

**Deutscher Bundestag**  
Ausschuss für Inneres und Heimat

Ausschussdrucksache  
**19(4)696 A**

JOHANNES GUTENBERG  
UNIVERSITÄT MAINZ



JOHANNES GUTENBERG-UNIVERSITÄT MAINZ - 55099 Mainz

FACHBEREICH 03  
JURA  
Lehrstuhl für Öffentliches Recht  
und Informationsrecht, insbe-  
sondere Datenschutzrecht

Universitätsprofessor  
Dr. Matthias Bäcker

Johannes Gutenberg-  
Universität Mainz  
Jakob-Welder-Weg 9  
55128 Mainz

Tel. +49 6131 39 28173  
Fax +49 6131 39 28172

matthias.baecker@uni-mainz.de  
www.baecker.jura.uni-mainz.de/

## Stellungnahme

zu dem Entwurf eines Gesetzes zur Anpassung der Regelungen über  
die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung  
des Bundesverfassungsgerichts vom 27. Mai 2020

(BT-Drs. 19/25294)

## Gliederung

Ergebnisse .....	3
I. Übermittlung von und Zugriff auf Telemediendaten .....	4
1. Vorklärungen.....	4
a) Differenzierung und Abgrenzung von Telemedien und Telekommunikation .....	4
b) Kategorien und Sensibilität von Telemediendaten.....	6
2. Übermittlung von und Zugriff auf Bestandsdaten .....	10
3. Übermittlung von und Zugriff auf Nutzungsdaten .....	11
4. Inhaltsüberwachung von Telemedien.....	12
II. Zuordnung dynamischer IP-Adressen .....	13

## Ergebnisse

1. Die vorgesehenen Regelungen zur Übermittlung von und zum sicherheitsbehördlichen Zugriff auf Telemediendaten verfehlen teilweise die verfassungsrechtlichen Anforderungen.
  - a) Die Erlaubnisse zur Übermittlung von Telemedien-Bestandsdaten in § 15a Abs. 1 Satz 1, Abs. 3 TMG-E tragen der spezifischen Sensibilität dieser Datenkategorie, die sie von Telekommunikations-Bestandsdaten abhebt, nicht hinreichend Rechnung. Unverhältnismäßig sind zumindest die Erlaubnisse, Telemedien-Bestandsdaten zur Abwehr einfacher Gefahren für die öffentliche Sicherheit und zur Verfolgung beliebiger Straftaten und Ordnungswidrigkeiten zu übermitteln. Ebenso unverhältnismäßig sind zumindest die korrespondierenden Zugriffsermächtigungen in § 22a Abs. 1 Satz 1 Nr. 2 BPolG-E, § 10 Abs. 1 Satz 1 und § 30 Abs. 1 Satz 1 ZFdG-E sowie § 100j Abs. 1 Satz 1 Nr. 2 StPO-E i.V.m. § 46 Abs. 1 OWiG.
  - b) Erst recht unverhältnismäßig sind § 15a Abs. 1 Satz 1, Abs. 3 TMG-E, soweit diese Regelungen auch die Übermittlung von Telemedien-Nutzungsdaten zulassen, die intensiver in Grundrechte eingreift als die Übermittlung von Telemedien-Bestandsdaten. Ungeachtet ihrer etwas strengeren Fassung bestehen auch gegen die vorgesehene strafprozessuale Zugriffsermächtigung in § 100g Abs. 1 Satz 2 StPO-E verfassungsrechtliche Bedenken, da sie der potenziell hohen Sensibilität dieser Datenkategorie nicht vollumfänglich Rechnung trägt.
2. In dem Entwurf fehlen Ermächtigungen zur Inhaltsüberwachung von Telemedien. Solche Ermächtigungen sind nicht etwa deshalb entbehrlich, weil Überwachungen auf die Ermächtigungen der Sicherheitsbehörden zu Telekommunikationsüberwachungen (etwa in § 100a StPO) gestützt werden könnten. Die Übermittlung von und der Zugriff auf Telemedieninhalte und Telemedien-Nutzungsdaten sollten stattdessen einheitlich geregelt werden, um fruchtlose Abgrenzungsschwierigkeiten zwischen beiden Datenkategorien zu vermeiden. Wegen der hohen Sensibilität sowohl von Nutzungsdaten als auch von Inhalten sollten diese Eingriffe an die für Telekommunikationsüberwachungen geltenden Voraussetzungen gebunden werden.
3. Die in § 113 Abs. 1 Satz 3, Abs. 3 und Abs. 5 TKG-E enthaltenen Erlaubnisse zur Übermittlung von Bestandsdaten, die durch die Zuordnung einer dynamischen IP-Adresse ermittelt wurden, verletzen unionsrechtliche Vorgaben, soweit für die Zuordnung Vorratsdaten (§§ 113a ff. TKG) verarbeitet werden dürfen.

4 Der Gesetzentwurf behebt im Wesentlichen die Mängel des geltenden Telekommunikationsrechts und des Fachrechts der Sicherheitsbehörden, die das Bundesverfassungsgericht in seinem zweiten Bestandsdatenbeschluss vom 27. Mai 2020 (Az. 1 BvR 1873/13) aufgezeigt hat.

Gleichwohl stehen einige der vorgesehenen Regelungen mit höherrangigem Recht nicht in Einklang. Hierfür gibt es zwei Gründe: Erstens trägt der Gesetzentwurf der spezifischen Sensibilität von Telemediendaten nur unzureichend Rechnung (unten I). Zweitens entspricht die gesetzliche Erlaubnis zur Auflösung dynamischer IP-Adressen unter Verwendung bevorrateter Telekommunikations-Verkehrsdaten zwar den verfassungsrechtlichen Maßstäben des zweiten Bestandsdatenbeschlusses. Sie verfehlt jedoch die strengeren unionsrechtlichen Anforderungen, die der Gerichtshof der Europäischen Union in seinem dritten Vorratsdatenurteil vom 6. Oktober 2020 (Rs. C-511/18, C-512/18 und C-520 – La Quadrature du Net u.a.) herausgearbeitet hat.

