MASTER THESIS

zur Erlangung des akademischen Grades

MASTER OF LAWS (LL.M.)

Informationsrecht und Rechtsinformation

AN DER UNIVERSITÄT WIEN

(UNIVERSITÄTSLEHRGANG FÜR INFORMATIONSRECHT UND RECHTSINFORMATION)

Vorgelegt von: Mag. Michael Binder

Begutachtet von: ao. Univ.Prof. Dr. JAHNEL Dietmar

Meinen Eltern

"Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."

Benjamin Franklin, 1706 – 1790

Inhaltsverzeichnis

I. Literaturverzeichnis 6
II. Abkürzungsverzeichnis 8
III. Anmerkungen 8

1. Einleitung 9
1.1. Die Richtlinie 2006/24/EG 9
1.2. Der Kampf gegen den internationalen Terrorismus und die organisierte Kriminalität 9
1.3. Umkehr der Unschuldsvermutung 10
1.4. Bewegungsprofile – Rückschlüsse auf den Inhalt einer Kommunikation 11
1.5. Data-Mining 11
1.6. Reaktionen zur Novelle des Telekommunikationsgesetzes 2003 12
1.7. Fehlende Kostenregelung 13
1.8. Strittige Kompetenzgrundlage 13
1.9. Europäische Reaktionen 13
2. Richtlinie 2006/24/EG 14
2.1. Allgemeines 14
2.2. Daten natürlicher und juristischer Personen 14
2.3. Kategorien von auf Vorrat zu speichernden Daten 15
2.4. Speicherfristen 15
2.5. Datenschutz und Datensicherheit 16
2.6. Sanktionen 16
2.7. Fazit 16
3. Historischer Hintergrund der Richtlinie 16
3.1. Terroranschläge in New York City, Madrid und London 16
3.2. Schlußfolgerungen des Rates in Brüssel vom 20 September 2001 17
3.3. Erklärung zum Kampf gegen den Terrorismus 17

3.4. Rahmenbeschluss vom 28. April 2004 17
3.5. Exkurs - Die dritte Säule 18
3.6. Bericht des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments 19
3.7. Schlußfolgerungen des Vorsitzes vom 15. Juli 2005 22
3.8. Entwurf der Richtlinie 2006/24/EG (Vorratsdatenrichtlinie) 22
4. Kompetenzgrundlage zur Erlassung der Vorratsdatenrichtlinie 24
4.1. Prinzip der begrenzen Einzelermächtigung 24
4.2. Art 95 EGV 24
4.3. Klage Irlands 26
5. Die Rechtslage in Österreich vor der Vorratsdatenspeicherung 30
5.1. Datenschutzgesetz 2000 und Telekommunikationsgesetz 2003 30
5.2. Datenarten 31
5.3. Datenschutz nach dem Datenschutzgesetz 2000 33
5.4. Datenschutz nach dem Telekommunikationsgesetz 2003 34
5.5. Kommunikationsgeheimnis 36
5.6. Auskunftspflichten nach der bisherigen Rechtslage 37
6. Umsetzung der Vorratsdatenrichtlinie in österreichische Recht 43
6.1. Benutzer 43
6.2. Telefondienst 44
6.3. Benutzerkennung 44
6.4. Standortkennung 44
6.5. Erfolgloser Anrufversuch 44
6.6. Dynamische IP-Adresse als Stammdatum 44
6.7. Exkurs IP-Adressen 45
6.8. Kritik an der Zuordnung der dynamischen IP-Adresse zu den Stammdaten 46
6.9. Vorratsdaten 47
6.10. Mit beträchtlicher Strafe bedrohten Handlungen 49

6.11. Auskunftspflichten der Betreiber nach der neuen Rechtslage 52
6.12. Sanktionen 54
7. Gemeinschaftsrecht und nationale Grundrechte 55
7.1. Allgemeines 55
7.2. Vorratsdatenspeicherung und Gemeinschaftsgrundrechte 55
7.3. Das Recht auf Achtung des Privat- und Familienlebens (Art 8 EMRK) 56
7.4. Grundrecht auf Datenschutz 63
7.5. Der Schutz des Fernmeldegeheimnisses 64
8. Kosten 65
8.1. Allgemeines 65
8.2. Wirtschaftliche Auswirkungen 65
8.3. Rechtsprechung des VfGH 66
8.4. Stellungnahmen im Begutachtungsverfahren 67
9. Zusammenfassung 68
10. Danksagung 70

I. Literaturverzeichnis

Berka, Lehrbuch Grundrechte (2000)
Breyer, Rechtsprobleme der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung und ihrer Umsetzung in Deutschland, StV 4/2007
Damjanovic/Holoubek/Kassai/Lehofer/Urbantschitsch, Handbuch des Telekommunikationsrechts (2006)

Fabrizy, StGB und ausgewählte Nebengesetze, MANZ Kurzkommentar, 8. Auflage (2002)
Feiel, Datenspeicherung auf Vorrat und Grundrechtskonformität, jusIT 2008/46, 97
Gitter/Schnabel, Die Richtlinie zur Vorratsspeicherung und ihre Umsetzung in das nationale Recht, MMR 7/2007
Jahnel, Datenschutz im Internet, Rechtsgrundlagen, Cookies und Web-logs, ecolex 2001, 89
Kosta/Dumortier, The Retention Directive and the principles of European protection legislation, MR-Int 2007, 130
Kunnert, Der sicherheitspolizeiliche Griff nach Telekommunikationsdaten, in *Jahnel*, Jahrbuch Datenschutzrecht und E-Government 08 (2008)
Mayer-Schönberger/Brandl, Datenschutzgesetz, 2. Auflage (2006)
Öhlinger, Verfassungsrecht, 5. Auflage (2003)
Otto/Seitlinger, Die „Spitzelrichtlinie". Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG, MR 2006
Reindl-Krauskopf, Data Retention: Sicherheit versus Freiheit, in *Reiter/Wittmann-Tiwald*, Goodbye Privacy, Grundrechte in der digitalen Welt, Grundrechtstag 2007 (2008)
Schmidbauer, Die Problematik der gespeicherten Daten, in *Reiter/Wittmann-Tiwald*, Goodbye Privacy, Grundrechte in der digitalen Welt, Grundrechtstag 2007 (2008)
Schmidbauer, Die Spitzelrichtlinie, Artikel auf Internet4jurists, 5/2006
http://www.internet4jurists.at/news/aktuell95.htm
Schwaighofer, Die neue Strafprozessordnung, Einleitung – Gesetzestext – Anmerkungen (2008)
Seidl, Data-Mining und Datenschutz, Masterthesis, Informationsrecht und Rechtsinformation, Universität Wien (2003)
Seiler, Strafprozessrecht, 9. Auflage (2008)
Sorger, Übermittlung von Fluggastdaten in die USA, in *Jahnel*, Jahrbuch Datenschutzrecht und E-Government 08 (2008)
Steinmaurer, Die Speicherung der Daten auf Vorrat oder Ist es leichter, die sprichwörtliche Nadel zu finden, wenn wir den Haufen Heu größer machen?, in *Reiter/Wittmann-Tiwald*, Goodbye Privacy, Grundrechte in der digitalen Welt, Grundrechtstag 2007 (2008)
Thun-Hohenstein/Cede/Hafner, Europarecht, Ein systematischer Überblick mit den Auswirkungen der EU-Erweiterung, 5. Auflage (2005)
Westphal, Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten, Neues aus Brüssel zum Verhältnis von Sicherheit und Datenschutz in der Informationsgesellschaft, thema: Der gläserne Mensch, juridikum 2006, 34
Wüstenberg, Vorratsdatenspeicherung und Grundrechte, MR-Int 2006/91

Stellungnahme des Europäischen Datenschutzbeauftragten zur Vorratsdatenrichtlinie, C 298 vom 29. November 2005
Art 29 Datenschutzgruppe, WP 113
Art 29 Datenschutzgruppe, WP 119
Deutsche Vereinigung für Datenschutz e.V., Hintergrundinformationen zur Pressemitteilung vom

30. September 2004

Stellungnahmen im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 (61/ME (XXIII. GP)

Stellungnahme des europäischen Zentrums für e-commerce und internetrecht vom 15. Mai 2007

Stellungnahme des Österreichischen Rechtsanwaltskammertags vom 29. Mai 2007

Stellungnahme der ISPA vom 21. Mai 2007

Stellungnahme des Verbandes der Österreichischen Musikwirtschaft vom 15. Mai 2007

Stellungnahme des ORF vom 21. Mai 2007

Stellungnahme der Telekom Austria vom 21. Mai 2007

Stellungnahme der Datenschutzkommission vom 23. Mai 2007

Stellungnahme der ARGE DATEN - Österreichische Gesellschaft für Daten-schutz

vom 21. Mai 2007

Stellungnahme der Industriellenvereinigung vom 18. Mai 2007

II. Abkürzungsverzeichnis

ABGB	Allgemeines bürgerliche Gesetzbuch
Abs	Absatz
Art	Artikel
BGBl	Bundesgesetzblatt
Datenschutzrichtlinie	Richtlinie 2002/58/EG
DSG 2000	Datenschutzgesetz 2000
e-center	europäische zentrum für e-commerce
ECG	E-Commerce-Gesetz
EGMR	Europäischer Gerichtshof für Menschenrechte
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
EMRK	Europäische Menschenrechtskonvention
ErlRV	Erläuternde Bemerkungen zur Regierungsvorlage
ErwG	Erwägungsgrund
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
ggf	gegebenenfalls
gem	gemäß
iSd	im Sinne des
ISPA	Internet Service Provider Austria
IP-Adresse	Internetprotokolladressen
iVm	in Verbindung mit
iwS	im weiteren Sinn
MBG	Militärbefugnisgesetz
mwN	mit weiteren Nachweisen
NotifG 1999	Notifikationsgesetz
OGH	Oberster Gerichtshof
S	Seite
SPG	Sicherheitspolizeigesetz
StGB	Strafgesetzbuch
StGG	Staatsgrundgesetz
StPO	Strafprozessordnung
TKG	Telekommunikationsgesetz 2003
UrhG	Urheberrechtsgesetz
Vgl	Vergleiche
Vorratsdatenrichtlinie	Richtlinie 2006/24/EG
VfGH	Verfassungsgerichtshof
Z	Ziffer

III. Anmerkungen

Sämtliche Stellungnahmen zum dem österreichischen Entwurf der Novelle des TKG 2003 sind abrufbar unter: http://www.parlinkom.gv.at/PG/DE/XXIII/ME/ME_00061/pmh.shtml

Die angeführten URLs wurden letztmals am 15. September 2008 überprüft.

1. Einleitung

1.1. Die Richtlinie 2006/24/EG

Am 13. April 2006 ist, während der österreichischen Ratspräsidentschaft, die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verbreitet werden, und zur Änderung der Richtlinie 2002/58/EG (Vorratsdatenspeicherung, Data Retention) im Amtsblatt der Europäischen Union veröffentlicht worden[1].

Die Vorratsdatenrichtlinie trat gemäß Art 16 am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft, sohin am 3. Mai 2006. Gemäß Art 15 hätten die Mitgliedstaaten bis zum 15. September 2007 jene Rechts- und Verwaltungsvorschriften setzen müssen, um die Richtlinie in ihren jeweiligen Jurisdiktionen umzusetzen. Allerdings konnten die Mitgliedstaaten bis zum 15. März 2009 die Anwendung der Richtlinie auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail aufschieben. Jene Mitgliedstaaten, die von dieser Möglichkeit Gebrauch machen wollten, mußten hiervon den Rat und die Kommission unterrichten. Die entsprechende Erklärung wurde im Amtsblatt der Europäischen Union veröffentlicht. Insgesamt 16 Staaten, darunter auch Österreich, machten von dieser Möglichkeit Gebrauch und stellten die Anwendung der Richtlinie auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail zurück[2].

Die Vorratsdatenrichtlinie hat – wie im Folgenden gezeigt wird – bereits im Vorfeld für Unruhe und Diskussionen gesorgt. Ungeachtet der umzusetzenden Inhalte der Vorratsdatenrichtlinie, wird bereits die Kompetenz des europäischen Richtliniengebers in Frage gestellt. Inhaltlich wird die Vorratsdatenrichtlinie vor allem wegen des Eingriffs in grundrechtliche geschützte Positionen, aber auch wegen der fehlenden Kostenregelung zugunsten der Anbieter, die letztlich durch die Vorratsdatenspeicherung zumindest teilweise öffentliche Aufgaben wahrnehmen, gerügt.

1.2. Der Kampf gegen den internationalen Terrorismus und die organisierte Kriminalität

[1] Abl. EG 2006 L 105, 54 Die Richtlinie ist im Internet abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:01:DE:HTML

[2] Die anderen Staaten waren die Niederlande, Estland, das Vereinigte Königreich, Zypern, Griechenland, Luxemburg, Slowenien, Schweden, Litauen, Lettland, Tschechien, Belgien, Polen, Finnland und Deutschland

Als große und aktuelle Bedrohung werden heute die organisierte Kriminalität und der Terrorismus empfunden. Auf diese Bedrohung reagieren die Staaten zusehends mit anderen Strategien. Nicht mehr punktuelle Reaktionen stehen im Vordergrund, vielmehr erscheint es den Staaten wichtig, möglichst viele Informationen über Bürger zu sammeln, weil sie hoffen, dadurch abstrakte Gefahren bereits im Vorfeld erkennen zu können[3].

Mit der Richtlinie 2006/24/EG, die sowohl kompetenzrechtlich als auch inhaltlich strittig ist, versucht der europäische Gesetzgeber die Ermittlung, Feststellung und Verfolgung von Straftaten zu erleichtern und in die Bekämpfung des internationalen Terrorismus und der organisierten Kriminalität einzugreifen.

Nach Art 5 der Vorratsrichtlinie müssen Daten, die zur Rückverfolgung und Identifizierung der Quelle einer Nachricht erforderlich sind, auf Vorrat gespeichert werden. Dies betrifft beim Telefonfestnetz und Mobilfunk beispielsweise die Rufnummer des Anrufenden und beim E-Mail-Verkehr einschließlich der Internet-Telefonie die zugewiesene Benutzererkennung sowie den Namen und die Anschrift des Teilnehmers, dem eine Internetprotokolladresse (IP-Adresse) zugewiesen worden ist. Ferner müssen die Daten zur Identifizierung des Adressaten einer Nachricht sowie die Daten, die zur Bestimmung des Standorts mobiler Geräte benötigt werden, gespeichert werden. Die Vorratsdatenrichtlinie sieht grundsätzlich vor, dass die Daten für einen Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren auf Vorrat zu speichern sind. Gemäß Art 12 Abs 1 der Vorratsdatenrichtlinie kann sogar für einen begrenzten Zeitraum und bei Vorliegen besonderer Umstände die maximale Speicherfrist verlängert werden, wobei der jeweilige Mitgliedstaat die Kommission hiervon unverzüglich zu unterrichten hat.

Durch die Umsetzung der Vorratsdatenrichtlinie ins innerstaatliche Recht soll daher die Möglichkeit geschaffen werden, die technischen Fortschritte im Bereich der elektronischen Kommunikation im Rahmen der Ermittlung, Feststellung und Verfolgung von Straftaten, insbesondere der organisierten Kriminalität, zu nutzen. Zur Erreichung dieses Zieles sollen Anbieter von öffentlichen Kommunikationsnetzen, daher regelmäßig private Unternehmen, dazu verpflichtet werden, Verkehrs- und Standortdaten, die beim Erbringen von Kommunikationsdiensten erzeugt oder verarbeitet werden, für Zwecke der Strafverfolgung zu speichern. Eine Speicherung von Inhalten übertragener Nachrichten ist gemäß Art 1 Abs 2 der Vorratsdatenrichtlinie weiterhin unzulässig.

Die Vorratsdatenrichtlinie, beziehungsweise die Umsetzung der Vorratsdatenrichtlinie in österreichisches Recht, ermöglicht sohin die verdachts- und anlassunabhängige sowie umfassende Vorratsspeicherung von Stamm-, Verkehrs- und Standortdaten aller Nutzer von Telekommunikationsdienstleistungen in Österreich, wobei weiters die auf Vorrat gespeicherten Daten rückwirkend bis zu sechs Monaten einer Auskunft unterliegen.

---

[3] *Reindl-Krauskopf*, Data Retention: Sicherheit versus Freiheit, in *Reiter/Wittmann-Tiwald*, Goodbye Privacy, Grundrechte in der digitalen Welt, Grundrechtstag 2007, 65

1.3. Umkehr der Unschuldsvermutung

Inhaltlich strittig ist die Vorratsdatenrichtlinie vor allem deshalb, weil die Mitgliedstaaten durch die entsprechende Umsetzung in innerstaatliches Recht dafür Sorge zu tragen haben, dass seit dem 15. September 2007 Anbieter von öffentlichen Kommunikationsnetzen, Verkehrs- und Standortdaten flächendeckend auf Vorrat zu speichern haben, ohne dass diese Datenspeicherung durch konkrete Verdachtsmomente gerechtfertigt ist oder ohne den Betroffenen die Möglichkeit einzuräumen, dagegen Widerspruch einzulegen.

Der Umstand, dass die Daten aller Nutzer der Telekommunikationsdienste gespeichert werden, und zwar auch dann, wenn der Nutzer keine Veranlassung dazu gegeben hat, daher ohne konkreten Verdacht, ist besonders hervorzuheben. Dies hat im Ergebnis zur Folge, dass grundsätzliche alle Menschen, die öffentlich zugängliche elektronische Kommunikationsdienste oder öffentliche Kommunikationsnetze nutzen, daher zum Beispiel ein Telefon verwenden, verdächtig sind, eine mit gerichtlicher Strafe bedrohte Handlung, beziehungsweise eine gerichtlich strafbare Handlung begangen zu haben. Die Vorratsdatenrichtlinie und deren Umsetzung führen daher im Grunde zu einer Umkehr der Unschuldsvermutung.

1.4. Bewegungsprofile – Rückschlüsse auf den Inhalt einer Kommunikation

Bedenken gegen die Vorratsdatenrichtlinie werden insbesondere auch deswegen geäußert, weil Verkehrs- und Standortdaten Aufschluß darüber geben, wer wann mit wem und von welchem Ort aus kommuniziert hat, sei es per Telefon, Mobiltelefon, Email oder Internet. Die Verwendungsmöglichkeiten dieser Kommunikationsdaten sind dabei nicht zu unterschätzen: Mit ihrer Hilfe können Bewegungsprofile erstellt, (geschäftliche) Kontakte rekonstruiert und Freundschaftsbeziehungen identifiziert werden. Auch wenn keine Inhaltsdaten gespeichert werden, führt die Vorratsdatenspeicherung dazu, dass bei regelmäßiger Kommunikation zu oder zwischen bestimmten Nutzern, Rückschlüsse auf die Nutzer möglich sind. Auch Rückschlüsse auf den Inhalt der Kommunikation, auf persönliche Interessen und die Lebenssituation der Kommunizierenden werden durch die Vorratsdatenspeicherung möglich. Dem Argument, wonach rechtschaffende Bürger nichts zu verbergen haben, muß daher aus diesem Grund entgegen getreten werden.

Regelmäßige Anrufe bei einer Selbsthilfe Gruppe oder bei einem Arzt, etc… lassen beispielsweise Rückschlüsse auf den Anrufer zu, weswegen diesem (womöglich unbescholtenen) Anrufer, die Speicherung der Verkehrs- und Standortdaten sehr wahrscheinlich nicht recht sein werden. Darüber hinaus werden zum Teil auch durch die weitreichende Überwachung nachteilige gesellschaftliche Entwicklungen befürchtet[4].

[4] Stellungnahme des europäischen Zentrum für e-commerce und internetrecht im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007

Die Vorratsdatenspeicherung läßt daher Rückschlüsse auf Art und Intensität von Beziehungen, Interessen, Gewohnheiten und Neigungen und nicht zuletzt auch auf den jeweiligen Kommunikationsinhalt zu und vermitteln – je nach Art und Umfang der angefallenen Daten – Erkenntnisse, die an die Qualität eines Persönlichkeitsprofils heranreichen[5].

Daneben erlauben es Kommunikationsdaten, jeden „Klick" und jede Eingabe im Internet minutiös zu rekonstruieren[6]. Die Vorratsdatenspeicherung berührt daher das Grundrecht auf Achtung des Privat- und Familienlebens gemäß Art 8 EMRK.

1.5. Data-Mining

Die Einführung einer Pflicht zur Vorratsspeicherung von Daten, wie sie in der Vorratsdatenrichtlinie vorgesehen ist, führt zu umfangreichen Datenbanken. Diese Daten könnten gewerblich genutzt oder von den Strafverfolgungsbehörden zu Ausforschungszwecken und für Data-Mining benutzt werden[7].

Das europäische zentrum für e-commerce und internetrecht (im folgenden e-center) warnt dementsprechend davor, dass das wahre Eingriffspotential einer flächendeckenden und verdachtsunabhängigen Vorratsspeicherung von Standort- und Verkehrsdaten vor allem im Hinblick auf moderne Technologien (Data-Mining) deutlich wird. Als Data-Mining bezeichnet man die softwaregestützte automatisierte Vorhersage von Lösungsvorschlägen auf Basis von bekannten Verhaltensschemata aus der Vergangenheit sowie die Ermittlung von bisher unbekannten Zusammenhängen, Mustern und Trends in sehr großen Datenbanken. Ziel des Data-Mining ist es, neues Wissen freizulegen, zu entdecken und es zu nutzen[8]. Im Rahmen des Data-Mining werden daher große Datenbestände nach wiederkehrenden Mustern durchsucht. Dies ermöglicht es beispielsweise durch die Frequenz der Kommunikation oder die Häufigkeit und Dauer des gemeinsamen Aufenthalts im Bereich einer Funkzelle soziale Beziehungen mit gewissen Wahrscheinlichkeiten zu rekonstruieren. Darüber hinaus ist es möglich ganze soziale Netze, ihre Ausbreitung sowie allfällige hierarchische Strukturen abzuleiten. Würden derartige Verfahren zur Kriminalitätsprävention eingesetzt, so käme es tatsächlich zu einer Ermittlung aller Personen, deren Kommunikationsprofil mit einer gewissen statistischen Wahrscheinlichkeit auf kriminelles Verhalten hinweist[9].

1.6. Reaktionen zur Novelle des Telekommunikationsgesetzes 2003

---

[5] *Breyer*, Rechtsprobleme der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung und ihrer Umsetzung in Deutschland, StV 4/2007

[6] *Breyer,* StV 4/2007

[7] Stellungnahme des Europäischen Datenschutzbeauftragten zur Vorratsdatenrichtlinie, RZ 11, C 298 vom 29. November 2005

[8] *Seidl*, Data-Mining und Datenschutz, Masterthesis, Informationsrecht und Rechtsinformation, Universität Wien (2003), 2, mwN, abrufbar unter:
http://www.rechtsprobleme.at/doks/datamining_datenschutz_seidl.pdf

[9] Stellungnahme des europäischen Zentrum für e-commerce und internetrecht im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007

Die Vorratsdatenrichtlinie soll durch eine Novelle des Telekommunikationsgesetzes 2003 (im folgenden TKG 2003) in den österreichischen Rechtsbestand umgesetzt werden. Im Rahmen des Begutachtungsverfahrens zum Entwurf der Novelle des TKG 2003 sind über 90 Stellungnahmen eingelangt, wovon 37 auf der Website des Parlaments[10] veröffentlicht worden sind. Die Reaktionen in den Stellungnahmen zum Gesetzesentwurf der Novelle des TKG 2003 sind durchaus vielfältig, je nachdem, welche Interessen vertreten werden.

Franz Schmidbauer bezeichnet die Vorratsdatenrichtlinie in einem Aufsatz, der auf der Website von www.internet4jurists.at abrufbar ist[11], als „Die Spitzelrichtlinie" und kritisiert die Datenspeicherung als eklatanten Eingriff in die Privatsphäre, der nur nach den strengen Kriterien des Art 8 EMRK zulässig ist.

Der Österreichische Rechtsanwaltskammertag führt in seiner Stellungnahme vom 29. Mai 2007 aus, dass die verdachtsunabhängige und flächendeckende Vorratsspeicherung von im Zuge eines Kommunikationsdienstes erzeugten oder verarbeiteten Verkehrs- und Standortdaten aller Österreicher zweifelsohne einen Eingriff in das Recht auf Achtung der Privatsphäre aber auch der Korrespondenz („Briefverkehr"), wie es in Art 8 EMRK zum Ausdruck kommt, darstellt[12].

Ähnlich äußert sich die ISPA in der Stellungnahme vom 21. Mai 2007, wonach der Eingriff in die Grundrechte so gering wie möglich gehalten werden sollte, weil die verdachtsunabhängige Speicherung von Kommunikationsdaten aller Bürger einen massiven Grundrechtseingriff darstellen würde[13].

