Die Vorratsdatenspeicherung als Spielball höchstgerichtlicher Rechtsprechung

Von Prof. Dr. **Jens Puschke**, LL.M. (King's College), Marburg*

Die Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten ist eines der besonders intensiv diskutierten Sicherheitsprojekte der vergangenen zwei Jahrzehnte. Die hierzu ergangenen Urteile des BVerfG und des EuGH weisen in den Auswirkungen auf die Zulässigkeit einer solchen Maßnahme erhebliche Differenzen auf, basieren aber auf vergleichbaren rechtlichen Prämissen. Rechtskulturelle Differenzen können insofern weniger in den materiellen Grundlagen der Entscheidungen als in kompetenziellen Fragen erblickt werden.

I. Einleitung

Das Verhältnis von Sicherheit und Freiheit ist Inhalt grundlegender gesellschaftlicher Debatten. Die vertretenen Einstellungen divergieren nach politischen Anschauungen und aufgrund kultureller Prägungen. Nicht umsonst wird übergreifend von einer „Sicherheitskultur" gesprochen. Wo die Grenzen von in Grundrechte eingreifenden Sicherheitsmaßnahmen liegen, wird gerade für den Umgang mit Kriminalität kontrovers diskutiert. Die Diskussion erfolgt regional, innerhalb der Nationalstaaten und auf der Ebene der Europäischen Union mit unterschiedlicher Intensität und Schwerpunktsetzung. Im rechtlichen Diskurs spielen dabei Sicherheitsgesetze und ihre Ausgestaltung eine bedeutsame Rolle. Dies ruft die nationale und europäische höchstgerichtliche Rechtsprechung auf den Plan, die angehalten ist, absolute Grenzen für staatliche Eingriffsbefugnisse mit Blick auf die Grundrechte zu definieren. Bei der Beurteilung einer der beachtenswertesten sicherheitsrechtlichen Regelungen der vergangenen Jahre, der Vorratsdatenspeicherung, traten inmitten eines langen politischen Tauziehens inhaltliche Differenzen in Entscheidungen des BVerfG und des EuGH zu Tage. Der Beitrag beschäftigt sich mit den Regelungen zur Vorratsdatenspeicherung und den hierzu ergangenen Entscheidungen. Dabei wird auch der Frage nachgegangen, ob sich die inhaltlichen Abweichungen in den Urteilen des BVerfG und des EuGH als rechtskulturelle Differenzen auf einer vertikalen Ebene zwischen europäischer und deutscher Rechtsprechung deuten lassen.[1]

II. Hintergründe der Diskussion um die Vorratsdatenspeicherung

1. Ausweitung des nationalen und europäischen Sicherheitsrechts

Die Verfolgung und Verhütung von Straftaten ist ein zentraler Gegenstand nationaler und europäischer Politik und Gesetzgebung. Entsprechend hat das Sicherheitsrecht in den vergangenen Jahrzehnten eine beträchtliche Ausdehnung erfahren. Dies gilt in Deutschland für die Erweiterung des Strafrechts und der Eingriffsbefugnisse in der Strafprozessordnung in gleicher Weise wie für Maßnahmen im Polizeirecht und im Recht der Nachrichtendienste.[2] Ausgeweitet wird auch die allgemeine Strafverfolgungsvorsorge, insbesondere durch die Ansammlung und Verknüpfung großer Datenbestände, wozu neben dem Aufbau einer Antiterrordatei[3] und der Speicherungspflicht für Fluggastdaten[4] auch die im Zentrum dieses Beitrages stehende Vorratsdatenspeicherung von Verkehrsdaten der Telekommunikation zählt. Diese Entwicklung betrifft nicht nur Deutschland: Sie lässt sich in vielen Mitgliedstaaten der Europäischen Union in ähnlicher Weise aufzeigen und steht im Zusammenhang mit dem Fortschreiten einer Sicherheitsgesellschaft.[5] Sie ist zudem nicht allein durch die nationalen Rechtsordnungen bestimmt, sondern geht häufig auf europäische Initiativen und Vorgaben zurück.[6]

2. Parallele Entwicklung datenschutzrechtlicher Vorgaben

Parallel hierzu werden grundrechtliche Schutzstandards intensiv diskutiert und sind Grundlage und Gegenstand vielzähliger nationaler und europäischer Gerichtsentscheidungen. Gerade in einem sich ausdehnenden Sicherheitsrecht müssen rechtsstaatliche Begrenzungen ausreichende Beachtung finden und gegen die Überbetonung von Sicherheitsbelangen gesetzt werden. Dies gilt in besonderer Weise für das Strafrecht als „schärfstes Schwert" des Staates und konkret für das Strafverfahrensrecht als geronnenes Verfassungsrecht[7] und als Seismograph der Staatsverfassung[8]. Für Letzteres gewan-

---

* Prof. *Dr. Jens Puschke* ist seit dem 17.10.2016 Inhaber der Professur für Strafrecht, Strafprozessrecht, Kriminologie und Medizinstrafrecht an der Philipps-Universität Marburg. Der Beitrag stellt eine angepasste Fassung seiner öffentlichen Antrittsvorlesung dar, die er am 22.6.2018 in der Aula der Alten Universität gemeinsam mit *Stefanie Bock*, *Sven Simon* und *Constantin Willems* unter dem Oberthema „Rechtskulturelle Differenzen in Europa" gehalten hat.

[1] Siehe zum vagen und vielschichtigen Begriff der Rechtskultur *Mankowski*, Rechtskultur, 2016, S. 1 ff.

[2] Vgl. nur *Puschke*, in: Goeckenjan/Puschke/Singelnstein (Hrsg.), Für die Sache – Kriminalwissenschaften aus unabhängiger Perspektive, Festschrift für Ulrich Eisenberg zum 80. Geburtstag, 2019, S. 695 (698 ff.).

[3] BGBl. I 2006, S. 3409.

[4] BGBl. I 2017, S. 1484; hierzu die eingehende Kritik von *Arzt*, DÖV 2017, 1023.

[5] Vgl. nur *Singelnstein/Stolle*, Die Sicherheitsgesellschaft, 3. Aufl. 2012, S. 17 ff.; zur Rechtskultur in der Risikogesellschaft *Mankowski* (Fn. 1), S. 142 ff.

[6] Zu den Einflüssen auf das materielle Strafrecht s. bei *Bock*, ZIS 2019, 298 m.w.N.; hinsichtlich einer Vorfeldkriminalisierung vgl. *Puschke*, Legitimation, Grenzen und Dogmatik von Vorbereitungstatbeständen, 2017, S. 32 ff.

[7] Siehe hierzu *Jahn*, JuS 2005, 1057.

[8] *Roxin/Schünemann*, Strafverfahrensrecht, 29. Aufl. 2017, § 2 Rn. 1.

nen in den vergangenen Jahrzehnten das Recht auf Privatheit, das Recht auf informationelle Selbstbestimmung und das Grundrecht des Art. 10 GG als datenschutzrechtliche Grundprämissen zunehmend an Bedeutung. Dies ist Folge der beträchtlichen Steigerung der Relevanz von Informationen und Daten für die Strafverfolgung, was zur Einführung einer Vielzahl eingriffsintensiver verdeckter Eingriffsbefugnisse zur Informationsbeschaffung in die StPO geführt hat. Gleiches gilt für informatorische Maßnahmen im Vorfeld der Strafverfolgung, wie die Vorratsdatenspeicherung. Auch diese werden für eine umfassende Bewertung eines strafrechtsbezogenen Grundrechtsschutzes immer bedeutsamer, da sie auch mit dem Ziel eingeführt werden, Erkenntnisse für spätere Strafverfahren zu erbringen.

