Prof. Dr. Matthias Bäcker, LL.M. Mannheim, den 16. September 2020

Folgerungen aus dem zweiten Bestandsdatenbeschluss des BVerfG für die durch das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität geschaffenen Datenverarbeitungsregelungen

Rechtsgutachten im Auftrag der Bundestagsfraktion Bündnis 90/Die Grünen

Inhalt

Ergebnisse
Auf der Grundlage des zweiten Bestandsdatenbeschlusses des BVerfG (vom 27. Mai 2020 – Az. 1 BvR 1873/13, 2618/13) sind die Regelungen des Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität über Übermittlung und Weiterverarbeitung von Telemediendaten wie folgt zu bewerten:

1. Offensichtlich verfassungswidrig sind

    a) § 15a Abs. 1 Sätze 1 und 3, Abs. 2 Satz 1, Abs. 3 Satz 1 Nr. 1, 2 und 4 TMG, soweit die Übermittlung von Bestandsdaten durch Zuordnung einer IP-Adresse an Strafverfolgungs-, Gefahrenabwehr-, Zoll- und Gewerbebehörden erlaubt wird,

    b) die Ermächtigung zum Abruf von Zugangsdaten in § 100j Abs. 1 Satz 2,

    c) die aus § 46 Abs. 2 OWiG i.V.m. § 100j Abs. 1 Satz 1 Nr. 2 StPO folgende Ermächtigung, Bestandsdaten unter Zuordnung einer IP-Adresse abzurufen, um jegliche Ordnungswidrigkeiten zu verfolgen,

    d) die Ermächtigung zum Abruf von Bestandsdaten – mit oder ohne Zuordnung einer IP-Adresse – in § 10 Abs. 1 Sätze 1 und 2 BKAG.

2. In einem Verfahren vor dem BVerfG würden mit hoher Wahrscheinlichkeit als verfassungswidrig eingestuft

    a) § 15a Abs. 1 Satz 1, Abs. 2 Satz 1 Nr. 3, Abs. 3 Satz 1 Nr. 4 TMG, soweit die Übermittlung von Bestandsdaten ohne Zuordnung einer IP-Adresse an Zoll- und Gewerbebehörden zur Verhütung bestimmter Straftaten und Ordnungswidrigkeiten erlaubt wird,

    b) § 15a Abs. 1 Satz 1, Abs. 2 Satz 1, Abs. 3 Satz 1 TMG, soweit die Übermittlung von Nutzungsdaten erlaubt wird.

3. Wegen verfassungsrechtlicher Zweifelsfragen erscheint der Ausgang einer verfassungsgerichtlichen Kontrolle offen hinsichtlich

    a) von § 15a Abs. 1 Satz 1, Abs. 2 Satz 1 Nr. 3, Abs. 3 Satz 1 Nr. 4 TMG, soweit die Übermittlung von Bestandsdaten ohne Zuordnung einer IP-Adresse an Zoll- und Gewerbebehörden zur Wahrnehmung der Prüfungsaufgaben nach § 2 Abs. 1 und 3 SchwarzArbG erlaubt wird,

    b) der Ermächtigung zum Abruf von Nutzungsdaten zum Zweck der Strafverfolgung in § 100g Abs. 1 Sätze 1 und 2 StPO,

    c) der Ermächtigung zum Abruf von Zugangsdaten in § 10 Abs. 1 Satz 3 BKAG.

4. Keine verfassungsrechtlichen Bedenken bestehen gegen

    a) § 15a Abs. 1 Satz 1, Abs. 2 Satz 1, Abs. 3 Satz 1 Nr. 1 bis 3 TMG, soweit die Übermittlung von Bestandsdaten ohne Zuordnung einer IP-Adresse erlaubt wird,

b) § 15a Abs. 1 Sätze 1 und 3, Abs. 2 Satz 1 Nr. 3, Abs. 3 Satz 1 Nr. 3 TMG, soweit die Übermittlung von Bestandsdaten durch Zuordnung einer IP-Adresse an Nachrichtendienste erlaubt wird,

c) die Erlaubnis zur Übermittlung von Zugangsdaten in § 15b Abs. 1 Satz 1, Abs. 2 Satz 1 TMG,

d) die Ermächtigung zum Abruf von Bestandsdaten, auch unter Zuordnung einer IP-Adresse, zur Strafverfolgung in § 100j Abs. 1 Satz 1 Nr. 2 StPO,

e) die Ermächtigung zum Abruf von Identifikationsdaten in § 10a Abs. 1 BKAG,

f) (bei isolierter Betrachtung) die Übermittlungspflicht in § 3a Abs. 2 und 4 NetzDG; es fehlt jedoch an der zwingend erforderlichen korrespondierenden Weiterverarbeitungsermächtigung im BKAG.

I. Gutachtenauftrag

Die Bundestagsfraktion Bündnis 90/Die Grünen hat mich beauftragt, in einem Rechtsgutachten die Konsequenzen zu erörtern, die sich aus dem zweiten Bestandsdatenbeschluss des BVerfG[1] für die durch das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität in seiner vom Bundestag verabschiedeten Fassung[2] geschaffenen Datenverarbeitungsregelungen ergeben. Die mir vorgelegte Leistungsbeschreibung lautet:

> „Rechtsgutachtliche Prüfung und Stellungnahme, inwieweit sich aus dem am 17. Juli 2020 veröffentlichten Beschluss des Bundesverfassungsgerichts vom 27. Mai 2020 - 1 BvR 1873/13, 1 BvR 2618/13 (Bestandsdatenauskunft II) Folgerungen (Änderungsnotwendigkeiten) für das am 18.Juni 2020 in der Fassung der Beschlussempfehlung auf Drs 19/20163 vom Bundestag beschlossene (mit Stand 16.9.2020 noch nicht verkündete) ‚Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität' ergeben für die dort geschaffenen neuen Regelungen im Telemediengesetz, in der Strafprozessordnung, im Bundeskriminalamtgesetz und im Netzwerkdurchsetzungsgesetz, und wie derartige Änderungen verfassungskonform auszugestalten sind (Regelungsvorschläge, kein förmlicher Gesetzentwurf)."

Die Gutachtenfrage bedarf zweier Vorklärungen (unten II). Im Anschluss wird die Verfassungsmäßigkeit der durch das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität geschaffenen Datenübermittlungserlaubnisse (unten III) und Datenabrufermächtigungen (unten IV) sowie der in das NetzDG eingefügten Pflicht zur Meldung bestimmter Inhalte an das BKA (unten V) im Einzelnen erörtert.

II. Vorklärungen

Um die durch das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität geschaffenen Regelungen verfassungsrechtlich zu würdigen, bedarf es zweier Vorklärungen. Die erste betrifft die rechtliche Strukturierung des behördlichen Zugriffs auf private Datenbestände. Zweitens hängt die Frage, ob und welche Folgerungen sich aus dem zweiten Bestandsdatenbeschluss für das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität ziehen lassen, maßgeblich davon ab, inwieweit sich die in diesem Beschluss behandelten Kategorien von Telekommunikationsdaten und die hier in Rede stehenden Telemediendaten hinsichtlich ihrer grundrechtlichen Sensibilität vergleichen lassen.

1. Rechtliche Strukturierung des behördlichen Zugriffs auf private Datenbestände

Das BVerfG geht im zweiten Bestandsdatenbeschluss von der mittlerweile in der Rechtsprechung etablierten zweigliedrigen Struktur des sicherheitsbehördlichen Zu-

---

[1] BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13; der Beschluss wird im Folgenden nach Randnummern zitiert.
[2] BT-Drs. 19/20163.

griffs auf private Datenbestände aus, die das Gericht mit dem – gleichfalls seit geraumer Zeit eingeführten – Bild einer Doppeltür illustriert.[3] Ein solcher Zugriff vollzieht sich danach in zwei Schritten, die jeweils eigenständiger Regelung bedürfen.

