JOHANNES GUTENBERG-UNIVERSITÄT MAINZ - 55099 Mainz

FACHBEREICH 03
JURA
Lehrstuhl für Öffentliches Recht und Informationsrecht, insbesondere 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 Bekämpfung des Rechtsextremismus und der Hasskriminalität

(BT-Drs. 19/17741)

## Gliederung

## Ergebnisse

1. Die in § 3a NetzDG-E vorgesehene Pflicht zur sofortigen Übermittlung von Identifikationsdaten an das Bundeskriminalamt verletzt höherrangiges Recht. Eine solche Pflicht ist nur in einem zweistufigen Verfahren als zweiter Schritt verhältnismäßig, nachdem das Bundeskriminalamt in einem ersten Schritt die übermittelten Inhalte geprüft und einen strafprozessualen Anfangsverdacht bejaht hat.

2. Die vorgesehene Ermächtigung des Bundeskriminalamts zum Zugriff auf Telemedien-Bestandsdaten in § 10 Abs. 1 Satz 1 Nr. 1, Satz 2 BKAG-E geht weiter als die zugehörige Übermittlungserlaubnis in § 15a Abs. 2 Satz 1 TMG-E, da sie einen Zugriff auch im Vorfeld von präventivpolizeilicher Gefahr und strafprozessualem Anfangsverdacht zulässt. Sie verletzt zudem das Recht auf informationelle Selbstbestimmung, da sie den Eingriffsanlass weder in tatsächlicher noch in materieller Hinsicht näher konturiert und qualifiziert.

3. § 15a Abs. 4 Satz 1 und § 15b Abs. 3 Satz 1 TMG-E verletzen die bundesstaatliche Kompetenzordnung, soweit diese Vorschriften eine Pflicht zu Datenübermittlungen auch in Fällen normieren, in denen die Regelungskompetenz für den behördlichen Datenzugriff bei den Ländern liegt. Im Übrigen sind die Vorschriften weitgehend redundant, da sich Übermittlungspflichten zumeist auch im behördlichen Fachrecht finden. Sie können und sollten ersatzlos gestrichen werden.

4. Die in § 15a Abs. 2 Satz 1 TMG-E enthaltene Übermittlungserlaubnis für Telemedienanbieter ist zu weit gefasst und unverhältnismäßig, soweit sie sich auf Telemedien-Nutzungsdaten erstreckt. Gegen die vorgesehene strafprozessuale Zugriffsermächtigung in § 100g Abs. 1 Satz 2 StPO-E bestehen gleichfalls verfassungsrechtliche Bedenken, da sie der potenziellen besonderen Sensibilität dieser Datenkategorie nicht vollumfänglich Rechnung trägt.

5. In dem Entwurf fehlt eine strafprozessuale Ermächtigung zur Inhaltsüberwachung von Telemedien. Entgegen der Entwurfsbegründung ist eine solche Ermächtigung nicht deshalb entbehrlich, weil eine solche Überwachung auf die Ermächtigung zu Telekommunikationsüberwachungen in § 100a StPO gestützt werden könnte. Dieser Ansatz birgt erhebliche Rechtsunsicherheit und Risiken für die Effektivität der Strafverfolgung.

6. Die Erlaubnis zur Übermittlung von Telemedien-Zugangsdaten in § 15b Abs. 2 Satz 1 TMG-E und die Ermächtigung zum Zugriff auf solche Daten in § 100j Abs. 1 Satz 2 StPO-E sind inkongruent. Wegen der sehr hohen Sensibilität dieser Datenkategorie sollte die Übermittlungsschwelle des § 15b Abs. 2 Satz 1 TMG-E in die strafprozessuale Ermächtigung überführt werden.

7. Die Zitierung des Fernmeldegeheimnisses in Art. 7 des Entwurfs ist selbst dann noch unvollständig, wenn der Änderungsvorschlag des Bundesrates umgesetzt wird. Als Art. 10 GG einschränkende Norm muss auch § 100g StPO-E (Art. 2 Nr. 2 des Entwurfs) zitiert werden, da sich der Schutzbereich des Fernmeldegeheimnisses zumindest auf manche Telemedien-Nutzungsdaten erstreckt.

4 In der knappen Zeit, die mir zur Verfügung stand, war mir eine umfassende Stellungnahme zu allen verfassungsrechtlichen und gesetzgebungstechnischen Fragen, die der Entwurf aufwirft, nicht möglich. Ich beschränke mich darum im Folgenden auf zwei Themenkomplexe: die Pflicht bestimmter Netzwerkbetreiber zur Meldung bestimmter Inhalte an das Bundeskriminalamt (unten I) sowie die Regelungen zur Übermittlung von Telemediendaten an Sicherheitsbehörden und zum behördlichen Zugriff auf diese Daten (unten II). Außen vor bleiben damit insbesondere die vorgesehenen Änderungen im materiellen Strafrecht, die gleichfalls teilweise erhebliche Probleme bergen.[1] Hierzu kann ich gegebenenfalls in der Anhörung mündlich Stellung nehmen.

## I. Meldung strafbarer Inhalte an das Bundeskriminalamt

Gegen die vorgesehene Pflicht von Netzwerkbetreibern, bestimmte mutmaßlich strafbare Kommunikationsinhalte an das Bundeskriminalamt zu melden (§ 3a NetzDG-E), bestehen keine fundamentalen verfassungsrechtlichen Bedenken.[2] Allerdings reicht diese Pflicht hinsichtlich der mit zu übermittelnden Identifikationsdaten teils zu weit. Folgefragen wirft die Weiterverarbeitung der übermittelten Daten durch das Bundeskriminalamt auf.

### 1. Keine grundlegenden verfassungsrechtlichen Bedenken

Im Grundansatz ist die in § 3a NetzDG-E enthaltene Meldepflicht verfassungskonform. Insbesondere wird hiermit nicht etwa in rechtsstaatlich bedenklicher Weise eine genuin hoheitliche Tätigkeit an Private delegiert. Die Meldepflicht fügt sich vielmehr in ein Gefüge vergleichbarer Pflichten marktmächtiger Unternehmen ein, mit denen diese zur Unterstützung hoheitlicher Aufsichts- und Sanktionsaufgaben in Dienst genommen werden.

Meiner Ansicht nach ist es auch vertretbar, die Bearbeitung der Meldungen unter die Zentralstellenaufgabe des Bundeskriminalamts zu subsumieren, wenngleich es sich um einen Grenzfall handelt. Die Meldepflicht soll dazu dienen, dass das Bundeskriminalamt – in strafprozessualer Terminologie – in den Meldefällen Vorermittlungen anstellt, um das Vorliegen eines Anfangsverdachts zu prüfen und eine zuständige Landesstrafverfolgungsbehörde zu ermitteln. Eine solche Tätigkeit weicht von den üblicherweise unter den Zentralstellenbegriff subsumierten Service- und Koordinationstätigkeiten[3] deutlich ab und nähert sich einer operativen Aufgabe zumindest an. Die Zuständigkeit der Zentralstelle lässt sich aber mit der in der Gesetzesbegründung vorgebrachten Erwägung begründen, dass sich bei den in § 3a Abs. 2 Nr. 3 NetzDG-E genannten Kommunikationsdelikten im Internet eine zuständige Strafverfolgungsbehörde nicht ohne weite-

---

[1] Vgl. die Stellungnahme des Sachverständigen Prof. Dr. Engländer.

