



Ausarbeitung

Auswirkungen der neuen EuGH-Rechtsprechung zur Vorratsdatenspeicherung auf die Tätigkeit der Geheimdienste

Auswirkungen der neuen EuGH-Rechtsprechung zur Vorratsdatenspeicherung auf die Tätigkeit der Geheimdienste

Aktenzeichen: WD 3 - 3000 - 240/20
Abschluss der Arbeit: 6. November 2020 (zugleich letzter Zugriff auf Internet-Quellen)
Fachbereich: WD 3: Verfassung und Verwaltung

Die Wissenschaftlichen Dienste des Deutschen Bundestages unterstützen die Mitglieder des Deutschen Bundestages bei ihrer mandatsbezogenen Tätigkeit. Ihre Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten der Wissenschaftlichen Dienste geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegende, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab dem jeweiligen Fachbereich anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

Inhaltsverzeichnis

1.	Bisherige Rechtsprechung des EuGH zur Vorratsdatenspeicherung und Fragestellung	4
2.	Wesentliche Aussagen der neuen EuGH-Urteile	6
2.1.	Geltung des EU-Rechts für jegliche Kooperationspflichten der TK-Anbieter mit Geheimdiensten und Strafverfolgungsbehörden	6
2.2.	Keine anlasslose umfassende Vorratsdatenspeicherung	7
2.3.	Partielle Ausnahmen zum Schutz der nationalen Sicherheit sind möglich	8
3.	Auswirkung der Urteile auf die Tätigkeit der Geheimdienste in Deutschland	9
3.1.	Bisherige Umsetzung der Vorratsdatenspeicherung in Deutschland	9
3.2.	Keine direkte Geltung der neuen EuGH-Urteile für Geheimdienste in Deutschland	10
3.3.	Keine Regelung der Tätigkeit der Geheimdienste durch EU-Recht außerhalb von Speicher- und Weiterleitungspflichten für private TK-Anbieter	10
4.	Geltung des EuGH-Urteils C-623/17 (Privacy International) in Großbritannien nach dem Brexit	11

1. Bisherige Rechtsprechung des EuGH zur Vorratsdatenspeicherung und Fragestellung

Die sog. Vorratsdatenspeicherung (VDS) wird seit vielen Jahren in Deutschland sowie in anderen Mitgliedstaaten der Europäischen Union (EU) bzw. auf der Ebene der EU kontrovers diskutiert.¹ Es handelt sich dabei um die **anlasslose Speicherung** von Telekommunikationsdaten durch private Anbieter (TK-Anbieter) zum Zweck der Weiterleitung an staatliche Stellen, die diese Daten dann zur Strafverfolgung, Gefahrenabwehr, etwa zur Terrorismusbekämpfung bzw. zu nachrichtendienstlichen Zwecken nutzen können.² Den (umstrittenen) Vorteilen, die die Vorratsdatenspeicherung den staatlichen Stellen im Rahmen ihrer Tätigkeit mit sich bringt,³ stehen die damit verbundenen Eingriffe in die Grundrechte der betroffenen Bürger gegenüber, die sowohl auf nationaler Ebene als auch auf der EU-Ebene durch die **EU-Grundrechtecharta (GRC)**⁴ bzw. durch die **ePrivacy-Richtlinie** von 2002⁵ garantiert werden. Der EuGH überprüft dabei als „Hüter der EU-Grundrechtecharta“, inwieweit die nationale Gesetzgebung zur Vorratsdatenspeicherung den Anforderungen des EU-Rechts genügt.⁶ Im Übrigen sind hinsichtlich der Eingriffe in die nationalen Grundrechte die nationalen (Verfassungs-)Gerichte bzw. für die Eingriffe in die Europäische Menschenrechtskonvention der Europäische Gerichtshof für Menschenrechte zuständig. Sobald das EU-Recht und seine Auslegung betroffen sind, werden die Rechtsfragen wegen des Anwendungsvorrangs des EU-Rechts⁷ durch nationale Gerichte dem EuGH vorgelegt.

