJW 2012, 2617 (2619 ff.).

210 Ständige Konferenz der Innenminister und -senatoren der Länder Sammlung der zur Veröffentlichung freigegebenen Beschlüsse der 191. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder. Berlin, den 23.11.2010, S. 12, abrufbar unter: http://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/10-11-19/Beschluesse.pdf?__blob=publicationFile&v=2 [31.1.2019].

211 *Breyer*, in: *Bettina* (Hrsg.), S. 17; *Gietl*, K&R 2007, 545 (550).

Fall. Die Gesamtaufklärungsquote in Deutschland hat sich bei Durchführung der Maßnahme von 54,8% im Jahr 2008 auf 56,0% im Jahr 2010 gesteigert.[212] Die Aufklärungsquote der Computerkriminalität ist im Gegenteil von 37,5% im Jahr 2009 auf 35,8% im Jahr 2010 gesunken.[213] Dies zeichnet nicht das Bild einer eindrucksvollen Verbesserung. Ferner erfolgten die registrierten Zugriffe auf gespeicherte Vorratsdaten nach der Durchführung der Vorratsdatenspeicherung gemäß des Gutachtens des Max-Planck-Instituts 2011 auch nur in einer sehr kleinen Zahl von Verfahren.[214] Wird etwa die Statistik in Niedersachsen als Beispiel genommen, wurden im Jahr 2008 3% und 2009 3.3% der Verfahren mit Abfrage der Verkehrsdatenabfragen insgesamt durchgeführt, einschließlich der Vorratsdatenabfrage.[215]

Entgegen der Behauptung im Evaluationsbericht der Europäischen Kommission über die Durchführung der Vorratsdatenspeicherung sowie deren Auswirkungen,[216] dass aus der Statistik und Beispielen der Mitgliedsstaaten eine wertvolle Rolle der Vorratsdatenspeicherung zur Verhütung und Bekämpfung von Kriminalität bejaht werden könne, hat das Gutachten die Statistik und die Beispiele, die sich auf die Evaluation gestützt haben, als nicht aussagekräftig und als ungeeignete Grundlage für eine Evaluation kritisiert.[217] Denn vor allem hätten nur ein Drittel der Mitgliedstaaten die nachgefragten Statistiken vollständig übermittelt. Anschließend sei bei den vorgelegten Daten der Mitgliedstaaten auch nicht zwischen Vorratsdatenabfragen und regulären Verkehrsdatenabfragen differenziert geworden. Ferner seien die verschiedenen Art der Datenabfragen sowie die Deliktsschwere nicht aufgegliedert geworden und schließlich seien die als Beispiel übermittelten Einzelfälle von Mitgliedsstaaten wenig tauglich, die Behauptung der Europäischen Kommission nachzuweisen.[218] Mangels der vollständigen und systematischen Daten könnten keine zuverlässigen Folgerungen darüber gezogen werden, ob und inwieweit die Vorratsdatenspeicherung den Sicherheitsschutz verbessert hat.[219] Die Schlussfolgerung aus dem Evaluationsbericht ist deswegen nicht überzeugend.

---

212 Polizeiliche Kriminalstatistik Bundesrepublik Deutschland, Berichtsjahr 2010, Bundeskriminalamt (Hrsg.), S. 77.

213 Polizeiliche Kriminalstatistik Bundesrepublik Deutschland, Berichtsjahr 2010, Bundeskriminalamt (Hrsg.), S. 248.

214 *Albrecht*/*Kilchling*, S. 120.

215 *Albrecht*/*Kilchling*, S. 121.

216 Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG), von der Europäischen Kommission, Brüssel, den 18.4.2011, KOM (2011) 225 endgültig, S. 28.

217 *Albrecht*/*Kilchling*, S. 133.

218 *Albrecht*/*Kilchling*, S. 130 f.

219 *Albrecht*/*Kilchling*, S. 130.

Soweit fehlt es an durchschlagenden statistischen Belegen, die darauf hindeuten könnten, dass die Vorratsdatenspeicherung die Strafverfolgung und Gefahrenabwehr in erheblichem Maße verbessern oder eine für den Sicherheitsschutz unentbehrliche Maßnahme darstellen kann. Darüber, wie die große Menge der gespeicherten Vorratsdaten bei der Strafverfolgung technisch verarbeitet wird und wie der Täter dadurch ermittelt wird, gibt es noch keine umfängliche Darstellung.[220] Vielmehr zeigen bereits durchgeführte Untersuchungen und Statistiken, dass die Vorratsdatenspeicherung in nur geringem Maße einen Beitrag zur Strafverfolgung geleistet hat.[221] Die Sicherheitslage hängt auch nicht deutlich von der Durchführung der Vorratsdatenspeicherung ab und der Wegfall dieser Maßnahme würde auch nicht zu reduzierten Schutzmöglichkeiten führen.[222]

Infolgedessen lässt sich feststellen, dass die förderliche Bedeutung der Vorratsdatenspeicherung für Strafverfolgung und Gefahrenabwehr zwar in Einzelfällen bejaht wird, aber insgesamt nur beschränkt und die Erhöhung der Aufklärungsquote nicht entscheidend ist. Im Vergleich zu den besonders schwerwiegenden Grundrechtsbeeinträchtigungen ist diese beschränkte förderliche Wirkung auf den Zweck im Rahmen der Abwägung zu berücksichtigen.

(3) Abwägung

Es unterliegt keinem Zweifel, dass die Vorratsdatenspeicherung mit der großen Streubreite wegen ihrer Verdachtsunabhängigkeit und Anlasslosigkeit einen besonders intensiven Eingriff in das Fernmeldegeheimnis darstellt.[223] Eine solche Speicherung kann den Nutzern der Telekommunikationsdienste zahlreiche belastende Wirkungen entgegenbringen.

Vor allem enthält die flächendeckende Speicherung das große Risiko der Enthüllung sowie des Missbrauchs der gespeicherten Telekommunikationsdaten sowohl durch staatliche Stellen als auch Private.[224] Angesichts der

---

220 *Hoeren*, Kriminalistik 2015, 469 (469).

221 So auch *Albrecht*/*Kilchling*, S. 219; *Breyer*, S. 17; *Moser-Knierim*, S. 203; *Leutheusser-Schnarrenberger*, DuD 9/2014, 589 (591); *Puschke*, DANA 2006, 65 (69).

222 *Albrecht*/*Kilchling*, S. 219, 220; *Hoeren*, Kriminalistik 2015, 469 (471).

223 Vgl. *Hermes*, in: *Dreier* (Hrsg.), GG 2013, Art. 10 Rn. 69.

224 BVerfGE 125, 260 (320); vgl. *Breyer*, S. 221 ff., S. 228 ff.; *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 92; *Szuba*, S. 104; *Moser-Knierim*, S. 184-185; *Dix*/*Petri*, DuD 2009, 531 (534); *Gietl*, K&R 2007, 545 (545 f.); *Roßna-*

Sensibilität der Verkehrsdaten ist die belastende Wirkung für den Nutzer besonders groß, wenn es um die Bereiche Gesundheit, Sexualleben oder die Beratung in sozialen Notlagen geht.[225] Ferner ist der Bürger mit dem Risiko konfrontiert, *„weiteren Ermittlungen ausgesetzt zu werden, ohne selbst Anlass dazu gegeben zu haben"*[226], oder sogar falsch verdächtigt zu werden.[227] Darüber hinaus rufe die Vorratsdatenspeicherung ein diffuses bedrohliches Gefühl hervor, dauerhaft überwacht zu werden.[228] Die Vertraulichkeit der Telekommunikationsvorgänge wird beeinträchtigt, wenn der Nutzer oder die Nutzerin bei der Telekommunikationsverbindung weiß, dass alle seine bzw. ihre Verkehrsdaten protokolliert und eventuell verwendet werden.[229] Damit kann die Vorratsspeicherung durch den psychischen Druck das Verhalten des Einzelnen beeinflussen.[230]

„Wer etwa damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte verzichten."[231]

Ein anlassloser und verdachtsunabhängiger Eingriff mit großer Streubreite könne also nicht nur das Fernmeldegeheimnis, sondern auch durch Einschüchterungseffekte die Ausübung von anderen Grundrechten beeinträchtigen.[232] Ob von dem Ausmaß oder der Intensität des Eingriffs der Vorratsspeicherung das Risiko von Einschüchterungseffekten ausgeht, ist eine unbeantwortete Frage. Dies liegt aber wohl sehr nahe. Da fast jeder Bürger von der Vorratsdatenspeicherung betroffen ist, können die allgemeinen Einschüchterungseffekte letztlich das Gemeinwohl dadurch beeinträchtigen, dass die Selbstbestimmung gehemmt wird, *„die elementare Funktionsbedingung*

---

gel/*Bedner*/*Knopp*, DuD 2009, 536 (537); *Pfitzmann*/*Köpsell*, DuD 2009, 542 (546); *Breyer*, StV 2007, 214 (219); *Puschke*/*Singelnstein*, NJW 2008, 113 (118); *Hornung*/*Schnabel*, DVBI 2010, 824 (827); *Bizer*, DuD 2007, 586 (588 f.).

225 BVerfGE 65, 1 (48); 125, 260 (334); siehe auch *Burkert*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, S. 105; *Breyer*, S. 218; *Hensel*, DuD 2009, 527 (529).

226 BVerfGE 125, 260 (320).

227 *Breyer*, S. 219 f.; *Szuba*, S. 104; ein Beispiel bei der Vorratsspeicherung der IP-Adresse siehe *Alsbih*, DuD 2011, 482 (486); *Puschke*, DANA 2006, 65 (70).

228 BVerfGE 125, 260 (320), dagegen *Pagenkopf*, in: *Sachs* (Hrsg.), GG 2014, Art. 10, Rn. 8.

229 BVerfGE 125, 260 (320).

230 Vgl. BVerfGE 65, 1 (42).

231 BVerfGE 65, 1 (43).

232 BVerfGE 113, 29 (46); 115, 320 (354 f.); 120, 378 (402), dagegen siehe *Bull*, in: *van Ooyen*/*Möllers* (Hrsg.), S. 642.

eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlich demokratischen Gemeinwesen ist".[233]

Während die flächendeckende Vorratsspeicherung die Nutzer mit vielfältigen Risiken belastet, werden keine ausreichenden Vorkehrungen zum Schutze der Datensicherheit gegen diese Risiken nach den Kriterien getroffen, die zu den notwendigen Bedingungen für eine verhältnismäßige Vorratsdatenspeicherung vom BVerfG vorgegeben wurden.[234] Nach den Vorgaben zur Vorratsdatenspeicherung (§ 113a Abs. 10 TKG a.F.) haben die Diensteanbieter die Qualität und den Schutz der Vorratsdaten nach der im Bereich der Telekommunikation erforderlichen Sorgfalt zu beachten und durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich von ihnen ermächtigten Personen möglich ist. Diese Regelung reicht in dieser Pauschalität den Anforderungen an die Datensicherheit nicht aus. Statt einer nur allgemein erforderlichen Sorgfalt muss die fragliche Vorratsspeicherung im Rahmen der Verhältnismäßigkeit einem besonders hohen Sicherheitsstandard gerecht werden.[235] In den novellierten Regelungen zur Vorratsdatenspeicherung beinhaltet § 113d TKG einen umfangreichen Katalog mit Anforderungen an die Datensicherheit.

(4) Bewertung der Angemessenheitsabwägung der Vorratsdatenspeicherung vom Bundesverfassungsgericht

Trotz der als schwerwiegend festgestellten Grundrechtsbeeinträchtigungen der Vorratsdatenspeicherung hat das BVerfG geurteilt, dass sie nicht von vornherein unverhältnismäßig im engeren Sinne ist.[236] Die Begründung des BVerfG liegt darin, dass die Vorratsdatenspeicherung – grundsätzlich und auch in der Ausgestaltung wie sie dem BVerfG vorlag – keine von der ständigen Rechtsprechung strikt verbotene Sammlung von personenbezogenen Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken ist.[237]

Dies ist durchaus kritikwürdig: Zwar hängt der Zugriff und die Verwendung der Vorratsdaten nach Vorgaben der Vorratsdatenspeicherung immer von einem bestimmtem Anlass ab, aber in der Phase der Vorrats*speicherung* fehlt es am näheren Anknüpfungspunkt zwischen zu speichernden Daten und später

233 BVerfGE 115, 320 (355).
234 Vgl. 125, 260 (334).
235 BVerfGE 125, 260 (348 f.).
236 BVerfGE 125, 260 (318).
237 BVerfGE 125, 260 (320, 321).

eventuellen Verwendung. Damit kann die Ansicht nur schwer überzeugen, dass Telekommunikationsdaten für einen bestimmten Zweck zu speichern sind.[238]

Anschließend hat das BVerfG weiter begründet, dass statt jeglicher Kommunikation oder Aktivitäten der Bürger nur Telekommunikationsverkehrsdaten erfasst würden und damit keine Totalerfassung der persönlichen Daten geschehe, sodass sie das Fernmeldegeheimnis in noch hinnehmbarer Weise beschränke.[239] Jedoch ist es angesichts des allumfassenden Speicherungsumfangs, der starken Aussagenkraft von Verkehrsdaten und der langen Speicherungsdauer zweifelhaft, ob die Beeinträchtigung wirksam begrenzt werden kann. Im Hinblick auf vielfältige Nutzungs- und Verknüpfungsmöglichkeiten der gespeicherten Daten mit anderen Datensammlungen können Persönlichkeits- und Bewegungsprofile mit Leichtigkeit erstellt werden.[240] Damit droht durch die Vorratsdatenspeicherung den Bürgern ein großes Risiko der Totalerfassung – auch dann, wenn die zu speichernden Daten auf Verkehrsdaten beschränkt werden.

Ferner hat das BVerfG betont, dass die Telekommunikationsdaten nicht unmittelbar vom Staat gespeichert werden dürften, sondern erst in einem zweiten Schritt wegen bestimmter Anlässe nach rechtlich näher festgelegten Kriterien von den zuständigen Stellen verwendet werden dürften.[241] Diese Ansicht ist nur insoweit zutreffend, als Zugriff und Verwendung der Vorratsdaten von befugten Behörden wirksam dadurch begrenzt würden, dass sie sowohl materielle als auch verfahrensrechtliche Voraussetzungen erfüllen müssten. Daraufhin hat das BVerfG festgestellt, dass eine Vorratsdatenspeicherung durch eine gesetzliche Ausgestaltung, die dem Eingriffsgewicht angemessen Rechnung trägt, den Verhältnismäßigkeitsanforderungen im engeren Sinne genügen könne.[242] Es sei ferner zu berücksichtigen, dass die Vorratsdatenspeicherung wegen ihrer Bedeutung für die effektive Strafverfolgung und Gefahrenabwehr ein spezifisches hilfreiches Mittel in der modernen Gesellschaft für die Antwort auf die neue Bedrohungslage wäre.[243] Die Rekonstruierung des Telekommunikationsverkehrs könne ohne Telekommu-

238 Siehe auch *Bizer*, DuD 2007, 586 (587 f.); *Dix*/*Petri*, DuD 2009, 531 (532 f.).
239 BVerfGE 125, 260 (322).
240 BVerfGE 115, 166 (189 f.); 125, 260 (319); *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 107; *Gitter*/*Schnabel*, MMR 2007, 411 (414); *Puschke*/*Singelnstein*, NJW 2008, 113 (118); *Kutscha*, LKV 2008, 481 (485).
241 BVerfGE 125, 260 (321).
242 BVerfGE 125, 260 (321).
243 BVerfGE 125, 260 (322).

nikationsdaten nicht ermöglicht werden, und der Gesetzgeber dürfe zum Zweck der öffentlichen Sicherheit aufgrund eines Interessenausgleichs entscheiden, wie weit die Telekommunikationsdaten zu speichern seien.[244]

Ein Interessenausgleich muss jedoch im Rahmen der Maßgaben des Rechtsstaatsgebots durchgeführt werden. Eine anlasslose Verkehrsdatenspeicherung aller Bürger entspreche den rechtsstaatlichen Anforderungen nicht. Soweit die Telekommunikationsdaten anlasslos und für zukünftige Verwendungen, die bei der Speicherungsphase noch nicht als hinreichend bestimmten Zweck gelten, gespeichert werden, kann dieses Defizit nicht durch eine konkrete strenge Ausgestaltung kompensiert werden.[245]

Bezweifelt wird außerdem die behauptete Bedeutung der Vorratsdatenspeicherung, die effektive Strafverfolgung und Gefahrenabwehr zu fördern. Zwar besteht noch keine gründliche und maßgebende statistische Überprüfung der wirklichen Funktion der Vorratsdatenspeicherung – eine solche Untersuchung ist sehr kompliziert, dabei müssten zahlreiche Elemente berücksichtigt werden[246] – aber den vorhandenen Statistiken und Untersuchungen lässt sich entnehmen, dass eine ersichtliche Förderung und damit verbundene Unverzichtbarkeit dieser Maßnahme nicht in jedem Fall gegeben ist.

Die Befürchtung, dass ohne Vorratsdatenspeicherung die Ermittlungsarbeit nur schwierig durchgeführt werden könne, ist wohl nicht begründet. Um eine positive Wirkung auf Strafverfolgung zu ermöglichen, müssen alle Nutzer der Telekommunikationsdienste stark belastet werden. Eine solche Maßnahme kann dem Verhältnismäßigkeitsgrundsatz im engeren Sinn nicht entsprechen. Der Spielraum kommt dem Gesetzgeber aufgrund eines Interessenausgleichs zu, wie das BVerfG betont hat, dass

„die Verfassung den Gesetzgeber nicht grundsätzlich daran hindert, die traditionellen rechtsstaatlichen Bindungen im Bereich des Polizeirechts auf der Grundlage einer seiner Prärogative unterliegenden Feststellung neuartiger oder veränderter Gefährdungs- und Bedrohungssituationen fortzuentwickeln.“[247] *„Die Balance zwi-*

244 BVerfGE 125, 260 (323).

245 Vgl. *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 10 Rn. 73.

246 Die Untersuchung im Gutachten von *Albrecht/Kilchling* vom Max-Planck-Institut ist in diesem Punkt sehr ausführlich und überzeugend. Trotzdem wurde im Gutachten erklärt, dass es an geeigneten Daten und spezifischen empirischen Untersuchungen fehlt; so könne die tatsächliche Wirkung der Vorratsdatenspeicherung nur eingeschränkt beurteilt werden, siehe *Albrecht*/*Kilchling*, S. 218.

247 BVerfGE 115, 320 (360).

schen Freiheit und Sicherheit darf vom Gesetzgeber neu justiert, die Gewichte dürfen jedoch vom ihm nicht grundlegend verschoben werden.“[248]

Insofern hat das BVerfG die vorsorgliche Speicherung der Telekommunikationsdaten zwar nicht verboten, aber eine weitere vorsorgliche anlasslose Datensammlung sehr streng begrenzt.

Um eine Totalerfassung aller Aktivitäten der Bürger zu vermeiden, darf die Speicherung der Telekommunikationsdaten auf Vorrat nicht als Vorbild für die Schaffung der Vorratsdatenspeicherung in anderen Bereichen dienen, sondern muss eine Ausnahme bleiben.[249] Dafür sei der Gesetzgeber bei der neuen Gesetzgebung einer vorsorglichen Datensammlung verpflichtet, die Gesamtheit der verschiedenen schon existierenden Datensammlungen zu beachten.[250] Das BVerfG hat hervorgehoben,

„[d]ass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss.“[251]

Diese Anforderung der *„Überwachung-Gesamtrechnung“*[252] des BVerfG hat der Gesetzgeber bei der künftigen Gesetzgebung in Bezug auf Sicherheitsmaßnahme zu beachten.[253] Es gehört zur Aufgabe des Gesetzgebers, Freiheit und Sicherheit bei der Gesetzgebung ständig auszugleichen und diesen Ausgleich an die neuen technischen und gesellschaftlichen Bedingungen anzupassen.[254] Konkrete Kriterien für eine derartig hinreichende Betrachtung, ob und inwiefern eine Überwachungsmaßnahme allein oder mit anderen zusammen zu einer Totalerfassung führen könnte, hat das BVerfG nicht erklärt. Dies kann für den Gesetzgeber problematisch werden, weil der Handlungsspielraum in diesem Fall unüberschaubar ist.[255] Jedoch ist absehbar, dass diese Anforderungen in Zukunft weiter entwickelt und konkretisiert wer-

248 BVerfGE 115, 320 (360).
249 BVerfGE 125, 260 (323 f.)
250 BVerfGE 125, 260 (324).
251 BVerfGE 125, 260 (324).
252 *Roßnagel*, NJW 2010, 1238 (1242); *Moser-Knierim*, S. 236 ff.
253 Bei dieser Achtungspflicht hält *Roßnagel* die Durchführung einer doppelten Verhältnismäßigkeitsprüfung für notwendig, siehe *Roßnagel*, NJW 2010, 1238 (1242); *Moser-Knierim* hat diese Achtungspflicht als Beobachtungs- Prüfungs- und Abstimmungspflicht konkretisiert, siehe *Moser-Knierim*, S. 242 ff.
254 Zur Aufgabe des Gesetzgebers Freiheit und Sicherheit auszugleichen siehe *Thiel*, S. 182 ff.
255 Siehe auch *Petri*, in: *Roßnagel* (Hrsg.), S. 126 f.; *Hornung*/*Schnabel*, DVBI 2010, 824 (827).

den.[256] Von Bedeutung ist, dass dem Gesetzgeber eine Pflicht ausdrücklich auferlegt wird, eine Überwachungsgesellschaft dadurch zu vermeiden, dass er die Entwicklung der technischen und gesellschaftlichen Bedingungen beachten und bei der Gesetzgebung die mögliche hemmende Wirkung auf die Freiheitswahrnehmung der Bürger beachten und diese vermindern muss.

Eine Totalerfassung aller Aktivitäten der Bürger kann zwar nicht durch eine allgemeine Speicherung der persönlichen Daten aus einzelnen Lebensbereichen ermöglicht werden, aber dieses Risiko droht schon, wenn die vielen schon vorhandenen Datensammlungen miteinander in Verbindung gebracht werden.[257] Werden die zahlreichen bereits vorhandenen Datensammlungen und die wegen des großen Entwicklungspotenzials der Telekommunikationstechnik immer vielfältigeren Nutzungs- und Verknüpfungsmöglichkeiten berücksichtigt, ist diese „Achtungspflicht" der Gesetzgeber vom BVerfG angemessen und begrüßenswert.

256 Auch *Roßnagel*, NJW 2010, 1238 (1242).
257 Sehe auch *Gietl*, DuD 2010, 398 (403).

II. Die Vereinbarkeit der Vorratsdatenspeicherung mit den datenschutzrechtlichen Anforderungen aus dem Recht auf informationelle Selbstbestimmung

1. Das Rechts auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung wurde vom BVerfG im Volkszählungsurteil von 1983 aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) entwickelt.[258] In der Mikrozensus-Entscheidung vom 16.7.1969 hatte das BVerfG erläutert, dass ein „Innenraum" des Einzelnen für die freie und selbstverantwortliche Entfaltung seiner Persönlichkeit erforderlich ist. Dieser Persönlichkeitsbereich werde von einer staatlichen – wenn auch bewertungsneutralen – Einsichtnahme eingeschränkt.[259] Dieser Ansatz wird im Volkszählungsurteil aufgenommen und im Hinblick auf die Bedingungen moderner Informationsverarbeitungstechnologien fortgeführt.[260]

Die wegweisende Bedeutung dieses Urteils vom BVerfG für die Entwicklung des Datenschutzrechts kann kaum überschätzt werden. In diesem Urteil hat das BVerfG das Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts eingeführt und festgestellt, dass die freie Entfaltung der Persönlichkeit unter den modernen Bedingungen den Schutz des Rechts auf informationelle Selbstbestimmung voraussetze. Zudem ist die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, zu gewährleisten.[261] Mit Hilfe der automatischen Datenverarbeitung könnten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person unbegrenzt gespeichert und jederzeit mit Leichtigkeit abgerufen werden. Die grundsätzliche Herrschaft über die eigenen persönlichen Daten der Bürger werde hierdurch gefährdet. Sie ist besonders schutzbedürftig.[262]

Auf die wesentliche Bedeutung des Rechts auf informationelle Selbstbestimmung ist das BVerfG darüber hinaus insoweit eingegangen, als dass es

---

258 BVerfGE 65, 1 (41 ff.).

259 BVerfG 27, 1 (6f.).

260 Siehe *Horn*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 2 Rn. 116; *Trute*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, S. 171 Rn. 25; *Thiel*, S. 222f.

261 BVerfGE 65, 1 (43), siehe auch *Murswiek*, in: *Sachs* (Hrsg.), GG 2014, Art. 2 Rn. 72ff; Jarass, in: Jarass/Pieroth, GG 2016, Art. 2 Rn. 37; *Trute*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, S. 162, Rn. 7f.

262 BVerfGE 65, 1 (42); 115, 320 (342); 120, 274 (303f.); 120, 378 (397f.).

eine unentbehrliche Bedingung der freien individuellen Selbstbestimmung als Teil einer freien Gesellschaft ist.[263] So wurde auf seine fundamentale Bedeutung für das auf die Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger gegründete freiheitlich demokratische Gemeinwesen geschlossen.[264] Ein freiheitlich demokratisches Gemeinwesen setzt vor allem voraus, dass der Bürger frei und freiwillig bei gesellschaftlichen Angelegenheiten mitwirken kann. Unter den neuen modernen technischen Bedingungen können persönliche Einzelangaben unbegrenzt gespeichert und auf sie zugegriffen werden, ohne dass der Betroffene deren Verwendung zur Kenntnis nehmen oder darauf Einfluss nehmen kann.[265] Somit drohe dem Einzelnen die Gefahr, die tatsächliche Kontrolle über seine eigenen persönlichen Daten zu verlieren, womit die individuelle Verhaltensfreiheit und ein damit verbundenes freiheitliches demokratisches Gemeinwesen beeinträchtigt werde.[266]

Um die Herrschaft der Bürger über ihre eigenen persönlichen Daten unter heutigen und auch künftigen Bedingungen zu schützen, wurde im Volkszählungsurteil nicht nur eine Beschränkung für die staatliche Erhebung und Verwendung bezüglich der Volkszählung festgelegt, sondern auch verfassungsrechtliche Anforderungen für den staatlichen Umgang mit personenbezogenen Daten insgesamt umrissen.[267] Dem Recht auf informationelle Selbstbestimmung wird ein verfassungsmäßiger Rang beigemessen. Das Recht wurde als verfassungsrechtliche Grundlage des Datenschutzes ausgebaut.[268]

2. Schutzbereich und Beschränkung des Rechts auf informationelle Selbstbestimmung

Das BVerfG hat den Schutzbereich, den Eingriff sowie die verfassungsrechtliche Rechtfertigung des Rechts auf informationelle Selbstbestimmung fortlaufend konkretisiert und entwickelt.[269] Das Recht auf informationelle

---

263 BVerfGE 65, 1 (41); *Murswiek*, in: *Sachs* (Hrsg.), GG 2014, Art. 2 Rn. 73;

264 BVerfGE 65, 1 (43 ff.); *Murswiek*, in: *Sachs* (Hrsg.), GG 2014, Art. 2 Rn. 73.

265 BVerfGE 65, 1 (42), siehe auch *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 102.

266 Dafür hat das BVerfG erklärt: „Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder eine Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte verzichten.“, BVerfGE 65, 1 (43), dazu siehe auch *Murswiek*, in: *Sachs* (Hrsg.), GG 2014, Art. 2 Rn. 73.

267 BVerfGE 65, 1 (41 ff.); siehe *Abel*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, S.209.

268 *Abel*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, S. 209.

269 Ausführlich dazu siehe *Thiel*, S. 229 ff.

Selbstbestimmung schützt die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[270]

„Der Schutzumfang beschränkt sich nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb grundrechtlich geschützt werden. Auch der Umgang mit personenbezogenen Daten, die für sich genommen nur geringen Informationsgehalt haben, kann, je nach seinem Ziel und den bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten, grundrechtserhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit des Betroffenen haben.“[271]

Denn es gibt unter den Bedingungen der automatischen Datenverarbeitung keine *„belanglosen“* Daten mehr.[272] Geschützt werden alle personenbezogenen Daten, also alle *„Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person.“*[273] Unerheblich ist, ob die personenbezogenen Daten die Privat- oder die Intimsphäre betreffen oder nicht.[274] Der Schutz des Rechts auf informationelle Selbstbestimmung beschränkt sich auch nicht nur auf die automatisierte Datenverarbeitung, sondern generell auf die staatliche Erhebung und Verarbeitung personenbezogener Daten.[275]

Das Recht auf informationelle Selbstbestimmung ist jedoch nicht schrankenlos gewährleistet.[276] Die freie Entfaltung der Persönlichkeit innerhalb der sozialen Gemeinschaft setze auch voraus, dass der Einzelne unter den Bedingungen des ungehinderten Datenverkehrs frei kommunizieren könne.[277] Genau deswegen lässt das Recht auf informationelle Selbstbestimmung keine absolute unbegrenzte Herrschaft über eigene Daten zu, sondern der Einzelne muss auch Einschränkungen seines Rechts auf informationelle Selbstbestimmung dulden, um überwiegende Allgemeininteressen wahren zu können.[278]

---

270 BVerfGE 65, 1 (43); *Murswiek*, in: *Sachs* (Hrsg.), GG 2014, Art. 2 Rn. 72; *Horn*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art.2 Rn. 50; *Dreier*, in: *Dreier* (Hrsg.), GG 2013, Art. 2 Rn. 79.

271 BVerfGE 120, 378 (398 f.).

272 BVerfGE 65, 1 (45); 115, 320 (350); 118, 168 (185); 120, 378 (398 f.); 128, 1 (45).

273 BVerfGE 65, 1 (42).

274 BVerfGE 65, 1 (45), siehe auch *Jarass*, in: *Jarass/Pieroth*, GG 2016, Art. 2 Rn. 42;

275 *Di Fabio*, in: *Maunz*/*Dürig* (Begr.), GG 2017, Art. 2 Rn. 176.

276 BVerfGE 65, 1 (43).

277 BVerfGE 65, 1 (44).

278 BVerfGE 65, 1 (44).

In ständiger Rechtsprechung, insbesondere durch die Entscheidungen *„Rasterfahndung“*,[279] *„Online-Durchsuchung“*[280] und *„Automatisierte Kennzeichenerfassung“*[281], verlangt das BVerfG, dass Beschränkungen des Rechts auf informationelle Selbstbestimmung nur durch gesetzliche Ermächtigungen zulässig sind, in denen der Anlass, der Zweck und die Grenzen der Beschränkungen nach dem rechtsstaatlichen Gebot der Normenklarheit bereichsspezifisch, präzise und normenklar bestimmt werden. Des Weiteren müssen sie auch dem Verhältnismäßigkeitsprinzip entsprechen.[282] Außerdem müsse der Gesetzgeber angesichts der Gefährdungen unter den Bedingungen der automatischen Datenverarbeitung ausreichende organisatorische und verfahrensrechtliche Maßnahmen treffen, um dem Missbrauch personenbezogener Daten und der daraus resultierenden Gefahr einer Verletzung des Persönlichkeitsrechts vorzubeugen.[283]

3. Abgrenzung des Rechts auf informationelle Selbstbestimmung vom Fernmeldegeheimnis und das Verhältnis zwischen beiden Grundrechten

Bei der Prüfung der Verfassungsmäßigkeit der Vorratsdatenspeicherung ist das Verhältnis zwischen dem Recht auf informationelle Selbstbestimmung und dem Recht auf Fernmeldegeheimnis von Bedeutung. Die Vorratsdatenspeicherung ist für das Recht auf informationelle Selbstbestimmung insoweit relevant, als dass die Daten von den Umständen des Telekommunikationsvorgangs zu den personenbezogenen Daten zugeordnet und verarbeitet werden müssen.[284] Deswegen überschneiden sich der Schutzbereich des Rechts auf informationelle Selbstbestimmung und dem Recht auf Fernmeldegeheimnis. Dafür hat das BVerfG schon wiederholt festgelegt, dass das Recht auf informationelle Selbstbestimmung neben Art. 10 GG nicht zur Anwendung komme, wenn es sich auf den Telekommunikationsvorgang beziehe. Art. 10 GG enthalte spezielle Regeln für die durch Eingriffe erhobenen Daten und verdränge die allgemeine Vorschrift.[285] Einerseits enthält Art. 10 GG in seinem Anwendungsbereich *„eine spezielle Garantie“*[286], die das Recht auf in-

279 BVerfGE 115, 320 (320 ff.).
280 BVerfGE 120, 274 (274 ff.).
281 BVerfGE 120, 378 (378 ff.).
282 BVerfGE 65, 1 (44).
283 BVerfGE 65, 1 (44), dazu *Dreier*, in: *Dreier* (Hrsg.), GG 2013, Art. 2 Rn. 96.
284 *Pagenkopf*, in: *Sachs* (Hrsg.), GG 2014, Art. 10 Rn. 53; *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 10 Rn. 87; *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 98.
285 BVerfGE 100, 313 (358); 110, 33 (53); 113, 348 (364); 125, 260 (310).
286 BVerfGE 67, 157 (171); 100, 313 (357).

formationelle Selbstbestimmung verdrängt, andererseits stehen die beiden Grundrechte in einem Ergänzungsverhältnis zueinander.[287]

„Greift Art. 10 GG nicht ein, werden die technischen Kommunikationsdaten durch das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. mit Art. 1 Abs. 1 GG geschützt.“[288]

Obwohl die Sonderregelung die allgemeine Vorschrift verdrängt, lassen sich die im Volkszählungsurteil entwickelten Maßstäbe weitgehend auf die spezielle Garantie im Fernmeldegeheimnis übertragen, soweit die mittels Eingriff in das Fernmeldegeheimnis erlangten Daten die Verarbeitung personenbezogener Daten betreffen würden.[289] Das Fernmeldegeheimnis

„entfaltet seinen Schutz nicht nur gegenüber staatlicher Kenntnisnahme von Fernmeldekommunikationen, die die Kommunikationspartner für sich behalten wollten, vielmehr erstreckt sich seine Schutzwirkung auch auf den Informations- und Datenverarbeitungsprozess, der sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließt, und den Gebrauch, der von den erlangten Kenntnissen gemacht wird (so schon für das Recht auf informationelle Selbstbestimmung)“.[290]

Deswegen kommt das Recht auf informationelle Selbstbestimmung bei der Verfassungsmäßigkeitsprüfung der Vorratsdatenspeicherung zwar nicht zur Anwendung. Die sich daraus ableitenden allgemeinen Anforderungen an die Datenerhebung und die Datenverarbeitung sind aber auch zum Schutz des Telekommunikationsgeheimnisses zu achten.[291] Bei der Vorratsdatenspeicherung werden alle Telekommunikationsdaten auf Vorrat gespeichert. Auf diese Daten greifen die zuständigen Behörden bei Bedarf zu und verwenden diese. Es geht somit um die Erhebung und Verarbeitung von personenbezogenen Daten. Infolgedessen ist es für die Verfassungsmäßigkeit der Vorratsdatenspeicherung relevant, ob die Speicherung, Aufbewahrung, Übermittlung und Verwendung der Telekommunikationsdaten den datenschutzrechtlichen Anforderungen entsprechen.

---

287 BVerfGE, Beschluss vom 22.8.2006 – 2 BvR 1345/03, Rn. 66.

288 BVerfGE, Beschluss vom 22.8.2006 – 2 BvR 1345/03, Rn. 67.

289 BVerfGE 100, 313 (359); dazu *Pagenkopf*, in: *Sachs* (Hrsg.), GG 2014, Art. 10 Rn. 53; *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 10 Rn. 110; *Roßnagel*, in: *Roßnagel* (Hrsg.), Handbuch des Datenschutzrechts, S. 1261, Rn. 6.

290 BVerfGE 100, 313.

291 Siehe auch *Hermes*, in: *Dreier* (Hrsg.), GG 2013, Art. 10 Rn. 103; *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 100.

4. Datenschutzrechtliche Anforderungen aus dem Recht auf informationelle Selbstbestimmung

Seit dem Volkszählungsurteil hat das BVerfG konkrete grundlegende Anforderungen an die Datenverarbeitung herausgearbeitet. Dazu gehören insbesondere die Grundsätze der Zweckbestimmung, Zweckbindung, Erforderlichkeit, Datensparsamkeit und Datenvermeidung, das Transparenzgebot und der wirksame Rechtsschutz.[292]

a) Grundsatz der Zweckbindung und Erforderlichkeit

Der Grundsatz der Zweckbindung hängt eng mit dem Grundsatz der Zweckbestimmung zusammen.[293] Nach dem Zweckbindungsgrundsatz dürfen die Verarbeitung und die Nutzung der personenbezogenen Daten grundsätzlich nur im Rahmen des zuvor bestimmten Zwecks stattfinden.[294] Zur Einhaltung des Zweckbindungsgrundsatzes muss die Zwecksetzung vor der Datenerhebung so genau wie möglich bestimmt werden.[295] Je genauer der Verarbeitungszweck definiert wird, desto effektiver werden die Verwendung sowie die weitere Aufbereitung der Daten begrenzt. So kann der Betroffene die Verarbeitung seiner personenbezogenen Daten besser kontrollieren.

Den Anforderungen der Zweckbestimmung entsprechend ist die Sammlung personenbezogener Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken daher streng verboten.[296] Die Vorratsdatenspeicherung bezieht sich auf die anlasslose Speicherung aller Telekommunikationsverbindungsdaten, auf den anlassbezogenen Zugriff sowie die Verwendung der gespeicherten Vorratsdaten von den zuständigen Behörden. Bei einer derartigen Ausgestaltung der Datenerhebung und -verwendung kommt die Frage auf, ob die vor der Speicherung noch nicht festgestellte Verwendung als ein bestimmter Zweck für die Vorratsspeicherung gesehen werden.

In Hinblick auf § 113b TKG a.F., also der Fassung, die dem BVerfG vorlag, wurde als Zweck für die Speicherung die Verwendung für die Strafverfol-

---

292 BVerfGE 65, 1 (46), dazu genaue Auseinandersetzung siehe in *Trute*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, S. 174-179; siehe auch *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 103-104.

293 Vgl. *Trute*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, S. 177 Rn. 40.

294 BVerfGE 65, 1 (46), dazu *Zezschwitz*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, S. 221 Rn. 1; *Kühling*/*Seidel*/*Sivridis*, S. 110.

295 Siehe auch *Kühling*/*Seidel*/*Sivridis*, S. 110; *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 103.

296 BVerfGE 65, 1 (46).

gung, der Gefahrenabwehr und der Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes angegeben. Diese *„bloß vagen Beschreibungen"*[297] reichten nicht aus. Dennoch sah das BVerfG in dieser Vorratsspeicherung einen Unterschied zur streng verbotenen Vorratsspeicherung zu unbestimmten und noch nicht bestimmbaren Zwecken.[298] Der Zweck der fraglichen Vorratsspeicherung wurde als *„[...] spätere [anlassbezogene] Übermittlung an die für die Strafverfolgung oder Gefahrenabwehr zuständigen Behörden[...]"*[299] festgestellt und als bestimmter Zweck anerkannt. Dies werde zum einen dadurch sichergestellt, dass in einem ersten Schritt die Speicherung durch verpflichtete Private erfolge und nicht durch den Staat selber.[300] Der Abruf der Daten durch den Staat erfolge in einem zweiten Schritt nur bei Vorliegen eines konkreten Anlass unter rechtlich normierten Voraussetzungen.[301]

Diese Argumentation des BVerfG ist durchaus kritikwürdig, da der Zweck der Speicherung grundsätzlich vor der Speicherung festzulegen ist. Es reicht für die Bestimmbarkeit des Speicherungszwecks nicht ohne Weiteres aus, diesen erst bei einem zukünftigen Abruf festzulegen. Gegen die Argumentation des BVerfG spricht ferner, dass nicht allein auf die Festlegung des Zwecks abgestellt werden darf. Das Prinzip der Erforderlichkeit verlange, so das BVerfG in einem früheren Urteil, dass erhobene personenbezogene Daten auf das zum Erreichen des Zwecks erforderliche Minimum beschränkt werden müssten.[302] Die Speicherung personenbezogener Daten muss damit erforderlich sein, um den verfolgten Zweck zu erreichen. Ansonsten dürften beliebige personenbezogene Daten uferlos auf Vorrat gespeichert werden.[303]

In der Speicherungsphase besteht weder eine konkrete Gefahr noch ein bewiesener Verdacht gegen bestimmte Personen. Ob die gespeicherten Daten später wirklich verwendet werden oder nicht, steht zum Zeitpunkt der Vorratsspeicherung noch nicht fest. Die Wahrscheinlichkeit einer Verwendung

297 *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 103.
298 BVerfGE 125, 260 (321).
299 BVerfGE 125, 260 (317).
300 BVerfGE 125, 260 (321).
301 BVerfGE 125, 260 (321 ff.), so auch *Bull*, in: *van Ooyen*/*Möllers* (Hrsg.), S. 643.
302 BVerfGE 65, 1 (46), dazu *Trute*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, S. 178 Rn. 43; *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 103;
303 Vgl. *Kühling*, K&R 2004, 105 (109).

stellt aber noch keinen bestimmten Zweck für die Vorratsdatenspeicherung dar.[304]

Auch die Normen, die sich auf die Verwendung der Vorratsdaten beziehen, müssen dem Zweckbestimmungsgrundsatz gerecht werden. Eine solche ist insbesondere § 100g StPO. Auch hier kann die Vereinbarkeit mit dem Zweckbestimmungsgrundsatz bemängelt werden. In § 100g StPO wird der Verwendungszweck mit der Verfolgung von einer *„Straftat von erheblicher Bedeutung"* und Straftaten von *„auch im Einzelfall erheblicher Bedeutung"* umrissen. Dies ist sehr allgemein und unklar formuliert. Dadurch besteht die Gefahr der Ausuferung der Verwendung von Vorratsdaten.[305]

Die allgemeine Beschreibung aus § 113b TKG a.F. (nun § 113c TKG), dass die Daten für eine *„spätere Verwendung"* gespeichert werden müssten, und auch die unklare Formulierung aus § 100g StPO können zur Ausweitung der Verwendungsmöglichkeiten der gespeicherten Daten führen. Ohne ausreichende Bestimmtheit des Verarbeitungszwecks der Daten können die Überschaubarkeit und Kontrollierbarkeit der Datenverwendung erheblich beeinträchtigt werden.

b) Vorkehrungsmaßnahmen für Datensicherheit

Wegen der großen Datenmengen und der weitreichenden Aussagekraft der Telekommunikationsdaten bieten die Vorratsdaten zahlreiche Verwendungsmöglichkeiten. Sie können selbst als nützliche Datenquelle benutzt und auch mit anderen Datensammlungen verbunden werden, wodurch genaue Persönlichkeits- sowie Bewegungsprofile erstellt werden können. Damit sind sie sowohl für öffentliche als auch für nicht-öffentliche Stellen sehr interessant.[306] Die Gefahr der Enthüllung und des Missbrauchs der Vorratsdaten steigt somit erheblich an. Um die gespeicherten Daten vor Enthüllung und Zugriff zu schützen, müssten technische und auch organisatorische Sicherheitsmaßnahmen mit hohem Sicherheitsstandard bei der Datenaufbewahrung und Datenübermittlung getroffen werden.[307] Eine entsprechende Norm muss

304 So auch *Gola*/*Klug*/*Reif*, NJW 2007, 2599 (2599); *Gitter*/*Schnabel*, MMR 2007, 411 (414); *Albers*/*Reinhardt*, ZJS 2010, 767 (711).

305 Siehe oben Erläuterung zu den Anforderungen in Bezug auf die Bestimmtheit; vgl. *Breyer*, StV 2007, 214 (217).

306 BVerfGE 125, 260 (325); *Breyer*, S. 213; *Gietl*, K&R 2007, 545 (546); *Bizer*, DuD 2007, 586 (588 f.); *Roßnagel*/*Bedner*/*Knopp*, DuD 2009, 536 (537).

307 BVerfGE 65, 1 (44); 125, 260 (325 f.); dazu *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 10, Rn. 25; *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 10 Rn. 92.

daher „[…] hinreichend anspruchsvolle und normklare […]“[308] Anforderungen enthalten, um dem Gebot der Verhältnismäßigkeit im engeren Sinne zu entsprechen.

Diesen Anforderungen entsprach § 113a Abs. 10 TKG a.F., so das BVerfG in seinem Urteil zur Vorratsdatenspeicherung, nicht.[309] Gemäß § 113a Abs. 10 TKG a.F. wurde den Diensteanbietern zwar zutreffend die Pflicht auferlegt, dass sie den Schutz der gespeicherten Verkehrsdaten sowie die im Bereich der Telekommunikation erforderliche Sorgfalt beachten und durch technische und organisatorische Maßnahmen sicherstellen müssen. Der Zugang zu den gespeicherten Daten war zudem ausschließlich speziell dazu ermächtigten Personen möglich. Nach dem BVerfG reichten diese Vorgaben jedoch für eine Maßnahme wie die Vorratsdatenspeicherung mit einem besonders schwerwiegenden Eingriffscharakter und der damit einhergehenden verfassungsrechtlich gebotenen Gewährleistung eines besonders hohen Sicherheitsstandards nicht aus.[310]

Die allgemein erforderliche Sorgfalt, die § 113a Abs. 10 TKG a.F. für die Sicherheit der Datenspeicherung statuierte, konnte, so das BVerfG, den besonders hohen Anforderungen an die Sicherheit der Datenspeicherung nicht Rechnung tragen.[311] Defizite der Datensicherheit könnten nur schwer kompensiert werden. Die Vorratsdaten müssten von den privaten Telekommunikationsanbietern gespeichert und aufbewahrt werden, die zusätzlich in Sicherheitsmaßnahmen investieren müssten, ohne die hierfür notwendigen Gewinne erwirtschaften zu können.[312] Das erforderliche hohe Schutzniveau sei für viele kleinere Betriebe angesichts ihrer Finanzkraft fast unzumutbar.[313] Damit genügten die Regelungen der Vorratsdatenspeicherung bezüglich der Datensicherheit den verfassungsrechtlichen Anforderungen nicht. Zurzeit finden sich die novellierten und erweiterten Regelungen zur Datensicherheit in § 113d TKG.

---

308 BVerfGE 125, 260 (325).
309 BVerfGE 125, 260 (347).
310 BVerfGE 125, 260 (348).
311 BVerfGE 125, 260 (348).
312 Vgl. BVerfGE 125, 260 (325); *Albers*/*Reinhardt*, ZJS 2010, 767 (772); *Pfitzmann*/*Köpsell*, DuD 2009, 542 (544).
313 Siehe *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 145; *Freiling*, Technischer Bericht TR-2009-005, S. 19.

c) Transparenzgebot

Das Recht auf informationelle Selbstbestimmung gewährleistet die Kontrolle des Einzelnen über seine persönlichen Daten. Daher ist die Transparenz der Datenerhebungs- und Datenverarbeitungsvorgänge für den Datenschutz von Bedeutung.[314] Die Betroffenen können den Verarbeitungsprozess ihrer Daten nur dann beeinflussen, wenn sie zur Kenntnis nehmen, *„wie, von wem und aus welchem Grund ihre Daten erfasst und verarbeitet werden, wie lange sie aufbewahrt werden und ob sie Zugriff auf ihre Daten haben und die Berichtigung oder Löschung der Daten verlangen können"*.[315] Ohne Kenntnis seien die Betroffenen nicht in der Lage, das Recht auf Berichtigung und Löschung auszuüben und die Unrechtmäßigkeit der Verarbeitung seiner Daten geltend zu machen.[316] Damit ist das Transparenzgebot eine zentrale Voraussetzung für den Schutz der informationellen Selbstbestimmung.[317]

Bei der Vorratsdatenspeicherung ist die Transparenz bezüglich des Abrufs und der Verwendung gespeicherter Telekommunikationsdaten von Gewicht. Nach § 100g StPO dürfen die gespeicherten Daten auch ohne Wissen des Betroffenen abgerufen werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten erforderlich ist. Nach dem BVerfG darf der Gesetzgeber für die Gefahrenabwehr und die Aufgabenerfüllung der Nachrichtendienste die Daten ohne Wissen des Betroffenen grundsätzlich verwenden.[318] Für die Strafverfolgung ist dies verfassungsrechtlich nur dann zulässig, wenn im Einzelfall ohne den Datenabruf der Zweck der Untersuchung vereitelt wird und richterlich angeordnet wird.[319] Die Pflicht einer zumindest nachträglichen Benachrichtigung bei der heimlichen Verwendung von persönlichen Daten ist vorzuschreiben.[320] Ausnahmen sind in Abwägung mit verfassungsrechtlich geschützten Rechtsgütern Dritter zulässig, aber auf das unbedingt Erforderliche zu beschränken.[321]

Den Vorgaben der Vorratsdatenspeicherung fehlt es vor allem an konkreten Beschränkungen für die heimliche Verwendung Vorratsdaten. § 100g StPO

---

314 *Trute*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, S. 174 Rn. 33.

315 Gesamtkonzept für den Datenschutz in der Europäischen Union, von der Europäischen Kommission, Brüssel, den 4.11.2010, KOM (2010) 609 endgültig, S. 6; *Kühling*/*Seidel*/*Sivridis*, S. 111.

316 BVerfGE 65, 1 (42 f.); 100, 313 (361); 125, 260 (335); *Kühling*/*Seidel*/*Sivridis*, S. 111.

317 Sehe auch *Trute*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, S. 174 Rn. 33.

318 BVerfGE 125, 260 (336).

319 BVerfGE 125, 260 (336).

320 BVerfGE 125, 260 (336).

321 BVerfGE 125, 260 (336).

hat einen zu weiten Anwendungsbereich. In diesem Aspekt hat sich die Vorschrift des § 100g StPO seit dem Urteil des BVerfG nicht geändert. Insbesondere enthält § 100g StPO einen nicht abschließenden Katalog von Straftaten, für deren Verfolgung eine Verwendung von Vorratsdaten möglich ist. Das Tatbestandsmerkmal „eine Straftat von auch im Einzelfall erheblicher Bedeutung" in § 100g Abs. 1 Nr. 1 StPO ohne klare Bewertungsmaßstäbe reicht nicht aus. Dies kann zu einer willkürlichen heimlichen Erhebung der Vorratsdaten führen. Die Vorschrift des § 100g StPO erfüllt damit das Transparenzgebot nicht. Diese Regelung stellt ohne abschließenden Katalog eine unklare Regelung dar und kann die heimliche Verwendung somit nicht rechtfertigen.

Die §§ 101 ff. StPO regeln die Benachrichtigungspflichten. Demgemäß sind die Zielpersonen sowie die erheblich mitbetroffenen Personen grundsätzlich nachträglich zu benachrichtigen. Ausnahmsweise unterbleibt die Benachrichtigung, wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen (§ 101 Abs. 4 S. 3 StPO). Ferner kann die Benachrichtigung auch unterbleiben, wenn die Betroffenen von der Maßnahme nur unerheblich betroffen wurden und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung haben (§ 101 Abs. 4 S. 4 StPO).

Das BVerfG hat festgestellt, dass der Umfang dieser vorgesehenen Benachrichtigungspflichten keinen verfassungsrechtlichen Bedenken ausgesetzt ist.[322] Jedoch fehle die richterliche Kontrolle über das Ausbleiben der Benachrichtigung nach § 101 Abs. 4 StPO, so das Gericht, und dies trage dem hohen Stellenwert der Benachrichtigung für eine transparente Verwendung der Vorratsdaten nicht hinreichend Rechnung.[323] Unklar war für BVerfG auch, auf welche konkreten Maßstäbe der Abwägung in § 101 Abs. 4 Satz 4 StPO Bezug genommen wird, nach denen zu beurteilen ist, ob die Adressaten unerheblich betroffen werden und ob sie Interesse an einer Benachrichtigung haben.[324] Wegen der weitverbreiteten Nutzung der Telekommunikationsmittel und der Vernetzung von Telekommunikation können zahlreiche verschiedene Benutzer betroffen sein, obwohl sich die Abfrage nicht unmittelbar auf sie bezieht. Ohne klare Maßstäbe für die Abwägung kann das Unterbleiben der Benachrichtigung dieser Personen willkürlich sein. Demzufolge wurde das Transparenzgebot insgesamt bei den Vorgaben der Vorratsdatenspeicherung nicht gewährleistet.

---

322 BVerfGE 125, 260 (353).
323 BVerfGE 125, 260 (354).
324 Siehe auch *Ziebarth*, DuD 2009, 25 (31); *Szuba*, S. 154; *Moser-Knierim*, S. 368.

Als Reaktion auf diese Kritikpunkte lagerte der Gesetzgeber die Verkehrsdatenabfrage aus dem § 101 StPO aus und schuf in § 101a StPO spezielle verfahrensrechtliche Anforderungen für die Verkehrsdatenabfrage. In dieser Vorschrift hat der Gesetzgeber unter anderem ein besonderes Augenmerk auf die Transparenzanforderungen gelegt. Gemäß § 101a Abs. 6 StPO sind die Beteiligten der betroffenen Telekommunikation von der Erhebung der Verkehrsdaten nach § 100g StPO zu benachrichtigen.

d) Wirksamer Rechtsschutz

Für die Gewährleistung eines effektiven Rechtsschutzes ist aus Karlsruher Sicht der Zugriff und die Verwendung der Vorratsdaten grundsätzlich unter Richtervorbehalt zu stellen.[325] Art. 10 GG enthält keinen Richtervorbehalt.[326] Aus Sicht des Gerichts ist eine vorbeugende Kontrolle durch eine unabhängige Instanz für die Ermittlungsmaßnahmen dennoch verfassungsrechtlich für Maßnahmen erforderlich, die zu einem schwerwiegenden Grundrechtseingriff führen würden.[327] *„Das Grundgesetz geht davon aus, dass Richter aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer strikten Unterwerfung unter das Gesetz (Art. 97 GG) die Rechte der Betroffenen im Einzelfall am besten und sichersten wahren können.“*[328] Bei der Durchführung der heimlichen staatlichen Ermittlungsmaßnahme sei eine unabhängige richterliche Kontrolle von besonders wesentlicher Bedeutung.[329]

Gemäß den Vorgaben in § 100g StPO dürfen die gespeicherten Daten auch ohne Wissen des Betroffenen abgefragt oder übermittelt werden. In diesem Fall ist ein Richtervorbehalt erforderlich, um den Betroffenen einen effektiven Rechtsschutz zu gewährleisten. Gefordert wird daher, dass sie *„in spezifischer und normenklarer Form mit strengen Anforderungen an den Inhalt und die Begründung der gerichtlichen Anordnung“*[330] vorgeschrieben werden muss. Die richterliche Anordnung muss zugleich *„das Erfordernis einer hinreichend substantiierten Begründung und Begrenzung der Abfrage der begehrten Daten“*[331] befolgen.