Völlig anders hingegen argumentiert der Verband der Österreichischen Musikwirtschaft in seiner Stellungnahme vom 15. Mai 2007, wonach der Entwurf der Novelle des TKG 2003 den Schutz geistigen Eigentums im Internet „gänzlich aushebeln" würde. In erster Linie wird die Einschränkung des Zwecks der Vorratsdatenspeicherung auf die Ermittlung, Feststellung und Verfolgung von mit beträchtlicher Strafe bedrohten Handlungen kritisiert, weil der Strafrahmen für nicht qualifizierte (daher nicht gewerbsmäßig begangene) Urheberrechtsverletzungen gemäß § 91 UrhG sechs Monate beträgt, wohingegen § 102a Abs 1 des Entwurfs eine Speicherung der Daten für einen Zeitraum von sechs Monaten zum Zweck der Ermittlung, Feststellung und Verfolgung von mit beträchtlicher Strafe bedrohten Handlungen gemäß § 17 SPG, einschließlich der Tatbestände der §§ 107 und 107a StGB, vorsieht. Gemäß § 17 SPG sind mit beträchtlicher Strafe bedrohte gerichtlich strafbare Handlungen jene Tatbestände, die mit mehr als einjähriger Freiheitsstrafe bedroht sind.

Weiters wird in der Stellungnahme des Verbandes der Österreichischen Musikwirtschaft auch die Speicherfrist von sechs Monaten als zu kurz bemängelt. Die Speicher-

[10] http://www.parlament.gv.at/PG/DE/XXIII/ME/ME_00061/pmh.shtml
[11] Siehe http://www.internet4jurists.at/news/aktuell95.htm
[12] Stellungnahme des Österreichischen Rechtsanwaltskammertags im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 29. Mai 2007
[13] Stellungnahme der ISPA im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom
21. Mai 2007

frist von sechs Monaten sei im Hinblick auf praktische Erfahrungen mit der Strafverfolgung völlig unzureichend[14].

1.7. Fehlende Kostenregelung

Ebenso wird die Vorratsdatenrichtlinie, beziehungsweise in Österreich auch die Umsetzung, deswegen kritisiert, weil keine Entschädigungsregelung zugunsten der privaten Unternehmen, die die Daten zu speichern haben, vorgesehen ist, obwohl private Unternehmen für staatliche Aufgaben zwangsweise (die Unterlassung der Speicherung von Vorratsdaten und der Auskunft sind Verwaltungsübertretungen) herangezogen werden[15].

1.8. Strittige Kompetenzgrundlage

Umstritten ist die Richtlinie auch deshalb, weil Zweifel bestehen, ob die Europäische Gemeinschaft über eine Kompetenz zum Erlaß der Richtlinie verfügt hat. Aus diesem Grund reichte Irland am 6. Juli 2006 eine Nichtigkeitsklage beim EuGH gegen die Richtlinie, beziehungsweise tatsächlich gegen den Rat der Europäischen Union und das Europäische Parlament als beklagte Parteien, ein, weil die gewählte Kompetenzgrundlage zur Erlassung der Richtlinie nach Ansicht Irlands zu unrecht auf Art 95 EGV gestützt worden sei. Die mündliche Verhandlung vor dem EuGH fand am 1. Juli 2008 statt. Das Verfahren ist zum Zeitpunkt der Beendigung dieser Arbeit noch anhängig.

1.9. Europäische Reaktionen

Innerhalb der Mitgliedstaaten der Europäischen Gemeinschaft regt sich ebenso Widerstand gegen die Vorratsdatenrichtlinie und deren Umsetzung in innerstaatliches Recht. Der Arbeitskreis Vorratsdatenspeicherung ist ein Zusammenschluß von Bürgerrechtlern, Datenschützern und Internet-Nutzern in Deutschland, die gegen die Vorratsdatenspeicherung und deren Umsetzung in Deutschland durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung, beziehungsweise durch die Änderung des deutschen Telekommunikationsgesetzes, – auch im Internet[16] – auftreten.

Der Zusammenschluß hat zudem eine Verfassungsbeschwerde beim Bundesverfassungsgericht eingebracht (Aktenzeichen 1 BvR 256/08 und 1 BvR 508/08)[17]. Über die Zulässigkeit der Vorratsdatenspeicherung und über den Antrag, das Verfahren dem Europäischen Gerichtshof vorzulegen, ist noch nicht entschieden worden. Das Gericht hat zunächst der deutschen Bundesregierung bis zum 31.10.2008 Gelegenheit gegeben, Stellung zu nehmen.

---

[14] Stellungnahme des Verbandes der Österreichischen Musikwirtschaft im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007 (ähnlich auch die Stellungnahme des ORF im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 21. Mai 2007)

[15] So etwa Stellungnahme der Telekom Austria im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 21. Mai 2007

[16] http://www.vorratsdatenspeicherung.de/

[17] http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr025608.html

2. Richtlinie 2006/24/EG

2.1. Allgemeines

Auf Grundlage der Richtlinie 2006/24/EG sind, wie bereits erwähnt, Verkehrs- und Standortdaten in Abweichung zu den bislang gültigen Grundsätzen der Richtlinie 2002/58/EG (Datenschutzrichtlinie) in Zukunft auf Vorrat zu speichern. Die Vorratsdatenrichtlinie bedeutet im Ergebnis einen vollständigen Paradigmenwechsel im europäischen Datenschutzrecht der elektronischen Kommunikation[18].

Die Datenschutzrichtlinie geht noch von einem grundsätzlichen Verbot der Speicherung von Nachrichten sowie den zugehörigen Verkehrs- und Standortdaten durch andere Personen als die Nutzer oder ohne deren Einwilligung aus[19] und sieht noch weitgehende Löschungs- beziehungsweise Anonymisierungspflichten vor, die im Wesentlichen nur dann außer Kraft gesetzt werden, insoweit der Anbieter die Daten zum Zweck der Abrechnung benötigt. Daraus folgte, dass Anbieter pauschal tarifierter Dienste (Flatrates) überhaupt keine (nicht anonymisierten) Verkehrsdaten speichern durften[20].

Ziel der Datenschutzrichtlinie ist gemäß Erwägungsgrund 2 die Achtung der Grundrechte. Gemäß des Erwägungsgrundes 30 der Datenschutzrichtlinie sollen die Systeme für die Bereitstellung elektronischer Kommunikationsnetze und –dienste so konzipiert werden, dass so wenig personenbezogene Daten wie möglich benötigt werden. Darüber hinaus sieht die Datenschutzrichtlinie für elektronische Kommunikation in Art 15 eine Aufbewahrung von Daten nur ausnahmsweise vor und stellt es den Mitgliedstaaten frei, entsprechende Rechtsvorschriften zu erlassen. Die Datenschutzrichtlinie ermächtigt daher in Art 15 Abs 1 lediglich die Mitgliedstaaten dazu, Rechtsvorschriften zur begrenzten Aufbewahrung von insbesondere Verkehrs- und Standortdaten zu erlassen. Nunmehr, daher nach Umsetzung der Vorratsdatenrichtlinie, sind die Mitgliedstaaten dazu verpflichtet.

Nach Umsetzung der Vorratsdatenrichtlinie müssen demgegenüber die in der Vorratsdatenrichtlinie genannten Daten gespeichert werden, selbst wenn sie der Anbieter nicht benötigt[21]. Zusammenfassend kann festgehalten werden, dass nach der Rechtslage vor der Vorratsdatenrichtlinie die Speicherung von Verkehrs- und Inhaltsdaten ohne konkreten Anlaß auf Vorrat ohne Einwilligung der betroffenen Nutzer grundsätzlich verboten gewesen ist.

2.2. Daten natürlicher und juristischer Personen

---

[18] www.Tkrecht.de, Nachricht vom 13. April 2006, abrufbar unter: http://www.tkrecht.de/index.php4?direktmodus=nachrichten&nid=20060413-1

[19] *Otto/Seitlinger*, Die „Spitzelrichtlinie", Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG, MR 2006, 227

[20] www.Tkrecht.de, Nachricht vom 13. April 2006, mwN, abrufbar unter: http://www.tkrecht.de/index.php4?direktmodus=nachrichten&nid=20060413-1

[21] www.Tkrecht.de, Nachricht vom 13. April 2006, abrufbar unter:

Während der Regelungsgegenstand der Datenschutzrichtlinie „nur" die Daten natürlicher Personen gewesen ist, umfaßt die Vorratsdatenrichtlinie nun auch die Daten juristischer Personen. Die Vorratsdatenrichtlinie definiert in Art 2 Abs 2 lit b den „Benutzer" als „jede juristische oder natürliche Person", womit sie sich vom „Nutzerbegriff" der Datenschutzrichtlinie unterscheidet, wonach nur eine „natürliche Person" Nutzer im Sinn der Datenschutzrichtlinie sein kann.

2.3. Kategorien von auf Vorrat zu speichernden Daten

Zu den von der Vorratsdatenrichtlinie umfaßten Daten zählen[22]

a) Name, Anschrift und Rufnummer des Anrufers, Name, Anschrift, IP-Adresse, Benutzerkennungen und Rufnummer des (surfenden oder absendenden) Internetnutzers;

b) Name, Anschrift und Rufnummer (ggf auch Rufweiterleitung und –umleitung) des Angerufenen, Benutzerkennung und Rufnummer des vorgesehenen Empfängers eines Anrufs mittels Internet-Telefonie, Name, Anschrift und Benutzerkennung des vorgesehenen Empfängers einer Nachricht/E-mail;

c) Datum und Uhrzeit des Beginns und Endes des Telefonats, Datum und Uhrzeit der An- und Abmeldung, die dynamische oder statische IP-Adresse und die Benutzerkennung des Nutzers von Internetzugang, Internet-E-mail- Dienst oder Internet-Telefon-Dienst;

d) bestimmte Daten zur Bestimmung der Art von Nachrichtenübermittlungen;

e) bestimmte Daten zur Bestimmung der Endeinrichtungen;

f) bestimmte Daten zur Bestimmung des Standortes mobiler Geräte.

Ob es sich bei den zu speichernden Daten um eine taxative oder eine demonstrative Aufzählung handelt, ist aus Art 5 der Vorratsdatenrichtlinie nicht unmittelbar erschließbar. Allerdings ergibt sich aus Art 3 der Vorratsdatenrichtlinie im Zusammenhang mit Bestimmungen der Datenschutzrichtlinie, dass die Aufzählung in Art 5 der Vorratsdatenrichtlinie eine taxative solche ist[23].

2.4. Speicherfristen

Die auf Vorrat gespeichert Daten sind gemäß Art 6 der Vorratsdatenrichtlinie nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weiterzugeben. Der Zeitraum, in dem die Daten aufzubewahren sind, hat gemäß Art 6 der Vorratsdatenrichtlinie sechs Monate bis zu zwei Jahren zu betragen, wobei gemäß Art 12 der Vorratsdatenrichtlinie den Mitgliedstaaten die Möglichkeit eröffnet wird, die maximale Speicherfrist von zwei Jah-

---

http://www.tkrecht.de/index.php4?direktmodus=nachrichten&nid=20060413-1

[22] *Wüstenberg*, Vorratsdatenspeicherung und Grundrechte, MR-Int 2006/91

[23] *Feiel*, Datenspeicherung auf Vorrat und Grundrechtskonformität, jusIT 2008/46, 97

ren für einen begrenzten Zeitraum zu verlängern, wenn besondere Umstände vorliegen.

In diesem besonderen Fall ist allerdings die Kommission über die ergriffenen Maßnahmen und die Gründe hierfür in Kenntnis zu setzen. Die Kommission ist zudem berechtigt, binnen sechs Monaten diese Maßnahmen abzulehnen, wenn und insoweit sie ein Mittel zur willkürlichen Diskriminierung oder eine verschleierte Beschränkung des Handels zwischen den Mitgliedstaaten feststellt, die das Funktionieren des Binnenmarkts behindert. Festzuhalten ist, dass die Kommission aktiv tätig werden muß. Sollte sie zu den relevanten Maßnahmen eines Mitgliedstaates, der die Speicherfrist verlängert hat, keine Stellungnahme abgeben, gelten die Maßnahmen als genehmigt.

2.5. Datenschutz und Datensicherheit

Die Daten sind so zu speichern, dass sie, sowie alle sonstigen damit zusammenhängenden erforderlichen Informationen, unverzüglich an die zuständigen Behörden weitergeleitet werden können.

Durch die Umsetzung in innerstaatliches Recht, haben die Mitgliedstaaten weiters dafür Sorge zu tragen, dass die Anbieter von öffentlich zugänglichen Kommunikationsdiensten und die Betreiber eines öffentlichen Kommunikationsnetzes umfangreiche Maßnahmen vorsehen, um den Datenschutz und die Datensicherheit zu gewährleisten. Insbesondere sind gemäß Art 7 geeignete technische und organisatorische Maßnahmen zu ergreifen, um Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust oder zufällige Änderung, unberechtigte oder unrechtmäßige Speicherung, Verarbeitung, Zugänglichmachung oder Verbreitung zu schützen. Ferner soll dafür Sorge getragen werden, dass nur besonders ermächtigte Personen Zugang zu den Daten haben. Jene Daten, die nicht abgefragt worden sind, sind nach Ablauf der Speicherfrist zu löschen.

In den Mitgliedstaaten ist gemäß Art 9 zumindest eine Kontrollstelle einzurichten, die für die Kontrolle jener Vorschriften zuständig ist, die zum Zweck der Datenschutz- und Datensicherheitsmaßnahmen gemäß Art 7 erlassen worden sind.

2.6. Sanktionen

Die Mitgliedstaaten haben weiters verwaltungs- und strafrechtliche Sanktionen vorzusehen, die dann zu verhängen sind, wenn der Zugang und/oder die Übermittlung der gespeicherten Daten rechtswidriger Weise, daher gegen die innerstaatlichen Rechtsvorschriften, erfolgt sein sollte. Diese Sanktionen haben wirksam, verhältnismäßig und abschreckend zu sein.

2.7. Fazit

Die Vorratsdatenrichtlinie umfaßt alle anfallenden Verkehrs- und Standortdaten betreffend die Kommunikationstechnik[24]. Somit ist jeder einzelne Telekommunikati-

[24] *Wüstenberg,* MR-Int 2006, 91

onsvorgang einer Person, beziehungsweise genauer eines Anschlussinhabers, Zeitpunkt und Dauer, sowie im Fall der Telefonie der Partner der Kommunikation, für eine Speicherfrist von sechs Monaten zuordenbar, wenn der Entwurf der österreichischen Umsetzung der Richtlinie in Kraft treten sollte. Die Richtlinie selbst gibt, wie weiter oben schon ausgeführt, eine Speicherfrist von sechs Monaten bis zwei Jahren vor.

3. Historischer Hintergrund der Richtlinie

3.1. Terroranschläge in New York City, Madrid und London

Historischer Hintergrund der Richtlinie sind die Terroranschläge vom 11. September 2001 in New York City, jene vom 11. März 2004 in Madrid und jene vom 13. Juli 2005 in London.

In den Erwägungsgründen der Richtlinie 2006/24/EG ist unter Punkt 8 ein entsprechender Hinweis angeführt, wonach in der vom Europäischen Rat am 25. März 2004 angenommenen Erklärung zum Kampf gegen den Terrorismus der Rat aufgefordert worden ist, Vorschläge für Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten zu prüfen. Zufolge des achten Erwägungsgrundes hat die beträchtliche Zunahme der Möglichkeiten bei der elektronischen Kommunikation dazu geführt, dass Daten über die Nutzung elektronischer Kommunikation besonders wichtig sind und daher ein wertvolles Mittel bei der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten und insbesondere der organisierten Kriminalität darstellen.

3.2. Schlußfolgerungen des Rates in Brüssel vom 20 September 2001

Vor dem Hintergrund der Terroranschläge in New York City faßte der Rat am 20. September 2001 in Brüssel in den Schlußfolgerungen zusammen, welche Maßnahmen im Kampf gegen den Terror gefaßt werden müssen. Insbesondere forderte der Rat die Kommission auf, Vorschläge zu unterbreiten, die es den Vollstreckungsbehörden ermöglichen sollte, strafbare Handlungen auch unter Verwendung elektronischer Kommunikation zu untersuchen.

Der Rat weist allerdings darauf hin, dass dafür Sorge zu tragen ist, dass ein Gleichgewicht zwischen dem Schutz personenbezogener Daten und der Notwendigkeit des Zugangs der Strafverfolgungsbehörden zu Daten für strafrechtliche Ermittlungszwecke gewährleistet wird[25].

3.3. Erklärung zum Kampf gegen den Terrorismus

Am 25. März 2004 verurteilte der Europäische Rat die Terroranschläge in Madrid vom 11. März 2004 und beauftragte in der Erklärung zum Kampf gegen den Terrorismus den Rat, über Maßnahmen in verschiedenen Bereichen zu beraten, damit der Rechtsrahmen ausgebaut werden könne. Insbesondere sollte der Rat über Vorschlä-

[25] Conclusions adopted by the Council (Justice and Home Affairs), Brussels, 20 September 2001, SN 3926/6/01, abrufbar unter http://ec.europa.eu/justice_home/doc_centre/police/chief/doc_police_task_force_de.htm

ge für Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch Diensteanbieter beraten, wobei unter anderem auch den Vorschlägen über die Aufbewahrung von Verkehrsdaten Vorrang eingeräumt werden sollte, damit diese bis zum Juni 2005 angenommen werden können[26].

3.4. Rahmenbeschluss vom 28. April 2004

Am 28. April 2004 legte der Rat der europäischen Union einen Entwurf eines Rahmenbeschlusses „über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus", vor[27].

Dieser Entwurf ging auf eine Initiative von Frankreich, Irland, Schweden und des Vereinigten Königreichs zurück. In den Erwägungsgründen zu diesem Rahmenbeschluss wird die Notwendigkeit, Daten auf Vorrat zu speichern damit begründet, die Quellen eines illegalen Inhalts, z.B. Kinderpornographie und rassistisches und fremdenfeindliches Material, sowie die Urheber von Angriffen auf Informationssystemen ermitteln und diejenigen identifizieren zu können, die an der Nutzung elektronischer Kommunikationsnetze für die Zwecke der organisierten Kriminalität und des Terrorismus beteiligt sind.

Aufgrund unterschiedlicher Rechtsvorschriften in den Mitgliedstaaten sei die Zusammenarbeit der für die Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten zuständigen Behörden beeinträchtigt. Für eine wirksame polizeiliche und justitielle Zusammenarbeit in Strafsachen müsse sichergestellt werden, dass alle Mitgliedstaaten die erforderlichen Schritte unternehmen, um bestimmte Datentypen eine gewisse Zeit für Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus, auf Vorrat zu speichern. Diese Daten sollen den Mitgliedstaaten zur Verfügung stehen. Erfaßt waren von diesem Rahmenbeschluss Verkehrs- und Standorten einschließlich Teilnehmer- und Nutzerdaten, die während elektronischer Kommunikationsvorgänge erzeugt werden. Inhaltsdaten waren von der Speicherpflicht nicht umfaßt.

Ziel dieses Vorschlages war daher die Erleichterung der justitiellen Zusammenarbeit in Strafsachen, indem die Rechtsvorschriften in den Mitgliedstaaten über die Vorratsspeicherung von Daten angeglichen werden.

Dieser Rahmenbeschluss sah in Art 4 Abs 1 vor, dass die Daten nach ihrer Erzeugung mindestens 12 und höchstens 36 Monate lang auf Vorrat gespeichert werden. Darüber hinaus sah dieser Entwurf die Möglichkeit für die Mitgliedstaaten vor, längere Fristen für die Vorratsspeicherung von Daten vorzusehen, insoweit dies eine notwendige, angemessene und verhältnismäßige Maßnahme innerhalb einer demokrati-

[26] Ratsdokument 7764/04 vom 28. März 2004
[27] Ratsdokument 8958/04 vom 28. April 2004

schen Gesellschaft ist. Der Vorschlag enthielt im Übrigen keine Entschädigungsregeln zugunsten der Anbieter für entstehende Kosten.

3.5. Exkurs - Die dritte Säule

3.5.1. Polizeiliche und justitielle Zusammenarbeit

Die im Titel VI EUV enthaltenen Bestimmungen über die polizeiliche und justitielle Zusammenarbeit in Strafsachen sind die vertragliche Grundlage für die unter dem Dach der EU erfolgende Zusammenarbeit der Gesamtheit der Mitgliedstaaten auf diesen Gebieten. Diese Dritte Säule stellt eine Ergänzung der Europäischen Gemeinschaften dar, die außerhalb der Gemeinschaft angesiedelt und in deren Supranationalität nicht einbezogen ist[28].

Gemäß Art 29 EUV und unbeschadet der Befugnisse der Europäischen Gemeinschaft verfolgt die Union das Ziel, den Bürgern in einem Raum der Freiheit, der Sicherheit und des Rechts ein hohes Maß an Sicherheit zu bieten, indem sie ein gemeinsames Vorgehen der Mitgliedstaaten im Bereich der polizeilichen und justitiellen Zusammenarbeit in Strafsachen entwickelt sowie Rassismus und Fremdenfeindlichkeit verhütet und bekämpft. Erreicht werden soll dieses Ziel durch eine engere Zusammenarbeit der Polizei-, Zoll- und Justiz- sowie anderer zuständiger Behörden in den Mitgliedstaaten, sowohl unmittelbar als auch unter Einschaltung von Europol und durch Annäherung der Strafvorschriften der Mitgliedstaaten.

3.5.2. Rahmenbeschlüsse

Rahmenbeschlüsse sind Teil der Rechtssetzung der dritten Säule. Hinsichtlich der durch Art 29 EUV erfaßten Angelegenheiten besteht nicht nur eine Konsultations- und Koordinationspflicht der Mitgliedstaaten (Art 34 Abs 1 EUV), sondern auch die Ermächtigung zur Rechtssetzung. Die Handlungsformen sind in Art 34 EUV geregelt. Nach Art 34 Abs 2 EUV ergreift der Rat Maßnahmen und fördert in der geeigneten Form und nach den geeigneten Verfahren, die in Titel VI EUV festgelegt sind, eine den Zielen der EU dienende Zusammenarbeit. Hierzu kann er gemeinsame Standpunkte, Rahmenbeschlüsse und Beschlüsse für jeden anderen Zweck annehmen sowie Übereinkommen erstellen. Für alle genannten Handlungsformen (mit Ausnahme von Durchführungsbeschlüssen) ist im Rat Einstimmigkeit erforderlich.

Rahmenbeschlüsse sind für die Mitgliedstaaten hinsichtlich des zu erreichenden Zieles verbindlich, überlassen jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel. Sie sind nicht unmittelbar wirksam. Eine unmittelbare Wirkung von Rahmenbeschlüssen, wie sie der EuGH in seiner Rechtsprechung zur Richtlinie erarbeitet hat, wird ausgeschlossen[29].

---

[28] *Thun-Hohenstein – Cede – Hafner*, Europarecht, Ein systematischer Überblick mit den Auswirkungen der EU-Erweiterung, 5. Auflage, 35 f

[29] *Thun-Hohenstein – Cede – Hafner*, Europarecht, Ein systematischer Überblick mit den Auswirkungen der EU-Erweiterung, 5. Auflage, 200

3.6. Bericht des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments[30]

Der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments (im Folgenden der Ausschuss), äußerte sich durch seinen Berichterstatter Alexander Nuno Alvaro (im Folgenden der Berichterstatter) kritisch zu diesem Rahmenbeschluss vom 28. April 2004. Folgende Punkte wurden ins Treffen geführt:

3.6.1. Rechtsgrundlage des Rahmenbeschlusses

Im endgültigen Bericht des Ausschusses vom 31. Mai 2005 – ein vorläufiges Arbeitsdokument vom 21. Jänner 2005 hatte noch keine Stellungnahme des Rechtsausschusses enthalten - wurde unter anderem die gewählte Rechtsgrundlage in Frage gestellt, die nicht mit der Europäischen Gesetzgebung in Einklang stünde.

Hinsichtlich der Kompetenzgrundlage führt der Berichterstatter aus, dass der Rat zu unrecht von seiner alleinigen Gesetzgebungsbefugnis gemäß Titel VI EUV ausgeht und sich zu unrecht auf Art 31 Abs 1 lit c iVm Art 34 Abs 2 lit b EUV beruft. Bei jenen im Rahmenbeschluss vorgeschlagenen Maßnahmen handelte es sich dem Bericht zufolge zum Teil um die Verpflichtung der Service Provider zur Aufbewahrung von Daten und um die Definition dieser Daten sowie um die Dauer der Aufbewahrung, wobei diese Maßnahmen dem Gemeinschaftsrecht (erste Säule) unterliegen würden.

Andererseits würden auch der Zugang und der Austausch der gespeicherten Daten innerhalb der Mitgliedstaaten geregelt. Dieses gemeinsame Vorgehen unterliegt jedoch dem Bereich der justitiellen Zusammenarbeit in Strafsachen und daher der dritten Säule.

Der Berichterstatter führt aus, dass zum Zeitpunkt des Entwurfes des Rahmenbeschlusses bereits Gemeinschaftsregelungen bestanden haben, die Verpflichtungen von Service Providern beinhalten. Bei diesen Gemeinschaftsregelungen handelt es sich zum einen um die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zum anderen um die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

Bei jenen Daten, die vom Rahmenbeschluss geregelt werden, handelt es sich um Daten iSd Art 1 iVm Art 2 a der Richtlinie 95/46/EG vom 24. Oktober 1995, die die allgemeinen Verpflichtungen der Mitgliedstaaten zur Gewährleistung des Schutzes der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Inhalt hat.

---

[30] Arbeitsdokument vom 21. Jänner 2005 (A6-0174/2005), abrufbar unter: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dt/553/553885/553885de.pdf

Die Richtlinie 2002/58/EG vom 12. Juli 2002 regelt darüber hinaus insbesondere auch die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation. Gespeicherte Daten sind dementsprechend dann zu löschen, wenn ihre Aufbewahrung nicht mehr gerechtfertigt ist. Art 15 der Richtlinie 2002/58/EG eröffnet den einzelnen Mitgliedstaaten allerdings die Möglichkeit, Daten für eine begrenzte Zeit aufzubewahren, sofern eine solche Beschränkung für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist.

