Meinhard Starostik

Rechtsanwalt

Rechtsanwaltskanzlei:
Schillstr. 9 ◆ 10785 Berlin
Tel.: 030 - 88 000 345
Fax: 030 - 88 000 346
email: Kanzlei@Starostik.de
USt-ID-Nr. DE165877648

Kanzlei vereidigter Buchprüfer:
Schwarzenberger Str. 7 ◆ 08280 Aue
Tel.: 03771-290 999

RA Starostik, Schillstraße 9, 10785 Berlin

An das
Bundesverfassungsgericht
Schloßbezirk 3
76131 Karlsruhe

Berlin, den 12. August 2010

AZ: 42/05
(bitte stets angeben)

Verfassungsbeschwerde

- 1 BvR 1299/05 -

Das Urteil des Hohen Gerichts vom 2. März 2010 zur Verkehrsdatenspeicherung gibt Anlass, dessen Auswirkungen auf die vorliegende Verfassungsbeschwerde zu erörtern.

Inhaltsübersicht

1 §§ 95 Abs. 3, 111 Abs. 4 TKG (Vorratsspeicherung von Bestandsdaten)

1.1 Verletzung des Artikels 10 GG

1.1.1 Eingriff in den Schutzbereich

In der Beschwerdeschrift und mit Schriftsatz vom 20.04.2007 ist im Einzelnen dargelegt worden, dass die §§ 95 Abs. 3, 111 Abs. 4 TKG Kommunikationsmittler zur Vorratsspeicherung von Bestandsdaten für die Dauer von 1-2 Jahren verpflichten und nicht nur berechtigen. Diese Pflicht zur Vorratsspeicherung betrieblich nicht erforderlicher Informationen über Fernmeldeteilnehmer greift in deren Grundrecht aus Art. 10 GG ein. Mit Schriftsatz vom 07.05.2009 ist ausgeführt worden, dass statische Anschlusskennungen wie Rufnummern einfachgesetzlich als Verkehrsdaten einzuordnen sind,[1] dass unabhängig hiervon aber auch als Bestandsdaten einzuordnende Telekommunikationsdaten in den Schutzbereich des Art. 10 GG fallen.[2]

1.1.2 Mangelnde Rechtfertigung

Der in den §§ 95 Abs. 3, 111 Abs. 4 TKG liegende Grundrechtseingriff ist nicht gerechtfertigt.

1.1.2.1 Überschreitung des Gesetzesvorbehalts

Mit der Beschwerdeschrift ist ausgeführt worden,[3] dass **der Gesetzesvorbehalt des Art. 10 Abs. 2 GG** schon dem Wortlaut nach eine einzelfallunabhängige Beschneidung des Fernmeldegeheimnisses nicht ermöglicht. Art. 10 Abs. 2 S. 1 GG bestimmt: „Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden." Beschränkungen des Fernmeldegeheimnisses, die ohne Anordnung im Einzelfall unmittelbar durch Gesetz erfolgen, sind danach unzulässig. Die §§ 95 Abs. 3, 111 Abs. 4 TKG machen keine Einzelfallanordnung zur Vorbedingung der dort vorgesehenen Telekommunikationsdatenspeicherung. Soweit das Bundesverfassungsgericht zur Begründung seiner gegenteiligen, vom Wortlaut des Art. 10 Abs. 2 S. 1 GG nicht gedeckten Auslegung des Art. 10 Abs. 2 GG einzig auf seinen Fangschaltungsbeschluss Bezug nimmt,[4] war dort lediglich entschieden worden, dass „[e]in Gesetz, welches Gesprächsbeobachtungen zur Abwehr bedrohender oder belästigender anonymer Anrufe erlaubte, [...] bei [...] hinreichenden verfassungsrechtlichen Vorkehrungen [...] verfassungsrechtlich zulässig" wäre.[5] Es ist dort keineswegs entschieden worden, dass Gesprächsbeobachtungen ohne Anordnung im Einzelfall zulässig seien. Dementsprechend ist die Rüge der Verletzung des Art. 10 Abs. 2 S. 1 GG aufrecht zu erhalten.

1.1.2.2 Verletzung des Zitiergebots

Die §§ 95 Abs. 3, 111 Abs. 4 TKG verstoßen auch gegen das Zitiergebot des Art. 19 Abs. 1 S. 2 GG, weil sie das eingeschränkte Grundrecht (Art. 10 GG) nicht nennen. Der Gesetzgeber hat den **Eingriff in das Fernmeldegeheimnis verkannt**.

1.1.2.3 Verletzung des Verhältnismäßigkeitsgebots

Die §§ 95 Abs. 3, 111 Abs. 4 TKG verletzen vor allem das Verhältnismäßigkeitsgebot. Es ist bereits umfassend ausgeführt worden, dass eine Vorratsspeicherung von Telekommunikationsdaten Allgemeininteressen kaum dient, auf der anderen Seite aber ins Blaue hinein und ohne Anlass

---

[1] Schriftsatz vom 07.05.2009, 6 und 29.

[2] Schriftsatz vom 07.05.2009, 1 ff.

[3] Beschwerdeschrift, 27.

[4] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 198.

[5] BVerfGE 85, 386 (401).

die gesamte Bevölkerung dem ständigen Risiko eines Missbrauchs oder Verlustes vertraulicher Daten sowie eines falschen Verdachts aufgrund der irrtumsanfälligen Telekommunikationsdaten aussetzt und dadurch **unzumutbar von freier Fernkommunikation abschreckt**.

1.1.2.3.1 Vorratsspeicherung von Name, Anschrift und Anschlusskennung

Soweit die angefochtenen Vorschriften – wie auch die Richtlinie 2006/24/EG – die Vorratsspeicherung von Name, Anschrift und Anschlusskennung der Nutzer öffentlicher Kommunikationsdienste über das Vertragsende hinaus vorsehen, ist ein **einheitlicher verfassungsrechtlicher Maßstab hinsichtlich sämtlicher zu speichernder Daten** anzulegen.[6] Die einfachgesetzliche Unterscheidung von Bestands- und Verkehrsdaten ist verfassungsrechtlich insoweit nicht von Bedeutung.

Folgt man bei der verfassungsrechtlichen Würdigung des Bundesverfassungsgerichts mit Urteil vom 2. März 2010, so ergibt sich daraus die Nichtigkeit der §§ 95 Abs. 3, 111 Abs. 4 TKG. Die Sicherheit der anlasslos vorzuhaltenden Kommunikationsdaten genügt nicht den verfassungsrechtlichen Anforderungen.[7] Der Verlust sämtlicher 17 Mio. Kundendaten von T-Mobile (jetzt: Telekom Deutschland) beispielsweise setzte Politiker, Funktionäre und andere exponierte Personen erheblichen Gefahren aus, weil ihre geheimen Privatanschriften Unbefugten in die Hände gelangt waren.[8] Die Daten gelangten auch an die Moderation der Comedy-Sendung „Schmidt & Pocher“ in der ARD, die dies zum Anlass nahm, den Fernsehmoderator Günther Jauch vor laufender Kamera unter dessen Privatnummer anzurufen und öffentlich vorzuführen.[9] Die §§ 95 Abs. 3, 111 Abs. 4 TKG sind zweitens verfassungswidrig, weil schon die von der EU beschlossene Mindestspeicherfrist von sechs Monaten dem Hohen Gericht zufolge an der Grenze des verfassungsrechtlich vertretbaren liege,[10] Kundendaten gemäß §§ 95 Abs. 3, 111 Abs. 4 TKG aber mindestens doppelt so lange aufzubewahren sind (1-2 Jahre).

Unserer Überzeugung nach ergibt sich die Nichtigkeit der §§ 95 Abs. 3, 111 Abs. 4 TKG bereits daraus, dass das **Prinzip einer anlasslosen, flächendeckenden Vorratsdatenspeicherung** - unabhängig von ihrer Ausgestaltung - das Gebot der Verhältnismäßigkeit verletzt. Die mit Urteil vom 2. März vertretene gegenteilige Auffassung des Hohen Gerichts kann nicht überzeugen. Dem Urteil fehlt eine Auseinandersetzung mit den empirischen Nachweisen des eklatanten Missverhältnisses zwischen Tragweite der Vorratsdatenspeicherung auf der einen und ihrem Ertrag auf der anderen Seite. Auch fehlt eine Auseinandersetzung mit den Belegen für die ebenso hohe Aufklärungsrate ohne Vorratsdatenspeicherung. Das Urteil setzt sich ferner nicht mit der Europäischen Menschenrechtskonvention und der diesbezüglichen Rechtsprechung des EGMR[11] und des Verfassungsgerichtshofs Rumäniens[12] auseinander, obwohl das Bundesverfassungsgericht im Fall konventionsverletzender Gesetze zur Abhilfe verpflichtet ist (Art. 13 EMRK) und das Grundgesetz nach Möglichkeit konventionskonform auszulegen ist.[13] Dem Urteil fehlt auch eine Auseinandersetzung mit der früheren Rechtsprechung des Bundesverfassungsgerichts, mit welcher eine allumfassende, permanente Vorratsdatenspeicherung nicht in Einklang zu bringen ist.[14]

---

[6] Näher Schriftsatz vom 05.05.2009.

[7] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 221 ff.

[8] Spiegel vom 04.10.2008, http://www.spiegel.de/wirtschaft/0,1518,581938,00.html.

[9] Sendung Nr. 22 vom 9. Oktober 2008, http://www.schmidt-news.com/showguide_schmidt-pocher2008.php.

[10] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 215.

[11] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, NJOZ 2010, 696.

[12] Verfassungsgerichtshofs Rumäniens, 1258 vom 08.10.2009, http://www.vorratsdatenspeicherung.de/content/view/342/79/lang,de/.

[13] BVerfG, 2 BvR 1481/04 vom 14.10.2004, Absatz-Nr. 32.

[14] Näher Schriftsatz vom 13.08.2008 im Verfahren 1 BvR 256/08, http://www.vorratsdatenspeicherung.de/images/schriftsatz_2008-08-13.pdf, 33.

Wenn das Bundesverfassungsgericht dabei bleibt, dass eine Vorratsdatenspeicherung deshalb verhältnismäßig sei, weil der Staat ihre Durchführung **Privatunternehmen** übertrage,[15] dann könnte der Staat auch in anderen Fällen die bisher geltenden verfassungsrechtlichen Grenzen durch Outsourcing sprengen. Die engen Voraussetzungen, die das Hohe Gericht etwa für Rasterfahndung oder Kfz-Massenabgleich aufgestellt hat,[16] wären nicht mehr bindend, wenn der Staat Private mit der Durchführung betraute. Es ist offensichtlich, dass dies nicht richtig sein kann. Es führte zu einer massiven Absenkung der rechtstaatlichen Anforderungen an die staatliche Datenverarbeitung, insbesondere im sensiblen Bereich der präventiven und repressiven Ermittlungstätigkeit staatlicher Behörden. Die Betrauung Privater kann eine Vorratsdatenspeicherung daher nicht rechtfertigen. Dass das Urteil für andere Vorhaben „größere Zurückhaltung" fordert,[17] ist zu unbestimmt als dass es ein Übergreifen des Prinzips einer permanenten, flächendeckenden Datensammlung ins Blaue hinein auf immer weitere Lebensbereiche verhindern könnte.

Das Bundesverfassungsgericht argumentiert weiter, die Telekommunikation weise ein **spezifisches Gefahrenpotential** auf. Sie erleichtere die Begehung klassischer Straftaten und habe neue Formen von Straftaten hervor gebracht, deren Begehung sich „weithin der Beobachtung" entziehe. Eine Rekonstruktion gerade der Telekommunikationsverbindungen sei daher für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung.[18] All dies als richtig unterstellt, rechtfertigt es gleichwohl nicht eine generelle und undifferenzierte, globale und pauschale Erfassung von Informationen über jegliche Telekommunikation der gesamten Bevölkerung. Spezifischen Gefahren und damit einher gehend einem besonderen Aufklärungsinteresse kann nämlich schon ohne Vorratsdatenspeicherung Rechnung getragen werden. Auch ohne Vorratsdatenspeicherung waren ausweislich einer repräsentativen Aktenanalyse des Max-Planck-Instituts 96% aller Auskunftersuchen nach § 100g StPO erfolgreich.[19] Zudem ist die Rekonstruktion und Überwachung der Telekommunikation technikbedingt ohnehin sehr viel leichter, geheimer und kostengünstiger zu bewerkstelligen als die Rekonstruktion und Überwachung unmittelbarer oder postalischer Kommunikation. Dementsprechend liegt die polizeiliche Aufklärungsquote im Bereich der Straftaten mit Tatmittel Internet daher seit jeher bei etwa 80% der bekannt gewordenen Internetkriminalität (2005: 84,9%, 2006: 84%, 2007: 82,9%, 2008: 79,8%, 2009 [Nordrhein-Westfalen]: 77,3%) und übersteigt damit deutlich die durchschnittliche Aufklärungsquote von Straftaten (2008: 54,8%). Sind Telekommunikationsverbindungen schon ohne Vorratsdatenspeicherung überdurchschnittlich häufig rekonstruierbar, können die Eigenarten der Telekommunikation nicht auch noch eine verdachtslose Vorratsdatenspeicherung rechtfertigen. Die Vorratsdatenspeicherung hat die Aufklärungsrate im Übrigen nicht weiter gesteigert.

Das Bundesverfassungsgericht argumentiert weiter, **hinsichtlich der Telekommunikationsdaten existiere mangels öffentlicher Wahrnehmbarkeit kein gesellschaftliches Gedächtnis**, das es wie in anderen Bereichen erlaubte, zurückliegende Vorgänge auf der Grundlage zufälliger Erinnerung zu rekonstruieren.[20] Demgegenüber ist bereits umfassend ausgeführt worden, weshalb dieser Unterschied teils nicht besteht und andernteils keine Identifizierungspflicht rechtfertigt.[21] Zur Vermeidung von Wiederholungen wird auf diese Ausführungen Bezug genommen. Auch ohne Identifizierungspflicht sind telekommunizierende Straftäter leichter zu

---

[15] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 214.

[16] BVerfGE 115, 320; BVerfGE 120, 378.

[17] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 218.

[18] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 216.

[19] MPI-Forschungsbericht, 253.

[20] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 217.

[21] Schriftsatz vom 05.05.2009, 8 f. und 15.

identifizieren als anders kommunizierende Straftäter, was die weit überdurchschnittliche Aufklärungsquote bei Straftaten mit Tatmittel Internet belegt.

Die Vorratsdatenspeicherung ist schließlich damit gerechtfertigt worden, dass die Verbreitung bestimmter **Vertragsgestaltungen** der Telekommunikationsdiensteanbieter die Verfügbarkeit von Daten reduziere.[22] Die verfassungsrechtliche Würdigung einer Vorratsdatenspeicherung im Telekommunikationsbereich kann sich indes nicht an überkommenen Vertragsgestaltungen der Telekommunikationsdiensteanbieter orientieren, sondern nur an nicht elektronisch vermittelter Kommunikation, bei der keinerlei Erfassung menschlicher Kontakte oder Identitäten bei einem Kommunikationsmittler erfolgt.

