Kritik der Vorratsdatenspeicherung

von Prof. Dr. D. Klesczewski

Kriminalpolitisch betrachtet, begann das Jahr mit einem Silvesterböller: Am 1. Januar trat ein Gesetz[1] in Kraft, das die Speicherung von Verkehrsdaten, die z. B. beim Telefonieren oder beim Versenden einer Email anfallen, auf Vorrat zur Pflicht macht. Dies geschah, um eine EG-Richtlinie[2] umzusetzen. Der Gang der Gesetzgebung war von außergewöhnlichem öffentlichen Interesse begleitet[3], und bewog Zehntausende dazu bewog, Verfassungsbeschwerde einzulegen[4]. Neben einer grundlegenden Reform von § 100g StPO fügt diese Teile des Gesetzes §§ 113a, 113b in das TKG ein.[5] Die grundlegenden Regelungen, finden Sie auf der Rückseite meines Thesenpapiers Sie lauten:

> „Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten nach Maßgabe der Absätze 2 bis 5 sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern.“ (§ 113a Abs. 1 S. 1 TKG)
>
> „Der nach § 113a Verpflichtete darf die allein auf Grund der Speicherungsverpflichtung nach § 113a gespeicherten Daten
> 1. zur Verfolgung von Straftaten,
> 2. zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder
> 3. zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes
> an die zuständigen Stellen auf deren Verlangen übermitteln, soweit dies in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf § 113a vorgesehen und die Übermittlung im Einzelfall angeordnet ist; für andere Zwecke mit Ausnahme einer Auskunftserteilung nach § 113 darf er die Daten nicht verwenden.“ (§ 113b S. 1 TKG)

---

[1] Gesetzentwurf, BT-Drs. 16/5846, S. 9 ff.; Stellungnahme des Bundesrates, BR-Drs. 275/07 (B), S. 1 ff.; Beschlussempfehlung des Rechtsausschusses des Bundestages, BT-Drs. 16/6979, S. 8 ff.; der Bundesrat hat keinen Einspruch eingelegt, Bundesrat, Stenografischer Bericht, Plenarprotokoll 839, S. 397 ff. (399).

[2] Richtlinie 2006/24/EG über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt und verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EU 2006, Nr. L 105, S. 54 ff.

[3] Vgl. nur H. Prantl, in: Süddeutsche Zeitung Nr. 294 v. 21. Dezember 2007, S. 4, 6.

[4] Näheres unter: www.vorratsdatenspeicherung.de/content/view/51/70/lang,de; mittlerweile sind in dieser Sache (2 BvR 256/08) drei einstweilige Anordnungen ergangen, deren erste bereits in Fachzeitschriften veröffentlicht ist (NStZ 2008, 290), während die beiden anderen bei www.juris.de zum download bereit stehen.

[5] BGBl. I 2007, S. 3198.

Worum geht es?

Verkehrsdaten geben darüber Aufschluss, wer wann mit wem zu welcher Zeit und von welchem Ort aus telefoniert oder elektronisch kommuniziert hat. Sie sind namentlich für die Strafverfolgungsbehörden und die Polizei von besonderer Bedeutung, lassen sich mit ihnen doch Bewegungsbilder in der realen wie in der virtuellen Welt erstellen, sowie geschäftliche und freundschaftliche Kontakte ermitteln. Ihre Aufzeichnung und Aufbewahrung berührt daher den Schutzbereich des Fernmeldegeheimnisses und des Rechts auf informationelle Selbstbestimmung. Gemäß § 97 TKG war ihre Speicherung nach Beendigung der Verbindung bisher nur zulässig, soweit dies zu Abrechnungszwecken erforderlich war. Dementsprechend konnten sich die Auskunftsersuchen nach dem alten § 100g StPO nur auf diese Daten beziehen. Mit der Neuregelung werden nun bestimmte Anbieter von Telekommunikationsdiensteleistungen vom Staat in die Pflicht genommen, Verkehrsdaten auch dann vorzuhalten, wenn sie dieser selbst nicht bedürfen. Hierin ist eine Vorratsdatenspeicherung zu sehen, deren verfassungsrechtliche Zulässigkeit dieser Beitrag überprüfen möchte.

Zunächst komme ich auf die europarechtlichen Vorgaben zu sprechen, die der Novelle des TKG zugrunde liegen (I. A.). Sodann untersuche ich die europarechtliche Rechtmäßigkeit der Richtlinie (I. B.). Schließlich wende ich mich der Umsetzung in das deutsche Recht und deren verfassungsrechtlicher Zulässigkeit zu (II.). Ausblick auf Stand und Entwicklung der Verfahren vor dem EuGH und dem BVerfG (III.).

I. Der europarechtliche Rahmen

A. Die Art. 16-21 der Cybercrime-Convention[6] schreiben den Vertragsstaaten vor, sicherzustellen, dass bestimmte Daten der Telekommunikation zur Verfolgung der in der Konvention näher umschriebenen Computerstraftaten erhoben und verwendet werden können.[7] Nach einigem Hin und Her wurde zur Schaffung europaweit einheitlicher Regelungen die Richtlinie 2006/24/EG erlassen.[8]

Diese Richtlinie verpflichtet die Mitgliedsstaaten dazu, Maßnahmen zu treffen, damit die Diensteanbieter Verkehrs– und Standortdaten für mindestens sechs Monate zum Zwecke der Verfolgung von schweren Straftaten sechs Monate auf Vorrat speichern. In Art. 5 findet sich ein Katalog der vorzuhaltenden Daten Diese Daten sind freilich gemäß Art. 3 nur insofern zu speichern, soweit sie anfallen, wenn die betreffenden Kommunikationsdienste bereitgestellt werden. Schließlich stellt es Art. 12 den Mitgliedsstaaten frei, längere Speicherungsfristen oder auch die Speicherung anderer Datenarten vorzusehen.