Eine Verpflichtung zur Vorratsdatenspeicherung wurde auf der EU-Ebene bereits 2006 durch die Richtlinie 2006/24/EG eingeführt. Mit Urteil vom 8. April 2014 (Digital Rights Ireland Ltd)⁸ erklärte der EuGH diese **Speicherungspflicht** dann als mit **Art. 7 und 8 GRC unvereinbar**. Die Eingriffe in das Recht auf Achtung des Privat- und Familienlebens (Art. 7 GRC) und in das Recht auf den Schutz personenbezogener Daten (Art. 8 GRC) seien von großem Ausmaß und besonderer Schwere,

-
- 1 Siehe etwa Bundeszentrale für Politische Bildung, Brauchen wir die Vorratsdatenspeicherung?, Debattenübersicht vom 16. Oktober 2015, <https://www.bpb.de/dialog/netzdebatte/202219/vorratsdatenspeicherung>.
 - 2 Sehl, Was das EuGH-Urteil für Deutschland bedeutet, Weg frei für Neuaufgabe der Vorratsdatenspeicherung, lto.de vom 6. Oktober 2020, <https://www.lto.de/recht/hintergruende/h/eugh-c62317-vorratsdatenspeicherung-inter-net-telefon-eu-staaten-sicherheit-terrorismus-datenschutz-speichern-deutschland-kinderpornographie/>.
 - 3 Siehe hierzu Leutheusser-Schnarrenberger, Goodbye Vorratsdatenspeicherung, Verfassungsblog vom 8. Oktober 2020, <https://verfassungsblog.de/goodbye-vorratsdatenspeicherung/>.
 - 4 Charta der Grundrechte der Europäischen Union (2000/C 364/01) vom 7. Dezember 2000, https://www.euro-parl.europa.eu/charter/pdf/text_de.pdf.
 - 5 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutz-Richtlinie für elektronische Kommunikation), <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32002L0058>.
 - 6 So Schaar, Analyse: EuGH beerdigt die Vorratsdatenspeicherung, heise online vom 8. April 2014, <https://www.heise.de/newsticker/meldung/Analyse-EuGH-beerdigt-die-Vorratsdatenspeicherung-2166159.html>.
 - 7 Ruffert, in: Calliess/Ruffert (Hrsg.), EUV/AEUV Kommentar, 5. Auflage 2016, AEUV Art. 1, Rn. 18.
 - 8 EuGH-Urteil vom 8. April 2014, Digital Rights Ireland Ltd (C-293/12 und C-594/12, <http://curia.europa.eu/juris/liste.jsf?language=de&num=C-293/12>).

ohne dass die Regelungen Bestimmungen enthielten, die gewährleisten könnten, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkte – etwa durch eine klare Begrenzung des Personenkreises, der Speicherfristen, der Zugangsvoraussetzungen sowie ausreichender Verfahrensgarantien für die Betroffenen.

Der EuGH setzte diese Linie im Urteil vom 21. Dezember 2016 (Tele2 Sverige u.a.)⁹ fort. In diesem Vorabentscheidungsverfahren befasste er sich mit dem Geltungsbereich und der Reichweite des Art. 15 Abs. 1 der ePrivacy-Richtlinie, der Ausnahmen vom Grundsatz der Vertraulichkeit der Kommunikation vorsieht. Nach einer Klarstellung, dass auch mitgliedstaatliche Regelungen zur VDS, in denen es vor allem um die Nutzung der Daten zum Zweck der Strafverfolgung ging, in den Anwendungsbereich des Unionsrechts fallen und diese sich daher an der GRC messen lassen müssen, bekräftigte der EuGH das **grundsätzliche Verbot** der **allgemeinen** und **unterschiedslosen Speicherung** von Verkehrs- und Standortdaten. Ausnahmen könnten zwar zur Verfolgung schwerer Straftaten zulässig sein, unterlägen aber wegen der Intensität des Eingriffs in die Gewährleistungen der GRC einer strikten Verhältnismäßigkeitsprüfung. Zwingend notwendig seien auch hier Maßnahmen zur Begrenzung des potenziell betroffenen Personenkreises durch objektive Kriterien, Vorschriften zur Sicherheit und zum Schutz der gespeicherten Daten und eine vorherige, unabhängige Kontrolle vor dem Datenabruf durch ein Gericht oder eine unabhängige Verwaltungsbehörde.¹⁰

Nach dieser EuGH-Entscheidung gerieten in verschiedenen EU-Mitgliedstaaten vermehrt **nationale nachrichtendienstliche Vorschriften** ins Visier der Gerichte. Die nationalen Gerichte hielten es für zweifelhaft, ob die strenge Linie des EuGH eins zu eins auch auf die Vorratsdatenspeicherung bzw. die Nutzung der Daten für nachrichtendienstliche Zwecke übertragen werden könne. So kamen die Regelungen aus Großbritannien,¹¹ Frankreich und Belgien¹² im Wege eines Vorabentscheidungsverfahrens zum EuGH, der in zwei umfassenden Urteilen nun darüber befunden hat, inwieweit diese nationalen Regelungen dem EU-Recht entsprechen.