1.1.2.3.2 Vorratsspeicherung sonstiger Bestandsdaten

Soweit die §§ 95 Abs. 3, 111 Abs. 4 TKG über die europarechtlich vorgesehene Vorratsspeicherung von Name, Anschrift und Anschlusskennung der Nutzer öffentlicher Kommunikationsdienste hinaus gehen, ist auch auf der Grundlage des Urteils vom 2. März eine **andere Beurteilung als im Fall des § 113a TKG** vorzunehmen. Das Hohe Gericht hat ausdrücklich erklärt, dass die Beurteilung der grundsätzlichen Zulässigkeit der Vorratsspeicherung von Verkehrsdaten nicht auf andere Datensammlungen übertragen werden dürfe[23] und hat auch seine verfassungsrechtliche Zulassung einer Vorratsdatenspeicherung weitgehend auf die EU-Vorgaben beschränkt. Es heißt in dem Urteil wörtlich: „*Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt vielmehr voraus, dass diese eine Ausnahme bleibt.*“[24]

Die hier angefochtenen §§ 95 Abs. 3, 111 Abs. 4 TKG betreffen nun **keine „Telekommunikationsverkehrsdaten“**. Das Bundesverfassungsgericht setzte sich zu seiner eigenen Rechtsprechung in Widerspruch, würde es eine Vorratsdatenspeicherung nun auch für Kunden-Bestandsdaten für verhältnismäßig erachten, die keine Telekommunikationsverkehrsdaten darstellen und deren Aufbewahrung auch sonst nicht europarechtlich vorgegeben ist, z.B. Geburtsdatum, Anschrift des Anschlusses, Gerätenummer von Mobilfunkgeräten, Datum des Vertragsbeginns, Bankverbindung, Kundennummer, Passwort, elektronischem Telefonbuch und Kurzwahlnummern. Sollte das Bundesverfassungsgericht die Pflicht zur Vorratsspeicherung aller Bestandsdaten gleichwohl für zulässig erachten, so zeigte sich, dass die postulierte Beschränkung der Zulässigkeit einer Vorratsdatenspeicherung auf „Telekommunikationsverkehrsdaten“ keinen Bestand hat und das Prinzip einer prophylaktischen Datenanhäufung immer weiter ausgeweitet werden wird.

1.2 Verletzung des Artikels 3 GG

In der **Beschwerdeschrift** ist ausgeführt worden, weshalb die §§ 95 Abs. 3, 111 Abs. 4 TKG gegen Art. 3 GG verstoßen. Diese Ausführungen bleiben richtig. Das Urteil vom 2. März behandelt Art. 3 GG nicht und musste dies auch nicht, weil die dort angefochtenen Vorschriften bereits aus anderem Grund nichtig waren. Sollte das Hohe Gericht die §§ 95 Abs. 3, 111 Abs. 4 TKG nicht schon wegen Verletzung von Art. 10 GG für nichtig erklären, bleibt die Unvereinbarkeit mit Art. 3 GG.

---

[22] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 217.

[23] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 218.

[24] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 218.

2 § 111 Abs. 1 S. 1 und Abs. 2 S. 1 TKG (Identifizierungszwang)

2.1 Verletzung des Artikels 10 GG

§ 111 Abs. 1 S. 1 und Abs. 2 S. 1 TKG verpflichten Telekommunikationsanbieter zur Identifizierung von Anschlussinhabern, selbst wenn dies betrieblich nicht erforderlich ist. Die Vorschriften **verbieten dadurch die anonyme Überlassung** von Telekommunikationsanschlüssen.

Dieser Zwang zur Erhebung betrieblich nicht erforderlicher Informationen über Fernmeldeteilnehmer greift in deren Grundrecht aus **Art. 10 GG** ein.[25] Mit Schriftsatz vom 07.05.2009 ist ausgeführt worden, dass statische Anschlusskennungen wie Rufnummern einfachgesetzlich als Verkehrsdaten einzuordnen sind,[26] dass unabhängig hiervon aber auch als Bestandsdaten einzuordnende Telekommunikationsdaten in den Schutzbereich des Art. 10 GG fallen.[27]

Der in § 111 Abs. 1 S. 1 und Abs. 2 S. 1 TKG liegende Grundrechtseingriff ist **nicht gerechtfertigt**: Der Gesetzesvorbehalt des Art. 10 Abs. 2 GG ist überschritten.[28] Das Zitiergebot ist verletzt.[29] Vor allem ist ein allgemeines Verbot der geschäftsmäßigen Überlassung anonymer Telekommunikationsanschlüsse unverhältnismäßig.[30] Es dient Allgemeininteressen kaum, setzt auf der anderen Seite aber ins Blaue hinein und ohne Anlass die gesamte Bevölkerung dem ständigen Risiko eines Missbrauchs oder Verlustes vertraulicher Daten sowie eines falschen Verdachts aufgrund der irrtumsanfälligen Telekommunikationsdaten aus und schreckt dadurch unzumutbar von freier Fernkommunikation ab, gerade wo einzelne Menschen oder die Allgemeinheit auf anonyme Informationen oder Beratung dringend angewiesen sind.[31]

Das **Urteil des Hohen Gerichts vom 2. März 2010** ändert nichts an dem Umstand, dass ein genereller und unterschiedsloser Identifizierungszwang für sämtliche Inhaber von Telekommunikationsanschlüssen das Verhältnismäßigkeitsgebot verletzt. Das Urteil behandelt die Zulässigkeit einer Identifizierungspflicht nicht, sondern setzt sich nur mit der Zulässigkeit einer Aufbewahrungspflicht für betrieblich ohnehin anfallende Daten (vgl. § 113a Abs. 1 S. 1 TKG a.F.) sowie einer Auskunftspflicht auseinander. Ob ohnehin vorhandene Daten unter bestimmten Voraussetzungen gespeichert oder beauskunftet werden müssen oder ob die anonyme Überlassung von Anschlüssen allgemein verboten wird, stellt einen grundlegenden Unterschied dar.

Soweit das Urteil zu § 113 TKG ausführt, der **Erkenntniswert von Bestandsdatenauskünften** bleibe punktuell und systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen ließen sich allein auf Grundlage solcher Auskünfte nicht verwirklichen,[32] droht die Funktion von Identitätsdaten als Schlüssel zu weiteren Kommunikationsdaten aus dem Blick zu geraten: Bei den Diensten Telefonie, E-Mail und Internet können Kommunikationspartner weithin das Kommunikations- und Internetnutzungsverhalten des Grundrechtsträgers anhand dessen Anschlusskennung, E-Mail-Adresse oder IP-Adresse aufzeichnen und nachvollziehen. Werden solche Aufzeichnungen (z.B. Liste eingehender Anrufe, eingegangene E-Mails, Internetnutzungs-Logfiles) dem Staat zur Verfügung gestellt, so bleibt der Erkenntniswert einer Auskunft des Kommunikationsmittlers über die Identität des

---

[25] Schriftsatz vom 07.05.2009, 40.

[26] Schriftsatz vom 07.05.2009, 6 und 29.

[27] Schriftsatz vom 07.05.2009, 1 ff.

[28] Beschwerdeschrift, 52.

[29] Beschwerdeschrift, 52.

[30] Beschwerdeschrift, 52 ff.

[31] Näher Schriftsatz vom 07.05.2009, 6 ff.

[32] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 256.

Anschlussinhabers keineswegs punktuell, sondern ermöglicht erst die personenbezogene, systematische Ausforschung des Kommunikations- und Informationsverhaltens eines Menschen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen. Das Bundesverfassungsgericht hat schon früh den zutreffenden Maßstab zur Bestimmung der Eingriffstiefe informationeller Maßnahmen herausgearbeitet: „*Dabei kann nicht allein auf die Art der Angaben abgestellt werden. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen*“.[33] Wenn der Gesetzgeber Kommunikationsmittler zur Identifikation ihrer Kunden zwingen will, so tut er dies gerade, um Information zur personenbezogenen Rekonstruktion von Inhalt und Umständen der Telekommunikation nutzen (lassen) zu können.

Soweit das Urteil vom 2. März 2010 ausführt, Bestandsdatenauskünfte hätten ein erheblich **weniger belastendes Gewicht** als die nahezu vollständige Speicherung der Daten sämtlicher Telekommunikationsverbindungen,[34] trifft dies jedenfalls auf einen allgemeinen Identifizierungszwang nicht zu. Solange eine anonyme Telekommunikation möglich ist (wie es die EG-Richtlinie 2006/24 zur Vorratsdatenspeicherung ausweislich ihres Art. 5 Abs. 1 Buchst. e Ziff. 2.vi voraus setzt), ist eine Verkehrsdatenspeicherung weitaus weniger belastend, weil man eine – eventuell missbräuchliche – Zuordnung und personenbezogene Auswertung gespeicherter Verkehrsdaten wenigstens noch mithilfe anonymer Kommunikation einigermaßen vermeiden kann. Die Identität der Kommunikationsteilnehmer und der Inhaber der genutzten Telekommunikationsanschlüsse ist integraler Bestandteil der Telekommunikation und nicht weniger schutzwürdig als diese selbst.[35]

In dem Urteil vom 2. März 2010 heißt es weiter, im Bereich des Internets bestehe wegen der zunehmenden Nutzung desselben – auch für Rechtsverletzungen – ein gesteigertes Interesse an der Möglichkeit, Kommunikationsverbindungen im Internet den jeweiligen Akteuren zuordnen zu können. In einem Rechtsstaat **dürfe das Internet keinen rechtsfreien Raum** bilden.[36] Dass das Internet auch ohne Identifizierungszwang weit von einem rechtsfreien Raum entfernt ist, ergibt sich indes bereits daraus, dass 21 der 27 EU-Mitgliedsstaaten keinen Identifizierungszwang für Inhaber von Telekommunikationsanschlüssen kennen[37] und man nicht ernsthaft behaupten kann, dass in diesen Nachbarstaaten das Internet ein rechtsfreier Raum wäre. Gleiches gilt für die deutsche Rechtsordnung bis 2004. Es ist nicht einmal belegt, dass ein Identifizierungszwang überhaupt eine statistisch nachweisbare Auswirkung auf Aufklärungsquote oder gar Kriminalitätsrate hätte.

Anders als bei der Vorratsdatenspeicherung kann ein **Konflikt mit Europarecht** die verfassungsrechtliche Beurteilung des allgemeinen Identifizierungszwangs gemäß § 111 Abs. 1 S. 1 und Abs. 2 S. 1 TKG nicht trüben, weil das Europarecht einen Identifizierungszwang nicht vorsieht.

Die Erwägung zur Verkehrsdatenspeicherung, dass elektronische Kommunikationsspuren **besonders flüchtig** seien, ist auf einen generellen Identifizierungszwang nicht übertragbar. Hier geht es gerade nicht darum, die Löschung flüchtiger Datenspuren zu verhindern, sondern

---

[33] BVerfGE 65, 1 (45).

[34] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 257.

[35] Schriftsatz vom 07.05.2009, 30.

[36] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 260.

[37] Europäische Kommission, Room Document,
http://www.vorratsdatenspeicherung.de/images/RoomDocumentEvaluationDirective200624EC.pdf, 11.

zusätzliche Informationen überhaupt erst zu gewinnen. Eine „Vorratsdatengewinnung“ weist gegenüber einer bloßen Aufbewahrung vorhandener Informationen eine neue Qualität auf: Mit § 111 Abs. 1 S. 1 und Abs. 2 S. 1 TKG will der deutsche Gesetzgeber die Kommunikationsvermittlung erstmals zur Gewinnung zusätzlicher Informationen instrumentalisieren.

Nach dem Willen des Bundesverfassungsgerichts soll seine **Entscheidung zur Vorratsspeicherung von Verkehrsdaten auf andere Datensammlungen nicht übertragen** werden. Die Verkehrsdatenspeicherung soll eine „Ausnahme“ bleiben.[38] Dann aber kann das Urteil vom 2. März nicht zur Rechtfertigung eines Zwangs zur Vorratserhebung anderer Daten dienen. Ob es dem Bundesverfassungsgericht gelingt, zu verhindern, dass schrittweise alle für die Strafverfolgung oder Gefahrenprävention nützliche Daten vorsorglich erfasst werden,[39] wird die Beurteilung des Identifikationszwangs des § 111 TKG zeigen.

Noch stärker als bei einer „Vorratsdatenspeicherung“ wohnte der verfassungsgerichtlichen Zulassung einer **„Vorratsdatengewinnung“** die Gefahr inne, dass sie auf immer weitere Lebensbereiche übergreift. Würde der Identifizierungszwang für Inhaber von Telekommunikationsanschlüssen mit der heutigen Bedeutung der Telekommunikation gerechtfertigt, so würde schon bald die heutige Bedeutung des Reiseverkehrs, des elektronischen Geschäftsverkehrs oder sonstigen Alltagsverhaltens herangezogen, um die Identifizierung der gesamten Bevölkerung bei alltäglichen Verrichtungen zu erzwingen. Auf diese Weise entstünde eine grundlegend andere als die freiheitliche Gesellschaft, die den Müttern und Vätern des Grundgesetzes vor Augen stand.[40]

Gerade weil das Bundesverfassungsgericht eine totale **Verkehrsdatenaufbewahrung** zugelassen hat, muss es die schädlichen Auswirkungen einer allgemeinen Verkehrsdatenspeicherung auf die freie und unbefangene Kommunikation in Deutschland begrenzen, indem es die anonyme Telekommunikationsnutzung wieder ermöglicht. Eine allgemeine Verkehrsdatenspeicherung wäre gänzlich unerträglich, wenn den betroffenen, oftmals auf nicht rückverfolgbare Kommunikation angewiesenen Personen[41] auch noch die Möglichkeit genommen würde, sich durch Verwendung anonymer Kommunikationsanschlüsse zu schützen.

2.2 Verletzung des Artikels 3 GG

In der **Beschwerdeschrift** ist ausgeführt worden, weshalb der Identifizierungszwang des § 111 TKG auch gegen Art. 3 GG verstößt.[42] Die dortigen Ausführungen bleiben zutreffend.

2.3 Verletzung des Artikels 5 GG

Mit **Schriftsatz vom 07.05.2009** ist ausgeführt worden, weshalb der Identifizierungszwang des § 111 TKG gegen das Grundrecht auf freie Meinungsäußerung (Art. 5 GG) verstößt.[43]

Den dortigen Ausführungen ist hinzuzufügen, dass der **Bundesgerichtshof** inzwischen anerkannt hat, dass Art. 5 GG das Recht auf anonyme Meinungsäußerung im Internet schützt.[44] § 111 TKG greift in dieses Recht ein, weil er die Überlassung anonymer Internetanschlüsse und Mobilfunkanschlüsse, welche einen Internetzugang ermöglichen, verbietet.

---

[38] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 218.

[39] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 218.

[40] Vgl. BVerfGE 7, 198 (205); 33, 1 (10); 72, 105 (115).

[41] Näher Schriftsatz vom 07.05.2009, 11.

[42] Beschwerdeschrift, 56 ff.

[43] Schriftsatz vom 07.05.2009, 10 f.

[44] BGHZ 181, 328, Abs. 50 ff.