---

325 BVerfGE 125, 260 (337); *Kühling*/*Seidel*/*Sivridis*, S. 58; *Hermes*, in: *Dreier* (Hrsg.), GG 2013, Art. 10 Rn. 74.
326 *Durner*, in: *Maunz*/*Dürig* (Begr.), GG 2017, Art. 10 Rn. 152.
327 BVerfGE 125, 260 (337); *Hermes*, in: *Dreier* (Hrsg.), GG 2013, Art. 10 Rn. 98.
328 BVerfGE 103, 142 (151).
329 BVerfGE 120, 274 (331).
330 BVerfGE 125, 260 (338).
331 BVerfGE 125, 260 (338).

Gemäß § 100g Abs. 2 Satz 1 StPO a.F. und nun § 101a Abs. 1 S. 1 StPO gilt § 100a Abs. 3 StPO entsprechend. Die Vorratsdaten sind also nur anlassbezogen und verdachtsabhängig abzufragen und zu übermitteln. Die Abfrage und Nutzung der Vorratsdaten dürfen nur nach einer richterlichen Anordnung nach § 101a Abs. 1 S. 1 i.V.m. § 100e Abs. 1 S. 1 StPO durchgeführt werden. Darüber hinaus wird auch eine vorbeugende richterliche Kontrolle in § 101a Abs. 6 i.V.m. § 101 Abs. 6 StPO für die Zurückstellung der Benachrichtigung vorgeschrieben.

Die vorbeugende richterliche Kontrolle der Datenabfrage und Datennutzung selbst und der Zurückstellung der Benachrichtigung hielt das BVerfG bereits zum Zeitpunkt des Urteils zur Vorratsdatenspeicherung für qualifiziert, die verfassungsrechtlichen Anforderungen zu gewährleisten.[332] Aber die formalen Anforderungen seien nicht hinreichend klar geregelt worden. Bei den Regelungen geht man nur von Mindestanforderungen an die Entscheidungsformel aus, spezielle Regelungen bezüglich der Abfrage und Verwendung der Vorratsdaten sind jedoch nicht vorgesehen worden.[333] Angesichts des besonders schweren Eingriffsgewichts der Vorratsdatenspeicherung reichen nur allgemeine formale Regelungen hinsichtlich des verfassungsrechtlichen Gebots vorbeugender richterlicher Kontrolle jedoch nicht aus. Aus diesem Grund wurden die verfahrensmäßigen Anforderungen an die Verkehrsdatenabfrage in den § 101a StPO ausgelagert.

III. Die Berufsfreiheit (Art. 12 Abs. 1 GG)

1. Eingriff in den Schutzbereich

Art. 12 Abs. 1 GG gewährleitet jedem Deutschen die Freiheit der Berufswahl und Berufsausübung. Ein Beruf ist dabei jede auf Dauer angelegte Tätigkeit, die der Schaffung und Erhaltung einer Lebensgrundlage diene oder dazu beitrage.[334] Juristische Personen können sich gemäß Art. 19 Abs. 3 GG auch auf die Berufsfreiheit berufen.[335] Die Berufsfreiheit schützt dem Einzelnen einerseits die freie Berufswahl, dass er frei entscheidet, überhaupt einen Beruf

---

332 BVerfGE 125, 260 (354).

333 BVerfGE 125, 260 (354 f.).

334 BVerfGE, 7, 377 (397); dazu *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 12, Rn. 5; *Nolte*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 12 Rn. 12; *Wieland*, in: *Dreier* (Hrsg.), GG 2013, Art. 12 Rn. 41 ff.

335 *Wieland*, in: *Dreier* (Hrsg.), GG 2013, Art. 12 Rn 56; *Mann*, in: *Sachs* (Hrsg.), GG 2014, Art. 12 Rn. 37.

zu ergreifen oder darauf zu verzichten.[336] Andererseits wird die Berufsausübung geschützt, sodass die gesamte berufliche Tätigkeit, insbesondere Form und Mittel, Umfang sowie Inhalt der beruflichen Betätigung frei ausgestaltet wird.[337] Ein Eingriff in die Berufsfreiheit liegt vor, wenn eine Regelung oder staatliche Maßnahme sich unmittelbar auf Berufe bezieht oder eine objektiv berufsregelnde Tendenz hat.[338] Unter der *„objektiv berufsregelnden Tendenz"* versteht man eine staatliche Maßnahme, die in erster Linie als rechtliche Rahmenbedingung für die Berufsausübung verstanden wird und infolge ihrer Gestaltung in einem engen Zusammenhang mit der Ausübung des Berufs steht.[339]

Gemäß den Vorgaben der Vorratsdatenspeicherung (§§ 113a bis 113g TKG) werden Diensteanbietern, die öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringen, Speicherungs- und Übermittlungspflichten auferlegt. Die freie Berufsausübung der Diensteanbieter wird damit zwar nicht final oder unmittelbar eingeschränkt, aber die Diensteanbieter sind zur Erfüllung zusätzlicher Pflichten in Bezug auf den Umfang der Speicherung von Telekommunikationsdaten verpflichtet. Die Veränderung der Berufsausübung ist auf die Durchführung der Vorratsdatenspeicherung zurückzuführen. Die Regelung der Vorratsdatenspeicherung betrifft damit die berufliche Tätigkeit der Diensteanbieter und hat objektiv berufsregelnde Tendenz.[340] Ein Eingriff von der Vorratsdatenspeicherung in die Berufsfreiheit der Telekommunikationsdienstanbieter liegt infolgedessen vor.

2. Verfassungsrechtliche Rechtfertigung

Nach Art. 12 Abs. 1 Satz 1 GG kann die Berufsausübung durch Gesetz oder auf Grund eines Gesetzes geregelt werden.[341] Die Einschränkung der Berufsfreiheit darf aber nur aus Gründen des Gemeinwohls durchgeführt werden, der Eingriff muss ferner den Anforderungen des Verhältnismäßigkeitsgrundsatzes erfüllen.[342] Die Speicherungs- und Übermittlungspflichten zie-

---

336 BVerfGE 58, 358 (364); dazu *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 12 Rn. 9; *Nolte*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 12 Rn. 35 f.

337 *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 12 Rn. 10; *Nolte*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 12 Rn. 39.

338 BVerfGE 22, 380 (384); BVerfGE 46, 120 (137); 95, 267 (302); dazu *Nolte*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 12 Rn. 79, 80; *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 12 Rn. 14 ff.

339 BVerfGE 70, 191 (214); 128, 1 (58); 111, 191 (213); dazu *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 12 Rn. 15;*Wieland*, in: *Dreier* (Hrsg.), GG 2013, Art. 12 Rn. 71.

340 So auch BVerfGE 125, 260 (359); *Szuba*, S. 182; *Breyer*, S. 278 f.

341 Siehe *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 12 Rn. 28.

342 BVerfGE 125, 260 (360); 30, 292 (316); dazu *Mann*, in: *Sachs* (Hrsg.), GG 2014,

len auf eine effektive Strafverfolgung und Gefahrenabwehr und dadurch besseren Sicherheitsschutz ab. Damit greift die Vorratsdatenspeicherung in die Berufsfreiheit aus *„vernünftiger Erwägung des Gemeinwohls"*[343] ein. Des Weiteren wird die Auferlegung der Speicherungs- und Übermittelungspflicht für diesen legitimen Zweck als ein geeignetes und erforderliches Mittel bejaht.

Fraglich ist jedoch, ob der Eingriff in die Berufsfreiheit angemessen ist. Das ist der Fall, wenn der Nutzen für das Gemeinwohl, dem die Beschränkung auf die Berufsfreiheit der Telekommunikationsdienstanbieter dient, nicht außer Verhältnis zur Schwere des Eingriffs steht.[344] Die fragliche Maßnahme dürfe den Betroffenen nicht übermäßig belasten, die Grenze der Zumutbarkeit bei einer Gesamtabwägung müsse noch gewahrt werden.[345]

Nach Ansicht des BVerfG wirkt die Auferlegung der Speicherung- sowie Übermittlungspflicht gegenüber den betroffenen Diensteanbietern typischerweise nicht übermäßig belastend.[346] Der Grund liegt zuerst darin, dass die Dienstanbieter unabhängig von den Speicherungspflichten der Vorratsdatenspeicherung über ein *„hohes Maß an Technikbeherrschung im Bereich der Telekommunikationsdatenerfassung, -speicherung und -verarbeitung"* verfügen müssten, um ihre Unternehmen auf dem Telekommunikationsmarkt zu betreiben. Ferner würden sie zum eigenen betrieblichen Zweck ohnehin einen Großteil der die Speicherungspflicht betroffenen Telekommunikationsdaten speichern. Anschließend hätten die Diensteanbieter technische und organisatorische Maßnahmen für die Gewährleistung der Datensicherheit unabhängig von der auferlegten Speicherungspflicht zu treffen. Die finanziellen Lasten daraus seien erstens nicht nur auf die Auferlegung der Vorratsspeicherung zurückzuführen und zweitens nicht unzumutbar.

Um Gemeinwohlbelange zu wahren, könne der Gesetzgeber den Privaten Pflichten im Rahmen ihrer Berufstätigkeit auferlegen. Die mit der Speicherungspflicht verbundenen Kosten könnten auf diese Weise insgesamt in den Markt verlagert werden. Eine Berufsausübungsregelung ist nur dann unverhältnismäßig, wenn sie bei einer Betroffenengruppe das Übermaßverbot verletze. Bei der Vorratsdatenspeicherung ist weder substantiiert vorgebracht

---

Art. 12 Rn. 142.

343 BVerfGE 7, 377 (405).

344 Siehe *Wieland*, in: *Dreier* (Hrsg.), GG 2013, Art. 12 Rn. 95.

345 *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 12 Rn 45.

346 BVerfGE 125, 260 (360 ff.).

noch erkennbar, dass die Kostenlasten in dieser Weise erdrosselnde Wirkungen haben. Hinsichtlich möglicher verbleibender Kostenlasten begegnet die Übermittlungspflicht auch keinen grundsätzlichen Bedenken, sodass eine Entschädigungsregelung vorgesehen werden müsste. Damit ist der Eingriff durch die Auferlegung der Pflichten bezüglich der Vorratsdatenspeicherung weder hinsichtlich des technischen Aufwands noch hinsichtlich der damit verbundenen finanziellen Belastung der Dienstanbieter unverhältnismäßig.[347]

Zwar speichern und bewahren die Dienstanbieter ohne die Speicherungspflichten durch Vorratsdatenspeicherung die Telekommunikationsdaten ohnehin auch für ihre eigenen betrieblichen Zwecke, aber die Auferlegung der Speicherungspflichten hat immerhin beträchtliche zusätzliche Belastungen erzeugt. Um die auferlegten Speicherungspflichten zu erfüllen, müssen die Dienstanbieter viele für Abrechnungs- oder Beweiszwecke sowie andere eigene Zwecke nicht erforderliche Daten protokollieren und aufbewahren. Für die Speicherung dieses riesigen Datenvolumens sind damit entsprechende zusätzliche Investitionen in Technik sowie Personal notwendig. Für viele Unternehmen kann die Erfüllung der zusätzlichen Pflichten dazu führen, dass die vorhandenen Einrichtungen nachgerüstet oder neue Geräte angeschafft werden müssen.

Außer solcher einmaligen Investitionskosten der Anlagen sind bei Diensteanbietern weiterhin ständige Einsatzkosten für Aufbewahrung der gespeicherten Daten zu besorgen.[348] Dazu können spezielle technische Ausrüstungen und angesichts der Anforderungen der Datensicherheit[349] hinsichtlich der Trennung von zu betrieblichen Zwecken gespeicherten Daten und der Vorratsdaten, der Trennung von Verkehrsdaten und Inhaltsdaten[350] und angesichts jeder Datenübermittlung zu den zuständigen Behörden auch ein Mehr an Speicherungskapazität gehören.[351] Den Anbietern entstehen demzufolge hohe Kosten, die kleine Unternehmen kaum leisten können.[352] Eine präzise Schätzung oder Untersuchung der insgesamt anfallenden Investitionskosten und sonstigen Kosten steht noch aus. Aber eine grobe Schätzung der Deutschen Telekom AG hat gezeigt, dass die zusätzliche Infrastruktur allein für

347 BVerfGE 125, 260 (361-363).
348 *Breyer*, S. 289; *Freiling*, Technischer Bericht TR-2009-005, S. 19; *Szuba*, S. 185 f.
349 BVerfGE 125, 260 (325).
350 Vgl. *Breyer*, S. 289.
351 Für eine Ausführliche Darstellung der praktischen Implementierung der Vorratsdatenspeicherungspflicht der Diensteanbieter siehe *Albrecht*/*Kilchling*, S. 178 ff.
352 Siehe *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 145; *Freiling*, Technischer Bericht TR-2009-005, S. 19.

Festnetztelefonie etwa 1 Million Euro kostet, und dass der Betrieb der Infrastruktur pro Monat 100.000 Euro kosten werde.[353] Ferner müssen die Diensteanbieter bei den zusätzlichen Speicherungs- und Übermittlungspflichten das gesteigerte Haftungsrisiko angesichts der eventuellen Datenenthüllung übernehmen, das ohne Auferlegung der Vorratsdatenspeicherung vermeidbar ist.[354]

Während die Diensteanbieter zusätzliche Pflichten erfüllen müssen, wird keine Regelung der Entschädigung in der Vorratsdatenspeicherung ausgestaltet. Ohne Entschädigung der zusätzlichen Kosten oder technischer sowie finanzieller Unterstützung stellt die Pflicht der Vorratsdatenspeicherung für die Diensteanbieter damit eine große zusätzliche Belastung dar. Zwar dürfen den Diensteanbietern für Gemeinwohlbelange Speicherungs- und Übermittlungspflichten auf deren Kosten auferlegt werden. Das bedeutet aber nicht, dass daraus entstehende Kosten ausschließlich von den Diensteanbietern getragen werden sollen. Die verfassungsrechtliche Rechtfertigung kommt der Vorratsdatenspeicherungspflicht nicht ohne Weiteres zu, sondern nur, sofern sie zu keiner erdrosselnden Wirkung wegen der Kostenlasten der Diensteanbieter führt.

Die Vorratsdatenspeicherungspflicht kann unverhältnismäßig sein, wenn ihre Belastung unangemessen ist im Vergleich zur ihrer förderlichen Wirkung auf den Zweck, der dem Gemeinwohl dient.[355] Der Nutzen der Vorratsdatenspeicherung erscheint im Vergleich zu den immensen Belastungen, die die Dienstanbieter tragen müssen, sehr beschränkt.[356] Für die beschränkte positive Wirkung werden die Dienstanbieter mit einem enormen Aufwand belastet. Der Eingriff durch Auferlegung der Vorratsdatenspeicherungspflicht in die Berufsfreiheit der Telekommunikationsdiensteanbieter ist insoweit nicht angemessen.

---

353 *Freiling*, Technischer Bericht TR-2009-005, S. 19; Noch ein Beispiel: der Vertreter eines Diensteanbieter schätzt Investitionskosten für Durchführung der Vorratsdatenspeicherungspflicht für sein Unternehmen auf 12 Mio. Euro, ausführliche Darstellung der praktischen Implementierung der Vorratsdatenspeicherungspflicht der Diensteanbieter siehe *Albrecht*/*Kilchling*, S. 180.

354 Vgl. *Gietl*, K&R 2009, 69 (70); *Breyer*, StV 2007, 214 (219); *Szuba*, S. 185.

355 Vgl. *Breyer*, S. 287.

356 Siehe oben die Erläuterung der Nutzen der Maßnahme der Vorratsdatenspeicherung.

IV. Zusammenfassung – Verfassungsrechtliche Vorgaben für die Vorratsdatenspeicherung

Bei der Vorratsdatenspeicherung werden Verbindungsdaten des Telekommunikationsverkehrs aller Nutzer verdachtsunabhängig und anlasslos auf Vorrat gespeichert, um für die zukünftige mögliche Strafverfolgung und Gefahrenabwehr zur Verfügung zu stehen. Die Speicherungspflicht betrifft die Daten der näheren Umstände des Telekommunikationsvorgangs und greift damit in das Fernmeldegeheimnis der Bürger ein.

Die Eingriffsintensität der Vorratsdatenspeicherung ist schwer zu quantifizieren. Denn sie betrifft alle Bürger und hat damit einen maximalen Wirkungsbereich. Infolge der hohen Aussagekraft der gespeicherten Daten und der Verbindungsmöglichkeit mit anderen personenbezogenen Daten führt die Vorratsdatenspeicherung zu dem großen Risiko, dass Persönlichkeits- und Bewegungsprofile der Bürger erstellt werden. Die spezifische Vertraulichkeitserwartung der Telekommunikation wird dadurch beeinträchtigt.

Hinzu kommt, dass ihre Durchführung weder von einem Verdacht gegen eine bestimmte Personen noch eine konkrete Gefahr abhängt. Eine solche vorsorgliche Vorratsspeicherung ist nichts anderes als eine Maßnahme, die auf dem Prinzip beruht, alle Bürger zu verdächtigen. Sie schafft hinsichtlich der umfassenden Streubreite und der immensen Verknüpfungsmöglichkeit mit anderen Datensammlungen eine systematische gesellschaftliche Überwachung. Des Weiteren wird die Unbefangenheit des Verhaltens der Bürger wegen der Befürchtung des Datenmissbrauchs sowie der Datenenthüllung und des bedrohlichen Gefühls des Beobachtet-seins gefährdet. Die Wahrnehmung der anderen Grundrechte kann dadurch behindert werden.

Im Vergleich mit den schweren Beeinträchtigungen des Eingriffs hat sich die Vorratsdatenspeicherung bei der Effektivierung der Strafverfolgung und Gefahrenabwehr nur sehr begrenzt positiv ausgewirkt. Zwar dient die Vorratsdatenspeicherung einem legitimen Zweck und funktioniert auch als eine geeignete und erforderliche Sicherheitsmaßnahme zur Strafverfolgung und Gefahrenabwehr. Aber zweifelhaft ist, ob die Maßnahme zu dem geschützten Interesse in einem angemessenen Verhältnis steht.

Wegen des Bezugs zur Verarbeitung persönlicher Daten müssen die Vorgaben der Vorratsdatenspeicherung die datenschutzrechtlichen Anforderungen nach der ständigen Rechtsprechung des BVerfG erfüllen. Diese aus dem Recht auf

informationelle Selbstbestimmung entwickelten allgemeinen Anforderungen gelten verfassungsrechtlich als Teil der bereichsspezifischen Grundrechte. Dazu gehören insbesondere der Zweckbestimmungsgrundsatz, das Erforderlichkeitsprinzip, der Zweckbindungsgrundsatz, die Vorkehrungsmaßnahme für Datensicherheit, das Transparenzgebot und der effektive Rechtsschutz.

Zwar stellt die Vorratsdatenspeicherung keine vom Bundesverfassungsgericht streng verbotene Speicherung von personenbezogenen Daten auf Vorrat zu unbestimmten und noch nicht bestimmbaren Zwecken dar, aber die *„spätere anlassbezogene Verwendung“* in der Speicherungsphase ist auch nicht als bestimmter Zweck zu qualifizieren. Dabei fehlt auch die Erforderlichkeit der Speicherung, da die Anknüpfung der zu speichernden Daten an die spätere mögliche Verwendung nicht gewiss ist. Mangels der Bestimmtheit der Speicherungszwecke kann der Zweckbindungsgrundsatz nur schwer befolgt werden.

Angesichts der großen Datenmenge und weitreichenden Aussagekraft der betroffenen Telekommunikationsdaten sind technische sowie organisatorische Sicherheitsmaßnahmen mit besonders hohem Sicherheitsstandard gegen Missbrauch und ungerechten Zugriff zu treffen. Darüber hinaus haben die Datenerhebungs- und Datenverarbeitungsvorgänge zur Erfüllung des Transparenzgebots grundsätzlich offen zu erfolgen. Dies stellt den Gesetzgeber insofern vor Probleme, als die Datenabfrage zur Zweckerreichung häufig heimlich abläuft. Hier ist also ein äußerst hohes Maß an gesetzgeberischem Feingefühl verlangt. Wegen des besonders schweren Eingriffsgewichts der Vorratsdatenspeicherung ist eine wirksame vorbeugende richterliche Kontrolle notwendig. Es muss eine vorbeugende richterliche Kontrolle für die Abfrage und Verwendung der Vorratsdaten selbst vorgeschrieben werden.

C. Vorratsdatenspeicherung aus europarechtlicher Sicht

I. Kompetenzfrage der Richtlinie zur Vorratsdatenspeicherung

Die Bekämpfung des Terrorismus wird als ein vorrangiges Ziel der Europäischen Union anerkannt.[357] Dazu ist effektive Strafverfolgung und Gefahrenabwehr in den Mitgliedstaaten und die Zusammenarbeit zwischen den Mitgliedstaaten erforderlich. Daher wurde eine einheitliche Vorratsspeicherungspflicht der Telekommunikationsdaten in der Europäischen Union als ein wirksames Instrument, das Strafverfolgung effektiveren und polizeiliche Zusammenarbeit intensivieren kann, wiederholt gefordert. Das Konzept der Vorratsdatenspeicherung wurde zwar anfänglich vom europäischen Gesetzgeber zurückhaltend behandelt, aber bald wegen der aktuellen Bedrohungslage schnell in die Tat umgesetzt.[358] Allerdings blieb die Rechtmäßigkeit der Richtlinie zur Vorratsdatenspeicherung stets fragwürdig. Vor allem wurde bezüglich der formellen Rechtmäßigkeit kritisiert, dass die Vorratsdatenspeicherung statt des Funktionierens des Binnenmarktes die polizeiliche und justizielle Zusammenarbeit in Strafsachen betreffe, womit sie zu den Regelungsgegenständen der dritten Säule gehörte und somit nicht durch eine Richtlinie geregelt werden müsste.[359] Irland hat aus diesem Grund am 6. Juni 2006 eine Nichtigkeitsklage gegen diese Richtlinie vor dem EuGH eingereicht. Die Klage wurde jedoch vom EuGH am 10. Februar 2009 abgewiesen.

In der Richtlinie wird begründet, dass eine einheitliche Vorratsspeicherungspflicht nötig sei, da die rechtlichen und technischen Unterschiede zwischen den nationalen Vorschriften zur Vorratsdatenspeicherung zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten den Binnenmarkt für elektronische Kommunikation beeinträchtigen würden.[360] Somit stellen die Ziele der Richtlinie die Harmonisierung der Pflicht für Diensteanbieter im Zusammenhang mit der Vorratsdatenspeicherung und die Sicherstellung der Vorratsdaten bei Bedarf dar.[361] In dieser Darstellung wird der Bezug der Vorratsdatenspeicherung zum Binnenmarkt insoweit unzutreffend hergestellt, als die uneinheitliche Speicherungspflicht der Diensteanbieter – unabhängig vom Zweck der Speicherungspflicht selbst –, als bestehen-

---

357 Schlussfolgerungen und Aktionsplan anlässlich der außerordentlichen Tagung des Europäischen Rates am 21. September 2001 in Brüssel, SN 140/01, S. 1.

358 Entstehung und Hintergründe der Richtlinie zur Vorratsdatenspeicherung siehe oben Kapitel 2, A.

359 Siehe zum Beispiel *Simitis*, NJW 2006, 2011 (2013); *Breyer*, StV 2007,214 (215f.); *Braum*, ZRP 2009, 174 (175); *Ambos*, JZ 2009, 468 (469); *Terhechte*, EuZW 2009, 199 (201); *Ziebarth*, DuD 2009, 25 (27).

360 ABI. EG Nr. L 105, S. 54.

361 ABI. EG Nr. L 105, S. 56.

des Hemmnis zur Errichtung des Binnenmarktes angesehen wird. Zwar zielt die Speicherungspflicht an sich auf die Stärkung der Sicherheit ab, aber die Vereinheitlichung dieser Pflicht hat faktisch Auswirkungen auf die Errichtung des Binnenmarkts. Damit darf die Vorratsdatenspeicherung zu einer Binnenmarktregelung gezählt und durch Richtlinie geregelt werden.

Mit dem Unterschied zwischen dem Zweck der Speicherungspflicht selbst und von der Richtlinie sowie die damit verbundene Frage, wie man in dieser Situation den Hauptzweck der fraglichen Regelung festlegt, hat sich der EuGH im Urteil zur Nichtigkeitsklage von Irland nur sehr kurz befasst. Zwar hat der EuGH bezüglich der Wahl der Rechtsgrundlage eines gemeinschaftlichen Rechtsakts zurecht betont, dass sie *„sich nach ständiger Rechtsprechung des Gerichtshofs auf objektive, gerichtlich nachprüfbare Umstände gründen, zu denen insbesondere das Ziel und der Inhalt des Rechtsakts gehören“* muss.[362] Aber er hat nicht beurteilt, ob und inwiefern die Wahl der Rechtsgrundlage für die fragliche Regelung im Hinblick auf Ziel und Inhalt rechtmäßig ist. Vielmehr hat er sich ohne Weiteres auf Binnenmarktkompetenz an sich konzentriert.[363]

In Bezug auf Zweck der fraglichen Regelung hat der EuGH verneint, dass die geregelten Maßnahmen die Strafverfolgung betreffen. Die Richtlinie regele vielmehr *„Tätigkeiten, die unabhängig von der Durchführung jeder eventuellen Maßnahme polizeilicher oder justizieller Zusammenarbeit in Strafsachen sind.“*[364] Den materiellen Gehalt der fraglichen Regelung stelle die wirtschaftliche Tätigkeit der Diensteanbieter dar und die Richtlinie betreffe in überwiegendem Maß das Funktionieren des Binnenmarkts.[365] Der Entstehungsgeschichte der Vorratsdatenspeicherung ist zu entnehmen, dass diese Maßnahme in erster Linie als ein Instrument der Strafverfolgung und Gefahrenabwehr gedacht ist. Die Richtlinie habe nichts anderes harmonisiert als die Speicherungspflicht der Diensteanbieter, damit die Vorratsdaten bei Bedarf der zuständigen Behörde in den Mitgliedstaaten zur Verfügung stehen. Das Argument des EuGH, dass Gehalt und Zweck der Richtlinie nicht auf Strafverfolgung gerichtet sind, kann insoweit nur bedingt überzeugen.

---

362 EuGH Urt. V. 10.2.2009, C-301/06, Rn. 60.

363 Vgl. *Terhechte*, EuZW 2009, 199 (203); *Braum*, ZRP 2009, 174 (174f.); *Szuba*, S. 79.

364 EuGH Urt. v. 10.2.2009, C-301/06, Rn. 82, 83.

365 EuGH Urt. v. 10.2.2009, C-301/06, Rn. 84, 85.

Seit der Vertrag von Lissabon in Kraft getreten ist, ist der Streit um die Rechtsgrundlage der Richtlinie allerdings nicht mehr virulent, da die damalige dritte Säule „Polizeiliche und justizielle Zusammenarbeit in Strafsachen" in den Vertrag über die Arbeitsweise der Europäischen Union (AEUV) integriert wurde. Die zur damaligen dritten Säule gehörenden Regelungsgegenstände können heute durch eine Richtlinie geregelt werden.[366] Die Kompetenzfrage der Richtlinie zur Vorratsdatenspeicherung wird somit vermieden. Für zukünftige Rechtsakte ist ein vergleichbares Problem auch nicht gegeben.

II. Vereinbarkeit der Vorratsdatenspeicherung mit den europäischen Grundrechten

Anlässlich der Nichtigkeitsklage am 6. Juni 2006 ist der EuGH nur auf die Rechtsetzungskompetenz der Richtlinie eingegangen. Fragen der materiellen Rechtmäßigkeit wurden nicht beantwortet. In der Literatur wurde vielfach angezweifelt, dass die Richtlinie mit den europäischen Grundrechten vereinbar sei.[367]

Seit dem Inkrafttreten des Vertrags von Lissabon ist der Grundrechtsschutz der EU neu strukturiert.[368] Vor allem hat die Grundrechtecharta der EU durch Anerkennung in Art. 6 Abs. 1 Vertrag über die Europäische Union (EUV) Rechtsverbindlichkeit erlangt. Sie steht damit im Primärrechtsrang und gilt als unmittelbare Rechtsquelle für den europäischen Grundrechtsschutz. Unter anderem tritt die Union nach Art. 6 Abs. 2 EUV der EMRK bei. Die Grundrechte, wie sie in der EMRK gewährleistet sind, sind nach Art. 6 Abs. 3 EUV als allgemeine Grundsätze Teil des Unionrechts. Die EMRK gilt also als eine *„Rechtserkenntnisquelle"* statt einer Rechtsquelle, da Rechtsquellen unmittelbar geltendes Recht darstellen würden, während Rechtserkenntnisquellen Grundlagen des Rechts darstellen und ihnen eine Orientierungsfunktion für

366 *Gundel*, in: *Ehlers* (Hrsg.), 2014, S. 839, Rn. 1, S. 862 Rn. 44; *Schwarze*, in: *Schwarze*/*Becker*/*Hatje*/*Schoo* (Hrsg.), 2012, Einführung, Rn. 48; *Hatje*/*Kindt*, NJW 2008, 1761 (1763); *Weber*, EuZW 2008, 7 (13), siehe auch *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 87; *Szuba*, S. 84.

367 Dazu siehe beispielhaft *Zöller*, GA 2007, 393 (411); *Gercke*, MMR 2008, 291 (293); *Westphal*, EuZW 2006, 555 (558); *Gola*/*Klug*/*Reif*, NJW 2007, 2599 (2599); *Leutheusser-Schnarrenberger*, ZPR 2007, 9 (10); *Bizer*, DuD 2007, 586 (587); *Petri*, DuD 2011, 607 (609 f.).

368 Dazu siehe *Ehlers*, in: *Ehlers* (Hrsg.) 2014, S. 37 Rn. 21 ff.; *Schwarze*, in: *Schwarze*/*Becker*/*Hatje*/*Schoo* (Hrsg.), 2012, Art. 19, Rn. 26; *Calliess*, in: *Calliess*/*Ruffert* (Hrsg.), 2016, EU-GRCharta Art. 1, Rn. 1; *Jarass*, GRCh 2016, Einleitung, Rn. 2-3; *Pache*/*Rösch*, NVwZ 2008, 473 (474 ff.); *Hatje/Kindt*, NJW 2008, 1761 (1766 f.); *Pache*/*Rösch*, EuR 2009, 769 (771 ff.); *Schroeder*, EuZW 2011, 462 (463 ff.); *Weiß*, EuZW 2013, 287 (287 f.).

die Auslegung einer Rechtsquelle zukommt.[369] Die Einwirkung der EMRK auf das EU-Recht wird jedoch dadurch gewährleistet, dass einerseits nach Art. 52 Abs. 3 GRCh die Rechte in der GRCh, die den durch die EMRK und die Grundfreiheiten garantierten Rechten entsprechen, die gleiche Bedeutung und Tragweite haben, wie sie ihnen in der genannten Konvention verliehen wird.[370] Andererseits darf keine Bestimmung in der Charta nach Art. 53 GRCh als eine Einschränkung oder Verletzung der Menschenrechte und Grundfreiheiten in der EMRK ausgelegt werden.[371] Die EMRK ist die wichtigste Rechtserkenntnisquelle des europäischen Grundrechtsschutzes.[372] Eine andere Rechtserkenntnisquelle der europäischen Grundrechte nach Art. 6 Abs. 3 GRCh stellt die gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten dar.

Die neu systematisierte rechtliche Grundlage liefert eigenen Grundrechtsschutz mit drei Schichten in der EU. Im Vergleich zur alten Rechtlage wird der Grundrechtsschutz in der EU durch die Verankerung der Grundrechtecharta im Primärrecht und die Bekräftigung der Einwirkung der EMRK verstärkt.[373] Die Richtlinie zur Vorratsdatenspeicherung war hieran zu messen.

1. Relevanz der europäischen Grundrechte

a) Art. 7 GRCh und Art. 8 Abs. 1 EMRK

Prüfungsmaßstab der Richtlinie zur Vorratsdatenspeicherung ist vor allem der Schutz des Privat- und Familienlebens nach Art.7 GRCh sowie Art. 8 Abs. 1 EMRK.

Das Recht auf Achtung des Privat- und Familienlebens wird in Art. 8 Abs. 1 EMRK festgelegt. In Art. 7 GRCh wird es übernommen. Die beiden Grundrechte haben nach Feststellung aus Art. 52 Abs. 3 GRCh identische Bedeutung und gleiche Tragweite.[374] Unter den Schutzbereich dieses Rechts fallen

---

[369] *Jarass*, GRCh 2016, Einleitung Rn. 1. Ausführlich zu EMRK als eine Rechtserkenntnisquelle der Grundrechte der EU sowie Unterschiede zwischen Rechtsquellen und Rechtserkenntnisquellen siehe auch *Ehlers*, in: *Ehlers* (Hrsg.) 2014, S. 36 Rn. 20 ff.; *Kingreen*, in: *Calliess*/*Ruffert* (Hrsg.) 2016, Art. 6 EUV Rn. 6 ff.

[370] Siehe auch *Ehlers*, in: *Ehlers* (Hrsg.) 2014, S. 37 Rn.22.

[371] Siehe auch *Ehlers*, in: *Ehlers* (Hrsg.) 2014, S. 37 Rn.22.

[372] *Kingreen*, in: *Calliess*/*Ruffert* (Hrsg.) 2016, Art. 6 EUV Rn. 7.

[373] Vgl. *Schroeder*, EuZW 2011, 462 (463f.).

[374] Siehe auch *Jarass*, GRCh 2016, Art. 7 Rn.1; *Bernsdorff*, in: *Meyer* (Hrsg.), GRCh 2014, Art. 7 Rn. 1; *Knecht*, in: *Schwarze*/*Becker*/*Hatje*/*Schoo* (Hrsg.), 2012, Art. 7

vier Teilbereiche und zwar das Privatleben, Familienleben, die Wohnung sowie die Kommunikation.[375] Diese vier Ausprägungen sind nicht klar voneinander zu trennen, sondern überschneiden sich und stellen die wichtigsten Einzelaspekte der Privatsphäre dar,[376] die angesichts der Entwicklung moderner Technologie zunehmend bedroht werden.[377] Zwar werde den Verpflichteten in Art. 7 GRCh wörtlich nur Achtungspflicht auferlegt, aber die Verpflichteten sollen nicht nur das Recht der Bürger achten, sondern auch Eingriffe in dieses Recht unterlassen und durch Gesetzgebung, Verwaltung sowie Rechtsprechung aktiv schützen.[378]

In Bezug auf die Richtlinie zur Vorratsdatenspeicherung wird der Teilbereich der Kommunikation betroffen. Anders als der Art. 8 EMRK, der von *„Korrespondenz"* spricht, wird Art. 7 GRCh das Wort *„Kommunikation"* verwendet. Dieser meint die *„vermittelte Kommunikation"*[379], die durch Dritte übermittelt wird und deswegen in größerem Maße dem Risiko von Eingriffen aussetzt ist.[380] Jedoch soll die in Art. 7 GRCh geregelte Kommunikation nicht auf vermittelte Kommunikation beschränkt werden, sondern für alle jetzigen Kommunikationsmöglichkeiten und künftigen technologischen Entwicklungen offenbleiben.[381] Das Recht des Schutzes der Kommunikation gewährleistet die Vertraulichkeit der Kommunikationsvorgänge natürlicher Personen. Dadurch sind die Kommunikationsvorgänge vor der willkürlichen Kenntnis des Staates in Bezug auf Inhalte oder Umstände der Kommunikation geschützt.[382] So stellt jede Überwachung, jedes Abhören sowie die Verhinderung der Übermittlung und Veränderung der Kommunikationsinhalte[383] durch die Union und ihre Organe sowie im Rahmen der Durchführung des

---

Rn. 1.

375 *Jarass*, GRCh 2016, Art. 7 Rn. 3 ff.; *Augsberg*, in: *von der Groeben*/*Schwarze*/*Hatje* (Hrsg.), 2015, GRCh Art. 7 Rn. 5 ff.; *Kingreen*, in: *Calliess*/*Ruffert* (Hrsg.), 2016, GRCh Art. 7 Rn. 3 ff.

376 Vgl. *Bernsdorff*, in: *Meyer* (Hrsg.), GRCh 2014, Art. 7 Rn. 1.

377 Vgl. *Jarass*, GRCh 2016, Art. 7 Rn. 3; *Bernsdorff*, in: *Meyer* (Hrsg.), GRCh 2014, Art. 7 Rn. 1.

378 *Bernsdorff*, in: *Meyer* (Hrsg.), GRCh 2014, Art. 7 Rn. 16; *Augsberg*, in: *von der Groeben*/*Schwarze*/*Hatje* (Hrsg.), 2015, GRCh Art. 7 Rn. 4.

379 *Jarass*, GRCh 2016, Art. 7 Rn. 25; *Augsberg*, in: *von der Groeben*/*Schwarze*/*Hatje* (Hrsg.), 2015, GRCh Art. 7 Rn. 9.

380 *Jarass*, GRCh 2016, Art. 7 Rn. 25; *Bernsdorff*, in: *Meyer* (Hrsg.), GRCh 2014, Art. 7 Rn. 24.

381 *Bernsdorff*, in: *Meyer* (Hrsg.), GRCh 2014, Art. 7 Rn. 24.

382 *Schorkopf*, in: *Ehlers* (Hrsg.) 2014, S. 611 Rn. 25; *Jarass*, GRCh 2016, Art. 7 Rn. 31; *Augsberg*, in: *von der Groeben*/*Schwarze*/*Hatje* (Hrsg.), 2015, GRCh Art. 7 Rn. 11; *Meyer-Ladewig*/*Nettesheim*, in: *Meyer-Ladewig*/*Nettesheim*/*von Raumer* (Hrsg.), EMRK 2017, Art. Rn. 94.

383 *Jarass*, GRCh 2016, Art. 7 Rn. 31; *Kingreen*, in: *Calliess*/*Ruffert* (Hrsg.), 2016, GRCh Art. 7 Rn. 13; *Knecht*, in: *Schwarze*/*Becker*/*Hatje*/*Schoo* (Hrsg.), 2012, Art. 7 Rn. 10.

Unionrechts durch die Mitgliedstaaten und ihre Organe[384] einen Eingriff in das Recht dar.

Nach den Vorgaben der Richtlinie waren die Mitgliedstaaten verpflichtet, die Regelungen der Mindestspeicherungspflicht zu harmonisieren. Die Telekommunikationsdaten mussten gemäß Art. 5 VDS-RL mindestens sechs Monate und höchstens zwei Jahre auf Vorrat gespeichert werden und bei Bedarf für den Abruf sowie für die Verwendung von zuständigen staatlichen Behörden zur Verfügung stehen. Demgemäß konnten die Telekommunikationsdaten aller EU-Bürger bis zu zwei Jahre ohne Anlass und unabhängig von einem konkreten Verdacht von den Telekommunikationsdiensteanbietern protokolliert werden. Die Privatheit sowie die Vertraulichkeit der Telekommunikationsvorgänge der Bürger werden durch eine solche Regelung beeinträchtigt, da die zu speichernden Daten die Umstände der Telekommunikationsvorgänge betreffen. Betroffen ist insbesondere das Recht des Schutzes der Kommunikation aus Art. 7 GRCh.

Spezielle Möglichkeiten zur Einschränkung des Rechts des Schutzes der Kommunikation enthält der Art. 7 GRCh nicht. Somit gilt die allgemeine Schrankenregelung nach Art. 52 Abs. 1 GRCh. Demgemäß sind Einschränkungen des Grundrechts durch Gesetz möglich. Sie dürfen nur vorgenommen werden, wenn sie den Wesensgehalt des Grundrechts achten und den Grundsatz der Verhältnismäßigkeit wahren. Die Einschränkungen sind verhältnismäßig, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen. Außerdem werden *„die speziellen Anforderungen"*[385] für Einschränkung dieses Rechts in Art. 8 Abs. 2 EMRK festgelegt, wonach in das Recht nur eingegriffen werden darf, wenn der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer. Darüber hinaus kommt der Kommunikation mit Rechtsanwälten besonderer Schutz zu.[386]

---

384 *Augsberg*, in: *von der Groeben*/*Schwarze*/*Hatje* (Hrsg.), 2015, GRCh Art. 7 Rn. 11.

385 *Augsberg*, in: *von der Groeben*/*Schwarze*/*Hatje* (Hrsg.), 2015, GRCh Art. 7 Rn. 13.

386 EGMR, Nr.59304/00 v. 24.2.2005, Rn. 22; siehe auch *Jarass*, GRCh 2016, Art. 7 Rn. 46.

Außerdem ist dem Recht auf Achtung des Privat- und Familienlebens in Art. 8 EMRK auch die datenschutzrechtliche Anforderung zu entnehmen, dass wirksame Vorkehrungen gegen Datenmissbrauch bei Datensammlungen, die das Privatleben betreffen, zu treffen sind.[387] Bei der Vorratsspeicherung ist somit erforderlich, angemessene Maßnahmen zu erlassen, um Datenenthüllung und -missbrauch vorzubeugen.

Nach dem Maßstab aus Art. 52 Abs. 1 GRCh und Art. 8 Abs. 2 EMRK darf die Vorratsdatenspeicherung zur Verhütung von Straftaten und zum Schutz der öffentlichen Sicherheit durchgeführt werden, wenn sie verhältnismäßig ist und den Wesensgehalt des Rechts aus Art. 7 GRCh nicht berührt. Zudem muss sie gesetzlich ausreichend bestimmt sein. Das heißt, dass der Speicherungsumfang, die Speicherungsdauer, die befugte Behörde, die Voraussetzung zum Abruf sowie Verwendung klar und präzise geregelt werden muss.

b) Art. 8 GRCh

Nach Art. 8 GRCh hat jeder das Recht auf Schutz seiner personenbezogenen Daten. In der Informationsgesellschaft kommt dem Schutz personenbezogener Daten aus Art. 8 GRCh elementare Bedeutung zu.[388] Somit wird das Recht auf Datenschutz ausdrücklich als eigenständiges europäisches Grundrecht festgestellt. Zudem findet sich dessen Schutz in Art. 16 AEUV und wurde sekundärrechtlich zunächst durch die Richtlinien 95/46/EG (Datenschutzrichtlinie) und 2002/58/EG konkretisiert.[389] Mit dem Inkrafttreten der Verordnung 2016/679 (Datenschutz-Grundverordnung) vom 25. Mai 2018 wurde die Datenschutzrichtlinie abgelöst. Der europäische Datenschutzrechtstandard wird wegen der unmittelbaren Geltung der Verordnung in größtem Umfang harmonisiert.[390]

Von zentraler Bedeutung ist die Definition des Begriffs der personenbezogenen Daten bei der Absteckung des Schutzbereichs von Art. 8 GRCh. Unter personenbezogene Daten fallen alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Hier kommt es nicht darauf an, ob diese In-

---

387 *Meyer-Ladewig/Nettesheim*, in: *Meyer-Ladewig*/*Nettesheim*/*von Raumer* (Hrsg.), EMRK 2017, Art. 8 Rn. 32.

388 Siehe *Jarass*, GRCh 2016, Art. 8 Rn. 2; *Kingreen*, in: *Calliess*/*Ruffert* (Hrsg.), 2016, GRCh Art. 8 Rn. 1.

389 Siehe *Schorkopf*, in: *Ehlers* (Hrsg.) 2014, S. 617 Rn. 40; *Jarass*, GRCh 2016, Art. 8 Rn. 2, 4a; *Augsberg*, in: *von der Groeben*/*Schwarze*/*Hatje* (Hrsg.), 2015, GRCh Art. 8 Rn. 1; *Knecht*, in: *Schwarze*/*Becker*/*Hatje*/*Schoo* (Hrsg.), 2012, Art. 8 Rn. 1.

390 *Albrecht*/*Jotzo*, Teil 1 Rn. 25; *Kühling*/*Raab*, in: *Kühling*/*Buchner* (Hrsg.), DSGO/BDSG 2018, Einführung, Rn. 1.

formationen sensibel sind oder sich auf Privatsphäre beziehen oder nicht.[391] Im Rahmen von Art. 8 GRCh ist jede Verarbeitung personenbezogener Daten relevant. Das Recht schützt den Bürger vor jeder unbefugten Sammlung, Speicherung, Veränderung, Übermittlung und Verwendung personenbezogener Daten. Nach Art. 8 Abs. 2 GRCh dürfen personenbezogene Daten nur mit Einwilligung der Betroffene oder aufgrund einer gesetzlichen Grundlage verarbeitet werden. Die Verarbeitung ist nach Treu und Glauben für festgelegte legitime Zwecke durchzuführen. Unter anderem ist der Transparenzgrundsatz zu wahren. So hat der Betroffene das Recht, Auskunft über die Verarbeitung seiner Daten zu erhalten und die Berichtigung der Daten zu erwirken.[392] Die Wesensgehaltsgarantie und das Verhältnismäßigkeitsprinzip in Art. 52 Abs. 1 GRCh sind außerdem bei jeder Verarbeitung einzuhalten.[393] Die Einhaltung des Grundrechts muss nach Art. 8 Abs. 3 GRCh von einer unabhängigen Stelle überwacht werden.

Demgemäß darf die Vorratsspeicherung von Telekommunikationsdaten nur im Falle einer gesetzlichen Grundlage und für legitime Zwecke zugelassen werden. Die Speicherung und spätere Verwendung der Vorratsdaten müssen die Grundsätze des Datenschutzes wie Zweckbestimmung, Zweckbindung, Erforderlichkeit, Transparenz sowie wirksamen Rechtsschutz einhalten. Effektive Maßnahmen der Datensicherheit sowie des Datenschutzes sind zu treffen, um Datenenthüllung sowie -missbrauch vorzubeugen. Der Wesensgehalt des Art. 8 GRCh muss dadurch gewahrt werden, dass die Vorratsspeicherung keine totale Registrierung der personenbezogenen Daten aller Bürger nach sich zieht. Die förderliche Wirkung der Vorratsdatenspeicherung für die öffentliche Sicherheit und die Beeinträchtigung des Rechts auf den Schutz personenbezogener Daten darf nicht außer Verhältnis zueinander stehen. Die Einhaltung dieser Anforderungen muss von einer unabhängigen Stelle kontrolliert werden.

Da die Herrschaft über die eigenen personenbezogenen Daten ein elementarer Aspekt der Privatsphäre ist, ist Art. 8 als *lex specialis* zu Art. 7 GRCh anzu-

---

391 Siehe *Kingreen*, in: *Calliess*/*Ruffert* (Hrsg.), 2016, GRCh Art. 8 Rn. 9; *Augsberg*, in: *von der Groeben*/*Schwarze*/*Hatje* (Hrsg.), 2015, GRCh Art. 8 Rn. 6; *Knecht*, in: *Schwarze*/*Becker*/*Hatje*/*Schoo* (Hrsg.), 2012, Art. 8 Rn. 5; *Bernsdorff*, in: *Meyer* (Hrsg.), GRCh 2014, Art. 8 Rn. 15; *Jarass*, GRCh 2016, Art. 8 Rn. 5, 6.

392 Siehe auch *Kingreen*, in: *Calliess*/*Ruffert* (Hrsg.), 2016, GRCh Art. 8 Rn. 14 ff.; *Jarass*, GRCh 2016, Art. 8 Rn. 11 ff.; *Augsberg*, in: *von der Groeben*/*Schwarze*/*Hatje* (Hrsg.), 2015, GRCh Art. 8 Rn. 12; *Knecht*, in: *Schwarze*/*Becker*/*Hatje*/*Schoo* (Hrsg.), 2012, Art. 8 Rn. 7 ff.

393 *Augsberg*, in: *von der Groeben*/*Schwarze*/*Hatje* (Hrsg.), 2015, GRCh Art. 8 Rn. 13; *Jarass*, GRCh 2016, Art. 8 Rn. 12a ff.

sehen.[394] Wenn personenbezogene Daten verarbeitet werden, die sich auf das Privatleben der Betroffenen beziehen, sind sowohl Art. 7 als auch Art. 8 GRCh relevant.[395] Bei der Vorratsdatenspeicherung sind Telekommunikationsdaten der Bürger für einen bestimmten Zeitraum zu speichern und später bei Bedarf von befugten Behörden abzurufen und zu verwenden. Damit handelt es sich bei der Vorratsdatenspeicherung um eine Verarbeitung personenbezogener Daten, die sich auf die Telekommunikation der Bürger bezieht, die einen wichtigen Teil des Privatlebens darstellt. Die Ausgestaltung der Richtlinie muss die beiden Grundrechte angemessen berücksichtigen, um verfassungskonform zu sein.

2. Das endgültige Urteil des EuGH am 8.4.2014 zur Richtlinie der Vorratsdatenspeicherung

Der Streit über die Vorratsdatenspeicherung wurde nicht durch das Urteil des BVerfG beendet. Einerseits war Deutschland damals immer noch verpflichtet, die Richtlinie zur Vorratsdatenspeicherung umzusetzen oder Deutschland drohte ein Bußgeld wegen der Vertragsverletzung. Andererseits wurden die Vorgaben der Vorratsdatenspeicherung zwar vom BVerfG für nichtig erklärt, auch wenn eine Speicherung der Telekommunikationsdaten auf Vorrat verfassungsrechtlich nicht schlechthin verboten ist.[396] Anders als eine von vornherein verbotene Datensammlung auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken könne eine Vorratsdatenspeicherung der Telekommunikationsverbindungsdaten mit einer, dem Eingriff adäquaten gesetzlichen Ausgestaltung vielmehr den Verhältnismäßigkeitsanforderungen genügen.[397] Das BVerfG hat im Urteil die Verfassungsmäßigkeit der Vorratsdatenspeicherung überprüft und gleichzeitig für eine neue Umsetzung der Vorratsdatenspeicherung konkrete und strenge Anforderungen formuliert.[398]

Wegen des Hinweises des BVerfG wurde häufig über die Verfassungsmäßigkeit der Vorratsdatenspeicherung in der Hinsicht diskutiert, dass eine grundrechtsmäßige Vorratsdatenspeicherung wohl möglich wäre, und wie sie danach konkret ausgestaltet werden könnte.[399] Jedoch wurde die Richtlinie zur

394 *Augsberg*, in: *von der Groeben*/*Schwarze*/*Hatje* (Hrsg.), 2015, GRCh Art. 8 Rn. 1; *Kingreen*, in: *Calliess*/*Ruffert* (Hrsg.), 2016, GRCh Art. 8 Rn. 1a; *Bernsdorff*, in: *Meyer* (Hrsg.), GRCh 2014, Art. 8 Rn. 13.

395 *Jarass*, GRCh 2016, Art. 8 Rn. 4.

396 BVerfGE 125, 260 (321).

397 BVerfGE 125, 260 (321).

398 BVerfGE 125, 260 (325 ff.).

399 Siehe auch *Leutheusser-Schnarrenberger*, DuD 2014, 589 (591). Untersuchung und Vorschlag über neue Vorratsdatenspeicherung vor dem endgültigen Urteil vom

Vorratsdatenspeicherung schließlich am 8 April 2014 vom EuGH für unvereinbar mit Art. 7 und 8 GRCh erklärt.[400] Ohne europarechtliche Grundlage müssen Mitgliedstaaten die Richtlinie zur Vorratsdatenspeicherung nicht mehr in nationales Gesetz umsetzen. Eine unterschiedslose und anlasslose Vorratsdatenspeicherung ist mit dem europäischen Grundrecht nicht vereinbar und eine derartige Vorratsspeicherung ist nicht mehr zulässig.

Der EuGH hat sich mit der lange diskutierten materiellen Rechtmäßigkeit der Richtlinie zur Vorratsdatenspeicherung auseinandergesetzt: ob die Richtlinie mit Art. 7 GRCh und Art. 8 GRCh vereinbar ist. Im Ganzen ist die Überprüfung im Urteil übereinstimmend mit dem BVerfG dreiteilig gegliedert und betrifft die Relevanz der betroffenen Grundrechte, der Eingriff in die Rechte und die Rechtfertigung des Eingriffs. Die Rechtfertigung des Eingriffs ist nach Art. 52 GRCh noch in drei Teile, und zwar die Unantastbarkeit des Wesensgehalts, dem Gemeinwohl dienenden Zielsetzungen und die Wahrung des Grundsatzes der Verhältnismäßigkeit unterteilt. Gemäß den Ausführungen im Rahmen der Verhältnismäßigkeit ist der Eingriff gerechtfertigt, wenn er zur Erreichung der verfolgten Ziele geeignet sind und nicht dessen Grenzen überschreite, was zur Erreichung dieser Ziele geeignet und erforderlich ist.[401]

a) Vorliegen des Eingriffs in Art. 7 und 8 GRCh

Nach den Vorgaben der Richtlinie 2006/24/EG sollen die Vorschriften der Mitgliedstaaten der Vorratsdatenspeicherung harmonisiert werden. Nach Art. 5 VDS-RL sollen bestimmte Telekommunikationsverbindungsdaten von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste gespeichert werden, um sicherzustellen, dass die Vorratsdaten bei Bedarf (Strafverfolgung) den zuständigen Behörden zur Verfügung stehen. Bei den zu speichernden Daten handelte es sich um die zur Identifizierung der Quelle der Nachricht sowie zur Bestimmung von Datum, Uhrzeit, Dauer und Art der Nachrichtenübermittlung, der Endeinrichtung von Benutzern und des Standorts mobiler Geräte benötigten Daten.[402] Aus denen könne sich insbesondere ergeben, wer wann, auf welchem Weg, mit welcher Person, wie lange und

EuGH siehe zum Beispiel *Roßnagel*/*Moser-Knierim*/*Schweda*, Interessenausgleich; *Schramm*/*Wegener*, MMR 2011, 9; *Ziebarth*, DuD 2009, 25; *Roßnagel*/*Bedner*/*Knopp*, DuD 2009, 536; *Petri*, in: *Roßnagel* (Hrsg.), S.123 ff.