Diese Ausarbeitung beschäftigt sich mit den wesentlichen Aussagen dieser zwei EuGH-Entscheidungen (unter 2.) und deren Auswirkungen auf die Tätigkeit der Geheimdienste in Deutschland (unter 3.). Abschließend wird auf die Geltung der EuGH-Entscheidung C-623/17 (Privacy International) in Großbritannien nach dem Brexit eingegangen (unter 3.).

9 EuGH-Urteil vom 21. Dezember 2016, Tele2 Sverige AB (C-203/15), <http://curia.europa.eu/juris/liste.jsf?num=C-203/15&language=de>.

10 Siehe hierzu Wissenschaftliche Dienste des Deutschen Bundestages, Aktueller Begriff Europa Nr. 05/20 vom 22. Oktober 2020, Die Vorratsdatenspeicherung in der Rechtsprechung des EuGH, <https://www.bundestag.de/resource/blob/800664/73fae213527da3664a98b56b011e77aa/Vorratsdatenspeicherung-Rechtsprechung-EuGH-data.pdf>.

11 Siehe EuGH-Urteil vom 6. Oktober 2020, Privacy International, C-623/17, <http://curia.europa.eu/juris/liste.jsf?language=de&td=ALL&num=C-623/17>.

12 Siehe EuGH-Urteil vom 6. Oktober 2020, La Quadrature du Net u.a., C-511/18, C-512/18 und C-520/18, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=11660616>.

2. Wesentliche Aussagen der neuen EuGH-Urteile

2.1. Geltung des EU-Rechts für jegliche Kooperationspflichten der TK-Anbieter mit Geheimdiensten und Strafverfolgungsbehörden

Vor dem EuGH standen die Regelungen zur Speicherung und Nutzung von Telekommunikationsdaten durch Sicherheits- und Nachrichtendienste aus Großbritannien (Kläger: Privacy International), Frankreich (Kläger: La Quadrature du Net u.a.) und Belgien (Kläger: Ordre des barreaux francophones et germanophone u.a.) zur Diskussion. In diesen Verfahren haben die Regierungen der genannten Länder argumentiert, es handle sich um Maßnahmen zum **Schutz der nationalen Sicherheit**, die nach Art. 15 Abs. 1 der ePrivacy-Richtlinie zulässig seien bzw. nach Art. 4 Abs. 2 des Vertrages über die Europäische Union (EUV)¹³ nicht dem EU-Recht, sondern **allein dem nationalen (Verfassungs-)Recht** unterfielen.¹⁴

Eine besondere Begründung zu dieser Argumentation wurde in dem Verfahren von Großbritannien (Privacy International) vorgetragen, wo private TK-Anbieter **nicht selbst** zur **Speicherung** der Kommunikationsdaten, sondern lediglich zu deren **Weiterleitung** an **Nachrichtendienste** nach einer entsprechenden Anweisung verpflichtet wurden. Die Daten wurden dann direkt bei den britischen Nachrichtendiensten in speziellen Datensätzen gespeichert und genutzt.¹⁵ Dieser Argumentation trat auch die Bundesregierung in ihrem Plädoyer in der mündlichen Verhandlung im September 2019 bei, in der die vier Verfahren gemeinsam behandelt wurden. Die Bundesregierung führte aus, das ungefilterte Weiterleiten von Daten sei eine **bloße technische Unterstützung** und als ein lediglich untergeordneter Beitrag zu einer **Aktivität des Staates** zum Schutz der nationalen Sicherheit im Sinne des Art. 4 Abs. 2 EUV zu bewerten.¹⁶ Auch die anderen Regierungen der beteiligten EU-Mitgliedstaaten argumentierten, ihnen müsse ein effektiver Schutz der nationalen Sicherheit im Sinne des Art. 4 Abs. 2 EUV möglich bleiben, sodass die ePrivacy-Richtlinie auf solche Maßnahmen generell nicht anwendbar sei.¹⁷

13 Vertrag über die Europäische Union, Fassung aufgrund des am 1. Dezember 2009 in Kraft getretenen Vertrages von Lissabon, https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0020.02/DOC_1&format=PDF.