[2] Nicht erörtert werden im Folgenden die allgemeinen Bedenken, die gegen das NetzDG insgesamt aus der bundesstaatlichen Ordnung der Gesetzgebungskompetenzen sowie aus dem Unionsrecht, insbesondere der E-Commerce-Richtlinie, abgeleitet werden. Diese Bedenken sind nicht neu und werden durch den Entwurf meines Erachtens zumindest nicht verschärft.

[3] Näher zu diesem Begriff aus kompetenzrechtlicher Sicht Bäcker, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, Rn. B 127 ff.

5 res bestimmen lässt. Insbesondere kann – entgegen einer Tendenz in der früheren Rechtsprechung – nicht einfach auf die bundesweite Zugänglichkeit der Inhalte abgestellt werden, um eine Zuständigkeit aller Staatsanwaltschaften in Deutschland zu begründen.[4]

**2. Verfassungs- und unionsrechtliches Gebot einer zweistufigen Ausgestaltung**

Jedoch reicht die Meldepflicht inhaltlich zu weit bzw. ist zu undifferenziert ausgestaltet. Sie verletzt darum in ihrer derzeit vorgesehenen Ausgestaltung höherrangiges Recht.

Gemäß § 3a Abs. 4 NetzDG-E soll der Netzwerkanbieter verpflichtet sein, dem Bundeskriminalamt neben dem mutmaßlich strafbaren Inhalt die letzte IP-Adresse und Portnummer des betroffenen Nutzers mitzuteilen. Hierbei handelt es sich um personenbezogene Daten, da mit ihrer Hilfe die Lokalisierung und Identifikation des Nutzers ermöglicht wird und auch werden soll.[5] Die Meldepflicht greift daher zum einen in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ein. Zum anderen ist sie als gesetzliche Datenverarbeitungspflicht, die eine Zweckänderung der übermittelten Daten bewirkt, an Art. 6 Abs. 1 Satz 1 lit. c, Abs. 3 sowie Art. 6 Abs. 4 i.V.m. Art. 23 Abs. 1 lit. d DSGVO zu messen.[6] Diese höherrangigen Regelungen verlangen übereinstimmend, dass die durch die Meldepflicht vorgegebene Datenübermittlung erforderlich ist, um das Ziel der Verfolgung bestimmter Straftaten zu erreichen.

Dies ist jedoch nicht durchweg der Fall. Die Prüfung des übermittelten Inhalts durch das Bundeskriminalamt kann und wird in vielen Fällen ergeben, dass dieser Inhalt entgegen der Ansicht des Netzwerkbetreibers keinen Straftatbestand erfüllt. Hiervon geht ersichtlich auch die Entwurfsbegründung aus, die eine weit höhere Zahl von Meldungen (250.000) als von anschließenden Ermittlungsverfahren (150.000) erwartet.[7] In einem solchen Fall ist eine Identifizierung des Nutzers, der den Inhalt veröffentlicht hat, nicht angezeigt und werden die Identifikationsdaten nicht benötigt. Verfassungsrechtlich unzulässig wäre insbesondere eine tatverdachtsunabhängige vorsorgliche Identifikation aller Nutzer, deren Inhalte gemeldet werden, durch Bestandsdatenabrufe auf der Grundlage von § 10 Abs. 1 Nr. 1, Abs. 2 BKAG i.V.m. § 113 Abs. 1 Satz 3 TKG. Diese Normen setzen bei verfassungskonformer Auslegung den Anfangsverdacht einer Straftat voraus[8] und ermöglichen daher keinen Datenabruf zu einem Zeitpunkt, in dem gerade noch nicht geklärt ist, ob ein Anfangsverdacht besteht oder nicht. Erforderlich ist die Übermittlung

---

[4] Näher zum Problem der für die Zuständigkeit maßgeblichen Bestimmung des Tatorts bei Internetstraftaten, die – wie zumindest die Mehrzahl der in § 3a Abs. 2 Nr. 3 NetzDG-E genannten Tatbestände – weder als Erfolgs- noch als konkrete Gefährdungsdelikte ausgestaltet sind, Heintschel-Heinegg, in: BeckOK StGB, Stand 2020, § 9 Rn. 19 ff.; Eser/Weißer, in: Schönke/Schröder, StGB, 30. Aufl. 2019, § 9 Rn. 7 ff.; Ambos, in: MüKo StGB, 3. Aufl. 2017, § 9 Rn. 26 ff.; Kudlich/Berberich, NStZ 2019, S. 633 ff.

[5] Vgl. BT-Drs. 19/17741, S. 44 f.

[6] Ich gehe hier davon aus, dass eine zweckändernde Datenverarbeitung sowohl einer Verarbeitungs- als auch einer Zweckänderungserlaubnis bedarf, wie hier etwa Buchner/Petri, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 6 DSGVO Rn. 181 ff. Die folgenden Ausführungen ließen sich allerdings auch auf der Grundlage der Gegenposition begründen, nach der Zweckänderungserlaubnis die Verarbeitungserlaubnis mitumfasst.

[7] BT-Drs. 19/17741, S. 29.

[8] Vgl. BVerfGE 130, 151 (206).

6 der in § 3a Abs. 4 Nr. 2 NetzDG-E genannten Daten daher nur, wenn die Prüfung durch das Bundeskriminalamt den Anfangsverdacht einer Straftat ergibt.

Hieraus folgt, dass die Meldepflicht zweistufig auszugestalten ist. Zunächst darf der Netzwerkanbieter nur zur Übermittlung des mutmaßlich strafbaren Inhalts verpflichtet werden. Erst nach einer inhaltlichen Prüfung, die einen Anfangsverdacht ergibt, darf er auch zur Übermittlung der Identifikationsdaten auf Anforderung des Bundeskriminalamts verpflichtet werden. Zulässig und sinnvoll ist es darüber hinaus, den Netzwerkanbieter zu verpflichten, gleichzeitig mit der Übermittlung des Inhalts die in § 3a Abs. 4 Nr. 2 NetzDG-E genannten Identifikationsdaten zu speichern und bis zu einer Rückmeldung des Bundeskriminalamts aufzubewahren („quick freeze“). Mit dem Erforderlichkeitsgrundsatz vereinbar und zudem möglicherweise sogar wirkungsvoller als die in § 3a Abs. 4 Nr. 2 NetzDG-E vorgesehene Meldepflicht wäre es darüber hinaus, den Netzwerkanbieter auch zu verpflichten, bis zur Rückmeldung des Bundeskriminalamts gegebenenfalls weitere Identifikationsdaten zu speichern, die bei einer zwischenzeitlichen Nutzung des Netzwerks durch den fraglichen Nutzer anfallen. Zur Beschleunigung der Identifizierung könnten die Netzwerkanbieter schließlich verpflichtet werden, die Identifikationsdaten mittels einer technischen Schnittstelle zum jederzeitigen automatisierten Abruf durch das Bundeskriminalamt vorzuhalten.