Erstens benötigt die private Stelle, die Daten an eine Sicherheitsbehörde übermitteln soll, hierzu eine gesetzliche Übermittlungserlaubnis.[4] Die Gesetzgebungskompetenz hierfür liegt bei dem Gesetzgeber, der für den Datenschutz bei der privaten Stelle hinsichtlich der betroffenen Datenkategorien zuständig ist.[5] Dieser Gesetzgeber trägt zugleich eine grundrechtliche Regelungsverantwortung für den Gesamtvorgang. Er muss durch normenklare Regelungen gewährleisten, dass der behördliche Zugriff auf die übermittelten Daten einem hinreichend gewichtigen Ziel dient und an eine hinreichende tatsächliche Eingriffsschwelle gebunden wird.[6]

Zweitens benötigt die Sicherheitsbehörde, die auf die Daten zugreifen soll, eine gesetzliche Zugriffsermächtigung.[7] Die Gesetzgebungskompetenz hierfür liegt bei dem Gesetzgeber, der für das Fachrecht der jeweiligen Sicherheitsbehörde zuständig ist.[8] Wenn für Übermittlungserlaubnis und Zugriffsermächtigung derselbe Gesetzgeber zuständig ist, kann er beide Komponenten in einer gemeinsamen Norm zusammenführen, muss dies allerdings hinreichend deutlich machen.[9] Im Übrigen darf die Zugriffsermächtigung hinsichtlich der Zugriffsvoraussetzungen strenger ausgestaltet werden als die Übermittlungserlaubnis.[10] Hingegen dürfen die Voraussetzungen der Zugriffsermächtigung aus Gründen der Normenklarheit[11] nicht hinter der Übermittlungserlaubnis zurückbleiben. Dies gilt auch dann, wenn die Übermittlungserlaubnis die Übermittlung an strengere Voraussetzungen bindet als es verfassungsrechtlich zwingend geboten wäre. Die Verfassungswidrigkeit der zu weit gefassten Zugriffsermächtigung ergibt sich in einem solchen Fall aus dem rechtsstaatswidrigen Widerspruch zwischen beiden Regelungen, nicht aus einem Unterschreiten des grundrechtlichen Mindeststandards.[12]

Die Ausführungen des BVerfG im zweiten Bestandsdatenbeschluss beziehen sich – entsprechend dem Verfahrensgegenstand – unmittelbar nur auf Datenübermittlungen, denen ein Abruf durch die zugreifende Sicherheitsbehörde vorausgeht. Es liegt jedoch auf der Hand, dass die hierzu getroffenen Aussagen sich im Ansatz auf Datenübermittlungen ohne vorausgehenden Abruf (sog. Spontanübermittlungen) übertragen lassen. Die zweigliedrige Struktur der Datenübermittlung folgt datenschutzrechtlichen Formungen, die für Spontanübermittlungen gleichfalls gelten. Eine private Stelle, die

---

[3] Rn. 93.
[4] Rn. 93.
[5] Rn. 105.
[6] Rn. 130, 134.
[7] Rn. 93.
[8] Rn. 108.
[9] Rn. 134.
[10] Rn. 130, 201.
[11] Bei einem – für dieses Gutachten nicht relevanten – Auseinanderfallen der Gesetzgebungskompetenzen für Übermittlungserlaubnis und Zugriffsermächtigung treten kompetenzrechtliche Gründe hinzu.
[12] Rn. 198 ff.

von sich aus Daten an eine Sicherheitsbehörde übermittelt, verarbeitet die übermittelten Daten und benötigt hierzu eine Erlaubnis. Unter anderem kann sich eine solche Erlaubnis aus einer Rechtspflicht zur Datenübermittlung ergeben.[13] Hinsichtlich der Gesetzgebungskompetenz und der Übermittlungsvoraussetzungen können für eine solche Übermittlungserlaubnis keine anderen verfassungsrechtlichen Anforderungen gelten als für eine Erlaubnis zu Datenübermittlungen auf Abruf. Die Sicherheitsbehörde, welche die Daten erhält, benötigt zwar zur bloßen Entgegennahme der Daten wohl noch keine gesetzliche Ermächtigung. Denn hierin dürfte noch keine Datenverarbeitung liegen, die einen Grundrechtseingriff und einen datenschutzrechtlichen Regelungsbedarf auslösen würde. Eine gesetzliche Ermächtigung ist jedoch jedenfalls erforderlich, sobald die Behörde die Daten zweckgerichtet weiterverarbeitet.[14]

Ungeklärt ist allerdings bislang, ob sich sämtliche Anforderungen, die sich aus den Grundrechten und dem Gebot der Normenklarheit für Abrufermächtigungen ergeben, ohne weiteres auf solche Weiterverarbeitungsermächtigungen erstrecken lassen. Soweit es um Spontanübermittlungen geht, die eine private Stelle aufgrund einer bloßen Übermittlungs*erlaubnis aus* eigenem Antrieb vornimmt, spricht hiergegen, dass sich solche Übermittlungen nicht durchweg im Einzelnen voraussehen lassen. Darum kann auch die Weiterverarbeitung der übermittelten Daten nicht präzise reguliert werden. Für die Weiterverarbeitung von Daten in solchen Fällen sollte darum eine allgemeine Ermächtigung zur Datenerhebung oder zur Datenverarbeitung ausreichen.[15] Beruht die Spontanübermittlung hingegen auf einer gesetzlichen Übermittlungs*pflicht*, so ist sie voraussehbar und regelbar.[16] Diese Erwägung spricht dafür, dass für gesetzliche Übermittlungspflichten zumindest grundsätzlich korrespondierende spezifische Weiterverarbeitungsermächtigungen zu schaffen sind, an die dieselben Anforderungen bestehen wie sie für gesetzliche Abrufermächtigungen gelten.

2. Eingriffsintensität des behördlichen Zugriffs auf Telemediendaten

Die Anforderungen an die gesetzlichen Übermittlungs- und Zugriffsvoraussetzungen hängen maßgeblich davon ab, wie intensiv die Datenübermittlung und die Weiterverarbeitung der übermittelten Daten in Grundrechte eingreifen. Für die Zwecke dieses Gutachtens ist vor allem wesentlich, inwieweit sich die Sensibilität der vom BVerfG im zweiten Bestandsdatenbeschluss behandelten Datenkategorien mit den im Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität behandelten Datenkategorien vergleichen lässt.

Das BVerfG befasst sich mit drei Datenkategorien: erstens mit Telekommunikations-Bestandsdaten allgemein, zweitens mit Telekommunikations-Bestandsdaten in dem Sonderfall, dass das auskunftsverpflichtete Unternehmen zur Beauskunftung eine dynamische IP-Adresse zuordnen muss, und drittens mit Zugangsdaten, die den Zugriff

---

[13] Vgl. Art. 6 Abs. 1 Satz 1 lit. c DSGVO.

[14] Vgl. für die hier interessierenden Tätigkeitsfelder der Verhütung und Verfolgung von Straftaten Art. 8 Abs. 1 RL (EU) 2016/680.

[15] Vgl. dazu, dass eine solche allgemeine Ermächtigung nicht für gezielte Abrufersuchen ausreicht, Rn. 196.

[16] Den Gesichtspunkt der Übermittlungsverpflichtung hebt hervor Rn. 196.

auf Endgeräte oder Speichereinrichtungen schützen. Das Gericht arbeitet die Sensibilität dieser Datenkategorien differenziert heraus und stellt an den Datenaustausch jeweils unterschiedliche Anforderungen.[17] Als allgemeine Kriterien zur Bestimmung der Eingriffsintensität nennt das BVerfG Art, Umfang und denkbare Verwendung der Daten sowie die Gefahr ihres Missbrauchs. Das Gericht verdichtet diese Kriterien sogleich auf die Zahl der Betroffenen und die Intensität der Beeinträchtigung.[18]

Das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität befasst sich mit drei Datenkategorien, die parallel zu den genannten Kategorien von Telekommunikationsdaten gehandhabt werden, nämlich erstens Telemedien-Bestandsdaten, zweitens Telemedien-Bestandsdaten in dem Sonderfall, dass das auskunftsverpflichtete Unternehmen zur Beauskunftung eine IP-Adresse[19] zuordnen muss, und drittens Passwörter und Zugangsdaten, die den Zugriff auf Endgeräte oder Speichereinrichtungen schützen. Es ist anzunehmen, dass die vom BVerfG herausgearbeiteten Anforderungen an den Abruf von Telekommunikationsdaten sich auf die entsprechenden Telemediendaten vollständig übertragen lassen. Hierfür lässt sich nicht nur die sprachliche und rechtssystematische Übereinstimmung der jeweiligen Datenkategorien anführen. Für eine Gleichsetzung der Sensibilität und damit der Eingriffsintensität sprechen auch die vom BVerfG angeführten Sachargumente.

Die Übermittlung von Telekommunikations-Bestandsdaten ist nach dem BVerfG ein Eingriff in das Recht auf informationelle Selbstbestimmung von „gewissem, wenn auch nicht sehr großem Gewicht“. Hierzu hebt das BVerfG auf die in § 111 TKG geregelte großflächige Datenbevorratung, die Verfügbarkeit individualisierender Angaben und die Heimlichkeit der Auskunftserteilung ab. Als intensitätsreduzierende Faktoren nennt das Gericht den Einzelfallbezug der Auskunftserteilung, die enge inhaltliche Begrenzung der Daten und den Umstand, dass teils von Entscheidungen der Telekommunikationsunternehmen abhängt, ob und welche Bestandsdaten verfügbar sind.[20] Die Sensibilität von Telemedien-Bestandsdaten bleibt hinter Telekommunikations-Bestandsdaten unter diesen Gesichtspunkten insoweit zurück, als es für Telemedienanbieter keine mit § 111 TKG vergleichbare Bevorratungspflicht gibt. Andererseits können Telemedien-Bestandsdaten je nach Telemedium weitaus aussagekräftiger sein als Telekommunikations-Bestandsdaten. Während praktisch jedermann Telekommunikationsdienste nutzt, kann schon die Information, dass eine Person einen bestimmten Telemediendienst in Anspruch nimmt, durchaus sensibel sein, etwa bei thematisch spezialisierten internetbasierten Verkaufs- oder Informationsplattformen. Zudem können Telemedien-Bestandsdaten sich auf mehr und persönlichkeitsrelevantere Informationen erstrecken als Telekommunikations-Bestandsdaten, etwa wenn ein Tele-

