

Kommunikation & Recht



Betriebs-Berater für

● Medien ● Telekommunikation ● Multimedia

9

K&R

- Editorial: Vom „Ä“ und „Ü“ im beA ... · *Dr. Florian Deusch*
- 565 Pflicht zur Angabe von Gesamtpreisen und die Mehrwertsteuersenkung im Online-Handel · *Martin Rätze*
- 569 Die Entwicklung des Datenschutzrechts im Jahr 2019
Dr. Flemming Moos
- 578 Geht der neue Glücksspielstaatsvertrag 2021 regulatorisch wirklich online? · *Prof. Dr. Christian Koenig*
- 584 Update Informationsfreiheits- und Transparenzrecht 2019/2020
Prof. Dr. Jens M. Schmittmann
- 588 EuGH: Datenübermittlung in die USA kann nicht länger mit „Privacy Shield“ legitimiert werden
mit Kommentar von *Carsten Kociok* und *Dr. Johanna M. Hofmann*
- 604 BVerfG: Regelungen zur Bestandsdatenauskunft sind verfassungswidrig
mit Kommentar von *Jan Spittka* und *Dr. Philipp Adelberg*
- 611 BGH: Cookie-Einwilligung II: Keine wirksame Einwilligung bei voreingestellten Häkchen
mit Kommentar von *Dr. Markus Lang*
- 625 BGH: Afghanistan Papiere II: Bei Presseveröffentlichung ist Urheberpersönlichkeitsrecht zu berücksichtigen
mit Kommentar von *Prof. Dr. Franz Hofmann*
- 630 Hanseatisches OLG Hamburg: Keine Pflicht zur Werbekennzeichnung von Influencer-Post bei offensichtlicher Werbung
mit Kommentar von *Michael Terhaag* und *Christian Schwarz*

23. Jahrgang

September 2020

Seiten 565 – 636

31 3. Die angegriffenen Entscheidungen beruhen auf den aufgezeigten verfassungsrechtlichen Fehlern und sind aufzuheben. Es ist nicht auszuschließen, dass die Gerichte bei erneuter Befassung zu einer anderen Entscheidung in der Sache kommen werden. [...]

Regelungen zur Bestandsdatenauskunft sind verfassungswidrig

BVerfG, Beschluss vom 27. 5. 2020 – 1 BvR 1873/13, 1 BvR 2618/13

Volltext-ID: KuRL2020-604, www.kommunikationundrecht.de

ECLI:DE:BVerfG:2020:rs20200527.1bvr187313

§§ 10, 40 BKAG; § 2 b, § 4 BNDG; § 22 a BPolG; § 8 d BVerfSchG; Art. 1 Abs. 1, Art. 2 Abs. 1, Art. 10 Abs. 1 GG; § 4 b MADG; § 113 TKG; § 7, § 15 ZFdG

1. Der Gesetzgeber muss bei der Einrichtung eines Auskunftsverfahrens auf Grundlage jeweils eigener Kompetenzen für sich genommen verhältnismäßige Rechtsgrundlagen sowohl für die Übermittlung als auch für den Abruf der Daten schaffen. Übermittlungs- und Abrufregelungen für Bestandsdaten von Telekommunikationsdiensteanbietern müssen die Verwendungszwecke der Daten hinreichend begrenzen, mithin die Datenverwendung an bestimmte Zwecke, tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz binden.

2. Schon dem Gesetzgeber der Übermittlungsregelung obliegt die normenklare Begrenzung der Zwecke der möglichen Datenverwendung. Eine Begrenzung der Verwendungszwecke erst zusammen mit der Abrufregelung kommt nur in Betracht, wenn die Übermittlungsregelung Materien betrifft, die allein im Kompetenzbereich des Bundes liegen und die Regelungen eine in ihrem Zusammenwirken normenklare und abschließende Zweckbestimmung der Datenverwendung enthalten.

3. Die Befugnis zum Datenabruf muss nicht nur für sich genommen verhältnismäßig sein, sondern ist – auch aus Gründen der Normenklarheit – zudem an die in der Übermittlungsregelung begrenzten Verwendungszwecke gebunden. Dabei steht es dem Gesetzgeber der Abrufregelung frei, den Abruf der Daten an weitergehende Anforderungen zu binden.

4. Trotz ihres gemäßigten Eingriffsgewichts bedürfen die allgemeinen Befugnisse zur Übermittlung und zum Abruf von Bestandsdaten für die Gefahrenabwehr und die Tätigkeit der Nachrichtendienste grundsätzlich einer im Einzelfall vorliegenden konkreten Gefahr und für die Strafverfolgung eines Anfangsverdachts. Die Zuordnung dynamischer IP-Adressen muss im Hinblick auf ihr erhöhtes Eingriffsgewicht darüber hinaus auch dem Schutz oder der Bewehrung von Rechtsgütern von hervorgehobenem Gewicht dienen. Es bedarf ferner einer nachvollziehbaren und überprüfbaren Dokumentation der Entscheidungsgrundlagen. Als Eingriffsschwelle kann im Bereich der Gefahrenabwehr und der nachrichtendienstlichen Tätigkeit das Vorliegen einer konkretisierten Gefahr ausreichen, soweit es um den Schutz von Rechtsgütern oder die Verhütung von Straftaten von zumindest erheblichem Gewicht

(allgemeine Bestandsdatenauskunft) oder besonderem Gewicht (Zuordnung dynamischer IP-Adressen) geht. (Leitsätze des Gerichts)

Sachverhalt

Die Beschwerdeführenden sind Inhaber von Festnetz- sowie Mobilfunkanschlüssen und nutzen Internetzugangleistungen verschiedener Diensteanbieter. Sie sehen sich durch die angegriffenen Vorschriften in ihren Grundrechten aus Art. 10 Abs. 1 GG sowie Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG verletzt.

Aus den Gründen

89 C. Die [überwiegend zulässigen] Verfassungsbeschwerden sind überwiegend begründet. Die angegriffenen Vorschriften genügen in weiten Teilen nicht den Anforderungen an die Verhältnismäßigkeit.

90 I. Die Regelungen zur Übermittlung und zum Abruf von Bestandsdaten greifen in das Recht auf informationelle Selbstbestimmung des Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ein. Soweit sie auch zur Übermittlung und zum Abruf von Bestandsdaten ermächtigen, die anhand dynamischer IP-Adressen bestimmt werden, liegt ein Eingriff in das speziellere Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG vor.

91 1. § 113 Abs. 1 S. 1 und 2 TKG sowie die damit korrespondierenden fachrechtlichen Abrufregelungen (§ 10 Abs. 1 S. 1 und 2, § 40 Abs. 1 S. 1 und 2 BKAG, § 22 a Abs. 1 S. 1 und 2 BPolG, § 7 Abs. 5 S. 1 und 2, § 15 Abs. 2 S. 1 und 2 ZFdG, § 8 d Abs. 1 S. 1 und 2 BVerfSchG sowie § 2 b S. 1 BNDG und § 4 b S. 1 MADG, soweit sie Bezug auf § 8 d Abs. 1 S. 1 und 2 BVerfSchG nehmen) greifen in das Recht auf informationelle Selbstbestimmung ein. [...]

91 2. § 113 Abs. 1 S. 3 TKG sowie die damit korrespondierenden fachrechtlichen Abrufregelungen (§ 10 Abs. 2, § 40 Abs. 2 BKAG, § 22 a Abs. 2 BPolG, § 7 Abs. 6, § 15 Abs. 3 ZFdG, § 8 d Abs. 2 S. 1 BVerfSchG sowie § 2 b S. 1 BNDG und § 4 b S. 1 MADG, soweit sie Bezug auf § 8 d Abs. 2 S. 1 BVerfSchG nehmen), die eine Zuordnung dynamischer IP-Adressen ermöglichen, greifen in Art. 10 Abs. 1 GG ein.

98 a) Art. 10 Abs. 1 GG gewährleistet das Telekommunikationsgeheimnis, das die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs vor einer Kenntnisnahme durch die öffentliche Gewalt schützt. [...]