400 EuGH, Urteil in Rechtssachen C-293/12 und C-594/12 v. 08.04.2014. Anmerkung dazu siehe *Durner*, DVBI 2014, 712; *Indra*, JZ 2014, 1109; *Classen*, EuR 2014, 441; *Petri*, ZD 2014, 296; *Wolff*, DÖV 2014, 608.

401 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 46.

402 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 26.

unter anderem wie häufig kommuniziert habe.[403] Die Speicherung dieser Verkehrsdaten betreffe die Kommunikationsvorgänge der Nutzer und damit unmittelbar und speziell das Privatleben.[404] Zudem beziehe die Vorratsdatenspeicherung sich auf eine Verarbeitung personenbezogener Daten im Sinne des Art. 8 GRCh. Deshalb sind Art. 7 und 8 GRCh in diesem Fall relevant.[405]

Nach dem EuGH werde die von der Richtlinie 2002/58/EG geregelte Löschungs- sowie Anonymisierungspflicht der Telekommunikationsdienstanbieter, die der Gewährleistung der Vertraulichkeit der Telekommunikation dient, nicht erfüllt.[406] Vielmehr müssen die Verkehrsdaten nach der Richtlinie auf Vorrat während eines bestimmten Zeitraums gespeichert werden. Die Verkehrsdaten betreffen die Telekommunikationsvorgänge der Nutzer und könnten das Privatleben einer Person bis ins Detail abbilden, womit die Vorratsdatenspeicherung einen Eingriff in das Recht auf Achtung der Privatsphäre darstelle.[407] Irrelevant sei, ob die betreffenden Informationen über das Privatleben sensiblen Charakter hätten oder ob die Betroffenen durch den Eingriff Nachteile erlitten haben könnten.[408] Ferner stelle der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten einen zusätzlichen Eingriff in Art. 7 GRCh dar.[409] Schließlich greife die Vorratsdatenspeicherung in das Recht auf Schutz personenbezogener Daten dadurch ein, dass sie eine Verarbeitung personenbezogener Daten vorsehe.[410] Der EuGH hat hierbei die Betroffenheit beider Grundrechte klar ausgeführt und den Eingriff der Richtlinie in die beiden Grundrechte bejaht.

b) Rechtfertigung des Eingriffs

Zur Prüfung der Rechtfertigung des Eingriffs zieht der EuGH Art. 52 Abs. 1 GRCh heran, der einen allgemeinen gesetzlichen Vorbehalt enthält, dass jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen werden und der Wesensgehalt dieser Rechte und Freiheiten geachtet werden muss.[411] Unter Wahrung des Verhältnismä-

403 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 26.
404 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 29.
405 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 29.
406 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 32.
407 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 34.
408 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 33.
409 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 35.
410 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 36.
411 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 38; *Ehlers*, in: *Ehlers* (Hrsg.) 2014, S. 564 Rn. 99; *Jarass*, GRCh 2016, Art. 52 Rn. 19.

ßigkeitsgrundsatzes dürften Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.[412]

c) Unantastbarkeit des Wesensgehalts

Der Wesensgehalt des Art. 7 GRCh werde angetastet, wenn die *Inhalte* der Telekommunikation generell einer Behörde zugänglich gemacht würden.[413] Das ist in der Richtlinie zur Vorratsdatenspeicherung nicht der Fall. Wie das BVerfG argumentiert auch der EuGH, dass gemäß Art. 1 Abs. 2 VDS-RL die Speicherung der *Inhalts*daten der Telekommunikationsvorgänge ausgeschlossen werde. Damit habe die Vorratsdatenspeicherung den Wesensgehalt des Rechts auf Achtung des Privatlebens nicht angetastet.[414]

Wie oben bereits analysiert ist die These unter heutigen informationstechnischen Bedingungen jedoch nicht mehr zutreffend, dass Inhaltsdaten unbedingt aussagekräftiger als Verkehrsdaten der Telekommunikation sind und Verkehrsdaten somit ohne weiteres weniger schutzwürdig sind als Inhaltsdaten.[415] Angesichts der Verwendungs- und Verknüpfungsmöglichkeit der Verkehrsdaten können genaue oder sogar genauere Persönlichkeits- oder Bewegungsprofile unabhängig von der Kenntnisnahme des Inhalts erstellt werden. Im Einzelfall können die Verkehrsdaten sogar aussagkräftiger als Inhaltsdaten sein.[416] An der Tatsache, dass Verkehrsdaten für Strafverfolgungsbehörden zunehmend interessant werden, [417] lässt sich erkennen, dass viele persönliche Informationen aus den Verkehrsdaten – allein oder verbunden mit anderen Daten – gezogen werden können.

Ferner ist die Abgrenzung zwischen Inhalts- und Verkehrsdaten insbesondere im Bereich des Internets zunehmend undeutlich geworden.[418] In vielen Fällen kann die Kenntnisnahme der Inhalte der Telekommunikation durchaus

---

412 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 38; *Jarass*, GRCh 2016, Art. 52 Rn. 34 f.; *Terhechte*, in: *Groeben*/*Schwarze*/*Hatje* (Hrsg.), Europäisches Unionrecht 2015, Art. 52 Rn. 8 f.

413 *Jarass*, GRCh 2016, Art. 7 Rn. 35.

414 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 39.

415 Siehe oben die Erläuterung der Angemessenheit Kapitel 2, B.I.3.c) dd); siehe auch *Dix*/*Kipker*/*Schaar*, ZD 2015, 300 (302).

416 Vgl. *Dix*/*Schaar*, in: Jahrbuch 2014, S. 19; *Dix*/*Kipker*/*Schaar*, ZD 2015, 300 (302).

417 Vgl. *Breyer*, S. 213.

418 Siehe auch *Breyer*, S. 214; *Dix*/*Schaar*, in: Jahrbuch 2014, S. 20; *Bock*/*Engeler*, DVBI 2016, 593 (595); *Freiling*, Technischer Bericht TR-2009-005, S. 22.

mittels der Verkehrsdaten verwirklicht werden.[419] Unter diesen Umständen kann eine Vorratsspeicherung der Verkehrsdaten nichts anders als eine Vorratsspeicherung der Inhaltsdaten sein.[420] Noch zu bedenken ist, dass Berufsgeheimnisträger von der Maßnahme nicht weniger Nachteile als durch eine Speicherung der Inhalte erleiden können.[421] Es ist somit sehr fragwürdig, ob der Wesensgehalt des Grundrechts auf Achtung des Privatlebens trotz Ausschluss der Inhaltsspeicherung noch gewahrt werden kann.

Im Ergebnis hat EuGH festgestellt, dass die Vorratsdatenspeicherung den Wesensgehalt des Rechts auf Schutz personenbezogener Daten aus dem Grund nicht antastet, weil Anforderungen an Datenschutz und Datensicherheit im Art. 7 der Richtlinie vorgesehen waren.[422]

d) Gemeinwohl dienende Zielsetzung

Eine dem Gemeinwohl dienende Zielsetzung der fraglichen Richtlinie hat der EuGH bejaht. Dabei hat er zwischen dem Ziel in den Vorschriften und dem materiellen Ziel der Richtlinie differenziert. Zwar werde das Ziel in Art. 1 Abs. 1 VDS-RL wörtlich als Harmonisierung der Vorschriften der Vorratsdatenspeicherung festgelegt, aber das materielle Ziel dieser Richtlinie bestehe darin, schwere Kriminalität durch die Verfügbarkeit von Daten effektiv zu bekämpfen und damit bessere öffentliche Sicherheit gewährleistet zu können. Damit verfolge die Richtlinie ein dem Gemeinwohl dienendes Ziel.[423]

In der Streitigkeit über die Rechtsgrundlage der Vorratsdatenspeicherungsrichtlinie im Jahr 2009 hat der EuGH die Begründung von Irland und der Slowakei ausdrücklich abgelehnt, dass das einzige Ziel oder das Hauptziel der Richtlinie die Kriminalitätsbekämpfung ist und im Vergleich dazu die Förderung des Funktionierens des Binnenmarkts als reines Nebenziel anzusehen ist.[424] Der materielle Gehalt der Richtlinie ist gemäß dem EuGH im Wesentlichen die Tätigkeit der Diensteanbieter im betroffenen Sektor des Binnenmarkts. Die Bestimmungen würden die Angleichung der nationalen Rechtsvorschriften bezüglich der Vorratsdatenspeicherung bezwecken.[425] Es ist zutreffend, dass das Hauptziel und das Nebenziel dieser Richtlinie zu un-

419 *Breyer*, S. 214 f; BVerfGE 125, 260 (342).
420 Siehe *Bock*/*Engeler*, DVBI 2016, 593 (595).
421 Siehe oben die Erläuterung der Nachteile der Vorratsdatenspeicherung zu den Berufsgeheimnisträgern.
422 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 40.
423 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 41-44.
424 EuGH, Rechtssachen C-301/06 v. 10.02.2009, Rn. 58, 59.
425 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 81, 84.

terscheiden sind, da die Vorratsdatenspeicherung sowohl auf die Kriminalitätsbekämpfung abzielt als auch durch Harmonisierung der entsprechenden Regelung tatsächlich auf den Binnenmarkt Wirkung ausübt. In einem jüngeren Urteil ist der EuGH auf diese Unterscheidung nicht mehr näher eingegangen. Stattdessen hat er zwischen dem wörtlichen Ziel und dem materiellen Ziel der Richtlinie differenziert.[426] Leider hat der EuGH nicht erklärt, nach welchen Kriterien das materielle Ziel zu bestimmen ist.

Angesichts der Geschichte der Richtlinie der Vorratsdatenspeicherung und auch ihres Inhalts an sich, hat sich die Richtlinie hauptsächlich auf die Kriminalitätsbekämpfung ausgerichtet. Die Vorratsdatenspeicherung wurde ursprünglich als ein Vorhaben vor dem Hintergrund der Verschärfung der Bedrohung durch Terrorismus und Schwerkriminalität behandelt.[427] Der Inhalt der Regelung hat sich auch wesentlich mit der Auferlegung der Speicherungs- und Übermittlungspflichten von Telekommunikationsdiensteanbietern befasst, damit die Strafverfolgung und Gefahrenabwehr effektiviert und die Sicherheit verbessert werden können. Deshalb ist eine dem Gemeinwohl dienende Zielsetzung der Richtlinie zur Vorratsdatenspeicherung ohne Problem zu bejahen.

e) Verhältnismäßigkeitsgrundsatz

Der Grundsatz der Verhältnismäßigkeit spielt im Rahmen der Rechtfertigung die zentrale Rolle.[428] Er wurde in den ständigen Rechtsprechungen als ein wesentlicher Grundsatz anerkannt und gilt über die Grundrechtscharta hinaus allgemein im Rahmen des Grundrechtsschutzes in der europäischen Union.[429] Der Verhältnismäßigkeitsgrundsatz verlangt, dass *„die Handlungen der Unionsorgane geeignet sind, die mit der fraglichen Regelung zulässigerweise verfolgten Ziele zu erreichen, und nicht die Grenzen dessen überschreiten, was zur Erreichung dieser Ziele geeignet und erforderlich ist.“*[430] Bei der Überprüfung dieses Grundsatzes im Fall der Vorratsdatenspeicherung hat der EuGH besonders hervorgehoben, dass die Richtlinie wegen der Eingriffsintensität und des Zusammenhangs zwischen Art. 7 und 8 GRCh strikt überprüft werden muss.[431] Damit wurde die Eingriffsintensität einer generellen Speicherung der Telekommunikationsdaten, die Erforderlichkeit einer strik-

426 Ähnlich wie *Ziebarth*, ZUM 2017, 398 (400 f.).
427 Siehe oben die Darstellung der Entstehungsgeschichte der Vorratsdatenspeicherung.
428 Vgl. *Ehlers*, in: *Ehlers* (Hrsg.) 2014, S. 570 Rn. 112.
429 *Ehlers*, in: *Ehlers* (Hrsg.) 2014, S. 570 Rn. 112.
430 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 46.
431 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 48.

ten Kontrolle dafür und der Zusammenhang zwischen dem Recht auf Schutz personenbezogener Daten und dem Recht auf Achtung des Privatlebens vom EuGH festgestellt.

Angesichts der wachsenden Bedeutung von Telekommunikationsverkehrsdaten für die Strafverfolgung wird die Vorratsdatenspeicherung vom EuGH als nützliches Mittel für die Ermittlung von Straftaten und damit geeignet zur Erreichung des Ziels der Richtlinie angesehen.[432] Zwar hat der EuGH den Zweck der Richtlinie als gemeinwohldienend bejaht, aber ob der Zweck auch bestimmt genug ist, hat der EuGH nicht behandelt. Das ist jedoch gemäß Art. 8 GRCh und auch gemäß Art. 5 Abs. 1 lit. b DSGVO von Bedeutung.[433]

Bei der Beurteilung der Erforderlichkeit der Vorratsdatenspeicherung hat der EuGH zu Recht betont, dass eine dem Gemeinwohl dienende Zielsetzung für sich genommen die Erforderlichkeit der Speicherungsmaßnahme für die Kriminalitätsbekämpfung nicht rechtfertigen könne.[434] Angesichts der besonderen Bedeutung des Schutzes personenbezogener Daten aus Art. 8 GRCh für das Recht auf Achtung des Privatlebens ist im Rahmen der Erforderlichkeit zu verlangen, dass sich die Ausnahmen von Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken müssten, um das Grundrecht auf Achtung des Privatlebens zu schützen.[435] Dafür müsse der Umfang und die Anwendung der Vorratsdatenspeicherung klar und genau geregelt werden. Ferner seien vorsorgliche Maßnahmen für gespeicherte Vorratsdaten gegen Datenmissbrauch und unberechtigte Datenabfrage oder Datennutzung zu treffen.[436] Solche Einschränkungen seien erforderlich, da der Eingriff der Vorratsdatenspeicherung wegen der umfassenden Streubreite der Speicherung,[437] der großen Wirkung auf das Alltagsleben,[438] der intensiven Aussagekraft der Telekommunikationsdaten[439] und der Undurchsichtigkeit der Zugriffe und Verwendung[440] besonders schwerwiegend sei – obwohl die Speicherung der Inhalte ausgeschlossen wurde.[441]

---

432 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 49.
433 Siehe *Schorkopf*, in: *Ehlers* (Hrsg.) 2014, S. 618 Rn. 43.
434 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 52.
435 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 52.
436 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 54.
437 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 56.
438 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 56.
439 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 27.
440 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 37.
441 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 28.

Zudem erzeuge die Ausgestaltung der Vorratsdatenspeicherung das Gefühl der ständigen Überwachung.[442]

Bei der Beurteilung, ob der Eingriff der Vorratsdatenspeicherung auf das absolut Notwendige beschränkt ist, hat der EuGH die Verdachtslosigkeit und Anlasslosigkeit der Vorratsdatenspeicherung als wesentliche Erwägungspunkte genannt. Alle Verkehrsdaten müssen unterschiedslos gespeichert werden, *„ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen*".[443] Die Speicherung gelte auch für Personen, bei denen keinerlei Anhaltspunkt dafür bestehe, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könne.[444] Die Achtung der Pflicht des Berufsgeheimnisses werde wegen dieser Ausnahmelosigkeit der Speicherung beeinträchtigt.[445] Zwischen den Vorratsdaten und einer Bedrohung der öffentlichen Sicherheit fehle der Zusammenhang und

„insbesondere beschränkt sie [d.i. die Richtlinie] die Vorratsdatenspeicherung 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."[446]

Eine derartige unterschiedslose und anlasslose Vorratsdatenspeicherung wurde somit nicht wirksam eingeschränkt.

Wie das BVerfG hat auch der EuGH die Regelungen zur Datensicherheit und Datenschutz der Vorratsdatenspeicherung als nicht hinreichend bestimmt kritisiert. Dass also die Vorkehrungen für Datenschutz der Vorratsdaten angesichts der großen Menge und des sensiblen Charakters nicht hinreichend klar und strikt vorgeschrieben worden seien.[447] Die besonders hohen technischen und organisatorischen Maßnahmen seien ebenso nicht sichergestellt. Insgesamt genüge sie den diesbezüglichen Anforderungen von Art. 8 der Charta nicht.[448]

---

442 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 37.
443 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 57.
444 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 58.
445 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 58.
446 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 59.
447 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 66.
448 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 66-67.

Über das BVerfG hinausgehend hat der EuGH noch folgende Erwägungen formuliert. Vor allem sei der Zugriff und die Verwendung nicht durch ein objektives Kriterium für *„schwere Straftaten"* eingeschränkt worden, das der Schwere des Eingriffs in die Grundrechte hinreichend Rechnung tragen könne.[449] Auch enthalte die Richtlinie keine materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang zu den Vorratsdaten, um Eingriffe auf das absolut Notwendige wirksam zu beschränken.[450] Dazu gehören insbesondere ein objektives Kriterium für die Zahl der befugten Personen zum Zugang der Vorratsdaten,[451] differenzierte Datenkategorien nach Maßgabe des Nutzens für ein geregeltes Ziel oder anhand der betroffenen Personen[452] und objektive Kriterien für die Feststellung der genauen Speicherungsfrist innerhalb von mindestens sechs bis höchstens 24 Monaten.[453] Nicht zuletzt werde der Speicherungsort auch nicht auf das Unionsgebiet beschränkt, was dazu führen könne, dass die Einhaltung der Anforderungen zur Datensicherheit und zum Datenschutz nicht durch eine unabhängige Kontrolle gewährleistet werde.[454] Somit wurde der Eingriff der Vorratsdatenspeicherung nicht auf das absolut Notwendige beschränkt.

Die Vereinbarkeit der Richtlinie mit dem Recht auf Freiheit der Meinungsäußerung in Art. 11 GRCh hat der EuGH nicht mehr geprüft, da die Grundrechtsmäßigkeit schon wegen Verstoßes gegen Art. 7 und 8 GRCh verneint wurde.[455] Dennoch hat der EuGH nicht ausgeschlossen, dass die Vorratsdatenspeicherung auch Auswirkungen auf die Nutzung von Telekommunikationsdiensten und damit auf die Ausübung der Meinungsfreiheit der Teilnehmer oder Benutzer habe.[456]

f) Zusammenfassung

Insgesamt hat der EuGH die materielle Rechtmäßigkeit der Richtlinie zur Vorratsdatenspeicherung verneint. Die besonders schwere Eingriffsintensität der Richtlinie in das Recht auf Achtung des Privatlebens und auf Schutz der personenbezogenen Daten hat der EuGH waren dafür ausschlaggebend. Ob-

449 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 60.
450 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 61.
451 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 62.
452 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 63.
453 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 64.
454 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 68.
455 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 70.
456 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 28.

wohl die Maßnahme ein dem Gemeinwohl dienendes Ziel verfolgt und sie auch geeignet ist, das legitime Ziel zu erreichen, wird die Vorratsspeicherung jedoch ohne Ausnahme insbesondere für Berufsgeheimnisträger und zudem anlasslos durchgeführt. Die Einschränkungen werden ferner nicht bestimmt genug formuliert. Die Beeinträchtigung durch die Vorratsdatenspeicherung wird nicht auf das absolut Notwendige beschränkt. Damit ist die Richtlinie zur Vorratsdatenspeicherung unverhältnismäßig und grundrechtswidrig. Dabei hat der EuGH ausführlich und intensiv dargelegt, welche Maßstäbe für künftige Regelungen zu beachten sind.[457]

Bei der Begründung hat der EuGH viele gemeinsame Standpunkte mit dem Bundesverfassungsgericht, insbesondere im Teil der Verhältnismäßigkeit.[458] Zum Beispiel hat der EuGH bei der Bestimmung der Eingriffsintensität die Aussagekraft von Verkehrsdaten festgestellt. Die Verletzung des Wesensgehalts vom Recht auf Achtung des Privatlebens wird auch vom EuGH verneint, weil die Inhalte der Telekommunikation von der Vorratsspeicherung ausgespart werden.[459] Bei der Analyse der Geeignetheit des Eingriffs hat er die dienende Funktion der Verkehrsdaten für Strafverfolgung und Gefahrenabwehr ebenfalls anerkannt. Ferner hat er bei der Abwägung die Datenschutz- und Datensicherheitsvorkehrungen als nicht hinreichend kritisiert.

Über oben genannten ähnlichen Erwägungen wie das BVerfG hinaus hat der EuGH noch andere Punkte beleuchtet. Etwa Telekommunikationsverkehrsdaten von Berufsgeheimnisträgern müssten wegen des sehr sensitiven Charakters von der Vorratsdatenspeicherung ausgenommen sein. Der EuGH gibt weitere Differenzierungskriterien vor: Es müsse danach differenziert werden, ob es eine mögliche Verbindung zu einer schweren Straftat gibt. In Abhängigkeit von verschiedenen Datenkategorien müsste jeweils eine bestimmte Speicherdauer vorgesehen sein. Eine anlasslose und allumfassende Speicherung sei jedenfalls nicht rechtmäßig.

---

457 Siehe auch *Classen*, EuR 2014, 441 (447); *Petri*, ZD 2014, 296 (301); *Kühling*, NVwZ 2014, 681 (682); *Boehm*/*Cole*, ZD 2014, 553 (553).

458 Siehe auch *Roßnagel*, MMR 2014, 372 (375); *Dix*/*Schaar*, in: Jahrbuch 2014, S. 18; *Durner*, DVBI 2014, 712 (714); *Kühling*, NVwZ, 2014, 681 (682); *Classen*, EuR 2014, 441 (443); *Koshan*, DuD 2016, 167 (169 f.).

459 Vgl. *Roßnagel*, MMR 2014, 372 (375).

3. Auswirkung des Urteils auf die europäische und nationale Gesetzgebung

a) Aussicht auf weitere vergleichbare Gesetzgebung auf europäischer Ebene?

Nach der Entscheidung des EuGH stellt sich vor allem die Frage, ob eine nach den Maßstäben dieses Urteils ausgestaltete Vorratsdatenspeicherung auf europäischer Ebene wieder eingeführt werden kann.[460] Zwar wurde die in der Richtlinie 2006/24/EG geregelte Vorratsdatenspeicherung untersagt, aber auf das Konzept einer Mindestspeicherung der Telekommunikationsdaten wird auf europäischer Ebene durchaus nicht verzichtet. Die Befürworter der Vorratsdatenspeicherung haben nicht aufgehört, sie als ein unverzichtbares Mittel zur Schwerkriminalitätsbekämpfung weiter zu fordern, während die Gegner das Urteil als Schlusspunkt der Vorratsdatenspeicherung verstehen.[461] In den Erwägungen des EuGH werden die Anforderungen ausgeführt, welche die Richtlinie nicht erfüllt und deswegen gegen die Grundrechte verstoßen hat. Es könnte daraus geschlussfolgert werden, dass eine Wiedereinführung der Vorratsdatenspeicherung möglich wäre, wenn sie den Anforderungen des EuGH genügen würde.[462] Diese Auffassung könnte sich auch auf das Ungültigkeitsurteil des BVerfG zur Umsetzungsregelung stützen, in dem festgestellt wird, dass eine vorsorgliche Verkehrsdatenspeicherung nicht von vornherein schlechthin verfassungswidrig ist. Sie könnte dem Verhältnismäßigkeitsprinzip genügen, wenn sie den strickten Anforderungen des Urteils gerecht werden würde.

Obwohl zwei Gerichthöfe das gleiche Entscheidungsergebnis hatten, dass die Regelungen der Vorratsdatenspeicherung ungültig sind, hat der EuGH aber anders als das BVerfG klar ausgedrückt, dass die anlasslose und unterschiedslose Vorratsdatenspeicherung nicht mit den europäischen Grundrechten vereinbar ist.[463] Eine vorsorgliche Speicherung der Verkehrsdaten, die keine differenzierten Regelungen oder Ausnahmeregelungen enthält und keinen Zusammenhang zwischen den Vorratsdaten und einer Bedrohung der Sicherheit fordert, ist nicht mehr zulässig, unabhängig von der konkreten

460 Siehe auch *Roßnagel*, MMR 2014, 372 (375).

461 Dazu siehe zum Beispiel damalige Meldungen unter: https://netzpolitik.org/2014/neue-eu-kommission-innenkommissar-avramopoulos-will-neuen-anlauf-fuer-vorratsdatenspeicherung/ [31.1.2019]; https://netzpolitik.org/2014/live-ticker-der-europaeische-gerichtshof-entscheidet-ueber-die-vorratsdatenspeicherung/ [31.1.2019].

462 Vgl. *Dix*/*Schaar*, in: Jahrbuch 2014, S. 21; *Kühling*, NVwZ 2014, 681 (683).

463 Siehe auch *Roßnagel*, MMR 2014, 372 (375).

Ausgestaltung.[464] Dies unterscheidet grundlegend das Urteil des EuGH von dem des BVerfG.[465] Im Konzept der Vorratsdatenspeicherung geht es genau darum, dass alle Telekommunikationsdaten ausnahmslos vor dem Eintritt der Gefahr und Begehen der Straftat anlasslos gespeichert werden. Irgendeine nähere Einschränkung oder Differenzierung lässt die Vorratsdatenspeicherung von ihrer eigentlichen Absicht abweichen. Jedenfalls wäre ihre Wirkung abgeschwächt. Eine Vorratsspeicherung der Telekommunikationsdaten, die alle Anforderungen des EuGH erfüllen würde, wäre auch nicht mehr als generelle Vorratsdatenspeicherung zu qualifizieren.[466] Damit scheint die Wiedereinführung einer Vorratsdatenspeicherung auf europäischer Ebene kaum Aussicht auf Erfolg haben.[467]

Es ist jedoch zu vermuten, dass eine modifizierte Vorratsdatenspeicherung erlassen wird, die nach den Anforderungen des EuGH zwischen bestimmten Zeiträumen, geografischen Gebiet, betroffenen Personenkreisen und Relevanz für die Straftatbekämpfung differenziert. Ob eine derartige Maßnahme grundrechtgemäß ist, hängt wiederum von der konkreten Ausgestaltung der materiellen Voraussetzung und der verfahrensrechtlichen Vorkehrungen gegen Datenmissbrauch und Datenenthüllung ab.

Angesichts der steigenden Tendenz, dass Sicherheits- und Strafverfolgungsbehörden immer mehr auf die Speicherung und Auswertung von personenbezogenen Daten angewiesen sind, lässt sich noch eine Frage aufwerfen, ob eine Vorratsspeicherung der personenbezogenen Daten in anderen Bereichen anhand des Urteils auch verboten ist. Im Urteil des EuGH wurde eine Vorratsdatenspeicherung in anderen Bereichen zwar nicht ausdrücklich als unzulässig festgestellt. Aber den Erwägungen des EuGH ist zu entnehmen, dass eine pauschale vorsorgliche Speicherung ohne nähere Differenzierung oder

---

464 So auch *Kunnert*, DuD 2014, 774 (777); *Petri*, ZD 2014, 296 (301); *Leutheusser-Schnarrenberger*, DuD 2014, 589 (592); *Roßnagel*, MMR 2014, 372 (375); *Roßnagel*, NJW 2016, 533 (538); *Boehm*/*Andrees*, CR 2016, 146 (152); *Kühling*, NVwZ 2014, 681 (683); *Priebe*, EuZW 2014, 456 (459); Ausarbeitung zur Vereinbarkeit des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten mit dem EuGH-Urteil vom 21. Dezember 2016 zur Vorratsdatenspeicherung von der Unterabteilung Europa (Fachbereich Europa), 12.01.2017, Aktenzeichen: PE 6 – 3000 – 167/16, S. 13.

465 Vgl. *Durner*, DVBI 2014, 712 (715); *Indra*, JZ 2014, 1109 (1113); *Kühling*, NVwZ 2014, 681 (683); *Dix*/*Schaar*, in: Jahrbuch 2014, S. 21.

466 Ob eine Vorratsspeicherung möglich ist, die allen Anforderungen des EuGH entspricht, ist auch praktisch sehr fragwürdig, siehe *Dalby*, in: *Kugelmann* (Hrsg.), S. 177. Vgl. *Dix*/*Schaar*, in: Jahrbuch 2014, S. 23; *Dalby*, in: *Kugelmann* (Hrsg.), S. 179.

467 Siehe auch *Indra*, JZ 2014, 1109 (1112); *Kühling*, NVwZ 2014, 681 (683).

Ausnahmergeln der personenbezogenen Daten in beliebigen Bereichen gegen die Grundrechtscharta verstoßen würde.[468]

Dies lässt sich auch dadurch begründen, dass der EuGH in dem Urteil am 6. Oktober 2015 bezüglich der Rechtmäßigkeit des EU-US-Safe-Harbor Abkommens[469] auf das Verbot einer unterschiedslosen Vorratsdatenspeicherung Bezug genommen hat:

„Nicht auf das absolut Notwendige beschränk ist eine Regelung, die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt wurden, gestattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne ein objektives Kriterium vorzusehen, das es ermöglicht, den Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strickt begrenzte Zwecke zu beschränken, die den sowohl mit dem Zugang zu diesen Daten als auch mit deren Nutzung verbundenen Eingriff zu rechtfertigen vermögen.“ [470]

Er weist darauf hin, dass eine unterschiedslose Vorratsspeicherung von personenbezogenen Daten generell verboten ist.[471] Damit ist eine vergleichbare Vorratsspeicherung der anderen personenbezogenen Daten mit den europäischen Grundrechten nicht vereinbar.[472]

b) Erforderlichkeit des Nachdenkens über Vorratsdatenspeicherung auf nationaler Ebene

Nach dem Ungültigkeitsurteil des EuGH hat ein Umsetzungsgesetz der Vorratsdatenspeicherung seine Rechtsgrundlage verloren, die Mitgliedstaaten sind nicht mehr verpflichtet, die Vorratsdatenspeicherung in das nationale Gesetz umzusetzen. Die Umsetzungsregelung der Vorratsdatenspeicherung in Deutschland wurde vom Bundesverfassungsgericht wegen Verstoß gegen das

---

468 Vgl. *Dix*/*Schaar*, in: Jahrbuch 2014, S. 23. Dagegen spricht, dass die Bedeutung des EuGH-Urteils mangels Vergleichbarkeit der verschiedenen Speichersysteme einschränkt sei, das Urteil des EuGH wegen der Eigenschaft der Verkehrsdaten sowie ihrer besonders wesentlichen Bedeutung für die Betroffene keine „Breitenwirkung“ für andere Datenspeicher habe, siehe *Dalby*, in: *Kugelmann* (Hrsg.),S. 181 ff.

469 EuGH Urteil in Rechtssache C-362/14 v. 06.10.2015.

470 EuGH, Urteil in Rechtssache C-362/14 v. 06.10.2015, Rn. 93.

471 Vgl. *Boehm*/*Andrees*, CR 2016, 146 (151).

472 Dazu siehe beispielhaft die Diskussion über Fluggastdatenspeicherung und -übermittlung: *Priebe*, EuZW 2014, 456 (459); *Dix*/*Schaar*, in: Jahrbuch 2014, S. 28; *Kunnert*, DuD 2014, 774 (781); *Boehm*/*Cole*, ZD 2014, 553 (556); *Boehm*/*Cole*, 2014, S. 58 ff.

Fernmeldegeheimnis aus Art. 10 GG für nichtig erklärt. Nun ist eine neue Umsetzung der Vorratsdatenspeicherung auch nicht mehr erforderlich. Trotzdem ist nicht ausgeschlossen, dass die Vorratsdatenspeicherung auf nationaler Ebene neu ausgestaltet und wieder eingeführt wird.[473] Denn gemäß dem BVerfG ist es möglich, eine gemäß den aufgestellten Anforderungen streng eingeschränkte Vorratsdatenspeicherung mit den Grundrechten in Einklang zu bringen. Bei der Wiedereinführung der Vorratsdatenspeicherung sollten jedoch die Aussagen des EuGH auch nicht unbeachtet bleiben.

Die Gültigkeit eines Gesetzes der Vorratsdatenspeicherung im Mitgliedstaat wird zwar nicht unmittelbar vom Urteil des EuGH beeinflusst. Aber das Gesetz muss dennoch den Anforderungen des EuGH gerecht werden: Dies liegt daran, dass Regelungen zur Vorratsdatenspeicherung im Anwendungsbereich des EU-Rechts liegen, genauer gesagt des Art. 15 der ePrivacy-RL, der nach dem Wegfall der Vorratsdatenspeicherungsrichtlinie wieder Bezugspunkt für eine nationale Regelung zur Vorratsdatenspeicherung ist.[474] Wie oben erwähnt haben das BVerfG und der EuGH zwar gleiche Entscheidungsergebnisse aber im Einzelnen durchaus unterschiedliche Einstellungen zur Vorratsdatenspeicherung. Eine anlasslose und unterschiedslose Vorratsspeicherung der Verkehrsdaten wird vom EuGH ausdrücklich abgelehnt und verboten. Auf nationaler Ebene kann zwar eine neu ausgestaltete Vorratsdatenspeicherung trotz des Urteils des EuGH realisiert werden. Wird die Achtungspflicht der Rechtsprechung des EuGH vom Mitgliedsstaat jedoch berücksichtigt, wird eine Gesetzgebung der Vorratsdatenspeicherung – auch wenn sie die strickten Anforderungen des Bundesverfassungsgerichts erfüllen würden – nicht mit der Auslegung des EuGH vereinbar sein. Es ist auch kaum möglich, die Vorratsdatenspeicherung so auszugestalten, dass sie die hohen rechtlichen Hürden beider Gerichte nimmt und gleichzeitig nicht von der eigentlichen Absicht abweicht.[475] Somit hat der Gesetzgeber die vorhandene Regelung der Vorratsdatenspeicherung nach den Anforderungen des EuGH neu nachzuprüfen und daran anpassen zu lassen.[476]

---

473 Eine Vorratsdatenspeicherung wird politisch mehrfach gefordert, dazu die Meldungen unter:
https://netzpolitik.org/2014/berliner-erklaerung-spd-innenminister-fordern-vorratsdatenspeicherung-immer-noch/ [31.1.2019];
http://www.spiegel.de/netzwelt/netzpolitik/bundesregierung-plant-gesetz-zur-vorratsdatenspeicherung-a-1022251.html [31.1.2019];
http://www.deutschlandfunk.de/sigmar-gabriel-wir-brauchen-die-vorratsdatenspeicherung.868.de.html?dram:article_id=314247 [31.1.2019].

474 Siehe auch *Boehm*/*Cole*, ZD 2014, 553 (555); *Dix*/*Schaar*, in: Jahrbuch 2014, S. 25; *Priebe*, EuZW 2014, 456 (458).

475 Vgl. *Dix*/*Schaar*, in: Jahrbuch 2014, S. 23; *Boehm*/*Cole*, 2014, S. 48.

476 Siehe auch *Kunnert*, DuD 2014, 774 (782); *Kühling*, NVwZ 2014, 681 (684);

c) Quick-Freeze-Verfahren

Das Konzept des Quick-Freeze-Verfahrens ist auf europäischer Ebene nicht völlig neu. Eine vergleichbare Maßnahme wurde schon in Art. 16 des Übereinkommens über Computerkriminalität im Jahr 2001 geregelt.[477] Demgemäß ist jede Vertragspartei verpflichtet, die erforderlichen gesetzlichen und andere Maßnahmen zu treffen, damit bestimmte Computerdaten einschließlich Verkehrsdaten umgehend gesichert werden können, insbesondere bei Gefahr des Verlusts oder der Veränderung bestimmter Computerdaten. In Anlehnung an dieses Verfahren wird vorgeschlagen, dass die Vorratsdatenspeicherung durch Quick-Freeze-Verfahren in Bezug auf die Verkehrsdaten zu ersetzen.[478] Statt alle Telekommunikationsdaten anlasslos zu speichern, werden beim Quick-Freeze-Verfahren nur bestimmte Telekommunikationsdaten bei einem bestimmten Verdachtsfall von Dienstanbietern aufgrund der Anordnung der zuständigen Behörde für einen bestimmten Zeitraum gesichert. Der spätere Zugriff auf die gespeicherten Daten und deren Nutzung ist durch eine richterliche Anordnung möglich.[479]

Das Verfahren spielt nicht nur in der akademischen Diskussion eine Rolle, sondern wird auch tatsächlich als gesetzgeberische Alternative für die Vorratsdatenspeicherung in Betracht gezogen.[480] Es ist umso erwägenswerter, als der EuGH nun eine anlasslose Vorratsspeicherung abgelehnt hat. Das Quick-Freeze-Verfahren wäre mit dieser Anforderung zu vereinbaren, weil es nur beim Einzelfall und wegen konkreter Gefahr durchgeführt wird.[481] In diesem Fall wäre das Quick-Freeze-Verfahren eine die Anforderungen des EuGH erfüllende Alternative zur Vorratsdatenspeicherung. Jedoch hat der

---

Boehm/*Cole*, 2014, S. 92 ff.

477 Das Übereinkommen des Europarats vom 23. November 2001 über Computerkriminalität, CETS 185, BGBI. 2008 II, Nr. 30, S. 1242 ff.

478 *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 180-182; vgl. Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. Oktober 2005, „Keine Vorratsdatenspeicherung in der Telekommunikation“, abrufbar unter: https://www.datenschutzzentrum.de/artikel/180-Entschliessung-Keine-Vorratsdatenspeicherung-in-der-Telekommunikation.html [31.1.2019]; Art. 29-Gruppe, Stellungnahe 4/2005 zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 202/58/EG (KOM (2005) 438 endg. vom 21.9.2005), 21. 10. 2005, WP 113, S. 3, 7.

479 Eckpunkte zur Verbesserung der Kriminalitätsbekämpfung im Internet von der FDP-Bundestagsfraktion, Stand: 9. November 2010, abrufbar unter: http://archiv.jimmy-schulz.com/content/fdp-bundestagsfraktion-eckpunkte-zur-verbesserung-der-kriminalitätsbekämpfung-im-internet-fr, S. 7

480 *Roßnagel*/*Moser-Knierim*/*Schweda*, S. 86.

481 Siehe auch *Dix*/*Schaar*, in: Jahrbuch 2014, S. 25.

EuGH diese Alternative in seinem Urteil nicht erwähnt. Ob darin gleich effektive und grundrechtsschonendere Alternative besteht, wurde vom EuGH nicht geklärt.[482]

Zwar kann das Verfahren den Betroffenen deutlich geringer belasten, aber die Grundrechtmäßigkeit des Verfahrens darf nicht deswegen ohne Weiteres bejaht werden. Wegen des sensiblen Charakters der Verkehrsdaten und deren besonderen Bedeutung für das Privatleben der Bürger ist das Quick-Freeze-Verfahren trotz seiner Anlassbezogenheit ebenso nach den strikten Maßstäben des EuGH zu überprüfen. Würde eine Einschränkung des Eingriffs in das Grundrecht nicht klar und präzise geregelt, oder würden strenge materiell- und verfahrensrechtliche Voraussetzungen nicht gewährleistet, wäre der Eingriff durch das Verfahren nicht auf das absolut Notwendige beschränkt. Zum Beispiel wenn die Straftatenschwelle oder Verdachtsschwelle für Verkehrsdatenanfragen zu niedrig oder nicht klar festgelegt würde, könnte das *„Einfrieren“* der Verkehrsdaten grenzenlos angeordnet werden.[483]

Ein grundrechtsmäßiges Quick-Freeze-Verfahren ist damit nur dann zulässig, wenn es so ausgestaltet wird, dass es den strengen Anforderungen des EuGH entspricht und der Eingriff somit auf das absolut Notwendige beschränkt wird. Dadurch können jedoch immer noch immense Kosten anfallen, die für die Durchsetzung der strengen Anforderung an den Datenschutz und die Datensicherheit angesetzt werden. Demgegenüber wird die Effektivität des Quick-Freeze-Verfahren für die Strafverfolgung und die Gefahrenabwehr bislang noch nicht genau untersucht. Insbesondere die förderliche Wirkung für Strafverfolgung und Gefahrenabwehr ist noch nicht endgültig geklärt. Zusammenfassend ist das Quick-Freeze-Verfahren als Alternative der Vorratsdatenspeicherung denkbar. Die Zulässigkeit hängt letztlich jedoch von der genauen Ausgestaltung ab.

d) Wirkung auf Grundrechtsschutz und Weiterentwicklung des Datenschutzrechts in Europa

Der lange Streit über die Rechtmäßigkeit der Vorratsdatenspeicherung wurde endlich auf europäischer Ebene entschieden. Zur Förderung eines gemeinsamen europäischen Grundrechtsschutzes hat der EuGH wiederum einen wesentlichen Beitrag geleistet.[484] Die Bedeutung dieses Urteils wird nicht

---

482 Vgl. *Kunnert*, DuD 2014, 774 (783 f.).
483 Vgl. *Kunnert*, DuD 2014, 774 (784).
484 Vgl. *Durner*, DVBI 2014, 712 (715); *Indra*, JZ 2014, 1109 (1110); *Kühling*, NVwZ

nur darauf begrenzt, dass die Rechtmäßigkeit der fraglichen Richtlinie beurteilt wurde. Vielmehr hat der EuGH den grundrechtlichen Maßstab für mit der Vorratsdatenspeicherung vergleichbare Sicherheitsmaßnahmen festgelegt.[485] Für eine künftige europäische Gesetzgebung des Datenschutzes ist der Maßstab von erheblicher Bedeutung.

Vor allem ist der EuGH auf den Schutzbereich des Rechts auf Privatleben in Art. 7 GRCh, des Rechts auf Schutz personenbezogener Daten im Art. 8 GRCh und das Verhältnis zwischen beiden Grundrechten bezüglich des Datenschutzes und der Privatsphäre ausführlich eingegangen.[486] Durch die Beurteilung, ob und inwieweit in die beiden Grundrechte von der Vorratsdatenspeicherung eingegriffen wird, wird die Relevanz des Art. 7 und 8 GRCh ausdrücklich dargestellt. Eine vorsorgliche anlasslose Vorratsspeicherung der Telekommunikationsdaten zum Zweck der Strafverfolgung und Gefahrenabwehr ist verboten. Eine derartige Vorratsspeicherung der personenbezogenen Daten in anderen Lebensbereichen der Bürger würde voraussichtlich auch gegen die genannten Grundrechte verstoßen,[487] da der Eingriff ohne differenzierte Regelung bezüglich des Zusammenhangs zwischen den zu speichernden Daten und einer Bedrohung der Sicherheit nicht auf "das absolut Notwendige" beschränkt ist.

Kernpunkt des EuGH-Urteils ist, dass eine vorsorgliche Speicherung der personenbezogenen Daten durch differenzierte materiell- sowie verfahrensrechtliche Regelung beschränkt werden muss, um sicherzustellen, dass die Speicherung erforderlich ist. Dazu muss zwischen den zu speichernden Daten und einer Bedrohung der Sicherheit ein Zusammenhang bestehen. Der Umfang der betroffenen Personen sowie die zu speichernden Datenkategorien sind angesichts des vorgegebenen Zusammenhangs auf ein Minimum zu reduzieren. Die Speicherungsdauer darf nicht pauschal vorgeschrieben werden, sondern ist abhängig von den zu speichernden Datenkategorien zu unterscheiden.

Außerdem müssen der Zugriff und die Verwendung der Vorratsdaten von den zuständigen Behörden klaren und strengen Einschränkungen unterliegen, um unbefugten Zugriff und eine uferlose Verwendung zu verhindern. Zu derarti-

---

2014, 681 (682f.); von *Danwitz*, DuD 2015, 581 (585); *Roßnagel*, MMR 2014, 372 (377).

485 Vgl. *Boehm*/*Cole*, ZD 2014, 553 (553); *Roßnagel*, MMR 2014, 372 (377).

486 Vgl. *Boehm*/*Cole*, ZD 2014, 553 (553); *Boehm*/*Cole*, 2014, S. 90.

487 Siehe auch *Roßnagel*, MMR 2014, 372 (376); *Dix*/*Schaar*, in: Jahrbuch 2014, S. 23.

ger Einschränkung gehört insbesondere die Bestimmung, die sicherstellen kann, dass die zugegriffenen Vorratsdaten später nur zum vorgeschriebenen Zweck genutzt werden dürfen.[488] Zu einer wirksamen Kontrolle des Zugriffs auf die Vorratsdaten gehört insbesondere eine vorherige richterliche Anordnung oder eine Kontrolle einer unabhängigen Verwaltungsstelle.[489] Die Zahl der zum Zugang zu den Vorratsdaten befugten Personen ist dem dienenden Zweck angemessen anzusetzen.[490]

Bei den technischen und organisatorischen Datenschutz- und Datensicherheitsmaßnahmen ist sicherzustellen, dass betroffene Daten während der Speicherung vor Missbrauch und unberechtigtem Zugriff geschützt werden.[491] Das Schutz- und Sicherheitsniveau muss der Sensibilität der gespeicherten Daten entsprechen.[492] Nach Ablauf der Speicherungsfrist müssen die Vorratsdaten sofort und unwiderruflich gelöscht werden.[493] Darüber hinaus müssen die fraglichen Daten im Unionsgebiet gespeichert werden, damit die Einhaltung der Anforderungen des Datenschutzes und Datensicherheit durch eine unabhängige Kontrolle gewährleistet werden kann.[494]

III. Modifizierte Vorratsdatenspeicherung in Deutschland

Trotz des Ungültigkeitsurteils des EuGH über die Richtlinie 2006/24/EG wurde die Vorratsdatenspeicherung in Deutschland neu ausgestaltet und im Jahr 2015 wiedereingeführt. Nun unterliegen diese Regelungen den Anforderungen gemäß BVerfG und EuGH.

1. Speicherungspflichten der Verkehrsdaten und Standortdaten

Gemäß den neuen Vorgaben der Vorratsdatenspeicherung müssen Telekommunikationsverkehrsdaten für zehn Wochen, und Standortdaten für vier Wochen im Inland gespeichert werden (§ 113b Abs. 1 TKG). Die Verpflichteten sind Erbringer öffentlich zugänglicher Telekommunikationsdienste (§ 113a Abs. 1 S. 1 TKG). Zu speichernde Daten sind die Rufnummer oder eine andere Kennung aller beteiligten Anschlüsse der Telefonverbindung, Datum und Uhrzeit, Beginn und Ende der Telefonverbindung und Angaben zu dem genutzten Dienst, wenn im Rahmen des Telefondienstes unterschiedliche

488 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 61.
489 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 62.
490 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 62.
491 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 66.
492 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 66.
493 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 67.
494 EuGH, Rechtssachen C-293/12 und C-594/12 v. 08.04.2014, Rn. 68.

Dienste genutzt werden können (§ 113b Abs. 2 Nr. 1-3 TKG). Bei der mobilen Telefonverbindung sind ferner die internationale Kennung für die beteiligten Anschlüsse und für Endgeräte, und Datum und Uhrzeit der ersten Aktivierung des im Voraus bezahlten Dienstes zu speichern (§ 113b Abs. 2 Nr. 4 TKG). Bei den Internet-Telefondiensten sind auch die IP-Adresse des beteiligten Anschlusses und zugewiesene Benutzerkennungen zu speichern (§ 113b Abs. 2 Nr. 5 TKG). Die Speicherungspflicht gilt auch bei der Übermittlung der Nachricht in allen Formen wie zum Beispiel SMS, MMS (§ 113b Abs. 2 S. 2 Nr. 1 TKG). Verkehrsdaten bei unbeantworteten Anrufen oder der erfolglosen Verbindung sind auch zu speichern (§ 113b Abs. 2 S. 2 Nr. 2 TKG). Bei den Internetzugangsdiensten muss die zugewiesene IP-Adresse der Teilnehmer, Kennung des Anschlusses und zugewiesene Benutzerkennung sowie Datum und Uhrzeit von Beginn bis Ende der Internetnutzung protokolliert werden (§ 113b Abs. 3 TKG). Zu speichernde Standortdaten sind die Bezeichnungen der Funkzellen, die bei Beginn der mobilen Telefonverbindung und der Internetverbindung genutzt wurden (§ 113b Abs. 4 S. 1 und 2 TKG). Auch die Daten, aus denen sich die geografische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben, sind zusätzlich zu speichern (§ 113b Abs. 4 S. 3 TKG).

Die Inhalte der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post werden von der Speicherungspflicht ausgeschlossen (§ 113b Abs. 5 TKG). Die Verkehrsdaten, die den in § 99 Abs. 2 TKG genannten Verbindungen zugrunde liegen, dürfen nicht gespeichert werden (§ 113b Abs. 6 TKG). Unter solchen Verbindungen versteht man die Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen, die dem sozialen oder kirchlichen Bereich zuzuordnen sind, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen (§ 99 Abs. 2 S. 1 TKG). Dies gilt nur für Anschlüsse, die in der Liste der Bundesnetzagentur aufgenommen werden (§ 99 Abs. 2 Satz 2 TKG). Die gespeicherten Daten müssen nach Ablauf der Speicherfristen unverzüglich, spätestens binnen einer Woche unumkehrbar gelöscht werden oder die unumkehrbare Löschung sichergestellt werden (§ 113b Abs. 8 TKG).

Im Vergleich mit der Umsetzungsregelung zur Richtlinie der Vorratsdatenspeicherung wird die modifizierte Speicherungspflicht prägnanter und eindeutiger vorgeschrieben. Der Umfang der zu speichernden Daten wird aber

keinesfalls verringert oder in irgendeiner Weise differenziert. Von der Speicherungspflicht sind immer noch fast alle Telekommunikationsdaten betroffen.

Statt alle Telekommunikationsdaten für eine einheitliche Dauer zu speichern, gibt es nun zwei unterschiedliche Speicherungsfristen. Ein anderer Versuch, die Anforderungen von BVerfG und EuGH zu erfüllen, besteht darin, dass die Verbindungsdaten der in § 99 Abs. 2 TKG genannten telefonischen Beratungen von Speicherungspflichten ausgeschlossen werden.

Trotz der oben genannten Anstrengungen genügt die neue Speicherungspflicht den Vorgaben des EuGH wohl nicht. Die neue Speicherungspflicht betrifft vor allem immer noch fast die gesamte Bevölkerung. Der Schutz der Berufsgeheimnisträger wird insoweit als unvollständig kritisiert, als nicht alle in § 53 Abs. 1 StPO genannten Berufsgeheimnisträger vor der Vorratsspeicherung geschützt werden.[495] Die Ausnahme der Speicherungspflicht gilt nur für Betroffene bestimmter telefonische Beratungen, die von der Bundesnetzagentur anerkannt werden. Der Schutz der anderen Berufsgeheimnisträger findet sich erst in den Vorschriften der Erhebung und Verwendung der Vorratsdaten. Es kann bezweifelt werden, dass dies für den Schutz der Vertrauensbeziehung ausreicht.[496] Ferner wird immer noch keine Verknüpfung zwischen den zu speichernden Daten und einer Bedrohung der öffentlichen Sicherheit gefordert. Alle Telekommunikationsdaten müssen nach wie vor allgemein gespeichert werden, ohne Differenzierung anhand irgendwelches Kriteriums wie Zeitraum, Gebiet oder Personenkreis festzulegen.[497] Damit bleibt die neue Speicherungspflicht eine anlasslose und flächendeckende Vorratsdatenspeicherung, die schon vom EuGH ausdrücklich abgelehnt wurde.

---

495 *Dix*/*Kipker*/*Schaar*, ZD 2015, 300 (302); *Gärtner*/*Kipker*, DuD 2015, 593 (597); Ausarbeitung zur Vereinbarkeit des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten mit dem EuGH-Urteil vom 21. Dezember 2016 zur Vorratsdatenspeicherung von der Unterabteilung Europa (Fachbereich Europa), 12.01.2017, Aktenzeichen: PE 6 – 3000 – 167/16, S.16 f.; *Roßnagel*, NJW 2017, 696 (698); *Dix*/*Kipker*/*Schaar*, ZD 2015, 300 (302).

496 Stellungnahme des Deutschen Anwaltvereins durch die Ausschüsse Gefahrenabwehrrecht, Informationsrecht und Strafrecht zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, Berlin, im Mai 2015, Stellungnahme Nr.: 25/2015, S. 13; *Henssler*/*Kleen*/*Riegler*, MedR 2016, 850 (851); *Gärtner*/*Kipker*, DuD 2015, 593 (597).

497 Vgl. *Ziebarth*, ZUM 2017, 398 (404); *Roßnagel*, NJW 2016, 533 (538); *Boehm*/*Andrees*, CR 2016, 146 (149);

2. Erhebungs- und Verwendungsbefugnis der gespeicherten Daten

Die gespeicherten Daten dürfen unter der Berufung auf eine gesetzliche Bestimmung an eine Strafverfolgungsbehörde zum Zweck der Verfolgung besonders schwerer Straftaten, an eine Gefahrenabwehrbehörde der Länder zum Zweck der Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person, oder für den Bestand des Bundes oder eines Landes übermittelt werden und für eine Auskunft nach § 113 Abs. 1 Satz 3 TKG durch die Telekommunikationsdienstanbieter verwendet werden (§ 113c Abs. 1 TKG). Das heißt, dass die gespeicherten Vorratsdaten durch die Dienstanbieter für Zwecke der Auskunft zu einer dynamischen IP-Adresse verwendet werden dürfen.

Als gesetzliche Bestimmung für die Erhebung der Vorratsdaten wird § 100g StPO neu gefasst. Demgemäß werden Befugnisse zur Erhebung der zum betrieblichen Zweck gespeicherten Verkehrsdaten, Erhebung der auf Vorrat gespeicherten Verkehrsdaten und Abfrage aller in einer Funkzelle angefallenen Verkehrsdaten erteilt. Die Vorratsdaten dürfen für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erhoben werden. Voraussetzungen dafür sind a) bestimmte Tatsachen die den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine der in § 100g Abs. 2 Satz 2 StPO bezeichneten, besonders schwere Straftat begangen hat oder zu begehen versucht hat, b) die Tat auch im Einzelfall besonders schwer wiegt, c) die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aufsichtlos wären und d) die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht (§ 100g Abs. 2 StPO).

Für Funkzellenabfragen wird eine neue und spezielle Regelung hinzugefügt. Alle in einer Funkzelle angefallenen Verkehrsdaten dürfen erhoben werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine schwere Straftat in § 100a Abs. 2 StPO begangen oder zu begehen versucht oder durch eine Straftat vorbereitet hat, soweit die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre (§ 100g Abs. 3 S. 1 StPO). Eine Funkzellenabfrage der Vorratsdaten ist unter den gleichen Voraussetzungen für die Erhebung der Vorratsdaten in § 100g Abs. 2 StPO zulässig. Für andere als die in § 113c Abs. 1

TKG genannten Zwecke dürfen die Vorratsdaten nicht verwendet werden (§ 113c Abs. 2 TKG). Ausnahmsweise dürfen die schon erhobenen Vorratsdaten für andere Strafverfahren zur Aufklärung einer Straftat, auf Grund derer eine Vorratsdatenabfrage angeordnet werden könnte, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person und zu Zwecken der Abwehr von konkreten Gefahren für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes weitergeleitet werden (§ 101a Abs. 4 Satz 1 StPO).