[17] Vgl. zu Bestandsdaten Rn. 138 ff. und 165 ff. sowie zu Zugangsdaten rudimentär Rn. 162.
[18] Rn. 129.
[19] Beim Abruf von Telemedien-Bestandsdaten macht es grundsätzlich keinen Unterschied, ob eine dynamische oder eine statische IP-Adresse aufgelöst wird. Für den Telemedienanbieter handelt es sich bei der IP-Adresse, von der ein bestimmter Kommunikationskontakt ausging, in jedem Fall um ein Nutzungsdatum, das zum Zweck der Beauskunftung mit unternehmensinternen Datenbeständen (vor allem Bestandsdaten) verknüpft wird.
[20] Rn. 138 ff.

mediendienst darauf beruht, den Nutzer*innen personalisierte Angebote aufgrund eines bei Beginn des Vertragsverhältnisses erstellten Interessenprofils zu unterbreiten. Insgesamt kann darum die Eingriffsintensität eines Telemedien-Bestandsdatenabrufs im Einzelfall weit über einen Abruf von Telekommunikations-Bestandsdaten hinausreichen. Im Rahmen einer typisierenden Betrachtungsweise erscheint es insgesamt angemessen, gemittelt über alle Anbieter die Sensibilität von Telekommunikations- und Telemedien-Bestandsdaten gleich zu veranschlagen.

Das Eingriffsgewicht der Übermittlung von Telekommunikations-Bestandsdaten steigt, wenn zum Zweck der Beauskunftung eine dynamische IP-Adresse zugeordnet wird. Zur Begründung verweist das BVerfG darauf, dass in diesem Fall ein Eingriff in das Fernmeldegeheimnis des Art. 10 GG und nicht lediglich in das Recht auf informationelle Selbstbestimmung vorliegt. Die Beauskunftung wirke auf die Kommunikationsbedingungen im Internet ein und begrenze den Umfang ihrer Anonymität, auch im Zusammenwirken mit der – derzeit allerdings weitgehend nicht vollzogenen – Bevorratungspflicht des § 113b Abs. 3 TKG. Zudem müssten die Diensteanbieter zur Beauskunftung Verkehrsdaten verarbeiten, denen von vornherein eine höhere Persönlichkeitsrelevanz zukomme als reinen Bestandsdaten.[21] Bei der Beauskunftung von Telemedien-Bestandsdaten anhand einer IP-Adresse kommt mangels einer Bevorratungspflicht wiederum ein intensitätssteigernder Rückgriff auf Vorratsdaten nicht in Betracht.[22] Zudem greift die Beauskunftung je nach Telemedium nicht durchweg in das Fernmeldegeheimnis, sondern teils lediglich in das Recht auf informationelle Selbstbestimmung ein.[23] In jedem Fall müssen jedoch für die Beauskunftung Nutzungsdaten verarbeitet werden, die zumindest typischerweise deutlich sensibler sind als Bestandsdaten. Das Sachargument, mit dem das BVerfG die besondere Eingriffsintensität begründet, lässt sich daher übertragen. Zudem gilt wiederum, dass Telemedien-Bestandsdaten eine höhere Sensibilität aufweisen können als Telekommunikations-Bestandsdaten. Hinzu kommt, dass bei der Beauskunftung von Telekommunikations-Bestandsdaten anhand einer dynamischen IP-Adresse die anfragende Sicherheitsbehörde bereits weiß, dass die betroffene Person Kundin des angefragten Unternehmens ist, und lediglich deren Identität erfahren möchte. Hingegen könnte ein Abruf von Telemedien-Bestandsdaten anhand einer IP-Adresse auch dazu genutzt werden herauszufinden, ob die Adressinhaberin einen bestimmten Telemediendienst überhaupt nutzt. Insgesamt erscheint es wiederum angemessen, das Eingriffsgewicht der Beauskunftung von Telekommunikations- und Telemedien-Bestandsdaten typisierend gleichzusetzen.

---

[21] Rn. 165 ff.

[22] In dem Sonderfall, dass ein Telemedienanbieter zugleich bevorratungspflichtiger Telekommunikationsanbieter ist, scheidet ein Rückgriff auf die bevorrateten Telekommunikations-Verkehrsdaten gleichfalls aus, da die Beauskunftung nach § 15a TMG nicht in dem abschließenden Katalog von Verwendungszwecken in § 113c Abs. 1 TKG aufgeführt wird.

[23] Hierfür kommt es darauf an, ob der Telemedienanbieter als Intermediär einen Kommunikationskontakt zwischen mindestens zwei anderen Personen vermittelt hat (beispielsweise bei einem E-Mail-Anbieter, dann ist Art. 10 GG einschlägig) oder ob er selbst Kommunikationspartner der betroffenen Person war (beispielsweise bei einem Online-Shop, dann ist der Datenabruf am Recht auf informationelle Selbstbestimmung zu messen).

Ohne Weiteres vergleichen lassen sich schließlich der Abruf von Zugangsdaten bei Telekommunikations- und bei Telemedienanbietern. Maßgeblich für die verfassungsrechtliche Beurteilung ist, dass es für einen solchen Abruf prinzipiell nur dann einen legitimen Grund gibt, wenn die Voraussetzungen vorliegen, um das Zugangsdatum zu nutzen.[24] Dies gilt unabhängig davon, ob die Zugangsdaten bei einem Telekommunikations- oder bei einem Telemedienanbieter vorliegen.

Schließlich regelt das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität sicherheitsbehördliche Zugriffe auf Telemedien-Nutzungsdaten und damit eine weitere Datenkategorie, die im zweiten Bestandsdatenbeschluss keine Entsprechung findet. Gleichwohl lassen sich dem Beschluss zumindest Anhaltspunkte für die Behandlung von Nutzungsdaten entnehmen. Rechtssystematisch entsprechen Telemedien-Nutzungsdaten den Telekommunikations-Verkehrsdaten. Die verfassungsrechtlich bedeutsame Sensibilität von Nutzungsdaten kann allerdings je nach Telemedium sehr unterschiedlich ausfallen. Unklar ist zudem, ob im Telemedienrecht ebenso wie im Telekommunikationsrecht noch eine weitere (ungeschriebene) Kategorie der Inhaltsdaten anzuerkennen ist und wie diese gegebenenfalls von Nutzungsdaten abzugrenzen sind.[25] Ob sich die Eingriffsintensität von Zugriffen auf Nutzungsdaten und auf Verkehrsdaten in vergleichbarer Weise typisierend gleichsetzen lässt, wie dies oben für Bestandsdaten begründet wurde, erscheint daher offen. Möglicherweise müssen Nutzungsdaten sogar als sensibler angesehen werden.[26] In jedem Fall aber sind Nutzungsdaten typischerweise sensibler als Bestandsdaten, da sie das Kommunikationsverhalten einer Person und nicht lediglich die Rahmenbedingungen ihrer Kommunikation zum Gegenstand haben und bei umfassender Erhebung und Auswertung die Erstellung aussagekräftiger Persönlichkeits- und Verhaltensprofile ermöglichen.[27] Der Abruf von Nutzungsdaten greift daher mit deutlich gesteigerter Intensität in Grundrechte ein, was sich in strengeren Anforderungen an das Eingriffsziel und die tatsächliche Eingriffsschwelle niederschlägt.

III. Erlaubnisse zur Übermittlung von Telemediendaten

Die für die Telemedienabieter erforderlichen Erlaubnisse zur Übermittlung von Telemediendaten an Sicherheitsbehörden finden sich in § 15a und § 15b TMG. Die Erlaubnisregelungen genügen auf der Grundlage des zweiten Bestandsdatenbeschlusses nur zum Teil den verfassungsrechtlichen Anforderungen. Teils sind sie hingegen offensichtlich verfassungswidrig, teils bestehen gegen sie zumindest erhebliche verfassungsrechtliche Bedenken.

1. Übermittlung von Bestandsdaten, § 15a Abs. 1 Satz 1, Abs. 2 Satz 1, Abs. 3 Satz 1 TMG

Soweit § 15a Abs. 1 Satz 1, Abs. 2 Satz 1, Abs. 3 Satz 1 TMG den Telemedienanbietern allgemein erlauben, Bestandsdaten ihrer Kunden an Sicherheitsbehörden zu

---

[24] Rn. 160 unter Verweis auf BVerfGE 130, 151 (209).
[25] Vgl. meine Stellungnahme für die öffentliche Anhörung des Rechtsausschusses vom 4. Mai 2020, S. 10 ff.
[26] In diese Richtung meine Stellungnahme für die öffentliche Anhörung des Rechtsausschusses vom 4. Mai 2020, S. 15.
[27] Vgl. zur höheren Sensibiltät von Verkehrsdaten im Vergleich zu Bestandsdaten Rn. 168.