Gemäß Artikel 47 EUV läßt aber der Vertrag über die Europäische Union die Verträge zur Gründung der Europäischen Gemeinschaften sowie die nachfolgenden Verträge und Akte zur Änderung oder Ergänzung der genannten Verträge unberührt. Es ist also nicht gestattet, durch einen auf den EU-Vertrag gestützten Rechtsakt den gemeinschaftlichen Besitzstand anzutasten.

Dementsprechend darf sich keine Regelung des EUV auf die Bestimmungen des EGV auswirken. Die Auswirkung auf das Gemeinschaftsrecht ergibt sich im vorliegenden Fall aus der Nichtbeachtung des bereits existierenden gemeinschaftlichen Rechtsrahmens. Daher fällt unter anderem die Verpflichtung der Provider zur Speicherung an sich, die Definition der zu speichernden Daten sowie die Aufbewahrungsdauer in den Regelungsbereich des EGV.

Der Berichterstatter beruft sich auf die inhaltlich gleichlautende Meinung des Rechtsausschusses des Europäischen Parlaments. In seiner Stellungnahme führt der Rechtsausschuss aus, dass bereits die Richtlinie 2002/58/EG eine Reihe von Verpflichtungen hinsichtlich der Arten der von den Betreibern aufzubewahrenden Daten und der Dauer ihrer Aufbewahrung festlegt. Jede Änderung daran, wie sie mit dem Entwurf eines Rahmenbeschlusses bezweckt wird, kann nicht Gegenstand eines auf den EU-Vertrag gestützten Rechtsinstruments sein.

3.6.2. Meinung des Rechtsausschusses

In der Sitzung vom 31. März 2005 hat der Rechtsausschuss dementsprechend beschlossen,

- dass die Harmonisierung der Arten von Daten, die von den Diensteanbietern aufzubewahren sind, und deren Aufbewahrungsdauer, Gegenstand des gemeinschaftlichen Besitzstands, wie er aus der Richtlinie 2002/58/EG hervorgeht, sind;
- dass ein auf Titel VI des EU-Vertrags gestützter Rahmenbeschluss, der darauf abzielt, solche Bestandteile zu ändern, die Bestimmungen der genannten Richtlinie berühren würde und folglich einen Verstoß gegen Artikel 47 des EU-Vertrags darstellen könnte;
- dass die geeignete Rechtsgrundlage für die Harmonisierung der Arten von Daten, die von den Diensteanbietern aufzubewahren sind und die Aufbewah-

rungsdauer dieselbe ist, die aus dem vorher bestehenden gemeinschaftlichen Rechtsrahmen hervorgeht, nämlich Artikel 95 des EG-Vertrags;

- und dass aufgrund dieser Erwägungen es denkbar wäre, zwei verschiedene Rechtsakte zu erstellen: den einen über die Harmonisierung der Arten von Daten, die von den Diensteanbietern aufzubewahren sind und die Aufbewahrungsdauer auf der Grundlage der ersten Säule (EG-Vertrag), den anderen über die Aspekte der Zusammenarbeit in Strafsachen, insbesondere den Zugang zu diesen Daten und ihren Austausch auf der Grundlage der dritten Säule (EU-Vertrag)[31]

3.6.3. Verhältnismäßigkeit der Maßnahme

Ebenso wurde die Verhältnismäßigkeit der im Rahmenbeschluss vorgesehenen Maßnahmen vom Berichterstatter in Zweifel gezogen, die nicht in einer angemessenen Zweck-Mittel-Relation stünden, weil sie weder geeignet noch erforderlich sind und eine unzumutbare Härte für die Betroffenen darstellen.

Einerseits bezweifelt der Berichterstatter, dass bei dem zu speichernden Datenvolumen eine zielführende Auswertung der Daten überhaupt möglich sei. Die Speicherung aller vom Vorschlag umfaßten Verkehrsdaten würde bei heutigem Verkehrsaufkommen eine Datenmenge von 20.000 - 40.000 Terabyte nach sich ziehen. Dieses Datenvolumen entspricht ungefähr 4 Mio km gefüllter Aktenordner, das seien zehn Aktenberge, die jeweils von der Erde bis zum Mond reichen würden. Bei dieser gewaltigen Datenmenge würde ein einmaliger Suchlauf bei einem Einsatz der vorhandenen Technik ohne zusätzliche Investitionen 50-100 Jahre dauern, weswegen die rasche Verfügbarkeit der angeforderten Daten somit zu bezweifeln sei.

Andererseits würden Teilnehmer aus dem Umfeld der organisierten Kriminalität und des Terrorismus die Verfolgbarkeit ihrer Daten leicht zu verhindern wissen. Möglichkeiten hierzu wären der Erwerb von Telefonkarten durch Strohmänner oder wechselnd eingesetzte Mobiltelefone von ausländischen Anbietern, die Nutzung öffentlicher Telefonzellen, die Veränderung der bei der Nutzung eines E-Mail-Service verwendeten IP-Adresse oder E-Mail-Adresse oder gleich die Nutzung von Internet Service Providern, die außerhalb Europas liegen und einer Verpflichtung bezüglich der Vorratsdatenspeicherung nicht unterliegen.

3.6.4. Unschuldsvermutung

Der Berichterstatter wirft zudem die Frage auf, inwieweit der Entwurf des Rahmenbeschlusses, beziehungsweise die darin vorgesehene Vorratsdatenspeicherung, mit dem Prinzip der Unschuldsvermutung vereinbar ist.

3.6.5. Kosten

Ferner releviert der Berichterstatter, dass der vorgeschlagene Rahmenbeschluss nicht auf die möglichen Belastungen der Betroffenen eingehen würde. Neben den tiefen

[31] Die Stellungnahme des Rechtsausschusses ist dem Bericht des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments vom 31. Mai 2005 angeschlossen.

Eingriffen in den Schutz der persönlichen Daten des Einzelnen, seien enorme Belastungen für die europäische Telekommunikationsindustrie, insbesondere für kleinere und mittlere Telekommunikationsunternehmen, zu befürchten.

3.6.6. Vereinbarkeit mit Art 8 der Europäischen Menschenrechtskonvention

Dem Bericht zufolge verletzt der Rahmenbeschluss das Recht auf Achtung des Privat- und Familienlebens gemäß Art 8 der Europäischen Menschenrechtskonvention (im folgenden EMRK), wonach jedermann Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs hat. Eingriffe einer öffentlichen Behörde in die Ausübung dieses Rechts sind gemäß Art 8 Abs 2 EMRK nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.

Die Datenüberwachung und -speicherungen sei dem Berichterstatter zufolge abzulehnen, sofern sie nicht drei grundlegende Kriterien erfüllen, die sich aus der Auslegung von Art 8 Abs 2 der EMRK durch den Europäischen Gerichtshof für Menschenrechte ergeben: Sie müssen gesetzlich vorgesehen, in einer demokratischen Gesellschaft notwendig sein und einem der in der Konvention aufgeführten legitimen Ziele dienen. Ob der Rahmenbeschluss diesen Anforderungen gerecht werde, sei aus Sicht des Berichterstatters zumindest fraglich.

3.6.7. Fazit des Berichtes des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlament

Zusammenfassend lehnte der Bericht des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments, den vorliegenden Entwurf eines Rahmenbeschlusses ab und forderte die vier Mitgliedstaaten auf, ihren Vorschlag zurückzuziehen. Der Berichterstatter erwartete von jenen Mitgliedstaaten, die den Entwurf vorgeschlagen haben, eine Studie vorzulegen, aus der die Notwendigkeit der geplanten Vorratsdatenspeicherung unzweifelhaft belegt werden würde. Der Bericht schlug ferner vor, die Verpflichtung zur Datenspeicherung, die Definition der zu speichernden Daten und die Dauer der Speicherung in einer von den übrigen Regelungen getrennten Richtlinie zu behandeln und fordert die Kommission auf, einen entsprechenden Vorschlag zu erarbeiten.

3.7. Schlußfolgerungen des Vorsitzes vom 15. Juli 2005

In den Schlußfolgerungen vom 16. und 17. Juni 2005 wünschte der Europäische Rat unter anderem, dass im zweiten Halbjahr 2005 vorrangig auch Gesetzgebungsarbeiten zur Stärkung der polizeilichen und justitiellen Zusammenarbeit erfolgen; dies insbesondere und soweit möglich im Hinblick auf den Informationsaustausch zwischen den Polizeibehörden, die Beweisanordnung, die Vorratsspeicherung von Telekom-

munikationsverkehrsdaten sowie den Informationsaustausch und die Zusammenarbeit betreffend der terroristischen Straftaten[32].

3.8. Entwurf der Richtlinie 2006/24/EG (Vorratsdatenrichtlinie)

3.8.1. Der Rahmenbeschluss vom 28. April 2004 wird nicht angenommen

Die Datenschutzgruppe „Artikel 29" stellte zu dem Rahmenbeschluss fest, dass die verbindlich vorgeschriebene Vorratsspeicherung von Verkehrsdaten unter den in dem Entwurf vorgesehenen Bedingungen nicht annehmbar ist, weil kein Beweis dafür erbracht worden ist, dass die Vorratsspeicherung zu Zwecken der öffentlichen Ordnung erforderlich ist. Eine entsprechende Analyse ergab, dass die von den Strafverfolgungsbehörden nachgefragten Daten überwiegend nicht älter als sechs Monate waren[33].

Die Datenschutzgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist das unabhängige Beratungsgremium der Europäischen Union in Datenschutzfragen und setzt sich aus den Vertretern der in jedem Mitgliedstaat des EWR bestehenden unabhängigen Datenschutz-Kontrollstellen zusammen. Neben ihrer Beratungsfunktion, nimmt sie auch zu Fragen des Datenschutzes in der Gemeinschaft gegenüber der Europäischen Kommission in Form von Sachverständigenbeiträgen Stellung. Darüber hinaus fördert sie die einheitliche Anwendung der allgemeinen Grundsätze der Richtlinien in allen Mitgliedstaaten durch die Zusammenarbeit der Datenschutz-Kontrollstellen[34].

Letztlich konnten sich die Mitgliedstaaten 2005 nicht auf den Rahmenbeschluss vom 28. April 2004 einigen, so dass alleine der Weg über die Richtlinie politisch gangbar war[35].

In weiterer Folge legte daraufhin die Kommission am 21. September 2005 den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG vor (KOM 2005/438 Endg.)[36].

Der Entwurf sah in Art 7 zunächst eine generelle Vorratsdatenspeicherung von einem Jahr vor. Für Daten im Zusammenhang mit elektronischen Nachrichtenübermittlungen, die ganz oder überwiegend unter Verwendung des Internet-Protokolls vorgenommen werden, sah der Entwurf eine Speicherungsfrist von sechs Monaten vor.

---

[32] Ratsdokument 10255/1/05/REV 1, Schlußfolgerungen des Vorsitzes vom 15. Juli 2005, abrufbar unter
http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/de/ec/85350.pdf
[33] Stellungnahme des Europäischen Datenschutzbeauftragten zur Vorratsdatenrichtlinie, RZ 14, C 298 vom 29. November 2005
[34] http://www.dsk.gv.at/site/6194/default.aspx
[35] *Breyer*, StV 4/2007
[36] KOM 2005/438 Endg., abrufbar unter
http://eur-lex.europa.eu/LexUriServ/site/de/com/2005/com2005_0438de01.pdf

3.8.2. Annahme der Vorratsdatenrichtlinie

Nach mehreren Änderungsvorschlägen[37] wurde die Richtlinie letztlich am 14. Dezember 2005 im Europäischen Parlament mit 378 Stimmen bei 197 Gegenstimmen und 30 Enthaltungen angenommen[38]. Das europäische Rechtsetzungsverfahren im Weg der Mitentscheidung wurde im Fall der Richtlinie 2006/24/EG besonders rasch durchgeführt. Der Zeitraum zwischen der Vorstellung des Richtlinienentwurfs durch die Kommission und der maßgeblichen Lesung durch das Europäische Parlament betrug weniger als drei Monate. Die Annahme durch den Rat erfolgte nach weiteren zwei Monaten[39]. Die Bedenken und Einwände, die der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments hinsichtlich des Rahmenbeschlusses vom 28. April 2004 vorgebracht hatte, wurden durch die Vorratsdatenrichtlinie nicht ausgeräumt.

Die Kompetenzgrundlage ist nach wie vor strittig (siehe weiter unten), die Kostenfrage der Anbieter bleibt ungeklärt und die Verhältnismäßigkeit des Grundrechtseingriffs ist zweifelhaft, wobei auch die Vorratsdatenrichtlinie eine Umkehr der Unschuldsvermutung bringt.

Anstatt feste Fristen vorzugeben, bleibt es denn Mitgliedsstaaten nun überlassen, eine Speicherungsverpflichtung von sechs Monaten bis zu zwei Jahren festzulegen, womit das Ziel der Harmonisierung der Rechts- und Verwaltungsvorschriften sehr wahrscheinlich gefährdet ist, beziehungsweise in Frage zu stellen ist. Strafverfolgungsbehörden werden sich daher nicht darauf verlassen können, dass europaweit die Daten gleich lang gespeichert werden. Zudem regelt die Vorratsdatenrichtlinie nicht, welche Tatbestände unter „schweren Straftaten" zu subsumieren sind, beziehungsweise wie hoch die Mindeststrafdrohung von Tatbeständen sind, die als „schwere Straftaten" zu gelten haben. Diese Festlegung bleibt sohin den Mitgliedstaaten überlassen.

4. Kompetenzgrundlage zur Erlassung der Vorratsdatenrichtlinie

4.1. Prinzip der begrenzten Einzelermächtigung

Nach dem in Art 5 Abs 1 EGV festgelegten Prinzip der begrenzten Einzelermächtigung wird die Gemeinschaft innerhalb der Grenzen der ihr im EGV zugewiesenen Befugnisse und gesetzten Ziele tätig. Die Rechtsetzungsorgane der Gemeinschaft dürfen gemäß Art 7 EGV grundsätzlich nur dann tätig werden, wenn in den Gemeinschaftsverträgen eine ausdrückliche Kompetenzzuweisung erfolgt ist.

---

[37] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A6-2005-0365+0+NOT+XML+V0//DE

[38] COD/2005/0182, abrufbar unter http://www.europarl.europa.eu/oeil/FindByProcnum.do?lang=2&procnum=COD/2005/0182

[39] *Westphal*, Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten, Neues aus Brüssel zum Verhältnis von Sicherheit und Datenschutz in der Informationsgesellschaft, thema: Der gläserne Mensch, juridikum 2006, 34, mwN

Ein Tätigwerden der Gemeinschaft allein aufgrund der Ziel- und Aufgabenkataloge der Gemeinschaftsverträge ist demnach grundsätzlich ausgeschlossen. Nach ständiger Rechtsprechung muß sich im Rahmen der Zuständigkeitsordnung der Gemeinschaft die Wahl der Rechtsgrundlage eines Rechtsakts auf objektive, gerichtlich nachprüfbare Umstände gründen[40].

4.2. Art 95 EGV

4.2.1. Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten

Das Europäische Parlament und der Rat begründen ihre Kompetenz zur Erlassung der Richtlinie 2006/24/EG „insbesondere" auf Art 95 EGV, demzufolge der Rat gemäß dem Verfahren nach Art 251 EGV und nach Anhörung des Wirtschafts- und Sozialausschusses die Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, welche die Errichtung und das Funktionieren des europäischen Binnenmarktes zum Gegenstand haben, erläßt. Demnach ist auch das Regelungsinstrument der Richtlinie zulässig, die schon mit einer qualifizierten Mehrheit beschlossen werden kann. Nach der Rechtsprechung des EuGH muß eine auf Art 95 EGV gestützte Intervention der Gemeinschaft mit dem Ziel der Beseitigung von Handelshemmnissen tatsächlich dazu geeignet sein, zur Beseitigung eines solchen Hemmnisses beizutragen[41].

4.2.2. Objektive Zielsetzungen

Diese Wahl der Kompetenzgrundlage wird vielfach in Frage gestellt[42]. Grundsätzlich ist zur Prüfung der Richtlinienkompetenz der Gemeinschaft auf die in der Richtlinie genannten objektiven Zielsetzungen abzustellen, wobei die in Erwägungsgrund 6 der Vorratsdatenrichtlinie angeführte Angleichung von Rechtsvorschriften zur Vorratsspeicherung, um Wettbewerbsverzerrungen zu vermeiden, nach Art 14 EGV ein legitimes Harmonisierungsziel ist. Allerdings werden darüber hinaus keine weitergehenden Harmonisierungsziele genannt.

Auch die Begründung, die Angleichung von Rechtsvorschriften zur Vorratsspeicherung anzustreben, um Wettbewerbsverzerrungen zu vermeiden, erscheint fraglich, weil im Zeitpunkt der Erlassung und des Inkrafttreten der Vorratsdatenrichtlinie nur in einigen Mitgliedstaaten entsprechende Bestimmungen zur Vorratsspeicherung bestanden. Die Richtlinie kann deshalb nicht zu einer Harmonisierung führen, weil in einigen Mitgliedstaaten eine Rechtsgrundlage für die Vorratsspeicherung von Kommunikationsdaten überhaupt erst begründet worden ist. Ungeachtet dessen überläßt die Richtlinie die konkrete Ausgestaltung – etwa die Speicherfristen – zum Teil den Mitgliedstaaten, weswegen aufgrund dieser Unbestimmtheit zu erwarten ist, dass

[40] EuGH C-42/97 (61997J0042), RZ 36

[41] Stellungnahme des Europäischen Datenschutzbeauftragten zur Vorratsdatenrichtlinie, RZ 40, C 298 vom 29. November 2005

[42] z.B. *Gitter/Schnabel*, Die Richtlinie zur Vorratsspeicherung und ihre Umsetzung in das nationale Recht, MMR 7/2007; Stellungnahme des Europäischen Zentrum für e-commerce und internetrecht im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007

Wettbewerbsnachteile in den einzelnen Mitgliedstaaten für die Telekommunikationsdiensteanbieter nicht ausgeräumt, sondern eher noch verstärkt werden.

4.2.3. Stoßrichtung und Ziel der Vorratsdatenrichtlinie

Erste Stoßrichtung und vorrangiges Ziel der Vorratsdatenrichtlinie ist, wie man den Erwägungsgründen 7, 8, 9 und 21 entnehmen kann, in erster Linie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten, insbesondere der organisierter Kriminalität und der Kampf gegen den Terrorismus[43]. Diese Zielsetzung ist allerdings in Titel VI des EUV, „Bestimmungen über die polizeiliche und justitielle Zusammenarbeit in Strafsachen", festgelegt worden.

Kommission, Europaparlament und Rat sind naturgemäß der Ansicht, die Richtlinie 2006/24/EG zu Recht auf Art 95 EGV gestützt zu haben, wobei sie sich auf eine „Legal Opinion", sohin ein Rechtsgutachten stützten, das von der Kommission und dem Rat beauftragt worden war. Diesem Gutachten zufolge sei die Speicherung von Kommunikationsdaten in der Richtlinie 2002/58/EG, daher in der ersten Säule, bereits umfassend gemeinschaftsrechtlich geregelt, weswegen die Einführung von Mindestspeicherfristen für solche Daten als Annex ebenfalls in die Kompetenz der Europäischen Gemeinschaft nach Art 95 EGV falle. Außerdem würden unterschiedliche nationale Vorschriften zur Vorratsspeicherung den Binnenmarkt beeinträchtigen.

Die Entscheidung, die Vorratsdatenspeicherung in einer Richtlinie und nicht in einer Verordnung zu regeln, wurde damit begründet, weil eine Verordnung angesichts der unterschiedlichen technischen Struktur, die die Betreiber in den verschiedenen Mitgliedstaaten verwenden, zu strikt gewesen wäre[44].

Einige Mitgliedstaaten wie Irland und die Slowakei vertreten demgegenüber die Auffassung, dass die dritte Säule der EU die korrekte Rechtsgrundlage gewesen wäre, weil Ziel der Datenspeicherung die Erleichterung der Strafverfolgung ist. Das dafür vorgesehene Instrument des Rahmenbeschlusses räumt den Mitgliedstaaten im Vergleich zu einer Richtlinie größeren Einfluß ein, weil Rahmenbeschlüsse von den Mitgliedstaaten einstimmig angenommen werden müssen (Art 34 Abs 2 EUV) und nicht der Zustimmung des Europäischen Parlaments bedürfen[45].

4.3. Klage Irlands

4.3.1. Nichtigkeitsklage

Dementsprechend hat Irland am 6. Juli 2006 eine Nichtigkeitsklage beim EuGH eingebracht und beantragt, die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 für nichtig zu erklären, weil sie nicht auf einer geeigneten Rechtsgrundlage erlassen worden sei. Weiters beantragt Irland, dem Rat der Eu-

[43] So auch *Westphal*, juridikum 2006, 34
[44] *Kosta/Dumortier*, The Retention Directive and the principles of European protection legislation, MR-Int 2007, 130, mwN
[45] *Breyer*, StV 4/2007

ropäischen Union und dem Europäischen Parlament die Kosten des Verfahrens aufzuerlegen[46].

Die Wahl von Art 95 EGV als Rechtsgrundlage für die Richtlinie (2006/24/EG) sei nach Ansicht Irlands mit einem wesentlichen Formfehler behaftet, weil weder Art 95 EGV noch eine andere Bestimmung des Vertrages eine geeignete Rechtsgrundlage für die Vorratsdatenrichtlinie gewesen seien. Irland brachte im Wesentlichen vor, dass der einzige, beziehungsweise der Hauptzweck der Vorratsdatenrichtlinie darin bestünde, die Ermittlung, Entdeckung und Verfolgung schwerer Verbrechen, einschließlich des Terrorismus, zu erleichtern. Unter diesen Umständen sei die einzig zulässige Rechtsgrundlage für die in der Vorratsdatenrichtlinie enthaltenen Maßnahmen Titel VI EUV, insbesondere die Art 30, 31 Absatz 1 Buchstabe c und 34 Absatz 2 Buchstabe b.

Weiters sei aus den Erwägungsgründen der Vorratsdatenrichtlinie ersichtlich, dass eine Berufung auf Art 95 EGV als Rechtsgrundlage unangemessen und unhaltbar sei. Die Vorratsdatenrichtlinie sei klar und eindeutig auf die Bekämpfung schwerer Verbrechen gerichtet. Auf Art 95 EGV gestützte Maßnahmen müßten die Angleichung der nationalen Rechtsvorschriften zum Schwerpunkt haben, die das Funktionieren des Binnenmarkts förderten. Ein Mangel aufgrund von Unterschieden der nationalen Rechtsvorschriften sei lediglich behauptet, aber nicht bewiesen worden. Das behauptete Ziel der Vorratsdatenrichtlinie, Verzerrungen des Binnenmarkts zu beseitigen, sei ein reines Nebenziel, das im Vergleich zu dem Hauptziel der Vorratsdatenrichtlinie, die Verbrechensbekämpfung, in den Hintergrund treten würde[47].

Mit der Nichtigkeitsklage Irlands wird daher lediglich ein Kompetenzverstoß geltend gemacht. Inhaltliche Bedenken, etwa ein Verstoß gegen Grundrechte, werden gegen die Vorratsdatenrichtlinie nicht vorgebracht.

Die Erfolgschancen der Klage werden als nicht gering eingeschätzt. Jedenfalls wird die Meinung vertreten, dass die Vorratsdatenrichtlinie kompetenzwidrig erlassen worden ist, weswegen sie vom EuGH für nichtig zu erklären ist[48]. Manche sind sogar der Ansicht, Irlands Nichtigkeitsklage gegen die Vorratsdatenrichtlinie werde „mit an Sicherheit grenzender Wahrscheinlichkeit" Erfolg haben. Sollte Irland im Verfahren vor dem EuGH tatsächlich obsiegen, müßte die Richtlinie 2006/24/EG in den Mitgliedstaaten nicht umgesetzt werden[49]. Nach manchen wäre damit allerdings nicht viel gewonnen. Otto und Seitlinger befürchten, dass selbst dann, wenn der EuGH die Ermächtigungsgrundlage des Art 95 EGV verneinen sollte und die Vorratsdatenrichtlinie für nichtig erklären sollte, die Umsetzung der Inhalte und Ziele der Vorratsdatenrichtlinie durch einen Rahmenbeschluss erfolgen würde[50].