Die erhobenen Daten sind entsprechend zu kennzeichnen und unverzüglich auszuwerten. Nach einer Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten (§ 101a Abs. 3 StPO). Die Erhebung von Verkehrsdaten der Berufsgeheimnisträger ist unzulässig, die in § 53 Abs. 1 Satz 1 Nr. 1 bis 5 StPO genannt werden. Schon erlangte Erkenntnisse dürfen nicht verwendet werden (§ 100g Abs. 4 StPO). Verkehrsdaten von nicht in der Liste der Bundesnetzagentur stehenden Berufsgeheimnisträger sind zwar zu speichern, aber demgemäß dürfen sie nicht verwendet werden.

In den neuen Regelungen zum Datenzugriff und der Datenverwendung werden viele Anforderungen des BVerfG und des EuGH beachtet und umgesetzt. Die Erhebung der Verkehrsdaten wird vor allem anhand der zwei unterschiedlichen Datenarten und zwar Verkehrsdaten im Sinne des § 96 Abs. 1 TKG und auf Vorrat gespeicherten Verkehrsdaten gesondert geregelt. Die Datenverwendung wird auch erst durch das *„Doppeltürverfahren“* ermöglicht, das heißt, dass eine Übermittlung nicht allein durch § 113c Abs. 1 TKG, sondern noch durch eigene fachspezifische Ermächtigungsgrundlagen zulässig sein muss.[498] Ferner wird die Funkzellenabfrage durch eine neue Sonderregelung geregelt. Darüber hinaus werden die Voraussetzungen, die ein Vorratsdatenabruf erfüllen muss, konkret aufgeführt. Der Verwendungszweck wird auf Verfolgung besonders schwerer Straftaten und Gefahrenabwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes begrenzt. Dafür werden besonders schwere Straftaten einzeln genannt, zu deren Verfolgung ein Vorratsdatenabruf zulässig ist. Dies entspricht den Anforderungen aus den beiden Urteilen: dass der Eingriff von der Vorratsdatenspeicherung klar und präzise vorgeschrieben, und an die Rechtfertigung der Verwendung gespeicherter Vorratsdaten besonders hohe Anforderungen gestellt werden müssen.

---

498 *Bär*, in: *Graf* (Hrsg.) 2018, TKG § 113c, Rn. 2; *Bär*, NZWiSt 2017, 81 (82).

Bezüglich der Reglung der Berufsgeheimnisträger werden zwar nicht alle Berufsgeheimnisträger von der Speicherungspflicht ausgeschlossen. Es ist aber die Tatsache zu berücksichtigen, dass es sehr schwierig ist, alle Berufsgeheimnisträger stets zu erkennen und den Telekommunikationsdiensteanbietern aktualisiert zur Verfügung zu stellen.[499] Der Schutz von Berufsgeheimnisträgern, insbesondere diejenigen, die nicht in die List von der Bundesnetzagentur aufgenommen sind, wird allerdings bei der Erhebung der Vorratsdaten noch gewahrt.[500]

Hinzu kommt, dass die gespeicherten Vorratsdaten nur zu geregelten Zwecken verwendet werden dürfen. Eine Zweckänderung ist nur ausnahmsweise unter den genannten Voraussetzungen zulässig. Die Verwendung der Vorratsdaten entspricht also dem Zweckbindungsprinzip.[501] Weiterhin wird die Verwendung der bereits durch eine entsprechende polizeirechtliche Maßnahme erlangten Vorratsdaten streng beschränkt. Der besonders sensible Charakter von Standortdaten wird berücksichtigt. Die Erhebung der zum geschäftlichen Zweck gespeicherten Standortdaten wird von § 100g Abs. 1 Satz 2 im Vergleich zu den frühen Vorschriften dadurch streng beschränkt, dass sie grundsätzlich ausgeschlossen werden.[502]

3. Entschädigung für Telekommunikationsunternehmen

Neu eingeführt wurden auch Regelungen zu Entschädigungen. Nach § 113a Abs. 2 TKG ist eine angemessene Entschädigung für notwendige Aufwendungen zu zahlen, welche den Verpflichteten durch die Umsetzung der Vorgaben entstehen, soweit dies zur Abwendung oder zum Ausgleich unbilliger Härten geboten erscheint. Für die Bemessung der Entschädigung sind die tatsächlich entstandenen Kosten maßgebend. Ferner entscheidet die Bundesnetzagentur über Anträge auf Entschädigung. Wegen des Fehlens einer Entschädigungsregelung wurde die frühere Umsetzungsregelung zur Vorratsda-

499 *Bär*, in: *Graf* (Hrsg.) 2018, TKG § 113b, Rn. 24; Gesetzentwurf der Fraktionen der CDU/CSUS und SPD, Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, Drucksache 18/5088, 09.06.2015, S. 33, Kritik und verfahrenstechnische Lösungsansatz dazu siehe zum Beispiel *Gärtner*/*Kipker*, DuD 2015, 593 (598 f.).

500 *Roßnagel*, NJW 2016, 533 (537).

501 Siehe auch *Roßnagel*, NJW 2016, 533 (536).

502 Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz zur Vorratsdatenspeicherung (Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten), Bearbeitungsstand: 15.05.2015, S. 29, abrufbar unter: https://netzpolitik.org/wp-upload/2015-05-15_BMJV-Referentenentwurf-Vorratsdatenspeicherung.pdf [31.1.2019].

tenspeicherung wiederholt kritisiert.[503] Zur Erfüllung der Speicherungs- und Übermittlungspflicht müssen die Telekommunikationsdiensteanbieter nicht nur den zusätzlichen Aufwand für Einrichtung und Personal belasten. Es entstehen den Anbietern auch Kosten für entsprechende organisatorische und technische Maßnahmen, um den besonders hohen Datensicherheitsstandard zu gewährleisten. Die zusätzlichen Kosten könnten andernfalls für kleine Unternehmen eine erdrosselnde Wirkung haben.[504]

Nach der neuen Regelung ist eine Entschädigung auf Antrag möglich. Eine Entschädigung setzt voraus, dass eine angemessene Entschädigung zur Abwendung oder zum Ausgleich unbilliger Härten geboten erscheint. Dafür müssen die Antragsteller darlegen, dass die Erfüllung der Speicherungspflichten für ihr Unternehmen erdrosselnde Wirkung haben könnte.[505] Für die Prüfung der Anträge ist die Bundesnetzagentur zuständig. Die Entschädigungsregelung ist zwar begrüßenswert, aber sie greift nur im Falle einer erdrosselnden Wirkung. Für andere Diensteanbieter, denen zwar keine erdrosselnde Wirkung droht, die aber trotzdem von der Pflicht belastet ist, greift die Regelung nicht.[506]

4. Gewährleistung der Datensicherheit

In § 113 d TKG wird den Erbringern öffentlich zugänglicher Telekommunikationsdienste ein Maßstab für die Gewährleistung der Datensicherheit gesetzt. Die gespeicherten Vorratsdaten sind durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung zu schützen. Zu derartigen Maßnahmen gehören insbesondere der Einsatz eines besonders sicheren Verschlüsselungsverfahrens, die Speicherung in gesonderten, von den für die üblichen betrieblichen Aufgaben getrennten Speichereinrichtungen, die Speicherung mit einem hohen Schutz vor dem Zugriff aus dem Internet, die Beschränkung des Zutritts zu den Datenverarbeitungsanlagen auf Personen, die durch den Verpflichteten besonders ermächtigt sind, und die notwendige Mitwirkung von mindestens

---

503 Siehe oben die Kritik des Mangels der Entschädigungsregelung zur Rechtfertigung des Eingriffs in die Berufsfreiheit der Telekommunikationsunternehmen, Kapitel 2, B.III.2.

504 Siehe auch *Roßnagel*, NJW 2016, 533 (536); *Bär*, in: *Graf* (Hrsg.) 2018, TKG § 113a Rn. 7-8; *Roßnagel*/*Moser-Knierim*/*Schweda* , S. 145; *Freiling*, Technischer Bericht TR-2009-005, S. 19.

505 Gesetzentwurf der Fraktionen der CDU/CSU und SPD, Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, BT-Drs. 18/5088, 09.06.2015, S. 37.

506 Siehe auch *Gärtner*/*Kipker*, DuD 2015, 593 (595); *Derksen*, NVwZ 2017, 1005 (1008 f.).

zwei Personen beim Zugriff auf die Daten, die dazu durch den Verpflichteten besonders ermächtigt worden sind. Zwecks der Datenschutzkonformität sind der Zeitpunkt, der Zweck und die Art jedes Zugriffs und die auf die Daten zugreifenden Personen zu protokollieren (§ 113e Abs. 1 TKG).

Bei Speicherung und Übermittlung der Vorratsdaten ist ein besonders hoher Standard der Datensicherheit und Datenqualität zu gewährleisten, dessen Einhaltung vermutet wird, wenn alle Anforderungen des Katalogs der technischen Vorkehrungen und sonstigen Maßnahmen erfüllt werden, den die Bundesnetzagentur im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erstellt (§ 113f Abs. 1 TKG). Neben den Angaben aus § 109 Abs. 4 TKG hat die Verpflichtete die Systeme, auszugehende Gefährdungen für die Systeme und getroffene oder geplante technische Vorkehrungen oder sonstige Maßnahmen bei Vorratsdatenspeicherung zusätzlich aufzunehmen (§ 113g TKG).

Angesichts des großen Volumens und sensiblen Charakters der Vorratsdaten besteht ein großes Risiko in Bezug auf Datenenthüllung und Datenmissbrauch. Die Ausgestaltung der Vorratsdatenspeicherung muss den besonders hohen Anforderungen an die Datensicherheit genügend Rechnung tragen.[507] In den neuen Regelungen zur Vorratsdatenspeicherung werden die konkreten Anforderungen insbesondere vom BVerfG an die Gewährleistung hinreichender Datensicherheit berücksichtigt und vollständig umgesetzt. Die technischen und organisatorischen Maßnahmen werden konkret aufgelistet. Dazu gehören die vom BVerfG erwähnte getrennte Datenspeicherung, sichere Verschlüsselung, das Vier-Augen-Prinzip für den Datenzugriff und Protokollierung der Verarbeitung von Vorratsdaten.[508] Ferner wird betont, dass sich das besonders hohe Maß an Datensicherheit am Stand der Technik und der Fachdiskussion orientieren muss. Der Maßstab der Beurteilung, ob ein besonders hoher Standard der Datensicherheit eingehalten wird, muss genau festgelegt werden. Hinzu kommt, dass die Maßnahmen zur Datensicherheit bei Durchführung der Vorratsdatenspeicherung in das Sicherheitskonzept zusätzlich aufgenommen werden müssen. Bemerkenswert ist außerdem, dass die Regelung zur Entschädigung neu hinzugefügt wurde, die gewissermaßen verhindert, dass die privaten Dienstanbieter wegen Kostendrucks nur begrenzte Anreize zur Gewährleistung von Datensicherheit haben.

---

507 BVerfGE 125, 260 (325).
508 BVerfGE 125, 260 (326 ff.).

5. Rechtsschutz und Sanktionen

In Bezug auf den Rechtsschutz werden der Richtervorbehalt, Datenkennzeichnung sowie Datenauswertung und Benachrichtigungspflichten in § 101a StPO vorgeschrieben. Anders als die einheitlichen Verfahrensregelungen bei verdeckten Maßnahmen in § 101 StPO werden Sonderregelungen speziell für die Erhebung der Vorratsdaten eingefügt.[509] § 101a Abs. 1 StPO enthält den Richtervorbehalt für die Erhebung der Vorratsdaten. Demgemäß darf die Vorratsdatenerhebung nur durch ein Gericht angeordnet werden. In der Entscheidungsformel sind neben den Angaben aus § 100b Abs. 2 StPO noch die zu übermittelnden Daten und der Zeitraum, für den sie übermittelt werden sollen, zu bezeichnen. Bei Funkzellenabfragen genügt eine räumlich und zeitlich eng begrenzte und hinreichend bestimmte Bezeichnung der Telekommunikation. Die Eilanordnung durch die Staatsanwaltschaft bei Gefahr im Verzug nach § 100b Abs. 1 S. 2 und 3 StPO gilt bei der Vorratsdatenerhebung nicht.

Die Beteiligten der betroffenen Telekommunikation sind nach § 101a Abs. 6 S. 1 StPO bezüglich der Erhebung der Verkehrsdaten zu benachrichtigen. Das Unterbleiben der Benachrichtigung ist unter Voraussetzungen aus § 101 Abs. 4 S. 2 bis 5 StPO zulässig und bedarf der Anordnung des zuständigen Gerichts. Ferner bedarf die Zurückstellung der Benachrichtigung stets der Anordnung des zuständigen Gerichts. Eine erstmalige Zurückstellung ist auf höchstens zwölf Monate zu befristen. Verstöße gegen die Verpflichtungen zur Datensicherheit nach dem geänderten § 149 Abs. 2 TKG können mit einer Geldbuße bis zu 500.000 Euro geahndet werden.

Für eine verfassungsmäßige Vorratsdatenspeicherung hat das BVerfG, wie dargestellt, strenge Anforderungen an das Transparenzgebot, den effektiven Rechtsschutz sowie effektive Sanktionen aufgestellt. Eine heimliche Verwendung der Vorratsdaten im Rahmen der Strafverfolgung ist demnach nur ausnahmsweise zulässig, wenn sie im Einzelfall erforderlich ist, zudem bedürfe sie einer richterlichen Entscheidung.[510] Die vorbeugende richterliche Kontrolle muss sich in *„spezifischer und normenklarer Form mit strengen Anforderungen an den Inhalt und die Begründung der gerichtlichen Anordnung verbinden."*[511] Der Richter muss sorgfältig prüfen, ob die Datenerhe-

---

509 *Bär*, in: *Graf* (Hrsg.) 2018, StPO § 101a Rn. 1 f.
510 BVerfGE 125, 260 (336).
511 BVerfGE 125, 260 (338).

bung den gesetzlichen Voraussetzungen *„einschließlich insbesondere der gesetzlich vorgeschriebenen Eingriffsschwelle“* entspricht und den Anordnungsbeschluss gehaltvoll begründen.[512] Bei einer heimlichen Verwendung der Vorratsdaten habe grundsätzlich zumindest eine nachträgliche Benachrichtigung zu erfolgen. Ein Unterbleiben der nachträglichen Benachrichtigung sei gerichtlich zu überprüfen.[513] Es sei auch erforderlich, die Benachrichtigungspflichten hinsichtlich der Vorratsdatenverwendung zum Zweck der Gefahrenabwehr oder Erfüllung der Aufgaben der Nachrichtendienste auszugestalten.[514] Eine Benachrichtigung könne unterbleiben, wenn die Betroffenen von der Datenerhebung nur unerheblich betroffen werden und anzunehmen ist, dass sie kein Interesse an der Benachrichtigung haben.[515]

Diese Anforderungen gemäß dem BVerfG werden in den neuen Regelungen umgesetzt. Vor allem ist die Erhebung der Vorratsdaten nach den neuen Regelungen dem strengen Richtervorbehalt zu unterliegen. Die Entscheidungsformel wird ferner speziell für Erhebung der Vorratsdaten und auch Funkzelleabfragen differenziert geregelt. Darüber hinaus wird die Möglichkeit der Eilanordnung durch die Staatsanwaltschaft bei Gefahr im Verzug bei der Erhebung der Vorratsdaten ausgeschlossen. Die Voraussetzung für Unterbleiben der Benachrichtigung verweist nach der neuen Regelung auf allgemeine Verfahrensregelung in § 101 Abs. 4 Satz 3 StPO. Das Unterbleiben und die Zurückstellung der Benachrichtigung muss unter richterlicher Kontrolle liegen.

Im Vergleich mit der früheren Umsetzungsregelung trägt die neue Regelung dem Gebot des effektiven Rechtsschutzes verbessert Rechnung. Die früheren Regelungen wurden kritisiert, weil es an einem Sanktionssystem fehlt, *„das Verstößen gegen die Datensicherheit kein geringeres Gewicht beimisst als Verstößen gegen die Speicherungspflichten selbst.“*[516] Als Erfüllung dieser Anforderung können Verstöße gegen Verpflichtungen zur Datensicherheit mit einer Geldbuße geahndet werden.[517] Somit trägt die neue Regelung bezüglich der Sanktionen den Anforderungen des BVerfG Rechnung.

---

512 BVerfGE 125, 260 (338).
513 BVerfGE 125, 260 (334 f.).
514 BVerfGE 125, 260 (336 f.).
515 BVerfGE 125, 260 (337).
516 BVerfGE 125, 260 (351).
517 Gesetzentwurf der Fraktionen der CDU/CSU und SPD, Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, BT-Drs. 18/5088, 09.06.2015, S. 44.

6. Zusammenfassung und Bewertung

Zusammenfassend hat die modifizierte Vorratsdatenspeicherung die Anforderungen aus den einschlägigen Urteilen des BVerfG und EuGH beachtet und in großen Teilen entsprechend umgesetzt.[518] Dazu gehören insbesondere die Regelung über den Schutz der Berufsgeheimnisträger, die Gewährleistung der Datensicherheit, den strengen Richtervorbehalt und die Entschädigung. Trotz der neuen strengeren Ausgestaltung stellt die neue Vorratsdatenspeicherung im Grunde immer noch eine unterschiedslose und anlasslose Speicherung der Verkehrsdaten aller Bürger dar, die vom EuGH ausdrücklich untersagt wurde. Insoweit liegt also auch bei den neuen Vorgaben immer noch das Problem ihrer Vereinbarkeit mit den europäischen Grundrechten vor. Darüber hinaus ist die Verfassungsmäßigkeit der neuen Regelung zudem insoweit fragwürdig, als sie immer noch anlasslos und verdachtsunabhängig durchgeführt wird. Auch ist ihre positive Wirkung auf Strafverfolgung und Gefahrenabwehr nicht hinreichend bewiesen.[519]

Zwar kann die Ungültigkeit und somit die Aufhebung der Richtlinie der Vorratsdatenspeicherung die Mitgliedstaaten nicht hindern, neue nationale Regelungen der Vorratsdatenspeicherung zu erlassen.[520] Aber statt nur eine Neuauflage des alten Modells einzuführen, hätte der Gesetzgeber nach dem Ungültigkeitsurteil des EuGH das Konzept einer flächendeckenden und verdachtsunabhängigen Vorratsspeicherung neu evaluieren sollen.[521] Die vorhandenen Vorgaben sind nun dringlich nach dem Maßstab aus dem Urteil des EuGH zu messen und an seinen Anforderungen anzupassen.[522]

IV. EuGH-Urteil zu nationalen Regelungen in Schweden und Großbritannien: Verbot der nationalen Regelung über unterschiedslose Speicherung der Verkehrsdaten

Trotz der im vorigen Abschnitt dargestellten Bedenken gegen die Vereinbarkeit der jetzigen Ausgestaltung der Vorratsdatenspeicherung mit den europäischen Grundrechten wird teilweise gar eine Ausweitung der Vorratsdatenspeicherung in Deutschland politisch gefordert.[523] Es muss dabei jedoch auf

---

518 Ähnlich siehe *Roßnagel*, NJW 2016, 533 (538); *Heißl*, DÖV 2016, 588 (594).
519 Vgl. *Dix*/*Kipker*/*Schaar*, ZD 2015, 300 (300).
520 Siehe auch *Priebe*, EuZW 2014, 456 (459).
521 Vgl. *Dix*/*Kipker*/*Schaar*, ZD 2015, 300 (301).
522 Siehe auch *Simitis*, NJW 2014, 2158 (2160).
523 Berliner Erklärung der Innenminister und -senatoren von CDU und CSU zu Sicherheit und Zusammenhalt in Deutschland, 19. August 2016, abrufbar unter: http://www.regierung-mv.de/serviceassistent/_php/download.php?datei_id=1577972

das Konzept einer allgemeinen und unterschiedslosen Vorratsspeicherung ganz verzichtet werden, wie der EuGH in seinem Richtlinienurteil und im in diesem Abschnitt zu besprechenden Urteil zum Thema der Vorratsdatenspeicherung vom 21. Dezember 2016 eine allgemeine und unterschiedslose Vorratsdatenspeicherung in den Mitgliedstaaten nochmals betont hat.[524] In diesem Urteil hat der Gerichtshof die Aussagen aus der Entscheidung über die Vorratsdatenspeicherungsrichtlinie im Wesentlichen wiederholt bzw. konkretisiert. Im Ergebnis wird durch dieses Urteil der oben festgestellte Befund der EU-Grundrechtswidrigkeit der deutschen Regelungen bekräftigt.

1. Zugrunde liegende Sachverhalte

Dem Urteil liegen zwei Rechtssachen zugrunde. In der Rechtssache C-203/15 klagte ein schwedischer Telekommunikationsdienstleister beim Stockholmer Verwaltungsgericht gegen eine Verfügung der Post- und TK-Behörde. Diese stützte sich auf die §§ 16-16f des schwedischen Gesetzes für elektronische Kommunikation, das die Vorratsdatenspeicherung für sechs Monate vorschrieb. Das Verwaltungsgericht legte dem EuGH die Frage vor, ob diese Regelung europakonform sei. Der zweiten Rechtssache, C-698/15, geht ein Rechtsstreit von drei Bürgern mit dem britischen Innenminister voran. Es geht um die Vereinbarkeit der Section 1 des Data Retention and Investigatory Powers Act 2014 mit dem Unionsrecht. Die Norm erlaubte es dem Innenminister ohne Zustimmungs- oder Genehmigungserfordernis, Telekommunikationsdienstleistern die Pflicht zur zwölfmonatigen Vorratsdatenspeicherung aufzuerlegen. Auch hier ging es beim EuGH darum, ob diese Regelung mit dem EU-Recht vereinbar ist.

2. Aussagen des EuGH

Wegen der Ungültigkeit der Richtlinie 2006/24/EG fällt die nationale Gesetzgebung einer Vorratsdatenspeicherung wieder in den Geltungsbereich des Art. 15 der Richtlinie 2002/58/EG.[525] Gemäß Abs. 1 dieser Vorschrift können die Mitgliedstaaten Rechtsvorschriften erlassen, die die Vertraulichkeit

---

[31.1.2019].

524 EuGH, Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 vom 21.Dezember 2016. NJW 2017, 717; ZD 2017, 124; EuZW 2017, 153; DVBI 2017, 177; DuD 2017, 187; NVwZ 2017, 1025; ZUM 2017, 414. Anmerkung dazu siehe *Roßnagel*, NJW 2017, 696; *Frenz*, DVBI 2017, 183; *Sandhu*, EuR 2017, 453; *Kipker*/*Schefferski*/*Stelter*, ZD 2017, 131.

525 Siehe auch *Boehm*/*Cole*, 2014, S. 47; *Roßnagel*, MMR 2014, 372 (376); *Kunnert*, DuD 2014, 774 (778); *Boehm*/*Cole*, ZD 2014, 553 (555); *von Danwitz*, DuD 2015, 581 (583); *Boehm*/*Andrees*, CR 2016, 146 (146); *Heißl*, DÖV, 2016, 588 (589); *Priebe*, EuZW 2014, 456 (458).

der Kommunikation beschränken, sofern eine solche Beschränkung für die nationale Sicherheit, die öffentliche Sicherheit und die Verhütung und Verfolgung von Straftaten erforderlich ist. Die Vorschrift sieht als Maßnahme zur Beschränkung der Vertraulichkeit der Kommunikation die Aufbewahrung von Daten vor, erkennt jedoch auch als Grenze einer solchen Regelung den Grundsatz der Verhältnismäßigkeit. Wegen der Relevanz der Verarbeitung personenbezogener Daten falle eine Regelung zur Speicherungspflicht der elektronischen Kommunikationsdienstanbieter in den Geltungsbereich.[526] Ebenfalls fällt eine Regelung des Zugangs der nationalen Behörden zu den Vorratsdaten in den Geltungsbereich des Art. 15 Abs. 1 der Richtlinie.[527]

Der EuGH ermächtigt die Mitgliedstaaten im Urteil von 2017 zum Erlass von Vorschriften über die Aufbewahrung von Daten zum Zweck der Kriminalitätsbekämpfung nur unter engen Voraussetzungen. Zwar erlaube Art. 15 Abs. 1 der e-Privacy Richtlinie den Mitgliedstaaten, Ausnahmen von der Schutzpflicht der Vertraulichkeit der Kommunikation und der damit verbundenen Verkehrsdaten aus Art. 5 Abs. 1 der Richtlinie vorzusehen, aber die Regelung des Art. 15 Abs. 1 sei im Licht der von der Charta garantierten Grundrechte nach der ständigen Rechtsprechung des Gerichtshofs eng auszulegen.[528] Der EuGH hat wiederum die besonders schwerwiegende Eingriffsintensität der Vorratsdatenspeicherung mit ähnlichen Begründungen wie im Ungültigkeitsurteil zur Richtlinie 2006/24/EG dargestellt.[529]

Der EuGH legt den Art. 15 Abs. 1 so aus, dass er im Lichte von Art. 7, 8 und 11[530] sowie Art. 52 Abs. 1 GRCh einem Mitgliedstaat nicht untersage, eine vorsorgliche gezielte Vorratsspeicherung der Verkehrs- und Standortdaten zur Bekämpfung der schweren Straftaten zu erlassen, sofern sie hinsichtlich Datenkategorien, Kommunikationsmittel, Umfang der betroffenen Personen und Speicherungsdauer auf das absolut Notwendige beschränkt sei.[531] Auch sei eine geografische Beschränkung in Bezug auf die betroffenen Personen an-

526 EuGH, Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 vom 21. Dezember 2016, Rn. 75.

527 EuGH, Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 vom 21. Dezember 2016, Rn. 76.

528 EuGH, Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 vom 21. Dezember 2016, Rn. 88 ff.

529 EuGH, Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 vom 21. Dezember 2016, Rn. 97-101. Vgl. Sandhu, EuR 2017, 453 (459 f.).

530 Im Urteil zur Richtlinie hat sich der EuGH die Vereinbarkeit mit Art. 11 GRC offengelassen („Unter diesen Umständen ist die Vereinbarkeit der Richtlinie 2006/24/EG mit Art. 11 der Charta nicht zu prüfen." Rn. 11). Im Urteil von 2017 äußert sich der EuGH näher zur Vereinbarkeit mit der Meinungsfreiheit Rn. 92 f.

531 EuGH, Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 vom 21. Dezember 2016, Rn. 108.

gezeigt. In den Ausführungen zu den Differenzierungsmerkmalen liegt der Schwerpunkt dieses Urteils. Bei einer vorsorglichen gezielten Vorratsspeicherung sei zudem ein Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel erforderlich.[532] Die Durchführung einer gezielten Vorratsspeicherung müsse sich auf objektive Anknüpfungspunkte stützen, das heißt, dass der Personenkreis damit bestimmt werden könnte, die zu speichernden Daten geeignet sein müssten, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern.[533]

Der EuGH hat außerdem bei der Begrenzung des Zugangs und der Verwendung der Vorratsdaten weiterhin klargestellt, dass vor allem der Zugang strikt einem der in Art. 15 Abs. 1 Satz 1 der Datenschutzrichtlinie genannten Zwecke dienen müsse und angesichts der schwerwiegenden Eingriffsintensität dieser Maßnahme vermöge im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nur die Bekämpfung der schweren Straftaten einen solchen Zugang zu den Vorratsdaten zu rechtfertigen.[534]

Anschließend sei grundsätzlich der Zugang zu den Daten von Teilnehmern oder registrierten Nutzern zu gewähren, nur in besonderen Situationen könnte der Zugang zu Daten der anderen Daten ebenfalls gewährt werden.[535] Zudem sei der Zugang zu den Vorratsdaten grundsätzlich einer vorherigen Kontrolle entweder durch ein Gericht oder eine unabhängige Verwaltungsstelle zu unterwerfen, ausnahmsweise nur bei hinreichend begründeten Eilfällen.[536] Schließlich müsse die nationale Regelung insbesondere vorsehen, dass die Daten im Unionsgebiet zu speichern und nach Ablauf ihrer Speicherungsfrist unwiderruflich zu vernichten seien.[537] Bezüglich der Bestimmtheit der nationalen Regelung zur Vorratsspeicherung, der materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang zu den Vorratsdaten sowie der wirksamen Vorkehrung gegen Missbrauchsrisiken und unberechtigten Zugriff

---

532 EuGH, Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 vom 21. Dezember 2016, Rn. 110.

533 EuGH, Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 vom 21. Dezember 2016, Rn. 111.

534 EuGH, Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 vom 21. Dezember 2016, Rn. 115.

535 EuGH, Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 vom 21. Dezember 2016, Rn. 119.

536 EuGH, Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 vom 21. Dezember 2016, Rn. 120.

537 EuGH, Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 vom 21. Dezember 2016, Rn. 122.

der gespeicherten Daten wiederholt der EuGH im Grunde genommen seine im Urteil am 8 April 2014 formulierten Anforderungen.[538]

3. Bedeutung des Urteils für nationale Regelungen insbesondere für Deutschland

Der EuGH hat durch die jüngste Entscheidung in erster Linie eine nationale Regelung der unterschiedslosen und anlasslosen Speicherung allumfassender Telekommunikationsdaten auf Vorrat aller Bürger ausdrücklich verboten. Jedoch wird den Mitgliedstaaten ein Regelungsspielraum für eine vorsorgliche gezielte Vorratsspeicherung der Telekommunikationsdaten überlassen. Mitgliedstaaten, die eine Vorratsdatenspeicherung weiterhin beabsichtigen, müssen die Anforderungen an eine Vorratsdatenspeicherung, die der EuGH in diesem Urteil präzisiert, berücksichtigen.[539] Die Erforderlichkeit von objektiven Anknüpfungspunkten zwischen den zu speichernden Daten und der Verfolgung von schweren Straftaten sowie der Gefahrenabwehr verringert das Defizit der Anlasslosigkeit und Verdachtsunabhängigkeit der allgemeinen Vorratsdatenspeicherung. Eine solche Vorratsspeicherung ist zulässig und kann gerechtfertigt sein, sofern ihr Eingriff nach den Anforderungen des EuGH auf das absolut Notwendige beschränkt wird.[540] Es besteht kein Zweifel, dass eine allgemeine verdachtsunabhängige Vorratsdatenspeicherung sowohl auf europäischer als auch auf nationaler Ebene wegen der Unvereinbarkeit mit den europäischen Grundrechten keine Zukunft hat.[541]

Die vorhandene Regelung der Vorratsdatenspeicherung in Deutschland ist, wie oben bereits ausgeführt,[542] mit den europäischen Grundrechten nicht vereinbar.[543] Sie ist wegen des Verstoßes gegen europäische Grundrechte aufzuheben, wenngleich sie strenger als früher gemäß den Maßstäben des EuGH und des BVerfG ausgestaltet worden ist.[544] Das Oberverwaltungsge-

---

538 EuGH, Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15 vom 21. Dezember 2016, Rn. 109 f.

539 Siehe auch *Sandhu*, EuR 2017, 453 (466).

540 Vgl. *Bär*, NZWiSt 2017, 81 (86); *Sandhu*, EuR 2017, 453 (461 ff.).

541 So auch *Sandhu*, EuR 2017, 453 (461); *Derksen*, NVwZ 2017, 1005 (1009); *Priebe*, EuZW 2017, 136 (139); *Ziebarth*, ZUM 2017, 398 (405).

542 Siehe Kapitel 2, C.III.6.

543 Siehe auch Ausarbeitung zur Vereinbarkeit des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten mit dem EuGH-Urteil vom 21. Dezember 2016 zur Vorratsdatenspeicherung von der Unterabteilung Europa (Fachbereich Europa), 12.01.2017, Aktenzeichen: PE 6 – 3000 – 167/16, S. 24; *Ziebarth*, ZUM 2017, 398 (404).

544 Vgl. *Roßnagel*, NJW 2017, 696 (698); *Ziebarth*, ZUM 2017, 398 (405); *Kunnert*, DuD 2014, 774 (783).

richt Nordrhein-Westfalen im Beschluss vom 22. Juni 2017 hat klar geäußert, dass die neue Ausgestaltung der Vorratsdatenspeicherung nach dem Ungültigkeitsurteil des EuGH vom 21. Dezember 2016 mit dem Recht der Europäischen Union nicht vereinbar sei.[545] Das könne als ein vorläufiges Signal vor dem Hauptsacheverfahren angesehen werden.[546]

4. Ausblick

Bei den anspruchsvollen Anforderungen des EuGH besteht das Problem, dass eine entsprechende Vorratsspeicherung in der Praxis nur schwierig, vermutlich kaum realisiert werden kann.[547] Es wird auch angezweifelt, dass die neue Vorratsdatenspeicherung tauglich bleibe, weil die konkrete Gefahr als erforderliche Voraussetzung einer zulässigen Vorratsspeicherung für Gefahrenabwehr erfüllt werden müsse.[548] Bei manchen Fällen im Bereich der Gefahrenabwehr, in denen etwa ein Terroranschlag spontan und unberechenbar begangen wird, könnte eine Durchführung der Maßnahme nach der Feststellung einer konkreten Gefahr für Schutz der öffentlichen Sicherheit vor derjenigen Gefahr zu spät sein.[549] Hierzu wurde berichtet, dass die Abwehr einer konkreten Gefahr mangels Verkehrsdaten nicht gelungen sei.[550] Gegen diese Behauptung spricht jedoch, dass auch die jahrelang geübte flächendeckende Vorratsspeicherung Terroranschläge keineswegs komplett verhindern konnte.[551]

Nun ist die abschließende Entscheidung des BVerfG zu den nationalen Vorschriften der Vorratsdatenspeicherung abzuwarten. Eine gezielte Vorratsspeicherung in den Mitgliedstaaten ist zwar zulässig. Wie eine solche Vorratsspeicherung konkret ausgestaltet wird, ist den Mitgliedstaaten überlassen. Die Option einer gezielten Vorratsdatenspeicherung bleibt dem deutschen Gesetzgeber noch offen, jedoch muss eine eventuelle Regelung die strengen Anforderungen einer zulässigen Vorratsspeicherung aus dem EuGH wegen des Verhältnismäßigkeitsprinzips einhalten. Es ist zu vermuten, dass auf europäischer Ebene eine neue Richtlinie über eine gezielte Vorratsspeicherung erlassen wird, um einen einheitlichen Ausgestaltungsrahmen aufzustellen.[552]

---

545 Oberverwaltungsgericht Münster, Beschluss v. 22.06.2017, Az. 13 B 238/17; so auch VG Köln, Urt. v. 20.4.2018, 9 K 7417/17.

546 *Gola*/*Klug*, NJW 2017, 2593 (2594).

547 *Sandhu*, EuR 2017, 453 (462 ff.); *Frenz*, DVBI 2017, 183 (185 f.); *Priebe*, EuZW 2017, 136 (139).

548 *Frenz*, DVBI 2017, 183 (185); *Nachbaur*, ZRP 2015, 215 (216).

549 *Frenz*, DVBI 2017, 183 (185).

550 *Albrecht*/*Kilchling*, S. 140, 146, 225.

551 *Albrecht*/*Kilchling*, S. 219.

552 Vgl. *Priebe*, EuZW 2017, 136 (139).

V. Zusammenfassung

Mit Blick auf die verschärfte Bedrohungslage durch Terrorismus und Cyberkriminalität wird der Freiheitsraum der Bürger durch immer mehr und strengere Sicherheitsmaßnahmen bedrängt. Es ist für den Gesetzgeber eine große Herausforderung, die Balance zwischen Sicherheit und Freiheit zu finden. Dafür muss die Ausgestaltung aller Sicherheitsmaßnahmen die verfassungsrechtlichen Anforderungen, insbesondere das Verhältnismäßigkeitsprinzip, einhalten.

Die Vorratsdatenspeicherung wird als eine vielversprechende Sicherheitsmaßnahme immer wieder vorgeschlagen, als ob sie der einzige Ausweg wäre, die Allgemeinheit gegen Terrorismus und schwere Kriminalität abzusichern. Das Aussparen der Inhaltsdaten der Telekommunikation und die vom Staat unabhängigen Verpflichteten lassen die fragliche Maßnahme harmlos, jedoch wirksam aussehen. Ihre Verfassungsmäßigkeit ist deswegen nicht als Entweder-Oder Frage zu beantworten.

Aber die Vorratsdatenspeicherung ist ihrem Wesen nach eine Überwachung der Telekommunikation *aller* Bürger. Wegen der zentralen Bedeutung der Telekommunikation für die Bürger in der heutigen Gesellschaft kann die negative Wirkung aus der Überwachung dieser Telekommunikation als hoch eingeschätzt werden. Die Wirkung der Maßnahme beschränkt sich auch nicht nur auf das Fernmeldegeheimnis der Bürger. Die Überprüfung der Verfassungsmäßigkeit der Vorratsdatenspeicherung ist besonders vorsichtig durchzuführen. Ansonsten würde ein fast unmerklicher aber entscheidender Schritt hin zur totalen Überwachungsgesellschaft gemacht.

In der Entwicklungsgeschichte der Vorratsdatenspeicherung haben das BVerfG und der EuGH ihre wesentliche Rolle als Hüter der Grundrechte ausgespielt. Das BVerfG hat zwar die Vorratsdatenspeicherung nicht abgelehnt, aber dem Gesetzgeber sehr hohe Hürden dafür gesetzt und Zurückhaltung bei weiterer vorsorglicher anlassloser Vorratsspeicherung gefordert. Der EuGH hat eine unterschiedslose Speicherung der Telekommunikationsdaten aller Bürger ausdrücklich verboten und wenig Raum für eine vergleichbare Vorratsspeicherung anderer personenbezogener Daten zugelassen. Von beiden Entscheidungen wurden rechtsstaatliche Hürden für die Vorratsdatenspeicherung aber auch für künftige vergleichbare Maßnahmen aufgestellt. Der Ge-

setzgeber muss die Anforderungen aus den Entscheidungen bei künftigen Gesetzgebungsvorhaben beachten.

Kapitel 3: Die Vorratsdatenspeicherung in China

A. Hintergründe und Vorgaben der Vorratsdatenspeicherung in der Volksrepublik China

Die Maßnahme der Vorratsdatenspeicherung wird auch in der Volksrepublik China (VR China) ergriffen und zielt ebenfalls, wie in Deutschland, auf Strafverfolgung und Gefahrenabwehr ab. Trotz des mit der EU vergleichbaren Zwecks werden den zuständigen Behörden durch die Regelungen zur Speicherung von Vorratsdaten jedoch viel weitgehendere Befugnisse erteilt. Wegen der sehr umfangreichen Speicherung der Telekommunikationsverkehrsdaten und unbeschränkten Verwendung der Vorratsdaten stellt die Maßnahme einen besonders gravierenden Eingriff in das Korrespondenzgeheimnis der Bürger dar. Zunächst werden die Hintergründe und die Vorgaben der Vorratsdatenspeicherung in der VR China dargestellt. Im Anschluss daran geht es um eine verfassungsrechtliche Bewertung der Regelungen. Zum Schluss sollen Möglichkeiten zur Verbesserung des Schutzniveaus für die Bürger herausgearbeitet werden. Hierbei soll eine Orientierung an den Vorgaben des EuGH und des BVerfG stattfinden.

I. Hintergründe der Vorratsdatenspeicherung in der VR China

Der Terrorismus ist ein weltweites Problem. Die VR China ist wie viele andere Länder der Bedrohung des Terrorismus ausgesetzt. Wie der Terrorismus effektiv zu bekämpfen ist, ist aktuell eine der dringlichsten Aufgaben der Sicherheitsgesetzgebung.[553] Zu bekämpfen ist darüber hinaus die neue Form der Kriminalität *„Cybercrime“*.[554] Aber auch die Begehung von traditioneller schwerer Kriminalität wird durch die Ausnutzung der neuen Informations- sowie Telekommunikationstechnologien erleichtert.

Parallel zur Bekämpfung des Terrorismus und der Kriminalität ist die Wahrung der Cyber-Sicherheit ein weiterer Schwerpunkt der Sicherheitspolitik der VR China. Beide sind für die Staatssicherheit sowie die öffentliche Sicherheit relevant.[555] Unter der Cyber-Sicherheit versteht man nicht nur die

---

553 Vorschläge zur Gesetzgebung sowie Bekanntmachung des Gesetzgebungsplans 2005 vom Staatsrat (关于做好国务院 2005 年立法工作的几点意见和国务院 2005 年立法工作计划的通知), Dokument aus dem Staatsrat, 2005, 3. In diesem Dokument werden die Erlasse des Antiterrorismusgesetzes und der Überarbeitung des Staatssicherheitsgesetzes erfasst.

554 *Yu*, Peking University Law Journal 2014/4, S. 1050; *Yu*, Journal of CUPL, 2015/4, S. 43; *Pi*, Chinese Legal Science 2003/4, S. 148.

555 *Xie*/*Yu*, S. 1 ff.; *Rao*, 2005, S. 59 ff.; *Ma*, 2007, S. 2 ff.; *Yu*, Legal Forum 2014/6,

physische Sicherheit der Informationsinfrastrukturen, die Sicherheit der Funktion der informationstechnischen Systeme und die Datensicherheit, sondern auch die Sicherheit des Inhalts im Internet, was die Behinderung sowie Beseitigung der illegalen Informationen im Internet impliziere.[556] In § 57 „Telekommunikationsregeln der VR China" werden 9 Typen der illegalen Informationen aufgelistet, jede Veröffentlichung, jedes Kopieren und Weitergeben sowie jede Verbreitung der illegalen Informationen ist verboten.

Vor diesem Hintergrund sind seit 2000 mehrere Sicherheitsgesetze und Verordnungen erlassen worden. In ihnen wird vorgeschrieben, umfangreiche personenbezogene Daten der Bürger vorrätig zu speichern, und diese später bei Bedarf zu verwenden. Dies ist nicht neu in der VR China. Zum Beispiel läuft seit Langem das scharf kritisierte System der Personalakte (Dang'an 档案). In diesem System werden zahlreiche personenbezogene Daten, einschließlich hochsensibler Daten der Bürger, im Namen der Regierung und Verwaltung protokolliert. In Bezug auf diese Akte hat der Bürger kein Recht auf Auskunft, Berichtigung, Löschung und Widerspruch.[557] Bis jetzt liegt keine spezielle Regelung für die Sammlung, Bewahrung sowie Verwendung der Personalakte vor. Der Bürger hat weder die Möglichkeit zu erfahren, ob, für welchen Zweck und inwiefern seine Personalakte von der befugten/unbefugten Stelle verwendet wird, noch einen Rechtsweg, sich vor der unbefugten Verwendung wirksam zu schützen.[558] In diesem System wird nur sehr wenig Raum für die Privatsphäre der Bürger gelassen.

Die Entwicklung der Informationstechnologie hat die staatliche Sammlung und Verwendung personenbezogener Daten erheblich erleichtert. Im Jahr 1982 wurden die in der dritten Volkszählung erhobenen personenbezogenen Daten zum ersten Mal vollumfänglich durch Computer verarbeitet.[559] Seitdem wurden zahlreiche Datenbanken zur Wahrnehmung staatlicher Aufgaben in den Bereichen von Volkszählung, öffentlicher Sicherheit, sozialer Sicherung, Gesundheitswesen und öffentlichem Personalwesen geplant und nacheinander aufgebaut.[560] Die Befugnis zur Sammlung sowie Verwendung per-

S. 5 f.

556 *Rao*, 2005, S. 59 f.; *Yu*, Legal Forum 2014/6, S. 7.

557 *Guo*, 2012, S. 11, Zum chinesischen System der Personalakte siehe *Chen*, 2007; *Liu*, 2013; *Zhang*, Archives Science Study 2009/3.

558 *Li*, Beijing Archives 2010/2, S. 17 f.

559 *Sun*, Legal Science 2007/7, S. 24.

560 Zur Geschichte der Entstehung und Entwicklung der staatlichen Datenbank der VR China siehe *Sun*, Legal Science 2007/7, S. 24 ff.; *Zhang*, 2011, S. 94 ff.; *Lü*, 2009, S. 135 f.

sonenbezogener Daten wird im Namen des öffentlichen Interesses immer wieder erweitert. Dies hat zwar ermöglicht, dass der Staat öffentliche Dienstleistungen besser anbieten kann, führt aber auch dazu, dass der Bürger vor dem Staat keine Privatsphäre mehr hat.[561]

In der VR China war die Entwicklung der Informations- sowie Kommunikationstechnologien in vielen Bereichen lange Zeit eher rückständig. Die Anwendung der neuen Technologien verbreitete sich langsam. In den letzten zwanzig Jahren hat sich dies jedoch in erstaunlich rasantem Tempo verändert. Bis zum Dezember 2016 betrug die Zahl der Nutzer von Festnetztelefonen 207 Millionen, der Nutzer von Mobiltelefonen 1,32 Milliarden und der Nutzer des Internet 731 Millionen.[562] Wegen der vielfältigen Anwendungsmöglichkeiten der Telekommunikationstechnologien ist die Abhängigkeit von der Nutzung der Telekommunikationsmittel, insbesondere des Mobiltelefons, schnell angewachsen. Nutzer des Mobilfunknetzes machen 95.1% aller Internetnutzer aus und zwar 695 Millionen. Sie kommunizieren mit Kurznachrichtendiensten (91.8% der Mobiltelefonnutzer), recherchieren (82.2%), bezahlen (67.5%), kaufen ein (63.4%), nutzen Online-Banken (48.0%), bestellen Essen (27.9%) und reservieren Taxis (24.17%).[563] Die Nutzung des Mobilfunknetzes ist aus dem Leben vieler Bürger heute nicht mehr wegzudenken. Vermutlich trifft dies sogar in der VR China noch mehr zu als in Deutschland und der EU.

Bei der Benutzung verschiedener Telekommunikationsdienste entsteht somit eine große Menge an personenbezogenen Daten, durch die Bewegungen und Handlungen der Bürger präzise und detailliert rekonstruiert werden können. Die Speicherung und Verwendung solcher Daten durch den Staat effektiviert einerseits die Wahrnehmung staatlicher Aufgaben, andererseits droht aber die Entwicklung eines Überwachungsstaats.[564] Vor dem Hintergrund der weltweit verschärften Bedrohungslage dürfen immer umfangreichere personen-

---

561 *Rao*, 2005, S. 118 f.

562 Statistik der Telekommunikationsindustrie 2016 vom Ministerium für Industrialisierung und Information, abrufbar unter: http://www.miit.gov.cn/n1146312/n1146904/n1648372/c5498087/content.html [31.1.2019]; 39. Statistik und Bericht der Entwicklung des Internets in der VR China vom China Internet Network Information Center, 1. 2017, S. 1, abrufbar unter: http://www.cnnic.net.cn/gywm/xwzx/rdxw/20172017/201701/t20170122_66448.htm [31.1.2019].

563 39. Statistik und Bericht der Entwicklung des Internets in der VR China vom China Internet Network Information Center, 1. 2017, S. 48, abrufbar unter: http://www.cnnic.net.cn/gywm/xwzx/rdxw/20172017/201701/t20170122_66448.htm [31.1.2019].

564 *Zhao*, Journal of Comparative Law 2017/2, S. 35 f.

bezogene Daten durch die Sicherheitsgesetzgebung erhoben und verwendet werden. Die Privatsphäre ist so einem noch größeren Risiko ausgesetzt. Der zunächst verstärkte Schutz der individuellen Freiheitsrechte, der zum großen Teil mit Hilfe der Entstehung sowie Entwicklung des Internets gefördert worden ist,[565] wird nun auf eine harte Probe gestellt.

II. Vorgaben der Vorratsdatenspeicherung in der VR China

Im Vergleich zu Deutschland ist der Umfang der Vorratsdatenspeicherung in der VR China weitaus größer. Die materiellen Voraussetzungen des Abrufs und der Verwendung werden nicht grundrechtschonend ausgestaltet und lassen den Betroffenen kaum Möglichkeiten, seine Grundrechte zu wahren. Eigentlich ist die Verwendung des Begriffs der Vorratsdatenspeicherung im chinesischen Kontext deshalb zweifelhaft. Der Begriff ist dort angezeigt, wo der Grundsatz in der Löschung der Daten besteht. Stellt die Speicherung den Normalfall dar, so erscheint der Begriff der Vorratsdatenspeicherung nicht unbedingt passend. Für eine bessere Verständlichkeit soll aber auch im Folgenden der Begriff der Vorratsdatenspeicherung verwendet werden. Gemeint ist damit die Speicherung von Daten. Nichtsdestoweniger gilt in der VR China die Vorratsdatenspeicherung auch als Sicherheitsmaßnahme wie in Deutschland. Sie stellt ebenso eine Ausnahme dar wie in der EU. Der Unterschied besteht somit mehr im Umfang als in grundsätzlicher Hinsicht. Im Folgenden werden die Regelungen für die Vorratsdatenspeicherung in China vorgestellt.

1. Relevante Rechtsquellen: Gesetz, Verordnung, Regel, Methode

Bislang besteht weder ein förmliches, einheitliches Telekommunikationsgesetz noch ein Telemediengesetz. Maßgebende Rechtsnormen sind zwei Verordnungen vom Staatsrat: die „Telekommunikationsregeln der VR China“ und die „Verwaltungsmethode für Internetinformationsdienste der VR China“. Die Telekommunikationsregeln stellen eine allgemeine Regelung über Telekommunikationsdienste dar und letztere hauptsächlich Regelungen über Telemediendienste. „Internetinformationsdienste“ ist eine wörtliche Übersetzung von „互联网信息服务 (hulianwang xinxi fuwu) “, was eine allgemeine Bezeichnung für Telemediendienste, insbesondere Inhalte-Provider, ist. In der VR China werden Telekommunikationsdienste nicht streng von Telemediendiensten unterschieden. Außer diesen beiden Rechts-

[565] Dazu siehe beispielweise *Hu*, 2008; *Qiu*/*Chen*, 2011; *Wu*, Contemporary Communication 2015/1, S. 17 ff.

quellen werden eine Reihe von Verordnungen und andere Regelwerke je nach Typen von Diensten erlassen. Nach § 80 Abs. 1 Gesetzgebungsgesetz der VR China (GGebG VRC) können Ministerien und Ausschüsse des Staatsrates per Beschluss und Erlass regelnd bzw. gesetzgebend tätig werden. Innerhalb des Zuständigkeitsbereichs einer jeweiligen Ministeriumsabteilung werden zudem typischerweise „Abteilungsregeln" erlassen. Diese können auch die Bezeichnung „Methode" (办法 „banfa") oder Regel (规定 „guiding") tragen. Verordnungen gehen Abteilungsregeln nach § 88 GGebG VRC vor. Wegen der regelmäßig gegebenen hohen Abstraktheit von Gesetzen und Verordnungen in der VR China dienen Abteilungsregeln de facto als wichtigste Rechtsquelle. Statt die Speicherungspflichten allgemein zu regeln, sind sie in verschiedenen Verordnungen und Abteilungsregeln verstreut. Einige dieser Regelungen sollen im Folgenden vorgestellt werden.