übermitteln, bestehen gegen die gesetzlichen Übermittlungserlaubnisse teilweise verfassungsrechtliche Bedenken. Insbesondere errichten diese Normen zwar weitgehend, aber nicht durchweg hinreichend strenge Tatbestandsvoraussetzungen, um die Übermittlung zu legitimieren.

Von Verfassungs wegen muss die Übermittlung bei präventiver Zielsetzung mindestens an eine konkrete Gefahr, eine „konkretisierte Gefahr“ für ein Rechtsgut von zumindest erheblichem Gewicht oder eine „drohende Gefahr“ für ein besonders gewichtiges Rechtsgut gebunden werden. Dies gilt für alle präventiv tätigen Behörden, insbesondere auch die Nachrichtendienste. Bei repressiver Zielsetzung ist der Anfangsverdacht einer Straftat oder einer Ordnungswidrigkeit zu fordern.[28]

Nach diesen Maßstäben sind die in § 15a Abs. 2 Satz 1 TMG geregelten Voraussetzungen einer Datenübermittlung zwar recht unscharf formuliert, reichen aber bei verfassungskonformer Auslegung überwiegend noch aus. Teils zu weit geht allerdings die in § 15a Abs. 2 Satz 1 Nr. 3, Abs. 3 Satz 1 Nr. 4 TMG geregelte Übermittlungserlaubnis.

Gemäß § 15a Abs. 2 Satz 1 Nr. 1, Abs. 3 Satz 1 Nr. 1 TMG dürfen Telemedienanbieter Bestandsdaten an Strafverfolgungsbehörden übermitteln, wenn dies im Einzelfall verlangt wird und erforderlich ist zur Verfolgung von Straftaten oder Ordnungswidrigkeiten. Das BVerfG hat aus den Vorgaben, dass es um einen Einzelfall gehen und die Übermittlung erforderlich sein muss, in seinem ersten Bestandsdatenbeschluss von 2012 zu § 113 TKG a.F. gefolgert, dieser Übermittlungstatbestand setze einen strafprozessualen Anfangsverdacht voraus.[29] Das BVerfG hat diese Passage des ersten Bestandsdatenbeschlusses affirmativ aufgegriffen.[30] Auch wenn diese Interpretation nicht zwingend erscheint, wird sie hier zumindest im Sinne einer verfassungskonformen Auslegung zugrunde gelegt. Wird § 15a Abs. 2 Satz 1 Nr. 1, Abs. 3 Satz 1 Nr. 1 TMG in diesem Sinne gelesen, errichtet die Norm angesichts der begrenzten Eingriffsintensität des Bestandsdatenabrufs hinreichende Übermittlungsvoraussetzungen.

§ 15a Abs. 2 Satz 1 Nr. 2, Abs. 3 Satz 1 Nr. 2 TMG erlaubt eine Datenübermittlung, wenn sie im Einzelfall verlangt wird und erforderlich ist zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung. Diese Übermittlungsvoraussetzung hat das BVerfG in seinem ersten Bestandsdatenbeschluss als konkrete Gefahr im polizeirechtlichen Sinne interpretiert und für hinreichend gehalten.[31] Diese Bewertung gilt nach wie vor.[32]

Nach § 15a Abs. 2 Satz 1 Nr. 3, Abs. 3 Satz 1 Nr. 3 TMG ist eine Datenübermittlung an die Nachrichtendienste von Bund und Ländern zulässig, wenn sie im Einzelfall verlangt wird und zur Erfüllung der gesetzlichen Aufgaben der Dienste erforderlich ist. Diesen Übermittlungstatbestand hat das BVerfG in seinem ersten Bestandsdatenbe-

---

[28] Vgl. zur Übermittlung von Telekommunikations-Bestandsdaten Rn. 145 ff.
[29] BVerfGE 130, 151 (206).
[30] Rn. 157.
[31] BVerfGE 130, 151 (205 f.).
[32] Vgl. wiederum Rn. 157.

schluss so interpretiert, dass die Übermittlung zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung geboten sein muss.[33] Auf der Grundlage dieser Interpretation handelt es sich hierbei, gemessen an den im zweiten Bestandsdatenbeschluss ausgeführten Präzisierungen zu den verfassungsrechtlichen Anforderungen an die Eingriffsvoraussetzungen des Nachrichtendienstrechts, um eine „konkretisierte Gefahr“ für ein besonders gewichtiges Rechtsgut.[34] Dieses Erfordernis genügt (nach wie vor) den verfassungsrechtlichen Anforderungen.

Kein Pendant im Telekommunikationsrecht fand und findet schließlich § 15a Abs. 2 Satz 1 Nr. 3, Abs. 3 Satz 1 Nr. 4 TMG, der eine Datenübermittlung an die Behörden der Zollverwaltung und die nach Landesrecht zuständigen Behörden erlaubt, wenn sie im Einzelfall verlangt wird und erforderlich ist zur Wahrnehmung von deren Prüfungsaufgaben nach § 2 Abs. 1 und 3 SchwarzArbG oder für die Verhütung und Verfolgung von damit zusammenhängenden Straftaten und Ordnungswidrigkeiten. Dieser Übermittlungstatbestand ist in zweierlei Hinsicht verfassungsrechtlich problematisch.

Erstens beschreiben § 2 Abs. 1 und 3 SchwarzArbG die in Bezug genommenen Prüfungsaufgaben rein final, ohne eine ausdrückliche tatsächliche Eingriffsschwelle zu errichten. Auch die allgemeinen Vorgaben eines Einzelfallbezugs und der Erforderlichkeit der Datenübermittlung gewährleisten für sich genommen noch nicht, dass die Datenübermittlung an einen hinreichenden tatsächlichen Eingriffsanlass gebunden wird. Der Übermittlungstatbestand lässt sich allerdings möglicherweise mit der Erwägung noch halten, dass die Prüfungsaufgaben ihrerseits an bestimmte wirtschaftliche Verhaltensweisen (wie die Beauftragung oder Erbringung von Dienst- oder Werkleistungen oder die Beschäftigung von Arbeitnehmer*innen) anknüpfen und hierdurch die Prüfungstätigkeit auch in tatsächlicher Hinsicht begrenzen.[35] Sodann könnte der Bekämpfung der in § 2 Abs. 1 und 3 SchwarzArbG genannten Rechtsverstöße auch ein gesteigertes Gewicht zuerkannt werden, so dass die Anforderungen an den Rechtsgüterschutz im Gefahrvorfeld noch gewahrt sind. Gleichwohl verbleiben zumindest verfassungsrechtliche Zweifel. Vorzugswürdig wäre eine Tatbestandsfassung, die ausdrücklich klarstellt, ob die Übermittlung einen Anlass im Einzelfall voraussetzt oder ob sie auch (möglicherweise beschränkt auf gewichtigere Rechtsverstöße) stichprobenartige Kontrollen ermöglichen soll.

Zweitens ist der Begriff der Verhütung von Straftaten und Ordnungswidrigkeiten sehr unscharf und errichtet für sich genommen auch in Verbindung mit den Vorgaben der Erforderlichkeit und eines Einzelfallbezugs noch keine Anforderungen an den tatsächlichen Eingriffsanlass. Das BVerfG betont vielmehr gerade für die Verhütung von Straftaten, dass es einer normenklar zu regelnden tatsächlichen Eingriffsschwelle bedarf.[36] An derartigen eingrenzenden Vorgaben fehlt es in § 15a Abs. 2 Satz 1 Nr. 3, Abs. 3

---

[33] BVerfGE 130, 151 (206).
[34] Vgl. Rn. 151.
[35] Vgl. allgemein zur Zulässigkeit anlassunabhängiger stichprobenartiger Kontrollen etwa im Wirtschaftsverwaltungsrecht BVerfGE 150, 244 (282).
[36] Rn. 225, 231; vgl. im Kontext von Datenübermittlungen bereits BVerfGE 141, 220 (336).

Satz 1 Nr. 4 TMG vollständig. Es spricht darum viel dafür, dass diese Übermittlungserlaubnis zumindest insoweit verfassungswidrig ist, als sie die Verhütung von Straftaten und Ordnungswidrigkeiten zum Gegenstand hat. Diese Tatbestandsalternative sollte daher gestrichen und durch eine Normfassung ersetzt werden, die klarstellt, dass eine Übermittlung die konkrete Gefahr bestimmter Straftaten voraussetzt.