**3. Weiterverarbeitung der übermittelten Daten**

Hinweisen möchte ich darauf, dass das Bundeskriminalamt die aufgrund von § 3a NetzDG-E übermittelten Daten nicht nur zur Einleitung einzelner Strafverfahren bzw. zur Abwehr konkreter Gefahren nutzen darf, sondern eine einzelfallübergreifende, strategisch ausgerichtete Weiterverarbeitung zulässig ist und kriminalistisch naheliegt. Dies wird aus der Entwurfsbegründung nicht deutlich, in der es heißt, die Daten seien „regelmäßig… nach Übermittlung der betreffenden Daten an die zuständige Strafverfolgungsbehörde“ zu löschen.[9] Bei Meldungen, zu denen das Bundeskriminalamt einen Tatverdacht bejaht, liegt nach meiner Einschätzung nahe, dass im Gegenteil die umgehende Löschung faktisch eher den Ausnahmefall darstellen wird.

Die Inhalte und ggfs. Identifikationsdaten werden dem Bundeskriminalamt in seiner Zentralstellenfunktion übermittelt. Sie können daher, ohne dass eine besonders legitimationsbedürftige Zweckänderung vorläge, im Rahmen der Zentralstellenaufgabe gemäß § 16 Abs. 1 i.V.m. § 12 Abs. 1 Satz 1 BKAG sowie ggfs. aufgrund von § 18 Abs. 1 Nr. 3 BKAG weiterverarbeitet werden. Der Begriff der Weiterverarbeitung schließt insbesondere eine Bevorratung der Daten im Informationssystem des Bundeskriminalamts (§ 13 BKAG) ein, um die Daten in späteren, noch nicht zwangsläufig absehbaren polizeilichen Verfahren nutzen zu können. Die Daten könnten etwa in Lagebilder bestimmter Phänomenbereiche oder in Analysen von Diskurszusammenhängen zur Früherkennung von Radikalisierungsprozessen und Gewaltereignissen einfließen. Die in § 3a Abs. 2 NetzDG-E für die Übermittlung vorgesehene Zweckbestimmung der „Ermöglichung der Verfolgung von Straftaten“ steht einer solchen Weiterverarbeitung nicht entgegen, da sie sprach-

[9] BT-Drs. 19/17741, S. 15.

7 lich zwanglos auch auf die Verfolgung zukünftiger, noch nicht absehbarer Straftaten (sog. Verfolgungsvorsorge) bezogen werden kann. Aus höherrangigem Recht bestehen hiergegen angesichts der begrenzten Eingriffsintensität der Weiterverarbeitung der übermittelten Daten keine prinzipiellen Bedenken.

Kritisch zu sehen wäre hingegen eine Weiterverarbeitung in Fällen, in denen das Bundeskriminalamt einen Tatverdacht verneint, weil es den gemeldeten Inhalt für (noch) zulässig hält. Für eine derartige Weiterverarbeitung ließen sich allerdings durchaus Rechtsgrundlagen finden. Neben der schon genannten Ermächtigung aus § 16 Abs. 1 i.V.m. § 12 Abs. 1 Satz 1 BKAG, die weder einen Tatverdacht noch eine auf die betroffene Person bezogene Kriminalprognose voraussetzt, kommt hierfür insbesondere § 18 Abs. 1 Nr. 4 BKAG in Betracht. Anknüpfungspunkt der Kritik müssen dementsprechend weniger die im Gesetzentwurf vorgesehenen Regelungen als die verfassungsrechtlich sehr zweifelhaften Bestandsnormen im BKAG sein. Ich sehe aus diesem Grund davon ab, die Kritik hier zu vertiefen.[10]

## II. Übermittlung von und Zugriff auf Telemediendaten

Der Entwurf sieht eine Reihe von Regelungen vor, welche die Übermittlung von Telemediendaten an Sicherheitsbehörden und den behördlichen Zugriff auf solche Daten rechtssicher ermöglichen sollen. Dieses Ziel wird allerdings nicht vollumfänglich erreicht. Insbesondere aufgrund einiger konzeptioneller Unklarheiten gibt der Entwurf die Datenverarbeitung teils in zu weitem Umfang frei und weist einige Lücken auf.

### 1. Vorfragen

Bevor die einzelnen vorgesehenen Regelungen näher erörtert und kritisiert werden können, bedarf es konzeptioneller Vorklärungen. Diese betreffen zum einen die juristische Konstruktion des sicherheitsbehördlichen Zugriffs auf gesellschaftliche Datenbestände, zu denen auch Telemediendaten zählen, zum anderen die Definition und Abgrenzung der für den Entwurf relevanten Datenkategorien.

#### a) Doppeltürmodell und grundrechtliche Regelungsverantwortung

Der sicherheitsbehördliche Zugriff auf gesellschaftliche Datenbestände wird datenschutzrechtlich als zweiaktiger Vorgang konstruiert: Das private Unternehmen, das bestimmte Daten an eine Sicherheitsbehörde transferiert, benötigt hierfür eine Übermittlungserlaubnis. Die Sicherheitsbehörde benötigt zur Entgegennahme und zum weiteren Umgang mit den Daten einer Zugriffsermächtigung. Das Bundesverfassungsgericht verwendet für diese Regelungsstruktur das

[10] Gegen die genannten Normen ist seit Mai 2019 eine von mir als Prozessbevollmächtigtem vertretene Verfassungsbeschwerde bei dem Bundesverfassungsgericht anhängig (Az. 1 BvR 1160/19), über die noch nicht entschieden und die zumindest bislang auch nicht zugestellt wurde. Der Text meiner Beschwerdeschrift ist abrufbar unter https://freiheitsrechte.org/home/wp-content/uploads/2019/10/2019-05-21-BKA-Gesetz-VB-anonymisiert.pdf.

8 Bild einer Doppeltür.[11] Das originär datenschutzrechtliche Doppeltürmodell ist in zweifacher Hinsicht verfassungsrechtlich bedeutsam:

Erstens ist die Gesetzgebungskompetenz für den Datentransfer anhand dieses Modells zu differenzieren.[12] Die Kompetenz für die Übermittlungserlaubnis liegt bei dem Gesetzgeber, der das Datenschutzrecht für die übermittelnde Stelle regeln darf. Für den Telemediendatenschutz ergibt sich aus Art. 74 Abs. 1 Nr. 11 GG eine konkurrierende Gesetzgebungskompetenz des Bundes.[13] Die Kompetenz für die Zugriffsermächtigung richtet sich hingegen nach der Gesetzgebungskompetenz für die jeweilige Sicherheitsbehörde, der ein Zugriff erlaubt werden soll. Dies führt wegen der differenzierten Kompetenzrechtslage für das Sicherheitsrecht zu einer zwischen Bund und Ländern aufgeteilten Regelungsbefugnis. So ist der Bund für die Regelung strafprozessualer Zugriffe gemäß Art. 74 Abs. 1 Nr. 1 GG zuständig, während Zugriffe durch die Landespolizeibehörden von den Ländern zu regeln sind.