## **I. Übermittlung von und Zugriff auf Telemediendaten<sup>1</sup>**

Im Anschluss an das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität enthält der Entwurf Regelungen zur Übermittlung von Kundendaten durch die Anbieter von Telemediendiensten an Sicherheitsbehörden sowie zum behördlichen Zugriff auf diese Daten.<sup>2</sup> Diese Regelungen knüpfen überwiegend an die Regelungen zur Übermittlung von und zum Zugriff auf Telekommunikationsdaten an. Dieser Regelungsansatz wird jedoch der spezifischen Sensibilität von Telemediendaten nicht gerecht.

### **1. Vorklärungen**

Um die verfassungsrechtlichen Mängel der vorgesehenen Übermittlungserlaubnisse und Zugriffsermächtigungen herauszuarbeiten, muss vorab geklärt werden, wie sich Telemediens- und Telekommunikationsdienste voneinander abgrenzen, welche Datenkategorien es für beide Diensttypen gibt und als wie sensibel Telemediendaten im Vergleich zu Telekommunikationsdaten anzusehen sind.

#### **a) Differenzierung und Abgrenzung von Telemedien und Telekommunikation**

Den Regelungen des Entwurfs liegt die in § 1 Abs. 1 Satz 1 TMG i.V.m. § 3 Nr. 24 TKG geregelte Differenzierung zwischen Telemediens- und Telekommunikationsdiensten zugrunde. Weil es sich um rechtlich getrennte Arten von Kommunikationsdiensten handelt, werden auch die Übermittlung der bei den Diensteanbietern anfallenden Daten an Sicherheitsbehörden sowie der behördliche Zugriff auf diese Daten ausdrücklich voneinander unterschieden.

---

<sup>1</sup> Die folgenden Ausführungen beruhen teilweise auf meiner Stellungnahme zu dem Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vom 4. Mai 2020. Ich habe sie jedoch an die zwischenzeitliche Entwicklung angepasst und meine früheren Positionen teils revidiert.

<sup>2</sup> Das sog. Doppeltürmodell, das diesem Regelungsansatz zugrunde liegt, wird im Folgenden als bekannt vorausgesetzt.

<sup>5</sup> Die Differenzierung zwischen beiden Dienstetypen hat eine Wurzel im Unionsrecht, da der Begriff des Telekommunikationsdienstes auf Art. 2 lit. c der früheren Rahmenrichtlinie für die elektronische Kommunikation<sup>3</sup> beruht. Der Gerichtshof der Europäischen Union hat diese Norm eng ausgelegt, sodass viele verbreitete internetbasierte Kommunikationsdienste nicht unter den unionsrechtlichen Begriff des elektronischen Kommunikationsdienstes fallen, da sie nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen. Konkret entschieden hat der Gerichtshof dies für E-Mail-Dienste.<sup>4</sup> Ebenso dürften zahlreiche weitere sogenannte Over-the-Top-Dienste zu behandeln sein, etwa Messengerdienste wie WhatsApp oder Soziale Medien wie Facebook (letztere auch insoweit, als sie Funktionen für den Nachrichtenaustausch zwischen Individuen enthalten). Solche Kommunikationsdienste sind dementsprechend nach gegenwärtigem Recht als Telemediendienste einzustufen.

Die Übermittlungserlaubnisse für Diensteanbieter, die das Telekommunikationsrecht enthält, können nicht auf Telemedienanbieter angewandt werden. Zudem beschränkt sich der Anwendungsbereich einiger Überwachungsermächtigungen im geltenden Sicherheitsrecht auf Datenerhebungen mit Bezug zur Telekommunikation im telekommunikationsrechtlichen Sinne. Es bedarf daher für telemedienbezogene Überwachungsmaßnahmen spezifischer Rechtsgrundlagen für die Übermittlung von Telemediendaten an Sicherheitsbehörden und den behördlichen Zugriff auf solche Daten. Der Entwurf soll solche Regelungen schaffen und dabei einen prinzipiellen Gleichlauf zwischen telekommunikations- und telemedienbezogenen Überwachungsmaßnahmen herstellen.

Die Begrifflichkeiten werden sich voraussichtlich in naher Zukunft verschieben. Der die frühere Rahmenrichtlinie ablösende Kommunikationskodex<sup>5</sup> hat den Anwendungsbereich des europäischen Telekommunikationsrechts neu gefasst. Gemäß Art. 2 Nr. 4 Kommunikationskodex umfasst der zentrale Begriff des elektronischen Kommunikationsdienstes nunmehr unter anderem interpersonelle Kommunikationsdienste, die über elektronische Kommunikationsnetze erbracht werden. Es kommt nicht mehr darauf an, ob solche Dienste ganz oder überwiegend in der Übertragung von Signalen bestehen. Dementsprechend sieht der aktuelle Entwurf eines Telekommunikationsmodernisierungsgesetzes<sup>6</sup> in § 3 Nr. 61 TKG-E eine entsprechende Erweiterung des deutschen Begriffs des Telekommunikationsdienstes vor. Sollte dieser Entwurf in Kraft treten,

---

<sup>3</sup> Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), ABl. L 108 vom 24. April 2002, S. 33, zuletzt geändert durch die Richtlinie 2009/140/EG vom 25. November 2009, ABl. L 337 vom 18. Dezember 2009, S. 37.

<sup>4</sup> EuGH, Urteil vom 13. Juni 2019, Rs. C-193/18 – Google LLC gegen Bundesrepublik Deutschland.

<sup>5</sup> Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation, ABl. L 321 vom 17. Dezember 2018, S. 36.

<sup>6</sup> Entwurf eines Gesetzes 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 (Telekommunikationsmodernisierungsgesetz), BR-Drs. 29/21.

<sup>6</sup> so wird sich der Begriff des Telekommunikationsdienstes erweitern und der Begriff des Telemediendienstes entsprechend verengen.<sup>7</sup> Dementsprechend werden zukünftig die Übermittlung von und der behördliche Zugriff auf Daten aus interpersonellen Over-the-Top-Kommunikationsdiensten auf die Regelungen zu stützen sein, die sich auf Telekommunikationsdaten beziehen. Die praktische Relevanz der im vorliegenden Entwurf vorgesehenen Regelungen zu Telemediendaten wird sich damit deutlich vermindern.