2. Speicherungspflicht

a) Verwaltungsmethode für E-Mail Dienste (互联网电子邮件管理办法)

Die Verwaltungsmethode für E-Mail Dienste (VM-E-Mail) wurde vom Ministerium für Industrie und Informationstechnologie am 7.11.2005 erlassen und trat am 20.3.2006 in Kraft. Gemäß § 10 VM-E-Mail sind die Anbieter der E-Mail Dienste verpflichtet, die Zeitpunkte der Versendung und des Empfangs, E-Mail Adresse und IP-Adresse des Absenders und Empfängers für 60 Tage zu speichern. Zudem haben die Anbieter sicherzustellen, dass die gespeicherten Daten für den Fall einer befugten Abfrage von zuständigen Behörden zur Verfügung gestellt werden.

b) Verwaltungsregel für SMS-Dienste (通信短信息服务管理规定)

Die Verwaltungsregel für SMS-Dienste (VR-SMS) wurde vom Ministerium für Industrie und Informationstechnologie am 6.5.2015 erlassen und trat am 30.6.2015 in Kraft. Hauptanliegen dieser Verwaltungsregel ist es, Spam-Nachrichten zu verhindern. SMS-Dienste meint dabei alle Übermittlungsdienste in Form von Text, numerischer Daten, Sprache, Abbildung oder sonstige Nachrichten in irgendwelcher Form (§ 37 Nr. 1 VR-SMS). Gemäß § 11 VR-SMS müssen die SMS-Dienstanbieter die Zeitpunkte der Versendung und des Empfangs der Nachrichten, Telefonnummer oder Kennung der absendenden und empfangenden Anschlüsse, An- und Abmeldung von Newslettern sowie die Inhalte der port-to-point Nachrichten speichern. Wäh-

rend point-to-point Nachrichten von einem Handy zu einem anderen Handy gesendet werden, werden port-to-point Nachrichten von einem Unternehmen, einem Dienstanbieter oder einer öffentlichen Stelle gleichzeitig an mehrere Handys gesendet. Die Protokollierung der An- und Abmeldung von Newslettern muss in der Laufzeit des Vertrags zwischen den Teilnehmern und den SMS-Dienstanbietern und nach der Beendigung des Vertragsverhältnisses fünf Monate aufbewahrt werden. Andere oben genannte Daten müssen auch mindestens fünf Monate gespeichert werden. Der Speicherungszweck wird nicht vorgeschrieben.

c) Verwaltungsmethode für Internetinformationsdienste (互联网信息服务管理办法)

Die Verwaltungsmethode für Internetinformationsdienste (VM-IInfD) wurde gleichzeitig mit den Telekommunikationsregeln vom Staatsrat erlassen und gilt als maßgebende Regelung im Telemedienbereich. Nach § 14 VM-IInfD müssen die Anbieter von Informationsdiensten im Internet, z.B. Nachrichten, Online-Ausgaben einer Zeitung oder Bulletin-Board-Service (BBS) – also Webforum-Dienste –, die angebotenen Inhalte, die Zeitpunkte der Veröffentlichung von Inhalten auf den entsprechenden Internetseiten, IP-Adressen oder Domainnamen der Nutzer für 60 Tage speichern.[566] Außerdem sind die Internetzugangsdiensteanbieter verpflichtet, den Zeitpunkt des Beginns und des Endes der Internetznutzung, den im Vertrag der Internetzugangsdienste festgelegten Kontonamen des Teilnehmers, IP-Adressen und Domainnamen der Nutzer, die Telefonnummer, wenn Internet über Telefonleitung benutzt wird, für 60 Tage zu protokollieren. Die Aufzählung der zu speichernden Daten in § 14 VM-IInfD ist zudem nicht abschließend. Die gespeicherten Daten müssen für eine befugte Abfrage von den zuständigen Staatsbehörden zur Verfügung gestellt werden.

d) Verwaltungsregeln für Video- und Audiosendungen im Internet (互联网视听节目服务管理规定)

Die Verwaltungsregeln für Video- und Audiosendungen im Internet (VR-VAI) wurden vom staatlichen Zentralamt für Rundfunk, Film und Fernsehen und Ministerium für Industrie und Informationstechnologie am 20.7.2007 erlassen und traten am 31.1.2008 in Kraft. Am 28.8.2015 wurden die VR-VAI novelliert. Nach § 16 S. 2 VR-VAI müssen die Anbieter der Dienste für Vi-

---

566 Zum Begriff Domainname siehe *Sieber*, in: *Hoeren*/*Sieber*/*Holznagel* (Hrsg.), 2014, Teil 1 Rn. 59; *Weidner-Braun*, S. 62.

deo- und Audiosendungen im Internet die eigenen oder fremden bereitgestellten Sendungen mindestens 60 Tage speichern. Der Speicherungszweck wird nicht klar festgelegt. In § 16 S. 3 VR-VAI wird geregelt, dass illegale Informationen nicht durch Video- und Audiosendungen verbreitet werden dürfen. Hieraus lässt sich systematisch auslegen, dass die genannten Daten zum Zweck des Verhinderns der Verbreitung illegaler Informationen zu speichern sind.

e) Verordnung für den Betrieb von Internet-Cafés (互联网上网服务营业场所管理条例)

Die Verordnung für den Betrieb von Internet-Cafés (VO-IC) wurde vom Staatsrat am 14.8.2002 erlassen und trat am 15.11.2002 in Kraft. Gemäß § 2 VO-IC sind Internet-Cafés gewerbliche Örtlichkeiten, in denen die Dienstleistung der Internetnutzung mittels Einrichtungen wie Rechner einem allgemeinen Publikum angeboten wird. Schulen, Universitäten und Bibliotheken, in denen Internetdienste für geschlossene Benutzergruppen angeboten werden, werden vom Anwendungsbereich ausgeschlossen. Anzumerken ist hierbei, dass Internet-Cafés in China viel weit verbreiteter sind als in Deutschland. Nach § 23 VO-IC müssen Betreiber der Internet-Cafés dafür Sorge tragen, dass der Personalausweis oder ein anderes Ausweisdokument aller Kunden kontrolliert wird, die Identitätsdaten aufgezeichnet und die Informationen über die Internetnutzung der Kunden gespeichert werden. Die Protokollierung muss mindestens 60 Tage aufbewahrt und für die befugte Abfrage von der Kulturverwaltungsabteilung und den Sicherheitsbehörden zur Verfügung gestellt werden. Es ist jedoch nicht klar, welche Daten zu den „Informationen über die Internetnutzung der Kunden“ gehören. Wird die chinesische Wortbedeutung berücksichtigt, können solche Informationen mindestens Telekommunikationsverkehrsdaten und Nutzungsdaten aus Telemediendiensten und sogar Inhaltsdaten umfassen. Um ein Internet-Café zu betrieben, muss der Betreiber die mit dem Diensteanbietern ausgestatteten Server und Software anschaffen. Vor diesem Hintergrund können Internet-Café-Betreiber die genannten Daten problemlos speichern.

f) Telekommunikationsregeln der VR China und Entwurf des Telekommunikationsgesetzes (电信条例和电信法草案)

In den vorhandenen Vorgaben besteht keine Speicherungspflicht der Verkehrsdaten aus der Telefondienstnutzung. Aber es ist nur schwer vorstellbar, dass die Verkehrsdaten in der Praxis nicht zum Zweck der Wahrnehmung

staatlicher Aufgaben auf Vorrat gespeichert werden. Aus oben aufgelisteten Vorgaben der Vorratsdatenspeicherung kann man bereits erkennen, dass eine Vorratsspeicherung bezüglich fast jedes Typs der Telemedien- sowie Telekommunikationsdiente angeordnet wird. Herrscht diese Tendenz der lückenlosen und umfassenden Vorratsspeicherung bei den Telekommunikations- sowie Telemediendiensteanbietern, ist es nahezu unmöglich, die Verkehrsdaten aus der Nutzung der Telefondienste von der Speicherungspflicht auszusparen.

Ein weiterer Grund für diesen Schluss liegt darin, dass im künftigen Telekommunikationsgesetz eine umfassende Vorratsspeicherung enthalten sein wird. Das „Telekommunikationsgesetz der VR China“ (TKG VRC) steht schon lange auf dem Gesetzgebungsagenda. Im Jahr 2004 wurde der Entwurf des Telekommunikationsgesetzes (TKG VRC-E) vom damaligen Ministerium für Informationstechnologie verfasst und dem Staatsrat vorgelegt. Bisher ist es nicht verabschiedet worden.[567] § 77 TKG VRC-E sieht vor, dass die Telekommunikationsdiensteanbieter verpflichtet sind, alle Nutzungsdaten der Benutzer mindestens 60 Tage zu speichern. Darin zeichnet sich ein eindeutiges Vorhaben ab: eine allumfassende Vorratsspeicherung einheitlich durch das Telekommunikationsgesetz durchzuführen. Problematisch ist, dass die Vorgabe höchst abstrakt ist. Es fehlt so etwa an einer Begriffsbestimmung für „alle Nutzungsdaten“. Der Speicherungszweck wird auch nicht klar festgelegt. Damit steht es nicht mit dem Bestimmtheitsangebot und Zweckfeststellungprinzip im Einklang.

g) Zwischenergebnis

Aus den vorgestellten Regelungen lassen sich die Eigenarten der Speicherungspflicht in der VR China erkennen. Es handelt sich um eine nahezu umfassende Speicherungspflicht. Es ist etwa festzustellen, dass die Speicherungspflicht nicht nur Telekommunikations- und Telemediendiensteanbieter, sondern auch Betreiber von Internet-Cafés betrifft. Hinzu kommt, dass die angebotenen eigenen und fremden Inhalte bei bestimmten Telemediendiensteanbietern zu speichern sind. Des Weiteren sind Inhalte der An- und Abmeldung für Newsletter sowie port-to-point Nachrichten zu speichern. Von den vorgestellten Regelungen können auch Grundrechte berührt werden. Betroffene Grundrechte können etwa das sogenannte Korrespondenzgeheimnis,

---

567 Der Gesetzentwurf des Telekommunikationsgesetzes wurde bisher noch nicht vom Staatsrat beraten. Die chinesische Fassung des Gesetzentwurfs ist abrufbar unter: http://www.taodocs.com/p-6363411.html [31.1.2019].

die Meinungsfreiheit und das allgemeine Persönlichkeitsrecht der Nutzer, aber auch die Berufsfreiheit und Kommunikationsfreiheit der Dienstanbieter sein (hierzu Kapitel 3, B.I.). Der Zweck von den Speicherungsmaßnahmen wird jedoch nur allgemein als „für die befugte Abfrage durch die zuständigen Staatsbehörden zur Verfügung stellen" angegeben. Oftmals besteht kein darüber hinausgehender eindeutiger Speicherungsweck. Werden die Vorgaben der Speicherungspflicht nach den Maßstäben des Bestimmtheitsgebots, des Zweckfeststellungs- und des Verhältnismäßigkeitsprinzips beurteilt, ist die Verfassungsmäßigkeit der Ausgestaltung der Speicherungspflicht in der VR China sehr fragwürdig (hierzu insbesondere Kapitel 3, B.II.).

3. Verwendung der Vorratsdaten

Beim staatlichen Zugriff auf personenbezogene Daten in Telekommunikations- sowie Telemedienbereich nehmen die vorhandenen Regelungen keine Unterscheidung zwischen den zum betrieblichen Zweck gespeicherten Daten und den auf Vorrat gespeicherten Daten vor. Die Befugnisse zum Zugriff sowie zur Verwendung personenbezogener Daten werden in den folgenden Gesetzen pauschal erteilt.

a) Strafprozessordnung der VR China (中华人民共和国刑事诉讼法)

Die Vorratsdaten dürfen zunächst zum Zweck der Aufklärung von Straftaten verwendet werden. In der Strafprozessordnung der VR China wird in § 52 vorgeschrieben, dass das Volksgericht, die Staatsanwaltschaft und die Polizeibehörde befugt sind, bei betroffenen Stellen, natürlichen und juristischen Personen Beweismaterial zu erheben und darauf zuzugreifen. Konkrete materielle Voraussetzungen des Zugriffs werden nicht geregelt. Die Befugnis des Volksgerichts zum Datenzugriff ist sehr umstritten. Denn in Art. 40 Verf VRC wird regelt, dass nur die Staatsanwaltschaft und Polizeibehörden nach einem gesetzlichen Verfahren das Korrespondenzgeheimnis der Bürger beschränken dürfen.[568]

b) Antiterrorismusgesetz der VR China (中华人民共和国反恐怖主义法)

Wegen der neuen Bedrohungslage für die öffentliche Sicherheit wurde das Antiterrorismusgesetz (ATG VRC) am 27.12.2015 erlassen und trat tags da-

568 *Li*, Modern Science & Technology of Telecommunications 2011/5, S. 40 ff.; *Sun*, Shandong Justice 2013/3, S. 74f.; *Tang*, Legal Science 2007/12, S. 13 f.; siehe hierzu im Einzelnen Kapitel 3, B.II.

rauf am 1.1.2016 in Kraft. Nach § 51 ATG VRC sind die öffentlichen Sicherheitsbehörden bei der Ermittlung einer Terroraktion oder zur Abwehr der Gefahr aus einer Terroraktion befugt, Daten bei betroffenen Stellen und Personen sowie Dritten zu erheben und darauf zuzugreifen. Alle Diensteanbieter der Telekommunikation sowie Telemedien sind verpflichtet, zur Aufrechterhaltung der öffentlichen Sicherheit und der Strafverfolgung den Polizeibehörden und Staatssicherheitsbehörden technische Unterstützung zur Verfügung zu stellen und bei der Aufgabenerfüllung mitzuwirken.[569] Nach der Schwere der Straftaten wird nicht differenziert.

c) Cyber-Sicherheitsgesetz der VR China (中国人民共和国网络安全法)

Das Cyber-Sicherheitsgesetz (CSG VRC) wurde am 7.11.2016 erlassen und trat am 1.6.2017 in Kraft. Nach § 28 CSG VRC sind Internetdiensteanbieter verpflichtet, bei der Gefahrenabwehr und der Strafverfolgung durch Polizei- und Staatssicherheitsbehörden technische Unterstützung zur Verfügung zu stellen und bei der Aufgabenerfüllung dieser Behörden mitzuwirken. Auch wenn die Regelung nicht näher darauf eingeht, in welcher Form die Internetdiensteanbieter kooperieren müssen, ist hiermit wohl auch die Zurverfügungstellung von Vorratsdaten gemeint.

d) Beschluss über die Stärkung des Online-Datenschutzes vom Ständigen Ausschuss des Nationalen Kongresses (全国人大常委关于加强网络信息保护的决定)

Am 31.12.2012 hat der Ständige Ausschuss des Nationalen Kongresses den „Beschluss über die Stärkung des Online-Datenschutzes“ (B-ODS) erlassen. Der Beschluss trat am selben Tag in Kraft. Der Ständige Ausschuss des Nationalen Kongresses gehört zum höchsten Machtorgan und übt die staatliche Gesetzgebungsgewalt aus. Es ist anzumerken, dass dieser Beschluss zwar Gesetzescharakter besitzt. Aber er wird kaum unmittelbar angewendet, da die Vorgaben sehr abstrakt sind. Er gilt in der Praxis eher als richtungsgebende Leitlinie, nach der entsprechende Verordnungen und Abteilungsregeln erlassen werden dürfen. Nach § 10 Abs. 1 B-ODS sind bestimmte Behörden innerhalb ihrer Zuständigkeit befugt, technische und andere erforderliche Maßnahmen zu treffen, um Straftaten wie Ausspähen und Abfangen von Da-

---

569 § 28 Cyber-Sicherheitsgesetz der VR China (中华人民共和国网络安全法) vom 07.11.2016.

ten, Datenhehlerei sowie Internetkriminalität insgesamt zu verhindern. Dabei müssen die betroffenen Diensteanbieter mitwirken und technische Unterstützung leisten. Ähnlich wie schon für das Cybersicherheitsgesetz ist nicht näher ausgeführt, was hierunter genau zu verstehen ist. Die Übermittlung von Verkehrs- und Inhaltsdaten sollte

e) Bestimmung über die Erhebung, Überprüfung und Bewertung der elektronischen Daten in Strafverfolgung (关于办理刑事案件收集提取和审查判断电子数据若干问题的规定)

Verfahrensrechtliche Anforderungen an die Datenverwendung finden sich im Dokument „Bestimmung über die Erhebung, Überprüfung und Bewertung der elektronischen Daten in Strafverfolgung“ (B-StED). Dieses wurde gemeinsam vom Obersten Volksgerichtshof, von der Obersten Staatsanwaltschaft und vom Ministerium für öffentliche Sicherheit am 9.9.2016 erlassen. Wegen der in vielen Fällen gegebenen Unklarheit von gesetzlichen Vorgaben werden konkrete Handlungsmaßstabe für Verwaltungsbehörden häufig durch derartige Bestimmungen bereitgestellt. Der Rechtscharakter derartiger Bestimmung ist unklar. Für eine genaue Charakterisierung ist der Inhalt der jeweiligen Bestimmung heranzuziehen. In der Praxis gelten sie als Leitlinie für das Handeln bestimmter Behörden. Nach § 13 B-StED muss eine schriftliche Mitteilung beim Datenzugriff bereitgestellt werden, in welcher die gefragten Daten angegeben werden. Der Datenbesitzer bzw. die jeweilige betroffene Stelle sind über den Datenzugriff vom Diensteanbieter zu benachrichtigen.

f) Zwischenergebnis

Zusammenfassend ist festzustellen, dass keine speziellen, eindeutigen und insbesondere begrenzende Vorgaben für den Zugriff auf und die Verwendung von Vorratsdaten vorliegen. In den oben aufgelisteten Vorschriften wird den jeweiligen Behörden die Befugnis zum Vorratsdatenzugriff pauschal ohne Differenzierung zwischen Speicherungszweck und Datenkategorien erteilt. Als Verwendungszweck gilt auch allgemein die „Strafverfolgung“, die „Gefahrenabwehr“ oder die „Ermittlung einer terroristischen Aktivität“ usw. Anforderungen an die Schwere der Tat bzw. der Gefahr werden nicht formuliert. Die verfahrensrechtliche Beschränkung aus § 13 B-StED stellt lediglich Anforderungen an die Diensteanbieter. Den Behörden werden aber keine Zugriffsbeschränkungen auferlegt. Der Zugriff und die Verwendung der Vorratsdaten werden weder durch materielle noch durch verfahrensrechtliche Anforderungen beschränkt. Dies kann dazu führen, dass die Vorratsdaten im

Namen der öffentlichen Sicherheit schrankenlos abgerufen und verwendet werden.

4. Gewährleistung des Datenschutzes sowie der Datensicherheit und des Rechtsschutzes

Die Vorratsdatenspeicherung in der VR China betrifft zahlreiche personenbezogene Daten. In mehreren Regelungswerken im Telekommunikations- sowie Telemedienbereich werden allgemeine datenschutzrechtliche Anforderungen formuliert. Jedoch wird die Vorratsdatenspeicherung – als Ausnahme – von solchen Regelung ausgenommen. Zum Beispiel werden in § 9 Abs. 1 bis 4 der „Regeln zum Schutz der personenbezogenen Daten der Nutzer von Telekommunikations- und Internetdiensten“ (R-PDT) des Ministeriums für Industrie und Informationstechnologie vom 16.7.2013 den Diensteanbietern allgemeine datenschutzrechtliche Vorgaben zur Datenspeicherung und Datenverwendung gemacht. Aber in § 9 Abs. 5 R-PDT wird betont, dass diese Bestimmung nur gilt, sofern ein Gesetz oder eine andere nicht etwas anderes vorsieht; die oben genannten Vorschriften zur Vorratsdatenspeicherung sind Bestimmungen in diesem Sinne. Die Vorgaben zur Vorratsdatenspeicherung beinhalten keine konkreten datenschutzrechtlichen Anforderungen speziell an die Vorratsdatenspeicherung. Das Einhalten von Sicherheitsmaßnahmen – wie die Vorratsdatenspeicherung eine darstellt – bedeutet allerdings nicht, dass datenschutzrechtliche Anforderungen komplett außer Acht gelassen werden dürfen. Wegen der Schwere des Eingriffs, der mit der Vorratsdatenspeicherung einhergeht, muss sie die entsprechenden Anforderungen soweit wie möglich mehr erfüllen, um unbefugten Zugriff und Missbrauch der öffentlichen Stelle zu verhindern.

Zurzeit besteht in China kein einheitliches Datenschutzgesetz. Vor 2012 waren die datenschutzrechtlichen Regelungen in verschiedenen Regelungswerken verstreut.[570] Wegen der rasanten Verbreitung der Telekommunikationsmittel und gestiegenen Abhängigkeit von der Telekommunikationstechnologie in allen Lebensbereichen führt der Mangel an wirksamen Datenschutzregelungen zu einem ernsten Problem. Um diesem Problem zu begegnen, wurde seit dem Jahr 2012 eine Reihe von Regelungswerken erlassen. Auch wenn es immer noch kein einheitliches Datenschutzgesetz gibt, so haben die Regelungen zum Datenschutz nun an Übersichtlichkeit gewonnen. Maßgebend sind der oben bereits erwähnte „Beschluss über die Stärkung des Onli-

570 Dazu siehe auch *Jiang*, DuD 2011, 642 (642 ff.); *Binding*, ZD 2014, 327 (327 ff.); *Zhou*, 2006; *Qi*, 2006; *Guo*, 2012.

ne-Datenschutzes“ (B-ODS) des Ständigen Ausschuss des Nationalen Volkskongresses und die „Regeln zu personenbezogenen Daten der Nutzer der Telekommunikations- und Internetdienste“ (R-TID).

Im § 1 Abs. 1 B-ODS wird erstmals festgestellt, dass personenbezogene Daten in der Online-Welt vom Staat geschützt werden. Nach §§ 2 bis 4 B-ODS dürfen die Diensteanbieter sowie andere unternehmerische und institutionelle Einheiten nur genau nach Rechtsvorschrift elektronische personenbezogene Daten sammeln und verwenden. Bei der Sammlung und Verwendung elektronischer personenbezogener Daten müssen sie den Grundsatz der Erforderlichkeit und der Transparenz einhalten. Zudem muss eine Einwilligung zur Datenverarbeitung vorliegen. Technische und andere erforderliche Maßnahme sind zu treffen, um der Enthüllung personenbezogener Daten vorzubeugen. Zwar ist anzuerkennen, dass in diesem Beschluss der Schutz von personenbezogenen Daten der Nutzer im Grundsatz festgelegt wird. Allerdings ist unklar, auf welche Daten sich der B-ODS im Einzelnen bezieht; es ist nur die Rede von „elektronischen Daten“. Hinzu kommt, dass staatliche Stellen vom B-ODS nicht adressiert werden. Dies führt zu einer großen Schutzlücke bezüglich Datenerhebung und -verwendung von staatlichen Stellen.

In den R-TID des Ministeriums für Industrie und Informationstechnologie aus dem Jahr 2013 werden den Diensteanbietern erstmals konkrete Vorgaben für die Erhebung und die Verwendung der personenbezogenen Daten zu betrieblichen Zwecken gemacht. Unter dem Begriff „personenbezogene Daten der Nutzer“ versteht man gemäß § 4 R-TID „die von den Anbietern der Telekommunikations- und Internetdienste beim Dienstanbieten erhobenen personenbezogenen Daten wie Name, Geburtsdatum, Nummer des Identitätsausweises, Anschrift, Telefonnummer, Nutzerkonto und Passwort sowie andere personenbezogenen Daten der Nutzer, die allein oder mit anderen Daten zusammen eine Identifizierung des Nutzer ermöglichen. Die Daten über die Zeit und den Ort der Nutzung der Dienste gehören auch dazu. Der Begriff der personenbezogenen Daten wird hiermit erstmals festgelegt. In Kapitel 3 der R-TID werden Anforderungen an organisatorische und technische Maßnahmen für die Datensicherheit aufgestellt, um Datenenthüllung sowie Datenmissbrauch zu verhindern. Diese Regelungen haben die Lücke beim Schutz von personenbezogenen Daten im Telekommunikationsbereich geschlossen.

Die Bedeutung des B-ODS und der R-TID kann kaum überschätzt werden. Obwohl die Vorschriften noch nicht konkret genug sind, wird die Lücke der

Datenschutzgesetzgebung im Telekommunikations- sowie Telemedienbereich endlich gefüllt. Nichtsdestoweniger bleibt es ein großes Problem, dass Datenerhebung und Datenverwendung von staatlichen Stellen nicht datenschutzrechtlich beschränkt werden. Insbesondere fehlt es an datenschutzrechtlichen Regelungen bezüglich der Speicherung und Verwendung von Vorratsdaten.

5. Rechtsschutz

Bezüglich des Rechtsschutzes unterliegt der Abruf und die Verwendung der Vorratsdaten von den befugten Behörden keinem Richtervorbehalt. Eine wirksame Rechtskontrolle nach vorhandenen Vorgaben kann weder durch einen Richter noch durch eine unabhängige Verwaltungsstelle durchgeführt werden. Es fehlt zusätzlich die Benachrichtigungspflicht. Der Betroffene hat also keine Möglichkeit zu erkennen, ob seine Verkehrsdaten für geregelte Zwecke verwendet werden oder nicht. Er kann sich deswegen nicht gegen unbefugte Verwendung wehren. Während die Sanktionen der Nichterfüllung der Speicherungspflicht von den Diensteanbietern klar und deutlich festgelegt werden, wird der Rechtsweg der Betroffenen nicht geregelt.

III. Zusammenfassung

Zusammenfassend stellt die Vorratsdatenspeicherung in der VR China im Vergleich zu der in Deutschland eine die Freiheit sowie die Privatsphäre der Bürger viel tiefer beschränkende Maßnahme dar. Sie wird nicht einmalig und einheitlich gesetzlich geregelt, die Vorgaben verstreuen sich vielmehr in verschiedenen Regelungswerken. Eine Besonderheit des chinesischen Rechts stellt die Vielzahl der verschiedenen Rechtsquellen dar. So sind die in diesem Abschnitt dargestellten Vorgaben zur Vorratsdatenspeicherung nicht in einem formellen Gesetz zu finden, sondern in verschiedenen Verwaltungsregeln und Verwaltungsmethoden. Diese Vorgaben haben gemeinsam, dass die keine Schutz- und Beschränkungsmechanismen vorsehen. Die Speicherung der Vorratsdaten ist dadurch sehr umfassend. Die zudem relativ unbestimmten Vorgaben führen so im Ergebnis zu einer uferlosen Speicherung und schrankenlosen Verwendung durch staatliche Stellen.

B. Verfassungsrechtliche Bewertung der Vorratsdatenspeicherung in der VR China

Die chinesische Verfassung (Verf VRC) enthält einen Grundrechtskatalog. In dieser Hinsicht weist die chinesische Verfassung Ähnlichkeiten mit westlichen Verfassungen auf. Der Bürger soll vor staatlichen Eingriffen geschützt werden. Der Unterschied besteht allerdings darin, dass die grundrechtlichen Verbürgungen in der Praxis eher unzureichend beachtet werden. Dies kann auch am Thema der Vorratsdatenspeicherung exemplifiziert werden. Der von der Verfassung – formal – garantierte Schutz wird im Hinblick auf die derzeitige Ausgestaltung der Vorratsdatenspeicherung in China im Ergebnis nicht gewährt.

I. Relevante Grundrechte

Zunächst sollen diejenigen Grundrechte dargestellt werden, die im Kontext der Vorratsdatenspeicherung relevant sind. Dies sind die Meinungsfreiheit, die Berufsfreiheit, die Unverletzlichkeit der Würde der Persönlichkeit und insbesondere die Freiheit und das Geheimnis der Korrespondenz. Es ist darauf hinzuweisen, dass es kein Auffanggrundrecht in der chinesischen Verfassung gibt, vergleichbar mit der allgemeinen Handlungsfreiheit aus Art. 2 Abs. 1 GG. Es gibt zwar auf einfachrechtlicher Ebene den Grundsatz des Vorbehalts des Gesetzes.[571] Dieser kann jedoch nicht die gleichen Wirkungen entfalten wie ein verfassungsrechtliches Auffanggrundrecht, was dazu dient, staatliches Handeln insgesamt zu begrenzen bzw. diesem eine Rechtfertigungsanforderung anheimstellen.

1. Freiheit der Meinungsäußerung

Im Art. 35 Verf VRC wird festgelegt, dass der Bürger die Freiheit der Rede, der Veröffentlichung von Publikation, der Versammlung, der Vereinigung, des Umzugs und der Demonstration hat. Diese Freiheiten gehören zur Freiheit der Meinungsäußerung,[572] dessen Wesen in der Freiheit von Äußerungen der *politischen* Meinung liegt.[573] Die Freiheit der Meinungsäußerung stellt eine Voraussetzung für die Ausübung vieler anderer Grundrechte dar. Sie ist zu gewährleisten, damit der Bürger bei den Angelegenheiten des Gemeinwesens mitwirken und seine Persönlichkeit entfalten kann.[574] Die Freiheit der Mei-

---

571 Siehe hierzu Kapitel 3, B. II. 1.

572 *Zhang*, 2014, S. 540 f.; *Lin*, 2015, S. 372; *Zhen*, 2000, S. 35 ff.; *Rao*, 2005, S. 88.

573 *Zhen*, 2000, S. 64; *Dong*, Journal of Northwest University of Politics and Law, S. 16.

574 *Dong*, Journal of Northwest University of Politics and Law, S. 16 und 20; *Zhen*, 2000, S. 110 f. und 116.

nungsäußerung wird nicht schrankenlos geschützt. Sie darf aufgrund des öffentlichen Interesses und der Rechte der anderen, insbesondere zum Schutz des Ehrenrechts und der Privatsphäre anderer beschränkt werden.[575] Bei der Beschränkung aus der Abwägung der kollidierenden Grundrechte ist das Verhältnismäßigkeitsprinzip von zentraler Bedeutung.[576] In die Freiheit der Meinungsäußerung wird eingegriffen, wenn eine staatliche Maßnahme faktisch die Äußerung sowie Verbreitung der Meinung verbietet, hemmt oder gebietet.[577]

Ob die Vorratsdatenspeicherung für die Freiheit der Meinungsäußerung der Nutzer relevant ist, beurteilt sich danach, welche Daten zu den „Nutzungsdaten" zählen. Beispielhaft kann dies anhand der Vorschrift des § 23 VO-IC[578] erörtert werden. Mangels Begriffsbestimmung der „Nutzungsdaten" ist es schwierig, dies zu beurteilen. „Nutzungsdaten" stellt keinen juristischen Begriff im engeren Sinne dar. Darunter kann man Informationen darüber verstehen, welche Telekommunikations- und Telemediendienste der Kunde in Internet-Cafés benutzt. „Nutzungsdaten" können somit Verkehrsdaten und auch Nutzungsdaten i.S.d. deutschen § 15 Abs. 1 TMG sein, und zwar diejenigen personenbezogenen Daten, die vom Diensteanbieter zum Zweck der Bereitstellung des Telemedienangebots und der Abrechnung von Diensteanbieter erhoben werden. Hierzu zählen insbesondere die Identifikationsdaten des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien. Bei der Nutzung der Telemediendienste wie etwa Online-Foren und Weibo (微博, ein Kurznachrichtendienst ähnlich wie Twitter) von Kunden der Internet-Cafés werden alle Nutzungsdaten nach Vorgaben der VO-IC gespeichert. Zu beachten ist, dass nach § 5 der „Verwaltungsregeln für Kontos der Nutzer im Internet" (互联网用户账号名称管理规定) für alle Nutzer der Telemediendienste eine Klarnamenpflicht gilt. Wenn die Klarnamenpflicht und die Speicherung der Nutzungsdaten kombinierend durchgeführt werden, kann dies die Meinungsäußerung der Nutzer berühren. Der Nutzer kann auf die Meinungsäußerung verzichten, da er Angst vor negativen Folgen der Meinungsäußerung hat. Die Speicherung der Nutzungsdaten kann die Meinungsäußerung hemmen.

---

575 *Zhen*, 2000, S. 257 ff.; *Rao*, 2005, S. 92.
576 *Chen*, in: Chinese Yearbook of Constitutional Law 2016, S. 38 ff.
577 *Schulze-Fielitz*, in: *Dreier* (Hrsg.), GG, Art. 5 Rn. 124.
578 Siehe Kapitel 3, A.II.2.e).

Bei der Beantwortung der Frage, welche Grundrechte der Inhalte-Provider bei der Vorratsspeicherung der aufbereiteten Informationen relevant sind, kommt es darauf an, welche Inhalte und welche Dienste der Inhalts-Provider genau anbietet. Einschlägige Grundrechte können die Meinungsfreiheit, Medienfreiheit, Freiheit von Kunst sowie Wissenschaft sein. Die Vorratsspeicherung der aufbereiteten Informationen hat die faktische Wirkung, dass die Inhalte-Provider durch Protokollierung der Inhalte dem psychischen Druck ausgesetzt sind, ungünstige Folgen zu tragen. Diese Wirkung verstärkt sich noch, da der Beurteilungsmaßstab der illegalen Informationen nicht gesetzlich eindeutig festgesetzt wird. Die Kommunikationsfreiheit der Inhalte-Provider ist von der Vorratsspeicherung betroffen.

2. Berufsfreiheit der Telekommunikationsdienstanbieter

Die Berufsfreiheit wird in Art. 42 Abs. 1 Verf VRC normiert und besagt, dass Bürger in der VR China das Recht und die Pflicht zu arbeiten haben. Das Recht auf Arbeit legt vom Wortlaut her nahe, dass der einzelne Arbeitnehmer ein Recht auf einen Arbeitsplatz hat und dass sich der Gehalt dieses Rechts darin erschöpft. Jedoch wird im Schrifttum vertreten, dass dadurch auch gewährleistet wird, dass der Bürger das Recht hat, den Beruf frei zu wählen und frei auszuüben,[579] sowie zum Beispiel Zeit, Stätte, und Inhalt der Betätigung frei zu wählen.[580] Die Berufsfreiheit ist kein unbeschränktes Recht. Es darf zum Schutz öffentlicher Interessen beschränkt werden. Beschränkungen der Berufsfreiheit von Staats wegen können durch Schaffung eines Anmeldungssystems, einer Genehmigungspflicht, aufgrund des Schutzes der öffentlichen Sicherheit und Ordnung sowie anderer spezieller Genehmigungen auferlegt werden.[581] Die Beschränkungen der Berufsfreiheit dürfen nicht übermäßig sein und dürfen nur dasjenige umfassen, was zum Schutz des öffentlichen Interesses erforderlich ist.[582] Die privaten Telekommunikationsdiensteanbieter haben nach den Vorgaben der Vorratsdatenspeicherung die Telekommunikationsdaten der Nutzer zu speichern, unabhängig davon, ob die Daten für den geschäftlichen Zweck erforderlich sind. Dafür wird ihnen ein zusätzlicher Aufwand auferlegt. Somit wird die Berufsfreiheit der privaten Telekommunikationsdienstanbieter durch die Speicherungspflicht beschränkt.

Fraglich ist, ob die staatlichen Telekommunikationsdienstanbieter sich auf die Berufsfreiheit berufen können. Gemäß Art. 16 Verf VRC dürfen staatliche

---

579 Siehe auch *Xue*, 2006, S. 67; *Chen*, China Legal Science 2011/1, S. 103.
580 Siehe auch *Song*, 2008, S. 510.
581 Siehe auch *Song*, 2008, S. 511 ff.
582 *Chen*, China Legal Science 2011/1, S. 104; *Song*, 2008, S. 517.

Unternehmen im Rahmen der gesetzlichen Bestimmungen die Unternehmen frei leiten. Auf den ersten Blick könnten sie mit privaten Dienstanbietern bei dem Grundrechtsschutz der Berufsfreiheit gleichgesetzt werden, falls sie sich auch in Privatrechtsform betätigen. Jedoch zielt die Begründung und Betätigung staatlicher Telekommunikationsdiensteanbieter vor allem darauf ab, dem öffentlichen Interesse zu dienen. Diese Unternehmen funktionieren als juristische Personen des öffentlichen Rechts, die in erster Linie öffentliche Aufgaben zu erfüllen haben. Deswegen sind staatliche Telekommunikationsdiensteanbieter keine berechtigten Grundrechtsträger und nur der private Telekommunikationsdienstanbieter kann sich auf die Berufsfreiheit berufen.[583]

3. Unverletzlichkeit der Würde der Persönlichkeit

Anders als in Deutschland, wo das Recht auf informationelle Selbstbestimmung vom Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) entwickelt wurde, könnte die Verfassungsgrundlage eines allgemeinen Datenschutzrechts aus Art. 38 Verf VRC, die Unverletzlichkeit der Würde der Persönlichkeit, abgeleitet werden. Nach Art. 38 S. 1 Verf VRC ist die Würde der Persönlichkeit der Bürger unverletzlich. Art. 38 S. 2 Verf VRC konkretisiert dies. Hiernach sind Beleidigungen, Diffamierungen und falsche Beschuldigungen gegen Bürger in jeglicher Form verboten.

Die Bedeutung und Funktion des Art. 38 Verf VRC ist umstritten. Eine Ansicht spricht davon, dass der damalige Wortlaut des Verfassungstexts von der Verfassung Italiens beeinflusst worden sei und die „Würde der Persönlichkeit der Bürger“ eine falsche Übersetzung der entsprechenden italienischen Wörter sein könne.[584] Trotzdem sei dieser Ausdruck zutreffend und es gebe Gemeinsamkeiten in Bedeutung zwischen dem und der Menschenwürde im Sinne des Art. 1 Abs. 1 GG.[585] Würden der erste und der zweite Satz getrennt betrachtet, werde das oberste Prinzip der Verfassung durch den ersten Satz festgestellt, wobei ihm eine ähnliche Bedeutung und Funktion wie der Unantastbarkeit der Menschenwürde aus Art. 1 Abs. 1 GG zukomme.[586] Der zweite Satz stelle nicht nur ein Verbot dar, sondern in Verbindung mit dem ersten Satz auch das allgemeine Persönlichkeitsrecht.[587] Aus dem Art. 38

---

583 Die Grundrechtsfähigkeit juristischer Personen des öffentlichen Rechts siehe *Wieland*, in: *Dreier* (Hrsg.), GG, Art. 12, Rn. 57.

584 *Lin*, Zhejiang Social Sciences 2008/3, S. 49.

585 *Lin*, Zhejiang Social Sciences 2008/3, S. 49.

586 *Lin*, Zhejiang Social Sciences 2008/3, S. 50 f.; ähnliche Auffassungen siehe auch *Liu*, China Legal Science 2007/1, S. 39ff; *Shangguan*, Jiangsu Social Sciences 2008/2, S. 80; *Yi*, Hehei Law Science 2012/12, S. 82 ff.

587 *Lin*, Zhejiang Social Sciences 2008/3, S. 52.

Verf VRC könnte sich also eine doppelte Schutzrichtung ergeben.[588]

Gegen diese These spricht, dass die zwei Sätze in Art. 38 Verf VRC nicht getrennt, sondern nur in Verbindung miteinander betrachtet werden dürfen.[589] Der historischen Auslegung zufolge sei der Art. 38 Verf VRC so ausgearbeitet worden, damit die Bürger Beleidigungen, Diffamierungen und falschen Beschuldigungen – was in der Zeit der kulturellen Revolution häufig vorgekommen ist – nicht mehr ausgesetzt sein würden.[590] Insofern sei das Persönlichkeitsrecht als einzelnes Grundrecht der Bürger im Art. 38 Verf VRC festgeschrieben worden. Art. 38 stelle Verf VRC auch kein oberstes Prinzip der Verfassung dar.[591]

Es kann als Defizit der chinesischen Verfassung bezeichnet werden, dass sie kein ausdrückliches oberstes Prinzip enthält, etwa dass die Menschenwürde unantastbar und seine Achtung und Gewährleistung der Ausgangspunkt und das wesentliche Ziel der Verfassung ist.[592] Art. 38 Verf VRC lässt sich weder nach Wortlaut, noch aus dem Kontext in der Verfassung[593] oder nach der Auslegung als oberstes Prinzip der Verfassung einstufen.

Art. 38 Verf VRC kann jedoch in die Richtung ausgelegt werden, dass in ihm das allgemeine Persönlichkeitsrecht normiert wird. Nach dem Wortlaut des Art. 38 Verf VRC sind Persönlichkeitsrechte wie der Ehrschutz der Bürger zu gewährleisten.[594] Jedoch schwer vorstellbar, dass sich der Schutz des Persönlichkeitsrechts nur auf diese aufgelisteten Rechte beschränken würde.[595] Der Inhalt des Persönlichkeitsrechts ist nicht auf das Verständnis einer bestimmten Zeit zu beschränken, sondern an die neuen gesellschaftlichen Bedingungen anzupassen. Daher ist es zutreffend, dass der Art. 38 Verf VRC als Feststellung des allgemeinen Persönlichkeitsrechts angesehen wird, dessen Schutzbereich nicht nur auf das Recht auf persönlichen Ruf und Ehre beschränkt, sondern angesichts der neuen gesellschaftlichen Bedingungen offen

588 *Lin*, Zhejiang Social Sciences 2008/3, S. 53.
589 *Xie*, Tribune of Political Science and Law 2010/4, S. 60 ff.
590 *Xie*, Tribune of Political Science and Law 2010/4, S. 60 ff.; *Kong*, Law Science 1982/12, S. 8.
591 *Xie*, Tribune of Political Science and Law 2010/4, S. 60 ff.; zu ähnlichen Auffassungen siehe auch *Li*, Contemporary Law Review 2011/6, S. 27 ff.; *Zheng*, China Legal Science 2012/2, S. 79 ff.; *Wang*, China Legal Science 2014/4, S. 103 ff.; *Wang*, China Legal Science 2017/3, S. 102 ff.
592 Siehe auch *Lin*, Zhejiang Social Sciences 2008/2, S. 50; *Xie*, Tribune of Political Science and Law 2010/4, S. 60.
593 *Wang*, China Legal Science 2017/3, S. 108.
594 Siehe auch *Zhang*, 2014, S. 535.
595 Siehe auch *Xie*, *Libin*, in: Mo/Xie (Hrsg.) 2009, S. 163.

bleibt.[596] Die Verwendung und der Austausch personenbezogener Daten stellt für den Bürger nun eine unentbehrliche Voraussetzung für die Entfaltung der Persönlichkeit und die Mitwirkung in Angelegenheiten des Gemeinwesens in der Informationsgesellschaft dar. Damit ist das Recht auf Schutz der personenbezogenen Daten als neu konturierter Inhalt des Persönlichkeitsrechts aus Art. 38 Verfassung der VR China zu erfassen.[597]

Die Vorratsspeicherung von Verkehrs- und Nutzungsdaten greift in das Recht auf Schutz der personenbezogenen Daten ein. Durch eine pauschale Vorratsspeicherung können vollständige und detaillierte Persönlichkeitsprofile mit Leichtigkeit erstellt werden. Der Eingriff wiegt besonders schwer wegen der Durchsetzung der Klarnamepflicht in der VR China. Um illegale Informationen zu behindern und zu beseitigen, wird die Klarnamenpflicht den Nutzern seit 1997 durch verschiedene Regelungswerke zur Registrierung von Domainnamen, Eröffnung von Online-Shops, Eröffnung eines Kontos für Online-Spiele, Eröffnung von Blogs usw. schrittweise auferlegt. Im Jahr 2013 wurde die Klarnamenpflicht in den „Regeln zur Registrierung mit Klarnamen der Telefon-Nutzer“[598], den „Verwaltungsregeln für Kontos der Nutzer im Internet“ [599] sowie den „Vorläufigen Verwaltungsregeln für Instant-Messeging-Dienste“[600] festgelegt. Bei Nutzung jeglicher Telekommunikations- sowie Telemediendienste müssen die Nutzer nun die Klarnamenpflicht erfüllen.

Die Eingriffsintensität der Vorratsspeicherung der Nutzungsdaten verschärft sich erheblich in Verbindung mit der Klarnamepflicht, da dadurch jedes Handeln der Nutzer im Telekommunikationsnetz sowie im Internet sehr durchsichtig geworden ist. Unter den vorhandenen, sehr lockeren Verwendungsvoraussetzungen der Vorratsdaten ist es dem Staat möglich, jedes Telekommunikationshandeln der Nutzer zur Kenntnis zu nehmen. Mangels strenger Anforderungen an Datenschutz sowie Datensicherheit setzen sich die Nutzer einem enormen Risiko der Datenenthüllung und des Datenmiss-

---

596 Siehe auch *Lin*, Zhejiang Social Sciences 2008/3, S. 52; *Zhao*, China Law Review 2017/1, S. 154 ff.

597 Ähnliche Auffassungen siehe auch *Zhao*, China Law Review 2017/1, S. 154 ff.; *Sun*, Legal Science 2007/7, S. 41; *Yao*, Political Science and Law 2012/4, S. 73 ff.

598 § 3 Regeln zum Registrierung mit Klarnamen der Telefon-Nutzer (电话用户真实身份信息登记规定) vom 16.07.2013.

599 § 5 Verwaltungsregeln für Kontos von Nutzern im Internet (互联网用户账号名称管理规定) vom 04.02.2015.

600 § 6 Vorläufige Verwaltungsregeln zur Entwicklung der öffentlich zugänglichen Informationsdienste durch Echtkommunikationsmittel (即时通信工具公众信息服务发展管理暂行规定) vom 07.08.2014.

brauchs aus.[601] Das Recht auf Schutz der personenbezogenen Daten wird faktisch ausgehöhlt. Der Würdeschutz sollte in jedem Fall in Bezug auf den Schutz von personenbezogenen Daten mitgedacht werden. Wegen der unzureichenden dogmatischen Ausdifferenziertheit des Würdeschutzes eignet sich dieses Grundrecht aber letztlich nicht für eine verfassungsrechtliche Prüfung der Regelungen zur Vorratsdatenspeicherung.

4. Freiheit und Geheimnis der Korrespondenz

Nach Art. 40 Verf VRC werden die Freiheit und das Geheimnis der Korrespondenz der Bürger geschützt. Geschützt sind nicht nur die traditionellen Kommunikationsvorgänge mittels Brief, sondern auch andere Kommunikationsformen. Zwar wird das Korrespondenzgeheimnis in der Verfassung ausdrücklich genannt, aber als eine spezielle Form des „Briefverkehrs" mittels Telekommunikationstechnologie sind die Freiheit der Telekommunikation und das Fernmeldegeheimnis geschützt.[602] Nur Polizeibehörde und Staatsanwaltschaft dürfen zum Zweck der öffentlichen Sicherheit oder Strafverfolgung nach gesetzlichem Verfahren den Briefverkehr, den Email-Verkehr und andere Arten der nicht unmittelbaren Kommunikation kontrollieren. Ansonsten darf keine Stelle oder Person in den Schutz des Korrespondenzgeheimnisses der Bürger eingreifen. Das Korrespondenzgeheimnis stellt den Kern des Art. 40 Verf VRC dar, weil die Korrespondenzfreiheit ohne Gewährleistung der Vertraulichkeit des Kommunikationsvorgangs nicht verwirklicht werden kann. Die Korrespondenzfreiheit wird als Zweck des Schutzes des Korrespondenzgeheimnisses angesehen. Der Bürger hat das Recht, durch jedes Mittel mit anderen frei zu kommunizieren. Dritte und staatliche Stelle dürfen Inhalte und nähere Umstände des Kommunikationsvorgangs der Bürger nicht kontrollieren, überwachen, belauschen oder protokollieren.[603]

Geschützt wird vor allem der Inhalt der Telekommunikation. Darüber hinaus sind nähere Umstände des Telekommunikationsvorgangs, wie zum Beispiel Zeit, Ort und Mittel des Telekommunikationsverkehrs schutzwürdig.[604] Der Ausschuss der Rechtsangelegenheit des Ständigen Ausschusses des Volkskongresses der Provinz Hunan hat in einer Antwort auf den Auslegungsantrag eines Telekommunikationsdienstanbieters dargestellt, dass die Informationen

---

601 *Guo*, 2012, S. 291; *Zhao*, Journal of Comparative Law 2017/2, S. 35; *Bu*, Tianjin Legal Science 2014/2, S. 29.

602 *Liu*, Zhejiang Academic Journal 2005/1, S. 169.

603 *Li*, Juridical Science Journal 2002/6, S. 26; *Zhou*, Legal Science 2006/6, S. 58 f.; *Zhang*/*Li*, Journal of Yunnan University Law Edition 2005/2, S. 41.

604 *Xie*, 2014, S. 187 f.; *Zhou/Wei*, Legal Science 2006/6, S. 58 f.; *Li*, Modern Science & Technology of Telecommunications 2011/5, S. 39 f.

über Telekommunikationspartner, Datum, Zeitpunkt, Dauer und Häufigkeit des Telekommunikationsverkehrs, aus dem privaten Leben sowie über den sozialen Verkehr der Teilnehmer unter das Korrespondenzgeheimnis zu fassen sind. Diese Informationen seien ein wesentlicher Teil des Telekommunikationsverkehrs und müssen geschützt werden, um die Privatsphäre der Bürger zu gewährleisten.[605] Dieser Antwort wurde vom Ausschuss für Rechtsangelegenheiten des Ständigen Ausschusses des Nationalen Volkskongresses zugestimmt.[606] Damit werden Inhaltsdaten, Verkehrsdaten und Standortsdaten vom Korrespondenzgeheimnis geschützt. Im deutschen Verfassungsrecht bezieht sich das Fernmeldegeheimnis auf den Kommunikationsvorgang, während die Daten über einen abgeschlossenen Kommunikationsvorgang durch das Recht auf informationelle Selbstbestimmung geschützt sind. Eine solche Trennung ist in der chinesischen Verfassung nicht angelegt. Ein Datenschutzrecht ist schlicht nicht vorhanden. Einerseits führt dies dazu, dass der Schutz von Daten nicht in vergleichbarer Weise gegeben ist. Andererseits sind Daten, die den Inhalt der Korrespondenz betreffen, geschützt, auch nachdem der Vorgang der Korrespondenz beendet ist.

Zu den Behörden, die das Korrespondenzgeheimnis beschränken dürfen, gehören nur Polizeibehörden und Staatsanwaltschaften. Zwar wurden Staatssicherheitsbehörden seit 1983 von Polizeibehörden in Bezug auf ihre Aufgaben getrennt[607] und ihnen bestimmte Befugnisse wie Strafverfolgung erteilt, aber begrifflich gesehen umfasst die Polizeibehörde immer noch die Staatssicherheitsbehörde.[608] Damit dürfen die Staatssicherheitsbehörden das Korrespondenzgeheimnis auch beschränken. Die Beschränkung ist nur zum Zweck der öffentlichen Sicherheit und der Strafverfolgung zulässig.

Die zu speichernden Telekommunikationsdaten gehören zu Umständen der Telekommunikationsvorgänge der Bürger. In das Korrespondenzgeheimnis der Bürger wird dadurch eingegriffen, dass ihre Telekommunikationsdaten auf Vorrat aufgezeichnet werden. Daher ist vor allem zu thematisieren, ob die Speicherung durch Telekommunikationsdiensteanbieter einen staatlichen

---

605 Dokument vom Ausschuss für Rechtsangelegenheiten vom Ständigen Ausschuss des Volkkongresses Hunan Provinz (湘人法工函, 2003, 23 号), 25.11.2003.

606 Dokument vom Ausschuss für Rechtsangelegenheiten vom Ständigen Ausschuss des Nationalen Volkskongresses (法工办复字, 2004, 3 号), 09.04.2004.

607 Beschluss über die Befugnis der Staatssicherheitsbehörde zur polizeilichen Ermittlung, Festnahme, Verhör und Vollstreckung der Festnahme von dem Ständigen Ausschuss des Nationalen Volkskongresses, 2.9.1983.

608 § 2 S. 2 Polizeigesetz der VR China (中华人民共和国人民警察法) vom 28.02.1995.

Eingriff darstellt. Dabei muss die besondere Eigenschaft der chinesischen staatlichen Telekommunikationsdiensteanbieter berücksichtigt werden. Bevor die Reform- und Öffnungspolitik in China durchgeführt wurde, waren Telekommunikationsdiensteanbieter staatliche Behörden, die Dienste anboten und gleichzeitig den Telekommunikationsmarkt regulierten. Nach der Reform ist die für Regulierung zuständige Abteilung weiterhin staatliche Behörde geblieben, während die betriebliche Abteilung zu den staatlichen Unternehmen gewechselt ist. Staatliche Telekommunikationsunternehmen sind somit keine staatlichen Behörden mehr.

Bislang wird der chinesische Telekommunikationsmarkt noch von drei Staatsunternehmen und zwar China Telekom, China Unicom und China Mobil, dominiert. Deren Anteile gehören alleine dem Staat. Nur der Markt der Mehrwerttelekommunikationsdienste wie zum Beispiel Zugangsdienste und Informationsdienste sind für private Unternehmen offen. Zwar betätigen sich die staatlichen Telekommunikationsunternehmen in Privatrechtsform, aber durch den Gründungszweck sind sie von privaten Unternehmen zu unterscheiden. Statt Profit zu erzielen, zielen staatliche Telekommunikationsunternehmen in erster Linie auf die Förderung des öffentlichen Interesses ab.[609] Somit fungieren staatliche Telekommunikationsunternehmen bei der Vorratsdatenspeicherung nicht als private Dritte, sondern als öffentliche Aufgaben wahrnehmende Staatsbehörden. Damit liegt in der Vorratsdatenspeicherung der staatlichen Telekommunikationsunternehmen ein unmittelbarer Eingriff vom Staat in das Korrespondenzgeheimnis der Bürger vor. Bei der Vorratsspeicherung von privaten Telekommunikationsunternehmen fungieren sie als unfreiwillige Hilfspersonen zur Erfüllung der staatlichen Aufgaben, die Vorratsspeicherung von privaten Telekommunikationsunternehmen ist damit auch dem unmittelbaren staatlichen Eingriff zuzurechnen.

5. Fazit

Mehrere Grundrechte werden von der Vorratsdatenspeicherung berührt. Dabei kann in Bezug auf die Betroffenen zwischen den Nutzern und Telekommunikationsunternehmen unterschieden werden. Bei den Telekommunikationsunternehmen ist die Frage der Grundrechte aus dem Grund zweifelhaft, da es sich um Staatsunternehmen handelt. In Bezug auf die Nutzer kommen für den Grundrechtsschutz der Würdeschutz aus Art. 38 Verf VRC und die Korrespondenzfreiheit bzw. das Korrespondenzgeheimnis aus Art. 40 Verf VRC

609 *Chen*, China Legal Science 2011/1, S. 100; siehe auch *Herdegen*, in: *Maunz*/*Dürig* (Begr.), Art. 1 Rn. 96.

in Betracht. In den Ausführungen hat sich jedoch gezeigt, dass Art. 38 Verf VRC das einschlägigere Grundrecht ist. Schwerpunktmäßig ist durch die Vorratsdatenspeicherung das Korrespondenzgeheimnis betroffen. Somit wird im Folgenden für die verfassungsrechtliche Bewertung das Korrespondenzgeheimnis herangezogen. Es ist darauf hinzuweisen, dass man aus Art. 38 Verf VRC ein Recht auf informationelle Selbstbestimmung kaum ableiten kann. Mangels eines solchen Rechts fehlt es der momentan an einer allgemeinen verfassungsrechtlichen Grundlage für den Datenschutz. Hierdurch entsteht eine große Schutzlücke. Grundrechtlicher Schutz für Telekommunikationsdaten ist aber insoweit gegeben, als diese sich auf die Korrespondenz beziehen. Inhalts-, Standorts- und Verkehrsdaten werden dadurch, solange ein Bezug zur Korrespondenz gegeben ist, von Art. 40 Verf VRC geschützt. Regelungen zur Vorratsdatenspeicherungen müssen diesen Schutz beachten.

Die Darstellung der in Frage kommenden Grundrechte hat jedoch auch offenbart, dass das grundrechtliche Schutzniveau in der VR China wesentlich weniger ausgeprägt ist als in Deutschland. Insbesondere ist der Schutz von personenbezogenen Daten nicht umfassend geschützt. Für den grundrechtlichen Schutz bietet das Korrespondenzgeheimnis die meisten Möglichkeiten, um eine allzu weitgehende Vorratsdatenspeicherung zu beschränken.

II. Rechtfertigung des Eingriffs in das Korrespondenzgeheimnis

Statt die Beschränkbarkeit und die Voraussetzungen der Beschränkung für jedes einzelne Grundrecht vorzusehen, wird nach Art. 51 Verf VRC allgemein geregelt, dass der Bürger bei Ausübung eines Grundrechts das Interesse des Staates, der Gesellschaft, des Kollektivs, und die Freiheit und das Recht anderer Bürger nicht beeinträchtigen darf. Nur für wenige Grundrechte, zum Beispiel die Eigentumsgarantie aus Art. 13 Verf VRC und das Korrespondenzgeheimnis aus Art. 40 Verf VRC, sind die Rechtfertigungsvoraussetzungen eigens festgelegt. Für das hier relevante Korrespondenzgeheimnis ist somit die Beschränkbarkeit aus Art. 40 Verf VRC selbst zu entnehmen. Weitere Vorgaben der verfassungsrechtlichen Rechtfertigung sind dem Art. 51 Verf VRC zu entnehmen bzw. aus der Verfassung abzuleiten.