Zu beachten ist, dass die Regelungsbefugnis des Gesetzgebers der Übermittlungserlaubnis lediglich die Erlaubnis, nicht aber die Pflicht zur Übermittlung umfasst. Das Bundesverfassungsgericht hat hierzu ausgeführt, eine Pflicht der Unternehmen zur Datenübermittlung sei als Teil des Abrufs kompetenziell den Gesetzgebern der Zugriffsermächtigungen zugewiesen, also in weitem Umfang den Ländern.[14]

Zweitens sind die materiellen verfassungsrechtlichen Anforderungen an den Gesamtvorgang zwischen den beiden Regelungen zu verteilen. Nach der Rechtsprechung des Bundesverfassungsgerichts trifft den Gesetzgeber, der für die Übermittlungserlaubnis zuständig ist, eine grundrechtliche Regelungsverantwortung für den Umgang mit den übermittelten Daten. Er muss die Zwecke der zulässigen Übermittlungen normenklar bestimmen und durch hinreichend strenge Tatbestandsvoraussetzungen gewährleisten, dass diese Übermittlungen den Verhältnismäßigkeitsgrundsatz wahren.[15] Bedeutsam ist dies insbesondere, wenn die Regelungskompetenzen für die Übermittlungserlaubnis und die Zugriffsermächtigung auseinanderfallen. In einem solchen Fall muss zwingend bereits die Übermittlungserlaubnis eine hinreichende tatbestandliche Übermittlungsschwelle errichten.

**b) Differenzierung und Abgrenzung von Telemedien und Telekommunikation**

Die vorgesehenen Regelungen beruhen auf der in § 1 Abs. 1 Satz 1 TMG i.V.m. § 3 Nr. 24 TKG geregelten Differenzierung zwischen Telemedien- und Telekommunikationsdiensten. Weil es sich um rechtlich getrennte Arten von Kommunikationsdiensten handelt, sollen auch die Übermittlung der bei der Diensteerbringung anfallenden Daten an Sicherheitsbehörden sowie der behördliche Zugriff auf diese Daten ausdrücklich voneinander unterschieden werden.

---

[11] Grundlegend BVerfGE 130, 151 (184); daran anknüpfend BVerfGE 141, 220 (333 f.); 150, 244 (278); 150, 309 (335).
[12] BVerfGE 130, 151 (200 ff.).
[13] Vgl. Heintzen, in: v. Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 73 Rn. 76.
[14] BVerfGE 130, 151 (201).
[15] Vgl. BVerfGE 125, 260 (344, 346); 130, 151 (201); 141, 220 (333 f.).

9 Die Differenzierung zwischen beiden Dienstetypen hat eine Wurzel im Unionsrecht, da der Begriff des Telekommunikationsdienstes durch Art. 2 lit. c der derzeit noch geltenden Rahmenrichtlinie für die elektronische Kommunikation[16] vorgeprägt wird. Der Gerichtshof der Europäischen Union hat diese Norm kürzlich eng ausgelegt, so dass zahlreiche 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.[17] 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 deutschem 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 Sicherheitsrecht auf Datenerhebungen mit Bezug zur Telekommunikation im telekommunikationsrechtlichen Sinne. Es bedarf daher für telemedienbezogene Überwachungsmaßnahmen spezifischer Rechtsgrundlagen, welche die Übermittlung von Telemediendaten an Sicherheitsbehörden und den behördlichen Zugriff auf solche Daten regeln. Der Entwurf soll solche Regelungen schaffen und dabei einen prinzipiellen Gleichlauf zwischen telekommunikations- und telemedienbezogenen Überwachungsmaßnahmen herstellen.

Die Begrifflichkeiten könnten sich in naher Zukunft verschieben. Der bis Ende des Jahres in deutsches Recht umzusetzende Kommunikationskodex[18] fasst den Anwendungsbereich des europäischen Kommunikationsrechts neu. Gemäß Art. 2 Nr. 4 Kommunikationskodex umfasst der zentrale Begriff des elektronischen Kommunikationsdienstes fortan unter anderem alle interpersonellen Kommunikationsdienste, die über elektronische Kommunikationsnetze erbracht werden. Es kommt danach – anders als nach geltendem Recht – nicht darauf an, ob solche Dienste ganz oder überwiegend in der Übertragung von Signalen bestehen. Mit der Umsetzung des Kommunikationskodex wird sich – unterstellt, es bleibt bei der aktuellen Terminologie im deutschen Recht – der Begriff des Telekommunikationsdienstes erweitern und der Begriff des Telemediendienstes entsprechend verengen.[19] Dementsprechend könnten die Übermittlung von und der behördliche Zugriff auf Daten aus interpersonellen Over-the-Top-Kommunikationsdiensten ab diesem Zeitpunkt auf die Regelungen zu stützen sein, die sich auf Telekommunikationsdaten

---

[16] 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.
[17] EuGH, Urteil vom 13. Juni 2019, Rs. C-193/18 – Google LLC gegen Bundesrepublik Deutschland.
[18] 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.
[19] Kiparski, CR 2019, S. 179 (180).

10 beziehen. Die praktische Relevanz der im Entwurf vorgesehenen Rechtsänderungen würde sich damit erheblich vermindern.

Zwingend wäre diese Schlussfolgerung allerdings nicht. Insbesondere enthält der Kommunikationskodex keine Regelungen zu der im vorliegenden Zusammenhang besonders relevanten Rechtsmaterie des Telekommunikations-Datenschutzes. Eine angestrebte Neuregelung dieser Materie ist bislang nicht gelungen. Bis auf Weiteres bleibt daher die alte Richtlinie über den Datenschutz bei der elektronischen Kommunikation maßgeblich. Da deren sachlicher Anwendungsbereich sich nach der Rahmenrichtlinie bestimmt, könnte es in Zukunft dazu kommen, dass ein regulierungsrechtlicher und ein datenschutzrechtlicher Telekommunikationsbegriff zu unterscheiden sind. Es erschiene dann naheliegend, für die Übermittlung von Kommunikationsdaten an Sicherheitsbehörden und den behördlichen Zugriff auf diese Daten auf den engeren datenschutzrechtlichen Telekommunikationsbegriff abzustellen.

Letztlich wird die Frage nach der zukünftigen Reichweite der auf Telemedien bezogenen Übermittlungs- und Überwachungsregelungen mittelbar vom deutschen Gesetzgeber zu beantworten sein, wenn er den Kommunikationskodex umsetzt. Meine Stellungnahme beschränkt sich im Folgenden auf den gegenwärtigen, möglicherweise kurzlebigen Rechtsstand.