---

[6] Übereinkommen über Computerkriminalität vom 23. November 2001, abrufbar unter: www.conventions.coe.int/Treaty/GER/Treaties/Html/185.htm; dazu: Breyer, DuD 2001, S. 592; Dix, DuD 2001, S. 588; Gerecke, Analyse des Umsetzungsbedarfs der Cybercrime Konvention – Teil 1, MMR 2004, S. 728.

[7] Näher: Gerecke, Analyse des Umsetzungsbedarfs der Cybercrime Konvention – Teil 2, MMR 2004, S. 801 (806).

[8] Näher: Breyer, Der staatliche Zugriff auf Telekommunikations-Bestandsdaten aus verfassungsrechtlicher Sicht, RDV 2003, 218; ders., StV 2007, S. 214 (215 f.); Gitter/Schnabel, Die Richtlinie zur Vorratsspeicherung und ihre Umsetzung in das nationale Recht, MMR 2007, S. 411; Hülsmann, Gegen EU-Vorratsdatenspeicherung - Stellungnahme des FiF e.V. und der DVD e.V. zur Vorratsdatenspeicherung für TK-Verkehrsdaten, DuD 2004, S. 734; Kühling, Freiheitsverluste im Austausch von Sicherheitshoffnungen im künftigen Telekommunikationsgesetz, K & R 2004, S. 105; Zöller, Vorratsdatenspeicherung zwischen nationaler und europäischer Strafverfolgung, GA 2007, S. 393.

B. Schon dieser Richtlinie ist nicht außer Streit. Gegen ihre formelle (1.) und materielle Rechtmäßigkeit (2.) bestehen durchgreifende Bedenken.

1. Bekanntlich folgt die Rechtssetzungskompetenz der EG dem Prinzip der begrenzten Einzelermächtigung. Insbesondere bedeutet dies, dass die Rechtssetzungsorgane der EG nur dort tätig werden dürfen, wo die EG-Verträge die Verbandskompetenzen der Gemeinschaften begründen.[9] Keine der im EGV zu findenden Spezialermächtigungen räumen ihr jedoch eine Kompetenz zur Regelung strafprozessualer Fragen ein.[10]

Für die Zuständigkeit der EG wird zwar geltend gemacht, zur Herstellung eines einheitlichen Binnenmarktes (Art. 95 Abs. 1 EGV) seien die Standards der Speicherung von Telekommunikationsdaten zu vereinheitlichen.[11] Dies ist jedoch nur dann zulässig, wenn bei den EG-Regelungen das Funktionieren des gemeinsamen Marktes im Vordergrund steht.[12] Die Richtlinie macht jedoch, wie dargestellt, lediglich Mindestvorgaben. Ein Harmonisierung kann von ihr daher weder erreicht werden, noch wird diese von ihr auch nur angestrebt.[13] Ferner lässt sich die Kompetenz nach Art. 95 Abs. 1 EGV auch nicht darauf stützen, es stehe eine Datenverarbeitung in Rede, die dazu diene, Dienstleistungen zu erbringen. Die Richtlinie erstreckt sich zwar nur auf Daten, welche die Diensteanbieter erheben, wenn sie Telekommunikation bereitstellen. Doch geht es ihr gerade darum, eine Pflicht zur Speicherung dieser Daten jenseits des Zeitraumes zu begründen, für den sie für

---

[9] Streinz, Europarecht, 7. Aufl., 2005, Rn. 436.
[10] Instruktiver Überblick über die Kompetenznormen mit Affinität zum Strafrecht bei Hecker, Europäisches Strafrecht,. 2. Aufl., 2007, § 8 Rn. 45-62.
[11] Vgl. die Juristische Analyse vom 23. 2. 2005, SEC (2005) 420, die für die Europäische Kommission erstattet wurde(abrufbar unter: www.statewatch.org/news/2005/apr/Commission-legal-opinion-data-rentention.pdf), bzw. das Rechtsgutachten des Juristischen Dienstes des Europäischen Rates vom 5. 4. 2005 (abrufbar unter: www.statewatch.org/news/2005/apr/Council -legal-opinion-data-rentention.pdf). Dazu auch BT-Drs. 16/5846, S. 29.
[12] EuGHE I 2002, S. 11453 (= EuGRZ 2003, S. 248); vgl. w. Oppermann, Europarecht, 3. Aufl., 2005, § 18 Rn. 17.
[13] Vgl. Breyer, StV 2007, S. 214 (215); Zöller, GA 2007, S. 393.

betriebliche Erfordernisse benötigt werden. Die Dinge liegen hier wie bei der Fluggastdatenübermittlung an die USA. Den zur Regelung dieser Materie ergangenen Beschluss des Europäischen Rates hat der EuGH vor kurzem wegen fehlender Kompetenz für nichtig erklärt.[14] Was dort festgestellt wurde, muss auch hier gelten.