Die Relevanz eines Datenschutzrechts, das staatliche Informationseingriffe zu begrenzen versucht, wurde in Deutschland zunächst national vor allem durch das Volkszählungsurteil[9] geprägt.[10] Daneben und im Zusammenhang hiermit wurden die Datenschutzgesetze von Bund und Ländern etabliert und erweitert. Es erging zudem eine Vielzahl von Entscheidungen des BVerfG im Bereich des Sicherheitsrechts, die neu geschaffenen Eingriffsbefugnissen zur Strafverfolgung, Straftatenverhütung oder Strafverfolgungsvorsorge aus dem Grundgesetz abgeleitete Grenzen setzten.[11] Auch auf europäischer Ebene hat der Datenschutz einen hohen Stellenwert,[12] wobei die in Art. 7 GRCh gewährleistete Achtung des Privat- und Familienlebens und der in Art. 8 GRCh festgeschriebene Schutz personenbezogener Daten zusammen mit weiteren europäischen datenschutzrechtlichen Vorgaben und Grundrechtsinterpretationen an Einfluss gewinnen.[13] Als Folge hiervon und in Verbindung mit den sicherheitsrechtlichen Bestrebungen auf europäischer Ebene beschäftigt sich auch der EuGH immer häufiger mit Fragen des Datenschutzes in Bezug auf sicherheitsrechtliche Belange.[14]

3. Nationale und europäische Schutzstandards

In der deutschen Diskussion um rechtsstaatliche Grenzen bei der Verfolgung und Verhütung von Straftaten wird mit Blick auf die verfassungsrechtlichen Grundsätze häufig der besonders hohe Schutzstandard, wie er sich aus dem Grundgesetz ergebe, hervorgehoben. Damit wird zumeist die Skepsis verbunden, dass der europäische Grundrechtsschutz dem deutschen nachstehe.[15] Insofern gilt insbesondere das materielle Strafrecht als eine der letzten Bastionen nationaler Gesetzgebung, das europäischen Einflüssen in seinem Kern entzogen und durch die strikten Vorgaben des Grundgesetzes eingehegt bleiben soll.[16] Gerade für das eingriffsintensive Strafrecht müssten die hohen Standards gewahrt bleiben, die das Grundgesetz vorsehe. Diese grundlegende Skepsis gegenüber geringeren europäischen Schutzstandards läuft im Hintergrund bundesverfassungsgerichtlicher Entscheidungen, strafrechtsbezogen vor allem im Lissabon-Urteil[17] und in dem Beschluss zur Auslieferung bei Abwesenheitsentscheidungen,[18] mit.

Für das materielle Strafrecht dient vor allem das verfassungsrechtlich verankerte und in Art. 1 GG verortete Schuldprinzip als unüberwindbare Identitäts- und Schutzstandardschranke gegenüber europäischen Vereinnahmungsversuchen, weshalb bei einem entsprechenden Verstoß hiergegen der Anwendungsvorrang von Europarecht vor dem Grundgesetz ausgeschlossen sei. Angesprochen sind damit insbesondere strafrechtsbezogene rechtskulturelle Differenzen auf einer horizontalen Ebene zwischen den Mitgliedstaaten der Europäischen Union, deren strafrechtstheoretischer Unterbau sich zum Teil fundamental unterscheidet.[19] In den bundesverfassungsgerichtlichen Entscheidungen wird deutlich, dass der Schuldgrundsatz als Ausfluss der Menschenwürdegarantie zur Verfassungsidentität gehöre und bei Akten deutscher Hoheitsgewalt auch mit Blick auf Handlungen anderer Staaten stets gewahrt bleiben müsse.[20]

Die Vehemenz, mit der das BVerfG auf die Einhaltung verfassungsrechtlicher Vorgaben im Verhältnis zu anderen Mitgliedstaaten und der Europäischen Union pocht, steht materiell in einem gewissen Widerspruch zur Zurückhaltung, die es bei der Etablierung verfassungsrechtlicher Grenzen gegenüber deutschen Strafnormen in der Vergangenheit üb-

[9] BVerfGE 65, 1.

[10] Siehe zur Beschreibung von Entwicklungsphasen des Datenschutzes *Bodenschatz*, Der europäische Datenschutz, 2010, S. 31 ff.

[11] Siehe etwa BVerfGE 93, 181; BVerfGE 100, 313; BVerfGE 103, 21; BVerfGE 109, 279; BVerfGE 112, 304; BVerfGE 120, 274; BVerfGE 133, 277; BVerfGE 141, 220.

[12] *Classen*, EuR 2014, 441 (442); *Rusteberg*, VBlBW 2007, 171 (171 f.); zur Notwendigkeit einer nationalen datenschutzrechtlichen Vielfalt *Masing*, NJW 2012, 2305 (2310 f.).

[13] Siehe etwa Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995; Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates v. 12.7.2002; Rahmenbeschluss 2008/977/JI des Rates v. 27.11.2008 sowie aktuelle Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates v. 27.4.2016 und Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates v. 27.4.2016; zu Entwicklung und Inhalten siehe *Bodenschatz* (Fn. 10), S. 181 ff.

[14] Vgl. EuGH, Urt. v. 30.5.2006 – C-317, 318/04 (Parlament u.a. v. Rat und Kommission u.a.) = EuZW 2006, 403 (mit Anm. *Westphal*); EuGH, Urt. v. 8.4.2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd u.a.) = NJW 2014, 2169; EuGH, Urt. v. 21.12.2016 – C-203/15, C-698/15 (Tele2 Sverige) = NVwZ 2017, 1025.

[15] Vgl. etwa *Dannecker*, in: Ambos/Bock (Hrsg.), Aktuelle und grundsätzliche Fragen des Wirtschaftsstrafrechts – 6. Deutsch-Französische Strafrechtstagung, S. 115; *Landau/Trésoret*, DVBl 2012, 1329 (1330, 1336 f.); siehe hierzu auch *Kühling*, NVwZ 2014, 681 (684); *Westphal*, K&R 2014, 410 (411); *Wolff*, DöV 2014, 608 (609).

[16] Siehe allerdings zu den umfassenden europarechtlichen Einflüssen auf das Strafrecht *Dannecker* (Fn. 15).

[17] BVerfGE 123, 267 (413).

[18] BVerfGE 140, 317.

[19] *Bock*, ZIS 2019, 298 (303 ff.).

[20] Siehe insbesondere BVerfGE 140, 317.

te.[21] Zu konstatieren ist zudem, dass sich zwar der theoretisch-dogmatische Unterbau des Strafrechts vor allem mit Blick auf das Schuldprinzip in Strafrechtsordnungen der Mitgliedstaaten der Europäischen Union unterscheidet. Jedoch haben auch europäisch initiierte und geprägte strafrechtliche Neuregelungen in den letzten Jahren, insbesondere im Bereich des Terrorismus-, Computer- und Wirtschaftsstrafrechts, Veränderungen deutscher Strafnormen mit sich gebracht, die diese Unterschiede zum Teil nivellieren, aber dennoch – jedenfalls bisher – von Verfassung wegen in der Sache nicht beanstandet wurden. Hinzuweisen ist etwa auf die Vorverlagerung, z.B. durch Vorbereitungsstraftatbestände im Terrorismusstrafrecht, die einen eigenständigen Schuldgehalt kaum noch erkennen lassen,[22] und auf die Frage, wie sich das „Law in Books" rechtstatsächlich als „Law in Action" darstellt.[23] Die Überzeugung vom (stets) höheren Schutzniveau des Grundgesetzes gerät weiter ins Wanken, wenn der Blick über die reinen Grundsätze des Strafrechts hinaus erweitert wird. Werden etwa die gerichtlichen Vorgaben zur Sicherungsverwahrung,[24] zum Brechmitteleinsatz,[25] zur überlangen Verfahrensdauer eines Strafverfahrens[26] oder zum rechtsstaatswidrigen Einsatz eines agent provocateurs[27] betrachtet, so zeigt sich, dass insbesondere der Europäische Gerichtshof für Menschenrechte Schutzmaßstäbe setzt, die auf nationaler Ebene nur zögerlich anerkannt und umgesetzt werden.