1. Gesetz

Zwar darf das Korrespondenzgeheimnis der Bürger aufgrund des Schutzes der staatlichen Sicherheit beschränkt werden, aber die Beschränkung ist nur auf gesetzlicher Grundlage zulässig. Auch ist das Verhältnismäßigkeitsprinzip

zu wahren, damit die Grundrechte nicht wegen willkürlicher Beschränkung ausgehöhlt werden.[610] In der VR China ist der Vorbehalt des Gesetzes allgemein in §§ 8 und 9 GGebG VRC geregelt. In § 8 GGebG VRC werden mehrere wesentliche Angelegenheiten aufgelistet, die durch Gesetz geregelt werden müssen. Hierbei handelt es sich etwa um Straftaten und Strafen, um grundlegende steuerrechtliche Regelungen und die Einziehung und Beschlagnahme nichtstaatlichen Vermögens. Jedoch sieht § 9 GGebG VRC vor, dass der Nationale Volkskongress und sein Ständiger Ausschuss den Staatsrat ermächtigen können, der Sache nach Verwaltungsrechtsnormen in Bezug auf die in § 8 GGebG VRC aufgelisteten Angelegenheiten auszuarbeiten, wenn sie noch nicht durch Gesetz geregelt worden sind. Ausgeschlossen sind die Angelegenheiten der Kriminalität und Strafe, Aberkennung der politischen Rechte der Bürger, die körperliche Freiheit beschränkende Zwangsmaßnahme und Sanktion des Justizsystems.

Aus §§ 8 und 9 GGebG VRC ergibt sich, dass zwischen dem relativen und dem absoluten Vorbehalt des Gesetzes zu unterscheiden ist.[611] Während die Angelegenheiten aus § 8 GGebG VRC abgesehen von den Angelegenheit in § 9 GGebG VRC durch Gesetz oder aufgrund eines Gesetzes geregelt werden müssen, dürfen die Angelegenheiten in § 9 GGebG VRC nur durch Gesetz vom Nationalen Volkskongress geregelt werden. Dieser absolute Vorbehalt des Gesetzes ähnelt somit dem in der deutschen Rechtswissenschaft anerkannten Parlamentsvorbehalt.[612] § 8 GGebG VRC, der den relativen Gesetzesvorbehalt enthält, wird als mangelhaft kritisiert, da auch die dortigen Angelegenheiten grundrechtsrelevant sind und nicht einem absoluten Vorbehalt unterstellt werden.[613] Der Geltungsbereich des absoluten Vorbehalts des Gesetzes ist somit stark beschränkt. Dies führt dazu, dass die Grundrechte der Bürger nicht vollständig vor der Verletzung durch staatliche Gewalt geschützt werden.[614]

---

610 Siehe auch *Chen*, Beschränkung auf Grundrecht, in: *Chen*, Band 1, 2010, S. 397; *Han*, Legal Forum 2005/1, S. 8 f.; *Xie*, Journal of Comparative Law 2014/4, S. 48 ff.; *Zhang*, Legal Forum 2005/1, S. 27; *Zhao*, Jurist 2011/2, S. 165 ff.; *Shi*, Journal of Comparative Law 2014/5, S. 167 ff.

611 *Ying*, Chinese Legal Science 2000/4, S. 6; *Sun*, Tribune of Political Science and Law 2011/2, S. 111; *Kang*, Jianghai Academic Journal 2012/2, S. 138; *Liu*, Journal of Henan Administrative Institute of Politics and Law, S. 104 f.

612 *Chen*, 2002, S. 35; siehe auch *Sun*, Tribune of Political Science and Law 2012/2, S. 108.

613 *Chen*, 2002, S. 37; *Kang*, Jianghai Academic Journal 2012/2, S. 138f.; *Liu*, Journal of Henan Administrative Institute of Politics and Law, S. 106.

614 *Ying*, Chinese Legal Science 2000/4, S. 6.

Verfassungsrechtlich ist anerkannt, dass jegliches staatliche Handeln, das grundlegende Bereiche betrifft, auf Grundlage eines Gesetzes erfolgen werden muss.[615] Insbesondere ist die Beschränkung der Grundrechte der Bürger aufgrund des Schutzes öffentlichen Interesses nur durch Gesetz zulässig. Das Gesetz muss sich hier auf die Vorgaben beziehen, die durch den Nationalen Volkskongress und seinen Ständigen Ausschuss erlassen werden[616] und dem Bestimmtheitsgebot genügen.

2. Zwecke

Art. 51 Verf VRC stellt eine allgemeine öffentliche Interessenklausel für die Rechtfertigung von Grundrechtseingriffen dar.[617] Die Grundrechte der Bürger dürfen danach allgemein zugunsten des Schutzes des öffentlichen Interesses beschränkt werden. In der Verfassung wird dieser Rechtsbegriff nicht genau festgestellt oder ihr Inhalt aufgelistet. Denn der Rechtsbegriff des „öffentlichen Interesses" sei erheblich abstrakt und ihre Inhalte könnten sich nach Entwicklung der Bedingungen der Gesellschaft ändern.[618] Der Gesetzgeber muss in einfachen Gesetzen den Inhalt des öffentlichen Interesses als Begründung der Beschränkung der Grundrechte immer konkret bestimmen, um eine willkürliche Beschränkung der Grundrechte zu verhindern.[619] Daneben stellt Art. 40 Verf VRC spezielle Eingriffsschranken auf. Zugunsten der staatlichen Sicherheit und der Aufklärung von Straftaten dürfen Eingriffe in das Korrespondenzgeheimnis vorgenommen werden. Der Begriff der staatlichen Sicherheit ist, wie der Begriff des öffentlichen Interesses, sehr weit.

Die Vorratsdatenspeicherung darf somit nur aufgrund des Schutzes überwiegender Interessen durchgeführt werden. Das durch Beschränkung der Grundrechte geschützte überwiegende Interesse ist in den Vorgaben der Vorratsdatenspeicherung konkret und deutlich zu verankern. Beschränkungen etwa „zum Zweck der öffentlichen Interessen", „zum Zweck der staatlichen Sicherheit" oder „zum Zweck der überwiegenden Interessen" reichen nicht aus.

---

615 Siehe hierzu *Yu*, Jurists´ Review 1999/3, S. 61 ff.; *Qin*/*Ye*, Law Review 2006/2, S. 9.

616 *Zhao*, Jurist 2011/2, S. 165; *Li*/*Zheng*, Jurists Review 2004/2, S. 66 ff.

617 *Hu*/*Wang*, Chinese Legal Science 2005/1, S. 23; *Han*, Legal Forum 2005/1, S. 9; *Zhao*, Jurist 2011/2, S. 163; *Shi*, Journal of Comparative 2014/5, S. 161.

618 *Chen*, Der Begriff des öffentlichen Interesses, in: *Chen*, Band 1, 2010, S. 259.

619 *Chen*, Der Begriff des öffentlichen Interesses, in: *Chen*, Band 1, 2010, S. 259; *Zhang*, Legal Forum 2005/1, S. 27.

3. Verhältnismäßigkeit

Das Verhältnismäßigkeitsprinzip wurzelt im Rechtsstaatsprinzip aus Art. 5 Verf VRC.[620] Das Rechtsstaatsprinzip ist folgenden Bestimmungen zu entnehmen:

„Kein Gesetz, keine administrative oder lokale Verordnung oder Vorschrift darf im Widerspruch zur Verfassung stehen. Alle Staatsorgane und Streitkräfte, alle politischen Parteien und gesellschaftlichen Organisationen und alle Betriebe und Institutionen müssen die Verfassung und die Gesetze einhalten."

Gemäß diesen Vorgaben ist eine Beschränkung der Grundrechte dem Verhältnismäßigkeitsprinzip zu unterwerfen, damit der Grundrechtsschutz nicht im Wesentlichen wegen der öffentlichen-Interesse-Klausel leerläuft. Zwar wird das Verhältnismäßigkeitsprinzip nicht ausdrücklich erwähnt, aber es ist als eine fundmentale Anforderung an die Verfassungsmäßigkeit staatlicher Eingriffe anerkannt. In der VR China wurde eine Verfassungsgerichtsbarkeit bislang nicht eingeführt, sodass eine Beschränkung der Grundrechte nicht durch Gerichte gemäß dem Verhältnismäßigkeitsprinzip überprüft werden kann. Jedoch muss der Gesetzgeber bei der Gesetzgebung dieses Prinzip beachten.[621] Das Verhältnismäßigkeitsprinzip verlangt, dass die Beschränkung der Grundrechte aufgrund legitimer Zwecke erfolgt. Ferner muss sie in Bezug auf den verfolgten Zweck geeignet, erforderlich und angemessen sein.[622] In Teil C dieses Kapitels werden die Anforderungen beschrieben, die zur Erfüllung dieser Voraussetzungen zu verlangen sind.

4. Fazit

Die Ausgestaltung der Vorratsdatenspeicherung in der VR China stellt einen Eingriff in das Korrespondenzgeheimnis dar. Die Darstellung der Anforderungen an die Eingriffsrechtfertigung legt den Schluss nahe, dass die mit den Regelungen zur Vorratsdatenspeicherung einhergehenden Eingriffe nicht gerechtfertigt sind. Dafür sind die Beschränkungen der Speicherung und insbesondere der Übermittlung und Weiterverwendung der Daten zu wenig ausgebildet. Im Gegenteil, es fehlt in den meisten Fällen an Beschränkungen. In

620 Siehe auch *Jiang*, 2005, S. 130 ff.; *Liu*, China Legal Science 2014/4, S. 137 ff.; *Men*, Legal Forum 2014/5, S. 95 ff.

621 Siehe auch *Zhao*, Jurist 2011/2, S. 166.

622 Die deutsche Dogmatik der Verhältnismäßigkeit wird in der VR China weitgehend rezipiert und angenommen; dazu siehe etwa *Jiang*, 2005; *Zhang*, Jurists Review 2008/1, S. 138 ff.; *Zhao*, Jurist 2011/2, S. 160 ff.; *Yu*/*Hong*, China Public Security (Academy Edition) 2007/3, S. 107 ff.; *Liu*, China Legal Science 2014/4, S. 133 ff.; *Men*, Legal Forum 2014/5, S. 94 ff.; *Hu*/*Xu*, Law Review 2005/6, S. 9 ff.

Anlehnung an die Anforderungen des EuGH könnte man sagen, dass die Vorratsdatenspeicherung nicht auf das Notwendige beschränkt ist. Zwar ist der grundrechtliche Schutz in China nicht so ausgeprägt und entwickelt wie in der EU und Deutschland. Die jetzige Ausgestaltung wird aber auch den Anforderungen der chinesischen Verfassung nicht gerecht.

Zwar ist das Rechtsgut der Sicherheit bisweilen schweren Bedrohungen in Form von Terrorismus und organisierter Kriminalität ausgesetzt, aber die Waage schlägt gegenwärtig zu sehr in Richtung Sicherheit aus. Die Vorratsdatenspeicherung in der vorliegenden Ausgestaltung beeinträchtigt den Grundrechtsschutz. Die Folgen werden sich angesichts der längst bestehenden Missachtung des Schutzes der Freiheit und Privatsphäre der Bürger in Zukunft wohl noch verschlimmern. Zu denken ist nur an das Personalakte-System zur Bewertung jedes einzelnen Bürgers. Wenn die Freiheitsgrundrechte und die Privatsphäre ausgehöhlt werden, wird der Sinn und Zweck von Sicherheit verloren gehen. Da es in der VR China an einer Verfassungsgerichtbarkeit und anderen effektiven Kontrollen über die Verfassungsmäßigkeit von Sicherheitsmaßnahmen fehlt, hängt der Grundrechtsschutz davon abhängen, dass der Gesetzgeber die verfassungsrechtlichen Grundsätze wie den Vorbehalt des Gesetzes, die Verhältnismäßigkeit und das Bestimmtheitsgebot in einfaches Recht umsetzt. Wegen der erheblichen negativen Wirkung der Vorratsdatenspeicherung auf die Grundrechte der Bürger, muss deren Ausgestaltung die verfassungsrechtlichen Grundsätze umso strenger einhalten. Zur Verwirklichung eines adäquaten Grundrechtsschutzes ist der Gesetzgeber verpflichtet, die Regelungen zur Vorratsdatenspeicherung neu auszugestalten.

C. Eckpunkte zur verfassungs- und insbesondere verhältnismäßigen Ausgestaltung der Vorratsdatenspeicherung in China – Orientierung am europäischen und deutschen Schutzniveau

Die bis hierhin herausgearbeiteten Probleme lassen sich nicht nur auf das noch unterentwickelte Gesetzgebungsniveau zurückführen, sondern auch auf die seit langem bestehende Missachtung der Freiheit und Privatsphäre der Bürger. Um dies zu ändern, wäre einer der schnellsten Wege den Zustand der Gesetzgebung in anderen Staaten kennenzulernen. Idealerweise könnte dies dazu führen, sich von den dortigen Gesetzen und Prinzipien inspirieren zu lassen. Die Gelegenheit ist nun günstig, insbesondere wenn die Gewährleistung der Grundrechte der Bürger inzwischen auch als Kernpunkt der Rechtspolitik in der VR China festgelegt wird. Das bedeutet aber nicht, dass jede Gesetzgebung eines anderen Staates in der VR China kopiert werden sollte. Sondern es ist wichtig zu untersuchen, wie ein Eingriff durch eine staatliche Sicherheitsmaßnahme durch die verfassungsmäßige Ausgestaltung effektiv beschränkt wird, um Grundrechte der Bürger zu schützen.

Die Vorratsdatenspeicherung dient in Deutschland und auch in China dem Zweck des Schutzes öffentlicher Sicherheit. Es ist für die chinesische Gesetzgebung daher sinnvoll zu untersuchen, wie das Fernmeldegeheimnis sowie andere relevante Grundrechte in Deutschland geschützt werden und wie die Ausgestaltung der Vorratsdatenspeicherung demgemäß beschränkt wird.[623] Gegebene Unterschiede sind zwar zu berücksichtigen, aber dies hindert nicht, gesetzgeberische Vorschläge für die Vorratsdatenspeicherung in Anlehnung an diejenigen in Deutschland zu machen, soweit die Vorschläge sachgerecht und mit dem gegenwärtigen Rechtsrahmen kompatibel sind. Folgende gesetzgeberische Anpassungen sind jedenfalls denkbar und teilweise auch notwendig.

---

623 Nach dem sogenannten Funktionalitätsprinzip der Rechtsvergleichung sei vergleichbar im Recht nur, was dieselbe Aufgabe und dieselbe Funktion erfülle, siehe *Zweigert*/*Kötz*, S. 33 ff.; siehe auch *Shen*, 1998, S. 30 ff. Die chinesische Gesetzgebung der Vorratsdatenspeicherung in Anlehnung an Deutschland zu verbessern setzt eine dem Funktionalitätsprinzip entsprechende Rechtsvergleichung voraus. Ist die Vorratsdatenspeicherung in beiden Ländern vergleichbar, kann die chinesische Ausgestaltung der Vorratsdatenspeicherung diejenige in Deutschland als Beispiel nehmen, um den Grundrechtsschutz zu stärken.

I. Verhältnismäßige Ausgestaltung des Schutzes für das Korrespondenzgeheimnis

Bislang wird der Schutz des Korrespondenzgeheimnisses noch nicht durch eine konkrete gesetzliche Regelung umgesetzt. Im Vergleich zu Inhaltsdaten wird die wesentliche Bedeutung der Verkehrsdaten für den Schutz des Korrespondenzgeheimnisses offensichtlich missachtet. Verkehrsdaten werden zurzeit nur als personenbezogene Daten durch allgemeine datenschutzrechtliche Regelungen geschützt. Dies führt zu einer großen Schutzlücke für das Korrespondenzgeheimnis. Momentan wird an einem Telekommunikationsgesetz gearbeitet. Das ist eine gute Gelegenheit, den Grundrechtsschutz des Korrespondenzgeheimnisses durch ein einfaches Gesetz umzusetzen. Konkret zu bestimmen sind wesentliche Begriffe, der Schutzbereich und die Schutzpflicht der Verpflichteten. Eine Wiederholung des Texts von Art. 40 Verf VRC reicht hierfür nicht aus. Dies wäre auch eine Annäherung an die Ausformung eines Datenschutzrechts.

Insbesondere sind Ausnahmeregelungen vom Schutz des Korrespondenzgeheimnisses festzulegen. Statt Verwaltungsregeln und Abteilungsregeln des Ministeriums darf die Vorratsdatenspeicherung nur durch ein künftiges Telekommunikationsgesetz geregelt werden. Angesichts des hohen Ranges des Korrespondenzgeheimnisses und auch des ausdrücklichen qualifizierten Vorbehalts aus Art. 40 Verf VRC ist vorzuschlagen, dass die Vorratsdaten nicht mehr für die Untersuchung von Ordnungswidrigkeiten verwendet werden dürfen. Ferner ist im Gesetz klarzustellen, dass die Vorratsdatenspeicherung darüber hinaus den vorhandenen allgemeinen datenschutzrechtlichen Regelungen entsprechen muss. Das Datenschutzniveau bei der Vorratsdatenspeicherung darf zumindest nicht niedriger als das vorhandene Schutzniveau gesetzt werden.

II. Bestimmtheitsgebot

Der Vorbehalt des Gesetzes verlangt, dass alles staatliche Handeln in grundlegenden Bereichen nur auf Grundlage eines förmlichen Gesetzes zulässig ist.[624] Die Einhaltung dieses Grundsatzes setzt die ausreichende Bestimmtheit der gesetzlichen Grundlage voraus. Das Bestimmtheitsgebot ist umso strenger zu befolgen, wenn grundrechtseinschränkende Normen mit gewichtigen Auswirkungen erlassen werden.[625] Das Problem der Vorratsdatenspei-

---

624 Dies ist insbesondere in der deutschen Rechtswissenschaft gut ausgebildet, siehe etwa *Jarass*, in: Jarass/Pieroth, GG, Art. 20, Rn. 69.

625 BVerfGE 41, 251 (264); 110, 33 (55); 130, 372 (388 ff.); *Schenke*, in: *Stern*/*Becker*

cherung in der VR China liegt darin, dass die vorhandenen Rechtsvorschriften immer sehr allgemein und unbestimmt geregelt werden. Dies kann zu einer totalen Speicherung und uferlosen Befugnis zum Zugriff führen.

Zum Beispiel ist der Begriff der Nutzungsdaten bislang nicht hinreichend bestimmt. Im chinesischen Kontext können Nutzungsdaten jedoch alle personenbezogenen Daten bedeuten, die wegen der Nutzung von Telekommunikations- sowie Telemediendienste angefallen sind. Unter anderem werden befugte Behörden sowie konkrete Voraussetzungen des Zugriffs und der Verwendung nicht bestimmt. Wegen der schwerwiegenden Eingriffsintensität der Vorratsdatenspeicherung muss klar festgelegt werden, welcher Behörde der Zugriff gestattet wird. Schlichte Verweise auf die „befugte Behörde", „zuständige Behörde" oder „betroffene Behörde" reichen nicht aus. Eine pauschale Erteilung der Verwendungsbefugnis genügt dem Bestimmtheitsgrundsatz ebenso nicht. Materielle Voraussetzung des Zugriffs und der Verwendung von Vorratsdaten müssen konkret und klar aufgelistet werden.

Das Gesetzgebungsgesetz der VR China vom 15.3.2000 wurde am 15.3.2015 novelliert. In § 6 GGebG wurde hinzufügt, dass gesetzliche Vorschriften eindeutig, konkret, gezielt und durchsetzbar sein müssen. Demgemäß hat die Ausgestaltung der Vorratsdatenspeicherung großen Raum für Verbesserungen.

III. Materielle, datenschutzrechtliche Anforderungen in den jeweiligen Vorschriften zur Vorratsdatenspeicherung

Es sind datenschutzrechtliche Regelungen bei der Vorratsdatenspeicherung selbst spezifisch vorzuschreiben. Die Grundsätze des Datenschutzrechts wie Zweckbestimmung und Zweckbindung sind in der Regelung für die Speicherung und Verwendung der Vorratsdaten umzusetzen. Daraufhin ist mindestens der Zweck der Vorratsdatenspeicherung klar und bestimmt festzulegen. Ferner sind Regelungen zur Höchstspeicherungsdauer und zur Löschungspflicht erforderlich. Eine Regelung des Verfahrens bezüglich der Speicherung und Übermittlung von Vorratsdaten ist auch erforderlich, um unbefugten Zugriff und Enthüllung der Vorratsdaten zu verhindern. Die Vorratsdatenspeicherung betrifft die Speicherung und Verwendung zahlreicher personenbezogener Daten. Ohne Regelung des Datenschutzes sowie der Datensicherheit ist sie nicht verhältnismäßig.

(Hrsg.), GG, Art. 10 Rn. 73.

IV. Bestimmungen zum Datenschutz und zur Datensicherheit im Allgemeinen

Zurzeit fehlt in der VR China ein einheitliches Datenschutzgesetz, die vorhandenen verstreuten datenschutzrechtlichen Regelungen[626] können einen wirksamen Schutz der Telekommunikationsdaten der Nutzer nicht gewährleisten. Die große Schutzlücke bei der Vorratsdatenspeicherung bezüglich des Datenschutzes sowie der Datensicherheit geht insbesondere auf das Fehlen von Ausnahmeregelungen für Vorratsdaten zurück.

In den Telekommunikationsregeln aus dem Jahr 2000 wird nur die Sicherheit des Telekommunikationsnetzes sowie der Telekommunikationsdaten betont.[627] Neben der Gewährleistung der physischen Integrität der gespeicherten Daten und des reibungslosen Funktionierens des Informationssystems werden jedoch das Verbot der illegalen Informationen und der Schutz des Korrespondenzgeheimnisses auch im Teil über Datensicherheit geregelt. Bisher herrscht die rechtspolitische Tendenz vor, Datensicherheit als allumfassende Kategorie einzusetzen und Schutzlücken des Datenschutzrechts in diesem Bereich durch Gewährleistung der Datensicherheit auszufüllen.

Dies lässt einerseits die Relevanz der Grundrechte bezüglich der Verarbeitung personenbezogener Daten in den Hintergrund treten, andererseits verwischt es die Schutzzwecke der Datensicherheit und des Datenschutzrechts. Während die Datensicherheit die physische Integrität des Informationssystems sowie der darin gespeicherten Daten durch die Entwicklung der Technik gewährleistet, handelt es sich beim Datenschutzrecht im Wesentlichen um das mit dem Umgang mit personenbezogenen Daten verbundene Persönlichkeitsrecht des Einzelnen durch Ausgestaltung der Rechte sowie Pflichten rund um die Erhebung, Verarbeitung und Verwendung personenbezogener Daten.[628] Zwar stellt die Datensicherheit eine unentbehrliche Voraussetzung des Datenschutzrechts – sie ist aber kein eigentliches Ziel des Datenschutzrechts. In den neuerlichen „Regeln zum Schutz der personenbezogenen Daten der Nutzer von Telekommunikations- und Internetdienste“ werden den Diensteanbietern grundsätzliche Regelungen für die Speicherung und Verwendung personenbezogener Daten der Nutzer auferlegt und vorbeugende technische sowie organisatorische Maßnahmen für die Datensicherheit angeordnet. Die Vorratsdatenspeicherung stellt eine Ausnahme zu den daten-

626 Siehe hierzu Kapitel 3, A.II.4.
627 §§ 57-66 Telekommunikationsregeln der VR China.
628 Siehe auch *Ernestus*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, S. 270, Rn. 1 ff.; *Lou*, 2010, S. 82 ff.

schutzrechtlichen Anforderungen dar. Als solcher geht es bei ihr nicht um die Vereinbarkeit mit diesen Anforderungen.

Ein einheitliches Datenschutzgesetz ist schon lange erwartet worden. Für ein einheitliches Datenschutzgesetz ist zu empfehlen, den Schutzzweck eindeutig festzulegen und den Datenschutz somit vom Schutz der Datensicherheit klar zu unterscheiden. Unter anderem sind im Zusammenhang bzw. teilweise synonym mit „personenbezogenen Daten" verwendete Begriffe wie „elektronische Daten" und „Online-Daten" zu vereinheitlichen. Dem Zweck des Datenschutzrechts entsprechend sind alle personenbezogenen Daten zu schützen, unabhängig von ihrem Medium, ihrer Form und Quelle, auch unabhängig davon, ob sie aus der Privatsphäre der Bürger herrühren. Man kann hier die Rechtsprechung des deutschen Bundesverfassungsgerichts zum Vorbild nehmen, dass es kein belangloses Datum gibt.[629]

In dem aktuellen normativen Dokument „Erklärung zu einigen Fragen bei Strafverfolgung der Kriminalität über Missbrauch der personenbezogenen Daten der Bürger", das der Oberste Volksgerichtshof und die Oberste Staatsanwaltschaft gemeinsam am 8.5.2017 erlassen haben, wurden personenbezogene Daten zum ersten Mal klar definiert. Personenbezogenen Daten sind demnach alle Daten, die in elektronischer oder anderer Form dargestellt werden und selbst oder mit anderen Daten zusammen bestimmte natürliche Personen identifizieren oder ihre Handlung widerspiegeln können. Einbezogen sind Name, Nummer des Ausweises, Anschrift, Adresse, Konto, Passwörter, Finanzen, Bewegungsprofil etc. Dies ist eine empfehlenswerte Definition der personenbezogenen Daten. Es ist denkbar, sich in anderen Regelungswerken auf diese Bestimmung zu beziehen, bis sie schließlich gesetzlich festgeschrieben wird.

V. Richterliche Kontrolle: Verfahrensrechtliche Gewährleistung des Grundrechtsschutzes

1. Problemstellung

In der VR China ist allgemein anerkannt, dass die Gewährleistung der Grundrechte der Bürger die wichtigste Aufgabe und das Ziel der Verfassung darstellt. Jedoch sind die Grundrechte der Bürger in der VR China noch nicht wirksam geschützt. Der Grund liegt vor allem darin, dass der Schutz der Grundrechte in der Verfassung nicht durch einfache Gesetze in vollem Um-

629 BVerfGE 65, 1 (45).

fang umgesetzt wird. Das Korrespondenzgeheimnis wird zwar in der Verfassung festgelegt und die Voraussetzung seiner Einschränkung im Vergleich zu anderen Grundrechte wird recht streng geregelt, aber in einfachen Gesetzen wie zum Beispiel die Strafprozessordnung und in Verwaltungsregeln wie den Telekommunikationsregeln wird der Schutz des Korrespondenzgeheimnisses einfach durch Wiederholung des Verfassungstexts vorgeschrieben, ohne weitere Konkretisierungen aufzustellen. Es lässt den Behörden zu großen Spielraum bei der Anwendung der Gesetze. Ohne konkrete Maßstäbe ist es auch schwierig für Richter, die Rechtmäßigkeit der Anwendung der Gesetze von den Behörden zu beurteilen.

Der Grund des unwirksamen Grundrechtsschutzes liegt unter anderem im Fehlen wirksamer Kontrolle öffentlicher Gewalt, vor allem durch eine Verfassungsgerichtsbarkeit. Die institutionalisierte Verfassungsgerichtsbarkeit spielt eine besonders wichtige Rolle bei der Effektivierung der Grundrechte.[630] Ohne die Verfassungsgerichtsbarkeit kann die öffentliche Gewalt nicht effektiv daraufhin überwacht werden, dass sie stets an die Maßstäbe der Verfassung gebunden ist.[631]

Über die Verfassungsgerichtsbarkeit wird in der VR China schon lange diskutiert. Sie wird z.T. gefordert,[632] aber dies bleibt bedauerlicherweise nur auf der theoretischen Ebene. Unter dem vorhandenen Rechtsrahmen darf der Bürger gegen einen Eingriff durch staatliche Stellen nicht Verfassungsbeschwerde erheben. Der Bürger darf gegen ein Gesetz vor dem Ständigen Ausschuss des Volkskongresses Normenkontrolle beantragen. Jedoch sind derartige Anträge bislang noch nicht einmal bearbeitet worden. Daraus ergibt sich das Problem, dass die Grundrechte zwar ausdrücklich im Verfassungstext normiert werden, aber kaum Wirkung entfalten. Mangels der institutionalisierten Verfassungsgerichtsbarkeit können die Bindungswirkungen der Verfassung momentan in der VR China kaum garantiert werden. Um die künftige Gesetzgebung zur Vorratsdatenspeicherung und auch andere vergleichbare Maßnahmen zu verbessern, sollte der Gesetzgeber vor allem den Rechtsweg durch ausdrückliche Regelungen im Verwaltungsprozessgesetz garantieren.

---

630 Dazu siehe *Dreier*, in: *Dreier* (Hrsg.), GG 2013, Vorbemerkungen, Rn. 58.

631 BVerfGE 6, 32 (40 f.); *Stern*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Einleitung, Rn. 110.

632 Dazu siehe zum Beispiel *Mo*, 2006; *Liu*, *Daoqin*, 2013; *Hu*, Jurists Review 1993/1, S. 51 ff.; *Xie*, *Weiyan*, in: *Mo*/*Xie* (Hrsg.) 2009, S. 260 ff.; *Cai*, Chinese Journal of Law 2005/5, S. 110 ff.

Mit der Einführung einer Verfassungsgerichtsbarkeit ist aber nicht zu rechnen. Es muss aber eine Problemlösung innerhalb des vorhandenen Rechtsrahmens gefunden werden. Dazu gehören die Auslegung der Verfassung durch den Ständigen Ausschuss des Nationalen Volkskongresses, die Anwendung der Verfassung im Einzelfall vom Volksgericht und eine Möglichkeit zur konkreten Normenkontrolle vor den Volksgerichten.

2. Richtervorbehalt zur Gewährleistung des Grundrechtsschutzes

Eine der erforderlichen Voraussetzung für wirksamen Grundrechtsschutz bei der Vorratsdatenspeicherung liegt darin, den Eingriff durch verfahrensrechtliche Vorkehrungen effektiv zu beschränken. Daraufhin ist insbesondere der Richtervorbehalt zu empfehlen. Mangels Verfassungsgerichtsbarkeit – eine nachträgliche gerichtliche Kontrolle der öffentlichen Gewalt – ist der Richtervorbehalt vor dem Zugriff und der Verwendung der Vorratsdaten von erheblicher Bedeutung.

In der Strafprozessordnung der VR China wird ein Richtervorbehalt für die Durchführung von Maßnahmen zur Strafverfolgung nicht ausdrücklich festgesetzt. Geregelt wird nur, dass die Durchführung technischer Maßnahmen zur Strafverfolgung durch strenge Billigung zulässig ist.[633] Jedoch wird der Umfang der technischen Maßnahmen, die für die Billigung zuständige Stelle und das konkrete Verfahren der Billigung nicht geregelt. In der Praxis wird die Billigung infolgedessen kaum eingeholt. Die Anforderung einer vorherigen Kontrolle für die Durchführung technischer Maßnahmen läuft grundsätzlich leer.[634] Es ist zu empfehlen, dass der Zugriff auf und die Verwendung der Vorratsdaten als technische Maßnahme zur Strafverfolgung der Strafprozessordnung unterstellt wird und dem Richtervorbehalt unterliegt.

Unter anderem verlangt der wirksame Grundrechtsschutz, dass bei einer Rechtsverletzung die tatsächliche Möglichkeit garantiert werden muss, die Gerichte anzurufen. Dafür ist vor allem die Benachrichtigungspflicht bei der Ausgestaltung der Vorratsdatenspeicherung sicherzustellen. Bezüglich der Garantie des effektiven Rechtswegs ist die Tatsache zu berücksichtigen, dass in China keine Verfassungsgerichtsbarkeit vorliegt.

---

633 § 148 Strafprozessordnung der VR China vom 01.07.1979, geändert am 17. 03. 1996 und am 14.03.2012.

634 Dazu siehe *Lan*, Criminal Science 2013/1, S. 66 ff.; *Cheng*, Tribune of Political Science and Law 2011/5, S. 76 ff.

3. Die Auslegung der Verfassung durch den Ständigen Ausschuss des Nationalen Volkskongresses

Wie oben erwähnt sind rechtliche Bestimmungen in der VR China häufig sehr abstrakt und nicht ausreichend konkretisiert. Das führt zur Willkür bei ihrer Anwendung. Eine nähere verfassungskonforme Interpretation ist stets nötig. Da die Verfassung an sich wegen ihrer Eigenschaft als grundlegende Bestimmung hoch abstrakt dargestellt wird, kann sich die Auslegung der Verfassung unter diesen Umständen auf die Gesetzgebung positiv auswirken.

Nach Art. 67 Abs. 1 Verf VRC hat der Ständige Ausschuss des Nationalen Volkskongresses die Befugnis, die Verfassung auszulegen. Eine derartige Auslegung ist rechtverbindlich.[635] Auf diese Weise soll der Ständige Ausschuss des Nationalen Volkskongresses konkrete Anforderungen und Maßstäbe des Grundrechtsschutzes zu den gesellschaftlichen Bedingungen passend festlegen, um das Defizit in der Gesetzgebung zu kompensieren und gleichzeitig eine zu häufige Änderung von Gesetzen zu vermeiden.[636] In diesem Sinne fungiert eine derartige Auslegung in der VR China als ergänzende Gesetzgebung.

Jedoch werden Anlass, Verfahren für eine Vorlage des Auslegungsantrags sowie das Auslegungsverfahren selbst nicht weiter vorgeschrieben. Bislang wurde in der Praxis noch nie ein Auslegungsantrag im Sinne des Art. 67 Abs. 1 Verf VRC vorgelegt. In der Praxis werden Auslegungsanträge durch den Gerichtshof zur genauen Bedeutung bestimmter Rechtsvorschrift im Einzelfall vorgelegt, manchmal können dann einzelne für ein Grundrecht relevante Begriffe betroffen sein. Die rechtlichen Auswirkungen einer derartigen Antwort des Ständigen Ausschuss des Nationalen Volkskongresses sind nicht klar. Zwar kann auf die Antwort als Entscheidungsgrundlage verwiesen werden, jedoch ist sie keine Auslegung im Sinne von Art. 67 Abs. 1 Verf VRC.

Um die Funktion der Auslegung der Verfassung im Sinne des Art. 67 Abs. 1 Verf VRC zu gewährleisten, sind genaue Regelungen über das Verfahren für die Vorlage, über die Form des Auslegungsantrags sowie über das Auslegungsverfahren festzusetzen. So wurde ein Entwurf für ein Gesetz über das Verfahren zur Auslegung der Verfassung schon im Jahr 2007 von Akademi-

635 Ausführliche Darstellung hierzu siehe *Bu*, 2009, S. 19 ff.

636 Vgl. *Qin*, Social Sciences in Chinese Higher Education Institutions, 2015/3, S. 25; Han, Zhejiang Social Sciences 2009/9, S. 16.

kern ausgearbeitet.[637] In diesem Entwurf werden zwischen einer Auslegung auf Antrag und einer Auslegung von Amts wegen differenziert. Antragsteller, Gründe des Auslegungsantrags und das konkrete Verfahren wie Entwurf, Lesung, Abstimmung, Verabschiedung sowie Bekanntmachung der Auslegung werden ausführlich geregelt. Wenn diesem Entwurf zugestimmt wird, kann das Gesetz die Lücke des Auslegungsverfahrens ausfüllen, ein gut funktionierendes Auslegungssystem in Bezug auf die Verfassung könnte die fehlende Verbindung zwischen der Verfassung und der Gesetzgebung im vorhandenen Rechtsrahmen zum Teil abmildern.

4. Die Anwendung der Verfassung durch den Gerichtshof

In Deutschland spielt das Bundesverfassungsgericht die ausschlaggebende Rolle bei der Gewährleistung der Grundrechte. Durch die wiederholten den Gesellschaftsbedingungen anpassenden Anwendungen hat der abstrakte Verfassungstext die nötige Vitalität erhalten, um die Funktion des Grundrechtsschutzes zu entfalten und sich weiter zu entwickeln. Somit ist es für einen zuverlässig funktionierenden Grundrechtsschutz von Bedeutung, eine spezielle Stelle vorzusehen, deren Aufgabe es ist, die Verfassungsmäßigkeit von staatlichem Handeln zu überprüfen.[638] In der VR China ist kein Verfassungsgericht eingerichtet. Unter dem vorhandenen Rechtsrahmen kann der Bürger auch keine Verfassungsbeschwerde beim Volksgericht erheben. In der VR China wird der Grundsatz der Gewaltenteilung nicht be- und verfolgt. Der Nationale Volkskongress mit seinen Ständigen Ausschuss ist das höchste Machtorgan. Im vorhandenen Rechtsrahmen der VR China hat das Volksgericht keine Befugnis, gesetzliche Bestimmungen und anderes hoheitliches Handeln wegen Verfassungswidrigkeit als ungültig sowie verfassungswidrig zu erklären. Allerdings haben sich die Volksgerichte in der Praxis gelegentlich auf die Verfassung berufen und als Grundlage für ein Urteils angewendet, wenn keine konkreten gesetzlichen Bestimmungen für eine Beurteilung vorhanden waren. Somit wird die Möglichkeit diskutiert, dass die Verfassung von den allgemeinen Volksgerichten angewendet werden kann.

Die Diskussion hat mit dem sogenannten „Ersten Fall der Justizialisierung der Verfassung“ im Jahr 1999 begonnen, bei dem sich ein Mittleres Volksgericht in einem Zivilprozess auf das Recht auf Bildung oder das Recht auf Erziehung aus Art. 46 Verf VRC bezogen hat. Beim Berufungsprozess hat das

---

637 Der chinesische Text dieses Entwurfs ist abrufbar unter: http://www.calaw.cn/article/default.asp?id=10166 [31.1.2019].

638 Vgl. *Han*, Study & Exploration 2007/1, S. 95.

Berufungsgericht sich über die Anwendung gesetzlicher Bestimmungen an das Oberste Volksgericht gewandt. Das Oberste Volksgericht hat in seiner Antwort vom 13.8.2001 festgestellt, dass das Recht der Klägerin auf Bildung aus Art. 46 Verf VRC verletzt wurde und die Beklagte der zivilrechtlichen Haftung unterfällt.[639] Diese Antwort des Obersten Volksgerichts wird als Anerkennung dafür angesehen, dass die Volksgerichte die Verfassung anwenden können. Allerdings wurde diese Auslegung am 24.12.2008 vom Obstersten Volksgericht ohne klare Begründung aufgehoben.[640] Über diese Frage gibt es bislang keine weitere offizielle Klarstellung. Die Zukunft der Anwendung der Verfassung ist somit weiterhin unklar.

Bei dieser Diskussion ist besonders zu verdeutlichen, dass vorliegende weder die Verfassungsgerichtsbarkeit noch die Justizialisierung der Verfassung das entscheidende Thema ist, sondern lediglich die Berufung auf die oder Auslegung der Verfassung von durch die Volksgerichte. Im vorhandenen Rechtsrahmen dürfen die Volksgerichte hoheitliches Handeln nicht aufgrund der Verfassung als verfassungswidrig erklären. Eine Beauftragung der Volksgerichte mit Aufgaben der Verfassungsgerichtsbarkeit ist mit dem vorhandenen politischen System sowie Rechtsrahmen unvereinbar.[641]

Zwar ist der vorhandene Rechtsrahmen zu berücksichtigen, aber die Anwendung der Verfassung von den Volksgerichten ist nicht von vornherein ausgeschlossen. Diskutiert wird die Möglichkeit, dass die Volksgerichte ihre Entscheidungen auf eine Auslegung der Verfassung gründen oder die gesetzliche Bestimmung, auf die es bei der Entscheidung ankommt, verfassungskonform auslegen. Diese sogenannte *„unmittelbare Anwendung“* der Verfassung wird von manchen Ansichten als einen möglichen Versuch im vorhandenen

639 Antwort vom Obersten Volksgericht über die Frage, ob man zivilrechtliche Haftung leisten muss, wenn er wegen Verletzung des Namensrechts in § 99 Allgemeine Grundsätze des Zivilrechts der VR China das Recht auf Bildung in Art. 46 Verf VRC verletzt, Juristische Auslegung, 2001, Nr. 25 vom 28.6.2001, abrufbar unter: http://gongbao.court.gov.cn/Details/635e70e2ab2f5969810116dbdff1f1.html [31.1.2019].

640 Beschluss von dem Obersten Volksgericht über Aufhebung folgender juristischen Auslegung vor dem Jahr 2007, Juristische Auslegung [2008] Nr. 15 vom 8.12.2008, abrufbar unter: http://www.npc.gov.cn/npc/xinwen/fztd/sfjs/2008-12/27/content_1465018.htm. Der Text des Berufungsurteil ist abrufbar unter: https://www.itslaw.com/detail?judgementId=01789f20-e91d-4f77-9aa0-4271e2dfc5d0&area=1&index=1&sortType=1&count=2&conditions=searchWord%2B 齐 玉 苓%2B1%2B 齐玉苓.

641 Siehe. *Hu*, Journal of Renmin University of China 1997/5, S. 62; *Xu*, The People´s Congress of China 2006/11, S. 45; *Tong*, China Legal Science 2008/6, S. 24; *Qin*, Journal of Comparative Law 2018/2, S. 69 f.; *Zhang*, China Legal Science 2008/3, S. 110 f.; *Xia*, Social Sciences in Guangdong, 2013/2, S. 237.

Rechtsrahmen angesehen, das Funktionieren der Verfassung durch die Volksgerichte zu fördern.[642] Der Ansatz der verfassungskonformen Auslegung der Gesetze in Deutschland wird als eine Argumentation für eine sogenannte „unmittelbare Anwendung" der Verfassung in der VR China allgemein vertreten. Jedoch stellt die verfassungskonforme Auslegung in Deutschland eine Methode der Auswahl mehrerer Auslegungsmöglichkeiten dar, damit Normerhaltung verwirklicht und die richterliche Zurückhaltung gegenüber dem Gesetzgeber gewahrt wird.[643] Die Entwicklung dieses Ansatzes ist eng mit der Verfassungsgerichtsbarkeit verbunden, die es in der VR China nicht gibt. Unter der verfassungskonformen Auslegung wird in großen Teilen der chinesischen Literatur vielmehr die Auslegung anhand der Verfassung verstanden.[644] Zwar wird dieser Ansatz in der VR China unterschiedlich verstanden,[645] aber die Absicht der Einführung dieses Ansatzes ist einheitlich und klar: Den Volksgerichte soll die Befugnis zur Auslegung der Verfassung und der damit verbundenen Anwendung der Verfassung erteilt werden.

Gegen die Anwendung der Verfassung durch die Volksgerichte spricht, dass nach der Verfassung der VR China nur der Ständige Ausschuss des Nationalen Volkskongresses die Befugnis hat, die Verfassung auszulegen. Damit dürfen die Volksgerichte die Verfassung nicht auslegen und auf Grundlage solcher Auslegung urteilen.[646] Hinzu kommt, dass nach Art. 131 Verf VRC die Volksgerichte ihre Gerichtsbarkeit gemäß den gesetzlichen Bestimmungen ausüben müssen. Die hiermit gemeinten gesetzlichen Bestimmungen umfassen die Verfassung nicht. Somit wird die Anwendung der Verfassung durch die Volksgerichte ausgeschlossen.[647] Darüber hinaus stelle die Verfassung die Grundlage des Gesetzes und maßgebliche Bestimmung dar. Sie dürfe wegen ihrer höchsten Abstraktheit nicht bei der Beurteilung herangezogen werden.[648]

---

642 *Shangguan*, Modern Law Science, 2008/2, S. 3 ff.; *Zhang*, China Legal Science 2008/3, S. 111 ff.; *Huang*, China Legal Science 2014/1, S. 293 ff.; *Zhu*, Modern Law Science 2017/1, S. 5 f.

643 *Dreier*, in: *Dreier* (Hrsg.), GG 2013, Art. 1 III Rn. 85; *Stern*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Einleitung Rn. 110; *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 20 Rn.67; BVerfG 49, 148 (157); 69, 1 (55); 83, 201 (214f); 95, 64 (93); 101, 312 (329).

644 Siehe auch *Wang*, The Jurist 2015/1, S. 45 ff.

645 Siehe *Huang*, China Legal Science 2014/6, S.281 ff.; *Wang*, The Jurist 2015/1, S. 45 ff.; *Zhang*, China Legal Science 2008/3, S. 111 ff.; *Xia*, China Legal Science 2017/1, S. 289 ff.; *Xie*, Zhejiang Academic Journal, 2014/6, S. 156 f.; *Xie*, Zhejiang Academic Journal, 2014/6, S. 156 f.

646 *Zhang*, China Legal Science 2008/3, S. 111; siehe auch *Huang*, China Legal Science 2014/6, S. 283.

647 *Tong*, China Legal Science 2008/6, S. 24.

648 *Hu*, Journal of Renmin University of China 1997/5, S. 60.

Die Abstraktheit der Verfassung ist jedoch keine zutreffende Argumentation gegen ihre Anwendung. Im Gegenteil begründet sie genau das Bedürfnis, die Verfassung bei der Anwendung stets auszulegen. Da die Auslegung der Verfassung vom Ständigen Ausschuss des Nationalen Volkskongresses in der Praxis mangels konkreter Regelung des Verfahrens faktisch nicht funktioniert, ist eine juristische Auslegung der Verfassung und darauf begründete Auslegung der gesetzlichen Bestimmung umso wichtiger, um eine bloße Formalität der Verfassung zu vermeiden. Das Problem bei der „unmittelbaren Anwendung" der Verfassung liegt allerdings darin, dass die effektive Kontrolle der Durchsetzung der Verfassung kaum wirklich gefördert wird, wenn die Volksgerichte die Verfassung zwar auslegen, sie jedoch nicht als Grundlage für eine etwaige Verfassungswidrigkeit staatlichen Handelns heranziehen dürfen.[649] Ohne die Garantie einer Verfassungsgerichtsbarkeit kann die sogenannte „unmittelbare Anwendung" der Verfassung die Anwendung der Verfassung nicht allein ersetzen. Diese dem vorhandenen Rechtsrahmen kompatibel erscheinende Anwendung kann eine Störung im Verhältnis zwischen den Volksgerichten und dem Gesetzgeber erzeugen.[650] Damit ist der Versuch, die „unmittelbare Auslegung" der Verfassung als Zwischenlösung für den Mangel an einer Verfassungsgerichtsbarkeit zu fördern, zwar konstruktiv, aber er hat wohl keine Aussicht auf Erfolg.

Diskutiert wird auch, ob die Volksgerichte die Verfassung in Privatrechtsbeziehungen anwenden können. Die Befürworter begründen die Durchsetzbarkeit der Anwendung der Verfassung in Privatrechtsbeziehungen vor allem mit der Theorie der Drittwirkung in Deutschland.[651] Bei der sogenannten Drittwirkung von Grundrechten wird in Deutschland zwischen der unmittelbaren und mittelbaren Drittwirkung differenziert. Die unmittelbare Drittwirkung ist sehr umstritten und damit nicht umfassend akzeptiert, während die mittelbare Drittwirkung in der Rechtsprechung und Literatur anerkannt wird. Gemäß ihr fungieren die Grundrechte nicht nur als Abwehrrechte, sondern auch als objektive Wertordnung. Der Richter hat zivilrechtliche Vorschriften im Lichte der Grundrechte auszulegen und anzuwenden.[652] Die Theorie der Drittwirkung in Deutschland ist sehr speziell und in Bezug auf Einzelheiten immer

649 Vgl. *Wang*, The Jurist 2015/1, S. 56 f.; *Xia*, China Legal Science 2017/1, S. 292.

650 Siehe *Xie*, China Legal Science 2009/6, S. 174 f.

651 *Feng*, Chinese Journal of Law 2017/3, S. 53 f.; *Chen*/*Qin*, Journal of Henan Administrative Institute of Politics and Law 2006/2, S. 52 ff.; *Jiao*/*Jia*, Xiamen University Law Review 2003/1, S. 234 ff.

652 *Jarass*, in: *Jarass*/*Pieroth*, GG 2016, Art. 1 Rn. 48, 52ff; *Dreier*, in: *Dreier* (Hrsg.), GG 2013, Vorb. Rn. 96 ff.; *Stern*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Einl. Rn. 42 ff.

noch umstritten. Sie ist mit der Entwicklung der Grundrechtstheorie in Deutschland sehr eng verbunden; eine direkte Anwendung der Drittwirkung in der VR China ist somit fundamentlos.[653] Deswegen ist die Geeignetheit der Anwendung der Verfassung in Privatrechtsbeziehungen momentan noch zu überdenken.

5. Konkrete Normenkontrollvorlagen durch die Volksgerichte

Gegen einen staatlichen Eingriff in die Grundrechte gibt es für den Bürger momentan zwei Rechtswege, und zwar die Verwaltungsklage und die Normenkontrolle. Wegen der engen Zulässigkeitsvoraussetzungen nach dem chinesischen Verwaltungsprozessgesetz (VwPG) kann der Bürger nicht gegen alle staatlichen Eingriffe Klage erheben. Um den Rechtsschutz zu verbessern, wurde das Verwaltungsprozessgesetz der VR China im Jahr 2014 novelliert. Der Umfang der klagefähigen Sachverhalte wurde erweitert und in neu hinzugefügten Vorgaben in § 3 VwPG wurde betont, dass das Recht der Bürger, juristischer Personen und sonstiger Organisationen, Klage zu erheben, gewährleistet werden muss. Trotzdem wurden Eingriffe in das Korrespondenzgeheimnis, wie zum Beispiel unbefugte Zugriffe auf und Missbrauch der Telekommunikationsdaten der Betroffenen von staatlichen Behörden immer noch nicht ausdrücklich in den Katalog der klagefähigen Sachverhalte erfasst.

Ein anderer möglicher Rechtsweg liegt in der Normenkontrolle nach § 99 GGebG VRC. Der Bürger kann, wie ausgeführt, dem Ständigen Ausschuss des Nationalen Volkskongresses einen schriftlichen Antrag auf Normenkontrolle für den Fall vorlegen, dass eine Verwaltungsrechtsnorm, territoriale Rechtsnorm, Autonomie- oder Einzelverordnung mit der Verfassung unvereinbar ist. Problematisch ist, dass dieses Recht auf Antrag einer Normenkontrolle nicht rechtsverbindlich ausgestaltet ist. Des Weiteren liegen keine konkreten Vorgaben für das Verfahren der Normenkontrolle und keine rechtlichen Maßstäbe für die Überprüfung vor. Die Normenkontrolle ist infolgedessen kaum durchsetzbar.[654] Seitdem das Gesetzgebungsgesetz in Kraft getreten ist, wurde kein vorgelegter Antrag vom Ständigen Ausschuss des Nationalen Volkskongress beantwortet.[655] Deswegen kann der Rechtsweg bei der Vorratsdatenspeicherung nicht durch die Normenkontrolle garantiert werden.

---

653 Siehe auch *Xia*, Social Sciences in Guangdong, 2013/2, S. 239 f.

654 Dazu siehe auch *Hu*, Studies in Law and Business 2003/5, S. 3 ff.; *Ye*, Journal of the Party School of CPC Xiamen Municipal Committee 2008/3, S. 40 ff.; *Wang*, Northern Legal Science 2010/1, S. 29.

655 Dazu siehe *Wang*, in: *Mo*/*Xie* (Hrsg.) 2009, S. 235.

In § 99 GGebG VRC wird geregelt, dass der Ständige Ausschuss des Nationalen Volkskongresses nach Antrag die Verfassungsmäßigkeit einer Verwaltungsrechtsnorm, territorialen Rechtsnorm oder Autonomie- oder Einzelverordnung prüft. Jedoch werden Gesetze und Abteilungsregeln eines Ministeriums nicht von der Normenkontrolle erfasst. Außerdem wurde keine weiteren Regelungen über das Verfahren des Antrags sowie das Verfahren der Prüfung erlassen.

In der Verfassung der VR China wird ausdrücklich im Art. 5 Verf VRC festgestellt, dass kein Gesetz, keine Verwaltungsrechtsnorm und territoriale Rechtsnorm im Widerspruch zur Verfassung stehen darf. Die Bindung an die Verfassung der gesetzgeberischen Gewalt muss demgemäß kontrolliert werden. Nach Art. 57 Verf VRC ist der Nationale Volkskongress und sein Ständiger Ausschuss das höchste Machtorgan und es kontrolliert nach Art. 62 und 67 Verf VRC die Durchsetzung der Verfassung. Im Art. 99 GGebG VRC werden Gesetze von der Normenkontrolle ausgespart. Andere nähere Regelungen für die Normenkontrolle sind auch nicht vorhanden. Wie oben erwähnt dürfen die Volksgerichte Gesetze sowie andere gesetzliche Bestimmung nicht für verfassungswidrig erklären. Unter den vorhandenen Rechtsrahmen wird deswegen die Bindung der gesetzgeberischen Gewalt an die Verfassung nicht effektiv überwacht.

Am 11. März 2018 ist die damalige Gesetzeskommission des Ständigen Ausschusses des Nationale Volkskongresses in Verfassungs- und Gesetzeskommission umbenannt worden. Das heißt, dass seine Aufgabe der Kontrolle zur Durchsetzung der Verfassung in Zukunft gestärkt werden sollte. Es kann sein, dass die Befugnis des Ständigen Ausschusses des Nationalen Volkskongresses zur Normenkontrolle auf das neue Organ übertragen wird. Zumindest sind nähere materielle sowie verfahrensrechtliche Anforderungen für die vorgesehene Normenkontrolle im Gesetzgebungsgesetz auszuarbeiten. Insbesondere ist denkbar, die konkrete Normenkontrolle mittels Vorlage durch die Volksgerichte als vorrangige Ausgestaltung der verfassungsrechtlichen Kontrolle der gesetzgeberischen Gewalt zu fördern. Zwar ist zu erwarten, dass die Kontrolle der Gesetze vom Ständigen Ausschuss durchzuführen ist. Jedoch führt es zu einem Dilemma, dass der Gesetzgeber Akte, die er selbst geschaffen hat, aktiv überprüfen muss. Die Effektivität einer solchen Kontrolle ist fragwürdig.[656] Deswegen ist eine gegenseitige Zusammenarbeit vom Ständigen

656 Vgl. *Lin*, Zhejiang Social Sciences 2010/5, S. 39; *Liu*/*Chen*, Contemporary Law Review 2015/1, S. 21; *Xia*, Social Sciences in Guangdong, 2013/2, S. 240; *Xia*, Po-

Ausschuss des Nationalen Volkskongresses und den Volksgerichten notwendig. Wenn ein Volksgericht eine gesetzliche Bestimmung, die für das Verfahren von zentraler Bedeutung ist, für verfassungswidrig hält, sollte es die Befugnis haben, beim Ständigen Ausschuss des Nationalen Volkskongresses eine Normenkontrolle einzuleiten.[657] Eine derartige Ausgestaltung steht auch nicht im Widerspruch zum vorhandenen Rechtsrahmen. Damit ist sie besonders zu berücksichtigen, um die verfassungsrechtliche Bindung der öffentlichen Gewalt effektiv zu kontrollieren.