Der voraussichtlich in Zukunft maßgebliche Begriff des interpersonellen Kommunikationsdienstes wird in § 3 Nr. 24 TKG-E legaldefiniert als

„ein gewöhnlich gegen Entgelt erbrachter Dienst, der einen direkten interpersonellen und interaktiven Informationsaustausch über Telekommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Telekommunikation veranlassen oder daran beteiligt sind; dazu zählen keine Dienste, die eine interpersonelle und interaktive Telekommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen.“

Diese Legaldefinition birgt nicht unbeträchtliche Interpretations- und Abgrenzungsprobleme, was angesichts der nahezu unüberschaubaren Vielfalt netzbasierter Kommunikationsdienste nicht überrascht. Klar als interpersonelle Kommunikationsdienste sind etwa E-Mail- oder auf den Austausch zwischen Einzelpersonen beschränkte Messengerdienste einzustufen. Öffentlich einsehbare Profile auf Sozialen Netzwerken unterfallen dem Begriff hingegen nicht. Abgrenzungsschwierigkeiten dürften zum einen bei Kommunikationsdiensten entstehen, die hinsichtlich der Adressaten von Nachrichten Konfigurationsmöglichkeiten eröffnen. So liegt es etwa, wenn ein Messengerdienst ermöglicht, Nachrichten über einen abonnierbaren Nachrichtenkanal an eine große oder sogar zahlenmäßig unbegrenzte Gruppe von Empfängern zu versenden, oder wenn ein Soziales Netzwerk ermöglicht, den Empfängerkreis von Veröffentlichungen auf einen abgegrenzten Personenkreis zu beschränken. Zum anderen stellt sich die Frage, wann genau eine interpersonelle Kommunikationsmöglichkeit als untrennbare und untergeordnete Nebenfunktion eines anderen Dienstes anzusehen ist. Diese Frage könnte etwa für Chatfunktionen von Online-Versandhändlern oder für Kommunikationskanäle von Online-Spielen relevant werden.<sup>8</sup>

### **b) Kategorien und Sensibilität von Telemediendaten<sup>9</sup>**

Der Entwurf verfolgt den Regulierungsansatz, Telekommunikations- und Telemediendienste hinsichtlich der Übermittlung von Kommunikationsdaten an Sicherheitsbehörden und des behördlichen Zugriffs auf solche Daten weitgehend gleichzubehandeln. Eine solche Parallelisierung beider Dienstetypen fand sich schon bislang (zumindest teilweise) in einigen Fachgesetzen der

---

<sup>7</sup> Kiparski, CR 2019, S. 179 (180).

<sup>8</sup> Vgl. Erwägungsgrund 17 zum Kommunikationskodex

<sup>9</sup> Außer Betracht bleiben im Folgenden Zugangsdaten, die nach dem Entwurf bei Telemediendiensten einem höheren Schutzniveau unterliegen sollen als bei Telekommunikationsdiensten. Hiergegen bestehen meines Erachtens keine verfassungsrechtlichen Bedenken.

7 Sicherheitsbehörden.<sup>10</sup> Ihre Überzeugungskraft hängt allerdings maßgeblich davon ab, inwieweit sich für Telekommunikations- und Telemediendienste vergleichbare Datenkategorien bilden lassen, hinsichtlich derer einem behördlichen Zugriff eine vergleichbare Eingriffsintensität zukommt.

Das Telekommunikations- und das Telemedienrecht kennen gleichermaßen die Datenkategorie der Bestandsdaten.<sup>11</sup> Hierbei handelt es sich jeweils um Daten, die für „die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses“ zwischen dem Diensteanbieter und dem Nutzer benötigt werden. Bestandsdaten sind mithin Basisdaten eines Nutzungsvertrags, die sich nicht auf einen konkreten Kommunikationsvorgang beziehen. Beispiele bilden Name, Anschrift oder Bankverbindung des Nutzers. Die Sensibilität von Telekommunikations-Bestandsdaten und Telemedien-Bestandsdaten erscheint auf den ersten Blick ohne weiteres vergleichbar.<sup>12</sup> Bei näherer Betrachtung erweist sich diese Bewertung jedoch als fragwürdig.

Telekommunikations-Bestandsdaten sind für sich genommen wenig sensibel. Insbesondere ist die Information, dass eine bestimmte Person von einem bestimmten Telekommunikationsdienst Gebrauch macht, bei isolierter Betrachtung weitgehend banal. Denn Telekommunikationsdienste werden von nahezu jedermann genutzt. Zudem sind die Angebote unterschiedlicher Diensteanbieter funktional weitgehend austauschbar. Die Nutzung eines bestimmten Dienstes eines bestimmten Anbieters sagt darum über sensible Umstände wie persönliche Eigenschaften oder Vorlieben der Nutzerin sowie über die möglichen Kommunikationsinhalte kaum etwas aus.<sup>13</sup> Eine gesteigerte Sensibilität erlangen Telekommunikations-Bestandsdaten erst im Zusammenwirken mit anderen Informationen, etwa indem die Telefonnummer, von der ein inkriminierender Anruf ausging, dem Anschlussinhaber zugeordnet wird.

Hingegen umfasst der Begriff des Telemediendienstes nicht nur weit verbreitete und inhaltlich neutrale Kommunikationsdienste, sondern auch zahlreiche Dienste, bei denen schon der Umstand der Nutzung Schlussfolgerungen von hoher Sensibilität ermöglicht. Beispielhaft sei die Nutzung eines webbasierten Forums oder einer Gruppe auf einem Sozialen Netzwerk genannt, in denen sich Betroffene über bestimmte Krankheiten austauschen. Zudem können sich Telemedien-Bestandsdaten auf mehr und persönlichkeitsrelevantere Informationen erstrecken als Telekommunikations-Bestandsdaten, etwa wenn ein Telemediendienst darauf beruht, den Nutzern personalisierte Angebote aufgrund eines zu Beginn des Vertragsverhältnisses erstellten Interessenprofils zu unterbreiten. Hierbei handelt es sich auch nicht nur um vernachlässigbare Sonderfälle, sondern eine durchaus beträchtliche Teilmenge aller Telemedien, vor allem wenn

---

<sup>10</sup> Vgl. beispielhaft für den Zugriff auf Telekommunikations-Verkehrsdaten und Telemedien-Nutzungsdaten § 52 BKAG. Hingegen enthält das BKAG bislang keine ausdrückliche Ermächtigung zur Erhebung von Telemedien-Bestandsdaten.

<sup>11</sup> § 3 Nr. 3 TKG (§ 3 Nr. 6 TKG-E); § 14 Abs. 1 TMG.

<sup>12</sup> So noch meine Stellungnahme zu dem Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vom 4. Mai 2020.