Mit Urteil vom 25.03.2010 hat zuletzt auch der **Oberste Gerichtshof Israels** entschieden, dass ein „Recht auf Anonymität“ besteht.[45] Unter Bezugnahme auf die Rechtsprechung des US-amerikanischen Supreme Court führt der Gerichtshof aus, dass Bestandteil des Rechts auf freie Meinungsäußerung auch das Recht auf anonyme Meinungsäußerung sei. Teilweise setze die Möglichkeit und Bereitschaft zur Äußerung einer Meinung voraus, dass dies anonym geschehen könne. Ursache könnten persönliche Gefühle wie Scham oder Mutlosigkeit sein, externer Druck oder die Besorgnis über Reaktionen der Außenwelt. Mitunter sei die Anonymität aber auch Bestandteil der zu äußernden Botschaft. Sie verhindere etwa, dass Annahmen über den Verfasser die geäußerte Meinung überlagern und verfälschen. Anonymität sei zugleich auch im Rahmen des Grundrechts auf Privatsphäre geschützt und ein wichtiger Bestandteil dieses Rechts. Anonymität gebe dem Betroffenen Kontrolle über Informationen über ihn. Im Bereich des Internets komme der Anonymität eine verstärkte Bedeutung zu. Das Internet ermögliche eine freie Meinungsäußerung in besonderem Maße. Auch im Rahmen des Rechts auf Privatsphäre komme der Anonymität im Internet besondere Bedeutung zu. Bei der Internetnutzung fielen – zum Teil unfreiwillig – Informationen über das Nutzungsverhalten an. Im Laufe der Zeit bildete sich so eine Datenbank mit persönlichen Daten, Meinungen und Interessen. Während früher alle Handlungen im Schutz der eigenen Wohnung vor Blicken von außen geschützt gewesen seien, könne im Zeitalter des Internets direkt und indirekt tief „in die Seele der Person eingedrungen“ werden. Diese Verletzung der Privatsphäre müsse „minimiert“ werden. Je größer die Möglichkeiten einer Auswertung des Nutzungsverhaltens, desto eher sei eine erhebliche Verhaltensänderung auf Seiten der Nutzer zu erwarten.

Larios hat eine Übersicht über **US-amerikanische Rechtsprechung** zum Schutz der Anonymität von Internetnutzern durch das Grundrecht auf freie Meinungsäußerung veröffentlicht.[46]

3 § 112 TKG (Automatisierter Bestandsdatenzugriff)

Zu § 112 TKG ist die Bemerkung voranzustellen, dass im Jahr 2009 die **Zahl der staatlichen Kenntnisnahmen** von Kommunikationsdaten nach § 112 TKG auf 4,5 Mio. und damit erneut stark angestiegen ist,[47] so dass nunmehr 1.000 zugriffsberechtigte Behörden täglich mindestens 12.000 Fernmeldeverhältnisse offen legen. Gegenüber 2001 hat sich die Zahl der staatlichen Kenntnisnahmen bereits verdreifacht, gegenüber früheren Jahren exponentiell gesteigert. Diese anhaltende Zugriffsexplosion lässt sich nicht durch veränderte Rahmenbedingungen erklären und verdeutlicht vielmehr, dass die Eingriffsvoraussetzungen des § 112 TKG mit dem verfassungsrechtlichen Stellenwert der Vertraulichkeit der Telekommunikation nicht in Einklang stehen.

3.1 Verletzung des Artikels 10 GG

3.1.1 Eingriff in den Schutzbereich

Mit **Schriftsatz vom 05.05.2009** ist umfassend dargelegt worden, weshalb der staatliche Zugriff auf Kundendaten, über die ein Kommunikationsmittler zur Vermittlung und Abrechnung von Telekommunikation verfügt, in das Fernmeldegeheimnis des betroffenen Kunden eingreift.[48] Das Urteil des Hohen Gerichts vom 2. März 2010 lässt die Richtigkeit dieser Ausführungen unberührt.

Nach ausführlicher Diskussion und mit vielen Nachweisen kommt **nun auch Welp** zu dem Ergebnis, dass ein Eingriff in das Fernmeldegeheimnis vorliegt, wenn Bestandsdaten erhoben werden, um die Identität der an einem konkreten Telekommunikationsvorgang Beteiligten zu

---

[45] Oberster Gerichtshof Israels, 4447/07 vom 25.03.2010, http://elyon1.court.gov.il/files/07/470/044/p10/07044470.p10.htm, Absatz-Nr. 11.

[46] Larios, Rutgers Law Record, Vol. 37, p. 36, 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1640133.

[47] Bundesnetzagentur, Jahresbericht 2009, 127 f.

[48] Schriftsatz vom 05.05.2009, 20 ff.

ermitteln. Da aber der Kommunikationsmittler nicht wissen könne, welchem Zweck ein Auskunftsersuchen diene, sei die Offenbarung der Identität des Inhabers einer (auch statischen) Telekommunikationskennung stets als Eingriff in Art. 10 GG zu bewerten.[49]

3.1.2 Mangelnde Rechtfertigung

Der in § 112 TKG liegende Grundrechtseingriff ist nicht gerechtfertigt.

3.1.2.1 Verletzung des Zitiergebots

§ 112 TKG verletzt das Zitiergebot des Art. 19 Abs. 1 S. 2 GG, weil er das eingeschränkte Grundrecht (Art. 10 GG) nicht nennt. Der Gesetzgeber hat den Eingriff in das Fernmeldegeheimnis verkannt.

3.1.2.2 Verletzung des Verhältnismäßigkeitsgebots

3.1.2.2.1 Einheitlicher Schutz des Fernmeldegeheimnisses

§ 112 TKG verletzt vor allem das Verhältnismäßigkeitsgebot. Wie bereits umfassend ausgeführt, sind die näheren Umstände eines Fernmelde-Vertragsverhältnisses integraler Bestandteil der in diesem Rahmen vermittelten Telekommunikation. Insbesondere die Information, wer unter welcher Kennung kommuniziert (hat), ist der Schlüssel zur Vertraulichkeit der Telekommunikation auch im Verhältnis zum Kommunikationspartner und ist **nicht typischerweise weniger schutzwürdig als Inhalt und Umstände** der einzelnen Kommunikationsvorgänge selbst.[50] Deswegen muss die Aufdeckung der Identität eines Kommunikationsteilnehmers oder der Kennung, unter welcher eine Person kommuniziert, denselben Voraussetzungen unterworfen werden wie sonstige Eingriffe in das Fernmeldegeheimnis (etwa § 100a StPO). Dass Identifikations- und Verbindungsdaten eine vergleichbare Sensibilität aufweisen, hat der Gesetzgeber inzwischen mit der Regelung zur Meldepflicht von Datenpannen in § 93 Abs. 3 TKG anerkannt. Der Verlust von Bestands- und Verkehrsdaten begründet danach gleichermaßen eine Informationspflicht. Die Begründung des Gesetzentwurfs zu § 93 Abs. 3 TKG führt dazu aus, die Meldepflicht beziehe sich „auf besonders sensible personenbezogene Daten“[51], wozu der Gesetzgeber Bestands- und Verkehrsdaten gleichermaßen zählt.

§ 112 TKG genügt den **Anforderungen des Verhältnismäßigkeitsgebots** danach nicht:

Erstens beschränkt er die Durchbrechung des Fernmeldegeheimnisses nicht auf die **Aufklärung schwerer Straftaten**[52] und die Abwehr von Gefahren für wichtige Rechtsgüter[53]. Er legt nicht einmal fest, zu welchen konkreten, klar definierten Zwecken Kenntnisnahmen überhaupt zugelassen werden sollen.[54]

Zweitens beschränkt § 112 TKG die Datenerhebung nicht auf **Beschuldigte/Störer** oder solche Personen, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für einen Beschuldigten/Störer bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte/Störer ihren Anschluss benutzt (vgl. § 100a StPO).

---

[49] Welp, Die Auskunftspflicht von Access-Providern nach dem Urheberrechtsgesetz (2009), 241 ff.

[50] Näher Schriftsatz vom 05.05.2009, 20 ff.

[51] Bundesregierung, BT-Drs. 16/12011, 34.

[52] Vgl. BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 228.

[53] Vgl. BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 231.

[54] Beschwerdeschrift, 80.

Drittens versäumt es § 112 TKG, eine richterliche Prüfung zur Voraussetzung für den Zugriff zu machen.[55] Weil alle Informationen über Fernmeldeverhältnisse vergleichbar schutzwürdig sind, überzeugt die nach der Art der Daten unterscheidende Auffassung des Bundesverfassungsgerichts zum Richtervorbehalt[56] nicht. Jedenfalls der durch § 112 TKG eröffnete **direkte staatliche Zugriff** auf ein Verzeichnis sämtlicher Anschlussinhaber Deutschlands begünstigt die jährlich millionenfache Aufhebung der Anonymität von Fernmeldeverhältnissen und genügt dem Verhältnismäßigkeitsgebot nicht. Mit Urteil vom 2. März hat das Bundesverfassungsgericht betont, dass der Prüfung und Bearbeitung von Auskunftsersuchen durch den Telekommunikationsmittler als einzigem Garant des Fernmeldegeheimnisses in diesem Verfahrensstadium eine zentrale Bedeutung zukomme. Deswegen sei „durch entsprechende Regelungen und technische Vorkehrungen sicherzustellen", dass staatliche Stellen „keinen direkten Zugriff auf die Daten" haben.[57] Die Daten dürften dem Staat „unmittelbar als Gesamtheit nicht zur Verfügung" stehen – eben dies ist aber die Folge des § 112 TKG. Auch zur Gewährleistung eines effektiven Rechtsschutzes und adäquater Sanktionen gehört es dem Bundesverfassungsgericht zufolge, „dass die Daten aufgrund der Anordnung von den Telekommunikationsunternehmen als speicherungsverpflichteten Dritten herausgefiltert und übermittelt werden, das heißt den Behörden also nicht ein Direktzugriff auf die Daten eröffnet wird. Auf diese Weise wird die Verwendung der Daten auf das Zusammenwirken verschiedener Akteure verwiesen und damit in sich gegenseitig kontrollierende Entscheidungsstrukturen eingebunden."[58] Selbst eine richterliche Anordnung ermächtige die Behörden nicht zu einem Direktzugriff auf die Daten.[59] Wenngleich sich diese Ausführungen des Hohen Gerichts unmittelbar nur auf anlasslos gespeicherte Verkehrsdaten bezogen haben, müssen sie für anlasslos gespeicherte oder sogar anlasslos erhobene Identifizierungsdaten nach § 111 TKG ebenso gelten. Insoweit steht die grundrechtlich geschützte Anonymität der Telekommunikation auf dem Spiel. Für den Fall, dass das Bundesverfassungsgericht einen Richtervorbehalt für Auskünfte nach § 112 TKG nicht anerkennen sollte, kommt einer manuellen Prüfung und Erledigung von Auskunftsersuchen durch die Verpflichteten eine noch größere Bedeutung zu. Ohne vorherige richterliche Prüfung stellen die Kommunikationsmittler nämlich die einzige Stelle dar, die wenigstens offensichtlich rechtswidrige Auskunftsersuchen zurückweisen können. Das automatisierte Abrufverfahren nach § 112 TKG stellt eine effektive Vorabkontrolle demgegenüber nicht sicher und führt zu einer zunehmenden Ausuferung und Zweckausweitung des Zugriffsverfahrens. Dies trägt dem verfassungsrechtlichen Schutz des Fernmeldegeheimnisses nicht Rechnung. Ein manuelles Auskunftsverfahren sichert die Rechtmäßigkeit und Verhältnismäßigkeit von Durchbrechungen des Fernmeldegeheimnisses auch dadurch, dass manuelle Auskünfte einen Entschädigungsanspruch begründen (§ 23 Abs. 1 JVEG) und der Abfragende seinen Grundrechtseingriff dadurch in erhöhtem Maße rechtfertigen muss.

Viertens gewährleistet § 112 TKG nicht die verfassungsrechtlich gebotene **Zweckbindung** erlangter Informationen,[60] die Kennzeichnung erhobener Daten[61] und die Benachrichtigung der Betroffenen[62].

Mit **Urteil vom 2. März 2010** hat das Bundesverfassungsgericht die Auffassung vertreten, die staatliche Identifizierung von Internetnutzern unterliege geringeren verfassungsrechtlichen

---

55 Vgl. BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 247 ff.

56 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 289.

57 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 214.

58 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 250.

59 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 283.

60 Beschwerdeschrift, 80.

61 Beschwerdeschrift, 80; Schriftsatz vom 20.04.2007, 40; jetzt auch BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 236.

62 Beschwerdeschrift, 80.

Anforderungen als die Erhebung des Inhalts oder der sonstigen Umstände einzelner Kommunikationsvorgänge.[63] Die dazu vorgebrachten Argumente überzeugen indes nicht:

Das Bundesverfassungsgericht stellt darauf ab, der Erkenntniswert von Auskünften etwa über den Inhaber einer Rufnummer bleibe **punktuell**. Systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen ließen sich allein auf Grundlage solcher Auskünfte nicht verwirklichen.[64] Bei dieser Argumentation droht indes die Funktion der Zuordnung einer Rufnummer als Schlüssel zu einer näheren Ausforschung der Telekommunikation des Betroffenen aus dem Blick zu geraten. Die Identifizierung eines Anschlussinhabers gegenüber einer staatlichen Stelle gefährdet die Vertraulichkeit und Unbefangenheit des Fernmeldeverkehrs, weil sie die Anonymität und Vertraulichkeit der zur Fernkommunikation erforderlichen Anschlusskennung aufhebt und die Ausforschung der vergangenen oder zukünftigen Fernkommunikation des Anschlussinhabers ermöglicht.[65] Bei den Diensten Telefon und E-Mail können Kommunikationspartner weithin das Kommunikations- und Internetnutzungsverhalten des Grundrechtsträgers anhand dessen Anschlusskennung oder E-Mail-Adresse aufzeichnen und nachvollziehen. Werden solche Aufzeichnungen (z.B. Liste eingehender Anrufe, eingegangene E-Mails) dem Staat zur Verfügung gestellt, so bleibt der Erkenntniswert einer Auskunft des Kommunikationsmittlers über die Identität des Anschlussinhabers keineswegs punktuell, sondern ermöglicht erst die personenbezogene, systematische Ausforschung des Kommunikations- und Informationsverhaltens eines Menschen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen. Das Bundesverfassungsgericht hat schon früh den zutreffenden Maßstab zur Bestimmung der Eingriffstiefe informationeller Maßnahmen herausgearbeitet: „*Dabei kann nicht allein auf die Art der Angaben abgestellt werden. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen*“.[66] Wenn der Gesetzgeber Kommunikationsmittler zur Identifikation ihrer Kunden zwingen will, so tut er dies gerade, um Information zur personenbezogenen Rekonstruktion von Inhalt und Umständen der Telekommunikation nutzen (lassen) zu können.