VI. Zusammenfassung

Bei der Durchführung der Vorratsdatenspeicherung sind wesentliche Grundrechte relevant, deren Schutz in der Verfassung der VR China eine Grundlage findet. Aber der Schutz der relevanten Grundrechte wird nicht wirksam garantiert, da einerseits die relevanten Grundrechte in der Verfassung nicht durch gesetzliche Bestimmungen vollständig umgesetzt sind und andererseits die Verfassungsmäßigkeit der gesetzlichen Bestimmungen nicht effektiv kontrolliert werden kann. In der Verfassung der VR China wird ausdrücklich festgestellt, dass der Ständige Ausschuss des Volkskongresses als das höchste Machtorgan die Befugnis hat, die Durchsetzung der Verfassung zu kontrollieren. Jedoch fehlt es an einer näheren Regelung über die Ausübung dieser Befugnis. In der Praxis hat es bislang auch kaum Beispiele dafür gegeben, dass der Ständige Ausschuss des Volkskongresses von dieser Befugnis erfolgreich Gebrauch gemacht hätte. Hinzu kommt, dass ein Verfassungsgericht, als wesentliche nachträgliche verfassungsrechtliche Kontrolle, in der VR China nicht eingerichtet ist. Die Volksgerichte dürfen unter dem vorhandenen Rechtsrahmen die Verfassungsmäßigkeit eines Gesetzes oder öffentlichen Handelns nicht überprüfen. Damit werden zwar relevante Grundrechte in der Verfassung festgelegt. Ein hinreichender Schutz ist damit aber noch nicht sichergestellt.

In Deutschland wird der Grundrechtschutz durch die institutionalisierte Verfassungsgerichtsbarkeit garantiert. Die deutsche Verfassungsgerichtsbarkeit kann nicht einfach in der VR China kopiert werden. Der Grund liegt nicht nur in den unterschiedlichen Entwicklungsniveaus, sondern auch in den unterschiedlichen Rechtsrahmen der beiden Länder. Allerdings ist es denkbar, sich an der institutionalisierten Verfassungsgerichtsbarkeit in Deutschland zu ori-

litical Science and Law 2016/2, S. 71 f.

657 Siehe auch *Xie*, *Weiyan*, in: *Mo*/*Xie* (Hrsg.) 2009, S. 264 f.

entieren und die verfassungsrechtliche Kontrolle der öffentlichen Gewalt unter dem vorhandenen Rechtsrahmen in der VR China zu stärken.

Vor allem ist die Ausübung der Befugnis des Ständigen Ausschusses des Volkskongresses zur Auslegung der Verfassung durch materielle sowie verfahrensrechtliche Regelungen zu verwirklichen. Durch Auslegung der Verfassung hat der Ständige Ausschuss des Volkskongresses die wesentlichen Begriffe, Schutzbereiche sowie Voraussetzungen der Beschränkung der Grundrechte klarzustellen, damit die Gesetzgebung klare Maßstäbe des Grundrechtsschutzes einhält. Darüber hinaus ist die Befugnis des Ständigen Ausschusses des Volkskongresses zur Kontrolle der Verfassungsmäßigkeit der Gesetze festzulegen. Hinsichtlich der Besonderheit des Rechtsrahmens der VR China ist die verfassungsrechtliche Kontrolle der Gesetze besser durch den Ständigen Ausschuss des Volkskongresses und die Volksgerichte gemeinsam durchzuführen. Obwohl zahlreiche unterschiedliche Konzepte in der vorhandenen Diskussion auftauchen, besteht jedoch Konsens darüber, dass die öffentliche Gewalt allgemein an die Verfassung zu binden ist. Dazu muss eine institutionelle verfassungsrechtliche Kontrolle gebildet werden. Bezogen auf die Frage nach dem "Wie" dieser Kontrolle liegt eine Orientierung an der Verfassungsgerichtsbarkeit in Deutschland nahe. Aber für eine Anlehnung ist ein volles Verständnis des Hintergrunds sowie der Entwicklungsgeschichte der deutschen Praxis und Ausgestaltung vorauszusetzen. Andernfalls würde ein bloßes Kopieren nur zu neuen Problemen führen. Der vorhandene politische sowie rechtliche Rahmen in der VR China ist bei dieser Diskussion immer zu berücksichtigen. Nur solche Konzepte, die mit dem vorhandenen Rechtsrahmen zusammenpassen, sind realistisch und durchsetzbar.

Kapitel 4: Fazit und Ausblick

Die weltweite Sicherheitslage ist so kompliziert wie vielleicht nie zuvor. Die Entstehung sowie die Entwicklung der Telekommunikations- und Informationstechnologie und die dadurch beförderte Globalisierung haben zahlreiche Vorteile sowohl für das individuelle als auch das öffentliche Wohl gebracht. Insgesamt scheint es, als sei man noch nicht voll darauf vorbereitet, den sich gleichzeitig stellenden Problemen entgegenzutreten. In den letzten Jahrzehnten haben Terrorismus und Cyberkriminalität als weltweite Sicherheitsrisiken herausgebildet. Sie haben schon immense Schäden verursacht. Die von ihnen ausgehenden potenziellen Gefahren werden wohl auch weiter existieren bzw. sich noch ausweiten.

Die Gewährleistung von Sicherheit stellt eine der wichtigsten Aufgaben des Staates dar. Auf die neue Bedrohungslage hat der Staat schnell zu reagieren und effektive Sicherheitsmaßnahmen zu erlassen, um den Terrorismus sowie die neue Art der Kriminalität zu bekämpfen und die öffentliche Sicherheit zu gewährleisten. Allerdings bedienen sich diejenigen, von denen die neuen Bedrohungen ausgehen, moderner Technologie. Die Folge ist ein Katz-und-Maus-Spiel.

Einerseits begegnen traditionelle Sicherheitsmaßnahmen großen Hindernisse bei der Strafverfolgung. Andererseits sind nachträgliche Sicherheitsmaßnahmen und Sanktionen nicht mehr so effektiv wie zuvor, die terroristischen Anschläge zu bekämpfen. Deswegen müssen Sicherheitsmaßnahmen dementsprechend an die neuen technischen und gesellschaftlichen Bedingungen angepasst werden. Um auf die neue Bedrohungslage besser zu reagieren, sind Sicherheitsmaßnahmen mit Hilfe der neuen Telekommunikations- und Informationstechnologie zur Bekämpfung der Kriminalität und zur Gefahrenabwehr zu treffen. Zudem sind vorsorgliche Sicherheitsmaßnahmen im Hinblick auf die Besonderheiten der neuen Bedrohungen von steigender Bedeutung. Da terroristische Anschläge massive und unersetzliche Verluste mit sich bringen, wirkt die Sicherheitsmaßnahme praktisch nur dann, wenn derartige Kriminalität *vor* der Begehung entdeckt und verhindert werden kann.

Grundsätzlich dürfen Sicherheitsmaßnahmen nach der Rechtsprechung des BVerfG zum Zweck der Strafverfolgung und Gefahrenabwehr die Grundrechte der Bürger einschränken. Die Einschränkung ist jedoch nur zulässig, wenn sie gesetzlich geregelt ist, den Wesensgehalt der Bürger nicht berührt,

einen legitimen Zweck verfolgt und auch im Übrigen verhältnismäßig ist sowie den einschlägigen Anforderungen aus ständigen Entscheidungen des BVerfG entspricht. Es ist vor allem zu bemerken, dass in die Freiheit und Privatsphäre der Bürger von der Sicherheitsmaßnahme mittels der neuen technischen Bedingungen mit Leichtigkeit sehr tief eingegriffen werden kann. Der Staat verfügt heute mit Hilfe neuer Informationstechnologien über zahlreiche umfassende personenbezogene Daten der Bürger. Unter anderem können technische Sicherheitsmaßnahmen ohne Wissen des Betroffenen durchgeführt werden. Der Betroffene kann den Eingriff kaum vorhersehen und vorsorglich seine Grundrechte wahren. Deswegen müssen die Sicherheitsmaßnahmen, die durch Sammlung und Verwendung personenbezogener Daten umgesetzt werden, immer sehr strengen Voraussetzungen unterliegen.

Des Weiteren wird ein Problem in der Tendenz zur Vorverlagerung der Sicherheitsmaßnahme dergestalt auftauchen, dass das Spektrum der Personen, die von der Maßnahme betroffen sind, nicht mehr nur auf Verdächtige beschränkt wird, sondern unterschiedslos auf die gesamte Bevölkerung ausgeweitet wird. Die Vorbeugung schwerer Kriminalität muss nicht zwangsläufig dazu führen, dass alle Bürger wie potenzielle Straftäter behandelt werden dürfen. Bei einer Sicherheitsmaßnahme, die die gesamte Bevölkerung betrifft und ohne bestimmten Verdacht oder konkreter Gefahr durchgeführt wird, muss man jedoch fragen, ob der Zweck zur Strafverfolgung und Gefahrenabwehr einen derartigen Eingriff immer noch ohne Zweifel legitimieren kann.

Ob solche Sicherheitsmaßnahmen erlaubt werden oder nicht, ist von entscheidender Bedeutung, wenn es darum geht, ob der Staat die allgemeine Überwachung einer oder mehrerer Handlungen der Bevölkerung als Sicherheitsmaßnahme zulassen darf. Es handelt sich dann nicht mehr um die allgemeine Sicherheitskontrolle am Flughafen oder am Bahnhof, sondern darum, dass man plötzlich einer Überwachung ohne Wissen ausgesetzt wird, weil man eine Internetseite besucht hat, die womöglich extreme Inhalte bereithält. Obwohl sich eine derartige Sicherheitsmaßnahme normalerweise nur auf eine bestimmte Verhaltensart der Bürger richtet, wird jedoch faktisch eine vernetzte Überwachungsgesellschaft geschaffen: wegen der unbegrenzten Nutzung der Informationstechnologie, die nur noch wenige Schritte von einer totalen Überwachungsgesellschaft entfernt ist.

Weder die Sicherheit noch die Freiheit stellt ein absolutes Schutzgut dar. Beide werden nicht schrankenlos gewährleistet, sondern in einer angemessenen Balance gehalten. Die angemessene Balance zwischen der Sicherheit und der Freiheit ist jedoch nicht immer leicht zu halten. Die Entwicklung der Vorratsdatenspeicherung in Deutschland hat ein gutes Beispiel dafür gegeben, wie gespannt die Beziehung zwischen den beiden Polen sein kann und wie schwierig das Herstellen einer Balance letztlich ist. Eine Neigung zu Sicherheit angesichts einer verschärften Bedrohungslage erscheint folgerichtig. Wie sehr die Waage in Richtung Sicherheit ausschlagen darf, unterliegt allerdings streng den verfassungsrechtlichen Vorgaben sowie Anforderungen der ständigen Rechtsprechung des BVerfG.

Inzwischen haben das BVerfG und der EuGH durch eine Reihe von Urteilen die Rolle als zuverlässiger Hüter der Grundrechte eingenommen. Trotz der verschärften Bedrohungslage haben sie die Vorratsdatenspeicherung nüchtern betrachtet und strenge konkrete verfassungsrechtliche Anforderungen für künftige, vergleichbare Sicherheitsmaßnahmen aufgestellt. Der Sicherheit dienende Einschränkungen der Grundrechte müssen wirksam auf das absolut Erforderliche reduziert werden. Eine totale Überwachung der Telekommunikation aller Bürger ist demnach auf keinen Fall verhältnismäßig. Die Vorratsdatenspeicherung stellt zwar keine totale Überwachung der Bürger dar, mit ihr geht der Gesetzgeber jedoch einen Schritt in diese Richtung. Das BVerfG und der EuGH haben diese bedenkliche Tendenz rechtzeitig gebremst und neue Anforderungen des Grundrechtsschutzes unter neuen technischen und gesellschaftlichen Bedingungen festgelegt.

In der VR China spielen die Freiheitsrechte und die Privatsphäre der Bürger traditionell eine untergeordnete Rolle. Im Falle einer Rechtsgüterkollision besitzen das staatliche und das kollektive Interesse gegenüber dem individuellen Interesse stets den Vortritt. Im Namen der öffentlichen Sicherheit werden die Grundrechte der Bürger nahezu willkürlich eingeschränkt. Unter den neuen technischen Bedingungen sind die Bürger größeren Gefahren denn je ausgesetzt. Staatlicher Eingriffe in Form von Sicherheitsmaßnahmen sind praktisch allgegenwärtig. Ohne konkrete gesetzliche Beschränkung für staatliche Sicherheitsmaßnahmen wird der gerade erst verstärkte Grundrechtsschutz angesichts der neuen Bedrohungslagen auf eine harte Probe gestellt.

Nun steht die VR China zurzeit am Anfang des Aufbaus eines sozialistischen Rechtsstaats. Die Stärkung des Grundrechtsschutzes stellt eines der wichtigs-

ten Ziele der Rechtspolitik dar. Wesentliche Grundsätze wie der Vorbehalt des Gesetzes, die Verhältnismäßigkeit und das Bestimmtheitsgebot können aus der Verfassung abgeleitet werden. Problematisch ist, dass die abstrakten verfassungsrechtlichen Vorgaben noch nicht hinreichend in einfachen Gesetzen und anderen untergesetzlichen Vorschriften konkretisiert werden. Obwohl die relevanten Grundrechte bei der Ausgestaltung der Vorratsdatenspeicherung zu beachten sind, fehlt es jedoch sowohl an materiellen als auch verfahrensrechtlichen Voraussetzungen bzw. Beschränkungen für den Zugriff und die Verwendung von Vorratsdaten, die den Grundrechtsschutz wirksam gewährleisten könnten. Ohne die Konkretisierung der verfassungsrechtlichen Anforderungen werden die Grundrechte der Bürger ausgehöhlt. Deswegen ist es die vorrangige Aufgabe des Gesetzgebers, die verfassungsrechtlichen Vorgaben in der Ausgestaltung der Vorratsdatenspeicherung umzusetzen. Dafür lohnt sich ein Blick auf die entsprechende Gesetzgebung in Deutschland.

Die Entwicklungsgeschichte und der Streit um die Vorratsdatenspeicherung in Deutschland ist für die VR China vor allem insoweit richtungsweisend, als die Vorratsdatenspeicherung, die in der VR China bislang nicht als ernsthaftes Problem erkannt worden ist, jedoch viele grundlegende Grundrechte der Bürger berührt. Die flächendeckende und allumfassende Speicherung der Telekommunikations- und Nutzungsdaten der Nutzer in der VR China schädigt – zu Ende gedacht – nicht nur die Freiheit und Vertraulichkeit der Telekommunikation, sondern auch das allgemeine Persönlichkeitsrecht. Wenn alle Telekommunikationsdaten und Nutzungsdaten der Bürger gespeichert werden und unter sehr lockeren Voraussetzungen für die staatliche Verwendung zur Verfügung stehen, ist es dem Bürger nicht möglich, seine Persönlichkeit frei zu entfalten. Eine darauf begründete freiheitliche und demokratische Gesellschaft kann auch deswegen nicht gedeihen.

Die Ausgestaltung der Vorratsdatenspeicherung in Deutschland ist für die VR China ferner deshalb von Interesse, weil die Befugnisse des Zugriffs auf die Vorratsdaten gemäß den verfassungsrechtlichen sowie datenschutzrechtlichen Vorgaben durch konkrete verfahrens- und materiellrechtliche Voraussetzungen beschränkt werden. Die verfassungsrechtlichen Anforderungen werden in der Ausgestaltung der Vorratsdatenspeicherung umgesetzt, um die relevanten Grundrechte zu gewährleisten. Das chinesische Telekommunikationsgesetz und das chinesische Datenschutzgesetz befinden sich derzeit im Entwurfsstadium. Dies ist eine gute Gelegenheit, die verfassungsrechtlichen Vorgaben so konkret wie möglich in beiden Gesetzen zu verankern. Zwar ist

das vorhandene Gesetzgebungsniveau zu berücksichtigen, aber die Einhaltung des Bestimmtheitsgebotes und die Feststellung der verfahrensrechtlichen Beschränkungen bei der Ausgestaltung der Vorratsdatenspeicherung erscheinen zumutbar und überaus sinnvoll.

Kapitel 5: Zusammenfassung der wesentlichen Thesen

1. In der Informationsgesellschaft sind neue Bedrohungslagen entstanden. Die Sicherheitsgesetzgebung muss sich den neuen technischen Bedingungen und den neuen Bedrohungslagen anpassen. Angesichts neuer Bedrohungslagen haben vorsorgliche Sicherheitsmaßnahmen immer mehr an Bedeutung gewonnen. Hierzu zählen insbesondere die Erhebung sowie die Verwendung umfangreicher personenbezogenen Daten.

2. Wegen des Wandels der Sicherheitsstrategie verschärft sich das Spannungsverhältnis zwischen Freiheit und Sicherheit. Freiheit und Sicherheit ergänzen sich gegenseitig: Ohne Sicherheit ist Freiheit nicht möglich, ohne Freiheit verliert Sicherheit ihren Sinn. Der Gesetzgeber muss bei der Ausbalancierung von Freiheit und Sicherheit vorsichtig sein. Dazu sind verfassungsrechtliche Anforderungen von zentraler Bedeutung. Zwar dürfen das Recht auf Handlungsfreiheit und das Privatsphäre der Bürger zum Schutz der öffentlichen Sicherheit beschränkt werden. Die Beschränkung muss jedoch auf das absolut notwendige Maß bleiben.

3. Die Vorratsdatenspeicherung wird als eine effektive Maßnahme zur Strafverfolgung und Gefahrenabwehr angesehen. Die Verfassungsmäßigkeit dieser Sicherheitsmaßnahme ist jedoch wegen der Unterschiedslosigkeit und Anlasslosigkeit der Speicherung sehr fragwürdig. Eine unterschieds- und anlasslose Speicherung der Daten auf Vorrat entspricht den rechtsstaatlichen Anforderungen nicht. Dies haben BVerfG und EuGH herausgearbeitet. Soweit der Verwendungszweck der personenbezogenen Daten bei der Speicherungsphase noch nicht bestimmt ist, kann das Defizit nicht durch eine strenge Ausgestaltung kompensiert werden.

4. Eine Vorratsdatenspeicherung ohne irgendeine Differenzierung der Betroffenen oder der zu speichernden Daten wird nicht wirksam eingeschränkt und ist mit der Grundrechtscharta der EU unvereinbar. Eine ähnliche Sicherheitsmaßnahme hat somit auch in der EU keine Zukunft mehr.

5. Aus vorhandenen Statistiken und Untersuchungen ergibt sich, dass die Effektivität und die damit verbundene Unverzichtbarkeit der Vorratsdatenspeicherung nicht unumstößlich feststehen. Im Hinblick zur besonders weitreichenden Grundrechtsbeeinträchtigung ist die Maßnahme ohne besondere Safeguards unangemessen und damit nicht verfassungsmäßig. Eine vorsorg-

liche Datenspeicherung darf nur nach engen Voraussetzungen und gezielt ausgeführt werden. Ein Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel ist absolut erforderlich.

6. Angesichts der globalen Bedrohungslage steht die Anpassung der Sicherheitsstrategie auch in der VR China im Fokus. Mangels effektiven Grundrechtsschutzes führt die uferlose Vorratsdatenspeicherung jedoch zur Aushöhlung des Grundrechtsschutzes. Eine Überwachungsgesellschaft ist dort im Entstehen begriffen bzw. teilweise schon entstanden.

7. Die Vorratsdatenspeicherung in der VR China stellt im Vergleich zu Deutschland einen viel weitgehenderen Eingriff dar. Dies liegt insbesondere daran, dass es an Beschränkungen für eine verhältnismäßige Ausgestaltung der Vorratsdatenspeicherung fehlt. In einer Reihe von Vorschriften werden Unternehmen dazu verpflichtet, Daten zu sammeln und bei Bedarf den Sicherheitsbehörden zur Verfügung zu stellen. Es fehlt hierbei an Beschränkungen der staatlichen Befugnisse in jeglicher Hinsicht.

8. In der chinesischen Verfassung gibt es kein Datenschutzgrundrecht. Auch fehlt es an einer Generalklausel wie der allgemeinen Handlungsfreiheit aus Art. 2 Abs. 1 GG. Es gibt zwar ein Grundrecht zum Schutz der Würde der Person. Dieses ist jedoch zu weit, um daraus spezielle Voraussetzungen für den Schutz von personenbezogenen Daten herzuleiten. Das Grundrecht, welches zur Beschränkung von Maßnahmen zur Speicherung von Vorratsdaten heranzuziehen ist, ist das Korrespondenzgeheimnis aus Art. 40 Verf VRC.

9. Es ist am chinesischen Gesetzgeber, den Schutz des Korrespondenzgeheimnisses durch einfaches Gesetz umzusetzen. Die Durchführung der Vorratsdatenspeicherung als eine Ausnahme ist nur durch Gesetz zulässig. Der mit der Vorratsdatenspeicherung einhergehende Eingriff muss durch klare und konkrete materielle sowie verfahrensrechtliche Anforderungen effektiv beschränkt werden. Wie in Art. 5 Verf VRC niedergelegt müssen auch die Grundrechte in der Praxis durchgesetzt werden. Derzeit ist dies nur unzureichend möglich.

10. Der Mangel des wirksamen Grundrechtsschutzes in der VR China hängt unter anderem mit dem Fehlen der Verfassungsgerichtsbarkeit zusammen. Innerhalb des vorhandenen Rechtsrahmens bieten sich Problemlösungen an.

Die Verstärkung der Verfassungskontrolle vom Ständigen Ausschuss des Volkskongresses ist momentan rational und durchsetzbar.

Literaturverzeichnis

Albers, *Marion* / *Reinhardt*, *Jörn*, Vorratsdatenspeicherung im Mehrebenensystem: Die Entscheidung des BVerfG vom 2.3.2010, in: Zeitschrift für das Juristische Studium (ZJS) 2010, S. 767-774,
zitiert als: *Albers*/*Reinhardt*, ZJS 2010, 767.

Albrecht, *Hans-Jörg* / *Kilchling*, *Michael*, *u.a.*, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten, Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht, im Auftrag des Bundesministerium der Justiz, 2., erweiterte Fassung, Juli 2011,
zitiert als: *Albrecht/Kilchling*, S.

Albrecht, *Jan Philipp* / *Jotzo, Florian*, Das neue Datenschutzrecht der EU, Baden-Baden 2017,
zitiert als: *Albrecht*/*Jotzo*, Teil, Rn.

Albrecht, *Jan Philipp*, Sicherheit statt Rechtsstaat – Der Konflikt bei der Vorratsdatenspeicherung spitzt sich zu, Forum Recht (FoR) 1/2007, S. 13-15,
zitiert als: *Albrecht*, FoR 1/2007, S.

Alsbih, *Amir*, Der reale Wert einer IP-Adresse, in: Datenschutz und Datensicherheit (DuD) 2011, S. 482-488,
zitiert als: *Alsbih*, DuD 2011, 482.

Alvaro, *Alexander*, Die Richtlinie zur Vorratsdatenspeicherung, in: Datenschutz-Nachrichten (DANA) 2006, S. 52 – 55,
zitiert als: *Alvaro*, DANA 2006, S.

Ambos, *Kai*, Anmerkung zu EuGH, Urteil vom 10.02.2009, Rs. C-301/06. Juristenzeitung (JZ) 2009, S. 468 – 471,
zitiert als: *Ambos*, JZ 2009, 468.

Baldus, *Manfred*, Art. 10, in: *Epping*, *Volker* / *Hillgruber*, *Christian* (Hrsg.), BeckOK Grundgesetz, 33. Edition, München 2017,
zitiert als: *Baldus*, in: *Epping*/*Hillgruber* (Hrsg.), GG 2017, Art. 10 Rn.

Beukelmann, *Stephan*, Surfen ohne strafrechtliche Grenzen, in: Neue juristische Wochenschrift (NJW) 2012, S. 2716-2621,
zitiert als: *Beukelmann*, NJW 2012, 2617.

Binding, *Jörg*, Grundzüge des Verbraucherdatenschutzrechts der VR China – Leitfaden für die Praxis, in: Zeitschrift für Datenschutz (ZD) 2014, S.327-336,
zitiert als: *Binding*, ZD 2014, 327.

Bizer, *Johann*, Vorratsdatenspeicherung: ein fundamentaler Verfassungsverstoß, in: Datenschutz und Datensicherheit (DuD) 2007, S. 586-589,
zitiert als: *Bizer*, DuD 2007, 586.

Bock, *Kirsten* / *Engeler*, *Malte*, Die verfassungsrechtliche Wesensgehaltsgarantie als absolute Schranke im Datenschutzrecht, in: Deutsches Verwaltungsblatt (DVBL) 2016, S. 593-599,
zitiert als: *Bock*/*Engeler*, DVBI 2016, 593.

Boehm, *Franziska* / *Cole Mark D.*, Studie zu den Folgen des EuGH-Urteils zur Vorratsdatenspeicherung – Auswirkungen auf Mitgliedstaaten, EU-Rechtsakte und internationale Abkommen, in: Zeitschrift für Datenschutz (ZD) 2014, S. 553-557,
zitiert als: *Boehm*/*Cole*, ZD 2014, 553.

Boehm, *Franziska*/*Cole Mark D.*, Data Retention after the Judgement of the Court of Justice of the European Union, Münster/Luxembourg, 30 June 2014,
zitiert als: *Boehm*/*Cole*, 2014, S.

Boehm, *Franziska* / *Andrees*, *Markus*, Zur Vereinbarkeit der Vorratsdatenspeicherung mit europäischem Recht: Bewertung der generellen Speicherpflicht nach EuGH und EGMR Rechtsprechung, in: Computer und Recht (CR) 2016, S. 146-154,
zitiert als: *Boehm*/*Andrees*, CR 2016, 146.

Braum, *Stefan*, „Parallelwertungen in der Laiensphäre“: Der EuGH und die Vorratsdatenspeicherung, Zeitschrift für Rechtspolitik (ZRP) 2009, S. 174-177,
zitiert als: *Braum*, ZRP 2009, 174.

Breyer, *Patrick*, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland (Vorratsspeicherung, traffic data retention), Berlin, 2005,
zitiert als: *Breyer*, S.

Breyer, *Patrick*, Rechtsprobleme der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung und ihrer Umsetzung in Deutschland, Strafverteidiger (StV) 2007, S. 214-220,
zitiert als: *Breyer*, StV 2007, 214.

Breyer, *Patrick*, Lästern, Flirten, Tratschen – und jemand schreibt mit, in: *Bettina Sokol* (Hrsg.), Persönlichkeit im Netz: Sicherheit – Kontrolle – Transparenz [Symposium 2007], Düsseldorf 2008, S. 13-23,
zitiert als: *Breyer*, in: *Bettina* (Hrsg.) 2008, S.

Breyer, *Patrick*, Personenbezug von IP-Adressen Internetnutzung und Datenschutz, in: Zeitschrift für Datenschutz (ZD) 2014, S. 400-405,
zitiert als: *Breyer*, ZD 2014, 400.

Bu, *Chao* (步超), Das Spannungsverhältnis zwischen der Klarnamenpflicht und der Erforderlichkeit der Datenspeicherung in der Gesetzgebung des Schutzes der personenbezogenen Daten online (论我国网络信息保护立法

中的实名制规制与信息收集必要性原则之张力), in: Tianjin Legal Science (天津法学) 2014/2, S. 25-31,
zitiert als: *Bu*, Tianjin Legal Science 2014/2, S.

Bug, *Mathias*, Terrorismusbekämpfung als Waffe gegen Alltagskriminalität – Argumentation und Wirklichkeit der Vorratsdatenspeicherung in Deutschland, in: Zeitschrift für Parlamentsfragen (ZParl) 2016, S. 670-692,
zitiert als: *Bug*, ZParl 2016, 670.

Bull, *Hans Peter*, Grundsatzentscheidungen zum Datenschutz im Bereich der inneren Sicherheit – Rasterfahndung, Online-Durchsuchung, Kfz-Kennzeichenerfassung, Vorratsdatenspeicherung und Antiterrordatei in der Rechtsprechung des Bundesverfassungsgerichts, in: *van Ooyen*, *Robert Chr.* / *Möllers*, *Martin H. W.* (Hrsg.), Handbuch Bundesverfassungsgericht im politischen System, 2. Auflage, Wiesbaden, 2015, S. 627-663,
zitiert als: *Bull*, in: *van Ooyen*/*Möllers* (Hrsg.) 2015, S.

Bär, *Wolfgang*, Die Neuregelung zur Erhebung von Verkehrsdaten (§ 100g StPO): Inhalt und Auswirkungen, in: Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt) 2017, S. 81-86,
zitiert als: *Bär*, NZWiSt 2017, 81.

Bär, *Wolfgang*, Anmerkung zum BVerfG Beschluss vom 6.7.2016 – 2 BvR 1454/13, in: Zeitschrift für Datenschutz (ZD) 2017, S. 135-137,
zitiert als: *Bär*, ZD 2017, 135.

Cai, *Dingjian* (蔡定剑), Studien zur Vorgehensweise der Verfassungsgerichtsbarkeit in der VR China (中国宪法司法化路径探索), in: Chinese Journal of Law (法学研究) 2005/5, S. 110-124,
zitiert als: *Cai*, Chinese Journal of Law 2005/5, S.

Calliess, *Christian* / *Ruffert*, *Matthias* (Hrsg.), EUV/AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, Kommentar, 5. Auflage, München 2016,
zitiert als: *Bearbeiter*, in: *Calliess*/*Ruffert* (Hrsg.), 2016, Art. Rn.

Calliess, *Christian*, Gewährleistung von Freiheit und Sicherheit im Lichte unterschiedlicher Staats- und Verfassungsverständnisse, Deutsches Verwaltungsblatt (DVBL) 2003, S. 1096-1105,
zitiert als: *Calliess*, DVBL 2003, 1096.

Chen, *Daoying* (陈道英) / *Qin*, *Qianhong* (秦前红), Neue Ansicht zur Drittwirkung der Grundrechte (对宪法权利规范对第三人效力的再认识——以对宪法性质的分析为视角), in: Journal of Henan Administrative Institute of Politics and Law (河南省政法管理干部学院学报) 2006/2, S. 49-55,
zitiert als: *Chen*/*Qin*, Journal of Henan Administrative Institute of Politics and Law 2006/2, S.

Chen, *Daoying* (陈道英), Auslegung des Art. 35 der Verfassung der VR China im Hinblick auf die Bedingungen des Internets (互联网条件下对我国《宪法》第 35 条的解释), in: Chinese Yearbook of Constitutional Law (中国宪法年刊) 2016, S. 33-46,
zitiert als: *Chen*, in: Chinese Yearbook of Constitutional Law 2016, S.

Chen, *Tan* (陈潭), Erschütterung der institutionellen Identität, Untersuchung des chinesischen Personalakte-Systems (单位身份的松动 ——中国人事档案制度研究), Nanjing 2007,
zitiert als: *Chen*, 2007, S.

Chen, *Xinmin* (陈新民), Chinesisches allgemeines Verwaltungsrecht (中国行政法学原理), Peking 2002,
zitiert als: *Chen*, 2002, S.

Chen, *Xinmin* (陈新民), Sozialistischer Rechtsstaat, Praxis aus Vietnam und der DDR als Ausgangspunkt (社会主义法治国之概念——从越南及东德的经验谈起), in: *Chen*, *Xinmin* (陈新民), Grundlegende Theorie des öffentlichen Rechts in Deutschland (德国公法学基础理论), Band 1, neu bearbeitete Auflage, Peking 2010, S. 112-162,
zitiert als: *Chen*, Sozialistischer Rechtsstaat, in: *Chen*, Band 1, 2010, S.

Chen, *Xinmin* (陈新民), Der Begriff des öffentlichen Interesses (公共利益的概念), in: *Chen*, *Xinmin* (陈新民), Grundlegende Theorie des öffentlichen Rechts Deutschland (德国公法学基础理论), Band 1, neu bearbeitete Auflage, Peking 2010, S. 228-260,
zitiert als: *Chen*, Der Begriff des öffentlichen Interesse, in: *Chen*, Band 1, 2010, S.

Chen, *Xinmin* (陈新民), Beschränkung auf Grundrechte (论宪法人民基本权利的限制), in: *Chen*, *Xinmin* (陈新民), Grundlegende Theorie des öffentlichen Rechts Deutschland (德国公法学基础理论), Band 1, neu bearbeitete Auflage, Peking 2010, S. 387-442,
zitiert als: *Chen*, Beschränkung auf Grundrechte, in: *Chen*, Band 1, 2010, S.

Chen, *Xiong* (陈雄), Zur Anwendung der Verfassung der VR China in Prozess (论诉讼中的中国宪法适用), in: Journal of Gansu Institute of Political Science and Law, 2001/2, S.1-4,
zitiert als: *Chen*, Journal of Gansu Institute of Political Science and Law, S.

Chen, *Zheng* (陈征), Verfassungsrechtliche Begrenzung für wirtschaftliche Tätigkeit des Staates, Aus der Sicht des Grundrechtsschutz der Privatunternehmer (国家从事经济活动的宪法界限——以私营企业家的基本权利为视角), in: China Legal Science (中国法学) 2011/1, S.98-109,
zitiert als: *Chen*, China Legal Science 2011/1, S.

Cheng, *Lei* (程雷), Frage in der Gesetzgebung der heimlichen Ermittlung (秘密侦查立法宏观问题研究), in: Tribune of Political Science and Law (政法论坛) 2011/5, S. 74-84,
zitiert als: *Cheng*, Tribune of Political Science and Law 2011/5, S.

Classen, *Claus Dieter*, Datenschutz ja – aber wie? : Anmerkung zum Urteil des EuGH vom 8.4.2014, verb. Rs. C – 293/12 und C – 594/12 (Digital Rights Ireland u. a.), in: Europarecht (EuR) 2014, S. 441-448,
zitiert als: *Classen*, EuR 2014, 441.

Dalby, *Jakob*, Konsequenzen des EuGH-Urteils zur Vorratsdatenspeicherung für die Datensammlung – eine Einordnung, in: *Kugelmann*, *Dieter* (Hrsg.), Migration, Datenübermittlung und Cybersicherheit – Grundfragen und ausgewählte Handlungsfelder der Zusammenarbeit von Sicherheits- und Strafverfolgungsbehörden in der EU, Baden-Baden 2016, S. 173-186,
zitiert als: *Dalby*, in: *Kugelmann* (Hrsg.), S.

Derksen, *Roland*, Unionsrechtskonforme Spielräume für anlasslose Speicherung von Verkehrsdaten? in: Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2017, S. 1005-1009,
zitiert als: *Derksen*, NVwZ 2017, 1005.

Di Fabio, *Udo*, Art. 2, in: in: *Maunz*, *Theodor* / *Dürig*, *Günter* (Begr.), Grundgesetz Kommentar, 81. Ergänzungslieferung September 2017, München 2017,
zitiert als: *Di Fabio*, in: in: *Maunz*/*Dürig* (Begr.), GG, 2017, Art. 2 Rn.

Di Fabio, *Udo*, Sicherheit in Freiheit, in: NJW 2008, S. 421-425,
zitiert als: *Di Fabio*, NJW 2008, 421.

Dix, *Alexander*, Freiheit braucht Sicherheit – Sicherheit braucht Freiheit, in: Bundeskriminalamt (Hg.), Informations- und Kommunikationskriminalität, Vorträge anlässlich der Herbsttagung des Bundeskriminalamtes vom 2. bis 4. Dezember 2003, München 2004, S. 159-168, abrufbar unter:

https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Herbsttagungen/2003/herbsttagung2003InformationsUndKommunikationskriminalitaet.html,
zitiert als: *Dix*, in: Bundeskriminalamt (Hg.) S.

Dix, *Alexander* / *Kipker*, *Dennis-Kenji* / *Schaar*, *Peter*, Schnellschuss gegen die Grundrechte – Plädoyer für eine ausführliche öffentliche Debatte in Sachen Vorratsdatenspeicherung, Zeitschrift für Datenschutz (ZD) 2015, 300-305,
zitiert als: *Dix*/*Kipker*/*Schaar*, ZD 2015, 300.

Dix, *Alexander*/*Petri*, *Thomas B*., Das Fernmeldegeheimnis und die deutsche Verfassungsidentität – Zur Verfassungswidrigkeit der Vorratsdatenspeicherung, in: Datenschutz und Datensicherheit (DuD) 2009, S. 531-535,
zitiert als: *Dix*/*Petri*, DuD 2009, 531.

Dix, *Alexander*/*Schaar*, *Peter*, Der EuGH zur Vorratsdatenspeicherung: Wegweisend für den gesamten Datenschutz, in: Jahrbuch Informationsfreiheit und Informationsrecht 2014, Berlin 2015, S. 17-28,
zitiert als: *Dix*/*Schaar*, in: Jahrbuch 2014, S.

Dong, *Heping* (董和平), Meinungsfreiheit als Grundrecht und ihre Funktion (言论自由的宪法权利属性及其功能), in: Journal of Northwest University of Politics and Law (西北政法学院学报) 1993/2, S. 14-20,
zitiert als: *Dong*, Journal of Northwest University of Politics and Law, S.

Dreier, *Horst* (Hrsg.), Grundgesetz Kommentar, 3. Auflage, Tübingen 2013,
zitiert als: *Bearbeiter*, in: *Dreier* (Hrsg.), GG 2013, Art. Rn.

Durner, *Wolfgang*, Anmerkung zu EuGH, Urteil vom 08.04.2014, - C-293/12 und C-594/12, in: Deutsches Verwaltungsblatt (DVBL) 2014, S. 712-715,
zitiert als: *Durner*, DVBI 2014, 712.

Durner, *Wolfgang*, Art. 10, in: *Maunz*, *Theodor* / *Dürig*, *Günter* (Begr.), Grundgesetz Kommentar, 81. Ergänzungslieferung September 2017, München 2017,
zitiert als: *Durner*, in: *Maunz*/*Dürig* (Begr.), GG 2017, Art. 10 Rn.

Ehlers, *Dirk* (Hrsg.), Europäische Grundrecht und Grundfreiheiten, 4. Auflage, Berlin/Boston 2014,
zitiert als: *Bearbeiter*, in: *Ehlers* (Hrsg.) 2014, S. Rn.

Eidam, *Lutz*, Anmerkung zum BVerfG Beschluss vom 6.7.2016 – 2 BvR 1454/13, in: NJW 2016, S. 3511-3512,
zitiert als: *Eidam*, NJW 2016, 3511.

Epping, *Volker* / *Hillgruber*, *Christian* (Hrsg.), BeckOK Grundgesetz, 33. Edition, München 2017,
zitiert als: *Bearbeiter*, in: *Epping*/*Hillgruber* (Hrsg.), GG 2017, Art. Rn.

Feng, *Jianpeng* (冯健鹏), Berufung der Verfassung in den Entscheidungen der Volksgerichte in der VR China und ihre Funktion – eine empirische Forschung aufgrund der veröffentlichten Urteile (我国司法判决中的宪法援引及其功能——基于已公开判决文书的实证研究), in: Chinese Journal of Law (法学研究) 2017/3, S. 44-59,
zitiert als: *Feng*, Chinese Journal of Law 2017/3, S.

Forgó, *Nikolaus* / *Heermann*, *Thorsten*, Vorratsdatenspeicherung 2015 – Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten, K&R 12/2015, 753-759,
zitiert als: *Forgó*/*Heermann*, K&R 2015, 753.

Forgó, *Nikolaus* / *Jlussi*, *Dennis* / *Klügel*, *Christian* / *Krügel*, *Tina*, Die Umsetzung der Richtlinie zur Vorratsdatenspeicherung – Europa tut sich schwer, in: Datenschutz und Datensicherheit (DuD) 2008, S. 680-682,
zitiert als: *Forgó*/*Jlussi*/*Klügel*/*Krügel*, DuD 2008, 680.

Forgó, *Nikolaus* / *Krügel*, *Tina*, Vorschriften zur Vorratsdatenspeicherung verfassungswidrig: Nach der Entscheidung ist vor der Entscheidung, in: Kommunikation & Recht (K&R) 2010, S. 217-220,
zitiert als: *Forgó*/*Krügel*, K&R 2010, 217.

Freiling, *Felix C.*, Zur Nutzung von Verkehrsdaten im Rahmen der Vorratsdatenspeicherung, Technischer Bericht TR-2009-005, 22. Juni 2009, abrufbar unter: https://ub-madoc.bib.uni-mannheim.de/2360/1/TR_2009_005.pdf,
zitiert als: *Freiling*, Technischer Bericht TR-2009-005, S.

Frenz, *Walter*, Anmerkung zu EuGH, v. 21.12.2016 – C-203/15 u. C-698/15 Tele2 Sverige – Keine Pflicht zur allgemeinen Speicherung von Verkehrs- und Standortdaten – EU-Datenschutz zwischen Terrorangst und Industrie 4.0, in: Deutsches Verwaltungsblatt (DVBL) 2017, S. 183-186,
zitiert als: *Frenz*, DVBL 2017, 183.

Gausling, *Tina*, Verdachtsunabhängige Speicherung von Verkehrsdaten auf Vorrat, C. H. Beck 2010.
zitiert als: *Gausling*, S.

Geppert, *Martin* / *Schütz*, *Raimund* (Hrsg.), Beck´scher TKG Kommentar, 4. Auflage, München 2013,
zitiert als: *Bearbeiter*, in: *Geppert*/*Schütz* (Hrsg.), TKG 2013, Paragraph Rn.

Gercke, *Marco*, Die Bekämpfung der Internetkriminalität als Herausforderung für die Strafverfolgungsbehörden, Multimedia und Recht (MMR) 2008, S. 291-298,
zitiert als: *Gercke*, MMR 2008, 291.

Germann, *Michael*, Gefahrenabwehr und Strafverfolgung im Internet, Berlin 2000,
zitiert als: *Germann*, S.

Gietl, *Andreas*, Die Einführung der Vorratsdatenspeicherung, in: Kommunikation & Recht (K&R) 2007, S. 545-550,
zitiert als: *Gietl*, K&R 2007, 545.

Gietl, *Andreas*, Das Schicksal der Vorratsdatenspeicherung, in: Datenschutz und Datensicherheit (DuD) 2008, S. 317-323,
zitiert als: *Gietl*, DuD 2008, 317.

Gietl, *Andreas*, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: Datenschutz und Datensicherheit (DuD) 2010, S. 398-403,
zitiert als: *Gietl*, DuD 2010, 398.

Gietl, *Andreas* / *Tomasic*, *Lovro*, Kompetenz der Europäischen Gemeinschaft zur Einführung der Vorratsdatenspeicherung, Anmerkung zu den Schlussanträgen von Generalanwalt Yves Bot im Verfahren C-301/06 vom 14.10.2008, DuD 2008, S. 795-800,
zitiert als: *Gietl*/*Tomasic*, DuD 2008, 795.

Gitter, *Rotraud* / *Schnabel*, *Christoph*, Die Richtlinie zur Vorratsspeicherung und ihre Umsetzung in das nationale Recht, Multimedia und Recht (MMR) 2007, S. 411-416，
zitiert als: *Gitter*/*Schnabel*, MMR 2007, 411.

Gola, *Peter* / *Klug*, *Christoph* / *Reif*, *Yvette*, Datenschutz- und presserechtliche Bewertung der „Vorratsdatenspeicherung“, in: Neue juristische Wochenschrift (NJW) 2007, S. 2599-2602，
zitiert als: *Gola*/*Klug*/*Reif*, NJW 2007, 2599.

Gola, *Peter* / *Klug*, *Christoph*, Die Entwicklung des Datenschutzes im ersten Halbjahr 2017, in: Neue juristische Wochenschrift (NJW) 2017, S.2593-2596,
zitiert als: *Gola*/*Klug*, NJW 2017, 2593.

Graf, *Jürgen-Peter* (Hrsg.), BeckOK StPO mit RiStBV und MiStra, 29. Edition, München 2018,
zitiert als: *Bearbeiter*, in: *Graf* (Hrsg.) 2018, Gesetz, Paragraph, Rn.

Graulich, *Kurt*, Telekommunikationsgesetz und Vorratsdatenspeicherung, in: Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2008, 485- 492，
zitiert als: *Graulich*, NVwZ 2008, 485.

Grzeszick, *Bernd*, Art. 20, in: *Maunz*, *Theodor* / *Dürig*, *Günter* (Begr.), Grundgesetz Kommentar, 81. Ergänzungslieferung September 2017, München 2017,
zitiert als: *Grzeszick*, in: *Maunz*/*Dürig* (Begr.), GG 2017, Art. 20 Rn.

Gundel, *Jörg*, 4. Teil § 27, in: *Ehlers*, *Dirk* (Hrsg.), Europäische Grundrecht und Grundfreiheiten, 4. Auflage, Berlin/Boston 2014,
zitiert als: *Gundel*, in: *Ehlers* (Hrsg.), 2014, S. Rn.

Gundermann, *Lukas*, E-Commerce trotz oder durch Datenschutz? in: Kommunikation & Recht (K&R) 2000, S. 225-235,
zitiert als: *Gundermann*, K&R 2000, 225.

Guo, *Yu* (郭瑜), Datenschutzrecht (个人数据保护法研究), Peking 2012,
zitiert als: *Guo*, 2012, S.

Gärtner, *Hauke* / *Kipker*, *Dennis-Kenji*, Die Neuauflage der Vorratsdatenspeicherung: Lösungsansätze für zentrale Kritikpunkte am aktuellen Gesetzentwurf, in: DuD 2015, S. 593-599,
zitiert als: *Gärtner/Kipker*, DuD 2015, 593.

Hammer, *Volker* / *Knopp*, *Michael*, Datenschutzinstrumente Anonymisierung, Pseudonyme und Verschlüsselung, DuD 2015, S. 503-509,
zitiert: *Hammer/Knopp*, DuD 2015, 503.

Han, *Dayuan* (韩大元), Analyse des öffentlichen Interesses im Verfassungstext (宪法文本中公共利益的规范分析), in: Legal Forum (法学论坛) 2005/1, S. 5-9,
zitiert als: *Han*, Legal Forum 2005/1, S.

Han, *Dayuan* (韩大元), Zur Bedeutung des Verfahrens der Verfassungsbeschwerde (论宪法诉愿程序的价值), in: Study & Exploration 2007/1, S. 94-99,
zitiert als: *Han*, Study & Exploration 2007/1, S.

Han, *Dayuan* (韩大元), (Bedeutung, Gedankengang und Rahmen des Gesetzes zum Verfahren der Auslegung der Verfassung《宪法解释程序法》的意义、思路与框架), in: Zhejiang Social Sciences (浙江社会科学) 2009/9, S. 15-22,
zitiert als: *Han*, Zhejiang Social Sciences 2009/9, S.

Han, *Dayuan* (韩大元), Konsens über die Anwendung der Verfassung aufgrund des Art. 126 Verfassung der VR China (以《宪法》第 126 条为基础寻求宪法适用的共识), in: Legal Science (法学) 2009/3, S. 4-10,
zitiert als: *Han*, Legal Science 2009/3, S.

Han, *Dayuan* (韩大元), Analyse des „Rechtsstaats“ in der Verfassung der VR China (中国宪法文本中“法治国家”规范分析), in: Jilin University Journal Social Sciences Edition (吉林大学社会科学学报) 2014/3, S. 67-74,
zitiert als: *Han*, Jilin University Journal Social Sciences Edition 2014/3, S.

Hatje, *Armin* / *Kindt*, *Anne*, Der Vertrag von Lissabon – Europa endlich in guter Verfassung? in: NJW 2008, S. 1761-1768,
zitiert als: *Hatje*/*Kindt*, NJW 2008, 1761.

Heißl, *Gregor*, Wiedereinführung der Vorratsdatenspeicherung: Analyse des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherdauer für Verkehrsdaten, in: Die öffentliche Verwaltung (DÖV) 2016, S. 588-594,
zitiert als: *Heißl*, DÖV 2016, 588.

Hensel, *Dirk*, Die Vorratsdatenspeicherung aus datenschutzrechtlicher Sicht: die Bildung von Persönlichkeitsprofilen und anderen Probleme der Vorratsdatenspeicherung, in: DuD, 2009, S. 527-530,
zitiert als: *Hensel*, DuD 2009, 527.

Henssler, *Martin* / *Kleen*, *Julia* / *Riegler*, *Andreas*, Auswirkungen der Vorratsdatenspeicherung auf das Berufsgeheimnis der Ärzte und Rechtsanwälte, in: Medizinrecht (MedR), 2016, S. 850-857,
zitiert als: *Henssler*/*Kleen*/*Riegler*, MedR 2016, 850.

Hermes, *Georg*, Art. 10, in: *Dreier*, *Horst* (Hrsg.), Grundgesetz Kommentar, 3. Auflage, Tübingen 2013,
zitiert als: *Hermes*, in: *Dreier* (Hrsg.), GG 2013, Art. 10 Rn.

Hetzer, *Wolfgang*, Terrorabwehr im Rechtsstaat, Zeitschrift für Rechtspolitik (ZRP) 2005, S. 132-135,
zitiert als: *Hetzer*, ZRP 2005, 132.

Hirsch, *Burkhard*, Aktuelle Sicherheitspolitik im Lichte des Verfassungsrechts, Eine notwendige Entgegnung, Erwiderung zu Schäuble, ZRP 2007, 210, ZRP 2008, S. 24-25,
zitiert als: *Hirsch*, ZRP 2008, 24.

Hiéramente, *Mayeul*, Legalität der strafprozessualen Überwachung des Surfverhaltens, in: Strafverteidiger – Forum (StraFo) 2013, S. 96-102,
zitiert als: Hiéramente, StraFo 2013, 96.

Hoeren, *Thomas* / *Sieber*, *Ulrich* / *Holznagel*, *Bernd* (Hrsg.): Handbuch Multimedia-Recht: Rechtsfragen des elektronischen Geschäftsverkehrs, 40. Ergänzungslieferung, München 2014,
zitiert als: Bearbeiter, in: *Hoeren*/*Sieber*/*Holznagel* (Hrsg.), 2014, Teil Rn.

Hoeren, *Thomas*, Vorratsdatenspeicherung im neuen Gewand: die Leitlinien des BMJV und ihre Auswirkung auf die Polizeiarbeit, in: Kriminalistik 2015, S. 469-472,
zitiert als: *Hoeren*, Kriminalistik 2015, 469.

Hoffmann-Riem, *Wolfgang*, Freiheit und Sicherheit im Angesicht terroristischer Anschläge, Zeitschrift für Rechtspolitik (ZRP) 2002, S. 497-501,
zitiert als: *Hoffmann-Riem*, ZRP 2002, 497.

Hoffmann-Riem, *Wolfgang*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, Juristenzeitung (JZ) 2008, S. 1009-1022,
zitiert als: *Hoffmann-Riem*, JZ 2008, 1009.

Horn, *Hans-Detlef*, Art. 2, in: *Stern*, *Klaus* / *Becker*, *Florian* (Hrsg.), Grundrechte-Kommentar, 2. Auflage, Köln 2016,
zitiert als: *Horn*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 2 Rn.

Hornung, *Gerrit* / *Schnabel*, *Christoph*, Verfassungsrechtlich nicht schlechthin verboten – Das Urteil des Bundesverfassungsgerichts in Sachen Vorratsdatenspeicherung, in: Deutsches Verwaltungsblatt (DVBI) 2010, S. 824-833,
zitiert als: *Hornung*/*Schnabel*, DVBI 2010, 824.

Hu, *Jinguang* (胡锦光), Untersuchung der Notwendigkeit und Realisierbarkeit der Verfassungsgerichtsbarkeit (宪法司法化的必然性与可行性探讨),in: Jurists Review (法学家) 1993/1, S. 51-52,
zitiert als: *Hu*, Jurists Review 1993/1, S.

Hu, Jinguang (胡锦光), Untersuchung der juristischen Anwendung der Verfassung der VR China (中国宪法的司法适用性探讨), in: Journal of Renmin University of China 1997/5, S. 58-63,
zitiert als: *Hu*, Journal of Renmin University of China 1997/5, S.

Hu, *Jinguang* (胡锦光), Voraussetzung der vom Bürger veranlassten Normenkontrolle (论公民启动违宪审查程序的原则), in: Studies in Law and Business (法商研究) 2003/5, S. 3-13,
zitiert als: *Hu*, Studies in Law and Business 2003/5, S.

Hu, *Jinguang* (胡锦光) / *Wang*, *Kai* (王锴), Abgrenzung des öffentlichen Interesses aus der Verfassung in der VR China (论我国宪法中公共利益的界定), in: Chinese Legal Science (中国法学) 2005/1, S. 18-27,
zitiert als: *Hu*/*Wang*, Chinese Legal Science 2005/1, S.

Hu, *Xiaohua* (胡肖华) / *Xu*, *Jing* (徐靖), Legitimation und Voraussetzung der Beschränkung der Grundrechte (论公民基本权利限制的正当性与限制原则), in: Law Review (法学评论) 2005/6, S. 3-10,
zitiert als: *Hu*/*Xu*, Law Review 2005/6, S.

Hu, *Yong* (胡泳), Die Kakophonie der persönlichen Meinungsäußerung und öffentlichen Diskussion im Zeitalter des Internets (众声喧哗—— 网络时代的个人表达与公共讨论), Guilin 2008,
zitiert als: *Hu*, 2008, S.

Huang, *Hui* (黄卉), Überdenken der Theorie der verfassungskonformen Auslegung (合宪性解释及其理论检讨), in: China Legal Science (中国法学) 2014/1, S.285-302,
zitiert als: *Huang*, China Legal Science 2014/1, S.

Huang, *Mingtao* (黄明涛), Unterschied zwischen den Begriffen der Verfassungsauslegung und der Möglichkeit der verfassungskonformen Auslegung

(两种“宪法解释”的概念分野与合宪性解释的可能性), in: China Legal Science (中国法学) 2014/6, S. 281-298,
zitiert als: *Huang*, China Legal Science 2014/6, S.

Indra, *Spiecker gen*. *Döhmann*, Anmerkung zu EuGH, Urteil v. 8. 4. 2014 – C-293/12, in: Juristen Zeitung (JZ) 2014, S. 1109-1113,
zitiert als: *Indra*, JZ 2014, 1109.