**c) Kategorien von Telekommunikations- und Telemediendaten**

Der Entwurf verfolgt erkennbar den Regulierungsansatz, Telekommunikations- und Telemediendienste hinsichtlich der Übermittlung von Kommunikationsdaten an Sicherheitsbehörden und des behördlichen Zugriffs auf solche Daten gleichzubehandeln. Eine solche Parallelisierung fand sich schon bislang (zumindest teilweise) in einigen Fachgesetzen der Sicherheitsbehörden.[20] Ihre Überzeugungskraft hängt allerdings maßgeblich davon ab, inwieweit sich für Telekommunikations- und Telemediendienste vergleichbare Datenkategorien bilden lassen, hinsichtlich derer einem behördlichen Zugriff jeweils eine gleichartige Eingriffsintensität zukommt.

Das Telekommunikations- und das Telemedienrecht kennen gleichermaßen die Datenkategorie der Bestandsdaten.[21] 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 ohne weiteres vergleichbar, so dass sich eine Gleichbehandlung hinsichtlich der Übermittlung und des behördlichen Zugriffs aufdrängt.

Einen Sonderfall der Bestandsdaten bilden die bisher nur im Telekommunikationsrecht ausdrücklich erwähnten Zugangsdaten. Hierbei handelt es sich um „Daten, mittels derer der Zugriff

---

[20] 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.

[21] § 3 Nr. 3 TKG; § 14 Abs. 1 TMG.

11 auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird".[22] Die Verarbeitung von Zugangsdaten durch die Diensteanbieter zu eigenen Zwecken wird dabei nicht besonders reguliert. Diese Unterkategorie ist nur für Datenübermittlungen an Sicherheitsbehörden bedeutsam.[23]

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,[24] zum anderen um die Verkehrsdaten. Dies sind Metadaten der Kommunikation, die „bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden."[25] Hierzu zählt beispielsweise die Information, zwischen welchen Rufnummern zu welcher Zeit ein Telefongespräch geführt wurde. Das geltende Sicherheitsrecht stellt an Zugriffe auf beide Datenkategorien teils identische Anforderungen (so etwa § 51 Abs. 1 und § 52 Abs. 1 BKAG). In anderen Regelungswerken wird hingegen der Zugriff auf Telekommunikations-Verkehrsdaten wegen deren – vermeintlich – geringerer Sensibilität unter weniger engen 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 Telemedienrecht 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 Telemedienrecht keine Datenkategorie, die den Inhalten der Telekommunikation entspräche. Dabei ist offenkundig, dass es auch Telemedieninhalte gibt. 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 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 über das Telemedium transportiertes Datum, das sich auf den abgeschlossenen Kaufvertrag bezieht. Bei den der Individualkommunikation dienenden Over-the-Top-Diensten wie E-Mail, Chat oder Instant Messaging erscheint es zumindest fragwürdig, ob sich die übermittelten Nachrichten als Nutzungsdaten einordnen lassen.

---

[22] § 113 Abs. 1 Satz 2 TKG; derselbe Wortlaut findet sich in § 15a Abs. 1 Satz 2 und § 15b Abs. 1 Satz 1 TMG-E.
[23] Vgl. zum verfassungsrechtlichen Hintergrund BVerfGE 130, 151 (207 ff.).
[24] Vgl. § 88 Abs. 1 Satz 1 TKG.
[25] § 3 Nr. 30 TKG.

12 Wie Telemedien-Inhaltsdaten zu behandeln sind, war lange umstritten. Teils wurde eine direkte oder analoge Anwendung der Vorschriften über Nutzungsdaten vertreten. Nach der Gegenauffassung sollten die 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.[26] Dies mag 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.[27] 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 Kommunikationsdienste mit unterschiedlichen kommunikativen Funktionen und Wirkungsweisen bezieht. Eine statische Webseite im World Wide Web, die lediglich zum Leseabruf zur Verfügung steht, ist ebenso ein Telemedium wie ein webbasiertes Diskussionsforum, ein E-Mail-Dienst oder ein Online-Shop. Zudem ist der Telemedienbegriff unterschiedlichen Abstraktionsstufen zugänglich und kann darum über- und untergeordnete Dienste gleichermaßen umfassen. Beispielsweise lässt sich ein Soziales Netzwerk 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, je nach Perspektive auch bei der Übermittlung von Nachrichten über Over-the-Top-Dienste). Denkbar ist auch, dieselben Daten für einen Dienst als Nutzungs- und für einen anderen Dienst als Inhaltsdaten einzustufen (so etwa, wenn ein Besucher eine Nachricht auf der Profilseite eines Sportartikelherstellers in einem Sozialen Netzwerk hinterlässt – Inhaltsdatum im Verhältnis zu dem Sportartikelhersteller, möglicherweise Nutzungsdatum im Verhältnis zu dem Netzwerkbetreiber).

Zudem liegt nahe, dass Nutzungs- und Inhaltsdaten je nach Dienst unterschiedlich sensibel sein können. Die Angabe, dass jemand einen bestimmten Dienst genutzt hat, kann aussagekräftiger und für den Betroffenen kritischer sein als die über diesen Dienst vermittelten Inhalte (so etwa bei der Nutzung eines webbasierten Diskussionsforums, bei dem die Inhalte, nicht aber die Nutzungsdaten öffentlich zugänglich sind). In anderen Fällen erscheinen die Inhalte zumindest ten-

---

[26] Schmitz, in: Spindler/ders., TMG, 2. Aufl. 2018, § 15 Rn. 84; Tinnefeld/Buchner, in: BeckOK DatenschutzR, Stand 2019, Syst. I Rn. 91 ff.

[27] 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 vollständig entzogen ist – aus Art. 8 RL (EU) 2016/680.

13 denziell sensibler als die Nutzungsdaten (so etwa 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**

Die vorgesehenen Regelungen über die Übermittlung von und den behördlichen Zugriff auf Telemedien-Bestandsdaten genügen nicht vollständig den verfassungsrechtlichen Anforderungen.

Gemäß § 15a Abs. 1 Satz 1, Abs. 2 Satz 1, Abs. 3 TMG-E darf ein Telemedienanbieter (unter anderem) Bestandsdaten an Sicherheitsbehörden zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung sowie für die Erfüllung nachrichtendienstlicher Aufgaben übermitteln. Diese Übermittlungsschwelle stimmt wörtlich mit dem für Telekommunikations-Bestandsdaten maßgeblichen § 113 Abs. 2 Satz 1 TKG überein. Die tatbestandlichen Voraussetzungen jener Norm hat das Bundesverfassungsgericht wiederum als „verfassungsrechtlich noch hinnehmbar“ bezeichnet.[28] Diese Bewertung lässt sich wegen der Strukturgleichheit und gleichartigen Sensibilität von Telekommunikations- und Telemedien-Bestandsdaten ohne weiteres auf die vorgesehene Regelung übertragen. Keine Bedenken bestehen des Weiteren gegen die strafprozessuale Zugriffsermächtigung in § 100j Abs. 1 Satz 1 Nr. 2 StPO-E, die den Zugriff von einem strafrechtlichen Tatverdacht abhängig macht.

