

Prof. Dr. Jan Dirk Roggenkamp
Prof. Dr. Frank Josef Braun

Korrespondenzadresse
c/o Digitalcourage e.V.
Marktstraße 18
33602 Bielefeld

Tel: 0521-1639 1639
Fax: 0521-6 11 72

An das
Bundesverfassungsgericht
Postfach 1771
76006 Karlsruhe

Bielefeld, den 17. Dezember 2021

Verfassungsbeschwerde Az.: 1 BvR 2683/16

hier: Novelliertes Telekommunikationsgesetz

In dem Verfassungsbeschwerdeverfahren mit dem Aktenzeichen **1 BvR 2683/16** wird anlässlich der Novellierung des Telekommunikationsgesetzes namens und mit Vollmacht der Beschwerdeführerinnen und Beschwerdeführer beantragt

die §§ 176 Abs. 1-4 und 8 sowie 177 Abs. 1 Telekommunikationsgesetz in der Fassung, die sie durch das Gesetz zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts vom 23. Juni 2021 (Bundesgesetzblatt I Seite 1858) erhalten haben, für unvereinbar mit Artikel 10, Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1, und Artikel 5 Abs. 1 des Grundgesetzes zu erklären.

Der in der in der am 28. November 2016 erhobenen Verfassungsbeschwerde (Az.: 1 BvR 2683/16) gemachte **Antrag zu 2.** wird insoweit umgestellt bzw. erstreckt.

Sollte von den Beschwerdeführerinnen und Beschwerdeführern Weiteres zu veranlassen sein, wird höflichst um einen entsprechenden Hinweis des Gerichts gebeten.

Begründung zum geänderten Antrag

Mit dem Gesetz zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts vom

23. Juni 2021 (Bundesgesetzblatt I Seite 1858) – im Weiteren „TKModG“ – wurde das Telekommunikationsgesetz (TKG) überarbeitet und neu gefasst, Art. 1 TKModG.

Die Regelungen traten gemäß Art. 61 Abs. 1 TKModG am 1. Dezember 2021 in Kraft.

Im Rahmen der Novellierung des TKG wurden die mit der Verfassungsbeschwerde vom 28. November 2016 (1 BvR 2683/16) angegriffenen Regelungen der §§ 113b Abs. 1 - 4 und 8 sowie 113c Abs. 1 des Telekommunikationsgesetzes in der Fassung, die sie durch das Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (Bundesgesetzblatt I Seite 2218 ff.) erhalten haben (im Weiteren „TKG a.F.“) nicht in dem Sinne aufgehoben, dass sie ersatzlos entfallen wären.

Im Gegenteil: Die bisherigen Regelungen wurden neu nummeriert in das novellierte TKG überführt. Die §§ 113a bis 113g TKG a.F. finden sich nunmehr in den §§ 175 bis 181 TKG wieder. Es wurden lediglich sprachliche Anpassungen vorgenommen. So verwendet das TKG beispielsweise nunmehr nicht mehr den Begriff „Telefondienst“, sondern „Sprachkommunikationsdienst“. Zudem wurden Verweisungen angepasst.

Diese Perpetuierung der Rechtslage erfolgte ausdrücklich und bewusst:

„Die Verpflichtungen zur Speicherung von Verkehrsdaten nach den bisherigen §§ 113a bis 113g sind Gegenstand nationaler sowie unionsrechtlicher gerichtlicher Überprüfung. Vor diesem Hintergrund werden die Vorschriften im Rahmen der vorliegenden Novelle inhaltlich nicht verändert.“ (BT-Drs. 19/26108, S. 369 f.)

Dementsprechend war der Antrag dahingehend umzustellen, dass sich die angegriffenen Vorschriften nunmehr in den folgenden §§ des neu gefassten TKG befinden:

- § 176 Abs. 1 – 4 und 8 TKG
- § 177 Abs. 1 TKG

Die hier gegenständlichen Vorschriften, die im Folgenden synoptisch (alte Fassung/novellierte Fassung) dargestellt werden, sind wie folgt gefasst:

Alte Fassung	Novellierte Fassung
§ 113b Pflichten zur Speicherung von Verkehrsdaten	§ 176 Pflichten zur Speicherung von Verkehrsdaten
(1) Die in § 113a Absatz 1 Genannten sind verpflichtet, Daten wie folgt im Inland zu speichern:	(1) Die in § 175 Absatz 1 Genannten sind verpflichtet, Daten wie folgt im Inland zu speichern:

1. Daten nach den Absätzen 2 und 3 für zehn Wochen, 2. Standortdaten nach Absatz 4 für vier Wochen. (2) Die Erbringer öffentlich zugänglicher Telefondienste speichern 1. die Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses, 2. Datum und Uhrzeit von Beginn und Ende der Verbindung unter Angabe der zugrunde liegenden Zeitzone, 3. Angaben zu dem genutzten Dienst, wenn im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, 4. im Fall mobiler Telefondienste ferner a) die internationale Kennung mobiler Teilnehmer für den anrufenden und den angerufenen Anschluss, b) die internationale Kennung des anrufenden und des angerufenen Endgerätes, c) Datum und Uhrzeit der ersten Aktivierung des Dienstes unter Angabe der zugrunde liegenden Zeitzone, wenn Dienste im Voraus bezahlt wurden, 5. im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen. Satz 1 gilt entsprechend 1. bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei treten an die Stelle der Angaben nach Satz 1 Nummer 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht; 2. für unbeantwortete oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe, soweit der Erbringer öffentlich zugänglicher Telefondienste die in Satz 1 genannten Verkehrsdaten für die in § 96 Absatz 1 Satz 2 genannten Zwecke speichert oder protokolliert. (3) Die Erbringer öffentlich zugänglicher Internetzugangsdienste speichern 1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse, 2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung, 3. Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen	1. Daten nach den Absätzen 2 und 3 für zehn Wochen, 2. Standortdaten nach Absatz 4 für vier Wochen. (2) Die Anbieter von Sprachkommunikationsdiensten speichern 1. die Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses, 2. Datum und Uhrzeit von Beginn und Ende der Verbindung unter Angabe der zugrunde liegenden Zeitzone, 3. Angaben zu dem genutzten Dienst, wenn im Rahmen des Sprachkommunikationsdienstes unterschiedliche Dienste genutzt werden können, 4. im Falle mobiler Sprachkommunikationsdienste ferner a) die internationale Kennung mobiler Endnutzer für den anrufenden und den angerufenen Anschluss, b) die internationale Kennung des anrufenden und des angerufenen Endgerätes, c) Datum und Uhrzeit der ersten Aktivierung des Dienstes unter Angabe der zugrunde liegenden Zeitzone, wenn Dienste im Voraus bezahlt wurden, 5. im Falle von Internet-Sprachkommunikationsdiensten auch die Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen. Satz 1 gilt entsprechend 1. bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei treten an die Stelle der Angaben nach Satz 1 Nummer 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht; 2. für unbeantwortete oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe, soweit der Anbieter öffentlich zugänglicher Sprachkommunikationsdienste die in Satz 1 genannten Verkehrsdaten für die in § 9 des Telekommunikation-Telemedien-Datenschutz-Gesetzes genannten Zwecke speichert oder protokolliert. (3) Die Anbieter öffentlich zugänglicher Internetzugangsdienste speichern 1. die dem Endnutzer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse, 2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung, 3. Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen
--	--