2. Übermittlung von Bestandsdaten bei Zuordnung anhand einer IP-Adresse, § 15a Abs. 1 Sätze 1 und 3, Abs. 2 Satz 1, Abs. 3 Satz 1 TMG

In weitem Umfang offensichtlich verfassungswidrig sind die Übermittlungserlaubnisse in § 15a Abs. 1 Sätze 1 und 3, Abs. 2 Satz 1, Abs. 3 Satz 1 TMG, soweit sie die Übermittlung von Bestandsdaten regeln, die einer bestimmten Person auf der Grundlage einer IP-Adresse zugeordnet werden.[37]

Das gesteigerte Eingriffsgewicht, das der Zuordnung einer IP-Adresse zukommt, muss durch strengere Übermittlungsvoraussetzungen ausgeglichen werden. Hierzu sind qualifizierte Anforderungen an das Eingriffsziel zu stellen. Im Bereich der Gefahrenabwehr bedarf es einer konkreten Gefahr für ein Rechtsgut von hervorgehobenem Gewicht, worunter insbesondere die strafrechtlich geschützten Rechtsgüter fallen. Soweit der Übermittlungsanlass ins Gefahrvorfeld verlegt wird, ist eine „konkretisierte Gefahr“ für ein besonders gewichtiges Rechtsgut zu verlangen, das in der Übermittlungsregelung normenklar zu beschreiben ist. Ist die Gefahrenabwehr auf die Verhütung von Straftaten bezogen, muss es sich um schwere Straftaten handeln, die in der Übermittlungserlaubnis abschließend festzulegen sind. Für den Bereich der Nachrichtendienste ist den Anforderungen an das Übermittlungsziel allerdings schon dadurch genügt, dass sich ihre Tätigkeit generell auf den Schutz besonders gewichtiger Rechtsgüter beschränkt. Im repressiven Handlungsfeld bedarf es des Anfangsverdachts einer Straftat oder einer besonders gewichtigen, in der Übermittlungserlaubnis ausdrücklich zu benennenden Ordnungswidrigkeit.[38]

Nach diesen Maßgaben verfehlen die Übermittlungserlaubnisse in § 15a Abs. 2 Satz 1, Abs. 3 Satz 1 in weitem Umfang offensichtlich die verfassungsrechtlichen Anforderungen, soweit sie eine Übermittlung von Bestandsdaten auf der Grundlage einer IP-Adresse ermöglichen.

§ 15a Abs. 2 Satz 1 Nr. 1, Abs. 3 Satz 1 Nr. 1 TMG erlaubt die Datenübermittlung zur Verfolgung jedweder Straftaten und Ordnungswidrigkeiten. Es fehlt damit hinsichtlich der erfassten Ordnungswidrigkeiten an der gebotenen tatbestandlichen Eingrenzung.[39]

Nach § 15a Abs. 2 Satz 1 Nr. 2, Abs. 3 Satz 1 Nr. 2 TMG ist eine Datenübermittlung zur Abwehr beliebiger Gefahren für die öffentliche Sicherheit oder Ordnung zulässig.

---

[37] Im Ergebnis wie hier Wissenschaftlicher Dienst des Bundestags, Ausarbeitung WD 10 - 3000 - 037/20 vom 16. September 2020, S. 24.
[38] Rn. 175 ff.
[39] Vgl. Rn. 186.

Der Übermittlungstatbestand beschränkt sich damit nicht auf die Abwehr von Gefahren für Rechtsgüter von hervorgehobenem Gewicht.[40]

Verfassungskonform ist allein die Übermittlungserlaubnis in § 15a Abs. 2 Satz 1 Nr. 3, Abs. 3 Satz 1 Nr. 3 TMG, die Übermittlungen an die Nachrichtendienste von Bund und Ländern regelt, da es insoweit einer tatbestandlichen Qualifikation des Schutzguts nicht bedarf.

Wiederum unzureichend ist § 15a Abs. 2 Satz 1 Nr. 3, Abs. 3 Satz 1 Nr. 4 TMG. Soweit diese Übermittlungserlaubnis auf die Prüfungsaufgaben nach § 2 Abs. 1 und 3 SchwarzArbG verweist, lässt sie sich allenfalls als Vorfeldregelung verstehen, die eine „konkretisierte Gefahr“ voraussetzt. Die in § 2 Abs. 1 und 3 SchwarzArbG in Bezug genommenen Rechtsverstöße sind jedoch angesichts der gesteigerten Eingriffsintensität des Bestandsdatenabrufs unter Zuordnung einer IP-Adresse zumindest nicht durchweg gewichtig genug, um eine solche Vorfeldregelung zu legitimieren. Beispielhaft ist die in § 2 Abs. 3 Nr. 1 SchwarzArbG genannte Aufnahme eines zulassungsfreien Gewerbes ohne gleichzeitige Anzeige zu nennen, bei der es sich um einen reinen Verfahrensverstoß handelt. Soweit § 15a Abs. 2 Satz 1 Nr. 3, Abs. 3 Satz 1 Nr. 4 TMG die Verhütung und Verfolgung von Straftaten und Ordnungswidrigkeiten nennt, fehlt es zum einen hinsichtlich der Verhütungsalternative an der erforderlichen tatsächlichen Eingriffsschwelle. Zum anderen genügt die pauschale Inbezugnahme von Ordnungswidrigkeiten nicht den qualifizierten verfassungsrechtlichen Anforderungen an das Übermittlungsziel. Nicht ausreichend ist, dass es sich um Ordnungswidrigkeiten handeln muss, die mit den Prüfungsaufgaben aus § 2 Abs. 1 und 3 SchwarzArbG zusammenhängen. Hieraus tritt nicht klar hervor, um welche Ordnungswidrigkeiten genau es sich handelt, zumal der geforderte Zusammenhang gesetzlich nicht näher beschrieben wird.

3. Übermittlung von Nutzungsdaten, § 15a Abs. 1 Satz 1, Abs. 2 Satz 1, Abs. 3 Satz 1 TMG

Als insgesamt verfassungsrechtlich defizitär stellen sich die in § 15a Abs. 2 Satz 1 und Abs. 3 Satz 1 TMG geregelten Übermittlungserlaubnisse dar, soweit sie auch die Übermittlung von Nutzungsdaten erlauben. Das Eingriffsgewicht einer solchen Übermittlung ist schwierig zu bestimmen, geht aber jedenfalls über die Übermittlung von Bestandsdaten – und zwar auch dann, wenn eine IP-Adresse zugeordnet wird – deutlich hinaus.[41] Dies schlägt sich insbesondere in gesteigerten verfassungsrechtlichen Anforderungen an das Gewicht der Ziele nieder, die mit einer Datenübermittlung verfolgt werden. Es bedarf daher im präventiven Handlungsfeld stets (also auch für die Nachrichtendienste) materiell qualifizierter Schutzgüter. Im repressiven Handlungsfeld muss die Übermittlung dazu dienen, herausgehobene Straftaten zu verfolgen. Wie hoch genau

---

[40] Vgl. Rn. 185.

[41] Ein geringeres Eingriffsgewicht kann der Übermittlung von Nutzungsdaten hingegen zukommen, wenn die Übermittlungserlaubnis nach dem Gegenstand und der Zielrichtung der Übermittlung beschränkt wird, vgl. zu der Abrufermächtigung in § 10a Abs. 1 BKAG unten IV.2.d). Eine derartige Beschränkung findet sich jedoch in § 15a Abs. 1 Satz 1, Abs. 2 Satz 1, Abs. 3 Satz 1 TMG nicht, so dass der verfassungsrechtlichen Würdigung das volle Spektrum denkbarer Datenübermittlungen zugrunde zu legen ist.

die Anforderungen zu veranschlagen sind, kann hier dahinstehen. In jedem Fall genügt die gesetzliche Übermittlungserlaubnis ihnen nicht, da sie die Übermittlung von Bestands- und von Nutzungsdaten unter denselben niedrigschwelligen Voraussetzungen zulässt.[42] Die Übermittlung von Nutzungsdaten muss vielmehr in einer separaten Regelung vorgesehen werden. Diese sollte der sehr diversen Sensibilität dieser Datenkategorie Rechnung tragen und bedarf darum noch erheblicher konzeptioneller Vorarbeiten, die den Rahmen dieses Gutachtens sprengen würden.

4. Übermittlung von Zugangsdaten, § 15b Abs. 1 Satz 1, Abs. 2 Satz 1 TMG

Keine verfassungsrechtlichen Bedenken bestehen gegen die Erlaubnis zur Übermittlung von Zugangsdaten in § 15b Abs. 1 Satz 1, Abs. 2 Satz 1 TMG. Die Übermittlung ist nur erlaubt zur Verfolgung besonders schwerer Straftaten, die in dem für Online-Durchsuchungen maßgeblichen Katalog in § 100b Abs. 2 StPO aufgezählt werden, sowie zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes. Die Datenübermittlung bedarf zudem einer richterlichen Anordnung. Diese Übermittlungstatbestände sind äußerst restriktiv formuliert und entsprechen Ermächtigungen zu Eingriffsmaßnahmen höchster Intensität. Unter diesen Voraussetzungen ist die Übermittlung von Zugangsdaten verfassungsrechtlich zulässig, da dann in jedem Fall auch die Datennutzung erlaubt werden darf. Dem Gesetzgeber der Abrufermächtigung bleibt überlassen sicherzustellen, dass Abruf und Nutzung miteinander verkoppelt werden, etwa indem in die Abrufermächtigung ein entsprechender Vorbehalt aufgenommen wird.