Mit dem Bedeutungsgewinn von staatlichen Eingriffen zur Informationsbeschaffung gewinnt die Frage an Relevanz, wie es um die nationalen und europäischen datenschutzrechtlichen Schutzstandards und ihr Verständnis als Begrenzung sicherheitsrechtlicher Eingriffe bestellt ist. Mit Blick auf grundlegende Wertungen des Verhältnisses von Freiheit, Datenschutz und Sicherheit, deren jeweilige Bedeutung in den Rechtsordnungen der Mitgliedstaaten der Europäischen Union und im Unionsrecht selbst unterschiedlich gewichtet werden, können rechtskulturelle Prägungen Bedeutung erlangen. Diese können sich nicht nur auf einer horizontalen Ebene im Verhältnis der Mitgliedstaaten untereinander zeigen. Auch die Europäische Union und ihre Institutionen können bereichsbezogen eine rechtskulturelle Prägung erfahren und entwickeln, die von derjenigen in einzelnen Mitgliedstaaten abweicht. Mit dem unterschiedlichen Umgang des BVerfG und des EuGH mit den Regelungen zur Vorratsdatenspeicherung tut sich nunmehr ein weiteres strafrechtlich und übergreifend sicherheitsrechtlich relevantes Feld auf, in dem europäische Schutzstandards die deutschen zu übersteigen scheinen. Zu fragen ist, ob dies Ausdruck einer europäischen Sicherheits- und Datenschutzkultur ist, die sich grundlegend von dem deutschen Zugang unterscheidet und somit rechtskulturelle Differenzen auf einer vertikalen Ebene zwischen einem deutschen und europäischen Rechtsverständnis in den Entscheidungen der obersten Rechtsprechungsorgane offenbart.

III. Historie und Inhalt der Regelungen zur Vorratsdatenspeicherung

Die Rechtsprechung des BVerfG und des EuGH ist vor dem Hintergrund der Historie der Regelungen zur Vorratsdatenspeicherung zu bewerten, die alles andere als kontinuierlich und ohne Brüche verlief.

1. Entwicklung bis zur aktuellen deutschen Gesetzeslage

Wie viele Debatten um gesetzliche Sicherheitsregelungen bekam auch die Diskussion um die Vorratsdatenspeicherung, jedenfalls auf europäischer Ebene, Aufwind nach den terroristischen Anschlägen auf das World Trade Center im Jahr 2001 sowie weiteren Anschlägen in Madrid und London. Nachdem die Umsetzung eines Rahmenbeschlussentwurfs des Ministerrates zur Einführung der Vorratsdatenspeicherung in den Mitgliedstaaten der EG auf Grundlage der polizeilichen und justiziellen Zusammenarbeit[28] in Strafsachen aus dem Jahr 2004 scheiterte, wurde im Jahr 2006 die Richtlinie 2006/24/EG[29] erlassen.[30] Sie sah die Pflicht der Telekommunikationsdienstleister zur Vorratsdatenspeicherung von sechs bis zu 24 Monaten mit einer entsprechenden Verpflichtung der Mitgliedstaaten, die Speicherung der Daten sicherzustellen, vor.[31] Die deutsche Umsetzung erfolgte mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21. Dezember 2007 mit der Einführung der beschriebenen Speicherpflichten im Telekommunikationsge-

[21] Vgl. etwa *Lagodny*, Strafrecht vor den Schranken der Grundrechte, 1996, S. 51 ff.; *Roxin*, StV 2009, 544 (545); *Swoboda*, ZStW 122 (2010), 24 (25); *Sieber/Vogel*, Terrorismusfinanzierung, 2015, S. 134.

[22] Siehe nur *Puschke*, KriPoZ 2018, 101 ff.

[23] Beispielhaft hierzu die Ausführungen des BVerfG zum Vollzugsdefizit bzgl. der gesetzlichen Regelungen zur Verständigung im Strafprozess, BVerfGE 133, 168 (233 ff.); siehe auch *Mankowski* (Fn. 1), S. 373 ff.

[24] EGMR, Urt. v. 17.12.2009 – 19359/04 (M. v. Deutschland) = NJW 2010, 2495.

[25] EGMR, Urt. v. 11.7.2006 – 54810/00 (Jalloh v. Deutschland) = JuS 2007, 264 (mit Anm. *Dörr*).

[26] EGMR, Urt. v. 22.1.2009 – 45749, 51115/06 (Kaemena und Thöneböhn v. Deutschland) = StV 2009, 561 (mit Anm. *Krehl*).

[27] EGMR, Urt. v. 23.10.2014 – 54648/09 (Furcht v. Deutschland) = NJW 2015, 3631.

[28] Rat der Europäischen Union DOK. 8958/04.

[29] Richtlinie des Europäischen Parlaments und des Rates v. 15.3.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG.

[30] Siehe zur Historie auch *Gundel*, EuR 2009, 536; *Oehmichen/Mickler*, NZWiSt 2017, 298 f.; *Sandhu*, EuR 2017, 453 (454 f.); *Ziebarth*, ZUM 2017, 398; zur Entstehungsgeschichte der europäischen Richtlinie *Rusteberg*, VBlBW 2007, 171 (173 f.); zu ersten Bestrebungen im Deutschen Bundestag vgl. BT-Drs. 13/4438.

[31] Überblicksartig zum Inhalt der Richtlinie nur *Westphal*, EuZW 2006, 555.

setz, deren Dauer mit sechs Monaten am untersten Rand der Richtlinienvorgaben angesiedelt war, sowie den Regelungen zum Datenabruf zur Strafverfolgung in der StPO.[32] Dieses Umsetzungsgesetz wurde vom BVerfG im Jahr 2010 aufgrund einer von über 34.000 Personen unterstützten Klage für nichtig erklärt.[33] Im Jahr 2014 hatte sodann der EuGH die europäische Richtlinie für nicht mit der Grundrechtecharta vereinbar und ungültig erklärt.[34]

2. Aktuelle Gesetzeslage in Deutschland

Trotz dieser unübersichtlichen Rechtslage und dem Wegfall einer europäischen Verpflichtung für eine nationale Regelung der Vorratsdatenspeicherung aufgrund der Rechtsprechung des EuGH wurde in Deutschland ein neues Gesetz eingeführt, das den Vorgaben des BVerfG entsprechen sollte und im Jahr 2015 in Kraft trat.[35] Es verpflichtete die Telekommunikationsunternehmen erneut zur Speicherung bestimmter Verkehrsdaten ab dem 1. Juli 2017. Diese Pflicht gilt unabhängig davon, ob die Speicherung der Daten für eigene Zwecke der Dienstleister erforderlich ist. Zudem gilt die Pflicht anlasslos, d.h. die Daten müssen unabhängig von einer bestimmten Gefährdungslage oder begangenen Straftaten gespeichert werden und betreffen nahezu alle Personen, die sich öffentlicher Telekommunikation bedienen. Ziel der Regelung ist es, die Verkehrsdaten zu sichern, um bei einem späteren Anlass, etwa zur Aufklärung einer Straftat, rückwirkend hierauf zurückgreifen zu können.

Dementsprechend verlangt § 113b TKG, dass die Kennungen, also vornehmlich die Rufnummern, von Anrufendem und Angerufenem bei Telefonaten ebenso wie der Zeitpunkt und die Dauer des Telefonates erfasst werden. Gleichermaßen sind bei SMS- und MMS-Nachrichten Sende- und Empfangsdaten zu speichern. Bei der Internetnutzung sind die jeweils zugewiesenen IP-Adressen ebenso wie Dauer und Zeitpunkt der Internetnutzung zu erfassen. Diese Daten sind für zehn Wochen zu speichern. Jeweils zu Beginn der Nutzung mobiler Telefon- und Internetdienste werden darüber hinaus auch die Funkzellenangaben und damit Standortdaten des Mobiltelefons für vier Wochen gespeichert. Explizit ausgenommen sind nach § 113b Abs. 5 TKG Inhalte der Kommunikation, also was gesprochen oder geschrieben wurde. Im Kern handelt es sich bei den relevanten Daten folglich um solche, die einen Einblick dahingehend ermöglichen, wann wer mit wem von wo aus und wie lange in welcher Form via Telekommunikation in Kontakt getreten ist.