101 b) Nach diesen Maßstäben greift § 113 Abs. 1 S. 3 TKG in das Grundrecht aus Art. 10 Abs. 1 GG ein, da er die Zuordnung dynamischer IP-Adressen zu ihren Anschlussinhabern ermöglicht. Gegenstand der Auskunft ist zwar allein der Anschlussinhaber der abgefragten IP-Adresse und damit ein Bestandsdatum. Soweit die Diensteanbieter hierüber Auskunft zu geben haben, müssen sie aber zunächst auf die von ihnen gespeicherten Verkehrsdaten sowie gegebenenfalls weitere unternehmensinterne Datenquellen (vgl. § 113 Abs. 1 S. 4 TKG), bei denen es sich ebenfalls um Verbindungsdaten handeln kann, zugreifen und diese auswerten. Soweit § 113 Abs. 1 S. 3 TKG die Nutzung von Verkehrsdaten eröffnet, die aufgrund der Regelungen zur Vorratsdatenspeicherung gespeichert wurden, ist die Vorschrift überdies schon deshalb an Art. 10 Abs. 1 GG zu messen, weil sie eine Folgeverwendung von Daten ermöglicht, die einmal in Form eines Eingriffs in

Art. 10 Abs. 1 GG erhoben worden sind (vgl. BVerfGE 125, 260, 312 f.).

102 c) Die angegriffenen fachrechtlichen Abrufregelungen begründen einen eigenständigen Eingriff in Art. 10 Abs. 1 GG, soweit sie zur Abfrage anhand einer dynamischen IP-Adresse bestimmter Bestandsdaten durch jeweils auskunftsberechtigte Behörden ermächtigen.

103 II. Die angegriffenen Vorschriften sind formell verfassungsgemäß. Insbesondere steht dem Bund sowohl für § 113 TKG als auch für die Abrufregelungen in den jeweiligen Fachgesetzen die Gesetzgebungskompetenz zu. [...]

122 III. Die angegriffenen Übermittlungsbefugnisse in § 113 TKG genügen in materieller Hinsicht nicht den verfassungsrechtlichen Anforderungen des Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG sowie des Art. 10 Abs. 1 GG.

123 1. Eingriffe in das Recht auf informationelle Selbstbestimmung und das Telekommunikationsgeheimnis bedürfen wie jede Grundrechtsbeschränkung einer gesetzlichen Ermächtigung, die einen legitimen Gemeinwohlzweck verfolgt und im Übrigen den Grundsatz der Verhältnismäßigkeit wahrt (vgl. BVerfGE 65, 1, 44; 100, 313, 359 f.; st. Rspr.). [...]

124 2. Die angegriffenen Übermittlungsregelungen dienen legitimen Zwecken und sind hierfür geeignet und erforderlich. [...]

127 3. Mit den Anforderungen der Verhältnismäßigkeit im engeren Sinne sind die Übermittlungsregelungen nur vereinbar, wenn sie die Verwendungszwecke der einzelnen Befugnisse gemessen an ihrem Eingriffsgewicht selbst hinreichend normenklar begrenzen (a). Diesen Anforderungen genügen die angegriffenen Befugnisse zur allgemeinen Übermittlung von Bestandsdaten (b), zur Übermittlung von Zugangsdaten (c) und zur Übermittlung von anhand einer dynamischen IP-Adresse bestimmter Bestandsdaten (d) nicht, wengleich die Regelungen zur Datensicherheit keinen Bedenken begegnen (e).

128 a) Dem Verhältnismäßigkeitsgebot im engeren Sinne genügen die Übermittlungsregelungen, wenn der mit ihnen verfolgte Zweck und die zu erwartende Zweckerreichung nicht außer Verhältnis zu der Schwere des Eingriffs stehen (vgl. BVerfGE 141, 220, 267 Rn. 98; 148, 40, 57 f. Rn. 49). Das Eingriffsgewicht bestimmt sich maßgeblich nach Art, Umfang und denkbarer Verwendung der Daten sowie der Gefahr ihres Missbrauchs (aa). Die Verwendungszwecke der Daten sind schon durch den Gesetzgeber der Übermittlungsregelung für sich genommen verhältnismäßig und normenklar zu begrenzen (bb). Im Übrigen muss die verfassungsrechtlich gebotene Datensicherheit bei Übermittlung der Daten gewährleistet sein (cc). [...]

136 b) Diesen Anforderungen genügt die in § 113 Abs. 1 S. 1 TKG geregelte Befugnis zur allgemeinen Bestandsdatenauskunft nicht. Ihre Reichweite ist mangels begrenzender Eingriffsschwellen unverhältnismäßig.

137 aa) Als Verwendungsregel für die nach §§ 95 und 111 TKG erhobenen Daten berechtigt § 113 Abs. 1 S. 1 TKG die Diensteanbieter zu deren Übermittlung. [...]

138 bb) Die in § 113 Abs. 1 S. 1 TKG eröffnete allgemeine Bestandsdatenauskunft begründet einen Eingriff in das Recht auf informationelle Selbstbestimmung von gewissem, wenn auch nicht sehr großem Gewicht. [...]

144 cc) Trotz ihres gemäßigten Eingriffsgewichts erweist sich die Übermittlungsbefugnis aufgrund ihrer Reichweite,

die durch keine Eingriffsschwellen begrenzt ist, als unverhältnismäßig.

145 (1) Auch unter Berücksichtigung des nicht sehr großen Eingriffsgewichts der in § 113 Abs. 1 S. 1 TKG geregelten Übermittlungsbefugnis und ihrer Bedeutung für die staatliche Aufgabenwahrnehmung im Bereich der Gefahrenabwehr, der Strafverfolgung und der Nachrichtendienste bedarf es begrenzender, spezifischer Eingriffsschwellen. [...]

146 (a) Erforderlich ist demnach bezogen auf die Gefahrenabwehr grundsätzlich eine im Einzelfall vorliegende konkrete Gefahr im Sinne der polizeirechtlichen Generalklauseln. Diese Schwelle umfasst auch den Gefahrenverdacht. Ebenso beschränkt sie Auskünfte nicht von vornherein auf Polizeipflichtige im Sinne des allgemeinen Polizei- und Ordnungsrechts. Sie ist damit jedoch nicht so entgrenzt, dass sie angesichts des gemäßigten Eingriffsgewichts unverhältnismäßig wäre. [...]

147 (b) Der Gesetzgeber ist von Verfassungs wegen aber nicht von vornherein für jede Art der Aufgabenwahrnehmung auf die Schaffung von Eingriffstatbeständen beschränkt, die dem tradierten sicherheitsrechtlichen Modell der Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren entsprechen. Vielmehr kann er die Grenzen unter besonderen Voraussetzungen auch weiter ziehen, indem er die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert (vgl. BVerfGE 141, 220, 272 Rn. 112). Allerdings muss stets gewährleistet bleiben, dass Annahmen und Schlussfolgerungen einen konkret umrissenen Ausgangspunkt im Tatsächlichen haben (BVerfGE 113, 348, 386). [...]

148 Eingriffsgrundlagen müssen daher regelmäßig zumindest eine hinreichend konkretisierte Gefahr verlangen. [...]

151 (c) Diese verfassungsrechtlichen Anforderungen gelten grundsätzlich für alle Eingriffsermächtigungen mit präventiver Zielrichtung. [...]

152 (d) Demgegenüber kann im Bereich der Strafverfolgung eine in tatsächlicher Hinsicht unterhalb des Anfangsverdachts liegende Eingriffsschwelle zur Vornahme von grundrechtsrelevanten Eingriffen nicht genügen. Zwar können für Maßnahmen mit präventiver Zielsetzung die Grenzen für bestimmte Bereiche auch weiter gezogen werden, indem die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert werden (oben Rn. 147). Voraussetzung ist aber stets eine tatsachenbezogene Grundlage. Auch die im Gefahrenabwehrrecht anerkannten Eingriffsschwellen der „konkretisierten Gefahr“ und der „drohenden Gefahr“, die in zeitlicher Hinsicht ins Vorfeld verlagert sind, setzen tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr voraus (vgl. BVerfGE 141, 220, 272 Rn. 112). Nichts Anderes gilt für Maßnahmen der Strafverfolgung. Auch im Vorfeldbereich kommen sie nur bei Vorliegen tatsächlicher Anhaltspunkte in Betracht (vgl. BVerfGE 113, 348, 386; 117, 244, 263). Vage Anhaltspunkte oder Vermutungen reichen demgegenüber nicht aus (vgl. BVerfGE 115, 166, 197 f.; 124, 43, 66 f.).