14 EuGH-Urteil (Privacy International) (Fn. 11), Rn. 26; EuGH-Urteil (La Quadrature du Net) (Fn. 12), Rn. 62.

15 EuGH-Urteil (Privacy International) (Fn. 11), Rn. 22 ff.

16 Plädoyer der Bundesrepublik Deutschland in den Rechtssachen C-623/17, C-511/18, C-512/18 und C-520/18 in der mündlichen Verhandlung vor dem EuGH in Luxemburg am 9. September 2019, https://fragdenstaat.de/anfrage/vorratsdatenspeicherung-deutsche-position-vor-dem-eugh-am-9-und-1092019/460349/anhang/bundesregierung-vds-eugh-6-9-2019-p_geschwaerzt.pdf; hierzu Rudl, Vorratsdatenspeicherung Bundesregierung plädiert für Datensammlung durch Geheimdienste, netzpolitik.org vom 11. Februar 2020, <https://netzpolieU-tik.org/2020/bundesregierung-plaedierte-fuer-datensammlung-durch-geheimdienste/>.

17 EuGH-Urteil (La Quadrature du Net) (Fn. 12), Rn. 89.

Dieser Argumentation ist der **EuGH** jedoch in beiden Urteilen¹⁸ **entgegengetreten** und betonte dabei, dass die nationalen Maßnahmen nicht allein deswegen dem Geltungsbereich der ePrivacy-Richtlinie entzogen werden könnten, weil sie mit dem Schutz nationaler Sicherheit begründet würden.¹⁹ Der EuGH sieht daher den Anwendungsbereich der ePrivacy-Richtlinie sowohl für Speicherpflichten der privaten TK-Anbieter als auch für Abrufbefugnisse durch Sicherheitsbehörden als eröffnet an. Lediglich in den Fällen, in denen keine Kooperationspflicht für private TK-Anbieter vorgeschrieben werde, unterlägen die geheimdienstlichen Maßnahmen nicht der ePrivacy-Richtlinie, sondern lediglich dem nationalen (Verfassungs-)Recht und der EMRK.²⁰

Diese enge Auslegung der Ausnahmeklausel zum Schutz der nationalen Sicherheit führt zu einem sehr kleinen Anwendungsbereich außerhalb des EU-Rechts und macht den **EuGH faktisch** zu einer **letzten Instanz** in Fragen des **Grundrechtsschutzes** in Europa.²¹

2.2. Keine anlasslose umfassende Vorratsdatenspeicherung

Der EuGH hielt in den beiden neuen Urteilen an seiner oben dargestellten bisherigen Linie fest, dass grundsätzlich eine **allgemeine** und **unterschiedslose Speicherungs-** bzw. **Weiterleitungspflicht** von Verkehrs- und Standortdaten für private TK-Anbieter mit dem Unionsrecht **unvereinbar** sei, da sich der Eingriff in die entsprechenden Grundrechte nicht auf das absolut Notwendige beschränke.²² Neben Art. 7 und Art. 8 GRC wird durch den EuGH zudem eine Gefahr für die Meinungsfreiheit aus Art. 11 GRC hervorgehoben, die zwar kein absolut geschütztes Recht sei, deren Bedeutung es jedoch gebiete, dass Einschränkungen nur durch verhältnismäßige und objektiv erforderliche Maßnahmen aufgrund eines Gesetzes möglich seien.²³

18 Die Verfahren C-511/18, C-512/18 und C-520/18 zu den Regelungen in Frankreich und Belgien wurden zu einem Verfahren verbunden, sodass am Ende zwei Urteile in zwei Verfahren ergangen sind. Es wird im Weiteren daher von zwei neuen EuGH-Urteilen gesprochen.

19 EuGH-Urteil (Privacy International) (Fn. 11), Rn. 44: „*the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law*“.

20 EuGH-Urteil (Privacy International) (Fn. 11), Rn. 48.

21 So Tuchfeld, Verfassungsblog vom 19. Oktober 2020, Towards a European Court of Fundamental Rights, How the European Court of Justice Becomes the Last Instance of Fundamental Rights Adjudication in Europe, <https://verfassungsblog.de/towards-a-european-court-of-fundamental-rights/>.