Jarass, *Hans D*., Charta der Grundrechte der Europäischen Union Kommentar, 3. Auflage, München 2016,
zitiert als: *Jarass*, GRCh 2016, Art. Rn.

Jarass, *Hans D.* / *Pieroth*, *Bodo*, Grundgesetz für die Bundesrepublik Deutschland: Kommentar, 14. Auflage, München 2016,
zitiert als: *Bearbeiter*, in: *Jarass*/*Pieroth*, GG 2016, Art. Rn.

Jiang, *Ge*, Datenschutzrecht in China: heute und morgen, in: DuD 2011, S. 642-647,
zitiert als: *Jiang*, DuD 2011, 642.

Jiang, *Xie* (姜昕), Verhältnismäßigkeitsprinzip im öffentlichen Recht (公法上比例原则研究), Dissertation, Jilin Universität (吉林大学) 2005,
zitiert als: *Jiang*, 2005, S.

Jiao, *Hongchang* (焦洪昌) / *Tang*, *Tong* (唐彤), Geltung des „Rechtsstaats“ in der Verfassung, Abgrenzung der Feststellung des „Rechtsstaates“ (论“依法治国”的宪法效力——兼谈“依法治国”规范的界定), in: Chinese Legal Science (中国法学) 1999/5, S. 33-41,
zitiert als: *Jiao*/*Tang*, Chinese Legal Science 1999/5, S.

Jiao, *Hongchang* (焦洪昌) / *Jia*, *Zhigang* (贾志刚), Theorie und Praxis der Drittwirkung der Grundrechte und ihre Bedeutung für die Justizialisierung der Verfassung in der VR China (基本权利对第三人效力之理论与实践

——兼论该理论对我国宪法司法化的指导意义), in: Xiamen University Law Review (厦门大学法律评论) 2003/1, S. 215-256,
zitiert als: *Jiao*/*Jia*, Xiamen University Law Review 2003/1, S.

Jiao, *Hongchang* (焦洪昌), Zum Spielraum der Anwendung der Verfassung der VR China von den Gerichten (论我国宪法司法适用的空间), in: Tribune of Political Science and Law (政法论坛) 2003/2, S. 18-23,
zitiert als: *Jiao*, Tribune of Political Science and Law 2003/2, S.

Kahler, *Thomas*, Vorratsdatenspeicherung: Wer spricht Recht? – BVerfG, EuGH, EGMR und die Klage gegen die Vorratsdatenspeicherung, in: DuD 2008, S. 449-454,
zitiert als: *Kahler*, DuD 2008, 449.

Kang, *Jingkui* (康敬奎), Mangel des Vorbehalts des Gesetzes im Gesetzgebungsgesetz und Verbesserungsvorschläge (立法法法律保留规则的缺失与完善), in: Jianghai Academic Journal (江海学刊) 2012/2, S. 136-142,
zitiert als: *Kang*, Jianghai Academic Journal 2012/2, S.

Karg, *Moritz*, IP-Adressen sind personenbezogene Verkehrsdaten, in: MMR-Aktuell 2011, 315811,
zitiert als: *Karg*, MMR-Aktuell 2011, 315811.

Karg, *Moritz*, Anmerkung zu BGH: Speicherung dynamischer IP-Adressen, in: MMR 2011, S. 345-346,
zitiert als: *Karg*, MMR 2011, 345.

Kingreen, *Thorsten*, Art. 6 EUV, in: *Calliess*, *Christian* / *Ruffert*, *Matthias* (Hrsg.), EUV/AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, Kommentar, 5. Auflage, München 2016,
zitiert als: *Kingreen*, in: *Calliess*/*Ruffert* (Hrsg.), 2016, Art. 6 EUV Rn.

Kipker, *Dennis-Kenji*, Informationelle Freiheit und staatliche Sicherheit – Rechtliche Herausforderungen moderner Überwachungstechnologien, Mohr Siebeck, 2016,
zitiert als: *Kipker*, S.

Kipker, *Dennis-Kenji* / *Schefferski*, *Julia* / *Stelter*, *Mattea*, Allgemeine und unterschiedslose Vorratsdatenspeicherung unzulässig, in: ZD 2017, S. 131-132,
zitiert als: *Kipker*/*Schefferski*/*Stelter*, ZD 2017, 131.

Kong, *Lingwang* (孔令望), Die neue Verfassung schützt die Würde der Persönlichkeit vor Eingriffen (新宪法保障公民的人格尊严不受侵犯), in: Law Science (法学) 1982/12, S. 7-8,
zitiert als: *Kong*, Law Science 1982/12, S.

Koshan, *Mansoor*, Vorratsdatenspeicherung – verfassungsrechtliche Rahmenbedingungen und rechtspolitische Verortung, in: DuD 2016, S. 167-171,
zitiert als: *Koshan*, DuD 2016, 167.

Krings, *Günter*, Terrorismusbekämpfung im Spannungsfeld zwischen Sicherheit und Freiheit, Zeitschrift für Rechtspolitik (ZRP) 2015, S. 167-170,
zitiert als: *Krings*, ZRP 2015, 167.

Kunnert, *Gerhard*, Das Ende der Vorratsdatenspeicherung? – Analyse der Schlussanträge des Generalanwalts in den verb. Rs. C-293/12 u. C-594/12 vom 12.12.2013, DuD 2014, S. 103-108,
zitiert als: *Kunnert*, DuD 2014, 103.

Kunnert, *Gerhard*, EuGH zur Vorratsdatenspeicherung: Außer Spesen nichts gewesen? Analyse des Urteils v. 8.5.2014 (C-293/12 u. C-594/12), in: DuD 2014, S. 774-784,
zitiert als: *Kunnert*, DuD 2014, 774.

Kutscha, *Martin*, Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte, Landes- und Kommunalverwaltung (LKV) 2008, S. 481-486,
zitiert als: *Kutscha*, LKV 2008, 481.

Kühling, *Jürgen*, Freiheitsverluste im Austausch gegen Sicherheitshoffnungen im künftigen Telekommunikationsgesetz?: verfassungsrechtliche Determinanten am Beispiel der Vorratsdatenspeicherung, in: Kommunikation & Recht (K&R) 2004, S. 105-112,
zitiert als: *Kühling*, K&R 2004, 105.

Kühling, *Jürgen*, Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht, in: Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2014, S. 681-685,
zitiert als: *Kühling*, NVwZ 2014, 681.

Kühling, *Jürgen* / *Seidel*, *Christian* / *Sivridis*, *Anastasios*, Datenschutzrecht, 2. neu bearbeitete Auflage, München 2011,
zitiert als: *Kühling*/*Seidel*/*Sivridis*, S.

Kühling, *Jürgen* / *Buchner*, *Benedikt* (Hrsg.), Datenschutz-Grundverordnung / BDSG Kommentar, 2. Auflage, München 2018,
zitiert als: *Bearbeiter*, in: *Kühling*/*Buchner* (Hrsg.), DSGO/BDSG 2018, Teil, Gesetz, Paragraph / Artikel Rn.

Lan, *Yuejun* (兰跃军), Technische Maßnahmen zur Strafverfolgung aus rechtsvergleichender Sicht (比较法视野中的技术侦查措施), in: Criminal Science (中国刑事法杂志) 2013/1, S. 66-74,
zitiert als: *Lan*, Criminal Science 2013/1, S.

Leutheusser-Schnarrenberger, *Sabine*, Vorratsdatenspeicherung: ein vorprogrammierter Verfassungskonflikt, in: Zeitschrift für Rechtspolitik (ZRP) 2007, S. 9-13,
zitiert als: *Leutheusser-Schnarrenberger*, ZPR 2007, 9.

Leutheusser-Schnarrenberger, *Sabine*, Grundrechtsschutz im Europa des Lissaboner Vertrags: Trends und Perspektiven, in: DuD 2010, S. 519-522,
zitiert als: *Leutheusser-Schnarrenberger*, DuD 2010, 519.

Leutheusser-Schnarrenberger, *Sabine*, Die Beerdigung 1. Klasse der anlasslosen Vorratsdatenspeicherung in Europa, in: DuD 2014, S. 589-592,
zitiert als: *Leutheusser-Schnarrenberger*, DuD 2014, 589.

Leutheusser-Schnarrenberger, *Sabine*, Der EuGH stärkt den Zusammenhalt in der Europäischen Union, in: DuD 2016, S. 354-356,
zitiert als: *Leutheusser-Schnarrenberger*, DuD 2016, 354.

Li, *Enci* (李恩慈) / *Zheng*, *Xianjun* (郑贤君), Beschränkungen der Grundrechte im Fall Sun Zhigang (由孙志刚案看宪法基本权利的限制), in: Jurists Review (法学家) 2004/2, S. 64-68,
zitiert als: *Li*/*Zheng*, Jurists Review 2004/2, S.

Li, *Haiping* (李海平), Analyse der Würde des Menschen in der Verfassung (宪法上的人的尊严的规范分析), in: Contemporary Law Review (当代法学) 2011/6, S. 27-33,
zitiert als: *Li*, Contemporary Law Review 2011/6, S.

Li, *Lihong* (李莉鸿), Mangel des Auskunftsrechts im Personalakte-System und Verbesserungsvorschläge (人事档案知情权存在的种种弊端及其改进方法), in: Beijing Archives (北京档案) 2010/2, S. 17-18,
zitiert als: *Li*, Beijing Archives 2010/2, S.

Li, *Xiaofen* (李晓芬), Schutz der Freiheit des Briefverkehrs und des Briefgeheimnisses der Bürger (公民通信自由和秘密法律保护问题研究), in: Modern Science & Technology of Telecommunications (现代电信科技) 2011/5, S. 38-41,

zitiert als: *Li*, Modern Science & Technology of Telecommunications 2011/5, S.

Li, *Zhong* (李忠), Schutz der Freiheit des Briefverkehrs im Zeitalter des Internets (互联网时代通信自由的保护), in: Juridical Science Journal (法学杂志) 2002/6, S. 26-28,
zitiert als: *Li*, Juridical Science Journal 2002/6, S.

Lin, *Laifan* (林来梵), Die Würde der Menschen und die Würde der Persönlichkeit, zu Auslegungsmöglichkeiten des Art. 38 Verfassung der VR China (人的尊严与人格尊严——兼论中国宪法第 38 条的解释方案), in: Zhejiang Social Sciences (浙江社会科学) 2008/3, S. 47-55,
zitiert als: *Lin*, Zhejiang Social Sciences 2008/3, S.

Lin, *Laifan* (林来梵), Chinesische Verfassungsgerichtsbarkeit: ihre Besonderheit, Entstehung und Entwicklung (中国的“违宪审查”：特色及生成实态—— 从三个有关用语的变化策略来看), in: Zhejiang Social Sciences (浙江社会科学) 2010/5, S. 33-40,
zitiert als: *Lin*, Zhejiang Social Sciences 2010/5, S.

Lin, *Laifan* (林来梵), Skript des Verfassungsrechts (宪法学讲义), 2. Auflage, Peking 2015,
zitiert als: *Lin*, 2015, S.

Liu, *Daoqin*, Stellung und Funktion des Bundesverfassungsgerichts, Verfassungsgerichtsbarkeit und ihre Perspektiven in China, Frankfurt am Main 2013,
zitiert als: *Liu*, 2013, S.

Liu, *Liantai* (刘连泰), Vorbehalt des Gesetzes in § 8 und 9 Gesetzgebungsgesetz der VR China (评我国立法法第八条第九条关于“法律保留”制

度), in: Journal of Henan Administrative Institute of Politics and Law (河南省政法管理干部学院学报) 2003/3, S.102-107,
zitiert als: *Liu*, Journal of Henan Administrative Institute of Politics and Law, 2003/3, S.

Liu, *Maolin* (刘茂林) / *Chen*, *Minghui* (陈明辉), Logik der verfassungsrechtliche Kontrolle und das Konzept ihrer Einrichtung (宪法监督的逻辑与制度构想), in: Contemporary Law Review (当代法学) 2015/1, S. 20-28,
zitiert als: *Liu*/*Chen*, Contemporary Law Review 2015/1, S.

Liu, *Quan* (刘权), Wiederaufbau der Legitimation des Zwecks- und des Verhältnismäßigkeitsprinzips (目的正当性与比例原则的重构), in: China Legal Science (中国法学) 2014/4, S. 133-150,
zitiert als: *Liu*, China Legal Science 2014/4, S.

Liu, *Wei* (刘炜), Geschichte des Personalakte-Systems (人事档案历史变迁), in: Zeitung für Demokratie und Recht (民主与法制时报), 2013. 11. 04,
zitiert als: *Liu*, Zeitung für Demokratie und Recht, 2013. 11. 04.

Liu, *Suhua* (刘素华), Schutz der fundamentalen Menschenrechte im Zeitalter des Internets (网络时代通讯自由基本人权保护研究), in: Zhejiang Academic Journal 2005/1, S. 164-169,
zitiert als: *Liu*, Zhejiang Academic Journal 2005/1, S.

Liu, *Zhigang* (刘志刚), Verfassungsrechtliche Bedeutung der Würde der Persönlichkeit (人格尊严的宪法意义), in: China Legal Science (中国法学) 2007/1, S. 37-44,
zitiert als: *Liu*, China Legal Science 2007/1, S.

Lou, *Yaoxiong* (娄耀雄), Studie zum Telekommunikationsrecht (电信法学研究), Peking, 2010,
zitiert als: *Lou*, 2010, S.

Lü, *Yanbin* (吕艳滨), Informatisierter Rechtsstaat, Regierung unter eineim neuen Blickwinkel (信息法治——政府治理新视角), Peking 2009,
zitiert als: *Lü*, 2009, S.

Ma, *Minhu* (马民虎), Untersuchung der Rechtsprobleme und Lösungen für die Netzsicherheit (网络安全法律问题及对策研究), Xian 2007,
zitiert als: *Ma*, 2007, S.

Mahnken, *Eva*, Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten – Rechtstatsachen zum Beleg der defizitären Rechtslage, vom Bundeskriminalamt, Stand: 15. November 2005, abrufbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2005RechtslageImZusammenhangMitMindestspeicherungsfristen.html,
zitiert als: *Mahnken*, S.

Mann, *Thomas*, Art. 12, in: *Sachs*, *Michael* (Hrsg.), Grundgesetz Kommentar, 7. Auflage, München 2014,
zitiert als: *Mann*, in: *Sachs* (Hrsg.), GG 2014, Art. 12 Rn.

Maunz, *Theodor* / *Dürig*, *Günter* (Begr.), Grundgesetz Kommentar, 81. Ergänzungslieferung August 2018, München 2018,
zitiert als: *Bearbeiter*, in: *Maunz*/*Dürig* (Begr.), GG 2017, Art. Rn.

Mayer, *Franz*, Der Vertrag von Lissabon im Überblick, in: Juristische Schulung (JuS) 2010, S. 189-195,
zitiert als: *Mayer*, JuS 2010, 189.

Men, *Zhongjing* (门中敬), Verhältnismäßigkeitsprinzip als ein Verfassungsprinzip und seine Ableitung, aus Sicht des Konzepts der Toleranz (比例原则的宪法地位与规范依据), in: Legal Forum (法学论坛) 2014/5, S. 94-102,

zitiert als: *Men*, Legal Forum 2014/5, S.

Meyer-Ladewig, *Jens* / *Nettesheim*, *Martin* / *von Raumer*, *Stefan*, Europäische Menschenrechtskonvention, Handkommentar, 4. Auflage, Baden-Baden 2017,
zitiert als: *Bearbeiter*, in: *Meyer-Ladewig*/*Nettesheim*/*von Raumer* (Hrsg.), EMRK 2017, Art. Rn.

Meyer, *Jürgen* (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Auflage, Baden-Baden 2014,
zitiert als: *Bearbeiter*, in: *Meyer* (Hrsg.), GRCh 2014, Art. Rn.

Meyerdierks, *Per*, Sind IP-Adressen personenbezogene Daten? in: MMR 2009, S. 8-13,
zitiert als: *Meyerdierks*, MMR 2009, 8.

Meyer-Goßner, *Lutz* / *Schmitt*, *Bertram*, Strafprozessordnung: StPO, Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen, 59. Auflage, München 2016,
zitiert als: Bearbeiter, in: *Meyer-Goßner*/*Schmitt*, StPO 2016, Paragraph Rn.

Mo, *Jihong* (莫纪宏) (Hrsg.), Theorie und Praxis der Verfassungsgerichtsbarkeit (违宪审查的理论与实践), Peking 2006,
zitiert als: *Mo*, 2006, S.

Mo, *Jihong* (莫纪宏), Theorie des Verfassungsrechts in der Praxis (实践中的宪法学原理), Peking, 2007, S.
zitiert als: *Mo*, 2007, S.

Moser-Knierim, *Antonie*, Vorratsdatenspeicherung, Zwischen Überwachungsstaat und Terrorabwehr, Wiesbaden, 2014,
zitiert als: *Moser-Knierim*, S.

Murswiek, *Dietrich*, Art. 2, in: *Sachs*, *Michael* (Hrsg.), Grundgesetz Kommentar, 7. Auflage, München 2014,
zitiert als: *Murswiek*, in: *Sachs* (Hrsg.), GG 2014, Art. 2 Rn.

Münch, *Holger*, Praktische Nutzung der „Vorratsdatenspeicherung", in: ZRP 2015, S. 130-132,
zitiert als: Münch, ZRP 2015, 130.

Nachbaur, *Andreas*, Vorratsdatenspeicherung „light" – Rechtswidrig und allenfalls bedingt von Nutzen, in: ZRP, 2015, S. 215-217,
zitiert als: *Nachbaur*, ZRP 2015, 215.

Nolte, *Martin*, Art. 12, in: *Stern*, *Klaus*/*Becker*, *Florian* (Hrsg.), Grundrechte-Kommentar, 2. Auflage, Köln 2016,
zitiert als: *Nolte*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 12 Rn.

Pache, *Eckhard* / *Rösch*, *Franziska*, Der Vertrag von Lissabon, in: Neue Zeitschrift für Verwaltungsrecht (NVwZ), 2008, S. 473-480,
zitiert als: *Pache*/*Rösch*, NVwZ 2008, 473.

Pache, *Eckhard* / *Rösch*, *Franziska*, Europäischer Grundrechtsschutz nach Lissabon – die Rolle der EMRK und der Grundrechtecharta in der EU, in: Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2008, S. 519-522,
zitiert als: *Pache*/*Rösch,* EuZW 2008, 519.

Pache, *Eckhard* / *Rösch*, *Franziska*, Die neue Grundrechtsordnung der EU nach dem Vertrag von Lissabon, in: Europarecht (EuR) 2009, S. 769-789,
zitiert als: *Pache*/*Rösch*, EuR 2009, 769.

Pagenkopf, *Martin*, Art. 10, in: *Sachs*, *Michael* (Hrsg.), Grundgesetz Kommentar, 7. Auflage, München 2014,
zitiert als: *Pagenkopf*, in: *Sachs* (Hrsg.), GG 2014, Art. 10 Rn.

Petri, *Thomas*, Die Richtlinie 2006/24/EG zur Vorratsspeicherung von Telekommunikationsverkehrsdaten: ein Problem des europäischen Grundrechtsschutzes, in: DuD 2011, S. 607-610,
zitiert als: *Petri*, DuD 2011, 607.

Petri, *Thomas*, Gestaltungsanforderungen nach dem Urteil des Bundesverfassungsgerichts vom 2. März 2010, in: *Roßnagel*, *Alexander* (Hrsg.), Nutzerschutz – Rechtsrahmen, Technikpotentiale, Wirtschaftskonzepte, Dokumentation der Stiftungstagung (zugleich EMR – Workshop) der Alcatel-Lucent Stiftung für Kommunikationsforschung, des Instituts für Europäisches Medienrecht (EMR) und der Landesanstalt für Kommunikation (LFK) Baden – Württemberg am 29. und 30. April 2010 in der Landesanstalt für Kommunikation (LFK) Baden – Württemberg, Stuttgart, Auflage 2012, Nomos, S. 123 – 131,
zitiert als: *Petri*, in: *Roßnagel* (Hrsg.), S.

Petri, *Thomas*, Anmerkung zu EuGH: Richtlinie über die Vorratsdatenspeicherung ungültig, in: Zeitschrift für Datenschutz (ZD), 2014, S. 296-300,
zitiert als: *Petri*, ZD 2014, 296.

Pfitzmann, *Andreas* / *Köpsell*, *Stefan*, Risiken der Vorratsdatenspeicherung – Grenzen der Nutzungsüberwachung, in: DuD, 2009, S. 542-546,
zitiert als: *Pfitzmann*/*Köpsell*, DuD 2009, 542.

Pi Yong (皮勇), Ermittlungsmaßnahmen der Cybercrime-Konvention und Vergleich mit einschlägigen Regelungen des Strafverfahrens (《网络犯罪公约》中的证据调查制度与我国相关刑事程序法比较), in: Chinese Legal Science (中国法学) 2003/4, S. 148-163,
zitiert als: *Pi*, Chinese Legal Science 2003/4, S.

Priebe, *Reinhard*, Reform der Vorratsdatenspeicherung – strenge Maßstäbe des EuGH, Europäische Zeitschrift für Wirtschaftsrecht (EuZW), 2014, S. 456-459,
zitiert als: *Priebe*, EuZW 2014, 456.

Priebe, *Reinhard*, Vorratsdatenspeicherung und kein Ende: strenge Anforderungen des EuGH an nationale Regelungen, in: EuZW, 2017, S. 136-139,
zitiert als: *Priebe*, EuZW 2017, 136.

Puschke, *Jens*, Die Vorratsdatenspeicherung als Instrument der Strafverfolgung: zur Notwendigkeit der Begrenzung staatlicher Überwachung, in: Datenschutz-Nachrichten (DANA) 2006, S. 65-73,
zitiert als: *Puschke*, DANA 2006, 65.

Puschke, *Jens* / *Singelnstein*, *Tobias*, Telekommunikationsüberwachung, Vorratsdatenspeicherung und (sonstige) heimliche Ermittlungsmaßnahmen der StPO nach der Neuregelung zum 1. 1. 2008, NJW 2008, 113-119,
zitiert als: *Puschke*/*Singelnstein*, NJW 2008, 113.

Qi, *Aimin* (齐爱民), Rettung der Persönlichkeit in der Informationsgesellschaft: Allgemeiner Datenschutz (拯救信息社会中的人格：个人信息保护法总论), Peking 2009,
zitiert als: *Qi*, 2006, S.

Qin, *Qianhong* (秦前红) / *Ye*, *Haibo* (叶海波), Funktion der Gesetzgebung bei der Garantie der Menschrechte, aus Sicht des „Vorbehalts des Gesetzes“ (论立法在人权保障中的地位——基于“法律保留”的视角), in: Law Review (法学评论) 2006/2, S. 3-10,
zitiert als: *Qin*/*Ye*, Law Review 2006/2, S.

Qin, *Qianhong* (秦前红), Hintergründe zur Ausarbeitung des Gesetzes des Verfahrens zur Auslegung der Verfassung und Untersuchung der einschlägigen Probleme (《宪法解释程序法》的制定思路和若干问题探究), in: Social Sciences in Chinese Higher Education Institutions (中国高校社会科学), 2015/3, S. 24-38,
zitiert als: *Qin*, Social Sciences in Chinese Higher Education Institutions, 2015/3, S.

Qin, *Qianhong* (秦前红), Bedeutung, Grundsätze und Durchführung der Verfassungsgerichtsbarkeit (合宪性审查的意义、原则及推进), in: Journal of Comparative Law (比较法研究) 2018/2, S.66-77,
zitiert als: *Qin*, Journal of Comparative Law 2018/2, S.

Qiu, *Linchuan* (邱林川) / *Chen*, *Taowen* (陈韬文), Ereignisse in neuen Medien (新媒体事件研究), Peking 2011,
zitiert als: *Qiu*/*Chen*, 2011, S.

Rao, *Chuanping* (饶传平), Internetrecht, Untersuchung zu neuen Themen und Problemstellungen (网络法律制度——前沿与热点专题研究), Peking 2005,
zitiert als: *Rao*, 2005, S.

Roßnagel, *Alexander* (Hrsg.), Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003,
zitiert als: *Bearbeiter*, in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, S. Rn.

Roßnagel, *Alexander* (Hrsg.), Beck´scher Kommentar zum Recht der Telemediendienste, München 2013,
zitiert als: *Bearbeiter*, in: *Roßnagel* (Hrsg.), 2013, Gesetz, Paragraph, Rn.

Roßnagel, *Alexander*, Das Bundesverfassungsgericht und die Vorratsdatenspeicherung in Europa, in: DuD 2010, S. 544-548,
zitiert als: *Roßnagel*, DuD 2010, 544.

Roßnagel, *Alexander*, Datenschutz in einem informatisierten Alltag, Gutachten für die Friedrich-Ebert-Stiftung, Berlin 2007,
zitiert als: *Roßnagel*, 2007, S.

Roßnagel, *Alexander*, Die „Überwachungs-Gesamtrechnung“ – Das BVerfG und die Vorratsdatenspeicherung, in: Neue juristische Wochenschrift (NJW) 2010, S. 1238-1242,
zitiert als: *Roßnagel*, NJW 2010, 1238.

Roßnagel, *Alexander* / *Bedner*, *Mark* / *Knopp*, *Michael*, Rechtlinie Anforderungen an die Aufbewahrung von Vorratsdaten, in: DuD, 2009, S. 536-541,
zitiert als: *Roßnagel*/*Bedner*/*Knopp*, DuD 2009, 546.

Roßnagel, *Alexander*, Neue Maßstäbe für den Datenschutz in Europa: Folgerungen aus dem EuGH-Urteil zur Vorratsdatenspeicherung, in: Multimedia und Recht (MMR) 2014, S. 372-377,
zitiert als: *Roßnagel*, MMR 2014, 372.

Roßnagel, *Alexander*, Die neue Vorratsdatenspeicherung – Der nächste Schritt im Ringen um Sicherheit und Grundrechtsschutz, NJW 2016, 533-539,
zitiert als: *Roßnagel*, NJW 2016, 533.

Roßnagel, *Alexander*, Vorratsdatenspeicherung rechtlich vor dem Aus? in: NJW 2017, S. 696-698,
zitiert als: *Roßnagel*, NJW 2017, 696.

Roßnagel, *Alexander* / *Moser-Knierim*, *Antonie* / *Schweda*, *Sebastian*, Interessenausgleich im Rahmen der Vorratsdatenspeicherung – Analysen und Empfehlungen, Nomos, 2013,
zitiert als: *Roßnagel*/*Moser-Knierim*/*Schweda*, S.

Sachs, *Michael* (Hrsg.), Grundgesetz Kommentar, 7. Auflage, München 2014,
zitiert als: *Bearbeiter*, in: *Sachs* (Hrsg.), GG 2014, Art. Rn.

Sandhu, *Aqilah*, Die Tele2-Entscheidung des EuGH zur Vorratsdatenspeicherung in den Mitgliedstaaten und ihre Auswirkungen auf die Rechtslage in

Deutschland und in der Europäischen Union: Anmerkung zum Urteil des EuGH vom 21.12.2016 in der Rs. C-203/15, in: Europarecht (EuR) 2017, S. 453-469,
zitiert als: *Sandhu*, EuR 2017, 453.

Schenke, *Ralf P.*, Art. 10, in: *Stern*, *Klaus*/*Becker*, *Florian* (Hrsg.), Grundrechte-Kommentar, 2. Auflage, Köln 2016,
zitiert als: *Schenke*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. 10 Rn.

Schramm, *Marc* / *Wegener*, *Christoph*, Neue Anforderungen an eine anlasslose Speicherung von Vorratsdaten Umsetzungsmöglichkeiten der Vorgaben des Bundesverfassungsgerichts, in: Multimedia und Recht (MMR) 2011, S. 9-13,
zitiert als: *Schramm*/*Wegener*, MMR 2011, 9.

Schroeder, *Werner*, Neues zur Grundrechtskontrolle in der Europäischen Union, in: Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2011, S. 462-467,
zitiert als: *Schroeder*, EuZW 2011, 462.

Schwarze, *Jürgen* / *Becker*, *Ulrich* / *Hatje*, *Armin* / *Schoo*, *Johann* (Hrsg.), EU-Kommentar, 3. Auflage, Baden-Baden 2012,
zitiert als: *Bearbeiter*, in: *Schwarze*/*Becker*/*Hatje*/*Schoo* (Hrsg.), 2012, Artikel, Rn.

Shangguan, *Piliang* (上官丕亮), Die Würde der Persönlichkeit in der Verfassung (论宪法上的人格尊严), in: Jiangsu Social Sciences (江苏社会科学) 2008/2, S. 77-83,
zitiert als: *Shangguan*, Jiangsu Social Sciences 2008/2, S.

Shangguan, *Piliang* (上官丕亮), Weg und Vorgehensweise der gegenwärtigen Justizialisierung der Verfassung der VR China (当下中国宪法司法化的路径与方法), in: Modern Law Science (现代法学) 2008/2, S. 3-16,

zitiert als: *Shangguan*, Modern Law Science, 2008/2, S.

Shen, *Zongling* (沈宗灵), Studie zur Rechtsvergleichung (比较法研究), Peking 1998,
zitiert als: *Shen*, 1998, S.

Shi, *Wenlong* (石文龙), Zur Entwicklung des Systems der Beschränkung der Grundrechte in der VR China: Rechtvergleichende Analyse zwischen Art. 51 Verfassung der VR China und Art. 19 Grundgesetz in Deutschland (论我国基本权利限制制度的发展——我国《宪法》第 51 条与德国《基本法》第 19 条之比较), in: Journal of Comparative Law (比较法研究) 2014/5, S. 161-174,
zitiert als: *Shi*, Journal of Comparative Law 2014/5, S.

Sieber, *Ulrich*, in: *Hoeren*, *Thomas* / *Sieber*, *Ulrich* / *Holznagel*, *Bernd* (Hrsg.): Handbuch Multimedia-Recht: Rechtsfragen des elektronischen Geschäftsverkehrs, 40. Ergänzungslieferung, München 2014, Teil 1,
zitiert als: *Sieber*, in: *Hoeren*/*Sieber*/*Holznagel* (Hrsg.), 2014, Teil 1 Rn.

Simitis, *Spiros*, Daten – oder Tatenschutz – ein Streit ohne Ende? in: NJW 1997, S. 1902-1903,
zitiert als: *Simitis*, NJW 1997, 1902.

Simitis, *Spiros*, Übermittlung der Daten von Flugpassagieren in die USA: Dispens vom Datenschutz? in: Neue juristische Wochenschrift (NJW) 2006, S. 2011-2014,
zitiert als: *Simitis*, NJW 2006, 2011.

Simitis, *Spiros*, Hat der Datenschutz noch eine Zukunft? in: Recht der Datenverarbeitung (RDV) 2007, S. 143-153,
zitiert als: *Simitis*, RDV 2007, 143.

Simitis, *Spiros*, Die Vorratsdatenspeicherung: ein unverändert zweifelhaftes Privileg, in: Neue juristische Wochenschrift (NJW) 2014, S. 2158-2160,
zitiert als: *Simitis*, NJW 2014, 2158.

Simon, *Dirk*, Präzeptoraler Sicherheitsstaat und Risikovorsorge, Frankfurt am Main, 2009,
zitiert als: *Simon*, S.

Skouris, *Vassilios*, Leitlinien der Rechtsprechung des EuGH zum Datenschutz, in: Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2016, S. 1359-1364,
zitiert als: *Skouris*, NVwZ 2016, 1359.

Song, *Hualin* (宋华琳), Freiheit der Geschäftstätigkeit und ihre Beschränkungen, Ausgangsfall: Einschränkung des Abstands zwischen Apotheken (营业自由及其限制——以药店距离限制事件为楔子), in: Eigentumsgarantie und verwaltungsrechtlicher Schutz: Beiträge zur Jahrestagung 2007 der chinesischen Gesellschaft für Verwaltungsrecht (财产权与行政法保护：中国法学会行政法学研究会 2007 年年会论文集), Wuhan 2008, S. 504-518,
zitiert als: *Song*, 2008, S.

Specht, *Louisa* / *Müller-Riemenschneider*, *Severin*, Dynamische IP-Adressen: Personenbezogene Daten für den Webseitenbetreiber? Aktueller Stand der Diskussion um den Personenbezug, in: ZD 2014, S. 71-75,
zitiert als: *Specht*/*Müller-Riemenschneider*, ZD 2014, 71.

Stern, *Klaus* / *Becker*, *Florian* (Hrsg.), Grundrechte-Kommentar, 2. Auflage, Köln 2016,
zitiert als: *Bearbeiter*, in: *Stern*/*Becker* (Hrsg.), GG 2016, Art. Rn.

Sun, *Ping* (孙平), Schutz der Privatsphäre vor der staatlichen Datenbanken (政府巨型数据库时代的公民隐私权保护), in: Legal Science (法学) 2007/7, S. 23-41,
zitiert als: *Sun*, Legal Science 2007/7, S.

Sun, *Yifei* (孙艺飞), Abwägung beim Konflikt zwischen der Freiheit des Briefverkehrs und der Ermittlung von Ordnungswidrigkeiten (通信自由权与调查取证权冲突之消解), in: Shandong Justice (山东审判) 2013/3, S. 74-78,
zitiert als: *Sun*, Shandong Justice 2013/3, S.

Sun, *Zhanwang* (孙展望), Abgrenzung des Vorbehalts des Gesetzes zum Gesetzesvorbehalt, Zuordnung des § 8 Gesetzgebungsgesetz zum Vorbehalt des Gesetzes (法律保留与立法保留关系辨析——兼论立法法第 8 条可纳入法律保留范畴), in: Tribune of Politial Science and Law (政法论坛) 2011/2, S. 105-112,
zitiert als: *Sun*, Tribune of Political Science and Law 2011/2, S.

Szuba, *Dorothee*, Vorratsdatenspeicherung, Der europäische und deutsche Gesetzgeber im Spannungsfeld zwischen Sicherheit und Freiheit, Baden-Baden, 2011,
zitiert als: *Szuba*, S.

Tang, *Zhongmin* (唐忠民), Zwei Probleme des Schutzes der Freiheit des Briefverkehrs und des Briefgeheimnis (公民通信自由和通信秘密保护的两个问题), in: Legal Science (法学) 2007/12, S. 13-17,
zitiert als: *Tang*, Legal Science 2007/12, S.

Terhechte, *Jörg Philipp*, Rechtsangleichung zwischen Gemeinschafts- und Unionsrecht: die Richtlinie über die Vorratsdatenspeicherung vor dem EuGH, Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2009, S. 199-204,
zitiert als: *Terhechte*, EuZW 2009, 199.

Terhechte, *Jörg Philipp*, Art. 52, in: *von der Groeben*, *Hans* / *Schwarze*, *h.c. Jürgen* / *Hatje Armin* (Hrsg.), Europäisches Unionsrecht, 7. Auflage, Baden-Baden 2015,

zitiert als: *Terhechte*, in: *von der Groeben*/*Schwarze*/*Hatje* (Hrsg.), Europäisches Unionsrecht 2015, Art. 52 Rn.

Thiel, *Markus*, Die „Entgrenzung" der Gefahrenabwehr, Grundfragen von Freiheit und Sicherheit im Zeitalter der Globalisierung, Tübingen 2011,
zitiert als: *Thiel*, S.

Tong, *Zhiwei* (童之伟), Die Anwendung der Verfassung muss die Verfassung befolgen (宪法适用应依循宪法本身规定的路径), in: China Legal Science (中国法学) 2008/6, S. 22-48,
zitiert als: *Tong*, China Legal Science 2008/6, S.

Trimbach, *Herbert Josef* / *Dietrich*, *Knud*, Freiheit und Sicherheit in rechtspolitischer Balance am Beispiel der Höchstspeicherfrist (vormals „Vorratsdatenspeicherung"), in: Neue Justiz (NJ) 2015, S. 461-466,
zitiert als: *Trimbach*/*Dietrich*, NJ 2015, 461.

Trute, *Hans-Heinrich*, in: *Roßnagel*, *Alexander* (Hrsg.), Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003,
zitiert als: *Trute*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, S.

von Danwitz, *Thomas*, Die Grundrechte auf Achtung der Privatsphäre und auf Schutz personenbezogener Daten: die jüngere Rechtsprechung des Gerichtshofes der Europäischen Union, in: DuD 2015, S. 581-585,
zitiert als: *von Danwitz*, DuD 2015, 581.

von der Groeben, *Hans*/*Schwarze*, *h.c. Jürgen*/*Hatje Armin*, Europäisches Unionsrecht, 7. Auflage, Baden-Baden 2015,
zitiert als: *Bearbeiter*, in: *von der Groeben*/*Schwarze*/*Hatje* (Hrsg.), 2015, Art. Rn.

Wang, *Hui* (王晖), Konzept der Würde des Menschen und seine Institutionalisierung (人之尊严的理念与制度化), in: China Legal Science (中国法学) 2014/4, S. 103-118,
zitiert als: *Wang*, China Legal Science 2014/4, S.

Wang, *Kai* (王锴), Überdenken der verfassungskonformen Auslegung (合宪性解释之反思), in: The Jurist (法学家) 2015/1, S. 45-57,
zitiert als: *Wang*, The Jurist 2015/1, S.

Wang, *Kai* (王锴), Wirkung des allgemeinen Persönlichkeitsrechts auf das Zivilrecht (论宪法上的一般人格权及其对民法的影响), in: China Legal Science (中国法学) 2017/3, S. 102-121,
zitiert als: *Wang*, China Legal Science 2017/3, S.

Wang, *Xiuzhe* (王秀哲), Auslegung der Rechtsvorschriften der Normenkontrolle veranlasst vom Bürger im Gesetzgebungsgesetz (公民启动违宪审查的立法法相关条款解读), in: *Mo*, *Jihong* (莫纪宏) / *Xie*, *Weiyan* (谢维雁) (Hrsg.), Studien zum Staatsrecht (宪法研究) Band 10, Chengdu 2009, S. 234-243,
zitiert als: *Wang*, in: *Mo*/*Xie* (Hrsg.) 2009, S.

Wang, *Xiuzhe* (王秀哲), Probleme im Verfahren der Normenkontrolle veranlasst vom Bürger und Verbesserungsvorschläge (公民启动违宪审查的法律困境与制度完善), in: Northern Legal Science (北方法学) 2010/1, S. 29-35,
zitiert als: *Wang*, Northern Legal Science 2010/1, S.

Weber, *Albrecht*, Vom Verfassungsvertrag zum Vertrag von Lissabon, in: EuZW 2008, S. 7-14,
zitiert als: *Weber*, EuZW 2008, 7.

Weidner-Braun, *Ruth*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung, am Beispiel des personenbezogenen Datenverkehrs im WWW nach deutschem öffentlichen Recht, Berlin 2012,
zitiert: *Weidner-Braun*, S.

Weiß, *Wolfgang*, Grundrechtsschutz durch den EuGH: Tendenzen seit Lissabon, in: Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2013, S. 287-292,
zitiert als: *Weiß*, EuZW 2013, 287.

Westphal, *Dietrich*, Die neue EG-Richtlinie zur Vorratsdatenspeicherung – Privatsphäre und Unternehmerfreiheit unter Sicherheitsdruck, in: Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2006, S. 555-560,
zitiert als: *Westphal*, EuZW 2006, 555.

Wieland, *Joachim*, Art. 12, in: *Dreier*, *Horst* (Hrsg.), Grundgesetz Kommentar, 3. Auflage, Tübingen 2013,
zitiert als: *Wieland*, in: *Dreier* (Hrsg.), GG 2013, Art. 12 Rn.

Wolff, *Heinrich Amadeus*, Anmerkung zum Urteil des Europäischen Gerichtshofs vom 8.4.2014 zur Vorratsdatenspeicherung, in: Die öffentliche Verwaltung (DÖV) 2014, S. 608-612,
zitiert als: *Wolff*, DÖV 2014, 608.

Wu, *Huifan* (吴惠凡), Erleuchtung und Ernüchterung der Cyber-Bürger, von Wiederaufbau der Mitsprache zu politischer Mitwirkung (网络公民的启蒙与觉醒：从话语重构到政治参与), in: Contemporary Communication 2015/1, S.17-22,
zitiert als: *Wu*, Contemporary Communication (当代传播) 2015/1, S.

Xia, *Yinye* (夏引业), Eine kombinierte verfassungsrechtliche Kontrolle muss in der VR China eingerichtet werden (我国应设立虚实结合的宪法监督体制), in: Political Science and Law (政治与法律) 2016/2, S. 66-80,

zitiert als: *Xia*, Political Science and Law 2016/2, S.

Xia, *Zhenglin* (夏正林), Verbesserung der Institution der Anwendung der Verfassung der VR China (我国宪法适用体制的改善), in: Social Sciences in Guangdong (广东社会科学), 2013/2, S. 235-241,
zitiert als: *Xia*, Social Sciences in Guangdong, 2013/2, S.

Xia, *Zhenglin* (夏正林), Untersuchung der Theorie der verfassungskonformen Auslegung ("合宪性解释"理论辨析及其可能前景), in: China Legal Science (中国法学) 2017/1, S. 288-302,
zitiert als: *Xia*, China Legal Science 2017/1, S.

Xiao, *Weiyun* (肖蔚云), Die Verfassung als grundlegender Maßstab in der richterlichen Beurteilung (宪法是审判工作的根本法律依据), in: Juridical Science Journal (法学杂志) 2002/3, S. 3-4,
zitiert als: *Xiao*, Juridical Science Journal 2002/3, S.

Xie, *Libin* (谢立斌), Verfassungsrechtlicher und einfachgesetzlicher Schutz von personenbezogenen Daten (个人数据的宪法和法律保护), in: *Mo*, *Jihong* (莫纪宏) / *Xie*, *Weiyan* (谢维雁) (Hrsg.), Staatsrecht Forschung (宪法研究) Band 10, Chengdu 2009, S. 158-169,
zitiert als: *Xie*, *Libin*, in: *Mo*/*Xie* (Hrsg.) 2009, S.

Xie, *Libin* (谢立斌), Würde der Persönlichkeit in der VR China und Deutschland aus rechtsvergleichender Sicht, Gegenansicht zu Prof. Lin Laifan (中德比较宪法视野下的人格尊严——兼与林来梵教授商榷), Tribune of Political Science and Law (政法论坛) 2010/4, S. 53-67,
zitiert als: *Xie*, Tribune of Political Science and Law 2010/4, S.

Xie, *Libin* (谢立斌), Zum Schutz der Grundrechte durch die Gerichte (论法院对基本权利的保护), in: The Jurist (法学家) 2012/2, S. 32-42,
zitiert als: *Xie*, The Jurist 2012/2, S.

Xie, *Libin* (谢立斌), Auslegung der Verfassung (宪法解释), Peking 2014,
zitiert als: *Xie*, 2014, S.

Xie, *Libin* (谢立斌), Schutzniveau der gesetzgeberischen Gewährleistung der Grundrechte (论基本权利的立法保障水平), in: Journal of Comparative Law (比较法研究) 2014/4, S. 40-50,
zitiert als: *Xie*, Journal of Comparative Law 2014/4, S.

Xie, *Weiyan* (谢维雁), Aufbau eines kombinierten Systems der Verfassungsbeschwerde in der VR China (论我国复合型宪法诉讼制度的构建), in: *Mo*, *Jihong* (莫纪宏) / *Xie*, *Weiyan* (谢维雁) (Hrsg.), Staatsrecht Forschung (宪法研究) Band 10, Chengdu 2009, S. 260-272，
zitiert als: *Xie*, *Weiyan*, in: *Mo*/*Xie* (Hrsg.) 2009, S.

Xie, *Weiyan* (谢维雁), Verfassungskonforme Auslegung ist keine juristische Anwendung der Verfassung (论合宪性解释不是宪法的司法适用方式), China Legal Science (中国法学) 2009/6, S. 168-177,
zitiert als: *Xie*, China Legal Science 2009/6, S.

Xie, *Weiyan* (谢维雁), Zu Fällen der Anwendung der Verfassung (论宪法适用的几种情形), in: Zhejiang Academic Journal (浙江学刊), 2014/6, S. 151-158,
zitiert als: *Xie*, Zhejiang Academic Journal, 2014/6, S.

Xie, *Zhiyong* (解志勇) / *Yu Peng* (于鹏), Rechtsvergleichung der Gesetzgebung der Informationssicherheit (信息安全立法比较), Peking 2007,
zitiert als: *Xie*/*Yu*, S.

Xu, *Chongde* (许崇德), Fragen zur „Justizialisierung der Verfassung“ (“宪法司法化”质疑), in: The People´s Congress of China (中国人大) 2006/11, S. 44-45,

zitiert als *Xu*, The People´s Congress of China 2006/11, S.

Xue, *Changli* (薛长礼), Theorie des Rechts auf Arbeit (劳动权论), Dissertation, Jilin Universität (吉林大学) 2006,
zitiert als: *Xue*, 2006, S.

Yao, *Yuerong* (姚岳绒), Ableitung des Rechts auf informationelle Selbstbestimmung als Grundrecht (论信息自决权作为一项基本权利在我国的证成), in: Political Science and Law (政治与法律) 2012/4, S. 72-83,
zitiert als: *Yao*, Political Science and Law 2012/4, S.

Ye, *Haibo* (叶海波), Verbesserungsvorschläge für das Normenkontrollverfahren (论法规审查机制的完善), in: Journal of the Party School of CPC Xiamen Municipal Committee (厦门特区党校学报) 2008/3, S. 39-42,
zitiert als: *Ye*, Journal of the Party School of CPC Xiamen Municipal Committee 2008/3, S.

Yi, *Xifeng* (仪喜峰), Gewährleistung der Würde der Persönlichkeit aus Sicht der Legitimation der Verfassung (宪法正当性视野下的人格尊严保障), in: Hebei Law Science (河北法学) 2012/12, S. 78-84,
zitiert als: *Yi*, Hebei Law Science 2012/12, S.

Ying, *Songnian* (应松年), Ein entscheidendes Gesetz zur Förderung des Rechtsstaates: wichtige Fragen zum Gesetzgebungsgesetz (一部推进依法治国的重要法律——关于立法法中的几个重要问题), in: Chinese Legal Science (中国法学) 2000/4, S. 3-10,
zitiert als: *Ying*, Chinese Legal Science 2000/4, S.

Yu, *An* (于安), Problem bei der Umsetzung der Rechtspolitik des Rechtsstaates (依法治国方略的实施问题), in: Jurists´ Review (法学家) 1999/3, S. 61-62,
zitiert als: *Yu*, Jursts´ Review 1999/3, S.

Yuanshi, *Bu*, Einführung in das Recht Chinas, München 2009,
zitiert als: *Bu*, 2009, S.

Yu, *Chong* (于冲), Verbesserung und Entwicklung der Gesetzgebung für Strafsystem der Internetkriminalität – Vom Strafgesetzbuch 1997 zum Entwurf des 9. Änderungsantrags (网络犯罪罪名体系的立法完善与发展思路——从 97 年刑法到《刑法修正案（九）草案》), in: Journal of CUPL, 2015/4, S. 39-54,
zitiert als: *Yu*, Journal of CUPL (中国政法大学学报), 2015/4, S.

Yu, *Lingyun* (余凌云) / *Hong*, *Yanqing* (洪延青), Begrenzung der Befugnis zum Lauschangriff im Rahmen von Ermittlungstätigkeiten zur Bekämpfung der terroristischen Kriminalität (反恐侦查中的监听权力规制), in: China Public Security (Academy Edition) (中国公共安全(学术版)) 2007/3, S. 104-114,
zitiert als: *Yu*/*Hong*, China Public Security (Academy Edtion) 2007/3, S.

Yu, *Zhigang* (于志刚), Der Trend und die Strategie der Netzsicherheit im Gebiet der öffentlichen Sicherheit und Staatssicherheit (网络安全对公共安全，国家安全的嵌入态势和应对策略), in: Legal Forum (法学论坛) 2014/6, S. 5-19,
zitiert als: *Yu*, Legal Forum 2014/6, S.

Yu, *Zhigang* (于志刚), Evolution des Denkens des Internets und Gedankengang der Bestrafung der Internetkriminalität (网络思维的演变与网络犯罪的制裁思路), in: Peking University Law Journal (中外法学) 2014/4, S. 1045-1058,
zitiert als: *Yu*, Peking University Law Journal 2014/4, S.

Zhang, *Jianwen* (张建文), Wiederaufbau des Personalakte-Systems aus datenschutzrechtlicher Sicht (从个人资料保护看人事档案法制的改革), in: Archives Science Study (档案学研究) 2009/3, S. 27-29,
zitiert als: *Zhang*, Archives Science Study 2009/3, S.

Zhang, *Jie* (张杰) / *Li*, *Changxi* (李长喜), Schutz des Briefgeheimnisses (通信秘密法律保护研究), in: Journal of Yunnan University Law Edition 2005/2, S. 41-44,
zitiert als: *Zhang*/*Li*, Journal of Yunnan University Law Edition 2005/2, S.

Zhang, *Juan* (张娟), Öffentlich-rechtliche Untersuchung des Datenschutzes (个人信息的公法保护研究), Dissertation, China Universität von Politik- und Rechtswissenschaft (中国政法大学) 2011,
zitiert als: *Zhang*, 2011, S.

Zhang, *Qianfan* (张千帆), Einführung des Verfassungsrechts, Theorie und Anwendung (宪法学导论——原理与应用), 3. Auflage, Peking 2014,
zitiert als: *Zhang*, 2014, S.

Zhang, *Xiang* (张翔), Logik der Beschränkung von Grundrechten zwecks öffentlichen Interesses (公共利益限制基本权利的逻辑), in: Legal Forum (法学论坛) 2005/1, S. 24-27,
zitiert als: *Zhang*, Legal Forum 2005/1, S.

Zhang, *Xiang* (张翔), Theoretischer Aufbau der Beschränkung auf Grundrechte (基本权利限制问题的思考框架), in: Jurists Review (法学家) 2008/1, S. 134-139,
zitiert als: *Zhang*, Jurists Review 2008/1, S.

Zhang, *Xiang* (张翔), Zwei verfassungsrechtliche Fälle: die mögliche Wirkung der Verfassung auf die Justiz aus der Sicht der verfassungskonformen

Auslegung (两种宪法案件：从合宪性解释看宪法对司法的可能影响), in: China Legal Science (中国法学) 2008/3, S. 110-116,
zitiert als: *Zhang*, China Legal Science 2008/3, S.

Zhao, *Hong* (赵宏), Schranken-Schranken, Die Logik der Beschränkung von Grundrechten in Deutschland (限制的限制——德国基本权利限制模式的内在机理), in: Jurist (法学家) 2011/2, S. 152-166,
zitiert als: *Zhao*, Jurist 2011/2, S.

Zhao, *Hong* (赵宏), Gegenwart und Zukunft der Gesetzgebung des Schutzes des Rechts auf informationelle Selbstbestimmung in der VR China (信息自决权在我国的保护现状及其立法趋势前瞻), in: China Law Review (中国法律评论) 2017/1, S. 147-161,
zitiert als: *Zhao*, China Law Review 2017/1, S.

Zhao, *Hong* (赵宏), Von Information Disclosure zu Datenschutz, Änderung der Forschungsrichtung und Kernfrage des öffentlich-rechtlichen Datenschutzes (从信息公开到信息保护——公法上信息权保护研究的风向流转与核心问题), in: Journal of Comparative Law (比较法研究) 2017/2, S.31-46,
zitiert als: *Zhao*, Journal of Comparative Law 2017/2, S.

Zhen, *Shuqing* (甄树青), Meinungsfreiheit (论表达自由), Peking 2000,
zitiert als: *Zhen*, 2000, S.

Zheng, *Xianjun* (郑贤君), Funktion der Rechtsvorschrift der „Würde der Persönlichkeit“ in der chinesischen Verfassung (宪法“人格尊严”条款的规范地位之辨), in: China Legal Science (中国法学) 2012/2, S. 79-89,
zitiert als: *Zheng*, China Legal Science 2012/2, S.

Zhou, *Hanhua* (周汉华), Entwurf des Datenschutzgesetzes in der VR China und Begründung der Gesetzgebung aus wissenschaftlicher Sicht (中华人民共和国个人信息保护法专家建议稿及立法报告), Peking 2006,
zitiert als: *Zhou*, 2006, S.

Zhou, *Wei* (周伟), Problem beim Schutz der Freiheit des Briefverkehrs und des Briefgeheimnisses (通信自由与通信秘密的保护问题), in: Legal Science (法学) 2006/6, S. 57-62,
zitiert als: *Zhou*, Legal Science 2006/6, S.

Zhu, *Huhui* (朱福惠), Chinesischer Kontext und chinesische Logik der verfassungskonformen Auslegung von Gesetzen – Vorgehensweise der Anwendung der Verfassung durch die Volksgerichte (法律合宪性解释的中国语境与制度逻辑——兼论我国法院适用宪法的形式), in: Modern Law Science (现代法学) 2017/1, S. 3-16,
zitiert als: *Zhu*, Modern Law Science 2017/1, S.

Ziebarth, *Wolfgang*, Grundrechtskonforme Gestaltung der Vorratsdatenspeicherung – Überlegungen zu einer europa-, verfassungs- und datenschutzrechtskonformen Umsetzung, in: DuD 2009, S. 25-32,
zitiert als: *Ziebarth*, DuD 2009, 25.

Ziebarth, *Wolfgang*, Die Vorratsdatenspeicherung im Wandel der EuGH-Rechtsprechung, in: Zeitschrift für Urheber- und Medienrecht (ZUM) 2017, S. 398-405,
zitiert als: *Ziebarth*, ZUM 2017, 398.

Zimmer, *Heiko*, Zugriff auf Internetzugangsdaten, Unter besonderer Berücksichtigung der Verhältnismäßigkeit einer verdachtsunabhängigen Vorratsdatenspeicherung, Eine Interessenabwägung zwischen Datenschutz, Strafverfolgung und Urheberrecht im Internet, Frankfurt am Main 2012,
zitiert als: *Zimmer*, S.

Zweigert, *Konrad* / *Kötz*, *Hein*, Einführung in die Rechtsvergleichung, auf dem Gebiete des Privatrechts, 3.,neubearbeitet Auflage, Tübingen 1996,
zitiert als: *Zweigert*/*Kötz*, 1996, S.

Zöller, *Mark A*, Vorratsdatenspeicherung zwischen nationaler und europäischer Strafverfolgung, Goltdammer´s Archiv für Strafrecht (GA) 2007, S. 393-414,
zitiert als: *Zöller*, GA 2007, 393.