153 Danach reicht eine in tatsächlicher Hinsicht unterhalb des Anfangsverdachts angesiedelte Eingriffsschwelle im Bereich der Strafverfolgung nicht aus. Die Annahme eines Anfangsverdachts setzt lediglich das Vorliegen zureichender tatsächlicher Anhaltspunkte für eine Straftat voraus (vgl. BGH, Beschl. v. 12. 1. 2005 – 5 StR 191/04, Rn. 7). Solche tatsächlichen Anhaltspunkte liegen hinsichtlich ihrer Aussagekraft noch unter den für manche Ermittlungs-

maßnahmen geforderten „bestimmten Tatsachen“, weshalb der Anfangsverdacht bereits die Verdachtsstufe mit den geringsten in der Strafprozessordnung vorgesehenen tatsächlichen Voraussetzungen ist (vgl. BVerfGE 109, 279, 350; 129, 208, 268). Würden die Voraussetzungen noch weiter zurückgenommen, wären nur noch vage Anhaltspunkte gefordert.

154 (2) Diesen verfassungsrechtlichen Anforderungen genügt § 113 Abs. 1 S. 1 TKG nicht. Die Übermittlungsregelung öffnet das manuelle Auskunftsverfahren sehr weit, indem sie Auskünfte allgemein zum Zweck der Gefahrenabwehr, zur Verfolgung von Straftaten oder Ordnungswidrigkeiten sowie zur Erfüllung nachrichtendienstlicher Aufgaben erlaubt (§ 113 Abs. 2 S. 1 TKG) und dabei keine ihre Reichweite näher begrenzenden Eingriffsschwellen (vgl. [K&R 2012, 274 =] BVerfGE 130, 151, 205) enthält. Die Regelung ermöglicht die Erteilung einer Auskunft im Einzelfall vielmehr bereits dann, wenn dies zur Wahrnehmung der Aufgaben erfolgt.

155 (a) Trotz des für sich gesehen begrenzten Informationsgehalts der betreffenden Daten, ihrer engen Verwendungsmöglichkeiten sowie ihrer großen Bedeutung für eine effektive Aufgabenwahrnehmung der abfrageberechtigten Behörden sind die Verwendungszwecke nicht hinreichend begrenzt. Zwar handelt es sich bei den gesetzlich bestimmten Verwendungszwecken um zentrale Aufgaben der Gewährleistung von Sicherheit. In Anbetracht der zunehmenden Bedeutung der elektronischen Kommunikationsmittel und des heutigen Kommunikationsverhaltens der Menschen in allen Lebensbereichen sind die Behörden darauf angewiesen, insbesondere auch Telekommunikationsnummern individuell zuordnen zu können. Doch auch unter Berücksichtigung ihres nur gemäßigten Eingriffsgewichts ist die hier angegriffene Regelung zu weit gefasst, da Auskünfte bereits dann erteilt werden können, wenn sie in irgendeinem Zusammenhang zu der staatlichen Aufgabenwahrnehmung stehen und einen Einzelfallbezug erkennen lassen, ohne dass ein auf tatsächliche Anhaltspunkte gestützter Eingriffsanlass vorausgesetzt wird. Eröffnet sind damit vielfältige und in jeder Hinsicht unbegrenzte Verwendungen.

156 (b) Die erforderlichen Eingriffsschwellen können § 113 TKG auch nicht – wie noch der Vorgängerregelung – im Wege der Auslegung entnommen werden. [...]

159 (c) § 113 Abs. 1 S. 2 TKG, der zur Übermittlung von Zugangsdaten berechtigt, ist mit Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG unvereinbar.

160 aa) § 113 Abs. 1 S. 2 TKG erlaubt die Erteilung einer Auskunft von Daten, die als Zugangsdaten den Zugriff auf Endgeräte oder externe Speichereinrichtungen sichern. [...]

161 Die Erklärung der Verfassungswidrigkeit einer Norm hindert den Gesetzgeber zwar nicht daran, eine inhaltlich gleichlautende Bestimmung wiederum zu erlassen (vgl. BVerfGE 77, 84, 103 f.). Dabei kann er aber die vom BVerfG festgestellten Gründe der Verfassungswidrigkeit des ursprünglichen Gesetzes nicht übergehen. Eine Normwiederholung verlangt vielmehr ihrerseits besondere Gründe, die sich vor allem aus einer wesentlichen Änderung der für die verfassungsrechtliche Beurteilung maßgeblichen tatsächlichen oder rechtlichen Verhältnisse oder der ihr zugrundeliegenden Anschauungen ergeben können. Fehlen solche Gründe, ist das BVerfG nicht gehalten, die

bereits entschiedenen verfassungsrechtlichen Fragen erneut zu erörtern (BVerfGE 96, 260, 263).

162 bb) Solche Gründe sind hier nicht ersichtlich. [...]

163 d) Die in § 113 Abs. 1 S. 3 TKG neu geschaffene Befugnis, auch anhand einer dynamischen IP-Adresse bestimmte Bestandsdaten zu übermitteln, genügt nicht den Anforderungen der Verhältnismäßigkeit und verstößt damit gegen Art. 10 Abs. 1 GG.

164 aa) § 113 Abs. 1 S. 3 TKG regelt mit der erforderlichen Normenklarheit, dass auch über solche Bestandsdaten Auskunft erteilt werden darf, die anhand einer dynamischen IP-Adresse bestimmt werden. [...]

165 bb) § 113 Abs. 1 S. 3 TKG hat ein gegenüber der allgemeinen Bestandsdatenauskunft erhöhtes Eingriffsgewicht. [...]

166 (1) Die Begründung behördlicher Auskunftsansprüche zur Identifizierung dynamischer IP-Adressen hat aufgrund der Aussagekraft und der Verwendungsmöglichkeiten der zu beauskunftenden Bestandsdaten ein erhebliches Gewicht. [...]

167 Zwar hat die Zuordnung einer dynamischen IP-Adresse eine gewisse Ähnlichkeit mit der Identifizierung einer Telefonnummer. Die Abfrage des Inhabers einer Telefonnummer erbringt jedoch nicht ohne weiteres auch Informationen zu konkreten Telekommunikationsakten. Demgegenüber enthält eine Auskunft über den Anschlussinhaber einer dynamischen IP-Adresse in sich notwendig zugleich die Information, dass und von welchem Anschluss aus diese IP-Adresse zu einer bestimmten Zeit genutzt wurde. Da der Inhalt von Internetseiten elektronisch fixiert und länger wieder abrufbar ist, gibt die Individualisierung der IP-Adresse zugleich Auskunft über den Inhalt des Kontakts. Schon vom Umfang, vor allem aber vom Inhalt der Kontakte her, über die sie Auskunft geben kann, hat sie damit eine erheblich größere Persönlichkeitsrelevanz als die Identifizierung einer Telefonnummer und kann mit ihr nicht gleichgesetzt werden (vgl. [K&R 2012, 274 =] BVerfGE 130, 151, 204 mit Verweis auf BVerfGE 125, 260, 341 ff.).

168 (2) Das Eingriffsgewicht erhöhend wirkt sich weiter aus, dass die Diensteanbieter zur Bestimmung der zu beauskunftenden Daten auch Verkehrsdaten auswerten, denen von vornherein eine höhere Persönlichkeitsrelevanz zukommt als reinen Bestandsdaten. Zwar handelt es sich bei Verkehrsdaten nur um Verbindungsdaten, ohne dass dabei auch der Inhalt der Kommunikation erfasst würde. Aus Verkehrsdaten lassen sich aber bei umfassender Erhebung und Auswertung grundsätzlich aussagekräftige Persönlichkeits- und Bewegungsprofile erstellen (vgl. BVerfGE 125, 260, 319).

169 Das Gewicht des Eingriffs wird hier jedoch dadurch abgemildert, dass die um Auskunft ersuchenden Behörden bei der Zuordnung dynamischer IP-Adressen keine Kenntnis der Verkehrsdaten erhalten. [...]

170 (a) Dies gilt zunächst für die nach § 96 TKG erhobenen Verkehrsdaten. Hierbei handelt es sich um solche Verkehrsdaten, die die Diensteanbieter nach Maßgabe ihrer betrieblichen Erfordernisse in begrenztem Umfang und für den Einzelnen durch Vertragsgestaltung teilweise vermeidbar gemäß § 96 TKG speichern dürfen (vgl. BVerfGE 125, 260, 352). [...]