Internetprotokoll-Adresse unter Angabe der zugrunde liegenden Zeitzone. (4) Im Fall der Nutzung mobiler Telefondienste sind die Bezeichnungen der Funkzellen zu speichern, die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt wurden. Bei öffentlich zugänglichen Internetzugangsdiensten ist im Fall der mobilen Nutzung die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle zu speichern. Zusätzlich sind die Daten vorzuhalten, aus denen sich die geografische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben. [...] (8) Der nach § 113a Absatz 1 Verpflichtete hat die auf Grund des Absatzes 1 gespeicherten Daten unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfristen nach Absatz 1, irreversibel zu löschen oder die irreversible Löschung sicherzustellen.	Internetprotokoll-Adresse unter Angabe der zugrunde liegenden Zeitzone. (4) Im Falle der Nutzung mobiler Sprachkommunikationsdienste sind die Bezeichnungen der Funkzellen zu speichern, die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt wurden. Bei öffentlich zugänglichen Internetzugangsdiensten ist im Falle der mobilen Nutzung die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle zu speichern. Zusätzlich sind die Daten vorzuhalten, aus denen sich die geografische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben. [...] (8) Der nach § 175 Absatz 1 Verpflichtete hat die aufgrund des Absatzes 1 gespeicherten Daten unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfristen nach Absatz 1, irreversibel zu löschen oder die irreversible Löschung sicherzustellen.
§ 113c Verwendung der Daten	§ 177 Verwendung der Daten
(1) Die auf Grund des § 113b gespeicherten Daten dürfen 1. an eine Strafverfolgungsbehörde übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b genannten Daten zur Verfolgung besonders schwerer Straftaten erlaubt, verlangt; 2. an eine Gefahrenabwehrbehörde der Länder übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 113b genannten Daten zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes erlaubt, verlangt; 3. durch den Erbringer öffentlich zugänglicher Telekommunikationsdienste für eine Auskunft nach § 113 Absatz 1 Satz 3 verwendet werden. (2) Für andere Zwecke als die in Absatz 1 genannten dürfen die auf Grund des § 113b gespeicherten Daten von den nach § 113a Absatz 1 Verpflichteten nicht verwendet werden. (3) Die Übermittlung der Daten erfolgt nach Maßgabe der Rechtsverordnung nach § 110 Absatz 2 und der Technischen Richtlinie nach § 110 Absatz 3. Die Daten sind so zu kennzeichnen, dass erkennbar ist, dass es sich um Daten handelt, die nach § 113b gespeichert waren.	(1) Die aufgrund des § 176 gespeicherten Daten dürfen 1. an eine Strafverfolgungsbehörde übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 176 genannten Daten zur Verfolgung besonders schwerer Straftaten erlaubt, verlangt; 2. an eine Gefahrenabwehrbehörde der Länder übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der in § 176 genannten Daten zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes erlaubt, verlangt; 3. durch den Anbieter öffentlich zugänglicher Telekommunikationsdienste für eine Auskunft nach § 174 Absatz 1 Satz 3 verwendet werden. (2) Für andere Zwecke als die in Absatz 1 genannten dürfen die aufgrund des § 176 gespeicherten Daten von den nach § 175 Absatz 1 Verpflichteten nicht verwendet werden. (3) Die Übermittlung der Daten erfolgt nach Maßgabe der Rechtsverordnung nach § 170 Absatz 5 und der Technischen Richtlinie nach § 170 Absatz 6. Die Daten sind so zu kennzeichnen, dass erkennbar ist, dass es sich um Daten handelt, die nach § 176 gespeichert waren. Nach Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten.

Nach Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten.	
---	--

Mit Blick auf die nicht erfolgte inhaltliche Änderung der letztlich nur im TKG „verschobenen“ Regelungen wird die bereits dargelegte Unvereinbarkeit der angegriffenen Regelungen mit Artikel 10, Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1, und Artikel 5 Abs. 1 des Grundgesetzes nicht berührt. Die Beschwer besteht unverändert fort.

Dennoch soll vor dem Hintergrund der Novellierung des TKG klarstellend zu einigen Punkten der Beschwerdeschrift vom 28. November 2016 (1 BvR 2683/16 – i.W. Ausgangsbeschwerdeschrift) Stellung genommen werden:

Zu 5.3.2.2 Unbestimmtheit

Die in der Ausgangsbeschwerdeschrift getroffene Feststellung, dass der Begriff der „*ähnlichen Nachricht*“ in § 113 b Abs. 2 S. 2 Nr. 1 TKG a.F. zu unbestimmt ist, gilt mutatis mutandis auch für die „neue“ Regelung in § 176 Abs. 2 S. 2 Nr. 1 TKG. Es bleibt weiterhin offen, ob unter dem Begriff der den Kurz- bzw. Multimedia-Nachrichten „*ähnlichen Nachrichten*“ auch Instant-Messengerdienste bzw. über diese verschickte „Nachrichten“ zu subsumieren sind. Dies insbesondere, wenn sie von Diensteanbietern bereitgestellt werden, die (auch) „klassische Telefondienste“ erbringen. Indem der Gesetzgeber in § 175 Abs. 1 TKG den Kreis der Verpflichteten dahingehend einschränkt, dass „*Anbieter öffentlich zugänglicher Telekommunikationsdienste für Endnutzer, bei denen es sich nicht um nummernunabhängige interpersonelle Telekommunikationsdienste handelt*“ ausgeklammert werden, trägt er damit nicht zur Klärung der Frage bei.