---

[46] Rechtssache C-301/06
[47] Amtsblatt der Europäischen Union, C 237/5
[48] *Gitter/Schnabel,* MMR 7/2007, mwN
[49] *Breyer*, StV 4/2007
[50] *Otto/Seitlinger*, MR 2006, 227

Dass ausgerechnet Irland eine Nichtigkeitsklage eingebracht hat, erscheint insofern interessant, als Irland als eines der ersten europäischen Länder selbst schon vor der Vorratsdatenrichtlinie die Vorratsdatenspeicherung eingeführt und diese Richtlinie daher bereits umgesetzt hat. Die Gemeinschaft ermöglichte es den Mitgliedstaaten durch Art 15 der Richtlinie 2002/58/EG den strengen Datenschutz von Art 6 der Richtlinie 95/46/EG aufzuheben, wenn dies für die nationale Sicherheit (d.h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Die Datenschutzrichtlinie sah jedoch keinesfalls eine Verpflichtung zur Vorratsdatenspeicherung vor; sie ermöglichte sie lediglich. In Irland wurde die Vorratsdatenspeicherung von Telefonverbindungen in Form des Criminal Justice (Terrorist Offences) Act 2005 bereits (vorab) umgesetzt[51]

4.3.2. Präjudiz (Übermittlung von Fluggastdaten in die USA)

Ein ähnlicher Sachverhalt, beziehungsweise ein ähnlicher Kompetenzkonflikt, wurde dem EuGH bereits einmal zur Entscheidung vorgelegt. Mit Urteil vom 30. Mai 2006 erklärte der EuGH die Weitergabe von Fluggastdaten an die USA für rechtswidrig, weil der entsprechende Beschluss sich zu unrecht auf Artikel 95 EGV gestützt hatte[52].

In der Sache ging es darum, dass die Vereinigten Staaten nach den Terroranschlägen des 11. September (2001) Rechtsvorschriften (US Aviation and Transportation Security Act, im folgenden Security Act) [53] erließen, wonach Fluggesellschaften, die Flüge in die oder aus den Vereinigten Staaten oder über deren Gebiet durchführen, den amerikanischen Zoll- und Grenzschutzbehörden (Bureau of Customs and Border Protection of the Department of Homeland Security, im folgenden CBP) einen elektronischen Zugriff auf die Daten ihrer automatischen Reservierungs- und Abfertigungssysteme, die so genannten „Passenger Name Records" (PNR-Daten), gewähren müssen. Ein derartiger PNR wird bei jeder Flugbuchung erstellt und umfaßt insbesondere Name und Anschrift des Reisenden, Kreditkarteninformationen, Informationen zum Reiseverlauf, Sitzplatz, Gesundheitsdaten und Vielfliegerdaten. Um den amerikanischen Behörden Zugang zu diesen Daten zu ermöglichen, sollten die Fluggesellschaften durch eine „Pull Verbindung" einen Link einrichten, wodurch die amerikanischen Behörden freien Zugriff auf die Datenbanken der Fluggesellschaften erhielten[54].

Weil die Kommission befürchtete, dass diese US-amerikanischen Rechtsvorschriften mit den Rechtsvorschriften der Gemeinschaft und der Mitgliedstaaten über den

---

[51] Abrufbar unter http://www.oireachtas.ie/documents/bills28/acts/2005/a0205.pdf
Vgl. auch http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-140716
[52] Az.: C-317/04 und C-318/04
[53] US Aviation and Transportation Security Act vom 19. November 2001
[54] *Sorger*, Übermittlung von Fluggastdaten in die USA, in *Jahnel*, Jahrbuch Datenschutzrecht und E-Government 08, 191 (192)

Schutz personenbezogener Daten in Widerspruch stünden, nahm sie Verhandlungen mit den amerikanischen Behörden auf, um ein bilaterales Abkommen über die Übermittlung der PNR-Daten zu schließen und damit Rechtssicherheit und ein bestmögliches Datenschutzniveau zu ermöglichen. Die USA setzten unterdessen die Anwendbarkeit des Security Act auf europäische Fluglinien, beziehungsweise auf Flüge von der oder in die Europäische Union bis zum 5. März 2003 aus. Nach diesem Zeitpunkt sollte allerdings der Security Act auch auf europäische Fluglinien uneingeschränkt Anwendung finden. Im Falle der Nichtbeachtung des Security Act nach diesem Zeitpunkt, drohten den europäischen Fluggesellschaften Geldstrafen bis zu USD 6.000,00 pro einreisendem Passagier und der Entzug von Landrechten.

Nach Abschluß dieser Verhandlungen erließ die Kommission am 14. Mai 2004 zu 2004/535/EG eine Angemessenheitsentscheidung gemäß Art 25 Abs 6 Datenschutzrichtlinie, die Voraussetzung für die Übermittlung von Daten in Drittstaaten ist. Mit dieser Angemessenheitsentscheidung wurde festgestellt, dass das United States Bureau of Customs and Border Protection (im folgenden CBP) einen angemessenen Schutz für PNR-Daten, die aus der Gemeinschaft übermittelt werden, gewährleistet. Das CBP gab eine Verpflichtungserklärung („undertakings") ab, in welchem geregelt wurde, auf welche Art und Weise das CBP Daten nutzen darf. Darüber hinaus enthielt diese Verpflichtungserklärung Bestimmungen über die Zweckbindung der Daten, eine Liste von 34 Datenkategorien, weiters Bestimmungen über die Vorgehensweise beim Zugriff auf die PNR Daten und die Weitergabemöglichkeit der Daten sowie Informations-, Auskunfts- und Widerspruchsrechte der Betroffenen. Die Übermittlung von sensiblen Daten (Daten aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen) wurde ausgeschlossen, dafür wurde eine Speicherdauer von bis zu acht Jahren festgelegt[55].

Daraufhin erließ der Rat am 17. Mai 2004 auf der Grundlage von Art 95 EGV einen Beschluss zu 2004/496/EG, mit dem der Abschluß eines Abkommens zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die im Hoheitsgebiet der Mitgliedstaaten der Gemeinschaft ansässigen Fluggesellschaften an das CBP genehmigt wurde. Dieses Abkommen wurde am 28. Mai 2004 in Washington unterzeichnet und ist am selben Tag in Kraft getreten.

Die gemäß Art 29 der Datenschutzrichtlinie eingesetzte Datenschutzgruppe äußerte bereits am 13. Juni 2003 Bedenken hinsichtlich des Datenschutzniveaus, das von der CBP zugesagt worden war.

Das Europäische Parlament beantragte daraufhin gemäß Art 230 Abs 3 EGV beim EuGH, den Beschluss des Rates[56] und die Angemessenheitsentscheidung[57] der Kommission für nichtig zu erklären. Das Europäische Parlament rügte, dass weder Art 95

[55] *Sorger*, Übermittlung von Fluggastdaten in die USA, in *Jahnel*, Jahrbuch Datenschutzrecht und E-Government 08, 191 (193)
[56] C-317/04
[57] C-318/04

EGV eine geeignete Rechtsgrundlage für den Beschluss noch Art 25 Datenschutzrichtlinie eine solche für die Angemessenheitsentscheidung war. Das Abkommen diene der Terrorismusbekämpfung, weswegen sie nicht in den Anwendungsbereich der ersten Säule fiele. Weiters wurde ein Verstoß gegen wesentliche Grundsätze der Datenschutzrichtlinie, eine Verletzung des Grundrechtes gemäß Art 8 EMRK und eine Unvereinbarkeit mit dem Grundsatz der Verhältnismäßigkeit geltend gemacht.

Der EuGH verband die beiden Rechtssachen und erklärte beide Rechtsakte aus formalen Gründen für nichtig[58]. Weder die Angemessenheitsentscheidung der Kommission noch der Beschluss des Rates beruhten nach Ansicht des EuGH auf einer geeigneten Rechtsgrundlage. Die materiellen datenschutzrechtlichen Probleme blieben vom EuGH indes unbehandelt[59].

Der EuGH erkannte im wesentlichen, dass die Angemessenheitsentscheidung der Kommission nicht rechtsgültig auf der Grundlage der Richtlinie 95/46/EG (Datenschutzrichtlinie) erlassen werden konnte, weil die Datenschutzrichtlinie keine Anwendung auf die Verarbeitung von personenbezogenen Daten findet, die für Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen. Der EuGH stellte fest, dass die Datenschutzrichtlinie gemäß Art 3 nicht auf die Verarbeitung von personenbezogenen Daten zu Zwecken der öffentliche Sicherheit, der Landesverteidigung, der Sicherheit des Staates und der Tätigkeiten des Staates im strafrechtlichen Bereich Anwendung findet.

Aus der Angemessenheitsentscheidung ergab sich jedoch, dass amerikanische Rechtsvorschriften, die die Verbesserung der Sicherheitslage zum Gegenstand haben, die Rechtsgrundlage für die Datenübermittlung waren und die Gemeinschaft die Vereinigten Staaten uneingeschränkt im Kampf gegen den Terrorismus unterstützte, weswegen die PNR-Daten ausschließlich für Zwecke der Verhütung und Bekämpfung des Terrorismus und damit verknüpfter Straftaten sowie anderer schwerer Straftaten, einschließlich der internationalen organisierten Kriminalität, verwendet wurden.

Weil daher die Angemessenheitsentscheidung nicht in den Anwendungsbereich der Datenschutzrichtlinie fiel, schied diese als Ermächtigungsgrundlage aus. Folglich hat der Gerichtshof die Angemessenheitsentscheidung für nichtig erklärt.

Der Gerichtshof stellte weiters fest, dass Artikel 95 EGV in Verbindung mit Artikel 25 der Datenschutzrichtlinie die Zuständigkeit der Gemeinschaft für den Abschluß des gegenständlichen Abkommens mit den Vereinigten Staaten nicht begründen konnte. Das Abkommen betraf nämlich die gleiche Datenübermittlung wie die Angemessenheitsentscheidung, sohin eine Verarbeitung von Daten, die nicht in den Anwendungsbereich der Datenschutzrichtlinie fiel, weswegen der EuGH den Beschluss des Rates über die Genehmigung des Abkommens ebenfalls für nichtig erklärte.

---

[58] http://curia.europa.eu/de/actu/communiques/cp06/aff/cp060046de.pdf

[59] *Sorger*, Übermittlung von Fluggastdaten in die USA, in *Jahnel*, Jahrbuch Datenschutzrecht und E-Government 08, 191 (195)

Auch bei der Vorratsdatenrichtlinie geht es um Daten, die zunächst im Rahmen einer Dienstleistung (nämlich der Telekommunikation) erhoben worden sind und im Anschluß daran für Zwecke der Strafrechtspflege verwendet werden. Sollte der EuGH diesen Rechtsstandpunkt und diese Argumentation in den (verbundenen) Rechtssachen C-317/04 und C-318/04 beibehalten, könnte die Vorratsdatenrichtlinie tatsächlich der Nichtigkeit anheim fallen[60].

Das ursprüngliche Abkommen zwischen der EG und den USA wurde durch ein Übergangsabkommen abgelöst, das in weiterer Folge durch ein Folgeabkommen am 26. Juli 2007 ersetzt wurde. Diese neue Abkommen sieht nunmehr vor, dass das US Department of Homeland Security die Daten ausschließlich zu Zwecken der Verhütung und Bekämpfung des Terrorismus und damit zusammenhängender Straftaten, von sonstigen schweren Straftaten grenzüberschreitender Art, einschließlich der organisierten Kriminalität, sowie zu Zwecken der Verhütung und Bekämpfung der Flucht vor Haftbefehlen oder vor Gewahrsamnahme im Zusammenhang mit den genannten Straftaten verwenden wird. Festzuhalten ist, dass eine Definition von Straftaten, die mit dem Terrorismus zusammenhängen, oder von schweren Straftaten unterblieben ist, was somit Raum für Interpretation ermöglicht.

Ebenfalls festzuhalten ist, dass im neuen Abkommen eine Regelung fehlt, welche Stellen des US Department of Homeland Security Zugriff auf die PNR Daten erhalten sollen. Ferner kann das US Department of Homeland Security nach eigenem Ermessen die PNR Daten an andere Behörden weitergeben, insoweit diese Behörden Aufgaben im Bereich der Strafverfolgung, der öffentlichen Sicherheit oder der Terrorismusbekämpfung verfolgen und wenn die Weitergabe zu Zwecken verfolgt, diese Behörden bei der Prüfung oder Untersuchung von Fällen zu unterstützen, die im Zusammenhang mit der Terrorismusbekämpfung, der grenzüberschreitenden Kriminalität und der öffentlichen Sicherheit stehen.

Insgesamt unterliegen 19 Datenarten der Vereinbarung. Darunter sind insbesondere PNR-Buchungscode, Datum der Reservierung, Abflugdaten, Namen des Passagiers, verfügbare Vielflieger- und Bonusdaten, alle verfügbaren Zahlungsinformationen, Reiseverlauf, Sitzplatzinformationen und APIS Daten (Advanced Passenger Information System), worunter Namen, Biometriedaten, Geburtsdatum, Nationalität, Passnummer und Geschlecht des Passagiers fallen. Hingegen sind sensible Daten zu löschen.

Die PNR Daten werden nunmehr (beachtliche) sieben Jahre in einer aktiven analytischen Datenbank gespeichert. Danach werden die Daten in einen ruhenden, nicht operationellen Status überführt und weitere acht Jahre gespeichert. In einem Schreiben des US Department of Homeland Security wird vermerkt, dass erwartet wird, die Daten im Anschluß an diese langjährige Speicherdauer zu löschen. Immerhin sind die

[60] *Kosta/Dumortier*, MR-Int 2007, 130

betroffenen Passagiere berechtigt, in die über sie gespeicherten Daten Einsicht zu nehmen[61].

5. Die Rechtslage in Österreich vor der Vorratsdatenspeicherung

5.1. Datenschutzgesetz 2000 und Telekommunikationsgesetz 2003

Eingangs ist festzuhalten, dass die Nutzung der Möglichkeiten der Telekommunikation mit besonderen Gefährdungen verbunden ist, die vor allem aus der Einschaltung eines Vermittlers zur Überwindung der räumlichen Distanz resultieren. Anders als bei einer Kommunikation unter Anwesenden haben die Kommunikationspartner nicht die Möglichkeit, allein über die Rahmenbedingungen der Kommunikation zu bestimmen[62].

In Österreich ist der (allgemeine) Datenschutz im Datenschutzgesetz 2000 (DSG 2000) geregelt. Das Telekommunikationsgesetz 2003 (TKG 2003) beinhaltet darüber hinaus spezielle datenschutzrechtliche Bestimmungen, die auf die Besonderheiten der Telekommunikation abstellen. Gemäß § 92 Abs 1 TKG 2003 sind die Bestimmungen des Datenschutzgesetzes 2000 auch auf Sachverhalte anzuwenden, die das TKG 2003 regeln, insoweit das TKG 2003 – sozusagen als Ausnahme – nichts anderes bestimmt.

Während das Datenschutzgesetz 2000 allgemein natürliche oder juristische Personen, die die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten (Auftraggeber gemäß § 4 Abs 4 DSG), betrifft, richten sich §§ 92 ff TKG 2003 vor allem an Anbieter, das sind gemäß § 92 Abs 3 Z 1 TKG 2003 Betreiber von öffentlichen Kommunikationsdiensten. Es wird somit auf die öffentliche und gewerbliche Erbringung der Übertragung, beziehungsweise Weiterleitung von Signalen auf (nicht notwendigerweise eigenen) Kommunikationsnetzen abgestellt. Aus der Einbeziehung weiterer Kommunikationsinfrastrukturen ergibt sich folglich ein erweiterter Anwendungsbereich des sektorspezifischen Datenschutzes. Das Anbieten von Diensten innerhalb sog Corporate Networks, beziehungsweise Closed User Groups – auch wenn sie von einem Dritten und nicht vom Unternehmen selbst erbracht werden – begründet mangels des Merkmals der Öffentlichkeit keine Anbieterstellung iSd 12. Abschnitts des TKG 2003. Für Dienste der Informationsgesellschaft und nicht-öffentliche Kommunikationsdienste gilt jedoch der allgemeine datenschutzrechtliche Rahmen[63].

In Konkretisierung des Betroffenenbegriffs des DSG 2000 werden vom TKG 2003 Personen geschützt, die mit einem Anbieter einen Vertrag über die Inanspruchnahme der öffentlichen Kommunikationsdienste geschlossen haben (natürliche oder juristische Personen als „Teilnehmer" gem § 3 Z 19 TKG 2003) oder diesen Dienst für private

[61] *Sorger*, Übermittlung von Fluggastdaten in die USA, in *Jahnel*, Jahrbuch Datenschutzrecht und E-Government 08, 191 (203 f)
[62] *Damjanoviv/Holoubek/Kassai/Lehofer/Urbantschitsch*, Handbuch des Telekommunikationsrechts, 240 f
[63] *Damjanoviv/Holoubek/Kassai/Lehofer/Urbantschitsch*, Handbuch des Telekommunikationsrechts, 244 ff

oder geschäftliche Zwecke – auch nur faktisch – nutzen (natürliche Personen als „Benützer" gemäß 92 Abs 3 Z 2 TKG 2003).

5.2. Datenarten

Das TKG 2003 berücksichtigt die verschiedenen Schutzbedürfnisse und Interessenlagen und definiert verschiedene Datenarten. § 92 Abs 3 Z 3 bis 6 TKG 2003 unterscheidet Stamm-, Verkehrs- und Inhaltsdaten.

Die Begriffsbestimmungen des § 92 TKG 2003 orientieren sich an der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation. Einige Begriffsbestimmungen wurden jedoch ergänzt, um den spezifischen Regelungen des Telekommunikationsgesetzes zu entsprechen[64].

5.2.1. Stammdaten

Unter Stammdaten sind gemäß § 92 Abs 3 Z 2 TKG 2003 personenbezogene Daten zu verstehen, die für die Begründung, Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Teilnehmer und Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind. Das Gesetz zählt taxativ[65] den Familiennamen und Vornamen, den akademischen Grad, die Wohnadresse, die Teilnehmernummer und sonstige Kontaktinformation für die Nachricht, Information über Art und Inhalt des Vertragsverhältnisses und die Bonität auf.

5.2.2. Verkehrsdaten

Verkehrsdaten sind gemäß § 92 Abs 2 Z 4 TKG 2003 Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zweck der Fakturierung dieses Vorgangs verarbeitet werden. Verkehrsdaten sind Daten, die sich auf Teilnehmer oder Benutzer beziehen und für den Aufbau einer Verbindung verwendet werden. Gemäß des Erwägungsgrundes 15 der Datenschutzrichtlinie sind unter Verkehrsdaten insbesondere die aktive und passive Teilnehmernummer, die Art des Endgeräts, der Tarifcode, die Gesamtzahl der für den Abrechnungszeitraum zu berechnenden Einheiten, die Art, das Datum, der Zeitpunkt und die Dauer der Verbindung oder sonstigen Nutzung, die übermittelte Datenmenge, die Leitwege, das verwendete Protokoll, das Netz, von dem die Nachricht ausgeht oder an das sie gesendet wird, das Format der Nachricht, sowie andere Zahlungsinformationen, wie Vorauszahlungen, Ratenzahlung, Sperren des Anschlusses oder Mahnungen zu verstehen.

---

[64] ErlRV 128 BlgNr 22. GP

[65] *Damjanoviv/Holoubek/Kassai/Lehofer/Urbantschitsch*, Handbuch des Telekommunikationsrechts, 247 mwN

Unter Verkehrsdaten (iwS Entgeltabrechnungsdaten[66]) sind daher auch Daten zu verstehen, die bei paketvermittelten Diensten zur Übertragung insbesondere im Internet erzeugt werden wie auch die IP - Adresse.

Den Materialien zum Telekommunikationsgesetz 2003 zufolge sind Verkehrsdaten auch jene Informationen, die die gesamte Weiterleitung der Information über das elektronische Kommunikationsnetz umfassen und nicht nur die Weiterleitung an das elektronische Netz, womit die Weiterleitung der Informationen innerhalb des Netzes keiner datenschutzrechtlichen Regelung mehr unterliegen würde[67].

5.2.3.Zugangsdaten

Zugangsdaten sind gemäß § 92 Abs 3 Z 4a TKG 2003 jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und die für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind.

5.2.4. Inhaltsdaten, Nachricht

Inhaltsdaten sind gemäß § 92 Abs 3 Z 5 TKG 2003 die Inhalte übertragener Nachrichten, wobei die Bestimmung auf § 92 Abs 3 Z 7 TKG verweist. Eine Nachricht ist gemäß § 92 Abs 3 Z 7 TKG 2003 jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können.

Handelt es sich bei Stamm- und Verkehrsdaten jeweils um personenbezogene Daten, so sind Inhaltsdaten sämtliche Inhalte übertragener Nachrichten, mögen diese – isoliert betrachtet – auch keinerlei Personenbezug aufweisen[68].

5.2.5. Standortdaten

Standortdaten sind gemäß § 92 Abs 3 Z 6 TKG 2003 Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geographischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben.

In Abgrenzung zu Verkehrsdaten führte die Datenschutzrichtlinie und das TKG 2003 den Begriff der Standortdaten ein. Standortdaten beziehen sich auf den Standort des Endgeräts des Nutzers nach geographischer Länge, Breite und Höhe, die Übertragungsrichtung, den Grad der Genauigkeit der Standortinformationen, die Identifi-

---

[66] *Damjanoviv/Holoubek/Kassai/Lehofer/Urbantschitsch*, Handbuch des Telekommunikationsrechts, 247

[67] ErlRV 128 BlgNr 22. GP

[68] *Damjanoviv/Holoubek/Kassai/Lehofer/Urbantschitsch*, Handbuch des Telekommunikationsrechts, 247

zierung des Netzpunktes, an dem sich das Endgerät zu einem bestimmten Zeitpunkt befindet, und den Zeitpunkt, zu dem die Standortinformationen erfaßt worden sind. Solche Standortdaten ermöglichen es, bestimmte Dienste mit Zusatznutzen, etwa Straßenverkehrsleitsysteme, anzubieten.

5.3. Datenschutz nach dem Datenschutzgesetz 2000

5.3.1. Allgemeiner und besonderer Datenschutz

Bestimmungen zum Datenschutz enthalten ganz allgemein das DSG 2000, die das Grundrecht auf Datenschutz ausführenden §§ 6 ff DSG 2000, die die Zulässigkeit der Verwendung personenbezogener Daten regeln und im speziellen, als kommunikationsspezifischer Datenschutz, die §§ 96 bis 105 TKG 2003, die die Zulässigkeit der Verwendung von Stamm-, Verkehrs- und Inhaltsdaten regeln.

5.3.2. Treu und Glauben

Aufgrund des ergänzenden Charakters des kommunikationsspezifischen Datenschutzes sind auch bei Datenverwendungen nach den §§ 96 ff TKG 2003 insbesondere die allgemeinen Grundsätze des DSG 2000 zur Verwendung von Daten, etwa die Verwendung nach „Treu und Glauben", oder der konkretisierte Grundsatz der Zweckbindung zu beachten[69]. Zur näheren Festlegung dessen, was in einzelnen Bereichen als Verwendung von Daten nach Treu und Glauben anzusehen ist, können für den privaten Bereich die gesetzlichen Interessenvertretungen, sonstige Berufsverbände und vergleichbare Einrichtungen Verhaltensregeln ausarbeiten[70].

5.3.3. Zweckbindung

Darüber hinaus sieht das DSG 2000 ein zweistufiges Zulässigkeitskonzept für die Verarbeitung personenbezogener Daten (das sind gemäß § 4 Z 1 DSG 2000 Angaben über natürliche oder juristische Personen, deren Identität bestimmt oder bestimmbar ist) vor. Im Mittelpunkt dieser Zulässigkeitsprüfung steht die strikte Zweckbindung. Gemäß § 6 Abs 1 DSG 2000 dürfen Daten nur nach Treu und Glauben, auf rechtmäßige Weise verwendet werden, für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden und nur insofern, soweit sie für den Zweck der Datenanwendung wesentlich sind, und über diesen Zweck nicht hinausgehen.

Gemäß § 6 Abs 1 Z 5 DSG 2000 dürfen Daten nur solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt worden sind, erforderlich ist. Eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen, Vorschriften ergeben.

Gemäß § 7 Abs 1 DSG 2000 dürfen Daten nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen

---

[69] *Damjanoviv/Holoubek/Kassai/Lehofer/Urbantschitsch*, Handbuch des Telekommunikationsrechts, 248 ff

[70] *Mayer-Schönberger/Brandl*, Datenschutzgesetz, 2. Auflage, 26

Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen. Die Zulässigkeit der Datenverwendung ist nach dem DSG 2000 daher von schutzwürdigen Geheimhaltungsinteressen abhängig[71].

5.4. Datenschutz nach dem Telekommunikationsgesetz 2003

5.4.1. § 96 TKG 2003

Der das Datenschutzrecht beherrschende Zweckbindungsgrundsatz erfährt durch § 96 TKG 2003 eine konkrete Ausgestaltung, wonach Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten nur für Zwecke der Besorgung eines Kommunikationsdienstes ermittelt oder verarbeitet werden dürfen. Die Übermittlung dieser Daten darf gemäß § 96 Abs 2 TKG 2003 nur dann und insoweit erfolgen, soweit das für die Erbringung jenes Kommunikationsdienstes, für den diese Daten ermittelt und verarbeitet worden sind, durch den Betreiber erforderlich ist.

Der Anbieter, das ist gemäß § 92 Abs 2 TKG 2003 der Betreiber von öffentlichen Kommunikationsdiensten, ist gemäß § 96 Abs 3 TKG verpflichtet, den Teilnehmer oder Benutzer darüber zu informieren, welche personenbezogenen Daten er ermitteln, verarbeiten und übermitteln wird, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden. Diese Information hat gemäß § 96 Abs 3 TKG 2003 auch auf das Recht hinzuweisen, die Verarbeitung zu verweigern.

Die Ermittlung und Verarbeitung von Stammdaten sowie die Speicherung von Verkehrsdaten ist in § 97 TKG 2003, beziehungsweise in § 99 TKG 2003, zusätzlich geregelt worden.