Die Speicherungspflichten werden ergänzt durch gesetzliche Regelungen zum Zugriff auf die gespeicherten Daten. So regelt § 100g Abs. 2 und 3 StPO, dass bei einem Tatverdacht hinsichtlich einer besonders schweren Straftat die gem. § 113b TKG gespeicherten Daten erhoben werden dürfen, wenn dies für die Strafverfolgung erforderlich ist. § 100j Abs. 2 StPO ermöglicht einen Rückgriff auf die Verkehrsdaten zur Bestandsdatenauskunft. Weitere Zugriffsregelungen befinden sich in Gesetzen zur Gefahrenabwehr sowie im bayerischen Verfassungsschutzgesetz (Art. 15 Abs. 3).

3. Nachfolgende rechtliche Entwicklungen

Im Jahr 2016 entschied der EuGH, dass die nationalen Regelungen zur Vorratsdatenspeicherung in Großbritannien und Schweden nicht mit Unionsrecht vereinbar seien.[36] Für das nunmehr neue deutsche Recht schloss sich das OVG Münster dieser Betrachtung in der Sache an, woraufhin die verantwortliche Bundesnetzagentur die Verpflichtung zur Vorratsdatenspeicherung aussetzte.[37] Das Ergebnis dieser Odyssee für Deutschland ist nun, dass die beschriebenen gesetzlichen Regeln zwar bestehen, sich hieraus aber keine Rechtspflichten für die Telekommunikationsdienstleister ergeben.

Zurzeit sind mehrere Verfassungsbeschwerden gegen die bestehende gesetzliche Regelung in Deutschland beim BVerfG anhängig.[38] Eine Entscheidung in der Hauptsache steht noch aus. Allerdings hob das BVerfG in einer ablehnenden Entscheidung bzgl. einer einstweiligen Anordnung nach dem Urteil des EuGH aus dem Jahr 2016 bereits die Bedeutung der europäischen Rechtsprechung hervor.[39]

IV. Die Urteile des BVerfG und des EuGH

1. Inhaltliche Kernkriterien der Entscheidungen

Die aktuelle Rechtslage in Deutschland ist geprägt durch die Entscheidungen des BVerfG und des EuGH sowie durch das Bestreben des deutschen Gesetzgebers, die Vorratsdatenspeicherung national zu regeln.

a) BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08 u.a.

Die Entscheidung des BVerfG aus dem Jahr 2010, in der es das damalige deutsche Umsetzungsgesetz zur Vorratsdatenspeicherung aufgrund eines Verstoßes gegen das Grundgesetz

[32] BGBl. I 2007, S. 3198.
[33] BVerfGE 125, 260.
[34] EuGH, Urt. v. 8.4.2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd u.a.) = NJW 2014, 2169.
[35] BGBl. I 2015, S. 2218.
[36] EuGH, Urt. v. 21.12.2016 – C-203/15, C-698/15 (Tele2 Sverige) = NVwZ 2017, 1025.
[37] Vgl. Bundesnetzagentur, Verkehrsdatenspeicherung, Mitteilung zur Speicherverpflichtung nach § 113b TKG; siehe auch *Graf*, in: Graf (Hrsg.), Beck'scher Online-Kommentar, Strafprozessordnung, Stand: 1.1.2019, § 100a Rn. 220; vgl. auch VG Köln, Urt. v. 20.4.2018 – 9 K 7417/17.
[38] Siehe zu den Eilanträgen BVerfG, Beschl. v. 8.6.2016 – 1 BvQ 42/15 = NVwZ 2016, 1240; BVerfG, Beschl. v. 8.6.2016 – 1 BvR 229/16 = ZD 2016, 433; BVerfG, Beschl. v. 26.3.2017 – 1 BvR 141/16 = BeckRS 2017, 106846.
[39] BVerfG, Beschl. v. 26.3.2017 – 1 BvR 141/16 = BeckRS 2017, 106846 Rn. 1; siehe auch *Gola/Klug*, NJW 2018, 2608 (2609). In den vorausgehenden Eilentscheidungen (BVerfG, Beschl. v. 8.6.2016 – 1 BvQ 42/15, Rn. 18; BVerfG, Beschl. v. 8.6.2016 – 1 BvR 229/16, Rn. 19) wurde dabei allerdings, wie in der Entscheidung des BVerfG aus dem Jahr 2010, die Regelungen zum Abruf der Daten als entscheidend für die Eingriffstiefe benannt und nicht maßgeblich auf die Ausgestaltung der Speicherung als solche abgestellt, wie es der EuGH vornehmlich tat.

für nichtig erklärte, fußt materiell vornehmlich auf folgenden Erwägungen:

Bereits die Speicherung und nicht erst der Abruf der Daten stelle einen Eingriff in das Fernmeldegeheimnis des Art. 10 GG dar.[40] Dieser Eingriff sei zudem besonders schwerwiegend, was das BVerfG vornehmlich damit begründet, dass die Speicherung anlasslos und umfassend erfolge und sensible Daten betreffe, die Rückschlüsse auf die Privat- bzw. sogar Intimsphäre zuließen.

> „Die Aussagekraft dieser Daten ist weitreichend. Je nach Nutzung von Telekommunikationsdiensten seitens der Betroffenen lassen sich schon aus den Daten selbst – und erst recht, wenn diese als Anknüpfungspunkte für weitere Ermittlungen dienen – tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten eines jeden Bürgers gewinnen. [...] Auch aus diesen Daten lassen sich jedoch bei umfassender und automatisierter Auswertung bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen. Adressaten (deren Zugehörigkeit zu bestimmten Berufsgruppen, Institutionen oder Interessenverbänden oder die von ihnen angebotenen Leistungen), Daten, Uhrzeit und Ort von Telefongesprächen erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen derjenigen, deren Verbindungsdaten ausgewertet werden.“[41]

Zur Begründung der besonderen Eingriffstiefe stellt es zudem auf den sog. „chilling effect“, also Abschreckungseffekt, ab, wonach Bürgerinnen und Bürger durch verdeckte Überwachung von der Ausübung ihrer Grundrechte abgehalten werden können.

> „Besonderes Gewicht bekommt die Speicherung der Telekommunikationsdaten weiterhin dadurch, dass sie selbst und die vorgesehene Verwendung der gespeicherten Daten von den Betroffenen unmittelbar nicht bemerkt werden, zugleich aber Verbindungen erfassen, die unter Vertraulichkeitserwartungen aufgenommen werden. Hierdurch ist die anlasslose Speicherung von Telekommunikationsverkehrsdaten geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann.“[42]

Die damalige deutsche Regelung könne einen derart tiefgehenden Eingriff nicht rechtfertigen, so das BVerfG, da weder die Datensicherheit hinreichend sichergestellt[43] noch der Abruf der Daten auf die Bekämpfung schwerer Straftaten beschränkt sei.[44] Zudem wurden weitere Vorgaben zur Löschung und Kennzeichnung der Daten, zum Schutz von Vertrauensbeziehungen, zur Transparenz der Abfrage und zum Rechtsschutz postuliert.[45]

b) EuGH, Urt. v. 8.4.2014 – C-293/12, C-594/12, und EuGH, Urt. v. 21.12.2016 – C-203/15, C-698/15

Die vier bzw. sechs Jahre später ergangenen Entscheidungen des EuGH über die Ungültigkeit der Richtlinie selbst und über die Unionsrechtswidrigkeit der britischen und schwedischen Regelungen zur Vorratsdatenspeicherung basieren weitgehend auf den gleichen materiellen Prämissen wie die Entscheidung des BVerfG und kamen auch in großen Teilen zu vergleichbaren Ergebnissen.