Soweit der Erkenntniswert einer Auskunft über den Inhaber einer Rufnummer punktuell bleiben und systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen für sich genommen nicht rechtfertigen mag, ist dies bei der **Erhebung eines belanglosen Verbindungsdatums** oder dem Abhören eines einzelnen Telefongesprächs mit einem Nachbarn nicht anders. Tatsächlich ist die Kenntnis der Identität eines Kommunikationsteilnehmers in der Regel sehr viel aussagekräftiger als der (genaue) Inhalt oder einzelne Umstände (z.B. Verbindungsdauer, Datenvolumen) einer Kommunikation zwischen Unbekannten. Die vergleichbare Schutzwürdigkeit von Verkehrs- und Bestandsdaten ist besonders einleuchtend, wenn mithilfe von § 112 TKG die Anonymität eines konkreten Fernmeldevorgangs aufgehoben wird. Da der Kommunikationsmittler, die Aufsichtsbehörde oder ein Gericht aber oft nicht erkennen können, welchem Zweck ein Auskunftsersuchen dient, müssen dieselben Maßstäbe für jede Auskunft darüber gelten, wer über welche Kennung kommuniziert. Dasselbe gilt für die sonst nach § 112 TKG möglichen Auskünfte. Die Vertragsdaten eines Kommunikationsmittlers ermöglichen erst Fernkommunikation und ihre Abrechnung. Weil nun der freien Kommunikation eine herausragende Bedeutung in unserer Gesellschaft zukommt,

---

[63] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 254.

[64] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 256.

[65] Näher Schriftsatz vom 05.05.2009, 27 ff.

[66] BVerfGE 65, 1 (45).

müssen Informationen bei Kommunikationsmittlern unabhängig von ihrem Inhalt gleichermaßen besonders geschützt werden.

3.1.2.2.2 Anwendung der Rechtsprechung zur Identifizierung von Internetnutzern

Selbst wenn man die **vom Bundesverfassungsgericht zur Identifizierung von Internetnutzern entwickelten Maßstäbe** akzeptieren und auf § 112 TKG übertragen wollte, änderte dies nichts an der Verletzung des Verhältnismäßigkeitsgebots:

Das Bundesverfassungsgericht hat identifizierende Auskünfte **nur für die Verfolgung von Straftaten**, für die Verfolgung auch im Einzelfall besonders gewichtiger und ausdrücklich zu benennender Ordnungswidrigkeiten, für die Gefahrenabwehr und die Aufgabenwahrnehmung der Nachrichtendienste auf der Grundlage der allgemeinen fachrechtlichen Eingriffsermächtigungen zugelassen.[67] § 112 Abs. 2 TKG geht hierüber sowohl hinsichtlich des Kreises der abrufberechtigten Stellen wie auch hinsichtlich der zugelassenen Erhebungszwecke („zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich“) weit hinaus.

§ 112 TKG versäumt es auch, sicherzustellen, dass Auskünfte nicht ins Blaue hinein eingeholt werden, sondern nur aufgrund eines **Anfangsverdachts** oder einer konkreten Gefahr auf einzelfallbezogener Tatsachenbasis.[68] Eine solche Anforderung kann der Norm selbst im Wege der Auslegung nicht entnommen werden. Auch das Fachrecht gewährleistet die Einhaltung dieser Eingriffsschwelle nicht: § 112 TKG bestimmt erstens nicht normenklar, dass Zugriffe nur nach Maßgabe fachgesetzlicher Ermächtigungen zulässig sein sollen. Zweitens sieht das Fachrecht vielfach selbst nicht die erforderliche Eingriffsschwelle vor (z.B. für Nachrichtendienste, Notrufabfragestellen, Finanzdienstleistungsaufsicht, Zollverwaltung).

§ 112 TKG stellt ferner – anders als etwa das österreichische Recht – nicht sicher, dass die rechtlichen und tatsächlichen Grundlagen entsprechender Abfragen **aktenkundig** gemacht werden, wie es verfassungsrechtlich geboten ist.[69]

§ 112 TKG versäumt es weiter, **Benachrichtigungspflichten** jedenfalls dann vorzusehen, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird oder sonst überwiegende Interessen Dritter oder des Betroffenen selbst entgegenstehen, wie es verfassungsrechtlich geboten ist.[70] § 112 TKG gewährleistet nicht, dass der Grund für ein Absehen von der erforderlichen Benachrichtigung aktenkundig gemacht wird.[71]

Dem Argument der Bundesregierung, die erforderliche datenschutzrechtliche Regelung der Datenverwendung sei eine Frage des „**Fachrechts**“ und lasse die Verfassungsmäßigkeit der telekommunikationsrechtlichen Öffnungsnorm unberührt, hat das Bundesverfassungsgericht mit Urteil vom 2. März 2010 eine Absage erteilt. Es hat entschieden, dass der Gesetzgeber zu informationellen Grundrechtseingriffen nur ermächtigen darf, wenn er gleichzeitig für die Wahrung der verfassungsrechtlichen Anforderungen Sorge trägt. Wörtlich heißt es in dem Urteil vom 2. März 2010:

> „*§ 113b Satz 1 Nr. 2 und 3 TKG genügt den Anforderungen an eine hinreichende Begrenzung der Verwendungszwecke schon seiner Anlage nach nicht. Der Bundesgesetzgeber begnügt sich hier damit, in lediglich generalisierender Weise die Aufgabenfelder zu umreißen, für die ein Datenabruf möglich sein soll, ohne konkret die*

[67] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261 f.
[68] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261.
[69] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261.
[70] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 263.
[71] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 263.

> *Verwendungszwecke zu benennen. Deren Konkretisierung überlässt er vielmehr späterer Gesetzgebung, insbesondere auch der Gesetzgebung durch die Länder. Damit kommt er seiner Verantwortung für die verfassungsrechtlich gebotene Begrenzung der Verwendungszwecke nicht nach. Wenn er die Speicherung der Telekommunikationsverkehrsdaten anordnet, obliegt es ihm zugleich, auch die für deren verfassungsrechtliche Rechtfertigung erforderlichen Verwendungszwecke und Eingriffsschwellen sowie die zur Gewährleistung der Zweckbindung erforderlichen Folgeregelungen verbindlich festzulegen. Solche Festlegungen enthält § 113b Halbsatz 1 TKG nicht. Vielmehr wird durch die Pflicht der Diensteanbieter zur vorsorglichen Speicherung aller Telekommunikationsverkehrsdaten und gleichzeitig die Freigabe dieser Daten für die Verwendung durch die Polizei und die Nachrichtendienste im Rahmen annähernd deren gesamter Aufgabenstellung ein für vielfältige und unbegrenzte Verwendungen offener Datenpool geschaffen, auf den – nur durch grobe Zielsetzungen beschränkt – jeweils aufgrund eigener Entscheidungen der Gesetzgeber in Bund und Ländern zugegriffen werden kann. Die Bereitstellung eines solchen seiner Zwecksetzung nach offenen Datenpools hebt den notwendigen Zusammenhang zwischen Speicherung und Speicherungszweck auf und ist mit der Verfassung nicht vereinbar (siehe oben C V 5 a).*“[72]

Nichts anderes kann **für § 112 TKG** gelten. Wenn der Gesetzgeber in § 111 TKG die Speicherung bestimmter Kommunikationsdaten anordnet, obliegt es ihm zugleich, die für deren verfassungsrechtliche Rechtfertigung erforderlichen Verwendungszwecke und Eingriffsschwellen sowie die zur Gewährleistung der Zweckbindung erforderlichen Folgeregelungen verbindlich festzulegen. Solche Festlegungen enthält § 112 TKG nicht.

§ 112 Abs. 2 TKG ist danach erstens verfassungswidrig, weil es der Gesetzgeber versäumt hat, konkret die **Verwendungszwecke** der Daten zu benennen. § 112 TKG umreißt nur in generalisierender Weise die Aufgabenfelder, für die ein Datenabruf möglich sein soll. Dass § 112 TKG die Weitergabe personenbezogener Daten an bestimmte Behörden pauschal „zur Erfüllung ihrer gesetzlichen Aufgaben“ erlaubt,[73] anstatt klar festzulegen, „um welche konkreten, klar definierten Zwecke es sich dabei handelt“, verstößt gegen das Gebot der Normenklarheit.[74] § 112 Abs. 2 TKG ist zweitens verfassungswidrig, weil der Gesetzgeber es versäumt hat, die verfassungsrechtlich gebotenen Eingriffsschwellen (z.B. konkreter Verdacht einer Straftat, Straftatenkatalog) dort festzuschreiben. Dies verstößt gegen das Verhältnismäßigkeitsgebot. § 112 Abs. 2 TKG ist drittens verfassungswidrig, weil es der Gesetzgeber versäumt hat, die zur Gewährleistung der Zweckbindung erforderlichen Folgeregelungen verbindlich festzulegen. § 112 TKG fehlt namentlich die verfassungsrechtlich gebotene[75] Anordnung, dass die Verwendung erlangter Daten nur zur Verfolgung derjenigen Zwecke zulässig ist, zu deren Erreichung die Daten nach dem Gesetz erhoben werden durften, und dass die Daten zu löschen sind, wenn sie zu diesen Zwecken nicht mehr benötigt werden (Zweckbindungsgebot).

Im Hinblick auf die grundrechtlichen Benachrichtigungspflichten und die gerichtliche Kontrolle lässt das Bundesverfassungsgericht eine **Ausgestaltung durch die Fachgesetze** und damit gegebenenfalls auch durch Landesgesetze genügen.[76] Eine Verletzung dieser verfassungsrechtlichen Anforderungen soll also nur zur Nichtigkeit der fachrechtlichen Zugriffsnorm führen, nicht aber der im Telekommunikationsgesetz eröffneten Zugriffsmöglichkeit.

---

[72] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 285.

[73] Vgl. BVerfGE 65, 1 (66 f.) zu einer vergleichbaren Formulierung.

[74] BVerfG a.a.O.

[75] BVerfGE 65, 1 (46).

[76] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 286.

Dies ist **unbefriedigend**. Genügen die verfahrensrechtlichen Sicherungen des Fachrechts den verfassungsrechtlichen Anforderungen an die Erhebung von Telekommunikations-Bestandsdaten nicht, sollen nach Auffassung des Bundesverfassungsgerichts die fachgesetzlichen Generalklauseln wie § 161 StPO oder § 21 BPolG verfassungswidrig sein, soweit danach Bestandsdaten nach dem Telekommunikationsgesetz erhoben werden dürfen.[77] Der Gesetzgeber hatte § 161 StPO oder § 21 BPolG bei deren Erlass indes nicht die Funktion zugedacht, eine Ermächtigungsgrundlage für den Zugriff auf Telekommunikationsdaten nach § 112 TKG zu bilden, zumal § 112 TKG bei Inkrafttreten der meisten fachgesetzlichen Generalklauseln noch nicht galt. Dementsprechend können die fachgesetzlichen Generalklauseln den für Eingriffe in den Fernmeldeverkehr geltenden verfassungsrechtlichen Anforderungen keine Rechnung tragen. Die Nichtigkeitsfolge ausschließlich für die Generalklauseln gewährleistet auch keinen effektiven Rechtsschutz: Mit Erlass des § 112 TKG konnte Verfassungsbeschwerde gegen die unzureichenden fachgesetzlichen Generalklauseln schon deswegen nicht erhoben werden, weil die diesbezügliche Frist des § 93 BVerfGG bereits abgelaufen war. Bei Erlass der fachgesetzlichen Generalklauseln aber konnte man noch nicht damit rechnen, dass sie in Zukunft einmal zum automatisierten Zugriff auf eine Datei sämtlicher Telekommunikationsteilnehmer ermächtigen würden. Bei einem solchen Verständnis entstünde eine Rechtsschutzlücke.

Die **Einhaltung der verfassungsrechtlich unverzichtbaren Verfahrensgarantien ist** daher nur dann effektiv zu gewährleisten, wenn das Telekommunikationsrecht eine fachgesetzliche Zugriffsnorm zur Voraussetzung einer grundrechtseingreifenden Datenübermittlung macht, welche neben das Telekommunikationsrecht treten, die erforderlichen Verfahrensgarantien vorsehen und auf die Erhebung von Telekommunikationsdaten abgestimmt sein muss. Das Telekommunikationsrecht muss dazu normenklar festlegen, dass es nicht eigenständig zu Datenübermittlungen ermächtigt, sondern nur eine datenschutzrechtliche Öffnungsnorm bildet. Ermächtigt das Telekommunikationsrecht selbst zu Datenübermittlungen, dann muss es auch selbst die verfassungsrechtlich gebotenen Verfahrensgarantien gewährleisten. Ferner darf sich das Telekommunikationsrecht nur solchen Fachrechtsnormen öffnen, die nach dem Willen des Gesetzgebers der Erhebung von Telekommunikationsdaten dienen sollten. Insofern ist ein einfachgesetzliches Zitiergebot zu fordern, wie es § 113b TKG vorgesehen hat. Nur das Erfordernis eines solchen Zitats stellt sicher, dass fachrechtliche Zugriffsnormen den für Telekommunikationsdaten geltenden, besonderen verfassungsrechtlichen Anforderungen Rechnung tragen.

Anders als der ehemalige § 113b TKG stellt § 112 Abs. 2 TKG **nicht nur eine datenschutzrechtliche Öffnungsnorm** dar, sondern soll nach dem Willen des Gesetzgebers eine eigenständige Zugriffsermächtigung bilden. Dieser Regelungsinhalt ist im Wege der grammatikalischen, systematischen und historischen Auslegung bereits ausführlich dargelegt worden.[78] Während § 113b TKG ausdrücklich forderte, eine Datenübermittlung müsse „in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf § 113a vorgesehen“ sein, stellt § 112 Abs. 2 TKG erkennbar eine abschließende Regelung dar. Es gibt auch keine zu § 112 TKG korrespondierenden fachgesetzlichen Erhebungsermächtigungen, etwa nicht für Notrufabfragestellen.

Aufgrund des eindeutigen Wortlauts des § 112 Abs. 2 TKG ist es auch **nicht möglich, die Norm verfassungskonform dahin auszulegen**, dass sie auf die jeweiligen fachgesetzlichen Eingriffsermächtigungen verweise.[79] Selbst wenn man die Norm entgegen der hier vertretenen

---

[77] Vgl. Ziff. 2 des Urteils des BVerfG, 1 BvR 256/08 vom 2.3.2010.

[78] Schriftsatz vom 20.04.2007, 34 ff.

[79] So BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 289 zu § 113 Abs. 1 TKG.

Auffassung insoweit für auslegungsfähig hielte, wäre eine solche Auslegung jedenfalls mit dem auch in Art. 8 EMRK verankerten Gebot der Normenklarheit unvereinbar. Dem § 112 Abs. 2 TKG kann weder der betroffene Bürger, noch die eingreifende Behörde, noch das kontrollierende Gericht entnehmen, dass Datenübermittlungen eine fachgesetzliche Ermächtigung der jeweiligen Stelle voraus setzten und nur in deren Rahmen zulässig seien.