Ferner lässt sich die Zuständigkeit der EG auch nicht aus einer Annexkompetenz herleiten. Daran ließe sich nur denken, wenn die Speicherung von Telekommunikationsdaten bereits durch Richtlinien umfassend gemeinschaftsrechtlich geregelt wäre. Hier kommt allenfalls die Datenschutzrichtlinie[15] in Betracht. Diese Richtlinie stellt es aber den Mitgliedsstaaten gerade frei, ob sie eine Vorratsdatenspeicherung einführen wollen oder nicht. Damit bezweckt sie nicht, restriktive nationalstaatliche Regelungen unter Änderungsvorbehalt zu stellen. Eine derartige Auslegung dieser Regelung würde nicht zuletzt auf kompetenzrechtliche Probleme stoßen. Eine Ermächtigung zu einer solchen Vorratsdatenspeicherung zu den genannten Zwecken wäre nämlich der sog. „Dritten Säule"[16] zuzurechnen. Wie sich aus Art. 47 EUV ergibt, haben die Mitgliedstaaten hier jedoch keine Kompetenzen übertragen.[17] Dies berücksichtigt auch die Datenschutzrichtlinie selbst. Ihr Erwägungsgrund 11 stellt ausdrücklich fest, dass sie keine Auswirkungen hat auf das bestehende Gleichgewicht zwischen staatlichen Interessen und der Privatsphäre des Einzelnen. Die Datenschutzrichtlinie will daher lediglich nicht verbieten,

[14] EuGHE I 2006, S. 4721 (= NJW 2006, S. 2029) m. zust. Bespr. Simitis, NJW 2006, S. 2011 (2012); ebenso: Alvaro, Positionspapier zur Einführung einer Vorratsdatenspeicherung, RDV 2005, S. 47**;** Westphal, Die neue EG-Richtlinie zur Vorratsdatenspeicherung, EuZW 2006, S. 555 (557).
[15] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. 7. 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie); ABl. EG 2002. Nr. 201, S. 37 ff.
[16] Art. 29 ff. EUV.
[17] Böse, in: Schwarze, EU-Kommentar, 2002, Art. 29 EUV Rn. 8.

dass ein Mitgliedstaat unter Beachtung bestimmter Voraussetzungen eine Vorratsdatenspeicherung einführt.[18]

An dieser Kompetenzabgrenzung hat sich schließlich auch nichts durch das Urteil des EuGH[19] geändert, mit dem er den Rahmenbeschluss über den Schutz der Umwelt durch das Strafrecht[20] für nichtig erklärte.[21] Zwar geht der EuGH in seiner Entscheidung davon aus, dass in der in Art. 175 EGV enthaltenen Zuständigkeit für den Umweltschutz auch die Kompetenz enthalten sei, die Mitgliedsstaaten zum Erlass von Strafrechtsnormen auf diesem Rechtsgebiet anzuweisen. Doch setzt er damit lediglich seine Judikatur fort, mit denen er die Mitgliedsstaaten zur Durchsetzung von Gemeinschaftsrecht auch dazu verpflichtet, wirksame, abschreckende und verhältnismäßige Sanktionen vorzusehen.[22] Diese Rechtsprechung bezieht sich stets auf eine Rechtsmaterie, für welche die EG eine Einzelermächtigung besitzt, und folgert aus der Pflicht zu effektiver Umsetzung die Notwendigkeit zum Erlass von Strafnormen. Sie ist materiell rechtlich gedacht. Das Vorhalten von Verkehrsdaten zum Abruf für Strafverfolgungsbehörden ist dagegen eine strafverfahrensrechtliche Regelung. Strafprozesse werden aber wegen jedweder Tat durchgeführt, einerlei, ob deren Strafbarkeit auf der Umsetzung von Europarecht beruht oder nicht. Eine Anweisung zum Erlass bestimmter strafprozessualer Zwangsbefugnisse würde daher das Prinzip der begrenzten

[18] Wie hier: Hoeren, Recht der Access-Provider, 2004, Rn. 122 f.; a. A. wohl Ohlenburg, Die neue EU-Datenschutzrichtlinie 2002/58/RG – Auswirkungen und Neuerungen für elektronische Kommunikation, MMR 2003, S. 82 (86), die (sogar) einen Kompetenzverstoß annimmt.

[19] EuGHE I 2005, 9315 (= NVwZ 2005, S. 1289) m. krit. Anm. Heger, JZ 2006, S. 310; Wegener/Greenawalt, ZUR 2005, S. 585; krit. Bespr. Hefendehl, ZIS 2006, S. 161; Pohl, ZIS 2006, S. 213; kritisch ferner: Kaiafa-Gbandi, Aktuelle Strafrechtsentwicklung in der EU und rechtsstaatliche Defizite, ZIS 2006, S. 521; zust. dagegen: Böse, Strafe und Sanktionen im Europäischen Recht, GA 2006, S. 211; Diehm, Die „safe-harbour" Verordnung und das Urteil des EuGH zum Rahmenbeschluss über den Schutz der Umwelt durch das Strafrecht, wistra 2006, S. 366.

[20] Rahmenbeschluss über den Schutz der Umwelt durch das Strafrecht, ABl. EG 2003, L 29, S. 55 ff.

[21] So aber die Bundesregierung, BT-Drs. 16/5846, S. 29.

[22] EuGHE I 1989, 2965 (=EuZW 1990, S. 99) m. Anm. Bleckmann, WuR 1991, S. 285; Tiedemann, EuZW 1990, S. 100.

Einzelermächtigung sprengen. Zur Regelung einer Vorratsdatenspeicherung fehlt der EG daher die Kompetenz.