5.4.2. Verwendung von Stammdaten

Stammdaten dürfen für die Abwicklung des Rechtsverhältnisses (Abschluß, Durchführung, Änderung oder Beendigung des Vertrages mit dem Benutzer, Verrechnung der Entgelte) und die Erstellung von Teilnehmerverzeichnisses gemäß § 18 TKG 2003 sowie für die Erteilung von Auskünften an Notrufträgern ermittelt und verarbeitet werden. Gemäß § 97 Abs 2 TKG 2003 sind die Stammdaten spätestens nach Beendigung der vertraglichen Beziehungen mit dem Teilnehmer vom Betreiber zu löschen. Insofern Stammdaten für Fakturierungszwecke notwendig sind, ist eine weitere Aufbewahrung gemäß § 97 Abs 2 TKG 2003 zulässig.

5.4.3. Verwendung von Verkehrsdaten

Verkehrsdaten dürfen gemäß § 99 Abs 1 TKG 2003 grundsätzlich nicht gespeichert werden und sind vom Betreiber nach Beendigung der Verbindung unverzüglich zu

[71] *Mayer-Schönberger/Brandl*, Datenschutzgesetz, 2. Auflage, 21

löschen oder zu anonymisieren. Der genaue Zeitpunkt des Abschlusses der Übermittlung einer Nachricht, nach dem die Verkehrsdaten außer zu Fakturierungszwecken gelöscht werden sollen, kann von der Art des bereitgestellten elektronischen Kommunikationsdienstes abhängen. Bei einem Sprach-Telefonanruf ist die Übermittlung abgeschlossen, sobald einer der Teilnehmer die Verbindung beendet. Bei der elektronischen Post ist die Übermittlung dann abgeschlossen, wenn der Adressat der Nachricht – üblicherweise vom Server seines Diensteanbieters – abruft[72].

Sofern dies für Zwecke der Verrechnung von Entgelten, einschließlich der Entgelte für Zusammenschaltungen, erforderlich ist, hat der Betreiber gemäß § 99 Abs 2 TKG 2003 Verkehrsdaten, beziehungsweise Entgeltabrechnungsdaten, bis zum Ablauf jener Frist zu speichern, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann. Ist daher die Forderung gemäß § 1486 ABGB verjährt oder hat der Benutzer die Rechnung anerkannt und bezahlt, besteht kein Grund, diese Daten zu Zwecken der Aufrechnung aufzubewahren[73].

Ebenso dürfen diese Daten gemäß § 99 Abs 2 TKG 2003 nicht gelöscht werden, solange ein Verfahren vor der Schlichtungsstelle anhängig ist. Dies liegt allerdings vor allem im Interesse des Anbieters, weil er nach allgemeinen zivilrechtlichen Regeln im Streitfall nachweisen muß, dass der Benutzer die in Rechnung gestellten Leistungen auch bezogen hat. Der Umfang der gespeicherten Verkehrsdaten ist gemäß § 99 Abs 2 TKG 2003 auf das unbedingt notwendige zu beschränken.

Die Verwendung der Daten zu Marketingzwecken, für Dienste mit Zusatznutzen sowie sonstige Übermittlungen darf gemäß § 99 TKG 2003 nur auf Grund der jederzeit widerrufbaren Zustimmung der Nutzer erfolgen

Von der in Art 15 der Datenschutzrichtlinie für elektronische Kommunikation vorgesehenen Ermächtigung, Daten während einer begrenzten Zeit aufzubewahren, insoweit dies für die nationale Sicherheit (daher die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist, hat der österreichische Gesetzgeber (bislang) keinen Gebrauch gemacht[74].

Weil Entgeltabrechnungsdaten gemäß § 99 Abs 2 TKG 2003 nur gespeichert werden dürfen, soweit dies für Zwecke der Verrechnung erforderlich ist, ist bei Tarifmodellen, bei denen nicht nach der jeweiligen Verbindung unterschieden, sondern pauschal

[72] Siehe ErwG 27 Datenschutzrichtlinie für elektronische Kommunikation
[73] *Damjanoviv/Holoubek/Kassai/Lehofer/Urbantschitsch*, Handbuch des Telekommunikationsrechts, 254
[74] *Damjanoviv/Holoubek/Kassai/Lehofer/Urbantschitsch*, Handbuch des Telekommunikationsrechts, 255

pro Zeiteinheit abgerechnet wird, vor allem im Internet (sogenannte „Flatrate"), eine Speicherung grundsätzlich nicht erforderlich[75].

5.4.4. Inhaltsdaten

Inhaltsdaten dürfen gemäß § 101 Abs 1 TKG 2003 - sofern die Speicherung nicht einen wesentlichen Bestandteil des Kommunikationsdienstes darstellt – grundsätzlich nicht gespeichert werden. Ist allerdings aus technischen Gründen eine kurzfristige Speicherung erforderlich, hat der Anbieter nach Wegfall dieser Gründe die gespeicherten Daten unverzüglich zu löschen. Der Anbieter hat gemäß § 101 Abs 2 TKG 2003 durch technische und organisatorische Vorkehrungen sicherzustellen, dass Inhaltsdaten nicht oder nur in dem aus technischen Gründen erforderlichen Mindestmaß gespeichert werden. Sofern die Speicherung des Inhaltes Dienstemerkmal ist, sind die Daten unmittelbar nach der Erbringung des Dienstes zu löschen. Zu denken ist hierbei an die Speicherung von Inhaltsdaten im Rahmen sogenannter (Sprach-)Mailboxdiensten oder die Versendung von Kurznachrichten über einen Short Message Service (SMS). Die Pflicht zu ehestmöglichen Löschung besteht auch hier, wobei das Speicherverbot, beziehungsweise Löschungsgebot sich nicht an die an der Kommunikation beteiligten Benutzer bezieht[76].

5.4.5. Standortdaten

Standortdaten sind in der Regel ein Spezialfall der Verkehrsdaten und werden in den meisten Fällen von den Regelungen über Verkehrsdaten abgedeckt.

Ungeachtet der Verpflichtung der Betreiber gemäß § 98 TKG 2003 in Notfällen, die nur durch Auskünfte abgewehrt werden können, Betreiber von Notrufdiensten entsprechend zu informieren, dürfen gemäß § 102 Abs 1 TKG 2003 andere Standortdaten als Verkehrsdaten nur verarbeitet werden, wenn sie entweder anonymisiert werden oder die Nutzer hierzu eingewilligt haben. Diese Einwilligung ist jederzeit widerruflich. Darüber hinaus ist auch jenen Nutzern, die der Datenverarbeitung zugestimmt haben, gemäß § 102 Abs 2 TKG 2003 die Möglichkeit einzuräumen, diese Verarbeitung einfach und kostenlos zeitweise zu untersagen.

Zusätzliche Regelungen, bezogen auf den Standort des Teilnehmers, normiert Art 9 der Datenschutzrichtlinie. Diese Bestimmungen beziehen sich auf standortbezogene Mehrwertdienste und werden durch § 102 TKG 2003 abgedeckt.

§ 102 Abs 3 TKG 2003 umfaßt zudem located-based-services (standortbezogene Dienste). Dabei handelt es sich um Dienste, die dem Benutzer ortsbezogene Informationen anhand des vom Mobilfunknetz festgestellten, aktuellen Standorts des mobilen Endgerätes bereitstellen. Dadurch ist es möglich, einem Benutzer Adressen der

[75] *Jahnel*, Datenschutz im Internet, Rechtsgrundlagen, Cookies und Web-logs, ecolex 2001, 89
[76] *Damjanoviv/Holoubek/Kassai/Lehofer/Urbantschitsch*, Handbuch des Telekommunikationsrechts, 257

nächstgelegenen Tankstellen oder Hotels, etc… zur Verfügung zu stellen[77]. Die Verarbeitung von Standortdaten, die aufgrund der Bereitstellung eines Dienstes mit Zusatznutzen entstehen, ist auf das hierfür erforderliche Maß und auf Personen zu beschränken, die im Auftrag des Betreibers oder des Dritten handeln, der den Dienst mit Zusatznutzen anbietet.

5.5. Kommunikationsgeheimnis

Das Fernmeldegeheimnis ist in § 93 TKG 2003 geregelt und unterscheidet sich vom verfassungsrechtlich verankerten Schutz des Art 10a StGG und Art 8 EMRK vor allem im Adressatenkreis. Während die genannten Grundrechte in erster Linie als Abwehrrechte gegen den Staat konzipiert sind, soll § 93 TKG 2003 vor Eingriffen Privater schützen. Das Kommunikationsgeheimnis wendet sich daher an Anbieter und alle Personen, die an der Tätigkeit des Anbieters mitwirken. Keine Anwendung findet das Kommunikationsgeheimnis auf den Partner der Kommunikation. § 93 TKG 2003 soll die Vertraulichkeit der Kommunikation, beziehungsweise genauer, den Schutz der Privatsphäre umfassend sicherstellen[78].

Gemäß § 93 Abs 3 TKG 2003 ist das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Nutzer unzulässig.

5.6. Auskunftspflichten nach der bisherigen Rechtslage

5.6.1. Strafprozessordnung

Gemäß § 92 Abs 2 TKG 2003 bleiben die Bestimmungen der Strafprozessordnung durch die Bestimmungen des TKG 2003 unberührt.

Der Anbieter, daher der Betreiber von öffentlichen Kommunikationsdiensten, ist nach Maßgabe der Überwachungsverordnung (BGBl. II Nr. 418/2001) verpflichtet, alle Einrichtungen bereitzustellen, die zur Überwachung einer Telekommunikation nach den Bestimmungen der StPO erforderlich sind. Der Betreiber (gemeint wohl „Anbieter") ist gemäß § 94 Abs 2 TKG 2003 verpflichtet, an der Überwachung einer Telekommunikation nach den Bestimmungen der Strafprozessordnung im erforderlichen Ausmaß mitzuwirken.

Im 5. Abschnitt der Strafprozessordnung ist die Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung sowie Überwachung von Nachrichten und von Personen geregelt.

Gemäß § 134 Z 2 StPO ist die „Auskunft über Daten einer Nachrichtenübermittlung" die Erteilung einer Auskunft über Verkehrsdaten iSd § 92 Abs 3 Z 4 TKG 2003, über Zu-

[77] *Damjanoviv/Holoubek/Kassai/Lehofer/Urbantschitsch*, Handbuch des Telekommunikationsrechts, 257
[78] *Damjanoviv/Holoubek/Kassai/Lehofer/Urbantschitsch*, Handbuch des Telekommunikationsrechts, 263

gangsdaten iSd § 92 Abs 3 Z 4a TKG 2003 und über Standortdaten iSd § 92 Abs 3 Z 6 TKG 2003 eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft iSd des § 1 Abs 1 Z 2 NotifG 1999.

Im Sinne des § 1 Abs 1 Z 2 NotifG 1999 ist ein „Dienst" eine Dienstleistung der Informationsgesellschaft. Das ist jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung, wobei eine „im Fernabsatz erbrachte Dienstleistung" gemäß § 1 Abs 1 Z 2 lit a NotifG 1999 eine Dienstleistung ist, die ohne gleichzeitige physische Anwesenheit der Parteien erbracht wird. Eine „elektronisch erbrachte Dienstleistung" ist gemäß § 1 Abs 1 Z 2 lit b NotifG 1999 eine Dienstleistung, die mittels Geräten für die elektronische Verarbeitung, einschließlich digitaler Kompression, und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen und vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischen Weg gesendet, weitergeleitet und empfangen wird.

Eine „auf individuellen Abruf eines Empfängers erbrachte Dienstleistung" ist gemäß § 1 Abs 1 Z 2 lit c NotifG 1999 eine Dienstleistung, die durch die Übertragung von Daten auf individuelle Anforderung erbracht wird.

Gemäß § 134 Z 3 StPO ist das „Überwachen von Nachrichten" das Ermitteln des Inhalts von Nachrichten iSd § 92 Abs 3 Z 7 TKG 2003, die über ein Kommunikationsnetz iSd § 3 Z 11 TKG oder einen Dienst der Informationsgesellschaft iSd § 1 Abs 1 Z 2 NotifG 1999 ausgetauscht oder weitergeleitet werden.

Die Definition der Überwachung von Nachrichten in § 134 Z 3 StPO soll nach den Erläuternden Bemerkungen zur Regierungsvorlage zum Strafprozessreformgesetz[79] nicht mehr ausschließlich auf die Übertragung von Nachrichten durch Telekommunikation abstellen, sondern auch andere Übertragungstechniken berücksichtigen. Die Definition soll demnach auch bestimmte, mittels eines Computersystems übertragene Kommunikationen erfassen, welche allerdings – wie es dem Verständnis der Art 20 und 21 der Cyber-Crime-Konvention entspricht – die Übertragung der Kommunikation über Telekommunikationsnetzwerke vor deren Empfang durch ein anderes Computersystem einschließen können.

Die Überwachung von Nachrichten gemäß § 135 StPO erfaßt daher auch den Inhalt der Nachrichten, welcher durch Mithören, Abhören, Aufzeichnen, Abfangen, etc registriert, beziehungsweise sichergestellt werden soll.

Die Auskunft über Daten einer Nachrichtenübermittlung ist gemäß § 135 Abs 2 Z 1 StPO zulässig, wenn der dringende Verdacht besteht, dass eine von der Auskunft betroffene Person eine andere entführt oder sich sonst ihrer bemächtigt hat und sich die Auskunft auf Daten einer solchen Nachricht beschränkt, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung vom Beschuldigten übermittelt, empfangen oder gesendet wird.

[79] 25 BlgNR 23. GP

Sie ist gemäß § 135 Abs 2 Z 2 StPO ferner zulässig, wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zugestimmt hat.

Die Auskunft über Daten einer Nachrichtenübermittlung ist gemäß § 135 Abs 2 Z 3 StPO weiters zulässig, wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.

Die Auskunft über Daten einer Nachrichtenübermittlung ist gemäß § 137 Abs 1 StPO von der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen. Gemäß § 137 Abs 3 StPO darf die Auskunft über Daten einer Nachrichtenübermittlung sowohl für einen künftigen als auch für einen vergangenen Zeitraum angeordnet werden.

Gemäß § 138 Abs 2 StPO sind Anbieter iSd § 92 Abs 1 Z 3 TKG 2003 und sonstige Diensteanbieter iSd §§ 13, 16 und 18 Abs 2 des E-Commerce Gesetzes verpflichtet, Auskunft über Daten einer Nachrichtenübermittlung zu erteilen und an einer Überwachung von Nachrichten mitzuwirken.

Gemäß § 139 Abs 4 StPO sind auf Antrag des Beschuldigten oder von Amts wegen die Ergebnisse der Ermittlungsmaßnahme zu vernichten, wenn diese für ein Strafverfahren nicht von Bedeutung sein können oder als Beweismittel nicht verwendet werden dürfen. Betroffenen einer Ermittlungsmaßnahme steht gemäß § 139 Abs 4 StPO ebenfalls ein Antragsrecht zu, insoweit für sie bestimmte oder von Ihnen ausgehende Nachrichten oder Bilder, auf denen sie dargestellt sind, oder von ihnen geführte Gespräche betroffen sind.

Sämtliche Ergebnisse einer Überwachung einer Nachricht sind gemäß § 145 Abs 1 StPO vom Gericht nach rechtskräftigem Abschluß des Verfahrens zu löschen, soweit sie nicht in einem anderen, bereits anhängigen Strafverfahren als Beweismittel Verwendung finden. Ebenso hat auch die Staatsanwaltschaft im Fall der Einstellung des Verfahrens die Ergebnisse zu löschen.

5.6.2. Sicherheitspolizeigesetz

Das am 1. Jänner 2008 in Kraft getretene Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Grenzkontrollgesetz und das Polizeikooperationsgesetz geändert worden sind, hat unter anderem eine Neufassung, beziehungsweise Ergänzung jener Bestimmungen des § 53 SPG gebracht, welche die Auskunftsrechte der Sicherheitsbehörden gegenüber Betreibern öffentlicher Telekommunikationsdienste regeln. Derartige sicherheitspolizeiliche Anfragen bezogen sich bis zum 31. Dezember 2007, daher nach der alten Rechtslage, im Wesentlichen nur auf Namen, Anschrift und Teilnehmernummern. Nach der neuen Rechtslage reicht die Bandbreite zulässiger Anfragen für Zwecke der Gefahrenabwehr weit darüber hinaus und umfaßt zusätz-

lich nunmehr auch Anfragen nach IP-Adressen und nach dem Standort sowie der internationalen Mobilteilnehmerkennung (sogenannte International Mobile Subscriber Identity, kurz IMSI) von Mobiltelefonen[80].

Gemäß § 53 Abs 3a SPG sind die Sicherheitsbehörden nunmehr berechtigt, von Betreibern öffentlicher Telekommunikationsdienste gemäß § 92 Abs 3 Z 1 TKG 2003 und sonstigen Diensteanbietern gemäß § 3 Z 2 ECG Auskunft zu verlangen über

1. Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses,

2. Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung sowie

3. Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war,

wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen und sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen. Die Bezeichnung eines Anschlusses nach Z 1 kann für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluß geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen.

Diese Auskunftspflicht betrifft daher

1. die Erfüllung sicherheitspolizeilicher Aufgaben, womit gemäß § 3 SPG die Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit (ausgenommen die örtliche Sicherheitspolizei)umfaßt sind, und

2. die allgemeine Hilfeleistungspflicht gemäß § 19 SPG und Abwehr gefährlicher Angriffe gemäß § 21 SPG.

Die Sicherheitsbehörden trifft dann die erste allgemeine Hilfeleistungspflicht gemäß § 19 Abs 1 SPG, wenn Leben, Gesundheit, Freiheit oder Eigentum von Menschen gegenwärtig gefährdet oder eine solche Gefährdung unmittelbar bevorsteht.

Ein gefährlicher Angriff ist gemäß § 16 Abs 2 SPG die Bedrohung eines Rechtsgutes durch die rechtswidrige Verwirklichung des Tatbestandes einer gerichtlich strafbaren Handlung, die vorsätzlich begangen und nicht bloß auf Begehren eines Beteiligten verfolgt wird, sofern es sich um einen Straftatbestand nach dem Strafgesetzbuch (ausgenommen die Tatbestände nach den §§ 278, 278a und 278b StGB), nach dem Verbotsgesetz, nach dem Fremdenpolizeigesetz 2005 oder nach dem Suchtmittelgesetz handelt (ausgenommen Handlungen, die dem Erwerb oder Besitz eines Suchtmittels zum eigenen Gebrauch dienen). Ein gefährlicher Angriff ist gemäß § 16 Abs 3

[80] *Kunnert*, Der sicherheitspolizeiliche Griff nach Telekommunikationsdaten, in *Jahnel*, Jahrbuch Datenschutzrecht und E-Government 08, 83 (84 f)

SPG ferner ein Verhalten, das darauf abzielt und geeignet ist, eine Bedrohung gemäß § 16 Abs 2 SPG vorzubereiten, sofern dieses Verhalten in engem zeitlichen Zusammenhang mit der angestrebten Tatbestandsverwirklichung gesetzt wird.

Das Auskunftsbegehren ist nur dann gerechtfertigt, sofern die Maßnahme eine wesentliche Voraussetzung zur Erfüllung der den Sicherheitsbehörden übertragenen Aufgabe bildet, womit eine stärkere Betonung der Erforderlichkeit im Sinne einer Subsidiarität gegenüber gelinderen Eingriffen zum Ausdruck gebracht wird[81]. Die Regelung des § 53 Abs 3a Z 1 SPG stellt sich als gesetzliche Ermächtigung zur behördlichen Ermittlung personenbezogener Daten iSd § 1 Abs 2 DSG 2000 und damit zum Eingriff in das Grundrecht der Betroffenen auf Datenschutz dar. Dementsprechend ordnet § 51 Abs 2 SPG vorbehaltlich abweichender ausdrücklicher Bestimmungen an, dass auf das Verwenden personenbezogener Daten die Bestimmungen des DSG 2000 Anwendung finden. Gemäß § 6 Abs 1 Z 3 DSG 2000 dürfen Daten nur verwendet werden, soweit sie für den Zweck der Datenanwendung wesentlich sind und über diesen Zweck nicht hinausgehen. Darüber hinaus setzt die Zulässigkeit einer Datenverwendung voraus, dass die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen. Die Verhältnismäßigkeit zwischen angestrebtem Ziel und Mitteleinsatz muß daher gewahrt bleiben[82].

Die nunmehr erfolgte Aufnahme der IP-Adresse unter jene Daten, die einer Auskunftspflicht nach dem SPG unterliegen, hat eine Meinungsverschiedenheit zwischen den Sicherheitsbehörden und den Anbietern von Internetdiensten beendet. Die Sicherheitsbehörden vertraten bereits nach der alten Rechtslage (bis zum 31. Dezember 2007) die Auffassung, dass die IP-Adresse einer Auskunftspflicht nach dem SPG unterliegt. Die frühere gesetzliche Formulierung „Teinehmernummer eines bestimmten Anschlusses" hätte nach Ansicht der Sicherheitsbehörden, die Anbieter von Internetdiensten bereits zur Vorlage einer IP-Adresse verpflichtet, weil die IP-Adresse zum konkreten Zeitpunkt der Anfrage ein statisches Element gewesen sei. Die Anbieter von Internetdiensten teilten diese Rechtsauffassung nicht und verlangten einen Gerichtsbeschluss auf der Grundlage der StPO[83].

Gemäß § 63 Abs 1 SPG ist unverzüglich eine Richtigstellung oder Löschung vorzunehmen, wenn festgestellt wird, dass unrichtige oder entgegen den Bestimmungen dieses Bundesgesetzes ermittelte Daten aufbewahrt werden. Personenbezogene Daten sind ferner zu löschen, sobald sie für die Erfüllung der Aufgabe, für die sie verwendet worden sind, nicht mehr benötigt werden, es sei denn, für ihre Löschung wäre eine besondere Regelung getroffen worden.

---

[81] *Damjanoviv/Holoubek/Kassai/Lehofer/Urbantschitsch*, Handbuch des Telekommunikationsrechts, 273

[82] *Kunnert*, Der sicherheitspolizeiliche Griff nach Telekommunikationsdaten, in *Jahnel*, Jahrbuch Datenschutzrecht und E-Government 08, 83 (97)

[83] *Kunnert*, Der sicherheitspolizeiliche Griff nach Telekommunikationsdaten, in *Jahnel*, Jahrbuch Datenschutzrecht und E-Government 08, 83 (98)

Die Novelle des SPG wurde schon im Vorfeld, daher bereits im Begutachtungsstadium, kritisiert. Es wurde inbesondere auf das nunmehr (nach der Novelle des SPG) vorhandene Mißbrauchspotential hingewiesen, das darin liegt, dass Sicherheitsbehörden im Wege einer formlosen Anfrage, die unverzüglich und kostenlos zu beantworten ist, künftig nicht nur Stammdaten von Nutzern, sondern auch Verkehrsdaten erhalten werden. Es wird befürchtet, dass Auskunftsmöglichkeiten in der polizeilichen Praxis auch außerhalb konkreter Gefahrensituationen in Anspruch genommen werden und dadurch die Kommunikation unbescholtener Bürger ausgespäht würde.

Festzuhalten ist, dass die Sicherheitsbehörden die oben erwähnten Daten völlig formfrei und vor allem ohne richterliche Genehmigung anfordern können. Es fehlt jegliche, daher auch nachträgliche, richterliche Kontrolle über das Auskunftsrecht der Sicherheitsbehörden. Die Einrichtung eines Rechtsschutzbeauftragten, der zu informieren ist und der Auskunftsrechte hat sowie berechtigt ist, Räume zu betreten, in denen Überwachungsergebnisse aufbewahrt werden[84], wird als unzureichend betrachtet.

Ebenso wird releviert, dass Betroffene nur dann von einer Überwachung, beziehungsweise einem Auskunftsbegehren der Sicherheitsbehörden, Kenntnis erlangen, wenn ein Strafverfahren eingeleitet worden ist.

Darüber hinaus wurde gerügt, dass zentrale Gesetzesbegriffe, wie beispielsweise „konkrete Gefahrensituation" (zu) unbestimmt wären. Die Anbieter von Internetdiensten befürchteten, dass die Überwachung eine vermehrte Unsicherheit bei den Bürgern nach sich ziehen würde und dass es letztlich zu einer Abnahme der Internetnutzung käme.

Im Zusammenhang mit der Vorratsdatenspeicherung wurde vorgebracht, dass die Betreiber von Kommunikationsdiensten noch vor dem Inkrafttreten der entsprechenden Umsetzung der Vorratsdatenrichtlinie in die österreichische Rechtsordnung bereits zu einer Speicherung von Verkehrsdaten gezwungen werden, weil sie sonst die durch die SPG Novelle erweiterten Auskunftsbefugnisse der Sicherheitsbehörden nicht erfüllen könnten[85].

Zweifellos brachte die Novelle des SPG eine (weitere) Aushöhlung von Grundrechten. Die Sicherheitsbehörden sind im Grunde nach eigenem Ermessen berechtigt, Verkehrsdaten von Betreibern öffentlicher Kommunikationsdienste zu verlangen, ohne jedoch zuvor die Entscheidung eines Richters einholen zu müssen. Es fehlt ein effizienter Individualrechtsschutz. Die oben erwähnten Rechte des Rechtsschutzbeauftragten müssen meines Erachtens angesichts der weitreichenden Möglichkeiten der Sicherheitsbehörden als völlig unzureichend angesehen werden.