Ein „*nummernunabhängiger interpersoneller Telekommunikationsdienst*“ ist nach der „Begriffsbestimmung“ in § 3 Nr. 40 TKG (Hervorhebung nur hier) „*ein interpersoneller Telekommunikationsdienst, der weder eine Verbindung zu öffentlich zugewiesenen Nummerierungsressourcen, nämlich Nummern nationaler oder internationaler Nummernpläne, herstellt noch die Telekommunikation mit Nummern nationaler oder internationaler Nummernpläne ermöglicht*“.

Es bleibt unklar, wie Dienste zu beurteilen sind, die grundsätzlich als nummernunabhängiger Messengerdienst fungieren, jedoch eine zusätzliche Funktionalität zur Tätigung von Anrufen (oder Versendung von Nachrichten) an eine „herkömmliche“ Festnetz- oder Mobilfunknummer haben (so z.B. der Dienst Skype). Gleiches gilt für die bereits in der Ausgangsbeschwerde adressierten Angebote zum Versand von „Chat-Nachrichten“ von Anbietern „nummernabhängiger interpersoneller Telekommunikationsdienste“ wie der Deutschen

Telekom (vgl. die Darstellung des Dienstes Telekom App Message + in der Ausgangsbeschwerdeschrift unter 5.3.2.2).

Zu 5.3.2.5 Unzureichende Zweckbindung

Wie § 113c Abs. 1 Nr. 3 TKG a.F. ist auch § 177 Abs. 1 Nr. 3 TKG aufgrund unzureichender Zweckbindung der Auskunftsbefugnis verfassungswidrig. Die in der Ausgangsbeschwerdeschrift geäußerten Bedenken bestehen fort. Die von § 113c Abs. 1 Nr. 3 TKG a.F. in Bezug genommene Vorschrift des § 113 Abs. 1 TKG a.F. wurde zwischenzeitlich vom Gericht (BVerfG, Beschluss vom 27.5.2020 – 1 BvR 1873/13, 1 BvR 2618/13) für mit Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 und Art. 10 Abs. 1 GG unvereinbar erklärt.

In der Folge wurde § 113 TKG a.F. (insbesondere durch § 113 Abs. 5 TKG a.F., der sich nunmehr in § 174 Abs. 5 TKG findet) zwar präzisiert. Weiterhin wird jedoch durch § 174 Abs. 5 Nr. 1 TKG eine Bestandsdatenauskunft unter Verwendung aufgrund des § 176 TKG gespeicherter Daten zugelassen, *„soweit zureichende tatsächliche Anhaltspunkte für eine Straftat vorliegen und die in die Auskunft aufzunehmenden Daten erforderlich sind, um den Sachverhalt zu erforschen, den Aufenthaltsort eines Beschuldigten zu ermitteln oder eine Strafe zu vollstrecken“*. Damit ist erlaubter Verwendungszweck nach § 177 Abs. 1 Nr. 3 TKG letztlich die Verfolgung jeglicher Straftaten. Die bereits in der Ausgangsbeschwerdeschrift aufgezeigte Unvereinbarkeit mit dem vom Gesetzgeber selbst festgelegten Erhebungszweck (u.a. die Verfolgung von besonders schweren Straftaten) besteht damit fort.

Zu 5.3.5.6 Schutz der Vertrauensberufe

Auch nach der Novellierung des TKG ist – wie in der Ausgangsbeschwerdeschrift dargelegt – eine technisch mögliche Ausnahme von der Erhebung der Daten von Berufsgeheimnisträgern nicht vorgesehen. Die in § 113b Abs. 6 TKG a.F. enthaltene Verweisung auf § 99 Abs. 2 TKG a.F. führt im neu nummerierten § 176 Abs. 6 TKG nunmehr zu § 11 Abs. 5 und Abs. 6 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) welcher dem § 99 Abs. 2 TKG a.F. inhaltlich entspricht:

§ 99 Abs. 2 TKG a.F.	§ 11 Abs. 5 und 6 TTDSG
(2) Der Einzelverbindungs-nachweis nach Absatz 1 Satz 1 darf nicht Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen erkennen lassen, die grundsätzlich anonym bleibenden	(5) Der Einzelverbindungs-nachweis nach Absatz 1 Satz 1 darf nicht Verbindungen zu Anschlüssen erkennen lassen, 1. deren Inhaber Personen, Behörden oder Organisationen in sozialen oder kirchlichen

Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen. Dies gilt nur, soweit die Bundesnetzagentur die angerufenen Anschlüsse in eine Liste aufgenommen hat. Der Beratung im Sinne des Satzes 1 dienen neben den in § 203 Absatz 1 Nummer 4 und 5 des Strafgesetzbuches genannten Personengruppen insbesondere die Telefonseelsorge und die Gesundheitsberatung. Die Bundesnetzagentur nimmt die Inhaber der Anschlüsse auf Antrag in die Liste auf, wenn sie ihre Aufgabenbestimmung nach Satz 1 durch Bescheinigung einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts nachgewiesen haben. Die Liste wird zum Abruf im automatisierten Verfahren bereitgestellt. Der Diensteanbieter hat die Liste quartalsweise abzufragen und Änderungen unverzüglich in seinen Abrechnungsverfahren anzuwenden. Die Sätze 1 bis 6 gelten nicht für Diensteanbieter, die als Anbieter für geschlossene Benutzergruppen ihre Dienste nur ihren Teilnehmern anbieten.	Bereichen sind, die grundsätzlich anonym bleibenden Endnutzern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verpflichtungen zur Verschwiegenheit unterliegen, und 2. die die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur) in eine Liste aufgenommen hat. (6) Der Beratung im Sinne des Absatzes 5 Nummer 1 dienen neben den in § 203 Absatz 1 Nummer 4 und 5 des Strafgesetzbuches genannten Personengruppen insbesondere die Telefonseelsorge und die Gesundheitsberatung. Die Bundesnetzagentur nimmt die Inhaber der Anschlüsse auf Antrag in die Liste auf, wenn sie die Aufgabenbestimmung nach Absatz 5 Nummer 1 durch Bescheinigung einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts nachgewiesen haben. Die Liste wird zum Abruf im automatisierten Verfahren bereitgestellt. Die Verpflichteten nach § 3 Absatz 2 Satz 1, die Einzelbindungsnachweise erstellen, haben die Liste quartalsweise abzufragen und Änderungen unverzüglich in ihren Abrechnungsverfahren anzuwenden.
---	---

Sachliche Gründe dafür, dass die nach § 53 StPO zur Zeugnisverweigerung Berechtigten nicht – wie Stellen nach § 11 Abs. 5 und 6 TTD SG – von der Ausnahme der Speicherverpflichtung in § 176 Abs. 6 TKG erfasst werden, sind weiterhin nicht ersichtlich.

Zu 5.3.6.1 Vorratsspeicherung von IP-Adressen

Eine generelle und undifferenzierte Vorratsspeicherung der Identität der Internet-Nutzer würde die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers in noch höherem Maße als durch den Rückgriff auf Telefon-Verbindungsdaten ermöglichen: Die Kenntnis der IP-Adresse eines Internetnutzers macht unter Nutzung sogenannter „Logfiles“ der Diensteanbieter potenziell dessen gesamte Internetnutzung nachvollziehbar – nicht nur, mit wem er in Verbindung stand (wie bei Telefon-Verbindungsdaten), sondern auch die Inhalte, für die er sich im Netz interessiert hat (jede Eingabe, jeder Klick, jeder Download, jeder Beitrag/Post im Netz). In Logfiles speichern Telemedien fast durchwegs sämtliche Nutzungsdaten mitsamt der IP-Adresse auf Vorrat. Das vom Bundesverfassungsgericht 2010 noch angesprochene Verbot einer Vorratsspeicherung von Nutzungsdaten im Telemediengesetz ist nicht mehr in Kraft. Aus der IP-Adresse lässt sich auch der Aufenthaltsort ableiten; nach neuen Forschungsergebnissen sogar, ob sich der Nutzer zu Hause, auf der Arbeit oder unterwegs befindet (vgl. Pitsillidis, Xie, et. al. – *“How to Tell an Airport from a Home: Techniques and Applications”*, abrufbar unter <https://users.soe.ucsc.edu/~abadi/Papers/hotnets10.pdf>).

Mit Urteil vom 06.10.2020 (C-511/18, C-512/18 und C-520/18) hat der **EuGH** entschieden, es sei mit Unionsrecht vereinbar, zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorzusehen. Zur Begründung hat der EUGH ausgeführt, die IP-Adresse des Nutzers einer Internetverbindung, einer Internettelefonieverbindung und des Absenders einer E-Mail könne zwar „zur umfassenden Nachverfolgung der von einem Internetnutzer besuchten Internetseiten und infolgedessen seiner Online-Aktivität genutzt werden“, lasse für sich genommen aber nicht auf den Kommunikationspartner schließen und sei deshalb weniger sensibel. Die IP-Adresse könne zudem der einzige Anhaltspunkt zur Aufklärung einer Straftat sein, etwa im Bereich Kinderpornografie.