Über das verfassungsrechtlich zulässige Maß geht hingegen die vorgesehene Zugriffsermächtigung in § 10 Abs. 1 Satz 2 BKAG-E hinaus, zumindest soweit sie auf § 10 Abs. 1 Satz 1 Nr. 1 BKAG Bezug nimmt.

§ 10 Abs. 1 Satz 2 BKAG-E soll dem Bundeskriminalamt Bestandsdatenzugriffe unter anderem im Rahmen seiner Zentralstellenaufgabe „zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung“ ermöglichen. Diese Zugriffsermächtigung ermöglicht dem Bundeskriminalamt Datenerhebungen bereits weit im Vorfeld konkreter Gefahren oder strafprozessualer Ermittlungsverfahren. Das Bundeskriminalamt könnte danach Bestandsdatenzugriffe zur Unterstützung kriminalstrategischer Analysen nutzen, die es unabhängig von konkreten einzelfallbezogenen Verdachtsmomenten durchführt.

Damit sind die Grenzen des verfassungsrechtlich noch Hinnehmbaren auf der Grundlage der Rechtsprechung zu Telekommunikations-Bestandsdaten überschritten. Eine im Vorfeld von konkreter Gefahr oder Tatverdacht angesiedelte Zugriffsermächtigung erscheint zwar – auch angesichts der gemäßigten Eingriffsintensität von Bestandsdatenabfragen – nicht von vornherein ausgeschlossen.[29] Sie müsste jedoch zumindest entweder den Eingriffsanlass in tatsächlicher Hinsicht näher konturieren oder Qualifikationen im Hinblick auf das Gewicht drohender Schäden oder begangener Straftaten enthalten, um den grundrechtlichen Anforderungen zu genügen. Die

---

[28] BVerfGE 130, 151 (205 f.).
[29] Vgl. zu weitaus eingriffsintensiveren Überwachungsmaßnahmen BVerfGE 141, 220 (269 ff.).

14 vorgesehene Zugriffsermächtigung enthält hingegen keine besondere tatsächliche Eingriffsschwelle, sondern verweist lediglich auf die Zentralstellenaufgabe und das allgemeine datenschutzrechtliche Erforderlichkeitsgebot. Auch hinsichtlich der zu schützenden Rechtsgüter oder der zu verfolgenden Straftaten fehlt es an qualifizierenden Anforderungen. Dies gilt auch dann, wenn § 10 Abs. 1 Satz 2 BKAG-E im Zusammenhang mit der Aufgabenzuweisung in § 2 Abs. 1, Abs. 2 Nr. 1 BKAG gelesen wird, da der dort verwandte Begriff der „Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung“ wenig restriktiv gefasst ist.

Regelungstechnisch könnte § 10 Abs. 1 Satz 2 BKAG-E verfassungskonform gefasst werden, indem die Abfragebefugnis an das Erfordernis einer konkreten Gefahr oder eines Tatverdachts gebunden wird. Der Sinn der Ermächtigung läge dann vor allem darin, Krisensituationen aufzulösen oder Verdachtsmomenten nachzugehen, auf die das Bundeskriminalamt im Rahmen seiner Auswertungstätigkeit stößt. Eine Nutzung der Bestandsdatenabfrage für kriminalstrategische Analysen im Vorfeld konkreter präventivpolizeilicher oder strafprozessualer Verfahren – also im Rahmen der „Intelligence-Arbeit“ des Bundeskriminalamts – schiede hingegen aus.

Sollen dem Bundeskriminalamt hingegen Bestandsdatenabfragen gerade auch für kriminalstrategische Auswertungszwecke ermöglicht werden, müsste eine Vorfeldermächtigung geschaffen werden, deren Anwendungsbereich durch geeignete tatbestandliche Einengungen zu begrenzen wäre. Zudem müsste auch § 15 Abs. 2 Satz 1 TMG-E so angepasst werden, dass Datenübermittlungen im Gefahrvorfeld ermöglicht werden.

Schließlich verletzt § 15a Abs. 4 Satz 1 TMG-E teilweise die Kompetenzordnung. Diese Vorschrift sieht eine Übermittlungspflicht der Telemedienanbieter auch insoweit vor, als für die zugehörigen Zugriffsermächtigungen eine Gesetzgebungskompetenz der Länder besteht. Die Regelungsbefugnis für eine solche Übermittlungspflicht folgt jedoch der Regelungsbefugnis für die Abfrageermächtigung. Im Zusammenhang mit den bundesrechtlichen Zugriffsermächtigungen, die der Entwurf enthält, ist § 15a Abs. 4 Satz 1 TMG-E hingegen zwar kompetenzgemäß, aber redundant, da bereits diese Normen – systematisch korrekt – ausdrücklich eine Übermittlungspflicht begründen.[30] § 15a Abs. 4 Satz 1 TMG-E sollte daher ersatzlos gestrichen werden.

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

Zu weit gefasst und darum verfassungswidrig ist die Übermittlungserlaubnis in § 15a Abs. 1 Satz 1, Abs. 2 Satz 1, Abs. 3 TMG-E hingegen insoweit, als sie eine Übermittlung auch von Nutzungsdaten erlaubt. Daten dieser Kategorie sind zumindest in der Regel deutlich sensibler als Bestandsdaten. Eine Übermittlung kann darum nicht generell durch die Zwecke der Verfolgung von (irgendwelchen) Straftaten oder gar Ordnungswidrigkeiten, der Gefahrenabwehr sowie der Wahrnehmung nachrichtendienstlicher Aufgaben legitimiert werden. Vielmehr bedarf es einer materiell qualifizierten Eingriffsschwelle. Diese Eingriffsschwelle muss aufgrund der grund-

[30] Vgl. § 100j Abs. 5 StPO-E; § 10 Abs. 5 Satz 2 BKAG-E.

15 rechtlichen Regelungsverantwortung des Bundes zumindest insoweit zwingend im Telemedienrecht enthalten sein, als es um eine Übermittlung an Landessicherheitsbehörden geht. Diesem verfassungsrechtlichen Erfordernis wird der Entwurf nicht gerecht.

Verfassungsrechtlich problematisch ist darüber hinaus die vorgesehene strafprozessuale Zugriffsermächtigung in § 100g Abs. 1 Satz 2 StPO-E. Die geplante Norm verweist hinsichtlich der Eingriffsschwelle auf die Ermächtigung zum Zugriff auf Telekommunikations-Verkehrsdaten in § 100g Abs. 1 Satz 1 StPO-E. Danach ist der Datenzugriff zulässig zur Verfolgung von Straftaten von erheblicher Bedeutung[31] sowie von Straftaten, die mittels Telekommunikation begangen wurden. Ob diese recht offen gefasste Ermächtigung der Sensibilität von Telekommunikations-Verkehrsdaten vollauf gerecht wird, ist durchaus zweifelhaft, mag hier aber dahinstehen.[32] Beim Zugriff auf Telemedien-Nutzungsdaten verschärfen sich die Zweifel jedenfalls noch, da diese Datenkategorie schwierig abzugrenzen ist und potenziell ein extrem weites Spektrum an Datenarten umfasst, deren Aussagekraft über Telekommunikations-Verkehrsdaten noch deutlich hinausgehen kann. Angesichts dessen halte ich den Regelungsansatz von § 100g Abs. 1 Satz 2 StPO-E, den Zugriff auf Verkehrs- und Nutzungsdaten unter denselben Voraussetzungen zu ermöglichen, allenfalls dann für verfassungsrechtlich vertretbar, wenn Inhaltsdaten als eigenständige weitere Kategorie von Telemediendaten anerkannt werden und diese Kategorie so zugeschnitten wird, dass sie die besonders sensiblen Datentypen umfasst.