22 EuGH-Urteil (Privacy International) (Fn. 11), Rn. 83, 2. Leitsatz; EUGH-Urteil (La Quadrature du Net) (Fn. 12), Rn. 229, 1. Leitsatz.

23 EuGH-Urteil (Privacy International) (Fn. 11), Rn. 64: „*those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*“.

2.3. Partielle Ausnahmen zum Schutz der nationalen Sicherheit sind möglich

Aus Art. 15 Abs. 1 ePrivacy-Richtlinie folgen nach den beiden neuen EuGH-Urteilen allerdings wichtige **Ausnahmen** von diesem Grundsatz: Bei einer **tatsächlichen ernsthaften Bedrohung** für die **nationale Sicherheit**, die gegenwärtig oder vorhersehbar ist, bleibe ein enger Spielraum für eine allgemeine und unterschiedslose Speicherung von Telekommunikationsdaten. Diese Speicherung und der Abruf der Daten müsse aber durch **zeitliche Begrenzungen** und umfassende gerichtliche Kontrollmöglichkeiten verhältnismäßig ausgestaltet werden.²⁴

Auch bei der Verfolgung schwerer Straftaten soll eine verhältnismäßige Ausgestaltung der gezielten Speicherung von Daten verdächtiger Personengruppen anknüpfend an die Tele2 Sverige-Entscheidung aus dem Jahre 2016²⁵ möglich sein, sofern die Speicherung hinsichtlich der Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt bleibe.²⁶

Beispielhaft ist auch auf die Speicherung von IP-Adressen als weitere Ausnahme hinzuweisen, welche der EuGH als eine weniger intensive Grundrechtsbeeinträchtigung einstuft.²⁷ Die IP-Adresse erleichtere zwar die Zuordnung von Daten zu einer Person, gebe jedoch nur in begrenzterem Maße darüber Aufschluss, mit wem diese Person kommuniziere und in sonstiger Weise in Verbindung getreten sei. Die Gefahr, dass auf diesem Wege ein umfassendes Profil über Nutzerinnen und Nutzer erstellt werden könne, sei deshalb als geringer anzusehen.²⁸ Auch hier sollen allerdings die strikten Voraussetzungen des Grundsatzes der **Verhältnismäßigkeit** eingehalten werden, beispielsweise durch Speicherfristen und hinreichende gerichtliche Kontrollmöglichkeiten.

Darüber hinaus seien unionsrechtskonforme Ausgestaltungen nationaler Gesetze denkbar, die eine verlängerte Speicherung bereits gesammelter Daten von Telekommunikationsdienstleistern (etwa zu Abrechnungszwecken) ermöglichen.²⁹ Sie sollen in konkreten Verdachtsmomenten dazu beitragen, auf Gefährdungen der nationalen Sicherheit reagieren zu können oder die Ermittlungen schwerer Straftaten zu erleichtern. Auch hier müssen objektive und nicht diskriminierende Kriterien den betroffenen Personenkreis abgrenzen, um den Abruf durch die Sicherheitsbehörden und Nachrichtendienste auf das absolut Notwendige zu beschränken.

24 EuGH-Urteil (Privacy International) (Fn. 11), Rn. 78.

25 Siehe oben Fn. 9.

26 EuGH-Urteil (La Quadrature du Net) (Fn. 12), Rn. 140 ff.

27 EuGH-Urteil (La Quadrature du Net) (Fn. 12), Rn. 152 ff.

28 EuGH-Urteil (La Quadrature du Net) (Fn. 12), Rn. 154.

29 EuGH-Urteil (La Quadrature du Net) (Fn. 12), Rn. 160 ff., 168.

3. Auswirkung der Urteile auf die Tätigkeit der Geheimdienste in Deutschland

3.1. Bisherige Umsetzung der Vorratsdatenspeicherung in Deutschland

Der erste Versuch der Einführung der VDS in Deutschland diente der Umsetzung der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung, die ihrerseits in der Folgezeit durch den **EuGH** in dem Urteil von 2014 (Digital Rights Ireland Ltd) für **unwirksam** erklärt wurde.³⁰ Bereits zuvor im Jahre 2010 hatte das **Bundesverfassungsgericht** das deutsche Umsetzungsgesetz für **verfassungswidrig** erklärt.³¹

Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015³² stellte damit den zweiten Versuch der Einführung einer VDS in Deutschland dar, in dem der Gesetzgeber auf die bisherigen Vorgaben des Bundesverfassungsgerichts reagierte. In Art. 2 dieses Gesetzes wurden insbesondere Änderungen des Telekommunikationsgesetzes³³ vorgesehen: Nach § 113b TKG n.F. müssen die TK-Anbieter die **Verkehrsdaten** für **zehn Wochen** und die **Standortdaten** für **vier Wochen** speichern. Außerdem wurden in § 113d TKG n.F. **Vorkehrungen** zur Gewährleistung der **Sicherheit** der **Daten** vorgesehen. Nach § 113c TKG n.F. in Verbindung mit § 113 Abs. 1 S. 3 TKG dürfen die so gespeicherten Daten auch den **Nachrichtendiensten**, nämlich dem Bundesverfassungsschutz, dem Bundesnachrichtendienst (BND) und dem Militärischen Abschirmdienst (MAD) auf Anfrage zur Verfügung gestellt werden (sog. **manuelles Auskunftsverfahren**).

Die deutschen TK-Anbieter haben gegen diese Speicherpflichten erfolgreich vor den Verwaltungsgerichten geklagt.³⁴ Die **Bundesnetzagentur** setzte daraufhin die **Speicherpflichten aus** und sah von der Verfolgung etwaiger Verstöße gegen Speicherpflichten nach dem durch dieses Gesetz novellierten Telekommunikationsgesetz ab.³⁵ Inzwischen hat das **Bundesverwaltungsgericht** sich mit

30 Siehe oben Fn. 8.

31 BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08 u.a., NJW 2010, 833.

32 Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015, BGBl. I, S. 2218, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s2218.pdf.

33 Telekommunikationsgesetz (TKG) vom 22. Juni 2014, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl104s1190.pdf.

34 OVG Münster, Beschluss vom 22. Juni 2017 – 13 B 238/17, NVwZ-RR 2018, 43; VG Köln, Urteil vom 20. April 2018 – 9 K 3859/16, ZD 2018, 601.

35 Bundesnetzagentur, Mitteilung zur Speicherverpflichtung nach § 113b TKG vom 28 Juni 2017, https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html;jsessionid=D4F71FC38673C1A16E69195D6334AA05

einem **Vorabentscheidungsersuchen** zu der deutschen Regelung zur VDS an den **EuGH** gewandt.³⁶ Die Entscheidung in dem Verfahren steht noch aus.

3.2. Keine direkte Geltung der neuen EuGH-Urteile für Geheimdienste in Deutschland

Die neuen EuGH-Entscheidungen beziehen sich nur auf die nationale Gesetzgebung zur Vorratsdatenspeicherung in Großbritannien, Frankreich und Belgien und gelten daher **nicht direkt** für die Prüfung der Zulässigkeit der **deutschen Regelung** zur VDS, die nach der erfolgten Vorlage des Bundesverwaltungsgerichts beim EuGH noch aussteht.³⁷ In den Urteilen sind die Grundsätze der Einführung der VDS zum Zwecke u.a. des Schutzes der nationalen Sicherheit (siehe oben unter 2.1.) allerdings bereits mit beträchtlicher Tiefe herausgearbeitet, sodass davon ausgegangen werden kann, dass der EuGH diese Grundsätze auch bei der Prüfung der deutschen Regelung anwendet.³⁸ Danach dürfte die deutsche Regelung von 2015³⁹ kaum Bestand haben, denn sie sieht zwar kürzere Speicherfristen vor, die Speicherung soll danach jedoch immer ohne gesonderten Anlass erfolgen, was den oben genannten **Grundsätzen** des **EuGH nicht entspricht**.⁴⁰ Dem deutschen Gesetzgeber bleibt es jedoch unbenommen, entweder noch die Entscheidung des EuGH zu der deutschen Regelung abzuwarten, oder bereits jetzt ein neues Gesetz zur Vorratsdatenspeicherung unter Berücksichtigung der Vorgaben aus den beiden neuen EuGH-Urteilen zu erlassen.⁴¹

3.3. Keine Regelung der Tätigkeit der Geheimdienste durch EU-Recht außerhalb von Speicher- und Weiterleitungspflichten für private TK-Anbieter