171 (b) Für die Zuordnung einer dynamischen IP-Adresse können allerdings nicht nur die nach § 96 TKG erhobenen Verkehrsdaten ausgewertet werden, sondern grundsätzlich

auch die von öffentlich zugänglichen Telekommunikationsdiensten für zehn Wochen (§ 113 b Abs. 1 Nr. 1 TKG) anlasslos und systematisch gespeicherten Verkehrsdaten (vgl. BVerfGE 125, 260, 328, 352; siehe aber zur derzeitigen Handhabung der Speicherungspflicht oben Rn. 12). Damit geht grundsätzlich eine deutliche Erhöhung des Eingriffsgewichts einher. [...]

172 (c) Soweit gemäß § 113 Abs. 1 S. 4 TKG für die Auskunftserteilung anhand dynamischer IP-Adressen darüber hinaus sämtliche unternehmensinternen Datenquellen zu berücksichtigen sind, kommt dem keine weitere eingriffserhöhende Wirkung zu. [...]

173 (d) § 113 Abs. 1 S. 3 TKG eröffnet schließlich auch keine spezifischen Missbrauchsgefahren. [...]

174 cc) Unter Berücksichtigung seines gleichwohl erhöhten Eingriffsgewichts erfüllt § 113 Abs. 1 S. 3 TKG die sich aus dem Verhältnismäßigkeitsgebot ergebenden Anforderungen an eine hinreichende Begrenzung der Verwendungszwecke für die zu beauskunftenden Daten nicht.

175 (1) Soweit für die Zuordnung von IP-Adressen nicht nur auf die nach § 96 TKG erhobenen, sondern auch auf vorsorglich gespeicherte Verkehrsdaten zurückgegriffen werden darf, müssen verfassungsrechtlich zwar nicht die für die unmittelbare Verwendung der Gesamtheit der vorsorglich gespeicherten Verkehrsdaten geltenden besonders strengen Voraussetzungen gegeben sein (vgl. BVerfGE 125, 260, 340). Dem erhöhten Eingriffsgewicht muss gleichwohl durch hinreichend begrenzte Verwendungszwecke Rechnung getragen werden. Erforderlich sind grundsätzlich die Reichweite des § 113 Abs. 1 S. 3 TKG näher begrenzende Eingriffsschwellen sowie eine Beschränkung auf den Schutz oder die Bewehrung von Rechtsgütern von hervorgehobenem Gewicht.

176 (a) Die Zuordnung dynamischer IP-Adressen bedarf – wie die allgemeine Bestandsdatenauskunft – begrenzender Eingriffsschwellen, die sicherstellen, dass Auskünfte nicht ins Blaue hinein eingeholt werden können. Erforderlich sind daher grundsätzlich qualifizierte Eingriffsschwellen, die einen Anfangsverdacht oder eine konkrete Gefahr auf einzelfallbezogener Tatsachenbasis voraussetzen. Letzteres gilt für die Nachrichtendienste ebenso wie für alle zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung zuständigen Behörden (vgl. BVerfGE 125, 260, 343 f.).

177 (b) Zu den Anforderungen des Übermaßverbots gehört es zudem, dass die in § 113 Abs. 1 S. 3 TKG eröffnete Bestandsdatenauskunft durch einen im Verhältnis zum Grundrechtseingriff hinreichend gewichtigen Rechtsgüterschutz gerechtfertigt sein muss. [...]

178 Dem Eingriffsgewicht der individualisierten Zuordnung dynamischer IP-Adressen entspricht es daher, dass sie zu ihrer Rechtfertigung jeweils auf Gründe gestützt werden muss, die dem Schutz oder der Bewehrung von Rechtsgütern von hervorgehobenem Gewicht (vgl. BVerfGE 125, 260, 344) dienen. [...]

183 (2) Diesen Anforderungen genügt § 113 Abs. 1 S. 3 TKG nicht. Die Zuordnung dynamischer IP-Adressen ist an keine begrenzenden Eingriffsschwellen gebunden und daher unverhältnismäßig.

184 (a) § 113 Abs. 2 S. 1 TKG, der die Voraussetzungen der Übermittlung näher regelt und die Verwendungszwecke auch für die Zuordnung dynamischer IP-Adressen bestimmt, setzt weder einen Anfangsverdacht noch eine

auf tatsächliche Anhaltspunkte gestützte konkrete Gefahr voraus.

185 Bezogen auf die allgemeine Gefahrenabwehr fehlt zudem die – auch unter Zugrundelegung solchermaßen qualifizierter Eingriffsschwellen – erforderliche Begrenzung der Befugnis auf einen hinreichend gewichtigen Rechtsgüterschutz. [...]

186 Das Gleiche gilt bezogen auf die Strafverfolgung, soweit § 113 Abs. 2 S. 1 TKG die Auskunftserteilung zum Zweck der Verfolgung jeglicher Ordnungswidrigkeiten erlaubt. [...]

187 (b) Die Befugnis zur Zuordnung von IP-Adressen wird in § 113 Abs. 2 S. 1 TKG auch nicht durch abgesenkte Eingriffsschwellen begrenzt. Insbesondere eine konkretisierte Gefahr wird weder für die allgemeine Gefahrenabwehr noch für die Tätigkeiten der Nachrichtendienste vorausgesetzt. [...]

188 e) Demgegenüber bestehen gegen die hier angegriffenen Übermittlungsregelungen keine Bedenken im Hinblick auf die verfassungsrechtlich gebotene Datensicherheit. [...]

189 IV. Die mit § 113 TKG korrespondierenden Abrufregelungen genügen in materieller Hinsicht weitgehend nicht den verfassungsrechtlichen Anforderungen des Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG und des Art. 10 Abs. 1 GG.

190 1. Da Übermittlung und Abruf personenbezogener Daten je eigenständige Grundrechtseingriffe begründen, müssen auch die einzelnen Abrufregelungen in Abhängigkeit von dem jeweils betroffenen Grundrecht und ihrem Eingriffsgewicht den Anforderungen der Verhältnismäßigkeit sowie der Normenklarheit und Bestimmtheit genügen. Die relevanten verfassungsrechtlichen Anforderungen ergeben sich vor allem aus dem Grundsatz der Verhältnismäßigkeit im engeren Sinne, der voraussetzt, dass die Abrufregelungen auf einer jeweils eigenen hinreichend bestimmten gesetzlichen Grundlage beruhen, die die Datenverwendung auf spezifische Zwecke hinreichend begrenzt.

191 2. Die angegriffenen Abrufregelungen dienen – wie schon § 113 TKG (oben Rn. 124 ff.) – legitimen Zwecken und sind hierfür geeignet und erforderlich. [...]

194 3. Mit dem Verhältnismäßigkeitsgrundsatz im engeren Sinne sind die Abrufregelungen nur vereinbar, wenn die einzelnen Befugnisse zum Datenabruf hinreichend begrenzt und die notwendigen übergreifenden Anforderungen an Transparenz, Rechtsschutz und Kontrolle beachtet werden (a). Diesen Anforderungen genügen die angegriffenen Befugnisse zum allgemeinen Abruf von Bestandsdaten (b) im Gegensatz zu den Befugnissen zum Abruf von Zugangsdaten (c) weitgehend nicht. Ebenfalls in weitem Umfang nicht hinreichend eingegrenzt sind die Befugnisse zum Abruf von anhand einer dynamischen IP-Adresse bestimmter Bestandsdaten (d), welche zudem sämtlich nicht den verfassungsrechtlichen Anforderungen an die verfahrensrechtlichen Sicherungen genügen (e).

195 a) Den Anforderungen der Verhältnismäßigkeit im engeren Sinne genügen die angegriffenen Abrufregelungen, wenn der mit ihnen verfolgte Zweck seinerseits nicht außer Verhältnis zu der Schwere des Eingriffs steht. Die angegriffenen Regelungen müssen hinreichend bestimmt und normenklar eine qualifizierte Ermächtigungsgrundlage für den Datenabruf schaffen (aa). Sie müssen unter Berücksichtigung ihres Eingriffsgewichts und den jeweils verfolgten Zwecken hinreichende Verwendungsregeln

enthalten und insoweit für sich genommen verhältnismäßig ausgestaltet sein (bb). Die Befugnisse zum Datenabruf sind darüber hinaus – aus Gründen der Normenklarheit – auch an die in den Übermittlungsregelungen begrenzten Verwendungszwecke gebunden (cc). Im Übrigen folgen aus dem Verhältnismäßigkeitsgrundsatz für alle Abrufregelungen gewisse übergreifende Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle sowie an Regelungen zur Datennutzung und -löschung (dd). [...]