Diese Argumentation begegnet vielfältigen Einwänden. Sie ist auf den Gewährleistungsgehalt der **Grundrechte des Grundgesetzes nicht zu übertragen**. Die Vorratsspeicherung der IP-Adresse des Nutzers einer Internet(telefonie-)verbindung oder des Absenders einer E-Mail ist ebenso unverhältnismäßig wie es die Vorratsspeicherung anderer Kennungen ist.

Es ist nicht nachvollziehbar, warum die **Identifizierbarkeit eines Teilnehmers anhand einer IP-Adresse** unter geringeren Voraussetzungen möglich sein soll als seine Identifizierbarkeit

mit Hilfe anderer Verkehrsdaten (z.B. IMEI-Kennung, Zeitpunkt einer Telefonverbindung). Diese Schlechterstellung von Internetverbindungen führt zu unauflösbaren Wertungswidersprüchen: Ruft jemand mit unterdrückter Rufnummer zu einer bekannten Uhrzeit einen bekannten Zielanschluss an, so darf dies nicht auf Vorrat gespeichert werden. Erfolgt der Anruf dagegen unter Verwendung eines anonymen Internettelefondienstes (z.B. Skype), soll die Identifizierung des Anrufers möglich sein. Sendet jemand ohne Rufnummernübermittlung ein Telefax, so darf nicht auf Vorrat gespeichert werden. Wird dasselbe Dokument dagegen über ein anonymes E-Mail-Postfach versandt, soll die Identifizierung des Anschlussinhabers anhand der verwendeten IP-Adresse möglich bleiben. Diese Privilegierung einer Internet-Zielwahlsuche gegenüber einer Telefon-Zielwahlsuche ist sachlich nicht zu rechtfertigen. Auch ist nicht plausibel zu machen, weshalb für „unbedeutende“ Verkehrsdaten zu schon bekannten Verbindungen (z.B. Datenvolumen, Anrufdauer) ein höheres Schutzniveau bestehen soll als für die äußerst grundrechtsbelastende Feststellung der Identität eines noch unbekannten Kommunikationsteilnehmers.

Das Argument des EuGH, **aus der IP-Adresse selbst lasse sich nicht unmittelbar auf den Kommunikationspartner schließen**, überzeugt schon deshalb nicht, weil man mit diesem Argument auch alle Telefonverbindungen auf Vorrat speichern könnte, solange nicht die Rufnummer des Gesprächspartners festgehalten wird. Im Übrigen ist in einer E-Mail, deren Identifizierung der EuGH mittels IP-Vorratsspeicherung ermöglichen will, stets auch der Empfänger festgehalten. Der EuGH stellt allein auf die Art der verarbeiteten Daten ab. Seit dem Volkszählungsurteil ist aber anerkannt, dass für die Eingriffstiefe nicht die Art der verarbeiteten Daten entscheidend ist, sondern deren Nutzbarkeit und Verwendungsmöglichkeit (BVerfGE 65, 1, [45]). Dass die Zuordnung einer IP-Adresse zur Aufdeckung der gesamten Internetnutzung während der maßgeblichen Verbindung genutzt werden kann, erkennt der EuGH selbst an. Die Zuordnung einer dynamischen IP-Adresse kann die inhaltliche Rekonstruktion der gesamten Internetsitzung anhand von Nutzungsdaten (z.B. URL, „Referer“) und somit die Erstellung tiefgreifender Persönlichkeitsprofile ermöglichen, wie sie bei Telefon-Verbindungsdaten nicht erstellt werden können. Sie kann der Aufdeckung eines Pseudonyms dienen, anhand dessen jahrelang ohne Namensnennung veröffentlicht worden ist (z.B. durch einen Whistleblower über soziale Medien). Die für die verfassungsrechtliche Beurteilung entscheidende Nutzbarkeit (BVerfGE 65, 1 [45]) der Zuordnung aller IP-Adressen ist mitnichten weniger grundrechtsbelastend als beispielsweise die eines einzelnen Verbindungsdatensatzes mit Empfängernummer.

Aus IP-Adressen lässt sich im Übrigen ein **Bewegungsprofil** erstellen (vgl. Pitsillidis, Xie, et. al. – *“How to Tell an Airport from a Home: Techniques and Applications”*, abrufbar unter <https://users.soe.ucsc.edu/~abadi/Papers/hotnets10.pdf>).