Wie oben bereits unter Punkt 2.1. dargestellt, hat der EuGH in seinen beiden neuen Entscheidungen den Anwendungsbereich der ePrivacy-Richtlinie sowie der EU-Grundrechtecharta nur in den Fällen gesehen, in denen durch nationale Gesetzgebung eines EU-Mitgliedstaates privaten TK-Anbietern Speicher- oder Weiterleitungspflichten auferlegt werden. Werden solche Pflichten nicht auferlegt und den Sicherheitsbehörden bzw. Nachrichtendiensten sonstige Maßnahmen für einen Eingriff in die Vertraulichkeit der Kommunikation erlaubt, so ist die ePrivacy-Richtlinie nicht

36 BVerwG, Beschluss von 25. September 2019 – 6 C 12.18, NVwZ 2020, 1108.

37 Siehe Meldung von beck-online vom 6. Oktober 2020, Keine pauschale Vorratsdatenspeicherung, <https://rsw.beck.de/aktuell/daily/meldung/detail/eugh-keine-pauschale-vorratsdatenspeicherung>.

38 Janisch, EuGH zu Vorratsdatenspeicherung, Welche Konsequenzen das Urteil für Deutschland hat, Süddeutsche Zeitung vom 6. Oktober 2020, <https://www.sueddeutsche.de/digital/eugh-zur-vorratsdatenspeicherung-welche-konsequenzen-das-urteil-fuer-deutschland-hat-1.5056387>; Sehl (Fn. 2).

39 Siehe Fn. 32.

40 Leutheusser-Schnarrenberger (Fn. 3); Krempl, EuGH-Urteile: Der „alte Zombie“ Vorratsdatenspeicherung lebt, heise online vom 6. Oktober 2020, <https://www.heise.de/news/EuGH-Urteile-Der-alte-Zombie-Vorratsdatenspeicherung-lebt-4922543.html>.

41 Sehl (Fn. 2); Janisch (Fn. 38).

anwendbar, sondern lediglich nationales (Verfassungs-)Recht.⁴² Insofern sind direkte Vorratsdatenspeicherung bzw. ein anlassloser Zugriff auf Internet-Knoten durch Nachrichtendienste **ohne Inanspruchnahme privater TK-Anbieter nicht** durch das **EU-Recht verboten** und unterliegen allein dem nationalen Verfassungsrecht bzw. den Einschränkungen der Europäischen Menschenrechtskonvention, für die der Europäische Gerichtshof für Menschenrechte zuständig ist.⁴³

Aus der sog. **Doppeltürrechtsprechung** des **Bundesverfassungsgerichts**, wonach die Abfragebefugnisse der Sicherheitsbehörden bzw. der Nachrichtendienste gegenüber Privaten neben den Übermittlungspflichten Privater **gesondert geregelt** werden müssen,⁴⁴ ergibt sich auch, dass die Vorschriften für den Abruf von gespeicherten Telekommunikationsdaten für Nachrichtendienste (§ 8d BVerfSchG, § 2b BNDG und § 4b MADG, sog. **Bestandsdatenauskunft**) damit **nicht direkt** von der neuen **Rechtsprechung** des **EuGH betroffen** sind. Sie sind nach dem deutschen Verfassungsrecht zu beurteilen, dessen Prüfung dem Bundesverfassungsgericht obliegt. Die aktuell geltenden Vorschriften zur Bestandsdatenauskunft hat das Bundesverfassungsgericht im Mai 2020 für verfassungswidrig erklärt und dem Gesetzgeber Vorgaben gemacht, die bis zum 31. Dezember 2021 umgesetzt werden müssen.⁴⁵

4. Geltung des EuGH-Urteils C-623/17 (Privacy International) in Großbritannien nach dem Brexit

Im Zuge der Brexit-Vorbereitung hat Großbritannien den **European Union (Withdrawal) Act 2018** (weiter WA 2018)⁴⁶ verabschiedet. Dieser wurde am 23. Januar 2020 durch den **European Union (Withdrawal Agreement) Act 2020** (weiter WA 2020)⁴⁷ ergänzt.