<sup>13</sup> Dies gilt auch noch, wenn nach zukünftigem Recht die Nutzung interpersoneller Over-the-Top-Dienste wie E-Mail oder Instant Messaging einbezogen wird, da es sich hierbei zumindest in der Regel gleichfalls um weit verbreitete, inhaltlich neutrale und untereinander substituierbare Dienste handelt.

<sup>8</sup> zukünftig die der Individualkommunikation dienenden Over-the-Top-Dienste als Telekommunikationsdienste eingestuft werden. Derartige Telemedien von erhöhter Persönlichkeitsrelevanz müssen bei einer typisierenden Einschätzung der Sensibilität von Telemedien-Bestandsdaten berücksichtigt werden. Auch wenn es für Telemedien-Bestandsdaten anders als für Telekommunikations-Bestandsdaten<sup>14</sup> keine gesetzliche Bevorratungspflicht gibt,<sup>15</sup> weisen daher die Übermittlung von und der Zugriff auf Telemedien-Bestandsdaten bei abstrakt-genereller Betrachtung eine im Vergleich zu Telekommunikations-Bestandsdaten erhöhte Eingriffsintensität auf.<sup>16</sup>

Im Telekommunikationsrecht werden des Weiteren zwei Kategorien von Daten unterschieden, die sich jeweils auf konkrete Kommunikationsvorgänge beziehen. Dabei handelt es sich zum einen um die Kommunikationsinhalte, zum anderen um die Verkehrsdaten, also Metadaten der Kommunikation, die „bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden.“<sup>17</sup> Aus Verkehrsdaten ergibt sich beispielsweise die Information, zwischen welchen Rufnummern zu welcher Zeit ein Telefongespräch geführt wurde. Das geltende Sicherheitsrecht enthält uneinheitliche Wertungen dazu, inwieweit sich die Sensibilität beider Datenkategorien vergleichen lässt. Teilweise werden Zugriffe auf Telekommunikations-Verkehrsdaten und Inhaltsüberwachungen der Telekommunikation an dieselbe Eingriffsschwelle gebunden (so etwa § 51 Abs. 1 und § 52 Abs. 1 BKAG). Teilweise wird hingegen der Zugriff auf Telekommunikations-Verkehrsdaten wegen deren – vermeintlich – geringerer Sensibilität unter weniger strengen Voraussetzungen ermöglicht als Inhaltsüberwachungen der Telekommunikation (etwa in § 100a Abs. 1 und § 100g Abs. 1 StPO).

Schwieriger und kontroverser ist die Kategorisierung von Telemediendaten. Das Telemedierecht nennt ausdrücklich neben den Bestandsdaten nur die Nutzungsdaten als weitere Datenkategorie. Hierbei handelt es sich gemäß § 15 Abs. 1 TMG um Daten, die erforderlich sind, „um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen“. Beispielhaft nennt das Gesetz Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie den Umfang der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien. Die Telemedien-Nutzungsdaten entsprechen damit – zumindest auf den ersten Blick – den Telekommunikations-Verkehrsdaten. Hiervon geht auch der Entwurf erkennbar aus.

Hingegen findet sich im Telemedierecht keine Datenkategorie, die den Inhalten der Telekommunikation entspräche. Dabei ist offenkundig, dass es auch Telemedieninhalte gibt, die sich kaum als Metadaten der Telemediennutzung begreifen lassen. Bestellt beispielsweise jemand Waren bei einem Online-Versandhändler, so sind die im Rahmen der Bestellung anfallenden technischen Metadaten (beispielsweise die IP-Adresse, unter der die Bestellung aufgegeben

---

<sup>14</sup> Vgl. § 111 TKG.

<sup>15</sup> Vgl. zu diesem Gesichtspunkt und seiner Bedeutung für die Eingriffsintensität von Datenübermittlung und Datenzugriff BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 –, Rn. 139.

<sup>16</sup> Anders wegen des Fehlens einer Bevorratungspflicht noch mein im Auftrag der Bundestagsfraktion Bündnis 90/Die Grünen erstelltes Rechtsgutachten vom 16. September 2020.

<sup>17</sup> § 3 Nr. 30 TKG (ähnlich § 3 Nr. 70 TKG-E).

<sup>9</sup> wird, oder die Uhrzeit der Bestellung) Nutzungsdaten. Die Angabe, welche Waren der Nutzer bestellt hat, ist hingegen kein auf das Telemedium (die Website des Versandhändlers) bezogenes Nutzungsdatum, sondern ein mithilfe des Telemediums transportiertes Datum, das sich auf den abgeschlossenen Kaufvertrag bezieht. Bei den der Individualkommunikation dienenden Over-the-Top-Diensten wie E-Mail oder Instant Messaging erscheint es zumindest fragwürdig, ob sich die übermittelten Nachrichten als Nutzungsdaten einordnen lassen. Gleiches gilt etwa für Kommunikationsinhalte, die auf einer Profilseite bei einem Sozialen Netzwerk veröffentlicht werden.<sup>18</sup>

Ob Telemedien-Inhaltsdaten als eigenständige Datenkategorie anzuerkennen und wie sie zu behandeln sind, war lange umstritten. Teils wurde eine direkte oder analoge Anwendung der Vorschriften über Nutzungsdaten vertreten. Nach der Gegenauffassung sollte die Verarbeitung der Inhaltsdaten nach allgemeinem Datenschutzrecht zu beurteilen sein – mit der Konsequenz eines im Vergleich zu Nutzungsdaten schwächeren Schutzes. Der Streit wird heute vielfach für überwunden gehalten, da Telemediendaten spätestens seit Inkrafttreten des novellierten europäischen Rechtsrahmens generell dem allgemeinen Datenschutzrecht unterfielen und die Datenschutzregelungen des Telemedienrechts wegen des Anwendungsvorrangs der DSGVO unanwendbar seien.<sup>19</sup> Dies dürfte für Datenverarbeitungen durch den Telemedienanbieter zu eigenen Zwecken zutreffen, gilt jedoch nicht für die zweckändernde Übermittlung von Telemediendaten an eine Sicherheitsbehörde sowie für den sicherheitsbehördlichen Zugriff auf die Daten. Hinsichtlich dieser Datenverarbeitungen bestehen mitgliedstaatliche Regelungsspielräume.<sup>20</sup> Zur Ausfüllung dieser Spielräume könnte durchaus zwischen Nutzungs- und Inhaltsdaten differenziert werden.