2. Die Richtlinie verletzt aber zudem den Schutzbereich von Art. 8 EMRK. Art. 8 Abs. 1 beinhaltet sowohl den Datenschutz[23] als auch das Fernmeldegeheimnis.[24] Die Erhebung und Speicherung von Verbindungsdaten ohne Einwilligung des Betroffenen berührt damit den Schutzbereich von Art. 8 Abs. 1 EMRK.[25]

Zwar kann ein Eingriff gemäß Art. 8 Abs. 2 EMRK gerechtfertigt sein. Geht es um das Sammeln und Speichern von Informationen, stellt der EGMR hier besondere Anforderungen an die Gesetzesgrundlage. Insbesondere muss sie die Art zu speichernden Informationen und die Verwendungszwecke detailliert festlegen.[26] Erforderlich ist eine Maßnahme in einer demokratischen Gesellschaft nur, wenn in Anbetracht des Stellenwerts des garantierten Freiheitsrechts „ a pressing social need“ nach ihr besteht, sie einen legitimen Zweck verfolgt und ihre Belastungsintensität nicht außer Verhältnis dazu steht.[27] Zwar dienen strafprozessuale Zwangsmaßnahmen einem legitimen Ziel[28]. Die besondere Problematik der Vorratsdatenspeicherung besteht jedoch darin, dass es an einem Bezug zu einem konkreten Strafverfahren fehlt. Dementsprechend war das Europäische Parlament bei den Beratungen der Datenschutzrichtlinie noch davon ausgegangen, dass eine ausnahmslose elektronische Erfassung von

---

[23]EGMR Leander vs. Sweden, 26. 3. 1987 Series A no. 116; eingehend: Villiger, Handbuch der Europäischen Menschenrechtskonvention (EMRK) unter besonderer Berücksichtigung der schweizerischen Rechtslage, 2. Auflage 1999; Rn. 555.

[24]Zum Schutz der Vertraulichkeit der Telekommunikation: EGMR, Klass vs. Deutschland, v. 6. 9. 1978 Series A no. 28(= NJW 1979, S. 1755, 1756 ff.); Malone vs. United Kingdom, v. 2. 8. 1984 Series A no. 82 (=EuGRZ 1985, S. 17); P: G. u. J. H. Nr. 44787/98 v. 25. 9. 2001, RJD 2001-IX, Ziffer 42. (st. Rspr.); näher: Grabenwarter, Europäische Menschenrechtskonvention, 2.Aufl., 2005, § 22 Rn. 10, 24.

[25] EGMR, EuGRZ 1985, S. 17 (23).

[26] EGMR, Rotaru vs. Rumänien, Urt. v. 4. 5. 2000, RJD 2000-V, Ziffer 57; EGMR, Weber u. Saravia vs. Deutschland, Urt. v. 29. 6. 2006, NJW 2007, S. 1433; vgl. w. Grabenwarter, Europäische Menschenrechtskonvention, 2. Aufl., 2005, § 22 Rn. 35.

[27]Oppermann, Europarecht, 3. Aufl., 2005, § 2 Rn. 39.

[28] EGMR, Dudgeon, Urt. v. 22. 10. 1981, Serie A 45, Ziffer 49, 62; EGMR, Kruslin, Urt. v. 24. 4. 1990, Serie A 176-A, Ziffer 30 ff.; dazu: Grabenwarter, Europäische Menschenrechtskonvention, 2. Aufl., 2005, § 22 Rn. 34.

Telekommunikationsdaten von der Rechtsprechung des EGMR als unzulässig angesehen wird, wenn nicht wegen einer bestimmten Tat ermittelt wird.[29] Das gilt auch heute noch: Die Richtlinie verstößt daher gegen gegen Art. 8 Abs. 2 EMRK.[30]

3. Die von Irland vor dem EuGH gegen die Richtlinie 2006/24/EG angestrengte Nichtigkeitsklage[31] wird daher aller Voraussicht nach Erfolg haben.

Bis dahin ist der Stand so:
Auf die eingangs genannte Verfassungsbeschwerde hin hat das BVerfG eine einstweilige Anordnung erlassen, die es in weiteren Beschlüssen verlängert und ausgeweitet hat.[32]
Danach gilt bis au Weiteres: Die verpflichteten Diensteanbieter müssen zwar die in § 113a genannten Verkehrsdaten für sechs Monate speichern. Auf ein Auskunftsersuchen hin dürfen sie aber nur zum Zwecke der Verfolgung der in § 100a StPO genannten Straftaten bzw. (in Bayern) zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr erforderlich ist. Im Hauptsacheverfahren wird das BVerfG erst entscheiden, wenn der EuGH entschieden hat. Hier liegt immerhin schon der Schlussantrag des Generalanwalts vor.

---

[29] Ausschuss des Europäischen Parlaments für die Freiheiten und Rechte der Bürger, Justiz und innere Angelegenheiten: Zweiter Bericht betreffend den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, 24. 10. 2001, Dok.-Nr. A5-0374/2001, Abänderung 4; Artikel-29-Gruppe der EU, Überwachung, 5.

[30] Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder, Stellungnahme zur Anhörung der Europäischen Kommission Public Consultation on data retention, DuD 2004, S. 603.

[31] EuGH, Az: C-301/06; zitiert nach Breyer, StV 2007, S. 214 (215); Schlussanträge des Generalanwalts unter http://eur-lex.europa.eu.