So führt der EuGH im Rahmen der Verhältnismäßigkeitsprüfung und mit Blick auf das Grundrecht auf Achtung des Privat- und Familienlebens gem. Art. 7 und den Schutz personenbezogener Daten gem. Art. 8 der Charta der Grundrechte der Europäischen Union aus, dass bereits der Eingriff durch die breit gestreute Speicherung besonders schwer wiege und aus den gespeicherten Daten genauso sensible Informationen abgeleitet werden könnten wie aus dem Inhalt der Kommunikationen selbst. Nahezu inhaltsgleich mit den Ausführungen des BVerfG wird dargelegt:

> „Die Daten, die somit von den Betreibern elektronischer Kommunikationsdienste auf Vorrat zu speichern sind, ermöglichen die Rückverfolgung und Identifizierung der Quelle und des Adressaten einer Nachricht sowie die Bestimmung von Datum, Uhrzeit, Dauer und Art einer Nachrichtenübermittlung, der Endeinrichtung von Benutzern und des Standorts mobiler Geräte. […] Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren.“[46]

Mit Verweis auf die Freiheit der Meinungsäußerung und Informationsfreiheit gem. Art. 11 GRCh bedient sich der EuGH ebenso wie zuvor das BVerfG des Arguments des „chilling effects“:

> „Der Umstand, dass die Vorratsspeicherung der Daten vorgenommen wird, ohne dass die Nutzer der elektronischen Kommunikationsdienste darüber informiert werden, ist geeignet, bei den Betroffenen das Gefühl zu erzeugen,

[40] BVerfGE 125, 260 (318); wobei sich die Maßgaben des BVerfG zum Recht auf informationelle Selbstbestimmung weitgehend auf Art. 10 GG übertragen lassen (siehe auch BVerfGE 100, 313 [359]).
[41] BVerfGE 125, 260 (319).
[42] BVerfGE 125, 260 (320).
[43] BVerfGE 125, 260 (325 ff.).
[44] BVerfGE 125, 260 (328 f.).
[45] BVerfGE 125, 260 (332 ff.).
[46] EuGH, Urt. v. 21.12.2016 – C-203/15, C-698/15 (Tele2 Sverige), Rn. 98 f.; vgl. auch bereits EuGH, Urt. v. 8.4.2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd u.a.), Rn. 26 f.

> dass ihr Privatleben Gegenstand einer ständigen Überwachung ist."[47]

Die Anlasslosigkeit der Speicherung, die nicht hinreichend beschränkten Zugriffsmöglichkeiten der öffentlichen Behörden und zu geringe Anforderungen an die Datensicherheit[48] führen also auch nach dem EuGH im Ergebnis dazu, dass die Regelungen nicht verhältnismäßig und unionsrechtswidrig sind.

Anders als das BVerfG betont der EuGH aber die Notwendigkeit, dass die Pflicht zur Speicherung als solche auf das absolut notwendige Maß zu beschränken sei. Während das BVerfG die eigenständige, besonders hohe Eingriffsqualität der Speicherung zwar anerkennt, sie aber vornehmlich durch strikte Vorgaben für den Abruf der Daten als hinreichend beschränkbar ansieht, genügt dies dem EuGH nicht. Er führt in seinem Urteil aus dem Jahr 2016 aus:

> „Eine solche Regelung [Anm. des *Verf.*: Vorgaben zur Vorratsdatenspeicherung in Schweden und Großbritannien] verlangt keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit. Insbesondere beschränkt sie die Vorratsspeicherung weder auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung von Straftaten beitragen könnten […]. Eine nationale Regelung wie die im Ausgangsverfahren in Rede stehende überschreitet somit die Grenzen des absolut Notwendigen und kann nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden."[49]

Wenngleich sowohl das BVerfG als auch der EuGH die Möglichkeit einer Regelung zur Vorratsspeicherung zumindest formal nicht vollständig ausgeschlossen haben, führen die aufgestellten materiellen Kriterien des EuGH dazu, dass eine vollständig anlasslose Speicherung nicht mit den unionsrechtlichen Vorgaben in Einklang zu bringen ist. Allenfalls eine Vorratsdatenspeicherung „light" wäre somit noch denkbar. Die aufgestellten Voraussetzungen erfüllt auch die neue deutsche Regelung nicht,[50] die trotz der weitgehenden Umsetzung der vom BVerfG eingeforderten Beschränkungen[51] weiterhin die Speicherung von Verkehrsdaten ohne Bezug zu einer aktuellen Sicherheitslage verlangt.

2. Bewertung der Entscheidungsinhalte

Sowohl dem Urteil des BVerfG als auch den Urteilen des EuGH liegt ein Verständnis des Ausgleichs von Freiheitsbelangen auf der einen Seite und Fragen der Sicherheit auf der anderen Seite zugrunde. Dabei spielt der Verhältnismäßigkeitsgrundsatz zum Austarieren dieser Interessen die entscheidende Rolle, wobei sich beide Gerichte auf die Angemessenheitsprüfung in einem deutschen Dogmatikverständnis konzentrieren, wenngleich der EuGH diese Prüfung hier formal auf der Ebene der Erforderlichkeit vornimmt.[52]

An diesem zügigen Hinweggehen über die Geeignetheit der Vorratsdatenspeicherung als Mittel zur Strafverfolgungsvorsorge und insbesondere der Annahme, dass sie hierfür das relativ mildeste Mittel darstellt,[53] kann Kritik geübt werden, die die Entscheidungen beider Gerichte betrifft. Während für Deutschland vor allem das Bundeskriminalamt die unbedingte Notwendigkeit der Datenspeicherung betont, legen wissenschaftliche empirische Erhebungen nahe, dass der Vorratsdatenspeicherung allenfalls eine sehr eingeschränkte Bedeutung bei der Strafverfolgung zukommt. So zeichnet eine Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht in Freiburg (MPI), die Veränderungen bei der Strafverfolgung während und nach dem Bestehen der Speicherpflicht in Deutschland untersuchte, ein eher pessimistisches Bild von der Effektivität der Vorratsdatenspeicherung, wobei allerdings darauf hingewiesen wird, dass die statistische Datengrundlage noch sehr unsicher sei.[54] Es gebe keine belastbaren Hinweise darauf, dass Schutzmöglichkeiten durch den Wegfall der Vorratsdatenspeicherung reduziert worden wären. Auch seien Veränderungen in den Aufklärungsraten nicht sichtbar geworden. Zudem ist zu beachten, dass die zu einer effektiven Strafverfolgung notwendige eingehende Auswertung der Daten ressourcenintensiv sein kann und jedenfalls für bestimmte Deliktsbereiche noch andere Ermittlungsmaßnahmen zur Verfügung stehen. Dennoch ist den Gerichten im Ergebnis dahingehend zuzustimmen, dass die Beurteilung der Geeignetheit und Erforderlichkeit der Maßnahme von der Entscheidungsprärogative des Gesetzgebers als gedeckt anzusehen ist. Aus rechtlicher Sicht entscheidend für die Bewertung der Rechtmäßigkeit einer Vorratsdatenspeicherung ist somit die Frage, ob sich die Beschränkungen der Privatheit der Bevölkerung und des Datenschutzes als angemessen darstellen.

[47] EuGH, Urt. v. 21.12.2016 – C-203/15, C-698/15 (Tele2 Sverige), Rn. 100; vgl. auch bereits EuGH, Urt. v. 8.4.2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd u.a.), Rn. 28.

[48] EuGH, Urt. v. 8.4.2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd u.a.), Rn. 56 ff.; EuGH, Urt. v. 21.12.2016 – C-203/15, C-698/15 (Tele2 Sverige), Rn. 97 ff.

[49] EuGH, Urt. v. 21.12.2016 – C-203/15, C-698/15 (Tele2 Sverige), Rn. 106 f.

[50] *Oehmichen/Mickler*, NZWiSt 2017, 298 (306 f.); *Roßnagel*, NJW 2017, 696 (698); *Ziebarth*, ZUM 2017, 398 (404 ff.); offener *Derksen*, NVwZ 2017, 1005 (1009); *Sandhu*, EuR 2017, 453 (468 f.); *Wollenschläger*, NJW 2018, 2532 (2535).

[51] Siehe aber zu einer Kritik an fehlenden Speicherungsbeschränkungen für die Kommunikation mit beruflichen Vertrauenspersonen *Oehmichen/Mickler*, NZWiSt 2017, 298 (304).