Nach Sec. 7 WA 2018 behält das **Primär- und Sekundärrecht** der **EU** grundsätzlich **weiterhin Geltung** auch nach dem Austritt von Großbritannien aus der Europäischen Union, kann aber ggf. durch britische Gesetzgebung, etwa ein Parlamentsgesetz, abgeändert werden. Damit gelten sowohl die ePrivacy-Richtlinie als auch die EU-Grundrechtscharta auch nach dem Brexit in Großbritannien grundsätzlich weiter, solange keine abweichende Gesetzgebung erlassen wird.

Nach Sec. 6 Abs. 1 WA 2018 sind einfache britische Gerichte nicht an die Entscheidungen des EuGH gebunden, sofern diese **nach** dem Tag des Austrittes von Großbritannien aus der EU ergangen sind. Ebenso wenig ist ab diesem Zeitpunkt eine Vorabentscheidungsvorlage zum EuGH zur

42 EuGH-Urteil (Privacy International) (Fn. 11), Rn. 48: „By contrast, where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is not covered by Directive 2002/58, but by national law only.“

43 So auch Krempl (Fn. 40) mit Verweis auf den Rechtsprofessor Douwe Korff.

44 BVerfG, Beschluss vom 24. Januar 2012 – 1 BvR 1299/05, NJW 2012, 1419.

45 BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13, NJW 2020, 2699.

46 European Union (Withdrawal) Act 2018, <https://www.legislation.gov.uk/ukpga/2018/16/section/6/enacted>.

47 European Union (Withdrawal Agreement) Act 2020, https://www.legislation.gov.uk/ukpga/2020/1/pdfs/ukpga_20200001_en.pdf.

Auslegung des EU-Rechts möglich. Unter dem Zeitpunkt des Austrittes ist gem. Sec. 25 WA 2020 das Ende des Übergangszeitraums zu verstehen, also der **31. Dezember 2020**. Danach sind die beiden neuen **EuGH-Urteile zur VDS** für einfache britische Gerichte **grundsätzlich bindend**, da sie am 6. Oktober 2020 und damit noch vor dem Ende des Übergangszeitraums ergangen sind.

Allerdings sind der Oberste Gerichtshof von Großbritannien (the Supreme Court) und das Oberste Gericht von Schottland (the High Court of Justiciary) gem. Sec. 6 Abs. 4 WA 2018 nicht an die ergangene EuGH-Rechtsprechung gebunden und dürfen davon unter den gleichen Voraussetzungen abweichen, unter welchen sie von der eigenen bisherigen Rechtsprechung abweichen dürfen (Sec. 6 Abs. 5 WA 2018).

Außerdem wurde in Sec. 26 WA 2020 für den Kabinettsminister (Minister of the Crown) die Möglichkeit geschaffen, per Rechtsverordnung (by regulations) zu bestimmen, von welchen Entscheidungen des EuGH die britischen Gerichte auf welche Weise abweichen dürfen. Gegenwärtig ist es noch nicht klar, ob und wie davon Gebrauch gemacht werden soll. Das britische Justizministerium führt gegenwärtig Konsultationen hierzu durch.⁴⁸

Schließlich ist anzumerken, dass gegenwärtig ein endgültiges Freihandelsabkommen zwischen der EU und Großbritannien noch verhandelt wird.⁴⁹ Ob ein solches Abkommen zustande kommt bzw. welche einzelnen Themenkomplexe des EU-Rechts davon wie erfasst sein werden, lässt sich gegenwärtig noch nicht absehen. Es ist nicht auszuschließen, dass Großbritannien zusätzliche Verpflichtungen zu einer strikteren Einhaltung der EuGH-Rechtsprechung für die Zukunft eingehen wird.

48 UK Government, Consultation outcome Departure from retained EU case law by UK courts and tribunals, 2. Juli 2020, <https://www.gov.uk/government/consultations/departure-from-retained-eu-case-law-by-uk-courts-and-tribunals>; hierzu ausführlich Leckey/McCulloch, Consultation on ability of courts to depart from EU law after Brexit, Artikel vom 30. Juli 2020, <https://www.lewissilkin.com/en/insights/consultation-on-ability-of-courts-to-depart-from-eu-law-after-brexite>.

49 Vgl. hierzu Kapern, EU und Großbritannien, Die Knackpunkte der Brexit-Verhandlungen, Deutschlandfunk vom 14. Oktober 2020, https://www.deutschlandfunk.de/eu-und-grossbritannien-die-knackpunkte-der-brexite.2897.de.html?dram:article_id=477747.