**4. Inhaltsüberwachung von Telemedien**

Sowohl wegen der Interpretationsprobleme im Zusammenhang mit dem Begriff der Nutzungsdaten als auch aus Gründen der Rechtssicherheit ist es misslich, dass der Entwurf keine Regelung über die Überwachung von Telemedieninhalten vorsieht. Dem liegt anscheinend die Erwägung zugrunde, solche Überwachungen könnten auf § 100a StPO gestützt werden, da der dort verwendete Begriff der Telekommunikation auch die Kommunikation mittels Telemedien umfasse.[33] Ob diese Erwägung überzeugt, mag auf sich beruhen. Es ist jedenfalls nicht ratsam, sich bei der Überarbeitung der strafprozessualen Eingriffsermächtigungen an ihr zu orientieren.

Es trifft zwar zu, dass der sicherheitsbehördliche Zugriff auf Inhalte von Telemedien bislang – soweit sie nicht offen zugänglich sind und darum durch eine verdeckte Überwachung beschafft werden müssen – üblicherweise auf § 100a StPO gestützt wird. Dies gilt insbesondere für die Inhaltsüberwachung von Over-the-Top-Diensten, die (primär) der Individualkommunikation dienen.[34] Die Einstufung solcher Dienste als Telekommunikation im Sinne von § 100a StPO bedarf jedoch möglicherweise der Revision.

---

[31] Der Straftatenkatalog des § 100a Abs. 2 StPO wird lediglich beispielhaft in Bezug genommen.
[32] 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.
[33] Vgl. BT-Drs. 19/17741, S. 36.
[34] 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.

16 Nach der Rechtsprechung des Bundesgerichtshofs deckt sich der Telekommunikationsbegriff des § 100a StPO mit dem telekommunikationsrechtlichen Telekommunikationsbegriff.[35] Aufgrund des Urteils des Gerichtshofs der Europäischen Union zu E-Mail-Diensten steht nunmehr jedoch verbindlich fest, dass Over-the-Top-Dienste zumindest in der Regel gerade keine Telekommunikationsdienste im Sinne des Telekommunikationsrechts sind. Wird die bisherige Rechtsprechung des Bundesgerichtshofs zugrunde gelegt, verengt sich reflexartig auch der strafprozessuale Telekommunikationsbegriff. Die Inhaltsüberwachung von Telemedien kann dann nicht mehr auf § 100a StPO gestützt werden.

In der juristischen Literatur wird allerdings 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.[36] 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. Hiervon geht auch die Entwurfsbegründung erkennbar aus.

Eine Stellungnahme zu dieser Kontroverse ist hier entbehrlich. In jedem Fall sollte aus Gründen der Rechtssicherheit die Inhaltsüberwachung von Telemedien ausdrücklich in § 100a StPO aufgenommen werden. Hierdurch würde eine ansonsten drohende Begriffsverwirrung vermieden. Zudem wäre klargestellt, dass es für Telemedien neben Bestands- und Nutzungsdaten eine weitere Datenkategorie gibt, deren Erhebung besonders strengen Anforderungen genügen muss. Vor allem aber hat die in der Entwurfsbegründung verfochtene Position missliche Konsequenzen für die Praktikabilität einer Inhaltsüberwachung von Telemedien. Eine solche Überwachung wird oftmals auf eine Mitwirkung des Telemedienanbieters angewiesen sein. Es gibt jedoch keine Vorschrift, die eine solche Mitwirkung eindeutig anordnet. § 100a Abs. 4 StPO verpflichtet zur Mitwirkung an Telekommunikationsüberwachungen die Anbieter von Telekommunikationsdiensten (vgl. zu diesem Begriff § 3 Nr. 24 TKG) und verweist wegen der Reichweite ihrer Mitwirkungspflicht teilweise auf das Telekommunikationsgesetz und die Telekommunikations-Überwachungsverordnung. Damit wird ausdrücklich auf das Telekommunikationsrecht Bezug genommen, dem die Anbieter von Telemediendiensten gerade nicht unterfallen.[37] Hieraus resultiert

---

[35] 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.).

[36] Vgl. zur Diskussion Graf, in: BeckOK StPO, § 100a Rn. 18 ff.; Günther, in: MüKo StPO, 2014, § 100a Rn. 26 ff.

[37] Das Bundesverfassungsgericht hat zwar erst in jüngerer Zeit keine verfassungsrechtlichen Bedenken dagegen erhoben, dass einem E-Mail-Anbieter nach § 110 TKG Mitwirkungspflichten auferlegt wurden, vgl. BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 20. Dezember 2018 – 2 BvR 2377/16 –, NJW 2019, S. 584. Die diesem Beschluss zugrunde liegenden fachgerichtlichen Entscheidungen sind jedoch aufgrund des später ergangenen Urteils des EuGH zur Einstufung von E-Mail-Diensten obsolet. Eine Anwendung von § 110 TKG auf E-Mail-Anbieter ist heute meiner Ansicht nach unabhängig von den verfassungsrechtlichen Maßstäben einfachrechtlich nicht mehr vertretbar.

17 erhebliche Rechtsunsicherheit, die den Anbietern von Telemediendiensten nicht zumutbar ist und – sofern diese eine Mitwirkung wegen des Wortlauts von § 100a Abs. 4 StPO (meines Erachtens zu Recht) verweigern – die Tätigkeit der Strafverfolgungsbehörden erheblich behindern könnte.

Über die angezeigte Ergänzung von § 100a StPO um die Telemedien-Inhaltsüberwachung hinaus sollte zudem erwogen werden, nach dem Vorbild des Telekommunikationsrechts spezifische technische Vorgaben zu schaffen, um eine wirksame Überwachung zu ermöglichen.[38]

**5. Übermittlung von und Zugriff auf Zugangsdaten**

Die auf Telemedien-Zugangsdaten bezogenen Regelungen des Entwurfs sind systematisch nicht schlüssig gestaltet, worauf bereits der Bundesrat hingewiesen hat.[39] § 15b Abs. 2 Satz 1 TMG-E errichtet sehr hohe Anforderungen an die Übermittlung solcher Daten, die sich jedoch in der vorgesehenen Zugriffsermächtigung in § 100j Abs. 1 Satz 2 StPO-E nicht wiederfinden. Im Bild der Doppeltür stellt der Entwurf eine Gartenpforte neben ein Scheunentor. Dieser Mangel an Konsistenz ist nicht lediglich ein normästhetisches Problem, sondern begründet erhebliche Anwendungsprobleme. So wird das Gericht, das den Datenzugriff erlaubt (§ 100j Abs. 3 StPO), naheliegenderweise nur prüfen, ob die Voraussetzungen der weit gefassten strafprozessualen Zugriffsermächtigung vorliegen. Der Telemedienanbieter wird dann mit einem gerichtlichen Beschluss konfrontiert, den er zu erfüllen hat, obwohl die Voraussetzungen der für ihn geltenden Übermittlungserlaubnis nicht vorliegen. Die beiden Regelungen sollten daher aufeinander abgestimmt werden.