204 b) Die fachrechtlichen Regelungen, die allgemein zum Abruf von Bestandsdaten ermächtigen, genügen diesen verfassungsrechtlichen Anforderungen weitgehend nicht. Den übergreifenden verfahrensrechtlichen Anforderungen wird demgegenüber insoweit Genüge getan (vgl. unten e, Rn. 244 ff.).

205 aa) Die Abrufregelungen schaffen allerdings jeweils hinreichend bestimmt und normenklar spezifische Ermächtigungsgrundlagen für die durch § 113 TKG zur Übermittlung geöffneten Daten. Neben der Ermächtigung der abfrageberechtigten Behörden nehmen die Regelungen private Dritte in die Pflicht und schaffen damit spezifische Rechtsgrundlagen, die eigenständig eine Auskunftspflicht der Diensteanbieter begründen. Alle Regelungen bezeichnen die jeweils abfrageberechtigte Behörde und nehmen ausdrücklich auf die „nach §§ 95 und 111 TKG erhobenen Daten“ sowie auf § 113 TKG Bezug.

206 bb) Die angegriffenen Regelungen sind jedoch mit Blick auf ihr Eingriffsgewicht, das sich maßgeblich nach Art, Umfang und Verwendungsmöglichkeiten der betroffenen Daten bestimmt, überwiegend nicht verhältnismäßig ausgestaltet. Fast alle Regelungen setzen keine den Datenabruf begrenzenden Eingriffsschwellen voraus und enthalten solche auch nicht durch normenklare Verweisungen.

207 (1) Die allgemein zum Abruf von Bestandsdaten ermächtigenden § 10 Abs. 1 S. 1 BKAG, § 7 Abs. 5 S. 1, § 15 Abs. 2 S. 1 ZFdG, § 8 d Abs. 1 S. 1 BVerfSchG sowie § 2 b S. 1 BNDG und § 4 b S. 1 MADG, soweit sie auf § 8 d Abs. 1 S. 1 BVerfSchG verweisen, sind nicht hinreichend eingegrenzt und darum unverhältnismäßig. [...]

219 (2) Nur teilweise den Anforderungen der Verhältnismäßigkeit genügt § 40 Abs. 1 S. 1 BKAG, der das Bundeskriminalamt allgemein zum Abruf von Bestandsdaten ermächtigt, soweit dies für die Erforschung eines Sachverhalts oder die Ermittlung des Aufenthalts einer Person nach Maßgabe des § 39 Abs. 1 und 2 BKAG erforderlich ist. [...]

229 (3) § 22 a Abs. 1 S. 1 BPolG, der die Bundespolizei zum Abruf von Bestandsdaten ermächtigt, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes einer Person nach Maßgabe des § 21 Abs. 1 und 2 BPolG erforderlich ist, genügt den verfassungsrechtlichen Anforderungen ebenfalls nur teilweise. [...]

234 c) Die angegriffenen Befugnisse zum Abruf von Zugangsdaten (vgl. § 10 Abs. 1 S. 2, § 40 Abs. 1 S. 2 BKAG, § 22 a Abs. 1 S. 2 BPolG, § 7 Abs. 5 S. 2, § 15 Abs. 2 S. 2 ZFdG, § 8 d Abs. 1 S. 2 BVerfSchG sowie § 2 b S. 1 BNDG und § 4 b S. 1 MADG, soweit sie auf § 8 d Abs. 1 S. 2 BVerfSchG verweisen) sind für sich genommen hinreichend begrenzt und verhältnismäßig. Sie genügen auch den übergreifenden verfahrensrechtlichen Anforderungen (vgl. unten e, Rn. 244 ff.).

235 Alle Abrufregelungen setzen gleichlautend voraus, dass eine Auskunft nur verlangt werden darf, wenn die

gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. Die Regelungen stellen damit sicher, dass Zugangsdaten nicht unabhängig von den Anforderungen an deren Nutzung und damit gegebenenfalls unter leichteren Voraussetzungen abgefragt werden können (vgl. [K&R 2012, 274 =] BVerfGE 130, 151, 208 f.). [...]

237 d) Die Regelungen zum Abruf von Bestandsdaten, die anhand einer dynamischen IP-Adresse bestimmt werden (§ 10 Abs. 2, § 40 Abs. 2 BKAG, § 22 a Abs. 2 BPolG, § 7 Abs. 6, § 15 Abs. 3 ZFdG, § 8 d Abs. 2 S. 1 BVerfSchG sowie § 2 b S. 1 BNDG und § 4 b S. 1 MADG, soweit sie auf § 8 d Abs. 2 S. 1 BVerfSchG verweisen) sind ganz überwiegend nicht hinreichend eingegrenzt und schon deshalb unverhältnismäßig. Allein § 40 Abs. 2 BKAG genügt, soweit er auf § 39 Abs. 2 Nr. 2 BKAG Bezug nimmt, insoweit den verfassungsrechtlichen Anforderungen; er erfüllt jedoch seinerseits nicht die übergreifenden verfahrensrechtlichen Anforderungen (vgl. unten e, Rn. 244 ff.).

238 Zwar ist es aus Gründen der Verhältnismäßigkeit grundsätzlich nicht geboten, für den Abruf von Bestandsdaten, die anhand dynamischer IP-Adressen bestimmt werden, gegenüber der allgemeinen Bestandsdatenabfrage erhöhte Eingriffsschwellen vorzusehen (oben Rn. 176, 179). Erforderlich ist aber stets ein hinreichend gewichtiger Rechtsgüterschutz, der in Wechselwirkung mit der jeweiligen Eingriffsschwelle steht. Für die Zuordnung von IP-Adressen bedarf es selbst dann, wenn Eingriffsschwellen vorgesehen werden, die bezogen auf die Gefahrenabwehr eine konkrete Gefahr und bezogen auf die Strafverfolgung einen Anfangsverdacht voraussetzen, einer Beschränkung der Eingriffsbefugnis auf den Schutz von Rechtsgütern von hervorgehobenem Gewicht (oben Rn. 177 f.). Sind die Eingriffsschwellen hingegen herabgesetzt und will der Gesetzgeber für die Auskunft die Abwehr konkretisierter Gefahren genügen lassen, ist unter Berücksichtigung des spezifischen Eingriffsgewichts der Zuordnung dynamischer IP-Adressen jedenfalls eine Beschränkung auf besonders gewichtige Rechtsgüter geboten (oben Rn. 180). Diesen verfassungsrechtlichen Anforderungen werden die angegriffenen Regelungen – zusätzlich zu dem weitgehenden Fehlen begrenzender Eingriffsschwellen – überwiegend nicht gerecht.

239 aa) Die Abrufregelungen in § 10 Abs. 2 BKAG, § 40 Abs. 2 i. V. m. § 39 Abs. 1 und 2 Nr. 1 BKAG, § 22 a Abs. 2 i. V. m. § 21 Abs. 1 und 2 Nr. 1 BPolG, § 7 Abs. 6 und § 15 Abs. 3 ZFdG, § 8 d Abs. 2 S. 1 BVerfSchG sowie § 2 b S. 1 BNDG und § 4 b S. 1 MADG, soweit sie auf § 8 d Abs. 2 S. 1 BVerfSchG verweisen, knüpfen allein an die ihrerseits unverhältnismäßigen Voraussetzungen der Befugnis zum allgemeinen Abruf von Bestandsdaten an (oben Rn. 206 ff.) und sehen daher auch für die Zuordnung von IP-Adressen keine oder jedenfalls keine hinreichend begrenzenden Eingriffsschwellen vor. Sie genügen schon deshalb nicht den verfassungsrechtlichen Anforderungen und sind unverhältnismäßig. [...]