Hat der Gesetzgeber mit § 112 Abs. 2 TKG danach eine abschließende Regelung der Datenübermittlung geschaffen, so ist der in der Norm liegende Grundrechtseingriff nur gerechtfertigt, wenn das Verfahren der Datenerhebung und -verwendung den grundrechtlichen Anforderungen entspricht. Wie bereits ausgeführt, ist dies im Hinblick auf den gebotenen **Richtervorbehalt**, auf die verfassungsrechtliche Benachrichtigungspflicht[80] und auf die verfassungsrechtliche Kennzeichnungspflicht[81] nicht der Fall. Selbst wenn man mit dem Bundesverfassungsgericht einen Richtervorbehalt nicht fordern wollte, so ist doch wenigstens eine Prüfung durch das Telekommunikationsunternehmen geboten und genügt ein unmittelbarer staatlicher Datenzugang wie in § 112 TKG vorgesehen den verfassungsrechtlichen Mindestanforderungen nicht.[82]

Nicht zuletzt ist zu bedenken, dass das Bundesverfassungsgericht unter den mit Urteil vom 2. März 2010 entwickelten Voraussetzungen nur die Identifizierung der „Anschlussinhaber bestimmter IP-Adressen“ zugelassen hat, namentlich mit dem Argument der **von Telekommunikation ausgehenden Gefahren**.[83] Die Identifizierung der Anschlussinhaber bestimmter Rufnummern oder E-Mail-Adressen ist mit der IP-Adresse zwar vergleichbar. § 112 TKG geht darüber aber weit hinaus und ermöglicht Grundrechtseingriffe, die mit Gefahren der Telekommunikation überhaupt nichts zu tun haben: § 112 TKG kann nach Art eines Telefonbuchs selbst für solche Recherchen verwendet werden, bei denen Anschlusskennungen oder Telekommunikation keine Rolle spielen. Beschränkt auf die Menge der Anschlussinhaber ermöglicht es § 112 TKG, die bei Telekommunikationsanbietern hinterlegte Anschrift oder das Geburtsdatum einer Person zu ermitteln oder umgekehrt die unter einer bestimmten Anschrift, in einer Straße oder in einer Ortschaft wohnhaften Personen zu ermitteln. Er ermöglicht es, sämtliche Personen eines Familiennamens in einem bestimmten Ort, in einer bestimmten Straße oder in einem bestimmten Postleitzahlbereich zu ermitteln. Er ermöglicht es, zu einem Namen alle Personen zu ermitteln, deren Name ähnlich klingt oder geschrieben wird („sprachwissenschaftliche Verfahren“). Wie die ausufernden Zugriffszahlen belegen, ist § 112 TKG letztlich zu einem Bevölkerungsregister ausgebaut worden, das bezüglich Datenmenge, Aktualität, Zugriffsberechtigungen und Suchfunktionen weit über die Melderegister hinaus geht, bezüglich des Datenschutzes dagegen weit hinter dem Melderecht zurück bleibt. Dieses Abrufverfahren lässt nicht nur den grundrechtlich gebotenen, besonderen Schutz der Vertraulichkeit von Fernmeldeverhältnissen vermissen. Es senkt die Vertraulichkeit von Fernmeldeverhältnissen sogar noch weit unter das Maß an Vertraulichkeit herab, das bei anderen Unternehmen gespeicherte Kundendaten genießen. Allgemein sind Kundendaten gegen den Willen des Unternehmens nämlich nur im Wege von Zwangsbefugnissen wie einer Durchsuchung mit richterlicher Anordnung zu erlangen. Undenkbar ist ein direkter Online-Zugriff ohne Wissen des Unternehmens und mit vielfältigen Suchfunktionen. Dementsprechend hat der Bundesdatenschutzbeauftragte ausgeführt: „*Ein Anspruch, in einem ‚vereinfachten Verfahren‘ über die telekommunikationsspezifischen Daten hinausgehende beliebige Kundendaten zu erhalten, den es in anderen Branchen der Privatwirtschaft nicht gibt, lässt sich auch für den TK-Bereich nicht rechtfertigen*“.[84]

---

[80] Beschwerdeschrift, 80; Schriftsatz vom 20.04.2007, 39.

[81] Beschwerdeschrift, 80; Schriftsatz vom 20.04.2007, 40.

[82] Näher Seite 11 ff. oben.

[83] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 260.

[84] Bundesbeauftragter für den Datenschutz, 17. Tätigkeitsbericht 1997–1998, 208 f.

Wo die Identifizierung eines Anschlussinhabers oder auch die Ermittlung einer Anschlusskennung zum Zwecke ihrer Überwachung erfolgen soll, mag man mit den besonderen Gefahren der Telekommunikation abgesenkte Eingriffsschwellen begründen, wie es das Bundesverfassungsgericht getan hat.[85] In anderen Fällen aber muss es dabei bleiben, dass das Fernmeldegeheimnis die Vertraulichkeit der Fernmeldebeziehung einschließlich der zur Abrechnung erforderlichen Kundendaten schützt. Will der Staat Personendaten nur **wie aus einem Telefonbuch**, aus dem Melderegister oder aus der Kundendatei eines beliebigen Unternehmens nutzen, so muss er sich auf das Telefonbuch, das Melderegister und andere Kundendateien beschränken. Das Fernmeldegeheimnis erlaubt Durchbrechungen nur, wo der Grund des staatlichen Zugriffswunschs einen inneren Zusammenhang mit der Telekommunikation aufweist. Der Telekommunikation eigen ist nur die Verwendung von Anschlusskennungen, nicht allgemein die Angabe von Personendaten.

§ 112 TKG ist folglich auch auf der Grundlage der Ausführungen des Bundesverfassungsgerichts verfassungswidrig, weil er die Aufhebung der Vertraulichkeit von Fernmeldeverhältnissen nicht auf Fälle beschränkt, in denen anhand einer **vollständig bekannten Anschlusskennung** der Anschlussinhaber oder anhand vollständig bekannter Personendaten die Kennung der auf die Person registrierten Anschlüsse zum Zwecke ihrer Überwachung ermittelt werden sollen. In Anlehnung an § 100b StPO könnte bestimmt werden: „*In der Anordnung sind anzugeben 1. der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet, oder 2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes. Auf Grund einer Anordnung nach Ziff. 1 hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) die zur Person des Betroffenen gespeicherten Anschlusskennungen mitzuteilen. Auf Grund einer Anordnung nach Ziff. 2 sind der gespeicherte Name und die gespeicherte Anschrift des Inhabers der Kennung mitzuteilen.*“

3.1.2.2.3 Vergleichbarkeit der Identifizierung von Internetnutzern

Die vom Bundesverfassungsgericht entwickelten Anforderungen an die Identifizierung von Internetnutzern[86] dürfen im Fall des § 112 TKG **keinesfalls noch unterschritten** werden.

Eine Abweichung rechtfertigt nicht, dass die Ausführungen des Bundesverfassungsgerichts zu § 113 TKG im Zusammenhang mit der **mittelbaren Nutzung anlasslos und flächendeckend erhobener Verkehrsdaten** erfolgt sind. Auf diesen Umstand hat das Bundesverfassungsgericht bei Darstellung der für § 113 TKG maßgeblichen verfassungsrechtlichen Eingriffsgrenzen nicht abgestellt. Es hat umgekehrt Literatur zitiert, welche die Beauskunftung nicht auf Vorrat gespeicherter Daten behandelt.[87] Auch bei der Bestimmung der Eingriffstiefe hat das Gericht auf die Verwendungsmöglichkeiten der Daten abgestellt und nicht darauf, wie sie erhoben worden sind.[88] Ohnehin sind die Eingriffsgrenzen mit Urteil vom 2. März 2010 so weit gezogen worden, dass sie nicht zumutbar noch einmal abgesenkt werden können.

Eine Abweichung rechtfertigt auch nicht, dass die Ausführungen des Bundesverfassungsgerichts eine Identifizierung unter **interner Verwendung von Verkehrsdaten** betreffen, während § 112 TKG eine Identifizerung anhand einer Kundendatei betrifft. Das Bundesverfassungsgericht hat ausgeführt, dass die interne Auswertung von Verkehrsdaten für die verfassungsrechtliche Beurteilung ohne Bedeutung sei. Die Behörden erhielten selbst keine Kenntnis der ausgewerteten

---

[85] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 260.

[86] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261 ff.

[87] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261.

[88] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 258 f.

Verkehrsdaten. Die Verwendung der Verkehrsdaten führe allein zu der Auskunft, welcher Anschlussinhaber unter einer bereits bekannten Kennung im Internet angemeldet war. Eine solche Auskunft habe ihrer formalen Struktur nach eine gewisse Ähnlichkeit mit der Abfrage des Inhabers einer Telefonnummer. Ihr Erkenntniswert bleibe punktuell. Systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen ließen sich allein auf Grundlage solcher Auskünfte nicht verwirklichen.[89] Soweit für entsprechende Auskünfte seitens der Diensteanbieter unter den derzeitigen technischen Bedingungen Telekommunikationsverkehrsdaten ausgewertet werden müssen, werfe dieses keine prinzipiellen Bedenken auf.[90] Hält das Bundesverfassungsgericht die Identifizierung von Internetnutzern sonach im Wesentlichen mit der Abfrage des Inhabers einer Telefonnummer für vergleichbar, so können für den letzteren Fall auch keine (noch) geringeren Eingriffsvoraussetzungen gelten als für den ersten Fall.

Eine Abweichung rechtfertigt ferner nicht, dass die Ausführungen des Bundesverfassungsgerichts die Identifizierung von Internetnutzern anhand ihrer **IP-Adresse** betreffen, während § 112 TKG die Kenntnis einer festen Anschlusskennung oder von Personendaten voraus setzt. Wie soeben ausgeführt, sieht das Bundesverfassungsgericht darin keinen verfassungsrechtlich relevanten Unterschied. An einer Stelle weist das Urteil zwar auf das besondere Gewicht einer Aufhebung der Anonymität gerade der Internetnutzung hin,[91] jedoch nur um andererseits ein „gesteigertes Interesse“ gerade an der Zuordnung von Kommunikationsverbindungen im Internet auszumachen.[92] Insgesamt führt die Abwägung das Bundesverfassungsgericht somit zu einer Beurteilung, die für Auskünfte nach § 112 TKG – mindestens – gleichermaßen gelten muss.

3.1.2.3 Verletzung des Parlamentsvorbehalts

Hinsichtlich der in § 112 Abs. 3 TKG vorgesehenen „**Ähnlichkeitssuche**“ ist der Parlamentsvorbehalt verletzt.[93] § 112 verletzt Parlamentsvorbehalt und Gebot der Normenklarheit, weil die Vorschrift nicht selbst festgelegt, welche Angaben Suchanfragen mindestens enthalten müssen und über wie viele Personen Auskunft verlangt werden darf. Wegen der Grundrechtswesentlichkeit dieser Frage sind Regelungen in einer Rechtsverordnung (§ 112 Abs. 3 TKG), deren Erlass überdies freigestellt ist, nicht ausreichend.

3.2 Verletzung des Artikels 3 GG

In der **Beschwerdeschrift** ist ausgeführt worden, weshalb § 112 TKG auch gegen Art. 3 GG verstößt.[94] Die dortigen Ausführungen bleiben zutreffend.

4 § 113 TKG (Manueller Bestandsdatenzugriff)

4.1 Verletzung des Artikels 10 GG

4.1.1 Eingriff in den Schutzbereich

Mit **Schriftsatz vom 05.05.2009** ist umfassend dargelegt worden, weshalb der staatliche Zugriff auf Kundendaten, über die ein Kommunikationsmittler zur Vermittlung und Abrechnung von Telekommunikation verfügt, in das Fernmeldegeheimnis des betroffenen Kunden eingreift.[95] Statische Anschlusskennungen wie Rufnummern sind einfachgesetzlich als Verkehrsdaten

[89] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 256.
[90] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 260.
[91] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 258 f.
[92] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 260.
[93] Schriftsatz vom 20.04.2007, 40 f.
[94] Beschwerdeschrift, 85 f.
[95] Schriftsatz vom 05.05.2009, 20 ff.

einzuordnen.[96] Unabhängig hiervon fallen aber auch als Bestandsdaten einzuordnende Telekommunikationsdaten in den Schutzbereich des Art. 10 GG.[97]

Dass § 113 TKG in Art. 10 GG eingreift, hat das Bundesverfassungsgericht mit **Urteil vom 2. März 2010** nun jedenfalls für den Fall anerkannt, dass die Erteilung von Auskünften über Fernmeldeverhältnisse unter mittelbarer Nutzung von Verkehrsdaten erfolgt.[98] Dass die interne Verarbeitung von Verkehrsdaten als Abgrenzungskriterium für die Anwendbarkeit des Art. 10 GG nicht taugt und zu absurden Ergebnissen führt, ist indessen bereits erläutert worden.[99] Ob etwa die Benennung eines Gesprächsteilnehmers anhand von Verbindungsdaten oder Bestandsdaten erfolgt, ist gemessen am Schutzzweck des Fernmeldegeheimnisses unerheblich. In beiden Fällen ermittelt der Staat, zwischen welchen Personen Fernmeldeverkehr stattgefunden hat. Wie das Hohe Gericht zutreffend ausführt, werden intern genutzte Verbindungsdaten dem Anfragenden nicht mitgeteilt[100] und ist für ihn auch sonst ohne Bedeutung, auf welche Weise die Auskunft erteilt wird. Wegen der Diskussion hinsichtlich des Schutzbereichs des Fernmeldegeheimnisses wird im Übrigen auf die weiterhin zutreffenden Ausführungen mit Schriftsatz vom 05.05.2009 Bezug genommen.[101] Hinzuzufügen ist, dass der Europäische Gerichtshof für Menschenrechte in der Identifizierung eines Internetnutzers einen Eingriff in die „Vertraulichkeit der Kommunikation“ erkannt hat.[102]

Das Bundesverfassungsgericht meint, § 113 Abs. 1 TKG ermächtige bei verfassungsgemäßem Verständnis nicht zu **offenen Abfragen** der Behörden zu Anschlussinhabern, deren Telekommunikationsverbindungen diesen nicht bekannt seien.[103] Damit ermächtigt § 113 TKG aber erstens auch in der Auslegung des Bundesverfassungsgerichts zu offenen Abfragen über bekannte Verbindungen. Eine solche Anfrage könnte beispielsweise lauten: „Wer hat die Verbindung zu dem Anschluss 072191010 am 01.01.2009 um 12:01 hergestellt? Bitte nur Bestandsdaten mitteilen.“ Derartige Anfragen zielen auf die näheren Umstände einzelner Telekommunikationsvorgänge ab und dürfen geringeren Anforderungen als Verkehrsdatenauskünfte daher nicht unterliegen. Zweitens überzeugt die verfassungskonforme Auslegung des § 113 Abs. 1 TKG durch das Bundesverfassungsgericht nicht, so dass § 113 TKG auch Anfragen über unbekannte Telekommunikationsverbindungen abdeckt (z.B. „Welche Personen haben im Januar 2009 Verbindungen zu Telekommunikationsanschlüssen des Herrn X. hergestellt? Bitte nur Bestandsdaten mitteilen.“). Dass § 113 TKG so auszulegen ist, ist bereits ausführlich erläutert worden.[104] Der Wortlaut des § 113 TKG stellt rein formal auf die Art der übermittelten Daten ab und deckt jede Mitteilung von Bestandsdaten ab. Die Vorschrift stellt keinerlei Anforderungen an Vorkenntnisse der Behörde, an Ermittlungsziel, an Art und Inhalt der Anfrage oder an die zu ihrer Beantwortung zulässige Datenverarbeitung. Weder § 113 TKG noch § 100g StPO ist zu entnehmen, wann eine „Umgehung“ des § 100g StPO vorliegt. § 100g StPO ermächtigt allein zur Erhebung von Verkehrsdaten. Der Gesetzgeber hat nicht normenklar bestimmt, dass § 113 TKG keine Anwendung finden solle, wenn die Beauskunftung die interne Verwendung von Verkehrsdaten voraus setze. Das Bundesverfassungsgericht selbst verneint eine solche Beschränkung für den Fall wechselnder IP-Adressen.[105] Alleine aus dem Umstand, dass die Begründung eines Gesetzentwurfs die Zuordnung von IP-Adressen unter § 113 TKG subsumiert,

---

[96] Schriftsatz vom 07.05.2009, 6 und 29.