[32]

III. Die Grundgesetzwidrigkeit des Umsetzungsgesetzes

A. Grundrechte der Nutzer von Telekommunikationsanlagen

1. Das Auskunftsverfahren nach den §§ 113a, 113b TKG hat Verkehrsdaten zum Gegenstand. Bei ihnen handelt es sich um Umstände einer individuellen Telekommunikation. Deren Speicherung auf Vorrat und deren Mitteilung an Dritte berührt den Schutzbereich von Art. 10 GG.[33] Die öffentliche Gewalt soll grundsätzlich nicht nur nicht die Möglichkeit haben, sich Kenntnis vom Inhalt des über Fernmeldeanlagen geführten individuellen Informations- und Gedankenaustauschs zu verschaffen.[34] Das Fernmeldegeheimnis nach Art. 10 GG umfasst auch die Umstände der Kommunikation. Ob, wann und wie oft zwischen welchen Personen oder Fernmeldeanschlüssen Telekommunikation stattgefunden hat oder versucht worden ist, alles dies sind Tatsachen, die in das Fernmeldegeheimnis fallen.[35] Geschützt sind also vor allem die Verkehrsdaten.[36] Indem das Grundrecht die einzelnen Kommunikationsvorgänge grundsätzlich dem staatlichen Zugriff entzieht, will es die Bedingungen einer freien Telekommunikation überhaupt aufrechterhalten. Ein Meinungs- und Informationsaustausch mittels Fernmeldeanlagen soll nicht deswegen unterbleiben oder nach Form und Inhalt verändert verlaufen, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder -inhalte gewinnen.[37]

Zwar geht das BVerfG grundsätzlich davon aus, dass gespeicherte Verkehrsdaten nach Abschluss des Übertragungsvorgangs nicht mehr in das Fernmeldegeheimnis

---

[33] Vgl. BerlKommTKG/Klesczewski, § 88 Rn. 14 ff.
[34] BVerfGE 67, 157 (172); 100, 313 (358); m. Anm. Arndt, NJW 2000, S. 47.
[35] BVerfGE 67, 157 (172); 85, 386 (396).
[36] Wuermeling/Felixberger, Staatliche Überwachung der Telekommunikation, CR 1997, S. 230 (234); zust. BeckTKG-Komm/Bock, 3. Aufl., 2006,3. Aufl., 2006, § 88 Rn. 14.
[37] BVerfGE 100, 313 (314).

fallen.[38] Doch gilt dies nur, wenn diese sich im Herrschaftsbereich des betroffenen Kommunikationsteilnehmers befinden.[39] Da die Verkehrsdaten durch die Verpflichtungen aus § 113a TKG gerade im Herrschaftsbereich des Dienstanbieters verbleiben, sind sie auch nach Abschluss der Verbindung von Art. 10 Abs. 1 GG geschützt.

2. Die §§ 113a, 113b TKG verletzen Art. 10 GG. Zwar ist das Fernmeldegeheimnis mit einem Gesetzesvorbehalt versehen. Doch ist aus dem Verhältnismäßigkeitsprinzip abzuleiten, dass die Vertraulichkeit der Telekommunikation nur bei besonders wichtigen Gemeinschaftsinteressen, namentlich der Abwehr schwerer Gefahren für den Bestand der Bundesrepublik oder eines Landes, bzw. zur Verfolgung von Straftaten die unmittelbar die Existenz des Einzelnen oder unseres Gemeinwesens als Ganzes in Frage stellen.[40] Schon gemessen hieran ist fraglich, ob die §§ 113a, 113b TKG verfassungsrechtlichen Anforderungen standhalten. lassen sie doch die Speicherung und Mitteilung zum Zwecke der Verfolgung jedweder Straftat zu, § 113b S. 1 Nr. 1 TKG. Zwar setzt § 100g StPO den Verdacht einer Straftat vor erheblicher Bedeutung voraus, namentlich einer Katalogtat i. S. v. § 100a StPO. Schon hier kann man fragen, ob es sich bei jedem der dort aufgezählten Vergehen oder Verbrechen um derart schwere Straftaten handelt und wodurch die unbenannten Straftaten von erheblicher Bedeutung eigens gekennzeichnet sind[41]. Ausschlaggebend ist aber, dass § 100g StPO Abs. 2 S. 1 Nr. 2 StPO die Abfrage von Verkehrsdaten wegen jeder Straftat zulässt, soweit diese mittels Telekommunikation begangen worden ist.[42]

---

[38] BVerfGE 115, 166.
[39] Vgl. BerlKommTKG/Klesczewski, § 88 Rn. 13.
[40] BVerfGE 67, 157; 107, 299; dazu: Klesczewski, Das Auskunftsersuchen an die Post: die wohlfeile Dauerkontrolle von Fernmeldeanschlüssen? In: StV 1993, S. 382; vgl. w. Breyer, StV 2007, S. 214 (217).
[41] Kritisch hierzu: Breyer, StV 2007, S. 214 (217).
[42] BVerfG, NJW 2006, S. 3197 (3199) hält freilich diese Klausel auch für zulässig, soweit die Verhältnismäßigkeit im Einzelfall gewahrt wird.