243 bb) Dagegen enthalten zwar sowohl § 22 a Abs. 2 BPolG i. V. m. § 21 Abs. 2 Nr. 2 BPolG, als auch § 40 Abs. 2 i. V. m. § 39 Abs. 2 Nr. 2 BKAG hinreichend begrenzte Eingriffsschwellen (oben Rn. 227 f., 232). Doch nur § 40 Abs. 2 BKAG erfüllt auch die unter Berücksichtigung des Eingriffsgewichts der Zuordnung dynamischer IP-Adressen zu stellenden Anforderungen an den Rechtsgüterschutz, wonach die Zuordnung dynamischer IP-Adressen bei – wie hier – abgesenkten Eingriffsschwellen im Bereich der Straftatenverhütung der Verhütung zumindest schwerer Straftaten dienen muss (oben Rn. 181). § 22 a

Abs. 2 i. V. m. § 21 Abs. 2 Nr. 2 BPolG, der die Zuordnung dynamischer IP-Adressen bereits zur Verhütung von Straftaten mit erheblicher Bedeutung zulässt, genügt dem nicht.

244 e) Die angegriffenen Regelungen genügen im Wesentlichen den aus dem Verhältnismäßigkeitsgrundsatz folgenden übergreifenden Maßgaben an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle. Sie enthalten auch tragfähige Regelungen zur Nutzung der Daten sowie zur Datenlöschung. Verfassungsrechtlich zu beanstanden ist allerdings, dass den Behörden beim Abruf von anhand dynamischer IP-Adressen bestimmter Bestandsdaten keine Dokumentationspflichten auferlegt werden.

245 aa) Anders als für heimliche Maßnahmen von höherer Eingriffsintensität (vgl. BVerfGE 141, 220, 269 Rn. 105, 282 f. Rn. 134 ff.) bedarf es für die allgemeine Bestandsdatenauskunft aufgrund ihrer vergleichsweise geringen Eingriffsintensität keiner Benachrichtigungspflichten (vgl. [K&R 2012, 274 =] BVerfGE 130, 151, 210; vgl. auch EGMR, Breyer v. Germany, Urt. v. 30. 1. 2020, Nr. 50001/12, § 107 (nicht endgültig); EuGH, Urt. v. 2. 10. 2018, Ministerio Fiscal, C-207/16, [K&R 2018, 700 ff. =] EU:C:2018:788, Rn. 60 f.). Vielmehr reicht es unter Verhältnismäßigkeitsgesichtspunkten, wenn die Betroffenen von einer Auskunftserteilung im Rahmen von ihnen gegenüber ergriffenen Folgemaßnahmen erfahren und deren Rechtmäßigkeit dann fachgerichtlich überprüfen lassen können (vgl. BVerfGE 150, 244, 302 Rn. 154).

246 Im Hinblick auf Auskünfte, die eine erhöhte Eingriffsintensität aufweisen, wie die Zuordnung von IP-Adressen und – potentiell – die Auskunft über Zugangsdaten, sehen die fachrechtlichen Abrufregelungen eine nachträgliche Benachrichtigung grundsätzlich vor. [...]

247 bb) Eine aufsichtliche Kontrolle ist – wie verfassungsrechtlich geboten (vgl. BVerfGE 65, 1, 46; 133, 277, 369 Rn. 214; 141, 220, 284 f. Rn. 141; st. Rspr.) – vorgesehen. [...]

248 cc) Demgegenüber ist es mit den Anforderungen der Verhältnismäßigkeit nicht vereinbar, dass keine Pflicht zur Dokumentation der Entscheidungsgrundlagen für den Abruf solcher Bestandsdaten vorgesehen ist, die anhand einer dynamischen IP-Adresse bestimmt werden.

249 Angesichts der nur geringen Eingriffsintensität der allgemeinen Bestandsdatenauskunft ist auch unter Berücksichtigung des Umstands, dass die Maßnahme regelmäßig geheim erfolgt und Betroffene auch im Nachhinein nicht über eine erteilte Auskunft benachrichtigt werden, keine Dokumentation der Entscheidungsgrundlagen erforderlich. Sie ist auch nicht deshalb geboten, weil sich die Entscheidung über eine Bestandsdatenabfrage allein im Inneren einer Behörde vollziehen würde (dazu BVerfGE 150, 244, 303 Rn. 157). Zwar können allein die Behörden die materiellen Voraussetzungen eines Auskunftsverlangens sicherstellen. Sie treten aber jedenfalls insoweit nach außen, als sie ein schriftliches Auskunftsverlangen unter Angabe einer gesetzlichen Bestimmung an die Diensteanbieter richten müssen (vgl. § 113 Abs. 2 S. 1 TKG).

250 Dagegen kann die Zuordnung dynamischer IP-Adressen angesichts ihres erhöhten Eingriffsgewichts nur dann als verhältnismäßig angesehen werden, wenn die Entscheidungsgrundlagen für die Durchführung einer solchen Maßnahme nachvollziehbar und überprüfbar dokumentiert werden. Die rechtlichen und tatsächlichen Grundlagen entsprechender Auskunftsbegehren sind aktenkundig zu machen (BVerfGE 125, 260, 344). Zum einen rationalisiert

und mäßigt es die Entscheidung, wenn die entscheidende Behörde sich selbst über ihre Entscheidungsgrundlagen Rechenschaft ablegen muss. Zum anderen ermöglicht erst die Dokumentation eine aufsichtliche Kontrolle durch die Datenschutzbeauftragten. Schließlich wird durch die Dokumentation die verwaltungsgerichtliche Kontrolle erleichtert (vgl. BVerfGE 150, 244, 303 Rn. 157). Für den Abruf von Zugangsdaten bedarf es demgegenüber keiner Regelung genereller Dokumentationspflichten. Soweit sie aufgrund des Eingriffsgewichts im Einzelfall geboten sein sollten, ergeben sich entsprechende Anforderungen regelmäßig aus den jeweiligen Ermächtigungsgrundlagen zur Nutzung der Daten.

251 dd) Gesetzlich geregelter Berichtspflichten gegenüber Parlament und Öffentlichkeit bedarf es nicht. [...]

252 ee) Eine vorherige Kontrolle durch eine unabhängige Stelle, etwa in Form einer richterlichen Anordnung, ist aus Gründen der Verhältnismäßigkeit verfassungsrechtlich nicht geboten. Von daher begegnet es keinen Bedenken, dass die Abrufregelungen einfachrechtlich nur für den Abruf von Zugangsdaten einen Richtervorbehalt beziehungsweise im nachrichtendienstlichen Bereich eine vorherige Überprüfung durch die G 10-Kommission vorsehen und der für den Abruf von Zugangsdaten vorgesehene Richtervorbehalt zahlreiche Ausnahmen kennt. [...]

258 ff) Die Regelungen zur Sicherheit, weiteren Nutzung und Löschung der Daten durch die abfragenden Behörden genügen den verfassungsrechtlichen Anforderungen. [...]

262 E. Die angegriffenen Vorschriften sind überwiegend für mit Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 sowie mit Art. 10 Abs. 1 GG unvereinbar zu erklären. [...]

268 4. Die Unvereinbarkeitserklärung ist mit der Anordnung der vorübergehenden Fortgeltung bis zum Ablauf des 31. 12. 2021 verbunden. [...]

Kommentar

Regelungen zur Bestandsdatenauskunft mal wieder verfassungswidrig

RA Jan Spittka und
Rechtsreferendar Dr. Philipp Adelberg, Köln*

I. Hintergrund

Der Konflikt zwischen Datenschutz und staatlichen Sicherheitsinteressen geht in die nächste Runde: Nachdem der EGMR Anfang dieses Jahres die Registrierungspflicht für Prepaid-SIM-Karten nach § 111 TKG a. F. für (gerade noch) mit der EMRK vereinbar befand,¹ hat der Erste Senat des BVerfG nun erneut zur Frage der Verfassungsmäßigkeit der Auskunft über solche auf Vorrat gespeicherte Bestandsdaten Stellung genommen und § 113 TKG

* Jan Spittka ist Rechtsanwalt und Counsel bei DLA Piper und auf Datenschutzrecht und Cybersecurity spezialisiert. Dr. Philipp Adelberg ist Referendar bei DLA Piper. Mehr über die Autoren erfahren Sie auf S. VIII.