[52] *Classen*, EuR 2014, 441 (444).

[53] BVerfGE 125, 260 (317 f.); EuGH, Urt. v. 8.4.2014 – C-293/12, C-594/12 (Digital Rights Ireland Ltd u.a.), Rn. 49 f.

[54] MPI, Schutzlücken durch Wegfall der Vorratsdatenspeicherung?, 2011, S. 218.

Hinsichtlich der Verhältnismäßigkeit im engeren Sinne verdeutlichen beide Gerichte die besondere Eingriffstiefe, die in einer anlasslosen Speicherung von Verkehrsdaten der Telekommunikation liegt, die nunmehr auch weitgehend anerkannt zu sein scheint.[55] Auch der argumentative Rückgriff auf den „chilling effect", der insbesondere aus dem Volkszählungsurteil bekannt ist,[56] weist Plausibilität auf,[57] müsste aber durch bereichsspezifische empirische Analysen untermauert werden.[58] Dem Befund des tiefgehenden Eingriffs entsprechend werden von beiden Gerichten hohe Anforderungen an beschränkende Regelungen zur Datensicherheit, zum Abruf der Daten und zu Transparenzanforderungen aufgestellt. Diese von den Gerichten aufgezeigten Beschränkungen der Speicherung von Telekommunikationsverkehrsdaten auf Vorrat und deren Abrufs können überzeugen und messen der Privatheit, der informationellen Selbstbestimmung und dem Datenschutz einen hohen Stellenwert bei.

Im Grundsatz ebenfalls begrüßenswert sind die Beschränkungen einer Vorratsdatenspeicherung durch den EuGH, soweit sie über die Vorgaben des BVerfG hinausgehen.[59] Mit Blick auf den Eingriffscharakter der Speicherung als solcher muss jede einzelne Form der Datenverarbeitung der Verhältnismäßigkeitsprüfung standhalten. So ist die umfassende Speicherung sensibler Daten nur tolerabel, wenn sie auf das absolut notwendige Maß beschränkt wird. Zwar spielt für die Abwägung der Eingriffstiefe durch die Speicherung selbst mit bestehenden Sicherheitsinteressen auch eine entscheidende Rolle, unter welchen Voraussetzungen die gespeicherten Daten abgerufen werden können. Eine hohe Zugriffsschwelle und weitere Regelungen zur Datensicherheit und zur Transparenz der Datenverwendung rechtfertigen die Speicherung aller verfügbaren Daten allerdings nicht. Diese Beschränkungen können die Anlasslosigkeit der Speicherung nicht kompensieren. Der Zweck der Speicherung kann nur dann eine hinreichend beschränkende Wirkung entfalten, wenn er auch hinsichtlich des Umfangs und der Tiefe der Verpflichtung zur Datenerfassung als Abwägungskriterium einfließt und so den Zusammenhang zwischen der Datenspeicherung und einer Bedrohung der öffentlichen Sicherheit herstellt.[60]

Problematisch ist jedoch die Annahme des EuGH, dass der notwendige Zusammenhang zwischen dem Eingriff durch die Speicherung und der Bedrohungslage durch Begrenzungen der Speicherung von Daten hinsichtlich eines bestimmten Zeitraums, eines geografischen Gebietes oder eines bestimmten Personenkreises[61] in grundrechtskonformer Weise erfolgen könne. Die aufgezeigten Kriterien sind weit im Vorfeld einer konkreten Gefahr oder eines Tatverdachtes angesiedelt und weisen eine erhebliche Streubreite auf. Sie verlieren sich daher in vagen Gefährlichkeitsprognosen, die einer rechtlich nachprüfbaren Objektivierung nur schwer zugänglich sind und betroffene Personen erheblichen Diskriminierungsrisiken aussetzen würden.[62]

3. Unterschiede in den Entscheidungen als Ausdruck rechtskultureller Differenzen?

Es hat sich gezeigt, dass neben vergleichbaren Erwägungen auch beachtliche rechtliche Differenzen in der Rechtsprechung des BVerfG und des EuGH in Bezug auf die Grenzen einer Vorratsdatenspeicherung bestehen. Diese Differenzen sind folgenträchtig. Während das BVerfG eine Speicherung von Verkehrsdaten der Telekommunikation unter engen Bedingungen grundsätzlich zulässt, ist dem Gesetzgeber nach der Entscheidung des EuGH eine Vorratsdatenspeicherung, die vollständig von jedem aktualisierten Anlass gelöst ist, verwehrt.

a) Gewachsene inhaltliche Grundprämissen

Trotz dieser beträchtlichen Unterschiede in den Auswirkungen handelt es sich nicht um Entscheidungen, die auf inhaltsbezogene rechtskulturelle Differenzen zurückzuführen sind. Die Grenzen einer Vorratsdatenspeicherung betreffen, anders als das strafrechtliche Schuldprinzip, nicht kulturelle oder verfassungsrechtliche Identitäten[63] und Besonderheiten der Mitgliedstaaten. Sie entspringen nicht unmittelbar historisch über Jahrhunderte gewachsenen und vornehmlich national

[55] Einschränkend demgegenüber die abw. Meinungen der Richter Schluckebier, BVerfGE 125, 260 (365 ff.), und Eichberger, BVerfGE 125, 260 (380).

[56] BVerfGE 65, 1 (43).

[57] So auch *Marsch*, in: Hascher/Jung/Paris/Schulze (Hrsg.), Sicherheit und Freiheit, 2018, S. 77 (82); zur Kritik an der Begründung dieser überindividuellen Grundrechtsdimension allerdings Schluckebier, BVerfGE 125, 260 (365 ff.), und Eichberger, BVerfGE 125, 260 (380 f.); vgl. auch *Dreier*, in: Dreier (Hrsg.), Grundgesetz, Kommentar, Bd. 1., 3. Aufl. 2013, Art. 2 I Rn. 87.

[58] Zu allgemeinen sozialwissenschaftlichen Bestätigungstendenzen *Penney*, Berkeley Technology Law Journal 31 (2016), 117.

[59] Kritisch demgegenüber etwa *Kühling/Drechsler*, NJW 2017, 2950 (2955); *Sandhu*, EuR 2017, 453 (462 ff.); *Wolff*, DöV 2014, 608 (611).

[60] EuGH, Urt. v. 21.12.2016 – C-203/15, C-698/15 (Tele2 Sverige), Rn. 109 ff.; zur Kritik an „zweckentfernten" Eingriffen *Puschke* (Fn. 2), S. 707 ff.

[61] EuGH, Urt. v. 21.12.2016 – C-203/15, C-698/15 (Tele2 Sverige), Rn. 111. Diese Kriterien weisen eine gewisse Nähe zur deutschen Rechtsprechung zur Relevanz bestimmter Bedrohungsszenarien als Eingriffsvoraussetzungen auf, vgl. BVerwG, NVwZ 2017, 1057 (1060); BVerfG NVwZ 2017, 1526 (1529).

[62] Siehe auch *Sandhu*, EuR 2017, 453 (463); siehe beispielhaft den Verweis auf die Überwachung für „Araber bzw. Nordafrikaner" bei *Frenz*, DVBl 2017, 183 (185); von einer nichtdiskriminierenden Ausgestaltungsmöglichkeit ausgehend *Ziebarth*, ZUM 2017, 398 (403); skeptisch demgegenüber *Priebe*, EuZW 2017, 136 (139); vgl. insgesamt zudem *Puschke* (Fn. 2), S. 708 ff.