[97] Schriftsatz vom 07.05.2009, 1 ff.

[98] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 195.

[99] Schriftsatz vom 05.05.2009, 20.

[100] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 256.

[101] Schriftsatz vom 05.05.2009, 17 ff.

[102] EGMR, 2872/02 vom 02.12.2008 (K.U. gegen Finnland), Abs. 49.

[103] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 290.

[104] Schriftsatz vom 05.05.2009, 2 und 13 ff.

[105] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 290.

ergibt sich keinesfalls mit der grundrechtlich und von Art. 8 EMRK geforderten Normenklarheit, dass § 113 TKG die interne Verarbeitung von Verkehrsdaten allein in diesem Fall gestatte. Auch für die Normanwender ist dies nicht ersichtlich.

4.1.1.1 Verletzung des Zitiergebots

§ 113 TKG verletzt das Zitiergebot des Art. 19 Abs. 1 S. 2 GG, weil er das eingeschränkte Grundrecht (Art. 10 GG) nicht nennt. Der Gesetzgeber hat den Eingriff in das Fernmeldegeheimnis verkannt. Nach der **Rechtsprechung des Bundesverfassungsgerichts** ist eine Verletzung des Zitiergebots jedenfalls insoweit gegeben, als § 113 TKG zu Auskünften über wechselnde IP-Adressen ermächtigt[106] und damit in Art. 10 GG eingreift.[107]

4.1.1.2 Verletzung des Verhältnismäßigkeitsgebots

4.1.1.2.1 Einheitlicher Schutz des Fernmeldegeheimnisses

§ 113 TKG verletzt vor allem das Verhältnismäßigkeitsgebot. Wie bereits umfassend ausgeführt, sind die näheren Umstände eines Fernmelde-Vertragsverhältnisses integraler Bestandteil der in diesem Rahmen vermittelten Telekommunikation. Insbesondere die Information, wer unter welcher Kennung kommuniziert (hat), ist der Schlüssel zur Vertraulichkeit der Telekommunikation auch im Verhältnis zum Kommunikationspartner und ist **nicht typischerweise weniger schutzwürdig** als Inhalt und Umstände der einzelnen Kommunikationsvorgänge selbst.[108] Deswegen muss die Aufdeckung der Identität eines Kommunikationsteilnehmers oder der Kennung, unter welcher eine Person kommuniziert, denselben Voraussetzungen unterworfen werden wie sonstige Eingriffe in das Fernmeldegeheimnis (etwa § 100a StPO). Dassselbe gilt, soweit § 113 TKG den Zugriff auf Schlüssel zu Kommunikationsinhalten erlaubt (z.B. Zugriffscode für elektronischen Anrufbeantworter oder E-Mail-Postfach).

§ 113 TKG genügt den **Anforderungen des Verhältnismäßigkeitsgebots** danach nicht: Er beschränkt die Durchbrechung des Fernmeldegeheimnisses nicht auf die Aufklärung schwerer Straftaten[109] und die Abwehr von Gefahren für wichtige Rechtsgüter[110]. § 113 TKG beschränkt die Datenerhebung nicht auf Beschuldigte/Störer oder solche Personen, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für einen Beschuldigten/Störer bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte/Störer ihren Anschluss benutzt (vgl. § 100a StPO). § 113 TKG versäumt es ferner, eine richterliche Prüfung zur Voraussetzung für den Zugriff zu machen.[111] Der derzeitige § 113 TKG begünstigt die massenhafte Aufhebung der Anonymität von Fernmeldeverhältnissen und genügt dem Verhältnismäßigkeitsgebot nicht. Schon im Jahr 2006 identifizierte alleine die Deutsche Telekom AG 94.417 Inhaber von IP-Adressen, während es im Jahr 2003 noch 3.170 Personen waren.[112] Die unzureichenden Voraussetzungen des § 113 TKG ermöglichen erst diese ausufernde Aufhebung der Vertraulichkeit der Internetnutzung. § 113 TKG gewährleistet

---

[106] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 290.

[107] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 195.

[108] Näher Schriftsatz vom 05.05.2009, 20 ff.

[109] Vgl. BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 228.

[110] Vgl. BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 231.

[111] Vgl. BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 247 ff.

[112] Köbele, Wirtschaftsunternehmen – Verlängerter Arm der Strafverfolgungsbehörden?, https://www.datenschutzzentrum.de/sommerakademie/2007/sak2007-koebele-wirtschaftsunternehmen-verlaengerter-arm-der-sicherheitsbehoerden.pdf, 7.

schließlich nicht die verfassungsrechtlich gebotene Zweckbindung erlangter Informationen,[113] die Kennzeichnung erhobener Daten[114] und die Benachrichtigung der Betroffenen[115].

Die mindestens gebotene Erstreckung des Schutzniveaus des § 100g StPO auf Bestandsdaten und des § 100a StPO auf Schlüssel zum Zugriff auf Kommunikationsinhalte ist mit der **Rechtsprechung des europäischen Gerichtshofs für Menschenrechte** vereinbar. Der vom Gerichtshof beurteilte Fall einer mittels Telekommunikation begangenen öffentlichen Verleumdung im Internet[116] hätte nach den §§ 187 StGB, 100g Abs. 1 S. 1 Nr. 2 StPO ein Auskunftsrecht über die Identität des Anschlussinhabers begründet, ohne dass § 113 TKG erforderlich gewesen wäre. Auch hat es der Gerichtshof unbeanstandet gelassen, dass eine richterliche Genehmigung zur Voraussetzung einer Identifizierung von Internetnutzern gemacht wird.[117] Er hat in diesem Zusammenhang ausdrücklich das „Erfordernis" betont, „sicherzustellen, dass Befugnisse zur Kontrolle, Verhütung und Aufklärung von Straftaten so angewandt werden, dass ein rechtsstaatliches Verfahren und andere Garantien, die der Aufklärung von Straftaten und der Verfolgung von Straftätern legitime Grenzen setzen, in vollem Umfang eingehalten werden, einschließlich der Garantien aus den Artikeln 8 und 10 der Konvention, auf die sich auch Straftäter berufen können".[118] Eine Norm, die es wie § 113 TKG alleine in die Hand von Staatsanwaltschaft, Polizei und Nachrichtendiensten einerseits sowie des Anbieters andererseits legt, ob die grundrechtlichen Anforderungen an eine Offenlegung der Identität oder weiterer Kommunikationsdaten einschließlich der Zugangsdaten zu einem Nachrichtenspeicher gewahrt sind, gewährleistet das von Grundgesetz und EMRK gebotene grundrechtssichernde Verfahren nicht.

Mit **Urteil vom 2. März 2010** hat das Bundesverfassungsgericht die Auffassung vertreten, die staatliche Identifizierung von Internetnutzern unterliege geringeren verfassungsrechtlichen Anforderungen als die Erhebung des Inhalts oder der sonstigen Umstände einzelner Kommunikationsvorgänge.[119] Den dazu vorgebrachten Argumenten ist oben bereits ausführlich entgegen getreten worden.[120] Dass Identifikationsdaten eine vergleichbare Sensibilität wie Verbindungsdaten aufweisen, hat der Gesetzgeber inzwischen mit der Regelung zur Meldepflicht von Datenpannen in § 93 Abs. 3 TKG anerkannt. Der Verlust von Bestands- und Verkehrsdaten begründet danach gleichermaßen eine Informationspflicht. Die Begründung des Gesetzentwurfs zu § 93 Abs. 3 TKG führt dazu aus, die Meldepflicht beziehe sich „auf besonders sensible personenbezogene Daten"[121], wozu der Gesetzgeber Bestands- und Verkehrsdaten gleichermaßen zählt.

Die Argumentation, mit der das Bundesverfassungsgericht **geringere verfassungsrechtliche Anforderungen an die Identifizierung von Internetnutzern** stellt als an sonstige Eingriff in das Fernmeldegeheimnis, überzeugt nicht. Es ist nicht nachvollziehbar, warum die Identifizierung eines Teilnehmers anhand einer IP-Adresse geringeren Anforderungen unterliegen soll als seine Identifizierung anhand anderer Verkehrsdaten (z.B. IMEI-Kennung, Zeitpunkt einer Telefonverbindung). Diese Diskriminierung von Internetverbindungen führt zu unauflösbaren Wertungswidersprüchen: Ruft jemand mit unterdrückter Rufnummer zu einer bekannten Uhrzeit einen bekannten Zielanschluss an, so darf er anhand der bekannten Verbindungsdaten nach

---

113 Beschwerdeschrift, 80.

114 Beschwerdeschrift, 80; Schriftsatz vom 20.04.2007, 40; jetzt auch BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 236.

115 Beschwerdeschrift, 80.

116 EGMR, 2872/02 vom 02.12.2008 (K.U. gegen Finnland).

117 EGMR, 2872/02 vom 02.12.2008 (K.U. gegen Finnland), Abs. 49 und 21.

118 EGMR, 2872/02 vom 02.12.2008 (K.U. gegen Finnland), Abs. 48.

119 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 254.

120 Seiten 7 ff.

121 Bundesregierung, BT-Drs. 16/12011, 34.

Auffassung des Bundesverfassungsgerichts nur mit richterlicher Anordnung nach Maßgabe des § 100g StPO identifiziert werden („Zielwahlsuche"). Erfolgt der Anruf dagegen unter Verwendung eines anonymen Internettelefoniedienstes (z.B. Skype), so soll die Identifizierung des Anrufers anhand bekannter Verbindungsdaten (IP-Adresse, Zeit) ohne richterliche Anordnung und bereits zur Aufklärung des Verdachts einer „erheblichen" Ordnungswidrigkeit oder Bagatellstraftat zulässig sein. Sendet jemand ohne Rufnummernübermittlung ein Telefax, so darf seine Anonymität im Wege einer Zielwahlsuche nur mit richterlicher Anordnung nach Maßgabe des § 100g StPO aufgehoben werden. Wird dasselbe Dokument dagegen über ein anonymes E-Mail-Postfach versandt, so soll die Identifizierung des Anschlussinhabers anhand der verwendeten IP-Adresse ohne richterliche Anordnung und bereits zur Aufklärung des Verdachts einer „erheblichen" Ordnungswidrigkeit oder Bagatellstraftat zulässig sein. Die Privilegierung einer Internet-Zielwahlsuche gegenüber einer Telefon-Zielwahlsuche ist sachlich nicht zu rechtfertigen. Auch ist nicht plausibel zu machen, weshalb unbedeutende Verkehrsdaten zu schon bekannten Verbindungen (z.B. Datenvolumen, genaue Anrufdauer) einen besseren Schutz genießen sollen als die äußerst grundrechtsbedeutsame Identität eines noch unbekannten Kommunikationsteilnehmers. Soweit das Bundesverfassungsgericht dynamische IP-Adressen offenbar nicht anders als statische Anschlusskennungen behandeln will, könnte dieses Argument für andere Verkehrsdaten (z.B. IMEI-Kennung, Zeitpunkt einer Telefonverbindung) gleichermaßen angeführt werden. Letztlich lässt sich eine konsistente Gleichbehandlung aller Identifizierungen von Teilnehmern nur erreichen, wenn diese sämtlich als Eingriff in das Fernmeldegeheimnis anerkannt und den diesbezüglich für Verkehrsdaten anerkannten Anforderungen unterworfen werden.

Das Argument, im Rahmen einer Bestandsdatenauskunft würden **intern verarbeitete Verkehrsdaten nicht mitgeteilt**, stellt allein auf die Art der verarbeiteten Daten ab. Seit dem Volkszählungsurteil ist aber anerkannt, dass für die Eingriffstiefe nicht die Art der verarbeiteten Daten entscheidend ist, sondern deren Nutzbarkeit und Verwendungsmöglichkeiten.[122] Dass die Zuordnung einer IP-Adresse zur Aufdeckung der gesamten Internetnutzung während der maßgeblichen Verbindung genutzt werden kann, ist bereits ausgeführt worden.

Auf das Argument, **Bestandsdatenauskünfte beschränkten sich auf punktuelle Informationen**, ist bereits im Rahmen des § 112 TKG eingegangen worden.[123] Im Hinblick auf § 113 TKG überzeugt das Argument noch weniger: So kann die Zuordnung einer dynamischen IP-Adresse die inhaltliche Rekonstruktion der gesamten Internetsitzung anhand von Nutzungsdaten (z.B. URL, „Referer") und somit die Erstellung tiefgreifender Persönlichkeitsprofile ermöglichen, wie sie bei Telefon-Verbindungsdaten nicht erstellt werden können. Die für die verfassungsrechtliche Beurteilung entscheidende Nutzbarkeit[124] der Zuordnung einer IP-Adresse ist also sehr hoch. Soweit das Bundesverfassungsgericht darauf abstellt, dass die §§ 11 ff. TMG Internet-Diensteanbieter grundsätzlich zur Löschung von nicht für die Abrechnung erforderlichen Nutzungsdaten verpflichteten,[125] werden diese Vorschriften in der Praxis verbreitet nicht angewandt, von den Aufsichtsbehörden nicht durchgesetzt und gelten für die größten, im Ausland ansässigen Anbieter wie Google, Facebook oder eBay von vornherein nicht. Diese Anbieter erteilen gleichwohl grenzüberschreitend Auskünfte an deutsche Behörden über Internet-Nutzungsprotokolle und ermöglichen diesen dadurch den Nachvollzug potenziell jedes Klicks und jeder Eingabe eines Internetnutzers noch nach Monaten. Weiters ermöglicht § 113 TKG den Zugriff auf elektronische Adressbücher und sogar auf Schlüssel zum Abruf von Kommunikationsinhalten (§ 113 Abs. 1 S. 2 TKG). Solche Informationen ermöglichen ebenfalls

---

122 BVerfGE 65, 1, 45.

123 Seite 11 ff.

124 BVerfGE 65, 1, 45.

125 BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 270.

tiefgreifende Einblicke in die persönliche Lebenssituation sowie die Erstellung von Persönlichkeitsprofilen.

Das Bundesverfassungsgericht hat weiter argumentiert, es bestehe ein **gesteigertes Interesse** an der Möglichkeit, Kommunikationsverbindungen im Internet zum Rechtsgüterschutz oder zur Wahrung der Rechtsordnung den jeweiligen Akteuren zuordnen zu können. Gesteigert im Vergleich zu unmittelbarer Kommunikation oder zur Telefonnutzung wäre das Identifizierungsinteresse im Internet aber nur, wenn die durchschnittliche Internetverbindung häufiger zu Rechtsverletzungen eingesetzt würde als die durchschnittliche Telefonverbindung oder das durchschnittliche persönliche Gespräch. Dafür ist indes nichts ersichtlich oder gar empirisch belegt. Alleine die Tatsache, dass sich das Medium Internet zunehmend durchsetzt und dadurch naturgemäß die absolute Zahl der hier begangenen Straftaten im gleichen Maß steigt wie die Dauer der Nutzung des Mediums, rechtfertigt es nicht, von den sonst gültigen Eingriffsgrenzen abzugehen. Bei einer solchen Rechnung bliebe unbeachtet, dass die absolute Zahl der registrierten Straftaten seit Jahren fällt, die steigende Zahl registrierter Straftaten im Internet also eine bloße Verlagerung von Kriminalität in moderne Kommunikationsformen darstellt. Bei einer insgesamt fallenden Zahl von Delikten würde es dem Grundgesetz nicht gerecht, eine bloße Kriminalitätsverlagerung zur Rechtfertigung geringerer Eingriffsschwellen heranzuziehen. Dies würde zu einer zunehmenden Aushöhlung und Verminderung des Grundrechtsschutzes führen, anstatt ihn auf neue technische Medien möglichst ungeschmälert zu übertragen, wie es dem Zweck der Grundrechte alleine gerecht wird.