1 EGMR, 30. 1. 2020 – Nr. 50001/12 – Breyer gegen Deutschland; hierzu Spittka, K&R 2020, 263 ff.

sowie weitere Fachgesetze des Bundes für verfassungswidrig erklärt. Der Beschluss erging auf Verfassungsbeschwerde u. a. des Europaabgeordneten *Patrick Breyer* aus dem Jahre 2013. Die angegriffenen Normen dienten der Umsetzung der BVerfG-Entscheidung zu §§ 111 TKG a. F. aus dem Jahre 2012,² in der die Karlsruher Richter – auf die ebenfalls von *Breyer* geführte Verfassungsbeschwerde – die damaligen Vorgaben zur Bestandsdatenauskunft für teilweise verfassungswidrig erklärten. Nun befasste sich das BVerfG also mit ihrer Novellierung.

Gemäß § 113 Abs. 1 S. 1 TKG sind Anbieter von Telekommunikationsdiensten zur Übermittlung von Bestandsdaten im sog. manuellen Auskunftsverfahren berechtigt. Auf Verlangen bestimmter Behörden, wie z. B. Polizei, Verfassungsschutzbehörden und Bundesnachrichtendienst, haben sie Auskunft über nach § 111 TKG zu speichernde Bestandsdaten (wie Name, Geburtsdatum, Rufnummer des Anschlussinhabers) und gemäß § 95 TKG freiwillig zu betrieblichen Zwecken gespeicherte Kundendaten (wie Anschrift des Vertragspartners, Art des kontrahierten Dienstes) zu erteilen, ebenso nach § 113 Abs. 1 S. 2 TKG über vom Anbieter vergebene Zugangsdaten (wie PIN). § 113 Abs. 1 S. 3 TKG erlaubt die Bestimmung von Bestandsdaten anhand einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse.

Voraussetzung für die Auskunftserteilung ist laut § 113 Abs. 2 TKG, dass eine in Abs. 3 genannte Stelle sie für Zwecke der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung gesetzlicher Aufgaben der Nachrichtendienste unter Angabe einer Abrufregelung verlangt. § 113 TKG enthält also eine Auskunftspflicht, während sich das Recht der Behörden zur Abfrage aus den Abrufregelungen ergibt. Das BVerfG sprach bereits von einem „Doppeltürmodell“:³ Der Gesetzgeber müsse sowohl die Tür der Übermittlung als auch die zur Abfrage von Daten durchschreiten. Erst beide Rechtsgrundlagen gemeinsam berechtigten zu einem Datenaustausch. Die Verfassungsbeschwerden richteten sich gegen die Abrufregelungen, die lediglich vorgeben, dass die Auskunft zur Erfüllung bestimmter Aufgaben erforderlich sein muss.

II. Inhalt und Begründung der Entscheidung

Das BVerfG entschied, dass die Regelungen in § 113 TKG nicht mit dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) und dem Telekommunikationsgeheimnis (Art. 10 Abs. 1 GG) vereinbar sind. Zwar diene die Norm legitimen Zwecken (Effektivierung der Strafverfolgung, Gefahrenabwehr, Aufgabenerfüllung der Nachrichtendienste), jedoch sei sie unverhältnismäßig.

1. Erste Tür: Übermittlung

Die Übermittlungsbefugnisse aus § 113 TKG griffen zwar zunächst nur geringfügig in das Recht auf informationelle Selbstbestimmung ein, allerdings sei die Norm wegen ihrer Reichweite unverhältnismäßig, so das BVerfG. Das Eingriffsgewicht werde vor allem durch Art, Umfang und denkbare Verwendung der Daten sowie die Gefahr ihres Missbrauchs bestimmt. Auskünfte dürften nur bei einem auf tatsächliche Anhaltspunkte gestützten Anlass erteilt werden, selbst wenn es sich um Daten handele, deren Aussagekraft oder Verwendungsmöglichkeit nur begrenzt sei. Auskünfte für die allgemeine behördliche Aufgabenerfüllung seien unzulässig. Bereits die Übermittlungsregelungen müssten Eingriffsschwellen enthalten. Im Gefah-

renabwehrrecht sei eine im Einzelfall konkretisierte Gefahr erforderlich; diese verhältnismäßig geringe Eingriffsschwelle erfordere aber den Schutz besonderer Rechtsgüter. Da bei der Bestandsdatenauskunft allerdings nur ein Eingriff geringer Intensität vorliege, könne dieser bei Vorliegen einer konkretisierten Gefahr bereits dann gerechtfertigt sein, wenn er dem Schutz von Rechtsgütern von zumindest erheblichem Gewicht diene. Für die Strafverfolgung müsse wenigstens ein Anfangsverdacht vorliegen.

Mit diesen Vorgaben sei § 113 Abs. 1 S. 1 TKG unvereinbar. Der Anwendungsbereich der Vorschrift sei zu weit gefasst, da sie Auskünfte allgemein zum Zwecke der Gefahrenabwehr, der Verfolgung von Straftaten oder Ordnungswidrigkeiten oder zur Erfüllung nachrichtendienstlicher Aufgaben erlaube und keine näher begrenzenden Eingriffsschwellen enthalte. § 113 Abs. 1 S. 2 TKG, welcher der schon 2012 für verfassungswidrig erklärten Vorgängerregelung entspreche, sei ebenso verfassungswidrig. Zwar sei eine Normwiederholung nicht per se ausgeschlossen, allerdings müssten sich die Verhältnisse, die ihr zugrunde liegen, maßgeblich verändert haben, was das Gericht nicht zu erkennen vermag. Ebenfalls verfassungswidrig sei die Befugnis, durch dynamische IP-Adressen Bestandsdaten zu übermitteln. Ein solches Vorgehen habe ein höheres Eingriffsgewicht, weil es durch die Aussagekraft der Zuordnung einer dynamischen IP-Adresse, die eine Rekonstruktion der individuellen Internetnutzung ermögliche, und die Verwendung von Verkehrsdaten eine erhöhte Persönlichkeitsrelevanz aufweise. Nach den o. g. Grundsätzen sei daher die Zuordnung dynamischer IP-Adressen z. B. zur Verfolgung von Ordnungswidrigkeiten und für die Gefahrenabwehr jenseits des Schutzes besonders gewichtiger Rechtsgüter und der Verhütung zumindest schwerer Straftaten unverhältnismäßig. Dadurch, dass der Gesetzgeber in den entsprechenden Fachgesetzen keine Einschränkung durch das Erfordernis einer Gefahr für Rechtsgüter von hervorgehobener Bedeutung getroffen habe, ergebe sich die Verfassungswidrigkeit der Norm. Im Übrigen sei sie auch nicht mit Art. 10 Abs. 1 GG vereinbar.

2. Zweite Tür: Abruf

Ferner erachtet das BVerfG die Abrufregelungen⁴ größtenteils ebenfalls für verfassungswidrig. Der Abruf personenbezogener Daten stelle einen Grundrechtseingriff dar, der auf einer verfassungsmäßigen Grundlage beruhen müsse. Die Abrufregelungen seien jedoch unverhältnismäßig, da sie ebenfalls keine konkretisierten Eingriffsschwellen enthielten, sondern die Wahrnehmung öffentlicher Aufgaben genügen ließen. Die Abrufbefugnisse der Behörden seien allerdings nicht verfassungswidrig, da sie sicherstellten, dass Zugangsdaten nicht unabhängig von den Anforderungen an deren Nutzung abgerufen werden könnten. Zudem beurteilen die Richter die Regelungen zum Abruf von Bestandsdaten anhand dynamischer IP-Adressen als verfassungswidrig, da sie neben der fehlenden Eingriffsschwelle keine Pflicht zur nachvollziehbaren und überprüfaren Dokumentation der Entscheidungsgrundlagen vorsehen.