---

[84] §§ 91a SPG ff

[85] *Kunnert*, Der sicherheitspolizeiliche Griff nach Telekommunikationsdaten, in *Jahnel*, Jahrbuch Datenschutzrecht und E-Government 08, 83 (88 f)

5.6.3. E-Commerce Gesetz

Gemäß § 18 Abs 2 ECG haben die in den §§ 13 und 16 ECG genannten Diensteanbieter (Access- und Host-Provider) auf Grund der Anordnung eines dazu gesetzlich befugten inländischen Gerichtes, diesem alle Informationen zu übermitteln, an Hand deren die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Übermittlung oder Speicherung von Informationen abgeschlossen haben, zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen ermittelt werden können.

Das Gericht bedarf neben dieser Bestimmung einer weiteren gesetzlichen Grundlage (arg.: „… eines dazu gesetzlich befugten inländischen Gerichtes…"). Eine bloße „Note" reicht für die Zulässigkeit der Datenübermittlung nicht aus; es muß ein gerichtlicher Beschluss vorliegen.

Gemäß § 18 Abs 3 ECG haben die in § 16 genannten Diensteanbieter (Host-Provider) auf Grund der Anordnung einer Verwaltungsbehörde, dieser den Namen und die Adressen der Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, zu übermitteln, sofern die Kenntnis dieser Informationen eine wesentliche Voraussetzung der Wahrnehmung der der Behörde übertragenen Aufgaben bildet.

Gemäß § 18 Abs 4 ECG haben die in § 16 genannten Diensteanbieter (Host-Provider) den Namen und die Adresse eines Nutzers ihres Dienstes, mit dem sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, auf Verlangen dritten Personen zu übermitteln, sofern diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts haben sowie überdies glaubhaft machen, dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.

5.6.4. Urheberrechtsgesetz

Gemäß § 87b Abs 3 haben Vermittler im Sinn des § 81 Abs 1a UrhG (Access-Provider, Suchmaschinen-Betreiber, Caching-Anbieter, Host-Provider und Linksetzer) dem (in seinen Urheberrechten) Verletzten auf dessen schriftliches und ausreichend begründetes Verlangen Auskunft über die Identität des Rechteverletzers (Name und Anschrift) beziehungsweise die zur Feststellung des Verletzers erforderlichen Auskünfte zu erteilen. In die Begründung sind insbesondere hinreichend konkretisierte Angaben über die den Verdacht der Rechtsverletzung begründenden Tatsachen aufzunehmen. Der Verletzte hat dem Vermittler die angemessenen Kosten der Auskunftserteilung zu ersetzen. Dieser zivilrechtliche Anspruch steht daher Rechteinhabern zu, deren Rechte nach dem Urheberrechtsgesetz verletzt worden sind. Anspruchsgegner sind Vermittler iSd § 81 Abs1a UrhG. Im Streitfall über das Bestehen eines Auskunftsan-

spruchs entscheidet ein ordentliches Gericht. Ein Rechtsschutz der betroffenen Nutzer ist nicht vorgesehen[86].

5.6.5. Militärbefugnisgesetz

Gemäß § 22 Abs 2a MBG dürfen Militärische Organe und Dienststellen nach Abs 1 (das sind jene, die mit Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr betraut sind und zur Wahrnehmung der damit verbundenen Aufgaben Daten verarbeiten) von den Betreibern öffentlicher Telekommunikationsdienste jene Auskünfte über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses verlangen, die diese Organe und Dienststellen als wesentliche Voraussetzung zur Erfüllung von Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr benötigen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen.

5.6.6. § 90 Abs 6 TKG

Gemäß § 90 Abs 6 TKG 2003 sind Betreiber von Kommunikationsdiensten verpflichtet, Verwaltungsbehörden auf deren schriftliches und begründetes Verlangen Auskunft über Stammdaten im Sinne von § 92 Abs 3 Z 3 lit a bis e von Teilnehmern zu geben, die in Verdacht stehen, durch eine über ein öffentliches Telekommunikationsnetz gesetzte Handlung eine Verwaltungsübertretung begangen zu haben. In den Erläuterungen zu dieser Bestimmung heißt es dazu lediglich, dass die Verwaltungsbehörden diese Informationen zur Durchführung von Verwaltungsstrafverfahren benötigen. Offenbar soll sich die Auskunftspflicht nicht nur auf solche Verwaltungsstraftatbestände beziehen, die an öffentliche Kommunikationsnetze oder –dienste anknüpfen, sondern allgemein sämtliche Verwaltungsübertretungen erfassen, die auch nur mit Hilfe und auch unabhängig von elektronischer Kommunikation verwirklicht werden können[87].

5.6.7 Fazit (Auskunftspflichten nach der bisherigen Rechtslage)

Die Anbieter waren bislang aufgrund der oben erwähnten Vorschriften verpflichtet, Auskünfte über Verkehrsdaten, Zugangsdaten, Stammdaten und Standortdaten zu erteilen. Allerdings besteht diese Verpflichtung nur dann, insoweit Daten vorhanden sind. Es besteht bislang keine (rechtliche) Verpflichtung, Daten auf Vorrat zu speichern[88]. Auch nach den Bestimmungen der StPO ist es bislang nicht verlangt gewesen, dass neue technische Möglichkeiten geschaffen werden, um beispielsweise Daten zu sichern, die nur so kurz im System vorhanden sind, dass sie auf ein Ersuchen oder eine Anordnung hin kaum gesichert werden können. Es sollte lediglich eine eindeutige Befugnis geschaffen werden, welche die Sicherung und Weitergabe existie-

[86] Stellungnahme des europäischen Zentrum für e-commerce und internetrecht im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007
[87] *Damjanoviv/Holoubek/Kassai/Lehofer/Urbantschitsch*, Handbuch des Telekommunikationsrechts, 275
[88] *Otto/Seitlinger*, MR 2006, 227

render und rechtmäßig gespeicherter Daten im Zusammenhang mit strafrechtlichen Ermittlungen zu verlangen gestattet[89].

6. Umsetzung der Vorratsdatenrichtlinie in österreichische Recht

Die Umsetzung der Vorratsdatenrichtlinie in die österreichische Rechtsordnung soll durch eine Novelle des Telekommunikationsgesetzes 2003[90] erfolgen und die nachstehenden Neuerungen bringen. Zunächst ist allerdings festzuhalten, dass bisher kein nationaler Umsetzungsakt für die Vorratsdatenrichtlinie erlassen worden ist. Österreich ist daher in der Umsetzung der Vorratsdatenrichtlinie betreffend Telefonfestnetz und Mobilfunk säumig[91].

6.1. Benutzer

§ 92 Abs 3 Z 2 TKG 2003 definiert bislang den „Benutzer" und umfaßt nunmehr nicht nur natürliche Personen sondern auch juristische Personen. Damit folgt der österreichische Gesetzgeber den Vorgaben der Vorratsdatenrichtlinie, wonach auch die Legaldefinition des Gesetzesbegriffs „Benutzer" in Art 2 Abs 2 lit b „jede juristische Person" mitumfaßt.

6.2. Telefondienst

Die neue Bestimmung des § 92 Abs 3 Z 2a TKG 2003 beinhaltet nun auch eine Definition des Begriffes „Telefondienstes". Es handelt sich dabei um Sprachtelefonie einschließlich Dienste mit Zusatznutzen gemäß der bisherigen Bestimmung § 92 Abs 3 Z 9 und Z 10. Der österreichische Gesetzgeber hält sich auch in diesen Punkten an die Vorratsdatenrichtlinie. Unter die neue Ziffer 2a fallen gemäß den Erläuterungen zur Novelle neben der herkömmlichen Sprachtelefonie auch die in Art 2 Abs 2 lit c der Vorratsdatenrichtlinie aufgezählten Dienste, wie Sprachspeicherdienst, Konferenzschaltungen, Datenabrufungen, Zusatzdienste einschließlich Rufweiterleitung und Rufumleitung sowie Mitteilungsdienste und Multimediadienste. Ferner umfaßt der Begriff „Telefondienst" nun auch die elektronische Post.

6.3. Benutzerkennung

§ 92 Abs 3 Z 2b TKG 2003 bringt eine Definition des Begriffes „Benutzerkennung" und wird als eindeutige Kennung definiert, die Personen zugewiesen wird, wenn diese sich bei einem Internetanbieter oder einem Internet-Kommunikationsdienst registrieren lassen oder ein Abonnement abschließen. Diese neue Bestimmung ist aus der Vorratsdatenrichtlinie, genauer Art 2 Abs 2 lit d, übernommen.

6.4. Standortkennung

§ 92 Abs 3 Z 2c TKG 2003 definiert den Begriff „Standortkennung" als Stammdatum gemäß der bisherigen Bestimmung in § 92 Abs 3 Z 6 TKG 2003 und als Kennung der

[89] *Schwaighofer*, Die neue Strafprozessordnung, 283
[90] Der Entwurf samt Erläuterungen und Stellungnahmen ist abrufbar unter: http://www.parlinkom.gv.at/PG/DE/XXIII/ME/ME_00061/pmh.shtml
[91] *Feiel*, jusIT 2008/46, 97

Funkzelle, von der aus eine Mobilfunkverbindung hergestellt wird, beziehungsweise in der sie beendet wird. Mit dem Hinweis auf § 92 Abs 3 Z 6 TKG 2003 will der österreichische Gesetzgeber zum Ausdruck bringen, dass die Standortkennung eine Teilmenge der auch bisher bereits definierten Stammdaten ist. Im Übrigen folgt er auch hier dem europäischen Richtliniengeber in Art 2 Abs 2 lit e.

6.5. Erfolgloser Anrufversuch

§ 92 Abs 3 Z 2c TKG 2003 bringt die Definition des Begriffs „erfolgloser Anrufversuch", womit ein Telefonanruf gemeint ist, bei dem die Verbindung erfolgreich aufgebaut worden ist, der aber unbeantwortet bleibt oder bei dem das Netzwerkmanagement eingegriffen hat (daher es läutet ohne Antwort oder die angerufene Nummer ist besetzt). Diese Definition ist identisch mit jener in Art 2 Abs 2 lit f der Vorratsdatenrichtlinie.

6.6. Dynamische IP-Adresse als Stammdatum

§ 92 Abs 3 Z 3 lit a TKG 2003 wird an den Umstand angepaßt, dass nunmehr auch juristische Personen unter den Begriff „Benutzer" gemäß § 92 Abs 3 Z 2 TKG 2003 fallen und ergänzt nun den Begriff „Anschrift" um den Sitz beziehungsweise die Rechnungsadresse sowie Namen oder Bezeichnung bei juristischen Personen.

Festzuhalten ist, dass in dem Entwurf der Novelle des TKG 2003 in § 92 Abs 3 Z 3 lit a ein Verweis auf § 92 Abs 3 Z 4a lit a TKG 2003 erfolgt. Es ist anzunehmen, dass hier dem österreichischen Gesetzgeber ein sogenanntes Redaktionsversehen unterlaufen ist. Einerseits ist davon auszugehen, dass § 92 Abs 3 Z 4a TKG 2003 nicht novelliert werden sollte – diese Bestimmung enthielt (bislang) die Definition der Zugangsdaten – und andererseits enthielt diese Bestimmung keine lit a. Es ist daher davon auszugehen, dass ein Verweis auf § 92 Abs 4a lit a beabsichtigt war[92]. Daraus folgt, dass der Begriff „Stammdaten" nunmehr auch Daten umfaßt, die zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigt werden.

Es handelt sich das Telefonfestnetz und den Mobilfunk betreffend um die Rufnummer des Anrufers sowie den Namen und die Anschrift des Teilnehmers. Hinsichtlich des Internetzugangs, Internet E-Mail und der Internet-Telefonie handelt es sich um die zugewiesene Benutzerkennung, die Benutzerkennungen und die Rufnummer, die jeder Nachricht im öffentlichen Telefonnetz zugewiesen werden sowie um den Name, die Anschrift des Teilnehmers, dem eine Internetprotokoll-Adresse, Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war.

Darüber hinaus wird der Begriff „Stammdaten" insofern erweitert, als der österreichische Gesetzgeber nunmehr auch dynamische IP-Adressen den Stammdaten hinzurechnet[93]. In den Erläuterungen wird dazu ausgeführt, dass nunmehr auch dynamische IP Adressen zu den Stammdaten zählen. Der österreichische Gesetzgeber wollte damit die „klarstellende" Rechtsprechung (Urteil des OGH vom 26. Juli 2005 zu 11 Os

[92] So auch die Stellungnahme des europäischen Zentrum für e-commerce und internetrecht im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007

57/05z, 11 Os 58/05x und 11 Os 59/05v) auch im Gesetz umgesetzt wissen. Dies wird – wie weiter unten noch ausgeführt wird - vielfach in Frage gestellt.

6.7. Exkurs IP-Adressen

Alle Computer, die ständig oder zeitweise mit dem Internet verbunden sind, erhalten eine weltweit nur einmal vergebene IP-Nummer. Eine solche besteht – je nachdem, welcher Adressklasse die IP-Nummer unterliegt – aus vier maximal dreistelligen Ziffern von 0 bis 255. Die IP-Adresse kann auf Dauer zugewiesen sein („fixe IP-Adresse") oder nur vorübergehend für eine Internet-Session („dynamische IP-Adresse")[94].

IP-Adressen haben durchaus Ähnlichkeit mit Telefonnummern. Beide dienen nämlich dazu, Daten, die über Telekommunikationsnetze transportiert werden, bestimmten Anschlüssen zuzuordnen, beziehungsweise zuzuleiten[95].

Üblicherweise erhält ein Internetnutzer, der über einen Access-Provider einen Internetanschluss mietet, keine fixe IP-Adresse zugewiesen, sondern eine sogenannte dynamische IP-Adresse. Er erhält sohin aus dem dem Provider zur Verfügung stehenden Nummernvorrat eine IP-Adresse zugewiesen, die gerade frei ist (dynamisch vergebene IP-Adresse). Mit dieser IP-Nummer ist der Internetnutzer weltweit identifizierbar, weil das Internetprotokoll, auf dem der gesamte Datenverkehr im Internet basiert, dafür sorgt, dass diese Nummer bei jedem Schritt im Internet mitgeführt wird. Sie wird aber nicht nur bei jedem Aufsuchen einer Website vorgewiesen, sondern auch von jedem Webserver im Logfile bei jedem Betreten einer Website als auch bei jeder weiteren Bewegung innerhalb dieser Website gespeichert. Das exzessive Aufzeichnen der Daten ist daher Teil der Internettechnologie. Diese Speicherung kann dann zu einem rechtlichen Problem werden, wenn anonyme IP-Adressen mit realen Personendaten verknüpft werden; erst damit werden Maschinendaten zu personenbezogenen Daten. Eine Zuordnung einer IP-Adresse an eine juristische oder natürliche Person ist durch Einblick in das „WHOIS" Register möglich. In diesem Register sind weltweit alle Domain Inhaber und Inhaber von IP-Adressen eingetragen. Allerdings sind bei dynamischen IP-Adressen jene Access Provider eingetragen, denen die entsprechenden IP-Adressen zugeordnet sind. Die eigentlichen Nutzer sind unbekannte Kunden jener Unternehmen, denen von diesen Unternehmen die IP-Adressen zugewiesen worden sind. Eine Feststellung des jeweiligen Nutzers ist nur über die Zuordnungsdaten der Provider möglich. Bei diesen Zuordnungsdaten handelt es sich um personenbezogene Daten, die nach einer Empfehlung der Datenschutzkommission nur dann gespeichert werden dürfen, insoweit dies für Verrechnungszwecke unbedingt erforderlich ist (siehe unten unter 6.8.). Festzuhalten ist, dass die Speicherung von Telefonie Daten (Stammdaten, Verkehrsdaten und Standortdaten) und der Zugriff auf diese Daten schon bisher im TKG 2003, beziehungsweise in der StPO, geregelt gewesen sind. Die

---

[93] 61/ME XXIII. GP

[94] http://www.internet4jurists.at/news/aktuell95.htm

[95] *Kunnert*, Der sicherheitspolizeiliche Griff nach Telekommunikationsdaten, in *Jahnel*, Jahrbuch Datenschutzrecht und E-Government 08, 83 (103)

Internetdaten, die Daten aus der Nutzung des World Wide Web, sind bislang hingegen nur unzureichend vom TKG 2003 erfaßt worden[96].

6.8. Kritik an der Zuordnung der dynamischen IP-Adresse zu den Stammdaten

Das e-center stellt in Abrede, dass der OGH in dem entsprechenden Urteil feststellt, es würde sich bei IP-Adressen um ein Stammdatum handeln. Das e-center führt dazu aus, dass der OGH im Urteil zu 11 Os 57/05z zu entscheiden hatte, unter welchen Voraussetzungen ein Telekommunikationsdiensteanbieter Name und Anschrift eines Anschlussinhabers anhand einer IP-Adresse zu ermitteln und dem Gericht auf dessen Anordnung zu übermitteln hat. Entscheidend sei allerdings gewesen, dass nicht die IP-Adresse, sondern Name und Anschrift zu übermitteln waren. Im gegenständlichen Sachverhalt war die Privatanklägerin bereits in Kenntnis der Internetadresse, von der aus der Nutzer (im Verfahren der Verdächtige) agiert hatte. Das Auskunftsbegehren zielte daher lediglich daraufhin ab, Namen und Anschrift, sohin Stammdaten, desjenigen Kunden des Access Providers in Erfahrung zu bringen, dem dieses Adresse in einem bestimmten Zeitraum zugeordnet war.

Das e-center kritisiert die Zuordnung der dynamischen IP-Adresse zu den Stammdaten auch aus technischen Gründen. Die dem Nutzer zugewiesene dynamische IP-Adresse wird vom Computersystem des Anschlussinhabers als Quell-Adresse in jedem versendeten IP-Paket angegeben. Eine IP-Adresse kann aber nicht nur für die Zuordnung von versendeten IP-Paketen zu dem Anschluß des Versenders, sondern auch für die Zuordnung von IP-Paketen zu dem Anschluß des Empfängers verwendet werden. Andere Systeme verwenden daher spiegelbildlich die IP-Adresse als Ziel-Adresse für IP-Pakete, die an das Computersystem des Anschlussinhabers zu übermitteln sind. Eine dynamische IP-Adresse ist somit auch für die Zuordnung der verwendeten Netzwerkadressierungen zum Teilnehmer notwendig. Weil daher IP-Adressen im Rahmen des IP-Routings für Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz verarbeitet werden, sind dynamische IP-Adressen Verkehrsdaten iSd § 92 Abs 3 Z 4 TKG 2003 und im Besonderen Zugangsdaten iSd § 92 Abs 3 Z 4a TKG 2003[97].

Nach einer Empfehlung der Datenschutzkommission vom 11. Oktober 2006 sind dynamische IP-Adressen ausschließlich Verkehrsdaten und statische IP-Adressen sowohl Verkehrsdaten als auch Stammdaten. Statische IP-Adressen sind vor allem deswegen als Stammdatum anzusehen, wenn sie angesichts ihrer dauerhaften Vergabe in einem Verzeichnis mit den Identitätsdaten eines Teilnehmers verbunden sind. Verkehrsdaten dürfen beim Betreiber über die Herstellung und Aufrechterhaltung der Verbindung im Netz nur gespeichert werden, soweit dies für Verrechnungszwecke notwendig ist oder soweit die ausdrückliche Einwilligung des Betroffenen vorliegt[98].

---

[96] *Schmidbauer*, Die Problematik der gespeicherten Daten, in *Reiter/Wittmann-Tiwald*, Goodbye Privacy, Grundrechte in der digitalen Welt, Grundrechtstag 2007, 79

[97] Stellungnahme des europäischen Zentrum für e-commerce und internetrecht im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007, mwN

[98] GZ: K213.000/0005-DSK/2006

Die Datenschutzkommission hebt in ihrer Stellungnahme zum Entwurf der Novelle des TKG 2003 besonders hervor, dass eine statische IP-Adresse – ebenso wie eine Telefonnummer – einem namentlich bezeichneten Teilnehmer zugeschrieben wird, weswegen die statische IP-Adresse in Verbindung mit einem Namen tatsächlich kein Verkehrsdatum sei. Eine dynamische IP-Adresse kann nur im Zusammenhang mit einer konkreten Kommunikation zu einem konkreten Zeitpunkt einem bestimmten Nutzer zugeordnet werden, weswegen eine dynamische IP-Adresse notwendigerweise ein Verkehrsdatum ist[99].

Auch Schmidbauer ist der Ansicht, dass eine IP-Adresse nicht mit einer Rufnummer vergleichbar ist und insbesondere die Folgen der Offenlegung des Inhabers einer dynamischen IP-Adresse andere sind als bei der Bekanntgabe des Inhabers eines Telefonanschlusses. Er führt aus, dass die Offenlegung der Zuordnung einer IP-Adresse zu einem Nutzer diesen zum gläsernen Bürger macht, der auf Blick und Klick überwacht und ausgewertet wird. Die Offenlegung der Zuordnungsdaten (IP-Adresse zu einem Nutzer) kann dazu führen, dass ein Pseudonym eines Nutzers oder eine anonyme E-Mail Adresse enttarnt wird und dadurch das Vorleben des Nutzers zum Vorschein kommt. Leserbriefe, Webblogs oder Beiträge in Diskussions- und/oder Chatforen eines Nutzers können dadurch nachvollzogen werden. Eine Verknüpfung eines Nutzers zu einer IP-Adresse ermöglicht es, in Erfahrung zu bringen, was der Nutzer im Internet gemacht hat, weswegen die Bekanntgabe der Verknüpfung einer dynamischen IP-Adresse zu einem Nutzer mit der Bekanntgabe des Inhabers einer Telefonnummer nicht gleichgesetzt werden kann.

Schmidbauer fordert, dass bei einem Auskunftsersuchen genau geprüft wird, welcher Dienst betroffen ist und wie im konkreten Fall das Bedürfnis des Inhabers in Bezug auf Schutz von Privatsphäre und Kommunikationsgeheimnis zu bewerten ist. Dementsprechend soll bei der Auskunft ein deutlicher Unterschied gemacht werden, ob der Inhaber einer IP-Adresse im Netz veröffentlicht, kommuniziert oder nur passiv konsumiert hat. Jedenfalls soll nach Schmidbauer eine Auskunft nur nach sorgfältiger Prüfung durch ein Gericht erfolgen. Im Übrigen ist festzuhalten, dass auch auf europäischer Ebene Stimmen laut werden, wonach die Bekanntgabe der Zuordnung einer IP-Adresse keine bloße Bekanntgabe eines Stammdatums ist. Die Generalanwältin geht in ihrem Schlussantrag im Vorabentscheidungsverfahren „Productores de Música de Espana" (C-275/06) davon aus, dass es sich bei der Zuordnung einer IP-Adresse zum Inhaber um ein Verkehrsdatum handelt[100].

6.9. Vorratsdaten

Bei § 92 Abs 4a TKG 2003 in der Fassung des Entwurfs scheint abermals ein Redaktionsversehen passiert zu sein, weil § 92 TKG 2003 bislang keinen vierten Absatz umfaßte. Darüber hinaus sind in § 92 Abs 3 Z 1 bis Z 10 TKG 2003 Legaldefinitionen ange-

[99] Stellungnahme der Datenschutzkommission im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 23. Mai 2007

[100] *Schmidbauer*, Die Problematik der gespeicherten Daten, in *Reiter/Wittmann-Tiwald*, Goodbye Privacy, Grundrechte in der digitalen Welt, Grundrechtstag 2007, 79 (80)

führt, weswegen davon auszugehen ist, dass die Legaldefinition in § 92 Abs 3 Z 4b TKG 2003 erfolgen sollte[101].

In dieser Bestimmung werden nun jene Daten aufgelistet, die auf Vorrat zu speichern sind. Der österreichische Gesetzgeber folgt in dieser Bestimmung beinahe Wort für Wort der Vorratsdatenrichtlinie in Art 5. Infolge des Umstandes, dass Österreich gemäß Art 15 Abs 3 der Vorratsdatenrichtlinie die Umsetzung der Richtlinie im Hinblick auf die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail aufgeschoben hat, sind diese Kommunikationsdaten von dieser neuen Bestimmung noch nicht umfaßt.

Gemäß Erwägungsgrund 13 der Vorratsdatenrichtlinie sollte die Vorratsspeicherung von Daten so erfolgen, dass Daten nicht mehr als einmal auf Vorrat gespeichert werden. Weil aber ein Kommunikationsvorgang sowohl beim Quellnetz als auch beim Zielnetzbetreiber zu einer Datenverarbeitung führt, ist eine doppelte Datenverarbeitung nicht zu vermeiden. Dies hängt mit der für die Kommunikation notwendigen Interoperabilität verschiedener Netze zusammen. Weder die Richtlinie noch der Entwurf der Novelle des TKG 2003 sehen hier Lösungsansätze vor, was vielfach kritisiert wird[102].