Dem lässt sich nicht entgegen halten, es gehe nicht um die Inhalte, sondern nur um die Umstände einer Telekommunikation. Wie das Bundesverfassungsgericht immer wieder hervorgehoben hat, gibt es unter den Bedingungen elektronischer Datenverarbeitung kein belangloses Datum mehr.[43] Vielmehr steigt die Schutzwürdigkeit einer personenbezogenen Information mit den Verwendungsmöglichkeiten, die sie anderen bietet. Dabei enthalten gerade die Verkehrsdaten teilweise ein Potenzial an Verarbeitungsweisen (automatische Analyse, Abgleich mit anderen Datenbeständen), die manch ein Inhaltsdatum gar nicht an sich hat.[44] Verkehrsdaten lassen in zunehmendem Maße Rückschlüsse auf Art und Intensität von Beziehungen, auf Interessen, Gewohnheiten und Neigungen und nicht zuletzt anhand der Zielrufnummer auch auf den jeweiligen Kommunikationsinhalt zu und vermitteln - je nach Art und Umfang der angefallenen Daten - Erkenntnisse, die an die Qualität eines Persönlichkeitsprofils heranreichen können.[45] Nimmt man noch hinzu die Möglichkeit von Auskunftsersuchen anderer Behörden[46] oder Privater[47] hinzu, dann stehen die nach § 113a TKG gespeicherten Daten nahezu jedwedem Zweck zur Verwendung offen. § 113a Abs. 1 TKG führt daher zu einer Vorratsdatenspeicherung, die das Bundesverfassungsgericht bisher außerhalb statistischer Zwecke als verboten ansieht.[48]

[43] BVerfGE 65, 1 (45).
[44] Breyer, StV 2007, S. 214 (217).
[45] BVerfGE 115, 166.
[46] §§ 12 ff. EGGVG.
[47] § 406e StPO
[48] BVerfGE 65, 1 (42); und dezidiert neuerdings: BVerfGE 115, 320; vgl. w. Zöller, GA 2007, S. 393.

B. Grundrechte der Diensteanbieter.

Die Verpflichtung, bestimmte Kundendaten selbst dann zu erheben und zu speichern, wenn dazu keine betriebliche Notwendigkeit besteht, stellt eine Indienstnahme Privater für hoheitliche Zwecke dar (1.).[49] Diese ist nur dann zulässig, wenn es ein besonderer Zurechnungsgrund gegeben ist (2.).

1. Die Verpflichtung zur Vorhaltung einer Verkehrsdatenbank für staatliche Abfragen auf eigene Kosten stellt eine Indienstnahme Privater für hoheitliche Zwecke dar.[50] Darin liegt ein Eingriff in die nach Art. 12 Abs. 1 GG geschützte Berufsausübungsfreiheit.[51] Zwar verfolgt die gesetzliche Verpflichtung zur Speicherung der Verkehrsdaten vernünftige und sachgerechte Belange des Gemeinwohls[52]. Sie dient nämlich den Zwecken der Strafverfolgung und der Gewährleistung der Sicherheit des Staates, beides Gemeinwohlbelange mit Verfassungsrang.[53] Nicht unbestritten ist aber schon, ob die Indienstnahme für den Staat das mildeste geeignete Mittel darstellt, diese öffentliche Aufgabe zu erfüllen.

2. Lässt man die gegen die Effizienz[54] und die Erforderlichkeit[55][56] der Vorratsdatenspeicherung erhobenen

---

[49]Vgl. v. Hammerstein, Kostentragung für staatliche Überwachungsmaßnahmen nach der TKG-Novelle, MMR 2004, S. 222 (223/227); Wuermeling/Felixberger, CR 1997, S. 555 (561); Bedenken auch bei: BeckTKG-Komm/Bock, 3. Aufl., 2006, § 111 Rn. 21.

[50]v. Hammerstein, MMR 2004, S. 222 (223); BeckTKGKomm/Bock, 3.Aufl., 2006, § 110 Rn. 16; Koenig/Koch/Braun, Die Telekommunikationsüberwachungsverordnung: Neue Belastungen für Internet Service Provider und Mobilfunknetzbetreiber? Zugleich ein Beitrag zur Verfassungsmäßigkeit des § 88 TKG, K & R 2002, S. 289 (294); Manssen/Haß, Telekommunikations- und Multimediarecht, Stand: 2006**,** § 88 Rn. 40.

[51]BVerfGE 30, 292 (313); 68, 155 (170); zust. Maunz/Dürig/Scholz, Grundgesetz Kommentar, Stand Juni 2007, Art. 12 Rn. 146; ebenso: BeckTKG-Komm/Bock, 3. Aufl., 2006, § 110 Rn. 16; Koenig/Koch/Braun, K & R 2002, S. 289 (294); Manssen/Haß, Telekommunikations- und Multimediarecht, Stand: 2006**,** § 88 Rn. 39.

[52]Zu dieser Voraussetzung: BVerfGE 7, 337; 30, 292 (351 f.); 33, 240 (244); 68, 155 (171); näher: Breuer, in: Isensee/Kirchhof, Handbuch des Staatsrechts Bd. VI, 2. Aufl., 2001, § 148 Rn. 20.

[53]BVerfGE 49, 24 (56 f.); BVerfG, NJW 2003, S. 1787 (1789); BeckTKG-Komm/Ehmer, 2. Aufl., 2000, § 88 Rn. 47.

[54] Breyer, StV 2007, S. 214 (217 f.).

[55]Vgl. *v. Hammerstein*, MMR 2004, S. 222 (224); *Kube/Schütze*, Die Kosten der TK-Überwachung, CR 2003, S. 663 (666); *Schenke*, AöR 125 (2000), S. 1 ff.; *Scholz*, ArchivPT 1995, S. 169 (185); BeckTKG-Komm/*Bock*, 3. Aufl., 2006, § 110 Rn. 15.

[56] BT-Drs. 16/5846, S. 50.