III. Beurteilung der Entscheidung

Der Beschluss reiht sich in eine Folge von Entscheidungen, die die widerstreitenden Interessen des Datenschutzes und

2 BVerfG, 24. 1. 2012 – 1 BvR 1299/05, K&R 2012, 274 ff. – Bestandsdatenauskunft I.

3 BVerfG, 24. 1. 2012 – 1 BvR 1299/05, K&R 2012, 274 ff., Rn. 123 – Bestandsdatenauskunft I.

4 Vgl. § 22 a BPolG; §§ 7, 15 ZFdG; § 8 d BVerfSchG; § 4 b MADG; § 2 b BNDG; §§ 10, 40 BKAG bzw. §§ 7, 20 b, 22 BKAG a. F.

der staatlichen Sicherheitsinteressen diskutieren, ein. So kritisierte der Richter am EGMR *Ranzoni* in seiner *Dissenting Opinion* zur Entscheidung über die Registrierungspflicht für Prepaid-SIM-Karten⁵ das Doppeltürmodell scharf: Wenn allgemeine Ermittlungsbefugnisse zum Durchschreiten einer Tür bereits ausreichen, so liege kein ausreichender Schutz der massenhaft und auf Vorrat gespeicherten personenbezogenen Daten vor. Im Kern dreht sich die Entscheidung erneut um die Reichweite des Rechts auf informationelle Selbstbestimmung; die Feststellung der Unvereinbarkeit mit Art. 10 Abs. 1 GG scheint die grundsätzliche Argumentation der Verfassungsrichter lediglich zu flankieren. In Fortsetzung der Grundsätze des *Volkszählungsurteils*,⁶ laut denen das Recht auf informationelle Selbstbestimmung zum Schutz öffentlicher Interessen nur eingeschränkt werden darf, wenn dies unerlässlich ist, bewertet das BVerfG die Regelungen zur Bestandsdatenauskunft als unverhältnismäßig.

Im Ergebnis ist die keineswegs überraschende Entscheidung zu begrüßen, da sie eine maßvolle Abwägung zwischen Persönlichkeitsrechten und Maßnahmen der Gefahrenabwehr bzw. Strafverfolgung fordert. Die Bestandsdatenauskunft ist für letztere ein wichtiges und effektives Mittel, das jedoch als scharfes Schwert hinsichtlich der Voraussetzungen seines Einsatzes einer stark grundrechtlich geprägten Beschränkung bedarf. Nicht jede Ordnungswidrigkeit, nicht jede Gefahrenabwehrmaßnahme kann unter diesen Grundbedingungen Datenübermittlung und -abruf legitimieren. Interessant ist jedoch, dass dem BVerfG im Rahmen der Strafverfolgung ein Anfangsverdacht im Hinblick auf jede Straftat zu genügen scheint. Hier ist eine Einschränkung auf besonders schwere Straftaten – anders als bei der Gefahrenabwehr – nicht erforderlich. Für einen Richtervorbehalt beim Abruf dynamischer IP-Adressen, wie er zum Teil gefordert wurde, sahen die Verfassungsrichter ebenfalls keinen Bedarf.⁷ Gestaltet der Gesetzgeber nun die Bestandsdatenauskunft verfassungsgemäß aus, ist ein solcher Vorbehalt in der Tat nicht zwingend erforderlich.

IV. Ausblick

Das BVerfG hat ein weiteres Mal klargestellt, dass eine Einschränkung des Datenschutzes zugunsten staatlicher Sicherheitsinteressen nur bei hinreichender Begrenzung der Verwendungszwecke der Daten, tatbestandlichen Eingriffsschwellen und einem hinreichend gewichtigen Rechtsgüter-schutz zulässig ist. Im Übrigen müsse auch die verfassungsrechtlich gebotene Datensicherheit gewährleistet sein. Für verfassungswidrig, nicht für nichtig erklärte das BVerfG § 113 TKG. So wie bereits auch nach dem Beschluss von vor acht Jahren ist es nun am Gesetzgeber, die Norm bis zu dem Ablauf einer Übergangsfrist Ende 2021 zu überarbeiten. Bis dahin bleiben die Regelungen in Kraft, freilich unter der Prämisse einschränkender Vorgaben für ihre Anwendung. Ob dem Gesetzgeber eine verfassungsmäßige Ausgestaltung gelingen wird, bleibt angesichts der Historie gesetzgeberischer Unzulänglichkeiten auf diesem Gebiet⁸ aber fraglich. Die Bestandsdatenauskunft wird sehr wahrscheinlich weiter auf dem Prüfstand stehen.

5 EGMR, 30. 1. 2020 – Nr. 50001/12 – Breyer gegen Deutschland.

6 BVerfG, 15. 12. 1983 – 1 BvR 209/83, NJW 1984, 419 ff.

7 S. auch BVerfG, 2. 3. 2010 – 1 BvR 256/08, K&R 2010, 248 ff.; EuGH, 21. 12. 2016 – C-203/15, EuGH, 21. 12. 2016 – C-698/15, K&R 2017, 105.

8 Zuletzt BVerfG, 19. 5. 2020 – 1 BvR 2835/17, K&R 2020, 520 f. – Ausland-Ausland-Aufklärung.

Cookie-Einwilligung II: Keine wirksame Einwilligung bei voreingestellten Häkchen

BGH, Urteil vom 28. 5. 2020 – I ZR 7/16

Volltext-ID: KuRL2020-611, www.kommunikationundrecht.de

ECLI:DE:BGH:2020:280520UIZR7.16.0

Verfahrensgang: EuGH, 1. 10. 2019 – C-673/17, K&R 2019, 705 ff.; BGH, 5. 10. 2017 – I ZR 7/16, K&R 2018, 54 ff.; OLG Frankfurt a. M., 17. 12. 2015 – 6 U 30/15, K&R 2016, 197 ff.; LG Frankfurt a. M., 10. 12. 2014 – 2/6 O 30/14

§ 307 BGB; Art. 5 Abs. 3, Art. 2 lit. f RL 2002/58/EG; Art. 2 Nr. 5 RL 2009/136/EG; Art. 2 lit. h RL 95/46/EG; § 15 Abs. 3 TMG; § 1 UKlaG; Art. 4 Nr. 11 VO (EU) 2016/679

a) Eine wirksame Einwilligung in telefonische Werbung im Sinne von § 7 Abs. 2 Nr. 2 Fall 1 UWG liegt nicht vor, wenn der Verbraucher bei der Erklärung der Einwilligung mit einem aufwendigen Verfahren der Abwahl von in einer Liste aufgeführten Partnerunternehmen konfrontiert wird, das ihn dazu veranlassen kann, von der Ausübung dieser Wahl Abstand zu nehmen und stattdessen dem Unternehmer die Wahl der Werbepartner zu überlassen. Weiß der Verbraucher mangels Kenntnisnahme vom Inhalt der Liste und ohne Ausübung des Wahlrechts nicht, die Produkte oder Dienstleistungen welcher Unternehmer die Einwilligung erfasst, liegt keine Einwilligung für den konkreten Fall vor.

b) § 15 Abs. 3 S. 1 TMG ist mit Blick auf Art. 5 Abs. 3 S. 1 der RL 2002/58/EG dahin richtlinienkonform auszulegen, dass der Diensteanbieter Cookies zur Erstellung von Nutzungsprofilen für Zwecke der Werbung oder Marktforschung nur mit Einwilligung des Nutzers einsetzen darf. Eine elektronisch zu erklärende Einwilligung des Nutzers, die den Abruf von auf seinem Endgerät gespeicherten Informationen mithilfe von Cookies im Wege eines voreingestellten Ankreuzkästchens gestattet, genügt diesem Einwilligungserfordernis nicht. (Leitsätze des Gerichts)

Sachverhalt

Der Kläger ist der in die Liste qualifizierter Einrichtungen nach § 4 UKlaG eingetragene Bundesverband der Verbraucherzentralen. Die Beklagte bietet die Teilnahme an Gewinnspielen im Internet an. Am 24. 9. 2013 veranstaltete die Beklagte unter der Internetadresse „www.[...]de“ ein Gewinnspiel. Nach Eingabe der Postleitzahl gelangte der Nutzer hierbei auf eine Seite, auf der Name und Anschrift des Nutzers einzutragen waren. Unter den Eingabefeldern für die Adresse befanden sich zwei mit Ankreuzfeldern versehene Hinweistexte. Eine Teilnahme am Gewinnspiel war nur möglich, wenn mindestens das Häkchen vor dem ersten Hinweistext gesetzt wurde.

Der im ersten Hinweistext den Worten „Sponsoren und Kooperationspartner“ und „hier“ unterlegte elektronische Verweis führte zu einer Liste, die 57 Unternehmen, ihre Adresse, den zu bewerbenden Geschäftsbereich und die für die Werbung genutzte Kommunikationsart (E-Mail, Post oder Telefon) sowie nach jedem Unternehmen das unterstrichene Wort „Abmelden“ enthielt. Der Liste vorangestellt war folgender Hinweis: „Durch Anklicken auf dem