Keine verfassungsrechtlichen Bedenken ergeben sich im Übrigen daraus, dass bei den Telemedienanbietern aus Gründen der Datensicherheit in aller Regel die Zugangsdaten selbst gar nicht vorliegen dürften, sondern lediglich sogenannte Hashes, mit deren Hilfe Zugangsdaten geprüft werden können. Insbesondere ist die Datenübermittlung gleichwohl geeignet, um die gesetzlichen Übermittlungsziele zu erreichen. Insoweit ist zu beachten, dass der Gesetzgeber hinsichtlich der Frage der Eignung eine Einschätzungsprärogative genießt, die erst endet, wenn eine Eingriffsmaßnahme ersichtlich von vornherein nicht dazu beitragen kann, ihr Ziel zu erreichen. Es ist jedoch zumindest vorstellbar, dass die Gefahrenabwehr- und Strafverfolgungsbehörden gehashte Zugangsdaten mit entsprechenden Ressourcen und ggfs. Zusatzinformationen ermitteln und so den Zugangsschutz brechen können. In einem solchen Fall kann die Datenübermittlung einen Beitrag zur Gefahrenabwehr oder Strafverfolgung leisten.

IV. Ermächtigungen zum Abruf von Telemediendaten

Das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität schafft behördliche Ermächtigungen zum Abruf von Telemediendaten zum einen in der StPO für die Strafverfolgungsbehörden, zum anderen im BKAG für das BKA primär in seiner Zentralstellenfunktion. Diese Ermächtigungen genügen nur teilweise den verfassungsrechtlichen Anforderungen.

---

[42] Insoweit wie hier Wissenschaftlicher Dienst des Bundestags, Ausarbeitung WD 10 - 3000 - 037/20 vom 16. September 2020, S. 24.

1. Ermächtigungen in der Strafprozessordnung

a) Abruf von Bestandsdaten, § 100j Abs. 1 Satz 1 Nr. 2 StPO

Verfassungsrechtlich unbedenklich ist die allgemeine Ermächtigung zum Abruf von Bestandsdaten in § 100j Abs. 1 Satz 1 Nr. 2 StPO. Diese Vorschrift erlaubt einen Datenabruf, wenn ein strafprozessualer Anfangsverdacht vorliegt. Hierbei handelt es sich angesichts des begrenzten Eingriffsgewichts des Datenabrufs um einen hinreichenden Zugriffstatbestand.

b) Abruf von Bestandsdaten bei Zuordnung anhand einer IP-Adresse, § 100j Abs. 1 Satz 1 Nr. 2, Abs. 2 StPO

Nicht zu beanstanden ist die Ermächtigung zum Abruf von Bestandsdaten im strafrechtlichen Ermittlungsverfahren auch insoweit, als sie den Sonderfall der Zuordnung anhand einer IP-Adresse zum Gegenstand hat. Der von § 100j Abs. 1 Satz 1 Nr. 2 StPO vorausgesetzte Anfangsverdacht einer Straftat genügt auch insoweit als Eingriffsvoraussetzung den verfassungsrechtlichen Anforderungen.

Offensichtlich verfassungswidrig ist allerdings, dass diese Ermächtigung gemäß § 46 Abs. 2 OWiG auch zur Verfolgung beliebiger Ordnungswidrigkeiten genutzt werden kann. Insoweit bedarf es einer Beschränkung des Datenabrufs auf die Verfolgung besonders gewichtiger Ordnungswidrigkeiten. Rechtssystematisch liegt es nahe, diese Beschränkung im Ordnungswidrigkeitenrecht zu verankern. Das verfassungsrechtliche Defizit liegt damit in einem Unterlassen des Gesetzgebers und schlägt nicht auf die für sich genommen verfassungskonforme Eingriffsermächtigung in § 100j Abs. 1 Satz 1 Nr. 2, Abs. 2 StPO durch. Vielmehr sollte § 46 OWiG entsprechend ergänzt werden.

c) Abruf von Zugangsdaten, § 100j Abs. 1 Satz 2 StPO

Offensichtlich verfassungswidrig ist die Ermächtigung zum Abruf von Zugangsdaten in § 100j Abs. 1 Satz 2 StPO. Danach dürfen Strafverfolgungsbehörden solche Daten abrufen, wenn die gesetzlichen Voraussetzungen der Datennutzung vorliegen.

Dieser Eingriffstatbestand ist zwar für sich genommen verfassungsrechtlich nicht zu beanstanden. Insbesondere hat das BVerfG eine vergleichbare Norm, die sich auf Zugangsdaten bei Telekommunikationsanbietern bezog, für hinreichend bestimmt gehalten, obwohl sie die in Bezug genommenen Ermächtigungen zur Datennutzung nicht im Einzelnen aufgeführt hat.[43]

Die Vorschrift ist gleichwohl verfassungswidrig, weil ihr Anwendungsbereich über die korrespondierende Übermittlungserlaubnis in § 15b Abs. 1 Satz 1, Abs. 2 Satz 1 Nr. 1 TMG hinausgeht. Denn während die Übermittlungserlaubnis die Datenübermittlung auf die Verfolgung besonders schwerer Straftaten beschränkt, können die Voraussetzungen einer Datennutzung je nach Nutzungsermächtigung auch beim Verdacht einer weniger schweren Straftat vorliegen. So könnten abgerufene Zugangsdaten genutzt werden, um im Rahmen einer Wohnungsdurchsuchung auf der Grundlage von § 110

[43] Rn. 234 ff.

Abs. 3 StPO räumlich getrennte Speichermedien durchzusehen. Diese Nutzungsermächtigung stellt keine qualifizierten Anforderungen an die verfolgten Straftaten. Sie setzt lediglich eine Wohnungsdurchsuchung voraus, die ihrerseits gemäß § 102 StPO grundsätzlich beim Verdacht jeglicher Straftaten zulässig ist. Daraus resultiert ein partieller Widerspruch zwischen den zueinander gehörenden Eingriffsregelungen in § 15b Abs. 1 Satz 1, Abs. 2 Satz 1 Nr. 1 TMG und § 100j Abs. 1 Satz 2 StPO, der das Gebot der Normenklarheit verletzt und zur Verfassungswidrigkeit der zu weit gefassten strafprozessualen Abrufermächtigung führt. Die Tatbestände von § 100j Abs. 1 Satz 2 StPO und § 15b Abs. 1 Satz 1, Abs. 2 Satz 1 Nr. 1 TMG sollten daher angeglichen werden. Dabei bestehen unterschiedliche Regelungsoptionen, da § 15b Abs. 1 Satz 1, Abs. 2 Satz 1 Nr. 1 TMG restriktiver gefasst ist als dies verfassungsrechtlich geboten ist.

d) Abruf von Nutzungsdaten, § 100g Abs. 1 Sätze 1 und 2 StPO

Offen erscheint, ob die Ermächtigung zum Abruf von Nutzungsdaten in § 100g Abs. 1 Sätze 1 und 2 StPO vollständig den verfassungsrechtlichen Anforderungen genügt. Danach ist ein Datenabruf zulässig, wenn er zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung oder einer Straftat, die mittels Telekommunikation begangen wurde, erforderlich ist. Diese Ermächtigung parallelisiert den Abruf von Nutzungsdaten mit dem Abruf von Telekommunikations-Verkehrsdaten. Je nachdem, wie die Datenkategorie der Nutzungsdaten genau zugeschnitten wird, lässt sich allerdings durchaus begründen, dass Nutzungsdaten (erheblich) sensibler als Verkehrsdaten sein können und darum ein Abruf an strengere Anforderungen geknüpft werden muss. Im Übrigen ist bislang auch nicht geklärt, ob die Eingriffsvoraussetzungen in § 100g Abs. 1 Satz 1 StPO für den Abruf von Verkehrsdaten in jeder Hinsicht ausreichen. Eine detaillierte Ausarbeitung zu diesen Fragen würde allerdings den Rahmen des Gutachtenauftrags sprengen.

2. Ermächtigungen im BKAG

a) Abruf von Bestandsdaten, § 10 Abs. 1 Sätze 1 und 2 BKAG

Offensichtlich verfassungswidrig ist die Ermächtigung zum Abruf von Bestandsdaten in § 10 Abs. 1 Sätze 1 und 2 BKAG.[44] Danach darf das BKA solche Daten erheben, soweit dies zur Erfüllung seiner Zentralstellenaufgabe sowie seiner Schutzaufgaben (§ 6 und § 7 BKAG) erforderlich ist. Diesem Eingriffstatbestand fehlt es an einer hinreichenden tatsächlichen Eingriffsschwelle. Dies hat das BVerfG zu der Ermächtigung zum Abruf von Telekommunikations-Bestandsdaten in § 10 Abs. 1 Satz 1 BKAG bereits entschieden.[45] Das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität hat diese Regelung lediglich um eine Verweisungsnorm für den Abruf von Telemedien-Bestandsdaten ergänzt, aber nicht verändert. § 10 Abs. 1 Satz 1 BKAG bedarf jedoch einer grundlegenden Überarbeitung, die konzeptionelle Erwägungen zu den Bedarfen des BKA voraussetzt.