Die Speicherfrist soll gemäß § 102a Abs 1 TKG 2003 in der Fassung des Entwurfs der Novelle sechs Monate ab dem Zeitpunkt der Beendigung des Kommunikationsvorgangs betragen. Der österreichische Gesetzgeber hat sich daher dafür entschieden, die Speicherfrist am unteren Limit jenes Rahmen anzusetzen, der in der Vorratsdatenrichtlinie vorgesehen ist. Statistiken zur Rufdatenrückerfassung zeigen, dass rund 51 % der Überwachungen nicht über den Zeitraum von einem Monat ab Einlangen des Beschlusses hinausgehen. In „nur" rund 10 % der einlangenden Gerichtsbeschlüsse werden Rufdaten angefordert, die länger als sechs Monate zurückliegen, aber den Zeitraum von 12 Monaten nicht übersteigen. Zu bedenken ist, dass, wenn Daten länger und in noch größerem Umfang gespeichert werden, damit auch eine größere Mißbrauchsgefahr verbunden ist. Große Datenspeicher sind als Angriffsziele von außen gefährdet und mißbrauchs- und fehleranfälliger je größer sie sind. Eine höhere Fehleranfälligkeit birgt die Gefahr in sich, dass im Rahmen von Abfragen Ergebnisse produziert werden, die sich im Einzelfall unbeabsichtigt nachteilig auswirken können. Daraus folgt, dass durch die Erhöhung der zu speichernden Datenmengen gleichzeitig auch die Analyseaufwendungen steigen, weil nur durch immer konkretere Fragestellungen ein sinnvolles Ergebnis erzielt werden kann und die jeweilige Analyse einer immer strengeren Qualitätssicherung zu unterziehen ist[103]. Auch aus diesem Blickwinkel ist daher die Entscheidung des österreichischen Gesetzgebers, die Speicherfrist am unteren Ende anzusetzen, zu begrüßen.

---

[101] So auch die Stellungnahme des europäischen Zentrum für e-commerce und internetrecht im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007

[102] *Otto/Seitlinger*, MR 2006, 227; sowie Stellungnahme der Telekom Austria AG im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 21. Mai 2007

[103] *Steinmaurer*, Die Speicherung der Daten auf Vorrat oder Ist es leichter, die sprichwörtliche Nadel zu finden, wenn wir den Haufen Heu größer machen?, in *Reiter/Wittmann-Tiwald*, Goodbye Privacy, Grundrechte in der digitalen Welt, Grundrechtstag 2007, 73 (77)

Die Daten sind nach Ablauf der Speicherfrist, unbeschadet des § 99 Abs 2 TKG 2003, unverzüglich zu löschen[104].

6.10. Mit beträchtlicher Strafe bedrohten Handlungen

Die Vorratsdatenrichtlinie hat es letztlich den Mitgliedstaaten überlassen, festzulegen, welche Tatbestände als „schwere Straftaten" iSd Art 1 Abs 1 der Vorratsdatenrichtlinie anzusehen sind. Eine derartige Formulierung öffnet natürlich Tür und Tor für eine weite und unterschiedliche Interpretation des Begriffs „schwere Straftaten" in den Mitgliedstaaten. Auch der Europäische Datenschutzbeauftragte ist der Ansicht, dass die Begrenzung auf „schwere Straftaten" nicht präzise genug ist, wenn im Zusammenhang mit anderen schweren Straftaten als Terrorismus und organisierte Kriminalität um Zugang ersucht wird. Er empfahl dementsprechend, bereits in der Vorratsdatenrichtlinie eine Einschränkung auf bestimmte schwere Straftaten vorzunehmen[105].

In einigen früheren Entwürfen der Vorratsdatenrichtlinie war hingegen noch vorgesehen, auf jene, in Art 2 Abs 2 des Rahmenbeschlusses über den Europäischen Haftbefehl (2002/584/JI) angeführten, Straftaten zurückzugreifen[106]. Bei den in Art 2 Abs 2 angeführten Straftaten handelt es sich um jene Straftaten, die mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind und bei deren Vorliegen eine Übergabe aufgrund eines Europäischen Haftbefehls nach Maßgabe des Rahmenbeschlusses und ohne Überprüfung des Vorliegens der beiderseitigen Strafbarkeit erfolgt. Art 2 Abs 2 umfaßt insbesondere die Tatbestände der Beteiligung an einer kriminellen Vereinigung, des Terrorismus, des Menschenhandels und die sexuelle Ausbeutung von Kindern und Kinderpornografie[107].

§ 102a TKG 2003 in der Fassung der Novelle normiert nun die Pflicht der Anbieter und Betreiber öffentlicher Kommunikationsnetze, die zuvor unter § 92 Abs 4a TKG 2003 (beziehungsweise wohl tatsächlich § 92 Abs 3 Z 4b TKG 2003) angeführten Vorratsdaten für einen Zeitraum von sechs Monaten ab dem Zeitpunkt der Beendigung des Kommunikationsvorganges zum Zweck der Ermittlung, Feststellung und Verfolgung von mit beträchtlicher Strafe bedrohten Handlung gemäß § 17 SPG sowie der Tatbestände der §§ 107 StGB (Gefährliche Drohung) und 107a StGB (Beharrliche Verfolgung) zu speichern. Die Vorratsdaten sind nach Ablauf dieser Frist unverzüglich zu löschen. Der österreichische Gesetzgeber hat daher die Speicherfrist mit der in der Richtlinie vorgesehenen Mindestdauer festgelegt. Er hat allerdings bei der Definition des Begriffs „schwere Straftaten" auf § 17 SPG zurückgegriffen, wonach mit beträcht-

---

[104] *Feiel*, jusIT 2008/46, 97

[105] Stellungnahme des Europäischen Datenschutzbeauftragten zur Vorratsdatenrichtlinie, RZ 54, C 298 vom 29. November 2005

[106] *Otto/Seitlinger*, MR 2006, 227, mwN; so auch *Reindl-Krauskopf*, Data Retention: Sicherheit versus Freiheit, in *Reiter/Wittmann-Tiwald*, Goodbye Privacy, Grundrechte in der digitalen Welt, Grundrechtstag 2007, 65 (66)

[107] Der Rahmenbeschluss und eine vollständige Aufzählung ist abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:190:0001:0018:DE:PDF

licher Strafe bedrohte gerichtlich strafbare Handlungen jene Tatbestände sind, die mit mehr als einjähriger Freiheitsstrafe bedroht sind.

Der österreichische Gesetzgeber hat sich daher entschlossen, auch Tatbestände, die nach dem StGB als Vergehen eingestuft werden, in den Anwendungsbereich der Vorratsdatenspeicherung einzubeziehen. Gemäß § 17 Abs 1 StGB sind Verbrechen jene vorsätzlichen Handlungen, die mit lebenslänglicher oder mit mehr als dreijähriger Freiheitsstrafe bedroht sind. Alle anderen strafbaren Handlungen sind gemäß § 17 Abs 2 StGB Vergehen. Die Unterscheidung strafbarer Handlungen in die wesentlich größere Gruppe der Vergehen und in eine kleinere Gruppe von Verbrechen dient der Wertung der Taten und soll das besondere Gewicht der als Verbrechen eingestuften Straftaten herausheben und damit Schuldspruch und Strafausspruch einen besonderen Akzent geben[108].

Festzuhalten ist, dass unter die vorgesehene neue Bestimmung in § 102a TKG 2003 daher auch Fahrlässigkeitsdelikte fallen[109].

Dieser Umstand wird auch vom e-center kritisiert, wonach das öffentliche Interesse an der Ermittlung, Feststellung und Verfolgung von Fahrlässigkeitsdelikten im Vergleich zur Schwere des Grundrechtseingriff äußerst gering sei, weswegen eine Verhältnismäßigkeit – und daher Verfassungskonformität – zu verneinen sei[110].

Mit wenigen Ausnahmen, insbesondere des Verbandes der Österreichischen Musikwirtschaft (siehe oben), wurde die Strafgrenze von einem Jahr von verschiedenen Seiten als zu niedrig kritisiert. Auch die Datenschutzkommission bemängelt in ihrer Stellungnahme zum Entwurf der Novelle des TKG 2003 von 23. Mai 2007[111] im Lichte der Schwere des durch die Vorratsdatenspeicherung vorgenommenen Grundrechtseingriffs die Heranziehung des § 17 SPG als unverhältnismäßig und verweist auf § 17 StGB. Der Datenschutzkommission zufolge würde der Rückgriff auf § 17 SPG dazu führen, dass etwa zwei Drittel der Straftatbestände des StGB der Vorratsdatenspeicherung unterliegen, weswegen die Verwendbarkeit von gespeicherten Vorratsdaten zur Strafverfolgung nicht mehr die Ausnahme, sondern die Regel wäre. Dies würde substantiell die Abschaffung des Telekommunikationsgeheimnisses bedeuten.

Darüber hinaus führt die Datenschutzkommission ins Treffen, dass der Hinweis auf § 17 SPG als Grenze insoweit bedeutungslos sei, als im Zeitpunkt der Speicherung keine Begrenzung der zu speichernden Daten vorgenommen werden kann, weil nicht bekannt ist, ob die Kommunikation einer strafbaren Handlung dient, beziehungsweise gedient hat. Die Datenschutzkommission fordert dementsprechend eine Verwendungsbeschränkung für die Weitergabe der Vorratsdaten, weil eine Zweckbindung

[108] *Fabrizy*, StGB und ausgewählte Nebengesetze, 8. Auflage, § 17, RZ 2
[109] zB § 81 Abs 1 Z 3 StGB oder § 177 Abs 2 StGB
[110] Stellungnahme des europäischen Zentrum für e-commerce und internetrecht im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007
[111] Stellungnahme der Datenschutzkommission im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 23. Mai 2007

bei der Speicheranordnung infolge des Umstandes, dass eine Speicherverpflichtung nur alle Vorratsdaten unterschiedslos betreffen könne, wirkungslos sei.

Inhaltlich gleich argumentiert Reindl-Krauskopf, wonach im Zeitpunkt der Kommunikation selbst noch nicht feststeht, ob überhaupt ein Krimineller kommuniziert hat. Weil im Zeitpunkt der Kommunikation kein Tatverdacht besteht, kann in diesem Zeitpunkt auch nicht verläßlich entschieden werden, welche der anfallenden Daten später überhaupt für strafrechtliche Ermittlungen gebraucht werden. Sie fordert daher, dass Vorratsdaten nach richterlicher Entscheidung nur an Strafverfolgungsbehörden übermittelt werden, wenn die Ermittlungen wegen einer schweren Straftat geführt werden[112].

Reindl-Krauskopf wendet weiters ein, dass auch Art 8 EMRK (siehe dazu weiter unten) eine Verhältnismäßigkeit des Eingriffs gebietet. Nach ihrem Dafürhalten ist ursprünglicher und weiterhin dominierender Gedanke der Vorratsdatenrichtlinie die Bekämpfung des Terrorismus und der schweren Kriminalität. Vor diesem Hintergrund ist die nationale Umschreibung der schweren Straftat als jede Vorsatz- oder Fahrlässigkeitstat mit einer Strafdrohung von mehr als einem Jahr Freiheitsstrafe iSd § 17 SPG ergänzt um die gefährliche Drohung und beharrliche Verfolgung nicht haltbar. Das Kriminalstrafrecht berücksichtigt aus ihrer Sicht auch bei der Einteilung in Vergehen und Verbrechen gemäß § 17 StGB Gefahrenabwehraspekte. Darüber hinaus hat grundsätzlich jede Strafverfolgung auch die Funktion der Gefahrenabwehr und Prävention. Im Besonderen bezwecken Vorbereitungs- und Organisationsdelikte, gerade auch im Bereich des Terrorismus, die Erfassung und Abwehr von Gefahren im Vorfeld. Reindl-Krauskopf führt insbesondere die Delikte der kriminellen Organisation (§ 278a StGB) und der terroristischen Vereinigung (§ 278b StGB) sowie der Terrorismusfinanzierung (§ 278d StGB) ins Treffen, die allesamt den Verbrechensbegriff des § 17 StGB erfüllen. Sie hält es daher für konsequent und sachgerecht, die Definition des Verbrechens als Umschreibung der schweren Straftat zu verwenden[113].

Auch das e-center spricht sich dafür aus, die Zulässigkeit der Übermittlung der auf Vorrat gespeicherten Daten ohne Zustimmung des Anschlussinhabers von der Notwendigkeit, ein Verbrechen iSd § 17 StGB aufzuklären, abhängig zu machen. Mit Zustimmung des Anschlussinhabers sollte eine Datenübermittlung nur zur Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung zulässig sein[114]. Aus meiner Sicht ist dieser letzte Vorschlag allerdings im Hinblick auf das Verbot eines Zwangs zur Selbstbezichtigung abzulehnen. Das Verbot eines Zwangs zur Selbstbezichtigung gilt nach der Judikatur des VfGH für alle Strafverfahren, daher auch für Verwaltungsstrafverfahren, und zwar schon vor der förmlichen Verfahrenseinleitung. Es verbietet jeden rechtlichen Zwang zur selbst-

[112] *Reindl-Krauskopf*, Data Retention: Sicherheit versus Freiheit, in *Reiter/Wittmann-Tiwald*, Goodbye Privacy, Grundrechte in der digitalen Welt, Grundrechtstag 2007, 65 (71)
[113] *Reindl-Krauskopf*, Data Retention: Sicherheit versus Freiheit, in *Reiter/Wittmann-Tiwald*, Goodbye Privacy, Grundrechte in der digitalen Welt, Grundrechtstag 2007, 65 (70)
[114] Stellungnahme des europäischen Zentrum für e-commerce und internetrecht im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007

belastenden Aussage oder zur Lieferung sonstiger Beweismittel, die gegen den Betreffenden verwendet werden können[115].

Andererseits führt das e-center ins Treffen, dass der in § 102a Abs 1 TKG 2003 genannte Zweck auch zu eng gefaßt sei, weil er eine Handlung erfordert, die mit mehr als einjähriger Freiheitsstrafe bedroht ist. Dies stünde im Widerspruch zu § 149a Abs 2 Z 1 StPO (nunmehr § 135 Abs 2 Z2 StPO), wonach bei Zustimmung des Inhabers des Teilnehmeranschlusses bereits eine mit mehr als sechsmonatiger Freiheitsstrafe bedrohte Vorsatztat ausreicht. In diesem Zusammenhang ist allerdings zu ergänzen, dass hierfür eben die ausdrückliche Zustimmung des Inhabers der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, erforderlich ist.

Meines Erachtens liegt in der Bezugnahme des österreichischen Gesetzgebers auf § 17 SPG für die Definition von „schweren Straftaten" ein deutlicher Wertungswiderspruch zwischen dem Entwurf der Novelle des TKG 2003 und dem StGB vor. Es ist aus meiner Sicht nicht nachzuvollziehen, weswegen der österreichische Gesetzgeber auch Vergehen und Fahrlässigkeitshandlungen, also strafbare Handlungen, deren Handlungsunwert bislang als „geringfügiger" angesehen worden sind, in die Vorratsdatenspeicherungspflicht mit einbezieht. Es dürfen daher Zweifel angemeldet werden, ob der österreichische Gesetzgeber dadurch der Intention des europäischen Richtliniengebers, wonach die Daten zum Zweck der Ermittlung, Feststellung und Verfolgung von schweren Straftaten zu speichern sind, gerecht wird. Aus meiner Sicht ist der österreichische Gesetzgeber in diesem Punkt strenger als es aufgrund der Vorratsdatenrichtlinie notwendig gewesen wäre.

6.11. Auskunftspflichten der Betreiber nach der neuen Rechtslage

6.11.1. Auskunftspflicht gegenüber der Datenschutzkommission

In § 102a Abs 4 TKG normiert der Gesetzgeber, dass die Betreiber alle Anfragen und jede Übermittlung zu speichern haben und auf Ersuchen der Datenschutzkommission, die gemäß § 114a TKG 2003 in der Fassung der Novelle die Vollziehung von § 102a TKG 2003 kontrolliert, diese Protokolldateien unverzüglich der Datenschutzkommission zu übermitteln hat. Durch die Protokollierung des Datenzugriffs soll sichergestellt werden, dass Fälle eines vermuteten Datenmißbrauchs überprüft werden können. Die Speicherung kann sich ausschließlich auf Datenkategorien erstrecken, wohingegen der Dateninhalt selbst nicht von der Protokollierung erfaßt ist, weil dies – nach Ablauf von sechs Monaten nach Datenerfassung – im Widerspruch zu der normierten Löschungsverpflichtung stünde[116].

6.11.2. Auskunftspflicht gegenüber dem Bundesminister für Justiz

Weiters sieht der Entwurf der Novelle des TKG 2003 in § 102 b Auskunftspflichten gegenüber dem Bundesminister für Justiz vor. Anbieter und Betreiber öffentlicher Kom-

[115] *Berka*, Lehrbuch Grundrechte, RZ 475 f, mwN
[116] 61/ME XXIII. GP

munikationsnetze haben diesem auf schriftliches Verlangen Auskünfte zu erteilen, die für den Vollzug von § 102a TKG 2003 und der jährlichen Berichterstattung gegenüber der Europäischen Kommission notwendig sind.

Die Kommission hat gemäß Art 14 der Vorratsdatenrichtlinie dem Europäischen Parlament und dem Rat spätestens am 15. September 2010 eine Bewertung der Anwendung der Richtlinie sowie ihrer Auswirkungen auf die Wirtschaftsbeteiligten und die Verbraucher vorzulegen. Gemäß § 102 b TKG 2003 soll diese Verpflichtung der Betreiber „insbesondere" (diese Aufzählung ist daher nicht erschöpfend) Auskünfte darüber umfassen, in welchen Fällen im Einklang mit den Bestimmungen der StPO Daten an zuständige Behörden weitergegeben worden sind, wie viel Zeit zwischen dem Zeitpunkt der Vorratsspeicherung und dem Zeitpunkt der Anforderung der zuständigen Behörde vergangen ist und in welchen Fällen die Anfragen nach Daten ergebnislos geblieben ist.

Diese beiden Berichtspflichten gegenüber der Datenschutzkommission, beziehungsweise gegenüber dem Bundesminister für Justiz, wird von der Telekom Austria AG als überschießend betrachtet, weil zum einen eine derartige Verpflichtung der Betreiber in der Vorratsdatenrichtlinie nicht vorgesehen sei und zum anderen das Bundesministerium für Justiz über diese Daten bereits aufgrund der richterlichen Beschlüsse verfügen müßte. Darüber hinaus würden diese doppelten Berichterstattungspflichten den Betreibern weitere Kosten verursachen, ohne dass hierfür eine Notwendigkeit vorläge[117].

6.11.3. Weitere Auskunftspflichten?

Aus § 102b TKG 2003 geht hervor, dass eine Auskunft über die Vorratsdaten nur aufgrund der gesetzlichen Vorgaben der StPO zulässig ist. Der Entwurf der Novelle zum TKG 2003 trifft allerdings keine Aussage darüber, ob auch eine Verarbeitung, beziehungsweise eine Auskunftspflicht auch aufgrund anderer Materiengesetze zulässig ist. Zu denken ist dabei insbesondere an die bereits oben erwähnten Bestimmungen nach dem Sicherheitspolizeigesetz oder nach dem Militärbefugnisgesetz. Das e-center führt hierzu ins Treffen, dass auch § 53 Abs 3a Satz 1 SPG und auch § 22 Abs 2a MBG Auskunftspflichten von Betreibern öffentlicher Telekommunikationsdienstleistungen über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses vorsehen. Die Bestimmung eines Anschlusses wäre dementsprechend auch durch die Angabe eines konkreten Zeitpunktes in der Vergangenheit möglich, in dem dem Anschluß eine bestimmte IP-Adresse zugewiesen war, weswegen es in einem derartigen Fall zu einer Verarbeitung der nach § 102a Abs 1 TKG 2003 (in der Fassung der Novelle) gespeicherten Daten käme.

Das e-center befürchtet, dass eine Verarbeitung von nach § 102a Abs 1 TKG 2003 gespeicherten Daten zu dem Zweck der Ermittlung eines durch die Angaben der Behörden „bestimmten" Anschlusses ein außerordentlich großes Eingriffspotential aufweisen würde. Bereits eine geringfügige Ausweitung der derzeit nach dem Si-

[117] Stellungnahme der Telekom Austria AG im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 21. Mai 2007

cherheitspolizeigesetz, beziehungsweise dem Militärbefugnisgesetz, bestehenden Befugnisse würde ein technisches Verfahren ermöglichen, das einem Data Mining nahe käme. § 53 Abs 3a Satz 2 SPG würde bereits für den Bereich der Telefonie vorsehen, dass für die Erfüllung bestimmter Aufgaben die Bestimmung des Anschlusses auch durch die Bezeichnung des Zeitpunktes des Gesprächs und der passiven Teilnehmer erfolgen kann. Wäre die Bestimmung des Anschlusses auch durch die Angabe bestimmter Aufenthaltsorte (daher Cell-IDs) oder Kommunikationsparameter möglich, so würde eine derartige Datenverarbeitung eine Eingriffsintensität entwickeln, die einem automationsunterstützen Datenabgleich (Rasterfahndung) nahe käme.

Der technische Unterschied zwischen einem Data Mining in der beschriebenen Art und einer Rasterfahndung würde nur darin bestehen, dass im Rahmen einer Rasterfahndung mehrere (grundsätzlich kleinere) Datenbestände vereint werden, wohingegen bei einem Data Mining bereits ein zentraler Datenbestand von außerordentlicher Größe bestünde.

Erschwerend käme noch hinzu, dass der Rechtsschutz des Sicherheitspolizeigesetzes als auch des Militärbefugnisgesetzes unzureichend sei. Eine Zustimmung des Rechtsschutzbeauftragten für das Einschreiten der Sicherheitsbehörden sei gemäß § 91a SPG nur dann notwendig, wenn es sich um eine Aufgabe gemäß § 21 Abs 3 SPG (daher in den Fällen der Gefahrenabwehr) handelt oder eine erweiterte Gefahrenerforschung iSd § 21 Abs 3 SPG beabsichtigt sei. In diesen Fällen könnten besondere Ermittlungsmaßnahmen nach § 54 Abs 3 und Abs 4 SPG gesetzt werden oder gemäß § 53 Abs 5 SPG ermittelte Daten weiter verarbeitet werden. Aus einem Umkehrschluß ergäbe sich daher, dass eine Zustimmung des Rechtsschutzbeauftragten zur Ausübung der Befugnisse nach § 53 Abs 3a SPG nicht erforderlich sei. Darüber hinaus gäbe es keine Pflicht, den Rechtsschutzbeauftragten über die Ausübung der Befugnisse gemäß § 53 Abs 3a SPG zu informieren[118].

Das Militärbefugnisgesetz sieht in § 57 Abs 1 MBG die Einrichtung eines Rechtsschutzbeauftragten vor, dessen Aufgabe insbesondere die Prüfung der Rechtmäßigkeit von Maßnahmen der nachrichtendienstlichen Abwehr ist. In § 57 Abs 3 MBG sind umfangreiche Auskunftspflichten der militärischen Organe und Dienststellen gegenüber dem Rechtsschutzbeauftragten vorgesehen. Diese Auskunftspflichten gelten allerdings weder für Auskünfte und Unterlagen über die Identität von Personen oder über Quellen, deren Bekanntwerden die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde noch für Abschriften und Kopien, wenn das Bekanntwerden der Information die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde[119].

Das e-center spricht sich daher zu Recht dafür aus, dass eine Datenverarbeitung nur unter den Voraussetzungen der StPO rechtlich zulässig sein soll.

---

[118] Stellungnahme des europäischen Zentrum für e-commerce und internetrecht im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007

[119] Stellungnahme des europäischen Zentrum für e-commerce und internetrecht im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007

6.12. Sanktionen

Gemäß § 109 Abs 3 Z 17a TKG 2003 und § 109 Abs 3 Z 17b TKG 2003 ist die Nichteinhaltung der Verpflichtung zur Vorratsdatenspeicherung, beziehungsweise die Nichteinhaltung der Verpflichtung zur Auskunftserteilung jeweils eine Verwaltungsübertretung, die in beiden Fällen mit einer Geldstrafe von bis zu € 37.000,00 bedroht ist. Obwohl die Vorratsdatenrichtlinie in Art 14 Abs 2 die Mitgliedstaaten in die Pflicht nimmt, erforderliche Maßnahmen zu ergreifen, um sicherzustellen, dass der vorsätzliche Zugang zu oder die vorsätzliche Übermittlung von Vorratsdaten, die nach den innerstaatlichen Regelungen unzulässig sind, mit verwaltungsrechtlichen und strafrechtlichen Sanktionen, die wirksam, verhältnismäßig und abschreckend sein sollen, belegt werden, fehlt eine entsprechende Regelung im Entwurf der Novelle zum TKG 2003.

Die bestehende Bestimmung in § 108 TKG 2003, wonach eine in § 93 Abs 2 TKG 2003 bezeichnete Person (das ist der Betreiber oder eine Person, die an der Tätigkeit des Betreibers mitwirkt) mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen ist (insoweit die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist), wenn sie unbefugt über die Tatsache oder den Inhalt des Telekommunikationsverkehrs bestimmter Personen einem Unberufenen Mitteilung macht oder ihm Gelegenheit gibt, Tatsachen, auf die sich die Pflicht zur Geheimhaltung erstreckt, selbst wahrzunehmen, ist aus meiner Sicht nicht stichhältig. Es kann meines Erachtens zumindest fraglich sein, ob etwa die unzulässige und vorsätzliche Weitergabe von Vorratsdaten tatsächlich unter § 108 TKG 2003 subsumiert werden kann. Durch diese Weitergabe würde einem Unbefugten wohl nicht die Gelegenheit geboten worden sein, Tatsachen, auf die sich die Pflicht zur Geheimhaltung erstreckt, selbst wahrzunehmen. Ob dadurch über die Tatsache oder den Inhalt des Telekommunikationsverkehrs Mitteilung gemacht wird, kann aus meiner Sicht zumindest stark in Zweifel gezogen werden.