[63] Jedenfalls soweit sie keine Totalüberwachung begründen, siehe hierzu BVerfGE 125, 260 (324).

geprägten Vorstellungen, die sich einseitig auf Ebene der Europäischen Union verfestigt haben. Vielmehr handelt es sich um ein Themengebiet, das sich mit Blick auf die technische Entwicklung in den vergangenen Jahrzehnten europaweit auf ähnlicher Grundlage und durch gegenseitige Beeinflussung entwickelt hat. Der gemeinsam durchgeführte gesellschaftliche und rechtliche Prozess hinsichtlich des Umgangs mit Daten in der sog. Informationsgesellschaft und der demokratiekonstitutiven Bedeutung des Datenschutzes[64] hat innerhalb der Europäischen Union und ihrer Mitgliedstaaten im Kern gemeinsame Bewertungskriterien entstehen lassen. In der Sache geht es bei den Entscheidungen nicht um grundsätzliche Unterschiede oder Charakteristika eines deutschen und europäischen Datenschutzes.[65] Vielmehr werden anerkannte Argumente verhandelt und gesetzt. Dies zeigt sich auch an den den Entscheidungen zugrundeliegenden Prämissen, die weitgehend vom BVerfG aufgestellt und vom EuGH und von den Generalanwälten rezipiert wurden.[66] Dass aus diesen im Einzelnen unterschiedliche Ergebnisse abgeleitet werden können, ist ein wenig überraschender Befund. In dieser Hinsicht sprechen im Ergebnis auch die Entscheidungen zur Unzulässigkeit der Vorratsdatenspeicherungsgesetze in Belgien, Bulgarien, Österreich, Rumänien, Tschechien und Zypern gegen nationalstaatliche Sonderwege.[67] Auch das BVerfG hätte im Jahre 2010 zu einem entsprechenden Ergebnis gelangen können. Angesichts der starken Betonung des Datenschutzes in der rechtlichen Diskussion in Deutschland mit dem weltweit ersten Datenschutzgesetz aus dem Jahr 1970 in Hessen und dem wegweisenden Volkszählungsurteil des BVerfG aus dem Jahr 1983 sowie dem Rückgriff auf die überindividuelle Grundrechtsdimension des „chilling effect" hätte die Untersagung einer anlasslosen, strukturellen Speicherung von Verkehrsdaten nicht ferngelegen. In gleicher Weise war es vor der Entscheidung des EuGH aus dem Jahr 2014 keineswegs ausgemacht, dass aus Art. 7 und Art. 8 GRCh die Unzulässigkeit einer anlasslosen Speicherung der Telekommunikationsverkehrsdaten abgeleitet wird.

b) Die Bedeutung gerichtlicher Zuständigkeiten und Entscheidungskompetenzen

Institutionalisierte rechtskulturelle Differenzen können demgegenüber in den Begründungen der gerichtlichen Zuständigkeiten und Entscheidungskompetenzen erblickt werden, die sich insgesamt im Fluss befinden.[68] Insofern treffen bundesverfassungsgerichtliche Beharrungstendenzen und die Ausdehnung des eigenen Rechtsprechungskompetenzbereichs durch den EuGH – nicht zuletzt über den Anwendungsbereich von Unionsgrundrechten – aufeinander.[69]

So musste das BVerfG, um die Entscheidung über das nationale Gesetz zur Umsetzung von europäischem Recht überhaupt treffen zu können, annehmen, dass die durch die Richtlinie vorgegebene Verpflichtung der nationalen Gesetzgeber, eine Mindestspeicherungsdauer von sechs Monaten sicherzustellen, noch den Anforderungen des Art. 10 GG entsprechen würde, eine verfassungsrechtlich nicht zu beanstandende Umsetzung der Richtlinie somit grundsätzlich möglich sei.[70] Entsprechend hat das BVerfG auch keinen Anlass für ein Vorabentscheidungsverfahren vor dem EuGH gem. Art. 267 AEUV gesehen. Die Wirksamkeit der europäischen Richtlinie als solche wurde nicht als entscheidungserheblich angesehen, da die Richtlinie, insbesondere auch hinsichtlich der Regelungen zum Abruf der Daten durch nationale Strafverfolgungsbehörden, einen hinreichenden Spielraum zur verfassungskonformen Umsetzung belasse. Hieraus ergab sich möglicherweise bereits die Tendenz, den Schwerpunkt auf die Prüfung der Regelungen zum Abruf zu legen, die das BVerfG allein als Sache des nationalen Gesetzgebers und damit vollumfänglich als überprüfbar ansah. Ein Vorgehen, das sowohl hinsichtlich der Erzeugung eines unionsrechtswidrigen Zustandes durch die vollständige Nichtigkeitserklärung als auch bzgl. des Verzichtes auf eine Vorlage an den EuGH kritisch gesehen wird.[71]

Der EuGH wiederum begründete den Anwendungsbereich des Unionsrechts damit, dass die geprüften nationalen Regelungen nunmehr in den Geltungsbereich der sog. E-Privacy-Richtlinie[72] fielen. Art. 15 Abs. 1 dieser RL sieht die Möglichkeit vor, dass Mitgliedstaaten Ausnahmen von den Löschungspflichten für Verkehrsdaten regeln dürfen, die als Durchführung von Unionsrecht i.S.d. Art. 51 Abs. 1 S. 1 GRCh gewertet werden. Wenngleich der EuGH auch die

[64] *Westphal*, EuZW 2006, 555 (560); *Hefendehl*, JZ 2009, 165 (173).

[65] Diese Kriterien werden als bedeutsam für Rechtskulturen angesehen von *Mankowski* (Fn. 1), S. 2.

[66] *Classen*, EuR 2014, 441 (443); *Marsch* (Fn. 57), S. 81, 83.

[67] Verfassungsgerichtshof Brüssel, Entscheidung v. 11.6.2016 –84/2015; Oberstes Verwaltungsgericht Bulgariens, Entscheidung v. 11.12.2008 – 13627; Verfassungsgerichtshof Österreichs, Entscheidung v. 27.6.2014 – G 47/2012, G 59/2012, G 62/2012, G 70/2012, G 71/2012; Verfassungsgericht Rumäniens, Entscheidung v. 8.10.2009 – 1258; Verfassungsgericht Tschechiens, Urt. v. 22.3.2011 – Pl. ÚS 24/10; Oberster Gerichtshof Zyperns in den Beschwerdesachen, Entscheidung v. 1.2.2011 – 65/2009, 78/2009, 82/2009 und 15/2010-22/2010; siehe auch *Bäcker*, JA 2014, 1263 (1265).

[68] *Kingreen*, JZ 2013, 801 (810), spricht von tektonischen Verschiebungen.

[69] Offenkundige Disharmonie ergibt sich vor allem aus den Entscheidungen EuGH, Urt. v. 26.2.2013 – C-617/10 (Åklagare v. Åkerberg Fransson) = JZ 2013, 613 (mit Anm. *Dannecker*), und BVerfGE 133, 277; zur Antiterrordatei vgl. etwa *Derksen*, NVwZ 2017, 1005; *Gärditz*, GSZ 2017, 1 (5); *Kingreen*, JZ 2013, 801 (802); *Schiedermair/Mrozek*, DÖV 2016, 89 (93); zum Ringen um Deutungshoheit auch *Nußberger*, JZ 2018, 845 (852); konkret zu Fehlleistungen des BVerfG bzgl. der Vorratsdatenspeicherung *Giegerich*, ZEuS 2014, 3 (14 ff.); *Hornung/Schnabel*, DVBl 2010, 824 (828 f.).

[70] BVerfGE 125, 260.

[71] Vgl. etwa *Bäcker*, EuR 2011, 103 (114 ff.); *Giegerich*, ZEuS 2014, 3 (14 ff.); *Kingreen*, JZ 2013, 801 (809 f.); das Vorgehen als „Kniff" bezeichnend *Marsch* (Fn. 57), S. 81.

[72] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates v. 12.7.2002.

Regelungen zur Abfrage der Daten hierunter fasst, so bezieht sich diese Ausnahmeregelung primär auf die Speicherpflicht selbst.[73] Diese Auslegung der Richtlinie ist freilich umstritten.[74] Durch den Rückgriff auf Art. 15 der E-Privacy-Richtlinie tritt der Ausnahmecharakter für die Speicherung stärker hervor, als das bei der mehr auf eine Gesamtabwägung angelegten Prüfung anhand des Art. 10 GG der Fall ist. Auch das Datenschutzgrundrecht des Art. 8 GRCh als Maßstab für die EuGH-Rechtsprechung, das so kein Äquivalent im deutschen Grundgesetz hat, verdeutlicht die strikte Bindung jedes einzelnen Datenverarbeitungsvorgangs an den Zweck der Maßnahme und legt eine Beschränkung der Speicherungspflichten nahe.