Von einem **rechtsfreien Raum** wäre das Internet auch dann weit entfernt, wenn man die Anonymität des Nutzers und Bestandsdaten ebenso schützte wie die sonstigen Umstände der Telekommunikation. Es ist bereits ausgeführt worden, dass verschiedene Rechtsordnungen seit jeher Bestands- und Verkehrsdaten als „Kommunikationsdaten“ demselben einheitlichen Schutz und identischen Eingriffsschwellen unterwerfen. Niemand würde deswegen ernstlich das Internet in diesen Nachbarstaaten als rechtsfreien Raum bezeichnen. Es ist nicht einmal belegt, dass ein einheitlicher Schutz für Kommunikationsdaten überhaupt eine statistisch nachweisbare, negative Auswirkung auf Aufklärungsquote oder Kriminalitätsrate hätte.

Soweit das Urteil vom 2. März 2010 ausführt, die Offenlegung der Zuordnung einer Internetkennung habe ein erheblich **weniger belastendes Gewicht als eine Offenlegung nahezu vollständig gespeicherter Daten sämtlicher Telekommunikationsverbindungen**,[126] kann diesem Vergleich nicht beigetreten werden. Die Offenlegung nahezu vollständig gespeicherter Daten sämtlicher über einen Anschluss hergestellter Telekommunikationsverbindungen ist nämlich weitgehend bedeutungslos, solange die Identität des Anschlussinhabers nicht bekannt ist. Gerade die Aufhebung dieser Anonymität ermöglicht § 113 TKG in ausufernder Weite. Dass im Internet verbreitet freiwillig eine nahezu vollständige Speicherung der gesamten Telemediennutzung in sogenannten „Logfiles“ erfolgt und diese – anders als Verbindungsdaten – auch nicht dem Schutz des Fernmeldegeheimnisses unterliegen, ist bereits ausgeführt worden. Vor dem Hintergrund kooperationswilliger Telemedienanbieter, die nicht dem Fernmeldegeheimnis verpflichtet sind, stellt § 113 TKG regelmäßig den einzigen Schutz des Internetnutzers vor der potenziell vollständigen Aufdeckung seiner Nutzung eines Telemediums dar. Im Übrigen verkennt der Vergleich des Bundesverfassungsgerichts, dass § 100g StPO nicht nur für die vollständige Offenlegung sämtlicher Telekommunikationsverbindungen gilt, sondern auch etwa für die Mitteilung unbedeutender Verbindungsdetails zu bereits bekannten Verbindungen. Unter Berücksichtigung dessen ist nicht zu vermitteln, weshalb die zentrale Frage der Identität eines Kommunikationsteilnehmers, aber auch etwa seines elektronischen Telefonbuchs oder gar der Zugangsdaten zu seinen Kommunikationsinhalten (§ 113 Abs. 1 S. 2

[126] BVerfG, 1 BvR 256/08 vom 02.03.2010, Absatz-Nr. 257.

TKG) geringeren verfassungsrechtlichen Anforderungen unterliegen soll als unbedeutendste Verbindungsdetails. Dass § 100g StPO einerseits und § 113 TKG andererseits alleine nach der Art der zu beauskunftenden Daten unterscheiden, deren vergleichbare Nutzbarkeit und Verwendungsmöglichkeiten aber ignorieren, ist verfassungsrechtlich nicht haltbar. Es wurde bereits ausgeführt, dass insbesondere die Identität der Kommunikationsteilnehmer und der Inhaber der genutzten Telekommunikationsanschlüsse integraler Bestandteil der Telekommunikation und nicht weniger schutzwürdig als diese selbst ist.[127]

In Österreich hat der Oberste Gerichtshof (OGH) zudem erkannt, dass es gegen die **Art. 6 und 15 RiL 2002/58/EG** verstößt, einer Ermächtigung zur Auskunfterteilung über Bestandsdaten implizit die Befugnis zur internen Verarbeitung von Verkehrsdaten zu entnehmen:

> *„Der einfache Weg, **allein auf die Bekanntgabe von Stammdaten abzustellen** und die Vorgänge bei deren Ermittlung völlig auszublenden, ist damit gemeinschaftsrechtlich nicht gangbar (ebenso zur vergleichbaren Problematik im Strafverfahren DSK GZ K213.000/0005-DSK/2006). Vielmehr ist anzunehmen, dass Art 6 der RL 2002/58/EG und dessen Umsetzung in § 99 TKG 2003 der - im vorliegenden Fall erforderlichen - Verarbeitung von Verkehrsdaten für die Erteilung der hier begehrten Auskunft entgegensteht. Denn nach Absatz 1 dieser Bestimmung sind „Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes verarbeitet und gespeichert werden, [...] unbeschadet der Absätze 2, 3 und 5 des vorliegenden Artikels und des Artikels 15 Absatz 1 zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden.“ Die Absätze 2, 3 und 5 gestatten in weiterer Folge die Verarbeitung (und damit die Speicherung) von Verkehrsdaten für bestimmte Zwecke. Aus diesem Regelungszusammenhang ist abzuleiten, dass eine Verarbeitung von - wenngleich unter Umständen nach den Absätzen 2, 3 und 5 rechtmäßig gespeicherten - Daten für andere Zwecke nicht zulässig ist. Denn die Löschungspflicht hat offenkundig den Zweck, eine unzulässige Nutzung der Daten zu verhindern. Dieser Zweck würde durch die Zulässigkeit der anderweitigen Nutzung rechtmäßig gespeicherter Daten unterlaufen, ohne dass dies durch die Wertung der jeweiligen Ausnahmebestimmungen gedeckt wäre. Zudem verstieße eine solche Auffassung gegen den datenschutzrechtlichen Grundsatz der strikten Zweckbindung, wonach Daten, die für einen bestimmten Zweck gespeichert wurden, auch nur für diesen Zweck verarbeitet werden dürfen (Art 6 Abs 1 lit c der RL 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr; zum österreichischen Datenschutzrecht zuletzt etwa VfGH G 147/06 = VfSlg 18146, Punkt 2.3.1). [...]Eine allfällige Regelung hat jedoch nach Art 15 Abs 1 der RL 2002/58/EG durch „Rechtsvorschriften“ („legislative measures“ bzw „mesures législatives“) zu erfolgen. [...] Zum anderen kann die Annahme einer bloß impliziten Regelung dem gemeinschaftsrechtlichen Erfordernis einer Anordnung durch ‚Rechtsvorschrift‘ nicht genügen. Durch diesen formellen Gesetzesvorbehalt soll offenkundig Rechtssicherheit geschaffen werden, die bei Annahme einer bloß impliziten Anordnung, wie auch das vorliegende Verfahren beweist, nicht gegeben ist.“*[128]

4.1.1.2.2 Anwendung der Rechtsprechung zur Identifizierung von Internetnutzern

Selbst wenn man die vom Bundesverfassungsgericht zur Identifizierung von Internetnutzern **entwickelten Maßstäbe** akzeptieren wollte, änderte dies nichts an der Verletzung des Verhältnismäßigkeitsgebots:

---

[127] Schriftsatz vom 07.05.2009, 30.

[128] OGH, 4 Ob 41/09x vom 14.07.2009.

Das Bundesverfassungsgericht hat identifizierende Auskünfte nur für die Verfolgung von Straftaten, für die Verfolgung - auch im Einzelfall - besonders gewichtiger und ausdrücklich zu benennender **Ordnungswidrigkeiten**, für die Gefahrenabwehr und die Aufgabenwahrnehmung der Nachrichtendienste auf der Grundlage der allgemeinen fachrechtlichen Eingriffsermächtigungen zugelassen.[129] § 113 TKG stellt demgegenüber keine Anforderung an die Schwere der Ordnungswidrigkeit, deren Aufklärung den Eingriff rechtfertigen soll.

§ 113 TKG versäumt es auch, sicherzustellen, dass Auskünfte nicht ins Blaue hinein eingeholt werden, sondern nur aufgrund eines **Anfangsverdachts** oder einer konkreten Gefahr auf einzelfallbezogener Tatsachenbasis.[130] Eine solche Anforderung kann der Norm – wie schon zu § 112 Abs. 2 TKG aufgezeigt[131] – im Wege der Auslegung nicht entnommen werden, ohne das Gebot der Normenklarheit zu verletzen. Auch das Fachrecht gewährleistet die Einhaltung der verfassungsrechtlich gebotenen Eingriffsschwellen nicht: § 113 TKG bestimmt erstens nicht normenklar, dass Zugriffe nur nach Maßgabe fachgesetzlicher Ermächtigungen zulässig sein sollen. Zweitens sieht das Fachrecht vielfach selbst nicht die erforderliche Eingriffsschwelle vor. So setzen die §§ 8a Abs. 1 BVerfSchG, 4a MAD-G, 2a BND-G keine konkrete Gefahr auf einzelfallbezogener Tatsachenbasis voraus, sondern nur die „Erforderlichkeit" der Datenerhebung zur Aufgabenerfüllung. Gleiches gilt für § 21 BPolG, §§ 20b, 22 BKAG und eine Vielzahl von Datenerhebungsbefugnissen der Länder.

§ 113 TKG stellt ferner – anders als etwa das österreichische Recht – nicht sicher, dass die rechtlichen und tatsächlichen Grundlagen entsprechender Abfragen **aktenkundig** gemacht werden, wie es verfassungsrechtlich geboten ist.[132]

Weiter ist zu bedenken, dass das Bundesverfassungsgericht unter den mit Urteil vom 2. März 2010 entwickelten Voraussetzungen **nur die Identifizierung der „Anschlussinhaber bestimmter IP-Adressen" zugelassen** hat, namentlich mit dem Argument der von Telekommunikation ausgehenden Gefahren.[133] Die Identifizierung der Inhaber bestimmter Rufnummern oder E-Mail-Adressen ist mit der IP-Adresse zwar vergleichbar. § 113 TKG geht darüber aber weit hinaus und ermöglicht Grundrechtseingriffe, die mit Gefahren der Telekommunikation überhaupt nichts zu tun haben. § 113 TKG setzt keine Nutzung von Kommunikationsnetzen zu rechtswidrigen Zwecken voraus. Die Vorschrift ermöglicht die Verfolgung von Straftaten und die Abwehr von Gefahren, die mit Telekommunikation nichts zu tun haben. Andere Unternehmen müssen Daten nur unter den Voraussetzungen einer Beschlagnahme herausgeben.[134] Regelmäßig ist auch ein Durchsuchungsbeschluss erforderlich, weil sich die Datenträger in Geschäftsräumen befinden. Beschlagnahme und Durchsuchung setzen regelmäßig eine richterliche Anordnung voraus und sind den Nachrichtendiensten insgesamt versagt. Der Bedeutung von Kommunikationsdaten als Grundlage und Voraussetzung eines Telekommunikationsverhältnisses wird es nicht gerecht, dass gerade diese besonders sensiblen und vom Fernmeldegeheimnis geschützten Informationen unter geringeren Voraussetzungen zugänglich sein sollen als beliebige sonstige Kundendaten, selbst wenn keine Nutzung von Kommunikationsnetzen zu rechtswidrigen Zwecken voran gegangen ist. Die Ausgestaltung des § 113 TKG als allgemeines Ermittlungsinstrument und Bevölkerungsregister ist mit dem Fernmeldegeheimnis nicht in Einklang zu bringen. Dementsprechend hat der Bundesdatenschutzbeauftragte ausgeführt: „*Ein Anspruch, in einem ‚vereinfachten Verfahren' über die telekommunikationsspezifischen Daten hinausgehende*

[129] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261 f.
[130] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261.
[131] Seite 14 ff.
[132] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261.
[133] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 260.
[134] BVerfGE 113, 29, 50.

beliebige Kundendaten zu erhalten, den es in anderen Branchen der Privatwirtschaft nicht gibt, lässt sich auch für den TK-Bereich nicht rechtfertigen".[135]

Wo die Identifizierung eines Anschlussinhabers oder auch die Ermittlung einer Anschlusskennung zum Zwecke ihrer Überwachung erfolgen soll, mag man mit den **besonderen Gefahren der Telekommunikation** abgesenkte Eingriffsschwellen begründen, wie es das Bundesverfassungsgericht getan hat.[136] In anderen Fällen aber muss es dabei bleiben, dass das Fernmeldegeheimnis die Vertraulichkeit der Fernmeldebeziehung einschließlich der zur Abrechnung erforderlichen Kundendaten schützt. Will der Staat Personendaten nur wie aus einem Telefonbuch, aus dem Melderegister oder aus der Kundendatei eines beliebigen Unternehmens nutzen, so muss er sich auf das Telefonbuch, das Melderegister und andere Kundendateien beschränken. Das Fernmeldegeheimnis erlaubt Durchbrechungen nur, wo der Grund des staatlichen Zugriffswunschs einen inneren Zusammenhang mit der Telekommunikation aufweist. Der Telekommunikation eigen ist nur die Verwendung von Anschlusskennungen, nicht allgemein die Angabe von Personendaten. § 113 TKG ist folglich auch auf der Grundlage der Ausführungen des Bundesverfassungsgerichts verfassungswidrig, weil er die Aufhebung der Vertraulichkeit von Fernmeldeverhältnissen nicht auf Fälle der Identifizierung eines Anschlussinhabers oder auch der Ermittlung einer Anschlusskennung zum Zwecke ihrer Überwachung beschränkt.

Dem Argument der Bundesregierung, die erforderliche datenschutzrechtliche Regelung der Datenverwendung sei eine **Frage des „Fachrechts"** und lasse die Verfassungsmäßigkeit der telekommunikationsrechtlichen Öffnungsnorm unberührt, hat das Bundesverfassungsgericht nun eine Absage erteilt, wie zu § 112 TKG bereits erläutert worden ist. Wenn der Gesetzgeber in den §§ 95 Abs. 3, 111 TKG die Speicherung von Telekommunikationsdaten anordnet oder dazu ermächtigt, obliegt es ihm zugleich, die für deren verfassungsrechtliche Rechtfertigung erforderlichen Verwendungszwecke und Eingriffsschwellen sowie die zur Gewährleistung der Zweckbindung erforderlichen Folgeregelungen verbindlich festzulegen. Solche Festlegungen enthält § 113 TKG nicht.

§ 113 TKG ist danach verfassungswidrig, weil es der Gesetzgeber versäumt hat, die zur **Gewährleistung der Zweckbindung** erforderlichen Folgeregelungen verbindlich festzulegen. § 113 TKG fehlt namentlich die verfassungsrechtlich gebotene[137] Anordnung, dass die Verwendung erlangter Daten nur zur Verfolgung derjenigen Zwecke zulässig ist, zu deren Erreichung die Daten nach dem Gesetz erhoben werden durften, und dass die Daten zu löschen sind, wenn sie zu diesen Zwecken nicht mehr benötigt werden (Zweckbindungsgebot).