Damit ist allerdings noch nicht gesagt, wie hoch die einheitliche gesetzliche Eingriffsschwelle angesetzt werden sollte. Im Entwurf finden sich hierzu zwei unterschiedliche Ansätze. § 15b Abs. 2 Satz 1 TMG-E bindet die Datenübermittlung an starre Voraussetzungen, die sich an den verfassungsrechtlichen Anforderungen an Online-Durchsuchungen orientieren.[40] Hingegen macht § 100j Abs. 1 Satz 2 StPO-E den Datenzugriff davon abhängig, dass die Voraussetzungen für eine strafprozessuale Nutzung der übermittelten Daten vorliegen.

Der starre Ansatz des § 15b Abs. 2 Satz 1 TMG-E ist klar vorzugswürdig. Nur er schafft Rechtssicherheit und gewährleistet zuverlässig, dass der Datenzugriff den verfassungsrechtlichen Anforderungen genügt. Die in § 15b Abs. 2 Satz 1 TMG-E vorgesehene Eingriffsschwelle ist allerdings sehr hoch angesetzt. Dies ergibt dann Sinn, wenn eine Erhebung von Telemedien-Zugangsdaten aus sicherheitsbehördlicher Sicht faktisch nur in Betracht kommt, wenn mit Hilfe der Zugangsdaten die Nutzung eines komplexen Telemediums über einen längeren Zeitraum beobachtet werden soll, so dass die Überwachung als Online-Durchsuchung einzustufen ist. Sollten hingegen auch punktuellere Datennutzungen praktisch bedeutsam sein (etwa die einmalige ge-

---

[38] Sehr unspezifisch sind hingegen die – auf Inhaltsdaten auch nicht anwendbaren – § 15a Abs. 5 und § 15b Abs. 4 TMG-E formuliert.
[39] BT-Drs. 19/18470, S. 30.
[40] BT-Drs. 19/17741, S. 39.

 zielte Suche nach bestimmten Dateien), so könnte auch überlegt werden, statt einer einheitlichen Zugriffsschwelle den Zugriff auf Zugangsdaten als Annexmaßnahme in den jeweiligen Überwachungsermächtigungen (also etwa in den Ermächtigungen zu Online-Durchsuchungen oder zu Telekommunikationsüberwachungen) mitzuregeln und die Übermittlungserlaubnis entsprechend differenziert zu gestalten.

In diesem Zusammenhang seien zwei Anmerkungen gestattet, die sich nicht unmittelbar auf den geregelten Datenzugriff beziehen, sondern auf vor- und nachgelagerte Fragen:

Erstens erscheint mir zwingend geboten, dass der Zugriff auf Zugangsdaten immer nur in der Form erfolgen kann und darf, in der diese Daten bei den Telemedienanbietern aufgrund einer technisch-organisatorisch ordnungsgemäßen Datenhaltung vorliegen. Da insbesondere die Telemedienanbieter aus Gründen der IT-Sicherheit Zugangsdaten nicht im Klartext oder in einer für sie entschlüsselbaren Form speichern dürfen, können sie lediglich Daten herausgeben (sog. Hashwerte), auf deren Grundlage die Sicherheitsbehörden – gegebenenfalls mit erheblichem Aufwand – die eigentlichen Zugangsdaten (etwa Passwörter) zu ermitteln versuchen können. Eine denkbare Pflicht der Telemedienanbieter, Zugangsdaten im Klartext für sicherheitsbehördliche Zugriffe zu bevorraten, stünde weder mit Art. 32 DSGVO noch mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in seiner objektiv-rechtlichen Dimension in Einklang.

Zweitens bedarf es für die Nutzung der erlangten Zugangsdaten jeweils besonderer Rechtsgrundlagen, die sich im Entwurf nicht finden. Insbesondere ermöglicht das geltende Strafprozessrecht mangels ausdrücklicher Ermächtigung keine Nutzung mit dem Ziel, ein Konto auf einem Telemedium (beispielsweise einem Sozialen Netzwerk) zu übernehmen, um aktiv an Kommunikationsvorgängen mit Dritten teilzunehmen oder solche Kommunikationsvorgänge gar zu initiieren. Die bestehenden Ermächtigungen zu Online-Durchsuchungen und Telekommunikationsüberwachungen ermöglichen lediglich eine passive Beobachtung solcher Kommunikationsvorgänge.

Schließlich verletzt § 15b Abs. 3 Satz 1 TMG-E teils die Kompetenzordnung und ist teils überflüssig. Insoweit gilt das oben unter II.2. zu § 15a Abs. 4 Satz 1 TMG-E Ausgeführte entsprechend.

**6. Zitiergebot**

Die Zitierung von Art. 10 GG in Art. 7 des Entwurfs bezieht sich lediglich auf Vorschriften, die eine Zuordnung von dynamischen IP-Adressen vorsehen.[41] Auch der Vorschlag des Bundesrats zur Nennung weiterer Vorschriften beruht allein auf diesem Kriterium.[42] Dieses Kriterium greift jedoch zu kurz und erfasst nicht alle Eingriffe in das Fernmeldegeheimnis, die der Entwurf ermöglicht.

---

[41] BT-Drs. 19/17741, S. 46.
[42] BT-Drs. 19/18470, S.30

19 Das Fernmeldegeheimnis ist als eingeschränktes Grundrecht für alle Regelungen zu zitieren, die einen Eingriff in dieses Grundrecht ermöglichen. Der Schutzbereich von Art. 10 GG reicht teils weiter als der Telekommunikationsbegriff des Telekommunikationsrechts. Er umfasst prinzipiell alle mit der Fernmeldetechnik ausgetauschten Informationen. Dementsprechend hat das Bundesverfassungsgericht bereits mehrfach ausgeführt, dass der Schutz dieses Grundrechts sich auf E-Mails erstreckt,[43] die einfachrechtlich als Telemedien- und nicht als Telekommunikationsdienste anzusehen sind. Da zudem das Fernmeldegeheimnis sowohl die Inhalte als auch die Umstände der grundrechtlich geschützten Kommunikation umfasst, kann insbesondere die Erhebung von Telemedien-Nutzungsdaten in Art. 10 GG eingreifen. In Art. 7 muss darum auch noch § 100g StPO-E (Art. 2 Nr. 2) aufgeführt werden.

[43] BVerfGE 113, 348 (383); 120, 274 (307); 124, 43 (54); 125, 260 (310 f.).