V. Fazit und Ausblick

Die Historie europäischer und nationaler Vorgaben zur Vorratsdatenspeicherung ist ein Beispiel dafür, wie die Ausprägung eines im Ergebnis begrüßenswerten hohen Grundrechtsschutzes nicht erfolgen sollte. Europäische und nationale Alleingänge, das Ausreizen des als rechtlich möglich Angesehenen durch die Gesetzgebung und divergierende Gerichtsentscheidungen führen zu Rechtsunsicherheit und Rechtsverdruss.[75] Der Angleichung rechtlicher Kriterien des Grundrechts- und Datenschutzes, soweit sie möglich und nötig ist, müssen sich gerade die Gerichte verpflichtet fühlen. Die nationalen Gerichte, allen voran das BVerfG, können auf diese Weise die europäische Gesamtrechtsordnung mitgestalten,[76] die Herausbildung einer gesamteuropäischen Rechtskultur befördern und rechtliche und rechtskulturelle Differenzen zu beseitigen helfen, wo es sie zu beseitigen gilt. Hierzu müssen die bestehenden Dialogmöglichkeiten zwischen den nationalen Gerichten und dem EuGH möglichst umfassend genutzt werden.[77] Obwohl im Ergebnis ein Großteil der rechtlichen Erwägungen des BVerfG über die Bande gespielt[78] und ohne explizite Bezugnahme[79] in die Entscheidungen des EuGH eingeflossen sind, hätte sich die entstandene Rechtsunsicherheit vermeiden oder jedenfalls reduzieren lassen, wenn das BVerfG bereits im Jahr 2010 die Frage der Vorratsdatenspeicherung dem EuGH vorgelegt hätte.[80]

Für den Bereich des Datenschutzes hat der EuGH auf materieller Ebene nunmehr „geliefert" und beachtliche Schutzstandards gesetzt.[81] Mit Blick auf die beim BVerfG anhängigen Verfahren gegen die deutsche Neuregelung zur Vorratsdatenspeicherung kann der Schritt des Dialoges durch Vorlage nun nachgeholt werden. Angesichts der nach wie vor nicht eindeutigen Rechtslage wäre ein solches Vorgehen folgerichtig,[82] wenngleich es mit erheblichem Zeitaufwand bis zu einer abschließenden Entscheidung verbunden wäre.[83]

Für zukünftige Gesetzesvorhaben müssen europäische Grundrechtsstandards und das Datenschutzrecht ernstgenommen werden, woraus sich nunmehr auch Grenzen für das nationale Sicherheitsrechts ergeben. Dabei sollten Sicherheits- und Datenschutzrecht nicht als parallellaufende Rechtsmaterien verstanden werden, die sich lediglich gegenseitig begrenzen. Vielmehr erscheint es notwendig, die Materien bereits im Rahmen der Gesetzgebung als Einheit zu begreifen und die datenschutzrechtlichen Vorgaben schon beim Gegenstand der Sicherheitsgesetzgebung zu berücksichtigen. Für die Vorratsdatenspeicherung dürfte dies das Aus bedeuten,[84] will sich die Legislative nicht erneut in den Graubereich des Vielleicht-rechtlich-gerade-noch-Möglichen begeben und wiederum Rechtsunsicherheit schaffen.[85] Werden die von der

[73] EuGH, Urt. v. 21.12.2016 – C-203/15, C-698/15 (Tele2 Sverige), Rn. 75 f.

[74] Kritisch zur Anwendung der Unionsgrundrechte über die Ausnahmeregelung des Art. 15 Abs. 1 der RL 2002/58/EG *Schiedermair/Mrozek*, DÖV 2016, 89 (91 f.); *Wollenschläger/Krönke*, NJW 2016, 906 (907 ff.).

[75] Siehe auch *Nußberger*, JZ 2018, 845 (853 f.).

[76] *Kühling/Drechsler*, NJW 2017, 2950; *Kingreen*, JZ 2013, 801 (810 f.); vgl. auch *Bäcker*, EuR 2011, 103 (107 ff.), zu diesbezüglichen Chancen aus dem Vorratsdatenspeicherungsurteil des BVerfG.

[77] Dies gilt grundsätzlich für allgemeine Auslegungsfragen, aber auch für solche, bei denen Schutzlücken oder der Bruch mit Verfassungsidentitäten im Raum stehen; siehe zur Bezugnahme auf die verfassungsrechtliche Identität bei einer Totalüberwachung BVerfGE 125, 260 (324); vgl. auch *Hornung/Schnabel*, DVBl 2010, 824 (827 f.); *Papier*, NJW 2017, 3025 (3027); zu Möglichkeiten einer Einbettung in den Solange II-Vorbehalt *Bäcker*, EuR 2011, 103 (118 f.); zum Dialog der Gerichte über nationale Identitäten *Simon*, Grenzen des Bundesverfassungsgerichts im europäischen Integrationsprozess, 2016, S. 268 ff.; zum Dialog zwischen BVerfG und EGMR siehe *Nußberger*, JZ 2018, 845 (850 ff.).

[78] Der EuGH konnte über die Richtlinie und die Vorratsdatengesetze der jeweiligen Mitgliedsländer nur durch die Vorlagen des Österreichischen VerfGH und des Obersten Gerichts in Irland (High Court) sowie des Verwaltungsgerichts Stockholm (Kammarrät i Stockholm) und des Berufungsgerichts England & Wales (Court of Appeal) entscheiden.

[79] *Westphal*, K&R 2014, 410 (411).

[80] *Giegerich*, ZEuS 2014, 3 (14 ff.); *Marsch* (Fn. 57), S. 82; im Ergebnis so auch *Classen*, EuR 2014, 441 (446 f.); *Kühling/Drechsler*, NJW 2017, 2950 (2955); *Wolff*, DöV 2014, 608 (612).

[81] Vgl. auch *Bäcker*, JA 2014, 1263 (1273); *Classen*, EuR 2014, 441; auf eine Unausgewogenheit des europäischen Grundrechtsschutzes hinweisend *Gärditz*, GSZ 2017, 1 (4 f.).

[82] Siehe etwa *Schiedermair/Mrozek*, DÖV 2016, 89 (96); *Sandhu*, EuR 2017, 453 (467 f.); *Wollenschläger*, NJW 2018, 2532 (2536).

[83] Zur Möglichkeit der Anpassung der Entscheidungsprämissen des BVerfG an die Rechtsprechung des EuGH *Thym*, JZ 2015, 53 (57 ff.); zur Implementierung europäischer Schutzstandards in das Grundgesetz *Bäcker*, EuR 2015, 389.

[84] So auch *Derksen*, NVwZ 2017, 1005 (1006); *Priebe*, EuZW 2017, 136 (139); *Wolff*, DöV 2014, 608 (610).

[85] Siehe demgegenüber zu nationalen und europäischen Bestrebungen, die Vorratsdatenspeicherung in veränderter Form erneut zu etablieren, BT-Drs. 19/2079; BT-Drs. 19/2325; Working Paper des Europäischen Rates v. 12.4.2018 – WK 3974/2018 INIT; zu weiteren datenbezogenen Vorhaben auf

Vorratsdatenspeicherung betroffenen, nunmehr europäisch dominierten und ausgelegten Grundrechte in diesem Sinne als „paradigmatisch für das Verständnis der Rolle des Staates" angesehen,[86] dann bestehen Hoffnungen für die europaweite Etablierung eines ausgewogenen Verhältnisses von Privatheit, Datenschutz und Sicherheitsbelangen.

Ebene der EU *Monroy*, Bürgerrechte & Polizei/CILIP 2017, 22 ff.

[86] *Hefendehl*, JZ 2009, 165 (174).