Im Hinblick auf die grundrechtlichen Benachrichtigungspflichten und die gerichtliche Kontrolle lässt das Bundesverfassungsgericht eine **Ausgestaltung durch die Fachgesetze** und damit gegebenenfalls auch durch Landesgesetze genügen.[138] Eine Verletzung dieser verfassungsrechtlichen Anforderungen soll also nur zur Nichtigkeit der fachrechtlichen Zugriffsnorm führen, nicht aber der im Telekommunikationsgesetz eröffneten Zugriffsmöglichkeit. Aus den oben zu § 112 TKG genannten Gründen ist dies unbefriedigend. Die Einhaltung der verfassungsrechtlich unverzichtbaren Verfahrensgarantien ist nur dann effektiv zu gewährleisten, wenn das Telekommunikationsrecht eine fachgesetzliche Zugriffsnorm zur Voraussetzung einer grundrechtseingreifenden Datenübermittlung macht, welche neben das Telekommunikationsrecht treten, die erforderlichen Verfahrensgarantien vorsehen und auf die Erhebung von Telekommunikationsdaten abgestimmt sein muss. Das Telekommunikationsrecht

---

[135] Bundesbeauftragter für den Datenschutz, 17. Tätigkeitsbericht 1997–1998, 208 f.

[136] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 260.

[137] BVerfGE 65, 1 (46).

[138] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 286.

muss dazu normenklar festlegen, dass es nicht eigenständig zu Datenübermittlungen ermächtigt, sondern nur eine datenschutzrechtliche Öffnungsnorm bildet. Ermächtigt das Telekommunikationsrecht selbst zu Datenübermittlungen, dann muss es auch selbst die verfassungsrechtlich gebotenen Verfahrensgarantien gewährleisten. Ferner darf sich das Telekommunikationsrecht nur solchen Fachrechtsnormen öffnen, die nach dem Willen des Gesetzgebers der Erhebung von Telekommunikationsdaten dienen sollten. Insofern ist ein einfachgesetzliches Zitiergebot zu fordern, wie es § 113b TKG vorgesehen hat. Nur das Erfordernis eines solchen Zitats stellt sicher, dass fachrechtliche Zugriffsnormen den für Telekommunikationsdaten geltenden, besonderen verfassungsrechtlichen Anforderungen Rechnung tragen.

Anders als der ehemalige § 113b TKG stellt **§ 113 TKG nicht nur eine datenschutzrechtliche Öffnungsnorm** dar, sondern soll nach dem Willen des Gesetzgebers eine eigenständige Zugriffsermächtigung bilden. Dieser Regelungsinhalt ist im Wege der grammatikalischen, systematischen und historischen Auslegung bereits ausführlich dargelegt worden.[139] Während § 113b TKG ausdrücklich forderte, eine Datenübermittlung müsse „in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf § 113a vorgesehen" sein, stellt § 113 TKG erkennbar eine abschließende Regelung dar. Insbesondere bestimmt die Vorschrift nicht nur, der Diensteanbieter „dürfe" Auskünfte nach Maßgabe fachgesetzlicher Verpflichtungen erteilen, sondern dass er Auskünfte unter abschließend festgelegten Voraussetzungen zu erteilen „hat".

Gegen den eindeutigen Wortlaut des § 113 TKG ist es auch nicht möglich, die Norm **verfassungskonform dahin auszulegen**, dass sie auf die jeweiligen fachgesetzlichen Eingriffsermächtigungen verweise.[140] Selbst wenn man die Norm entgegen der hier vertretenen Auffassung insoweit für auslegungsfähig hielte, wäre eine solche Auslegung jedenfalls mit dem auch in Art. 8 EMRK verankerten Gebot der Normenklarheit unvereinbar. Dem § 113 TKG kann weder der betroffene Bürger, noch die eingreifende Behörde, noch das kontrollierende Gericht entnehmen, dass Datenübermittlungen eine fachgesetzliche Ermächtigung der jeweiligen Stelle voraus setzten und nur in deren Rahmen zulässig seien.

Hat der Gesetzgeber mit § 113 TKG danach eine **abschließende Regelung** der Datenübermittlung geschaffen, so ist der in der Norm liegende Grundrechtseingriff nur gerechtfertigt, wenn das Verfahren der Datenerhebung und -verwendung den grundrechtlichen Anforderungen entspricht. Dies ist im Hinblick auf die verfassungsrechtliche Benachrichtigungspflicht[141] und auf die verfassungsrechtliche Kennzeichnungspflicht[142] indes nicht der Fall.

4.1.1.2.3 Vergleichbarkeit der Identifizierung von Internetnutzern

Die vom Bundesverfassungsgericht entwickelten Anforderungen an die Identifizierung von Internetnutzern[143] dürfen **in den übrigen Fällen des § 113 TKG** keinesfalls noch unterschritten werden. Aus den zu § 112 TKG ausgeführten Gründen[144] rechtfertigt keine Abweichung, dass die Ausführungen des Bundesverfassungsgerichts zu § 113 TKG im Zusammenhang mit der mittelbaren Nutzung anlasslos und flächendeckend erhobener Verkehrsdaten erfolgt sind, während § 113 TKG auch Auskünfte ohne Verarbeitung von Verkehrsdaten erfasst. Eine Abweichung rechtfertigt ferner nicht, dass die Ausführungen des Bundesverfassungsgerichts

---

[139] Schriftsatz vom 20.04.2007, 34 ff.

[140] So BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 289 zu § 113 Abs. 1 TKG.

[141] Beschwerdeschrift, 80; Schriftsatz vom 20.04.2007, 39.

[142] Beschwerdeschrift, 80; Schriftsatz vom 20.04.2007, 40.

[143] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 261 ff.

[144] Seite 18 oben.

Auskünfte über Internetnutzer betreffen, während § 113 TKG auch zu Auskünften etwa über Telefonnutzer ermächtigt. Wie zu § 112 TKG ausgeführt,[145] sieht das Bundesverfassungsgericht darin keinen verfassungsrechtlich relevanten Unterschied. An einer Stelle weist das Urteil zwar auf das besondere Gewicht einer Aufhebung der Anonymität gerade der Internetnutzung hin,[146] jedoch nur um andererseits ein „gesteigertes Interesse" gerade an der Zuordnung von Kommunikationsverbindungen im Internet auszumachen.[147] Insgesamt führt die Abwägung das Bundesverfassungsgericht somit zu einer Beurteilung, die für alle Auskünfte nach § 113 TKG mindestens gleichermaßen gelten muss.

4.2 Verletzung des Artikels 3 GG

In der **Beschwerdeschrift** ist ausgeführt worden, weshalb § 113 TKG auch gegen Art. 3 GG verstößt.[148] Die dortigen Ausführungen bleiben zutreffend.

5 Rechtsfolge der Verfassungsverstöße

Nach § 95 Abs. 3 BVerfGG sind die grundrechtsverletzenden §§ 95 Abs. 3, 111, 112 und 113 TKG für **nichtig** zu erklären.

Abweichend von § 95 Abs. 3 BVerfGG sieht das **Bundesverfassungsgericht** mitunter von der Nichtigerklärung eines Gesetzes, das erfolgreich mit einer Verfassungsbeschwerde angefochten worden ist, ab. Von einer Nichtigerklärung ist in der Vergangenheit etwa mit der Begründung abgesehen worden, dass dadurch in die Gestaltungsfreiheit des Gesetzgebers eingegriffen oder ein Rechtszustand herbeigeführt würde, welcher der verfassungsmäßigen Ordnung noch weniger entspräche als die angegriffene Regelung. Teilweise ist von einer Nichtigerklärung abgesehen worden, weil diese unzumutbare Rechtsunsicherheit oder weitreichende Folgen für die öffentlichen Haushalte nach sich zöge. In den letzten Jahren sind Abweichungen von der gesetzlichen Nichtigkeitsfolge immer häufiger nur noch kursorisch begründet worden bis hin zu der lapidaren Angabe, eine zeitlich befristete Fortgeltung sei „noch hinnehmbar".

Dieser Praxis ist in der **Literatur** zu Recht mit vielfältigen Argumenten entgegen getreten worden.[149] Sie ist mit § 95 Abs. 3 BVerfGG allenfalls in Ausnahmefällen vereinbar, in denen zwingendes Verfassungsrecht einer Anwendung des § 95 Abs. 3 BVerfGG entgegen steht.[150] Mit dem Bundesverfassungsgericht kann man dies annehmen, wenn durch die Nichtigerklärung einer Norm ein Rechtszustand herbeigeführt würde, welcher der verfassungsmäßigen Ordnung noch weniger entspräche als die angegriffene Regelung. Ein solcher Fall liegt aber nur unter zwei Voraussetzungen vor: Erstens muss die Rechtsordnung ohne die angefochtene Norm verfassungswidrig sein („...der verfassungsmäßigen Ordnung noch weniger entspräche..."). Der Gesetzgeber muss also verfassungsrechtlich zu einer Neuregelung verpflichtet sein. Zweitens muss die Rechtsordnung ohne die angefochtene Norm noch weiter von der Verfassung entfernt sein als bei Geltung der Norm. Die angefochtene Norm muss also überwiegend von der Verfassung zwingend vorgegeben sein und sie nur zu einem kleineren Teil verletzen.

Ein solcher Fall liegt hier ersichtlich nicht vor. Die **Pflichten zur Identifizierung und Vorratsdatenspeicherung** nach den §§ 95 Abs. 3, 111 und 112 TKG sind nicht verfassungsrechtlich vorgegeben und verletzen die Grundrechte insgesamt. Die Folgen ihrer Nichtigerklärung sind problemlos tragbar. Noch bis vor wenigen Jahren kannte die deutsche

---

[145] Seite 18 oben.

[146] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 258 f.

[147] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 260.

[148] Beschwerdeschrift, 85 f.

[149] Bendixen, ZRP 2009, 85; Roth, NVwZ 2007, 754; Seer, NJW 1996, 285; Heußner, NJW 1982, 257.

[150] Ähnlich Roth, NVwZ 2007, 754 (756); Seer, NJW 1996, 285 (291); Heußner, NJW 1982, 257 (262).

Rechtsordnung keine Pflichten zur Identifizierung und Vorratsdatenspeicherung von Telekommunikationsdaten. In anderen westlichen Rechtsstaaten wie Österreich existieren vergleichbare Pflichten bis heute nicht, ohne dass die Telekommunikation dort etwa ein „rechtsfreier Raum" wäre.

Was die **Pflicht zur Auskunfterteilung über Teilnehmerdaten** nach § 113 TKG anbelangt, wird auch durch die Nichtigerklärung dieser Norm kein Rechtszustand herbeigeführt, welcher der verfassungsmäßigen Ordnung noch weniger entspräche als bei Fortgeltung des § 113 TKG. Die Rechtsordnung ist ohne eine Ermächtigung zu Eingriffen in das grundrechtlich geschützte Fernmeldegeheimnis nicht verfassungswidrig. Den Gesetzgeber trifft insbesondere keine Schutzpflicht dahin gehend, dass er verpflichtet wäre, staatlichen Stellen Eingriffe in das Fernmeldegeheimnis zu erlauben. Insoweit ist zu beachten, dass das Grundgesetz selbst anfänglich jeden solchen Eingriff in Art. 10 GG untersagt hat. Es hat zulässigerweise der freien Kommunikation aller den Vorrang vor dem möglichen Schutz oder der strafrechtlichen Verfolgung Einzelner eingeräumt. In ausländischen Staaten wie etwa Japan galt diese Rechtslage bis vor wenigen Jahren fort. Auch ohne jeden Eingriff in das Fernmeldegeheimnis ist eine den Schutzpflichten der Grundrechten und dem Rechtsstaatsprinzip genügende Gefahrenabwehr und Strafrechtspflege möglich. Dass für eine Übergangszeit der Zugriff auf Bestandsdaten versperrt, der Zugriff auf Verkehrs- und Inhaltsdaten aber eröffnet wäre, mag zwar einen Wertungswiderspruch darstellen, den sich der Gesetzgeber durch die ausufernde Gestaltung des § 113 TKG aber selbst zuzuschreiben hat und den er auch selbst wieder korrigieren kann.

Hielte man entgegen der hier vertretenen Auffassung den **Gesetzgeber in Ausnahmefällen für verfassungsrechtlich verpflichtet, Eingriffe in das Fernmeldegeheimnis zuzulassen**, so ginge § 113 TKG doch so weit über den verfassungsrechtlich gebotenen Mindeststandard hinaus, dass keine Rede davon sein kann, dass die Rechtsordnung ohne § 113 TKG noch weiter von der Verfassung entfernt wäre als bei Fortgeltung der Norm. Die Nichtigkeit des § 113 TKG ist auch nach dieser Auffassung noch immer der verfassungsnähere Zustand, zumal mit der Anonymität der Telekommunikation der Schutz kranker, ratsuchender oder bedrohter Menschen auf dem Spiel steht, die oftmals nur im Schutz der Anonymität zur Telekommunikation bereit sind.

Sollte das Hohe Gericht die hier vertretene Auffassung nicht teilen und einen kontinuierlichen staatlichen Zugriff auf Kommunikationsdaten für verfassungsrechtlich zwingend geboten erachten, so könnte die **Nichtigerklärung des § 113 TKG mit der Anordnung verbunden** werden, dass bis zum Inkrafttreten einer Neuregelung und längstens für die Dauer eines Jahres Zugriffsnormen für Verkehrsdaten auch auf Bestandsdaten anzuwenden sind und Zugriffsnormen für Telekommunikationsinhalte auch auf Schlüssel zum Zugriff auf Kommunikationsinhalte (z.B. Passwörter). Auf diese Weise könnte etwa zur Strafverfolgung nach Maßgabe der §§ 100a, 100g StPO weiterhin in angemessenem Maße auf Bestandsdaten zugegriffen werden, was den verfassungsrechtlichen Mindestanforderungen in jedem Falle gerecht würde. Dass der Gesetzgeber auch andere Regelungsmöglichkeiten haben mag, rechtfertigt es nicht, die Grundrechte in der Übergangszeit bis zu einer Neuregelung bis zur Grenze der verfassungsrechtlichen Zulässigkeit einzuschränken. Es kann nicht Aufgabe des Bundesverfassungsgerichts sein, eine vom Gesetzgeber zu weit gefasste Eingriffsnorm auf das verfassungsgemäße Maß zurückzuschneiden.[151] Das gilt erst recht, wenn der Gesetzgeber – wie hier – die Vorschrift bewusst unbestimmt gehalten und deshalb von einer entsprechenden Konkretisierung abgesehen hat.[152] Ein Absehen von der nach § 95 Abs. 3 BVerfGG gebotenen

[151] BVerfG, 1 BvR 2074/05 vom 11.3.2008, Absatz-Nr. 155.

[152] BVerfG, 1 BvR 2074/05 vom 11.3.2008, Absatz-Nr. 155.

Nichtigerklärung des § 113 TKG ist wegen der Möglichkeit einer verfassungsgerichtlichen Übergangsregelung nicht geboten.

Starostik
-Rechtsanwalt-