Bedenken mal beiseite, so steht jedenfalls fest, dass diese Indienstnahme Privater unzumutbar ist. Die Vorhaltung von Verkehrsdatenbanken belastet die betroffenen Anlagenbetreiber in erheblichem Ausmaß. Sowohl die Ausweitung der Kundendateien[57] als auch die Vorratsdatenspeicherung[58] führt jeweils zu einem Mehraufwand in mehrstelliger Millionenhöhe. Zwar haben die Diensteanbieter das Recht, die dadurch entstehenden finanziellen Belastungen auf ihre Kunden abzuwälzen.[59] Doch folgt daraus nicht ohne weiteres, dass es jedem Anlagenbetreiber auch gelingt, seine Preise am Markt durchzusetzen. Dies gilt umso mehr dort, wo ein Unternehmen mit einem Wettbewerber mit beträchtlicher Marktmacht – Stichwort Telekom - zu konkurrieren hat. Die Kostenabwälzung ist nicht jedem Diensteanbieter in gleicher Weise möglich. Je nach Größe des Anbieters und der Art seines Angebots führen die Implementierungskosten daher zu unterschiedlich großen Preisaufschlägen.[60] Dies führt zu Wettbewerbsverzerrungen, die dem Hauptzweck von § 1 TKG widersprechen.[61] Schließlich darf es nach dem BVerfG bei der verfassungsrechtlichen Beurteilung von Eingriffen nicht darauf ankommen, ob es dem Betroffenen gelingt, sich an anderer Stelle schadlos zu halten.[62]

Vielmehr dürfte der Staat die Abwälzung auf die Kunden nur zulassen, wenn ein besonderer Zurechnungsgrund für die Kostentragungspflicht besteht.[63] Daran fehlt es aber letztlich. Einen solchen Grund sieht das BVerfG zum einen in einer

---

[57]Vgl. BT-Drs. 15/2679, S. 6 f.; Ausschuss-Drs. 15(9)/949, S. 33.
[58] Breyer, StV 2007, S. 214 (216).
[59]VG Köln CR 2000, S. 747 (750); krit. BeckTKG-Komm/Bock, 3. Aufl., 2006, § 110 Rn. 21 m. w. N.
[60]Näher: Koenig/Koch/Braun, K&R 2002, S. 289 (297); vgl. v. Hammerstein, MMR 2004, S. 222 (226); Kube/Schütze, CR 2000, S. 663 (669).
[61]So auch: BeckTKG-Komm/Ehmer, 2. Aufl., 2000, § 88 Rn. 79; vgl. w. BeckTKG-Komm/Bock, 3. Aufl., 2006,§ 110 Rn. 14.
[62]BVerfGE 58, 137 (151); so auch Schmidt-Preuß, Kurzgutachten über „Die verfassungsrechtliche Anforderungen an die Entschädigung für Leistungen der Telekommunikations-Überwachung und Auskunftserteilung, 2005, S. 29. (abrufbar unter: www.bitkom.org)
[63]BGH NJW 1997, S. 574 (578).

besonderen Sach- und Verantwortungsnähe des Betroffenen[64], zum anderen in der der Nähe der zu übernehmenden Aufgabe zur Tätigkeit des Unternehmens und der Geringfügigkeit der Belastung.[65] Beides trifft auf die Vorhaltung einer Verkehrsdatenbank durch die betroffenen Netzbetreiber nicht zu:[66]

Zum einen sind alle Diensteanbieter nach § 88 Abs. 2 S. 1 TKG zur Wahrung des Fernmeldegeheimnisses verpflichtet. Hierzu gehört es auch, die Kenntnisnahme von Umständen einer individuellen Telekommunikation tunlichst vermeiden. Zu diesen Umständen zählen – wie dargelegt – auch die Verkehrsdaten. Anders als die Aufzeichnung der Inhalte eines Ferngesprächs stellt zwar die Erhebung und Verwendung von Verkehrsdaten keine schlechthin unternehmensfremde Tätigkeit dar. Denn es bedarf ja derselben, um überhaupt Fernmeldeverkehr vermitteln und abrechnen zu können. Doch ist hierbei der Grundsatz der Datensparsamkeit zu beachten.[67]

Aufgrund dessen lässt sich auch keine Parallele zur Pflicht zur Mineralölbevorratung ziehen, Gegenstand des „leading cases“ des BVerfG zu dieser Frage.

Wenngleich es hier wie dort zur unternehmerischen Tätigkeit gehört, Dinge (hier Daten, dort: Öl) aufzubewahren, so folgt daraus nicht, dass beides normativ gleichsteht. Während es für die Ölindustrie ökonomisch förderlich und rechtlich zulässig ist, Bevorratung zu betreiben, ist es den Anbietern von Telekommunikationsdienstleistungen strikt untersagt, beliebige Datensammlungen anzulegen. Das normative Bild ihrer

---

[64]BVerfGE 75, 108 (159); 77, 308 (337); 81, 156 (197 f.); 85, 226 (237); Albrecht, Zumutbarkeit als Verfassungsmaßstab, 1995, S. 176 f.; Breuer, in: Isensee/Kirchhof (Hrsg.): Handbuch des Staatsrechts, Bd. VI, 2. Aufl., 2001, § 148 Rn. 28.
[65]BVerfGE 22, 380; 30, 292; 44, 103; 57, 139; 95, 173.
[66] So auch BeckTKG-Komm/Bock, 3. Aufl., 2006, § 110 Rn. 18 f., der von fehlender Gruppenverantwortung und Gruppennützigkeit spricht.
[67] BerlKommTKG/Klesczewski, § 91 Rn. 23.