---

[44] Wie hier Wissenschaftlicher Dienst des Bundestags, Ausarbeitung WD 10 - 3000 - 037/20 vom 16. September 2020, S. 25.
[45] Rn. 208 ff., 213.

b) Abruf von Bestandsdaten bei Zuordnung anhand einer IP-Adresse, § 10 Abs. 1 Sätze 1 und 2, Abs. 2 BKAG

Gleichfalls offensichtlich verfassungswidrig ist die Ermächtigung zum Abruf von Bestandsdaten unter Zuordnung einer IP-Adresse in § 10 Abs. 1 Sätze 1 und 2, Abs. 2 BKAG.[46] Danach ist ein Bestandsdatenabruf stets unter denselben Voraussetzungen zulässig. Da § 10 Abs. 1 Sätze 1 und 2 BKAG mangels hinreichender Eingriffsschwelle generell keine taugliche Ermächtigung zum Abruf von Bestandsdaten darstellt, gilt dies erst recht für den eingriffsintensiveren Abruf unter Zuordnung einer IP-Adresse.[47]

c) Abruf von Zugangsdaten, § 10 Abs. 1 Satz 3 BKAG

Verfassungsrechtlich problematisch ist die Ermächtigung zum Abruf von Zugangsdaten in § 10 Abs. 1 Satz 3 BKAG. Danach setzt der Datenabruf voraus, dass die Voraussetzungen der Datennutzung vorliegen. Dieser Eingriffstatbestand ist für sich genommen verfassungskonform,[48] deckt sich aber zumindest dem Wortlaut nach nicht mit der Übermittlungserlaubnis in § 15b Abs. 1 Satz 1, Abs. 2 Satz 1 Nr. 1 TMG. Allerdings ist nicht klar, ob diese Divergenz zu einem Normwiderspruch führt, der das Gebot der Normenklarheit verletzt.

Hierfür könnte darauf abgestellt werden, ob sich eine Ermächtigung zur Nutzung von Zugangsdaten findet, deren Eingriffsvoraussetzungen den Tatbestand der Übermittlungserlaubnis unterlaufen könnten. Dies dürfte letztlich zu verneinen sein: Für die Zentralstellentätigkeit des BKA ist überhaupt keine Ermächtigung zur Nutzung von Zugangsdaten ersichtlich.[49] Für die Schutzaufgaben errichten denkbare Ermächtigungen wie die Regelungen zu Wohnungsdurchsuchungen[50] Eingriffsvoraussetzungen, die hinter § 15b Abs. 1 Satz 1, Abs. 2 Satz 1 Nr. 1 TMG nicht zurückbleiben.

Allerdings könnte der Anwendungsbereich von § 10 Abs. 1 Satz 3 BKAG ohne Änderung des Wortlauts der Norm erweitert werden, indem eine neue niedrigschwellige Nutzungsermächtigung geschaffen wird. Diese Erwägung spricht dafür, bereits in dem gegenwärtigen latenten Widerspruch zwischen Übermittlungserlaubnis und Abrufermächtigung eine Verletzung des Gebots der Normenklarheit zu sehen. Insgesamt erscheint offen, ob § 10 Abs. 1 Satz 3 BKAG den verfassungsrechtlichen Anforderungen genügt. Vorzugswürdig wäre in jedem Fall, die Tatbestände von § 10 Abs. 1 Satz 3 BKAG und von § 15b Abs. 1 Satz 1, Abs. 2 Satz 1 Nr. 1 TMG besser aufeinander abzustimmen.

d) Abruf von Identifikationsdaten, § 10a Abs. 1 BKAG

Keine verfassungsrechtlichen Bedenken bestehen gegen die Ermächtigung zum Abruf von Identifikationsdaten in § 10a Abs. 1 BKAG.[51] Diese Vorschrift regelt einen Sonder-

---

[46] Wie hier Wissenschaftlicher Dienst des Bundestags, Ausarbeitung WD 10 - 3000 - 037/20 vom 16. September 2020, S. 25.
[47] Vgl. Rn. 239; zu den Anforderungen an das Eingriffsziel Rn. 241 und 242.
[48] Vgl. Rn. 234 ff.
[49] Vgl. Rn. 236.
[50] § 63 Abs. 7, § 66 Abs. 1 Satz 3 BKAG.
[51] Im Ergebnis wie hier Wissenschaftlicher Dienst des Bundestags, Ausarbeitung WD 10 - 3000 - 037/20 vom 16. September 2020, S. 27.

fall des Abrufs von Nutzungsdaten, nämlich den Abruf solcher Daten, die zur Identifikation eines Telemediennutzers benötigt werden, wobei der Inhalt der Nutzung bereits bekannt ist. Ein beispielhafter Anwendungsfall ist der Abruf einer IP-Adresse, von der aus ein strafbarer Inhalt auf einem sozialen Netzwerk veröffentlicht wurde, bei dem Betreiber des Netzwerks.[52] Voraussetzung des Datenabrufs ist der Verdacht einer Straftat oder eine erhebliche Gefahr für die öffentliche Sicherheit. Zudem muss das Ziel des Datenabrufs darin bestehen, die zuständige Strafverfolgungsbehörde oder Polizeibehörde zu ermitteln, um die Identität des Nutzers und den Inhalt der Nutzung des Telemediendienstes an diese weiterzuleiten.

Die Eingriffsschwellen eines einfachen Tatverdachts und einer erheblichen Gefahr dürften angesichts der potenziell hohen Sensibilität von Nutzungsdaten zwar nicht generell ausreichen, um einen Abruf solcher Daten verfassungsrechtlich zu legitimieren. Das Gewicht des in § 10a Abs. 1 BKAG vorgesehenen Datenabrufs fällt jedoch wegen der Beschränkung auf Identifikationsdaten zu einem bereits bekannten Inhalt deutlich geringer aus. Die geregelte Maßnahme lässt sich nach ihrer Zielsetzung sowie in Art und Ausmaß der Datenverarbeitung in etwa mit einem Bestandsdatenabruf vergleichen, bei dem eine IP-Adresse zugeordnet wird. Den verfassungsrechtlichen Anforderungen an eine Maßnahme dieses Eingriffsgewichts, wie sie der zweite Bestandsdatenbeschluss konturiert, genügen die gesetzlichen Voraussetzungen des Datenabrufs.

V. Meldepflicht nach § 3a NetzDG und Weiterverarbeitung der Meldungen

Die in § 3a NetzDG vorgesehene Pflicht bestimmter Telemedienanbieter zur Meldung bestimmter Inhalte an das BKA ist für sich genommen verfassungskonform. Das BKA bedarf jedoch zur Weiterverarbeitung der übermittelten Daten einer korrespondierenden Weiterverarbeitungsermächtigung, die sich im geltenden Recht nicht findet.

Die Meldepflicht umfasst gemäß § 3a Abs. 2, Abs. 4 NetzDG zum einen bestimmte strafbare Inhalte, zum anderen bestimmte Nutzungsdaten, mit deren Hilfe die Urheber*innen dieser Inhalte identifiziert werden können. Diese Daten sind nicht sehr sensibel. Die zu meldenden Inhalte wurden von den betroffenen Nutzer*innen veröffentlicht oder zumindest in eine über eine Individualkommunikation hinausgehende Gruppenkommunikation eingestellt. Die Nutzer*innen mussten darum grundsätzlich mit einer Kenntnisnahme durch Dritte rechnen.[53] Die Übermittlung der Nutzungsdaten hat höheres Gewicht, da mit ihrer Hilfe die Anonymität bzw. Pseudonymität der Kommunikation aufgehoben wird.[54] Allerdings bleibt die Übermittlung auf einen eher schmalen Datenbestand beschränkt, der zumindest in der Regel keine Erkenntnisse über die Identität der Person hinaus ermöglicht, von der ein bestimmter öffentlicher Kommunikationsvorgang ausging.[55] Die übermittelten Nutzungsdaten lassen sich darum hinsichtlich ihrer Sensibilität mit Bestandsdaten vergleichen, die unter Zuordnung einer IP-Adresse beauskunftet werden.

---

[52] Vgl. BT-Drs. 19/20163, S. 44 f.
[53] Vgl. zum begrenzten grundrechtlichen Schutz öffentlicher und gruppenbezogener Kommunikation im Internet BVerfGE 120, 274 (344 ff.).
[54] Vgl. Rn. 166.
[55] Vgl. Rn. 169.