Die Abgrenzung dieser Datenkategorien bereitet allerdings im Detail erheblich größere Schwierigkeiten als die Abgrenzung zwischen Telekommunikationsinhalten und Telekommunikations-Verkehrsdaten. Grund hierfür ist, dass der Telemedienbegriff sich auf eine viel größere Zahl unterschiedlicher Dienste mit unterschiedlichen Funktionen und Wirkungsweisen bezieht. Eine statische Webseite im World Wide Web, die lediglich zum Leseabruf zur Verfügung steht, ist ebenso ein Telemedium wie ein E-Mail-Dienst, ein Online-Versandhandel oder ein Onlinespiel. Zudem ist der Telemedienbegriff unterschiedlichen Abstraktionsstufen zugänglich und kann darum über- und untergeordnete Dienste gleichermaßen umfassen. Beispielsweise lässt sich ein Soziales Netzwerk in seiner Gesamtheit ebenso als Telemedium einstufen wie eine einzelne auf diesem Netzwerk betriebene Profilseite eines Unternehmens. Je nach Dienst können Nutzungs- und Inhaltsebene verschwimmen (so beim Abruf der statischen Webseite). Denkbar ist auch, dieselben Daten für einen Dienst als Nutzungs- und für einen anderen Dienst als Inhaltsdaten

---

<sup>18</sup> Für eine Subsumtion solcher Kommunikationsinhalte unter § 15 TMG etwa Schmitz, in: Spindler/ders., TMG, 2. Aufl. 2018, § 15 Rn. 83.

<sup>19</sup> Schmitz, in: Spindler/ders., TMG, 2. Aufl. 2018, § 15 Rn. 84; Tinnefeld/Buchner, in: BeckOK DatenschutzR, Stand 2019, Syst. I Rn. 91 ff.

<sup>20</sup> Für die Übermittlung aus Art. 6 Abs. 1 lit. c, Abs. 3 sowie aus Art. 6 Abs. 4 i.V.m. Art. 23 Abs. 1 lit. a, c oder d DSGVO; für den Datenzugriff – soweit er nicht dem Anwendungsbereich des europäischen Datenschutzrechts ohnehin vollständig entzogen ist – aus Art. 8 RL (EU) 2016/680.

<sup>10</sup> einzustufen (so etwa, wenn ein Besucher eine Nachricht auf der Profildate eines Sportartikelherstellers in einem Sozialen Netzwerk hinterlässt – möglicherweise Inhaltsdatum im Verhältnis zu dem Sportartikelhersteller, an den sich die Nachricht richtet, möglicherweise Nutzungsdatum im Verhältnis zu dem Netzwerkbetreiber, der die Kommunikationsinfrastruktur bereitstellt).

Zudem liegt nahe, dass Nutzungsdaten und Kommunikationsinhalte je nach Telemediendienst unterschiedlich sensibel sein können. Die Information, dass jemand einen bestimmten Dienst genutzt und bestimmte Inhalte erzeugt oder auf sie zugegriffen hat, kann aussagekräftiger und für die betroffene Person kritischer sein als die Inhalte selbst (beispielsweise bei der Nutzung eines webbasierten Diskussionsforums, bei dem die Inhalte, nicht aber die Nutzungsdaten öffentlich zugänglich sind). In anderen Fällen erscheinen die Inhalte zumindest tendenziell sensibler als die Nutzungsdaten (beispielsweise bei Over-the-Top-Diensten, die der Individualkommunikation dienen, wie E-Mail oder Instant Messaging, sofern hier zwischen Nutzungs- und Inhaltsdaten unterschieden wird).

## **2. Übermittlung von und Zugriff auf Bestandsdaten**

Aufgrund dieser Überlegungen unterliegen die Erlaubnisse zur Übermittlung von Telemedien-Bestandsdaten in § 15a Abs. 1 Satz 1, Abs. 3 TMG-E und die zugehörigen Zugriffsermächtigungen teilweise verfassungsrechtlichen Zweifeln.

Die Übermittlungserlaubnisse in § 15a Abs. 3 TMG-E sind weitgehend identisch mit den Erlaubnissen zur Übermittlung von Telekommunikations-Bestandsdaten in § 113 Abs. 3 TKG-E, die sich ihrerseits an den in den Bestandsdatenbeschlüssen des Bundesverfassungsgerichts formulierten (Mindest-)Anforderungen orientieren. Diese Parallelführung trägt der erhöhten Sensibilität von Telemedien-Bestandsdaten und dem damit einhergehenden erhöhten Eingriffsgewicht der Datenübermittlung nicht Rechnung.

Das erhöhte Eingriffsgewicht der Übermittlung von Telemedien-Bestandsdaten muss sich in den Voraussetzungen der Datenübermittlung und des Datenzugriffs niederschlagen. Insbesondere müssen die Anforderungen an die hiermit verfolgten materiellen öffentlichen Interesse qualifiziert werden. Zwar ist in einer Übermittlung von Telemedien-Bestandsdaten an eine Sicherheitsbehörde und dem anschließenden Datenzugriff noch kein Grundrechtseingriff von hoher Intensität zu sehen, an den vergleichbare Anforderungen wie etwa an Inhaltsüberwachungen der Telekommunikation oder an die Übermittlung von Telekommunikations-Verkehrsdaten zu stellen wären. Gleichwohl wiegt nicht der gesamte Aufgabenkreis der Sicherheitsbehörden schwer genug, um diesen Grundrechtseingriff materiell zu legitimieren. Zu weit geht die vorgesehene Übermittlungserlaubnis zumindest insoweit, als sie die Datenübermittlung zur Verfolgung jeglicher Ordnungswidrigkeiten (§ 15a Abs. 3 Nr. 1 TMG-E) oder zur Abwehr sämtlicher Gefahren für die öffentliche Sicherheit (§ 15a Abs. 3 Nr. 2 lit. a, Nr. 4 lit. b aa TMG-E) zulässt.