unternehmerischen Tätigkeit wird durch § 97 Abs. 3 TKG vorgegeben. Danach sind nur die Verkehrsdaten zu speichern, die zur Abrechnungszwecken benötigt werden, und selbst diese sind so schnell wie möglich, spätestens aber sechs Monate nach Rechnungslegung zu löschen.[68] Nicht zuletzt ist eine längere Speicherung dieser Daten, wie dargelegt, ja auch mit erheblichem finanziellen Aufwand verbunden.[69]

Zum anderen stellen Strafverfolgung und Gefahrenabwehr originär staatliche Aufgaben dar.[70] Es besteht keine besondere Sach- und Verantwortungsnähe der betroffenen Netzbetreiber, den Behörden bei Erfüllung dieser Aufgaben behilflich zu sein. Dies ergibt sich nicht schon daraus, dass Telekommunikationsnetze zur Begehung von Straftaten genutzt werden können.[71] Das trifft auf eine Vielzahl anderer Dienstleistungen auch zu. Sie folgt ferner nicht aus dem Umstand, dass die Netzbetreiber auch potenziellen Verbrechern ein Medium zur Verfügung stellen.[72] Der Betrieb eines Telekommunikationsnetzes ist neutral. Für die möglicherweise strafbaren Inhalte eines Ferngesprächs ist der Netzbetreiber nicht verantwortlich.[73] Nicht zuletzt verbietet die Gewährleistung des Fernmeldegeheimnisses es den Diensteanbietern geradezu, von den Inhalten eines Ferngesprächs Kenntnis zu nehmen, § 88 Abs. 3 S. 1 TKG.[74] Dann aber kann von einer besonderen Sach- und Verantwortungsnähe der Diensteanbieter für diese möglicherweise kriminellen Gegenstände einer solchen Kommunikation nicht die Rede sein.

---

[68] BerlKommTKG/Klesczewski, § 97 Rn. 10 m. w. N.
[69] v. Hammerstein, MMR 2004, S. 222 (225); Holznagel/Bysikiewicz/Enaux/Nienhaus/Hermeter, Telekommunikationsrecht, 1. Aufl., S. 178 (197 f.).
[70] Schenke, Verfassungsrechtliche Probleme einer präventiven Überwachung der Telekommunikation, AöR 125 (2000), S. 1 (39); Scholz, Zur Kostenerstattungspflicht des Staates für gesetzliche Maßnahmen der Telefonüberwachung, ArchivPT 1995, S. 169 (170 f.); BeckTKG-Komm/Bock, 3. Aufl., 2006, § 110 Rn. 18; Götz, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. IV, 3. Aufl., 2006, § 85 Rn. 1 ff.
[71] So aber: Manssen/Haß, § 88 Rn. 47.
[72] So aber: Waechter, Bereitstellungspflicht für Fernmeldeanlagenbetreiber, VerwArch 87 (1996), S. 68 (82).
[73] v. Hammerstein, MMR 2004, S. 222 (225); Koenig/Koch/Braun, K & R 2002, S. 289 (295); zust. BeckTKG-Komm/Bock,§ 110 Rn. 18; a. A. Manssen/Haß, § 88 Rn. 46 f.
[74] Vgl. BVerfGE 85, 386; 107, 299; 115, 166 (189).

Die Sach- und Verantwortungsnähe folgt schließlich auch nicht daraus, dass der Staat durch die Privatisierung des Fernmeldewesens den Diensteanbietern die wirtschaftliche Betätigung erst ermöglicht hat.[75] Zwar trifft es zu, dass nicht nur die Deutsche Bundespost, sondern auch ihre Nachfolgerin, die Deutsche Telekom AG, die Überwachungskosten zu tragen hatte. Doch stand die Monopolisierung des Fernmeldewesens beim Staat in keinem Zusammenhang mit der Gewährleistung der Telefonüberwachung.[76] Folglich ist es auch nicht zwingend, durch die Privatisierung einer Aufgabe der Daseinsvorsorge, hier den Bereich der Telekommunikation, die Unternehmen zugleich auch noch für die hoheitliche Aufgabe der Gefahrenabwehr und Strafverfolgung in Dienst zu nehmen.

Fehlt es für Pflicht zur Vorhaltung einer Verkehrsdatenbank an dem erforderlichen besonderen Zurechnungsgrund, so stellt sie eine Indienstnahme Privater dar, welche nur dann verhältnismäßig ist, wenn der Staat eine Entschädigung leistet.[77] Da § 113a TKG eine Entschädigung bewusst nicht vorsieht[78], ist er als verfassungswidrig anzusehen. Das zieht die Verfassungswidrigkeit der darauf bezogenen Auskunftsverfahren nach § 113b TKG nach sich.

IV. Fazit

Der Silvesterböller, den der Gesetzgeber gezündet hat, hat sich daher leider als Rohrkrepierer erwiesen.

[75]So VG Köln CR 2000, 747; zuvor schon: Manssen, Das Telekommunikationsgesetz (TKG) als Herausforderung für die Verfassungs- und Verwaltungsdogmatik, ArchivPT 1998, S. 236 (242); Waechter, VerwArch. 87 (1996), S. 68 (94).
[76]Jeserich/Pohl/v. Unruh/Schilly, Deutsche Verwaltungsgeschichte, Bd. II, 1983, S. 257 (277).
[77]BVerfGE 33, 240 (244 f.); 85, 329 (334 f.); beide zur Sachverständigenentschädigung nach dem ZSEG.
[78] BT-Drs. 16/5846, S: 30.