Dass die IP-Adresse der **einzige Anhaltspunkt zur Aufklärung einer Straftat** sein kann, wie der EuGH anführt, unterscheidet sie nicht von anderen Verbindungsdaten. Auch bei mittels Telefon begangenen Straftaten können Verbindungsdaten der einzige Anhaltspunkt sein. Fakt ist, dass in Deutschland ohne IP-Vorratsdatenspeicherung Internetdelikte laut Kriminalstatistik nicht weniger erfolgreich aufgeklärt werden als sonstige Delikte. Schließlich gibt es außerhalb der Telekommunikationsnetze auch keine „Vorratsspeicherung von Spuren“ nur für den Fall, dass irgendwann einmal ein Strafverfolgungsinteresse entstehen könnte. Nach Inkrafttreten einer IP-Vorratsdatenspeicherung am 01.01.2009 ging die Aufklärungsquote leicht zurück. Dies beruhte darauf, dass eine Vorratsdatenspeicherung Straftäter zum Einsatz von Umgehungsstrategien veranlasst hat (z.B. Postversand von CD-Roms, Internetcafés, offene Netzzugänge, Anonymisierungsdienste, unregistrierte Prepaidkarten, nicht-elektronische Kommunikationskanäle), so dass ihre Kommunikation selbst im Verdachtsfall nicht mehr zu überwachen ist. Es war nicht nachzuweisen, dass eine IP-Vorratsdatenspeicherung einen statistisch signifikanten Beitrag zu der Zahl der aufgeklärten Straftaten leistete.

Auch EU-weite Untersuchungen haben keinen Zusammenhang zwischen Aufklärungsquote und in Kraft befindlicher Vorratsdatenspeicherung belegen können. 2020 kam der Wissenschaftliche Dienst des Europäischen Parlaments zu dem Ergebnis, dass es „nicht möglich zu sein [scheint], einen direkten Zusammenhang zwischen der Tatsache, ob Gesetze zur Vorratsdatenspeicherung bestehen oder nicht, und der Kriminalitätsstatistik herzustellen“ (siehe dazu <https://www.patrick-breyer.de/studie-straerverfolgung-funktioniert-ohne-vorratsdatenspeicherung/>). Auch eine Studie im Auftrag der EU-Kommission zu der Frage, wie häufig Kommunikationsdatenabfragen erfolgreich sind, kommt zu dem Ergebnis: Verkehrsdatenabfragen seien „selten erfolglos“. Zwischen den befragten Ermittlern „aus Mitgliedstaaten mit und ohne verpflichtende Vorratsdatenspeicherung sind nur geringfügige Unterschiede festzustellen“. In Frankreich und Portugal wurde häufiger von erfolglosen Abfragen berichtet als in Deutschland, obwohl dort Gesetze zur Vorratsdatenspeicherung in Kraft sind (European Commission, *„Study on the retention of electronic communications non-content data for law enforcement purposes“*, abrufbar unter: <https://op.europa.eu/en/publication-detail/-/publication/081c7f15-39d3-11eb-b27b-01aa75ed71a1>).

Was schließlich die strafrechtliche Verfolgung von **Kinderpornografie** angeht: Wie vierzehn Personen aus Zivilgesellschaft, Netzgemeinde, Journalismus, Recht und Wissenschaft sowie

eines Vereins von Missbrauchsoffern schon vor Jahren in einem Offenen Brief auseinandergesetzt haben, ist eine Vorratsdatenspeicherung ungeeignet zum Schutz von Kindern (abrufbar unter <https://www.daten-speicherung.de/index.php/intelligente-strategien-fuer-ein-sicheres-netz-ip-vorratsdatenspeicherung-stoppen/#kinder>). Das Max-Planck-Institut für ausländisches und internationales Strafrecht schreibt in seiner vom Bundesjustizministerium beauftragten Studie wörtlich: *„Insbesondere gibt es bislang keinen Hinweis dafür, dass durch eine umfängliche Verfolgung aller Spuren, die auf das Herunterladen von Kinderpornografie hindeuten, sexueller Missbrauch über den Zufall hinaus verhindert werden kann.“* (zitiert nach <http://www.vorratsdatenspeicherung.de/content/view/537/55/lang,de/>; Max-Planck-Institut für ausländisches und internationales Strafrecht, „Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten“, 2011, S. S. 222, 242). Die wenigsten Fälle von Kindesmissbrauch werden also durch Verfolgung von Kinderpornografie aufgeklärt. Umgekehrt gilt, dass anonyme Kommunikation Kinder schützt, indem sie anonyme Beratung, Selbsthilfe und Anzeigen ermöglicht.