Gleichfalls nicht in vollem Umfang tragfähig sind die in dem Entwurf enthaltenen Ermächtigungen zum Zugriff auf Telemedien-Bestandsdaten. Zu weit reichen zumindest die präventiv ausgerichteten Ermächtigungen in § 22a Abs. 1 Satz 1 Nr. 2 BPolG-E sowie § 10 Abs. 1 Satz 1 und § 30 Abs. 1 Satz 1 ZFdG-E, die Bestandsdatenabrufe zur Abwehr einer einfachen konkreten Gefahr für die öffentliche Sicherheit zulassen. Ebenfalls verfassungsrechtlich nicht tragfähig ist

<sup>11</sup> die strafprozessuale Ermächtigung in § 100j Abs. 1 Satz 1 Nr. 2 StPO-E, soweit diese Norm im Zusammenwirken mit § 46 Abs. 1 OWiG den Zugriff auf Telemedien-Bestandsdaten generell zur Verfolgung von Ordnungswidrigkeiten erlaubt, sowie in

### **3. Übermittlung von und Zugriff auf Nutzungsdaten**

Zu weit gefasst sind die Übermittlungserlaubnisse in § 15a Abs. 1 Satz 1, Abs. 3 TMG-E erst recht insoweit, als diese Vorschrift eine Übermittlung auch von Telemedien-Nutzungsdaten erlaubt. Daten dieser Kategorie sind zumindest in der Regel erheblich sensibler als Bestandsdaten. Eine Übermittlung kann darum nicht generell durch weit gefasste Zwecke wie beispielsweise die Verfolgung von (irgendwelchen) Straftaten oder gar Ordnungswidrigkeiten (§ 15a Abs. 3 Nr. 1 TMG-E) oder die Abwehr von Gefahren für die öffentliche Sicherheit und damit von beliebigen rechtswidrigen Handlungen (§ 15a Abs. 3 Nr. 2 lit. a, Nr. 4 lit. b aa TMG-E) legitimiert werden. Auch etwa Datenübermittlungen zu nachrichtendienstlichen Zwecken (§ 15a Abs. 3 Nr. 6-8 TMG-E) bedürfen angesichts der hohen Sensibilität von Nutzungsdaten und ungeachtet des generell hohen Gewichts der Schutzgüter des Nachrichtendienstrechts<sup>21</sup> eines materiell qualifizierten Erlaubnistatbestands.

Folgerichtig enthalten die bundesrechtlichen Fachgesetze der Sicherheitsbehörden, soweit sie den Zugriff auf Telemedien-Nutzungsdaten regeln, durchweg materiell qualifizierte Eingriffsvoraussetzungen.<sup>22</sup> Die weit gefassten Übermittlungserlaubnisse des Gesetzentwurfs stehen zu diesen Zugriffsermächtigungen in einem Wertungswiderspruch. Gleichfalls wertungswiderprüchlich ist, dass § 15a Abs. 4 TMG-E für eine Bestandsdatenübermittlung anhand einer dynamischen IP-Adresse – also eines Nutzungsdatums – höhere Anforderungen errichtet als für die Übermittlung des verwendeten Nutzungsdatums selbst. Die enger gefassten fachrechtlichen Zugriffsermächtigungen können die Mängel der zu weiten Übermittlungserlaubnisse jedenfalls insoweit nicht beheben, als diese auch Datenübermittlungen an Landessicherheitsbehörden zulassen. Soweit § 15a Abs. 1 Satz 1, Abs. 3 TMG-E die Übermittlung von Telemedien-Nutzungsdaten zulässt, ist die Norm daher zumindest teilweise verfassungswidrig.

Verfassungsrechtlich zweifelhaft ist darüber hinaus die vorgesehene strafprozessuale Ermächtigung zum Zugriff auf Nutzungsdaten in § 100g Abs. 1 Satz 2 StPO-E. Die geplante Regelung verweist hinsichtlich der Eingriffsschwelle auf die Ermächtigung zum Zugriff auf Telekommunikations-Verkehrsdaten in § 100g Abs. 1 Satz 1 StPO. Danach ist der Datenzugriff zulässig zur Verfolgung von Straftaten von erheblicher Bedeutung<sup>23</sup> sowie von Straftaten, die mittels Telekommunikation begangen wurden. Ob diese recht offen gefasste Ermächtigung der Sensibilität von Telekommunikations-Verkehrsdaten vollauf gerecht wird, ist durchaus fragwürdig, mag hier

---

<sup>21</sup> Vgl. BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 –, Rn. 151.

<sup>22</sup> Vgl. § 8a Abs. 2 Satz 1 Nr. 5 BVerfSchG (auch i.V.m. § 4a MADG und § 3 Abs. 1 Satz 2 BNDG); § 52 Abs. 1, Abs. 2 Satz 1 BKAG. Einen Sonderfall des Zugriffs auf Nutzungsdaten regelt § 10a Abs. 1 BKAG-E. Der materielle Zugriffstatbestand dieser Regelung ist zwar eher niedrig angesetzt, jedoch werden die zu erhebenden Daten und das Erkenntnisziel der Datenerhebung so eng zugeschnitten, dass die Norm insgesamt keinen verfassungsrechtlichen Bedenken unterliegt.

<sup>23</sup> Der Straftatenkatalog des § 100a Abs. 2 StPO wird lediglich beispielhaft in Bezug genommen.

<sup>12</sup> aber dahinstehen.<sup>24</sup> Beim Zugriff auf Telemedien-Nutzungsdaten verschärfen sich die verfassungsrechtlichen Zweifel jedenfalls noch, da diese Datenkategorie schwierig abzugrenzen ist und ein extrem weites Spektrum von Datentypen umfasst, deren Aussagekraft über Telekommunikations-Verkehrsdaten noch deutlich hinausgehen kann.

#### 4. Inhaltsüberwachung von Telemedien

Sowohl wegen der Interpretationsprobleme im Zusammenhang mit dem Begriff des Nutzungsdatums als auch aus Gründen der Rechtssicherheit ist es misslich, dass der Entwurf keine Regelungen über die Überwachung von Telemedieninhalten vorsieht. Dem liegt anscheinend die Erwägung zugrunde, solche Überwachungen könnten auf § 100a StPO und entsprechende Regelungen im präventiven Sicherheitsrecht gestützt werden, da der dort verwendete Begriff der Telekommunikation auch die Kommunikation mittels Telemedien umfasse.<sup>25</sup> Diese Erwägung überzeugt nicht. Jedenfalls ist es nicht ratsam, sich bei der Überarbeitung der sicherheitsrechtlichen Eingriffsermächtigungen an ihr zu orientieren.