Das Anliegen, die in § 3a Abs. 2 NetzDG genannten Straftaten zu verfolgen, kann die Übermittlung dieser Daten grundsätzlich rechtfertigen. Die Übermittlung wird auch an eine hinreichende tatsächliche Eingriffsschwelle gebunden, da der übermittelnde Telemedienanbieter konkrete Inhalte aufgrund einer eigenständigen Rechtsprüfung übermitteln muss. Problematisch ist allerdings, dass Inhalte und Nutzungsdaten gleichzeitig zu übermitteln sind. Denn die Nutzungsdaten werden grundsätzlich[56] nur benötigt, wenn das BKA bei seiner eigenen Rechtsprüfung den Anfangsverdacht einer Straftat bejaht. Nur in diesem Fall stellt sich die Frage, welche Behörde für die Strafverfolgung zuständig ist, die dann durch eine Zuordnung der übermittelten Nutzungsdaten mittels eines Bestandsdatenabrufs bei einem Telekommunikationsanbieter beantwortet werden kann. Eine gleichzeitige Übermittlung von Inhalten und Nutzungsdaten birgt darum das Risiko, dass das BKA Daten erhält, die es nicht nutzen darf. Wie das BVerfG im zweiten Bestandsdatenbeschluss für Zugangsdaten nochmals bekräftigt hat, ist eine Übermittlung von Daten, die (noch) nicht genutzt werden dürfen, grundsätzlich nicht erforderlich und darum unverhältnismäßig.[57]

Zur Rechtfertigung der in § 3a Abs. 4 NetzDG geregelten Pflicht zur sofortigen Übermittlung von Nutzungsdaten lässt sich allerdings anführen, dass wegen der kurzfristigen Löschung der für die Zuordnung erforderlichen Telekommunikations-Verkehrsdaten bei den Telekommunikationsanbietern ein besonderes Eilbedürfnis besteht. Wäre das BKA darauf verwiesen, nach der Sichtung der übermittelten Inhalte die Nutzungsdaten gesondert abzurufen, so könnte die damit verbundene Verzögerung eine Identifizierung der Personen, von denen die übermittelten strafbaren Inhalte ausgingen, vielfach vereiteln.[58] Angesichts dessen erscheint es verfassungsrechtlich vertretbar, eine einheitliche Übermittlungspflicht zu errichten, die sich auch auf die (noch) nicht nutzbaren Nutzungsdaten erstreckt.[59]

Dieser Beurteilung steht nicht entgegen, dass auch andere Vorgehensweisen denkbar wären. Insbesondere könnten die Telemedienanbieter verpflichtet werden, die zur Identifikation erforderlichen Nutzungsdaten statt an das BKA an den jeweiligen Telekommunikationsanbieter zu übermitteln. Dieser könnte verpflichtet werden, anhand der übermittelten Nutzungsdaten unverzüglich die Identität der Person zu ermitteln, von welcher der beanstandete Inhalt ausging, und dieses Telekommunikations-Be-

---

[56] Es ist vorstellbar, dass das BKA in bestimmten Fällen die Identität der Person feststellen will, obwohl es den übermittelten Inhalt nicht für strafbar hält. So könnte es etwa liegen, wenn Anhaltspunkte dafür bestehen, dass der Inhalt von einer Person stammt, zu der das BKA im Rahmen seiner Zentralstellenfunktion Daten sammelt, weil von ihr in Zukunft Straftaten erwartet werden (vgl. § 18 Abs. 1 Nr. 4 BKAG), und wenn der Inhalt ungeachtet seiner fehlenden strafrechtlichen Relevanz Rückschlüsse auf das zukünftige Verhalten dieser Person zulässt. Auch für derartige Weiterverarbeitungen bedürfte es jedoch besonderer Regelungen, siehe dazu sogleich im Text.

[57] Rn. 160.

[58] So jedenfalls die übereinstimmenden Einschätzungen mehrerer Praktiker in der Anhörung des Rechtsausschusses, vgl. im Wortlautprotokoll der Sitzung vom 6. Mai 2020 insb. S. 24 f. und 33 f.

[59] Die alternative Lösung, dass die Nutzungsdaten stattdessen an den jeweiligen Telekommunikationsanbieter übermittelt werden, der ggfs. auf Anforderung des BKA die übermittelte IP-Adresse zuordnet, ist wegen des dabei vorzusehenden Datenflusses an ein nicht grundrechtsgebundenes Privatunternehmen zumindest nicht zwingend weniger eingriffsintensiv als der im Gesetz vorgesehene Ansatz.

standsdatum dem BKA auf Anforderung zu übermitteln. Dieses *Quick Freeze*-Verfahren könnte sogar wirksamer sein als die unmittelbare Datenübermittlung an das BKA, da die Zuordnung der übermittelten Daten durch den Telekommunikationsanbieter nicht von einer vorherigen Verdachtsprüfung abhinge und somit Zeitverluste durch diese Prüfung vermieden werden könnten. Rechtspolitisch halte ich es darum für vorzugswürdig. Gleichwohl ist diese alternative Lösung nicht als (klar) milderes Mittel anzusehen, das zu ergreifen verfassungsrechtlich geboten wäre. Zum einen begründen die Datenübermittlung zwischen Telemedien- und Telekommunikationsanbieter und die anschließende Zuordnung der übermittelten Daten zu einer Person durch den Telekommunikationsanbieter ihrerseits Risiken für die betroffene Person, die nicht fundamental hinter dem Risiko einer unmittelbaren Übermittlung an das BKA zurückbleiben. Zum anderen würde das *Quick Freeze*-Verfahren eine Übermittlungsinfrastruktur zwischen Telemedien- und Telekommunikationsanbietern erfordern, deren Einrichtung und Betrieb erheblichen zusätzlichen Aufwand erzeugen dürften, der in eine Verhältnismäßigkeitsprüfung einzustellen wäre. Das *Quick Freeze*-Verfahren wäre darum insgesamt zulässig, ist aber nicht geboten.

Um eine (noch) nicht zu rechtfertigende vorzeitige Datennutzung auszuschließen, werden jedoch Weiterverarbeitungsregelungen für das BKA benötigt, welche das verfassungsrechtlich gebotene zweistufige Vorgehen hinreichend normenklar anordnen. Das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität hat hingegen die Weiterverarbeitung der übermittelten Daten durch das BKA überhaupt nicht geregelt. Diese richtet sich mithin nach den allgemeinen Vorschriften im BKAG, die sich im vorliegenden Zusammenhang jedoch als untauglich erweisen.

Im Rahmen der von § 3a Abs. 2 NetzDG in Bezug genommenen Zentralstellenaufgabe des BKA kommt als Weiterverarbeitungsermächtigung § 10 Abs. 1 Satz 1 Nr. 1, Abs. 2 BKAG in Betracht, der dem BKA ermöglicht, Telekommunikations-Bestandsdaten anhand von IP-Adressen abzurufen, um vorhandene Sachverhalte zu ergänzen.[60] Diese Norm ist jedoch zum einen allgemein zu weit gefasst und darum unverhältnismäßig.[61] Zum anderen eignet sie sich konzeptionell nicht, um Datenabrufe mit repressiver Zielsetzung anzuleiten. Denn von Verfassungs wegen bedürfen solche Abrufe zwingend eines strafprozessualen Anfangsverdachts.[62] Besteht ein solcher Verdacht, ist jedoch grundsätzlich der Anwendungsbereich des Strafprozessrechts eröffnet, zu dessen Vollzug mit Blick auf die in § 3a Abs. 2 Nr. 3 NetzDG aufgeführten Straftatbestände das BKA zumindest in aller Regel nicht zuständig ist.[63] Das geltende Recht enthält daher keine geeignete Rechtsgrundlage für die vom Gesetzgeber intendierte Weiterverarbeitung der nach § 3a Abs. 2 und Abs. 4 NetzDG übermittelten Daten.

---

[60] Von vornherein nicht ausreichend ist als Weiterverarbeitungsermächtigung § 2 Abs. 1 und 2 BKAG. Trotz des missverständlichen Wortlauts insbesondere von § 2 Abs. 2 Nr. 1 BKAG handelt es sich hierbei um eine bloße Aufgabenzuweisung, die dem BKA keine Befugnisse zu Datenverarbeitungen verleiht, wie hier etwa Graulich, in: Schenke/ders./Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 2 BKAG Rn. 1.
[61] Rn. 208 ff.
[62] Rn. 146, 153.
[63] Vgl. Rn. 212.

Soll das BKA im Rahmen seiner Zentralstellenaufgabe Ermittlungsmaßnahmen mit repressiver Zielsetzung durchführen, um die für die Strafverfolgung zuständige Behörde zu bestimmen, so bedarf es mithin einer spezifisch auf dieses Erkenntnisziel zugeschnittenen Ermächtigungsgrundlage. Das BVerfG hat dieses Erfordernis im zweiten Bestandsdatenbeschluss für Datenabrufe herausgearbeitet.[64] Es gilt ebenso für die Weiterverarbeitung von Daten, die das BKA aufgrund einer gesetzlichen Übermittlungspflicht ohne vorherigen Abruf übermittelt erhält. Zu § 3a Abs. 2 und Abs. 4 NetzDG muss daher eine korrespondierende Weiterverarbeitungsermächtigung im BKAG geschaffen werden. Diese Ermächtigung muss klarstellen, dass das BKA zunächst eine Verdachtsprüfung durchzuführen hat und erst bei Bejahung eines Tatverdachts die übermittelten Nutzungsdaten für einen Bestandsdatenabruf nutzen darf. Hierzu ist es erforderlich, aber auch ausreichend, den Bestandsdatenabruf an den Anfangsverdacht einer der in § 3a Abs. 2 Nr. 3 NetzDG genannten Straftaten zu binden.

[64] Rn. 212.