Laut Max-Planck-Institut für ausländisches und internationales Strafrecht erfolgen weniger als 5% der staatlichen IP-Auskunftsersuchen wegen eines Verdachts des Austauschs kinder- oder jugendpornografischer Darstellungen über das Internet (BT-Drs. 16/8434, S. 78). Auch nach der polizeilichen Kriminalstatistik 2020 betreffen nur 5% der polizeilichen Ermittlungen wegen Internetdelikten Fälle des Austauschs kinder- oder jugendpornografischer Darstellungen im Internet.

Im Jahr 2020 wurde die Verbreitung kinderpornografischer Schriften laut Kriminalstatistik zu 92,6% aufgeklärt – ohne eine Pflicht zur IP-Vorratsdatenspeicherung (Polizeiliche Kriminalstatistik 2020 – Ausgewählte Zahlen im Überblick, 2021, S. 14, Schlüssel 143200). Eine signifikante Steigerung im Fall einer IP-Vorratsdatenspeicherung ist – auch angesichts vielfältiger Umgehungsmöglichkeiten – nicht zu erwarten. Eher ist umgekehrt ein Ausweichverhalten und damit eine zurückgehende Aufklärungsquote zu erwarten.

Eine generelle und undifferenzierte Vorratsspeicherung unserer Identität im Internet zöge gerade das vom Bundesverfassungsgericht angesprochene **diffus bedrohliche Gefühl des Beobachtetseins** nach sich. Sie erfasst nämlich Internetverbindungen, die unter der Erwartung von Anonymität hergestellt werden. Bereits im Jahr 2009 nach Inkrafttreten der letzten IP-Vorratsdatenspeicherung gaben 46% der Bürger an, einen Internet-Anonymisierungsdienst zu nutzen oder nutzen zu wollen (infas-Umfrage im Oktober 2009, abrufbar unter <http://www.vorratsdatenspeicherung.de/images/infas-umfrage.pdf>), was sich nur durch ein hohes Anonymitätsinteresse erklären lässt.

Eine generelle und undifferenzierte Vorratsspeicherung würde das **Ende der Anonymität im Internet** bedeuten. der Sie würde es unmöglich machen, das Internet frei vom Risiko staatlicher Beobachtung (z.B. auch wegen eines falschen Verdachts), missbräuchlicher Offenlegung durch Mitarbeiter des Anbieters und versehentlichen Datenverlustes (z.B. wie bei T-Mobile geschehen) zu nutzen. Dadurch hätte auch eine IP-Vorratsdatenspeicherung unzumutbare Folgen, gerade in dem Bereich, in dem Menschen nur im Schutz der Anonymität überhaupt bereit sind, sich in einer Notsituation beraten und helfen zu lassen (z.B. Opfer und Täter von Gewalt- oder Sexualdelikten), ihre Meinung trotz öffentlichen Drucks zu äußern oder Missstände bekannt zu machen (Presseinformanten, anonyme Strafanzeigen, ausländische Dissidenten).

Nur höchst hilfsweise für den Fall, dass das Gericht all dem nicht folgen will, sei angeführt, dass es sich bei dem vom EuGH angesprochenen auf „das absolut Notwendige begrenzten Zeitraum“ um keinen längeren Zeitraum als sieben Tage handeln kann. Bereits mit der „freiwilligen Vorratsdatenspeicherung“ deutscher Internetzugangsanbieter für sieben Tage zur „Störungserkennung“ wird eine beträchtliche Aufklärungsquote bei Internetdelikten erreicht, die sich erfahrungsgemäß durch eine längere Speicherdauer nicht signifikant steigern ließe.

Fazit

Wie auch die §§ 113b Abs. 1 – 4 und 8 TKG a.F. sowie § 113c Abs. 1 TKG a.F. sind die (neu nummerierten und lediglich redaktionell angepassten) Regelungen in §§ 176 Abs. 1-4 und 8 sowie 177 Abs. 1 TKG aus den in der Ausgangsbeschwerdeschrift dargelegten Gründen mit Artikel 10, Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1, und Artikel 5 Abs. 1 des Grundgesetzes unvereinbar.



Prof. Dr. Frank Braun