Es trifft zu, dass der strafprozessuale Zugriff auf Inhalte von Telemedien – soweit sie nicht offen zugänglich sind und darum durch eine Überwachungsmaßnahme beschafft werden müssen – herkömmlich üblicherweise auf § 100a StPO gestützt wurde. Dies galt insbesondere für die Inhaltsüberwachung von Over-the-Top-Diensten, die (primär) der Individualkommunikation dienen.<sup>26</sup> Dem lag allerdings die in der strafprozessualen Praxis über lange Zeit nicht in Frage gestellte Auffassung zugrunde, solche Dienste seien als Telekommunikationsdienste einzustufen. Nach der neueren Rechtsprechung des Gerichtshofs der Europäischen Union ist dies jedoch gerade nicht der Fall, solange der europäische Kommunikationskodex nicht in deutsches Recht umgesetzt ist. In der strafgerichtlichen Rechtsprechung wird nunmehr eine Anwendung von § 100a StPO auf Over-the-Top-Dienste teils mit dem Argument begründet, der Erbringer eines Over-the-Top-Dienstes wirke am Signaltransport durch die Netzbetreiber und Zugangsdienstleister mit, weil er Datenpakete über das Internet versende und empfangt.<sup>27</sup> Dieses Argument läuft darauf hinaus, die gesetzliche Unterscheidung von Telekommunikations- und Telemedien-diensten schlicht zu ignorieren. Es überzeugt daher nicht. Nach der Rechtsprechung des Bundesgerichtshofs deckt sich hingegen der Telekommunikationsbegriff des § 100a StPO mit dem telekommunikationsrechtlichen Telekommunikationsbegriff.<sup>28</sup> Daher ist davon auszugehen,

---

<sup>24</sup> Diese Frage zu der – allerdings noch weiter gefassten – Vorgängerregelung in § 12 FAG a.F. offenlassend BVerfGE 107, 299 (315 f.), vgl. auch ebd., S. 322.

<sup>25</sup> Vgl. die Begründung zu dem Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, BT-Drs. 19/17741, S. 36.

<sup>26</sup> Vgl. beispielhaft zu der (im Beschluss nicht problematisierten) Überwachung eines E-Mail-Accounts auf der Grundlage von § 100a StPO BGH, Beschluss vom 11. August 2016 – StB 12/16; ferner BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 20. Dezember 2018 – 2 BvR 2377/16.

<sup>27</sup> So etwa LG Köln BeckRS 2020, 30090, Rn. 6 m.w.N.

<sup>28</sup> BGH, Urteil vom 14. März 2003 – 2 StR 341/02 –, NJW 2003, S. 2034; Beschluss vom 31. Januar 2007 – StB 18/06, NJW 2007, S. 930 (931 f.). In der juristischen Literatur wird hingegen vertreten, der Telekommunikationsbegriff des § 100a StPO sei nicht an dem technisch ansetzenden telekommunikationsrechtlichen Telekommunikationsbegriff, sondern an dem – teils engeren, teils weiterreichenden – Fernmeldegeheimnis des Art. 10 GG zu orientieren, vgl. zur Diskussion Graf, in: BeckOK StPO, § 100a Rn. 18 ff.; Günther, in: MüKo

<sup>13</sup> dass das geltende Recht keine Ermächtigungen für sicherheitsbehördliche Inhaltsüberwachungen von Telemediendiensten enthält.

Hierdurch entsteht eine Schutzlücke, die auch durch die anstehende Erweiterung des Telekommunikationsbegriffs auf interpersonelle Kommunikationsdienste nicht vollständig entfallen dürfte. Denn auch danach dürfte es weiterhin Kommunikationsdienste geben, die eine nicht-öffentliche Kommunikation ermöglichen, ohne dass sie als Telekommunikationsdienste einzustufen wären. An einer Inhaltsüberwachung solcher Dienste könnte durchaus ein sicherheitsbehördliches Interesse bestehen. Hinzu kommt, dass durch eine ausdrückliche Ermächtigung zum Zugriff auf Telemedieninhalte die schwierige, weitgehend aber auch fruchtlose Abgrenzung zwischen Inhalten und Nutzungsdaten vermieden werden könnte.

Es erscheint daher ratsam, in die Fachgesetze der Sicherheitsbehörden ausdrückliche Ermächtigungen aufzunehmen, die neben der Erhebung von Telemedien-Nutzungsdaten auch die Inhaltsüberwachung von Telemedien unter denselben Voraussetzungen zulassen. Die Eingriffsvoraussetzungen sollten sich an die Ermächtigungen zu Telekommunikationsüberwachungen anlehnen, um der hohen Sensibilität von Telemediendaten Rechnung zu tragen.

## II. Zuordnung dynamischer IP-Adressen

Gleichfalls nicht in jeder Hinsicht mit höherrangigem Recht vereinbar sind die in § 113 Abs. 1 Satz 3, Abs. 3 und Abs. 5 TKG-E enthaltenen Erlaubnisse für die Anbieter von Telekommunikationsdiensten, dynamische IP-Adressen einem Anschlussinhaber zuzuordnen und die resultierenden Bestandsdaten zu übermitteln. Diese Regelungen entsprechen zwar den verfassungsrechtlichen Anforderungen, die das Bundesverfassungsgericht in seinem zweiten Bestandsdatenbeschluss errichtet hat.<sup>29</sup> Sie verstoßen jedoch partiell gegen die unionsrechtlichen Vorgaben, die entgegen der Einschätzung des Bundesverfassungsgerichts<sup>30</sup> teilweise strenger ausfallen.

Die Übermittlungserlaubnisse des § 113 TKG sind am Unionsrecht zu messen, da der deutsche Gesetzgeber mit ihnen von den in Art. 6 Abs. 1 lit. c, Abs. 3 und Abs. 4 i.V.m. Art. 23 DSGVO und/oder in Art. 15 der Datenschutzrichtlinie für die elektronische Kommunikation<sup>31</sup> enthaltenen

---

StPO, 2014, § 100a Rn. 26 ff. Da zugleich aufgrund ausdrücklicher Verweise auf das Telekommunikationsgesetz unstreitig ist, dass der Telekommunikationsbegriff in den Ermächtigungen zur Erhebung von Bestands- und Verkehrsdaten (§ 100g und § 100j StPO) dem telekommunikationsrechtlichen Telekommunikationsbegriff entspricht, hat diese Auffassung zur Folge, dass der Begriff der Telekommunikation in unterschiedlichen strafprozessualen Eingriffsermächtigungen unterschiedlich zu verstehen ist. Dies erscheint normsystematisch wenig überzeugend.

<sup>29</sup> BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 –, Rn. 175 ff.

<sup>30</sup> BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 –, Rn. 261.

<sup>31</sup> 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 (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31. Juli 2002, S. 37, zuletzt geändert durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den

14 Öffnungsklauseln für mitgliedstaatliches Recht Gebrauch gemacht hat.<sup>32</sup> Diese Öffnungsklauseln sind im Licht der Grundrechte auf Achtung des Privat- und Familienlebens aus Art. 7 GRCh sowie auf Datenschutz aus Art. 8 GRCh auszulegen.

Nach der Rechtsprechung des Gerichtshofs der Europäischen Union bewirken die Übermittlung von und der behördliche Zugriff auf Bestandsdaten zur Identifizierung von Anschlussinhabern grundsätzlich keinen schweren Eingriff in diese Grundrechte. Dieser Eingriff darf darum allgemein zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten zugelassen werden, ohne dass diese Straftaten als schwerwiegend einzustufen sein müssten.<sup>33</sup> Dies gilt auch dann noch, wenn das mitgliedstaatliche Recht eine Pflicht zur allgemeinen Bevorratung bestimmter Identifikationsdaten vorsieht.<sup>34</sup>

Die unionsrechtlichen Anforderungen verschärfen sich hingegen, wenn zur Zuordnung dynamischer IP-Adressen Verkehrsdaten genutzt werden dürfen, die für sicherheitsbehördliche Zwecke bevorratet wurden. Der Gerichtshof hat in seinem dritten Vorratsdatenurteil klargestellt, dass die Mitgliedstaaten zwar eine anlasslose und flächendeckende Bevorratung von IP-Zuordnungsdaten (im Gegensatz zu anderen Verkehrsdaten) anordnen dürfen. Um dem Eingriffsgewicht der Datenbevorratung Rechnung zu tragen, muss die Bevorratung jedoch materiell qualifizierten öffentlichen Interessen dienen. Hinreichend gewichtige Interessen sind der Schutz der nationalen Sicherheit, die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit.<sup>35</sup>

Nach diesen Maßstäben dürften die Übermittlungserlaubnisse in § 113 Abs. 1 Satz 3, Abs. 3 und Abs. 5 TKG-E den unionsrechtlichen Anforderungen zwar insoweit entsprechen, als sie eine Zuordnung von IP-Adressen mithilfe von Verkehrsdaten zulassen, welche die Telekommunikationsanbieter zu eigenen Zwecken gespeichert haben. Hingegen stehen sie mit diesen Anforderungen insoweit nicht in Einklang, als sie in Verbindung mit § 113c Abs. 1 Nr. 3 TKG eine Bestandsdatenauskunft auch unter Verwendung von bevorrateten IP-Adressen ermöglichen.<sup>36</sup> Denn die Datenübermittlung wird nicht auf die vom Gerichtshof der Europäischen Union genannten qualifizierten Ziele oder gleichrangige Belange beschränkt. Sie wird vielmehr unter anderem

---

Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, ABl. L 337 vom 18. Dezember 2009, S. 11.

<sup>32</sup> Ob und inwieweit die Übermittlung von Bestandsdaten jeweils der DSGVO oder der Richtlinie 2002/58/EG unterfällt, ist durchaus problematisch, vgl. die wenig klaren Ausführungen in EuGH, Urteil vom 2. Oktober 2018, Rs. C-207/16 – Ministerio Fiscal, Rn. 40 ff. Für die vorliegende Stellungnahme kommt es allerdings auf die Abgrenzung der beiden Regelwerke nicht entscheidend an, da in jedem Fall § 113 TKG einer Öffnungsklausel des europäischen Datenschutzrechts unterfällt und unionsrechtlichen Anforderungen genügen muss.

<sup>33</sup> EuGH, Urteil vom 2. Oktober 2018, Rs. C-207/16 – Ministerio Fiscal, Rn. 53 ff.

<sup>34</sup> EuGH, Urteil vom 6. Oktober 2020, Rs. C-511/18, C-512/18 und C-520/18 – La Quadrature du Net u.a., Rn. 157 ff.

<sup>35</sup> EuGH, Urteil vom 6. Oktober 2020, Rs. C-511/18, C-512/18 und C-520/18 – La Quadrature du Net u.a., Rn. 152 ff.

<sup>36</sup> Die Bewertung der vorgesehenen Regelungen ist unabhängig davon, dass die Vorratsdatenspeicherung aktuell faktisch weitgehend ausgesetzt ist, da hier die Vereinbarkeit der Gesetzeslage und nicht der gegenwärtigen behördlichen Praxis mit höherrangigem Recht zu prüfen ist, vgl. zu den Grundrechten des Grundgesetzes BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 –, Rn. 171.

<sup>15</sup> zugelassen zur Verfolgung sämtlicher – also nicht nur schwerer – Straftaten (§ 113 Abs. 5 Nr. 1 TKG-E) sowie zur Abwehr von Gefahren für Rechtsgüter von hervorgehobenem – also nicht zwangsläufig von erheblichem oder gar überragendem<sup>37</sup> – Gewicht (§ 113 Abs. 5 Nr. 2 TKG-E). Zumindest fragwürdig ist darüber hinaus etwa, ob der gesamte Aufgabenbereich der Nachrichtendienste (§ 113 Abs. 3 Nr. 5-7, Abs. 5 Satz 2 TKG) dem engen unionsrechtlichen Begriff der nationalen Sicherheit unterfällt, der sich auf „die Verhütung und Repression von Tätigkeiten, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, wie insbesondere terroristische Aktivitäten“ beschränkt.<sup>38</sup>

---

<sup>37</sup> Vgl. zur Begriffsbildung BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 –, Rn. 178, sowie zu den höheren Anforderungen an Rechtsgüter von „erheblichem“ bzw. „besonderem“ Gewicht die Gesetzesbegründung, BT-Drs. 19/25294, S. 51.

<sup>38</sup> EuGH, Urteil vom 6. Oktober 2020, Rs. C-511/18, C-512/18 und C-520/18 – La Quadrature du Net u.a., Rn. 135.