Darüber hinaus fehlen Strafbestimmungen gegen unerlaubte Zugriffe. § 51 DSG setzt eine Datenverwendung in Gewinn- oder Schädigungsabsicht voraus, weswegen diese Bestimmung nicht ausreichend ist. Der Mißbrauch von Vorratsdaten sollte grundsätzlich strafbar sein und nicht lediglich dann, wenn ein Bereicherungs- oder Schädigungsvorsatz vorliegt, beziehungsweise festgestellt werden kann. Ungeachtet dessen fehlen auch Bestimmungen über eine Verpflichtung des Personals zur besonderen Verschwiegenheit im Umgang mit Daten aus der Vorratsdatenspeicherung[120].

7. Gemeinschaftsrecht und nationale Grundrechte

7.1. Allgemeines

[120] Stellungnahme der Datenschutzkommission im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 23. Mai 2007

Seitdem Österreich der Europäischen Union beigetreten ist, gilt das europäische Gemeinschaftsrecht als weitere Rechtsquelle neben dem innerstaatlichen Recht in Österreich. Weil das Gemeinschaftsrecht eine autonome Rechtsordnung ist, der ein Anwendungsvorrang gegenüber entgegenstehendem innerstaatlichen Recht – mit eingeschlossen dem Verfassungsrecht – zukommt, hatte der Beitritt Österreichs auch weitreichende Auswirkungen für die Grundfreiheiten und Menschenrechte. Der Anwendungsvorrang führt dazu, dass das Gemeinschaftsrecht auch dann anzuwenden ist, wenn seine Regelungen innerstaatlichen Grundrechten widersprechen. Vor allem ist es auch dem österreichischen VfGH verwehrt, irgendeine gemeinschaftsrechtliche Bestimmung nach Maßgabe der verfassungsrechtlichen Grundrechte zu beurteilen, weil über die Gültigkeit des Gemeinschaftsrechts nur der EuGH zu entscheiden befugt ist[121].

Die Richtlinie 2006/24/EG kann daher nicht am Maßstab österreichischer Grundrechte geprüft werden[122].

7.2. Vorratsdatenspeicherung und Gemeinschaftsgrundrechte

Das primäre Gemeinschaftsrecht enthält zwar keinen verbindlichen Grundrechtskatalog, doch zählen Grundrechte bereits nach der Rechtsprechung des EuGH zu den allgemeinen Rechtsgrundsätzen des Gemeinschaftsrechts. Die Grundrechte sind daher integraler Bestandteil der allgemeinen Rechtsgrundsätze, deren Wahrung der Gerichtshof zu sichern hat. Der Gerichtshof läßt sich dabei von den gemeinsamen Verfassungstraditionen der Mitgliedstaaten sowie von den Hinweisen leiten, die die völkerrechtlichen Verträge über den Schutz der Menschenrechte geben, an deren Abschluß die Mitgliedstaaten beteiligt waren oder denen sie beigetreten sind[123]. Der EuGH stützt sich vor allem auf die EMRK als gemeinsamen Nenner der europäischen Verfassungstraditionen[124].

Gemäß Art 6 Abs 1 EUV beruht die Union auf den Grundsätzen der Freiheit, der Demokratie, der Achtung der Menschenrechte und Grundfreiheiten sowie der Rechtsstaatlichkeit. Die Union achtet gemäß Art 6 Abs 2 EUV die Grundrechte, wie sie in der am 4. November 1950 in Rom unterzeichneten Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten als allgemeine Grundsätze des Gemeinschaftsrechtes ergeben.

Als Ausprägungen der allgemeinen Rechtsgrundsätze binden die Grundrechte des Gemeinschaftsrechts zum einen die sekundären Rechtsakte der Gemeinschaft. Verordnungen, Richtlinien oder Entscheidungen der Europäischen Gemeinschaften sind daher rechtswidrig, wenn sie gegen ein Gemeinschaftsgrundrecht verstoßen[125]. Der

---

[121] *Berka*, Lehrbuch Grundrechte, RZ 183 ff
[122] Stellungnahme des europäischen Zentrum für e-commerce und internetrecht im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007
[123] C-540/03
[124] *Öhlinger*, Verfassungsrecht, 5. Auflage, RZ 142, mwN
[125] *Berka*, Lehrbuch Grundrechte, RZ 201 ff, mwN

europäische Richtlinien-Geber ist daher gemäß Art 6 EUV primärrechtlich an die Europäische Menschenrechtskonvention gebunden. Ungeachtet dessen ist Österreich unmittelbar aufgrund eines völkerrechtlichen Vertrages zur Einhaltung der EMRK verpflichtet[126].

Kritisiert wird zuweilen allerdings, dass sich der EuGH bei der Prüfung des sekundären Gemeinschaftsrechts am Maßstab der Grundrechte – diese Befugnis ist durch den Vertrag von Amsterdam (Art 46 lit d EUV) ausdrücklich klargestellt worden – bislang als äußerst zurückhaltend erwiesen hat[127] und bisher praktisch keine einzige generelle gemeinschaftsrechtliche Regelung des Rates wegen eines Verstoßes gegen Gemeinschaftsgrundrechte für ungültig erklärt hat. Dazu kommt, dass sich der EuGH in allen strittigen Grundrechtsfragen bisher eher zu Ungunsten einer großzügigen Interpretation der Freiheitsrechte entschieden hat und den politischen Gestaltungsspielraum des Gemeinschaftsgesetzgebers ziemlich weit bemißt[128].

7.3. Das Recht auf Achtung des Privat- und Familienlebens (Art 8 EMRK)

Bereits die staatlich veranlaßte Datensammlung als solche (daher ungeachtet einer allfälligen Auswertung der gesammelten Daten) berührt nach heute herrschendem Grundrechtsverständnis das Recht auf Schutz der Privatsphäre nach Art 8 EMRK[129].

Das Recht auf Schutz der personenbezogenen Daten ist in Artikel 8 EMRK garantiert. Gemäß Art 8 Abs 1 EMRK hat jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz. Auch wenn der Schutz des Fernmeldegeheimnisses zwar nicht ausdrücklich genannt wird, so ist er doch nach der Rechtsprechung des EGMR vom Grundrecht auf Achtung des Privat- und Familienlebens nach Art 8 EMRK umfaßt[130].

In der Entscheidung zu 62617/00 (Copland gegen das Vereinigte Königreich) hat der Europäische Gerichtshof für Menschenrechte entschieden, dass die Sammlung und Speicherung von persönlichen Informationen hinsichtlich Telefon-, E-Mail- und Internetdaten ohne Wissen des Nutzers jedenfalls gegen Art 8 EMRK verstößt. Aus dieser Entscheidung folgt, dass Eingriffe in das Grundrecht nach Art 8 EMRK nur unter strengen Voraussetzungen zulässig sind[131].

Der Europäische Gerichtshof für Menschenrechte hat darüber hinaus betont, dass bei heimlicher Überwachung die Gefahr besteht, dass die Demokratie mit der Begründung, sie verteidigen zu wollen, unterminiert oder zerstört wird. Er hat ferner bekräftigt, dass die Vertragsstaaten zur Bekämpfung der Spionage oder des Terrorismus

---

[126] Stellungnahme des europäischen Zentrum für e-commerce und internetrecht im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007
[127] *Öhlinger*, Verfassungsrecht, 5. Auflage, RZ 142
[128] *Berka*, Lehrbuch Grundrechte, RZ 207
[129] *Reindl-Krauskopf*, Data Retention: Sicherheit versus Freiheit, in *Reiter/Wittmann-Tiwald*, Goodbye Privacy, Grundrechte in der digitalen Welt, Grundrechtstag 2007, 65 (67 f), mwN
[130] *Otto/Seitlinger*, MR 2006, 227, mwN
[131] *Kosta/Dumortier*, MR-Int 2007, 130, mwN; ebenso die Stellungnahme des europäischen Datenschutzbeauftragten zur Vorratsdatenrichtlinie, RZ 9 ff, C 298 vom 29. November 2005

nicht jede Maßnahme beschließen dürfen, die sie für angemessen halten. Eingriffe in das Grundrecht gemäß Art 8 EMRK müssen daher einem zwingenden Bedürfnis entspringen. Sie dürfen nur in Ausnahmefällen gestattet werden und müssen angemessenen Schutzmaßnahmen unterworfen sein. Die Vorratsspeicherung von Verkehrsdaten und Standortdaten zu Strafverfolgungszwecken muß strengen Auflagen genügen; sie darf insbesondere nur während eines bestimmten Zeitraums erfolgen und nur dann, wenn dies in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist[132].

Auch wenn – wie vorhin erwähnt – die EMRK nicht ratifiziert und damit nicht unmittelbar anwendbares Recht ist, anerkennt der EuGH ausgehend von den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten Maßnahmen als rechtswidrig an, die mit den von den Verfassungen der Mitgliedstaaten anerkannten Grundrechten unvereinbar sind. Die Verfassungen werden – neben den Menschenrechtsverträgen – nicht als Rechtsquellen, sondern als Rechtserkenntnisquellen genutzt.

Das Recht auf Achtung des Privatlebens schützt die einzigartige Persönlichkeit des Menschen in ihrer physischen, seelischen oder geistigen Existenz, wie sie sich in der Begegnung des Menschen mit sich selbst und in zwischenmenschlichen Bezügen äußert[133]. Zum geschützten Privatleben gehören mitunter auch sein privates Tun und Treiben, seine Kontakte mit engen Bezugspersonen und seine persönliche Identität.

In das Privatleben eines Menschen wird auch eingegriffen, wenn Außenstehende sich Informationen aus diesem Bereich verschaffen (sogenannte Informationsseingriffe). Das gilt für die erkennungsdienstliche Behandlung genauso wie für statistische Erfassungen, die jeweils nur bei entsprechendem öffentlichem Interesse und im Rahmen des Verhältnismäßigen zulässig sind. Bei dieser Abwägung kommt es auf die Art der Information an, deren sich der Staat bemächtigt, auf den Umfang der Datenerfassung und die weitere Verwendung der Daten und die Dauer ihrer Aufbewahrung. Verfassungswidrig wäre jedenfalls die vollständige „Durchleuchtung" eines Menschen oder die Anlage lückenloser Datenprofile. Die 1997 eingeführten polizeilichen Überwachungsmaßnahmen („großer Lauschangriff", „Rasterfahndung") stellen jedenfalls intensive Grundrechtseingriffe dar, weil hier Menschen ohne ihr Wissen im geschützten Bereich der Wohnung, daher in einer privaten Kommunikationssituation, belauscht, beziehungsweise eine Vielzahl von Daten auch von unbehelligten Bürgern verknüpft werden können[134].

Gemäß Art 8 Abs 2 EMRK darf eine Behörde in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.

---

[132] Art 29 Datenschutzgruppe, WP 113, mwN, aufrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm

[133] *Berka*, Lehrbuch Grundrechte, RZ 264 ff

[134] *Berka*, Lehrbuch Grundrechte, RZ 270

Weil gerade eine Demokratie darauf angewiesen ist, dass der Einzelne, der ihr angehört, nicht in allen seinen Bezügen einer Kontrolle durch die Öffentlichkeit unterworfen ist, muß sie in besonderer Weise die Privatheit ihrer Bürger respektieren. Denn gemessen an den Wertmaßstäben einer Demokratie ist der Staat nicht dazu legitimiert, die Freiheit des Individuums in Ansehung von Verhaltensweisen einzuschränken, die der Öffentlichkeit gegenüber nicht in Erscheinung treten und weder Gemeinschaftsinteressen noch auch legitime Interessen anderer Individuen irgendwie beeinträchtigen[135].

Ob die zuvor erwähnten Eingriffe, die die Vorratsdatenspeicherung bringen wird, in Art 8 Abs 2 EMRK ihre Deckung finden, hängt von der Bewertung der Gefahren ab, die der öffentlichen Sicherheit und Ordnung vor allem durch die Formen der organisierten Kriminalität drohen. Entscheidend ist auch die nähere Ausgestaltung dieser Eingriffe, weil der Staat – wenn er zu solchen Maßnahmen greift – den Eingriff möglichst gering halten muß und für den gehörigen Schutz vor Mißbräuchen zu sorgen hat. Denn Befugnissen zur geheimen Überwachung von Bürgern, wie sie für einen Polizeistaat typisch sind, können in einer demokratischen Gesellschaft nur bei außergewöhnlichen Situationen und in engen Grenzen zulässig sein[136].

Nach der Grundrechtsdogmatik des EuGH können Gemeinschaftsgrundrechte unter bestimmten Voraussetzungen eingeschränkt werden. Notwendig dafür ist neben einer gesetzlichen Grundlage – hier also die Richtlinie –, dass der Grundsatz der Verhältnismäßigkeit und der Wesensgehalt des Grundrechts beachtet wird.

Das Grundrecht auf Achtung des Privat- und Familienlebens (Art 8 Abs 2 EMRK) steht unter einem materiellen Gesetzesvorbehalt, wonach der Gesetzgeber nur dann zur Schrankensetzung ermächtigt ist, wenn die Beschränkung der Freiheit einem bestimmten öffentlichen oder individuellen Interesse dient und der Eingriff in eine grundrechtliche Freiheit zur Wahrung dieses Interesses zwingend erforderlich ist. Materielle Gesetzesvorbehalte ermächtigen zu Beschränkungen der gewährleisteten Freiheiten, wenn der Eingriff gesetzlich vorgesehen, er einem bestimmten, jeweils ausdrücklich angeführten Schutzgut (der Wahrung der öffentlichen Sicherheit, der Verteidigung der Ordnung, dem Schutz der Gesundheit, dem Schutz der Rechte und Freiheiten anderer, etc…) dient und der Eingriff in einer demokratischen Gesellschaft zur Erreichung dieses Zwecks notwendig ist[137].

7.3.1. Grundsatz der Verhältnismäßigkeit

Dass der Eingriff in das Grundrecht in einer demokratischen Gesellschaft notwendig sein muß, verankert den Grundsatz der Verhältnismäßigkeit als grundrechtliche „Schranken-Schranke". Der mit einem Grundrechtseingriff verfolgte legitime Zweck darf im Sinne einer Ziel-Mittel-Relation nicht außer Verhältnis zu dem damit verbundenen Eingriff in die Freiheitssphäre der betroffenen Grundrechtsträger stehen. In diesem Sinn verlangt der Grundsatz der Verhältnismäßigkeit, dass

[135] *Berka*, Lehrbuch Grundrechte, RZ 266 mwN
[136] *Berka*, Lehrbuch Grundrechte, RZ 270 mwN
[137] *Berka*, Lehrbuch Grundrechte, RZ 155

a. der vom Staat verfolgte Zweck legitim ist,

b. das vom Staat eingesetzte Mittel geeignet ist,

c. der Einsatz des Mittels zur Erreichung des Zwecks notwendig, beziehungsweise erforderlich ist und

d. insgesamt ein angemessenes Verhältnis (Adäquanz) zwischen dem eingesetzten Mittel und der damit verbundenen Grundrechtsbeeinträchtigung gewahrt bleibt (Verhältnismäßigkeit oder Proportionalität im engeren Sinn)[138].

Ad. a. Legitimer Ziel

Die Befugnis des Gesetzgebers nach freier Entscheidung bestimmte Anliegen als Gemeinwohlanliegen aufzugreifen, ist im Geltungsbereich der materiellen Gesetzesvorbehalte der EMRK begrenzt. Nach Art 8 Abs 2 EMRK darf der Gesetzgeber das Grundrecht nur zur Verfolgung bestimmter, namentlich angeführter Schutzgüter beschränken. Findet eine grundrechtsbeschränkende Regelung in einem solchen legitimen Eingriffsziel keine Deckung, ist sie schon aus diesem Grund verfassungs- beziehungsweise gemeinschaftsrechtswidrig.

Grundsätzlich ist es ein legitimes Ziel und ein berechtigtes Interesse des Staates, beziehungsweise des europarechtlichen Gesetzgebers, seine Bürger vor Kriminalität und Terrorattacken bestmöglich zu schützen, weswegen gegen die Vorratsdatenrichtlinie und deren Umsetzung in innerstaatliches Recht nichts einzuwenden ist, geht man davon aus, dass dieses Ziel und dieses Interesse im Vordergrund der Richtlinie steht und weniger die Harmonisierung europarechtlicher Vorschriften auf dem Gebiet der Datenvorratsspeicherung.

Franz Schmidbauer bestreitet allerdings die Zulässigkeit des Grundrechtseingriffs durch die Vorratsdatenspeicherung[139]. Aus seiner Sicht kann die Erleichterung der Aufklärung „gewöhnlicher Verbrechen" nicht den Eingriff in Grundrechtspositionen rechtfertigen. Es könne auch nicht angehen, dass ein zulässiger Grund darin liegt, dass Staatsanwaltschaften und Gerichte so überlastet sind, dass sie Verfolgungshandlungen erst viele Monate später nach einer Anzeige setzen könnten. Bei den oben erwähnten, in Art 8 Abs 2 EMRK genannten Ausnahmen, die einen Eingriff erlauben, ginge es nicht um die Aufklärung von geschehenen Verbrechen, sondern um vorbeugende Gefahrenabwehr. Dies stünde aber im Widerspruch zur beschlossenen Vorratsdatenrichtlinie, die lediglich die vorbeugende Sicherung möglichst vieler Daten zum Ziel hat, die nach einem gegebenen Anlassfall als Beweise in Frage kommen könnten, um eine Erleichterung der Verbrechensaufklärung zu ermöglichen.

[138] *Berka*, Lehrbuch Grundrechte, RZ 161
[139] *Schmidbauer*, „Die Spitzelrichtlinie", abrufbar unter: http://www.internet4jurists.at/news/aktuell95.htm

Dies ist nach Ansicht Schmidbauers nicht zulässig, wobei er ins Treffen führt, dass Ausnahmen vom Grundrechtsschutz einschränkend auszulegen sind. Schmidbauer spricht in weiterer Folge von „Überwachungsexzessen", die vor nicht allzu langer Zeit für einen Rechtsstaat westlichen Zuschnitts völlig undenkbar gewesen seien[140].

Ad. b. Eignung

Die zur Verfolgung des legitimen Zieles eingesetzten Mittel müssen geeignet sein, dieses Ziel auch tatsächlich zu erreichen. Die Freiheit der Bürger darf nicht beschränkt werden, wenn dadurch öffentliche Interessen gar nicht wirklich gefördert werden.

Vielfach wird allerdings genau diese Eignung, beziehungsweise die Erforderlichkeit der Vorratsdatenspeicherung in Frage gestellt[141]. So wird ins Treffen geführt, dass die auf Vorrat gespeicherten Daten den Strafverfolgern nur bei „unvorsichtigen Kleinkriminellen"[142] nützlich sein können. Es ist tatsächlich mit einfachen Mitteln möglich, eine Entdeckung zu verhindern, wobei insbesondere an im Ausland gekaufte Mobiltelefone oder an die Verwendung von Prepaid Mobiltelefonen oder öffentlichen Telefonzellen zu denken ist. Ebenso könnte die E-Mail Korrespondenz über Betreiber von Webservern geführt werden, die außerhalb der EU ihren Sitz haben und daher nicht dem Geltungsbereich der Vorratsdatenrichtlinie unterliegen. Ungeachtet dessen kann die Vorratsdatenrichtlinie durch Anonymisierungssoftware umgangen werden. Zudem ist es möglich, IP-Adressen zu fälschen, beziehungsweise ist es denkbar, entsprechend infizierte private PCs oder Server als Brücke zur Verfälschung der IP-Adresse zu Nutze zu machen[143].

Die Vorratsdatenrichtlinie beschränkt sich zudem in Art 5 darauf, Verkehrs- und Standortdaten in den Bereichen Telefonfestnetz, Mobilfunk, Internetzugang, Internet E-Mail und Internet-Telefonie zu speichern. Die Kommunikation mittels http, wie insbesondere die Kommunikation mit einem Web-Mail Service Provider ist hingegen nicht erfaßt. Ebenso wenig ist insbesondere auch nicht das File Transfer Protocol (FTP), das Protokoll Internet Relay Chat (IRC), alle Instant Messaging Protokoll, File Sharing (Peer2Peer-Protokolle) erfaßt [144].

Weiters scheint das Volumen der zu speichernden Daten eine angemessene Analyse dieser Daten nicht zuzulassen, denn bei Anwendung herkömmlicher Technologie dürfte die Durchsuchung des Datenvolumens von etwa 20.000 bis 40.000 Terabytes bis zu 100 Jahre dauern[145].

---

[140] http://www.internet4jurists.at/news/aktuell95.htm
[141] So z.B. StV 4/2007, S 218 f oder Stellungnahme des europäischen Zentrum für e-commerce und internetrecht im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007, 5 f
[142] *Breyer*, StV 4/2007
[143] *Feiel*, jusIT 2008/46, 97
[144] Stellungnahme des europäischen Zentrum für e-commerce und internetrecht im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007
[145] *Feiel*, jusIT 2008/46, 97, mwN

Ad. c. Notwendigkeit, beziehungsweise Erforderlichkeit der Grundrechtsbeschränkung

Unter diesem Gesichtspunkt ist zu prüfen, ob der Staat, beziehungsweise der europäische Gesetzgeber, die gewährleistete Freiheit nicht in einem größeren Maß einschränkt, als dies zur Erreichung des legitimen Eingriffszieles erforderlich ist. Insofern wird ein Gebot des gelindesten Mittel statuiert, wonach die Freiheit der Bürger nicht über das unbedingt Erforderliche hinausgehend beschränkt werden darf.

Bei der Beurteilung der Notwendigkeit und der Eignung sind schwierige Prognosen und Abschätzungen durchzuführen, weswegen es anerkannt ist, dass dem Gesetzgeber ein erheblicher Beurteilungsspielraum zukommt[146].

Eine fundierte Faktenlage über den Erfolg des Einsatzes der Vorratsdatenspeicherung im Vorfeld der Erlassung der Vorratsdatenrichtlinie, beziehungsweise entsprechende Studien, liegen nicht vor[147].

Ferner ist festzuhalten, dass es durchaus gelindere Mittel als die pauschale Vorratsspeicherung von Daten aller Nutzer gibt. In diesem Zusammenhang ist etwa an das „Fast Freeze – Quick Thaw" Modell zu denken, das die Cyber-Crime-Konvention des Europarates (Art 16 und 17) vorsieht. Nach dem "Fast Freeze - Quick Thaw" Verfahren („schnelles Einfrieren, rasches Auftauen") wird den Strafverfolgungsbehörden die Möglichkeit eingeräumt, auf von Betreibern gespeicherte Verkehrsdaten zuzugreifen. Wesentlich ist allerdings, dass gemäß Art 16 der Konvention, diese Daten lediglich für einen Zeitraum von 90 Tagen gespeichert werden dürfen[148]. Darüber hinaus werden bei diesem Verfahren weder die Kommunikationdienstesanbieter noch die Internet-Diensteanbieter zur generellen Speicherung von Verkehrsdaten verpflichtet. Bei diesem Verfahren wenden sich die Strafverfolgungsbehörden in begründeten Fällen an die Unternehmen und verlangen die Speicherung bestimmter Daten. Daraufhin haben die Behörden mehrere Wochen Zeit zum Sammeln von Beweismitteln, um eine richterliche Anordnung zu erwirken, worauf sie dann Zugriff auf die Daten erhalten[149]. Es ist allerdings auch festgestellt worden, dass dieses Verfahren zwar geringere Auswirkungen auf die Datenschutzgrundsätze hätte als die Vorratsdatenspeicherung, andererseits dafür nicht immer ausreichend ist, wenn es darum geht, Personen aufzuspüren, die in Terrorismus oder andere schwere Straftaten verwickelt sind und zuvor keiner kriminellen Aktivität verdächtigt worden sind[150].

Ad. d. Adäquanz

Im Rahmen der Adäquanz kommt es auf eine Abwägung der angestrebten öffentlichen Interessen mit dem Gewicht der beeinträchtigten Freiheit an. Die Beschrän-

[146] *Berka*, Lehrbuch Grundrechte, RZ 167
[147] *Feiel*, jusIT 2008/46, 97, mwN
[148] *Kosta/Dumortier*, MR-Int 2007, 130; die Cyber-Crime-Konvention ist abrufbar unter: http://www.ccc.de/cybercrime/mirror/FinalCybercrime.htm?language=de
[149] Art 29 Datenschutzgruppe, WP 113
[150] Stellungnahme des europäischen Datenschutzbeauftragten zur Vorratsdatenrichtlinie, RZ 20, C 298 vom 29. November 2005

kung der individuellen Freiheit ist nur zulässig, wenn sie durch überwiegende Interessen der Allgemeinheit oder überwiegender Interessen anderer gerechtfertigt werden kann.

Unter diesem Punkt ist hervorzuheben, dass die Vorratsdatenspeicherung keine Differenzierung zwischen den betroffenen Nutzern trifft. Es werden die Daten sämtlicher Nutzer gespeichert. Die bisher nur ausnahmsweise zulässige Speicherung von Daten wird durch die Vorratsdatenrichtlinie zur Regel. Der Ausgleich zwischen den Interessen an einer effizienten Wahrheitsfindung und Aufklärung von Straftaten und dem Interesse der Nutzer am Schutz seiner Privatsphäre fehlt völlig. Für die Möglichkeit der Verhinderung, Aufklärung oder Verfolgung von Straftaten Einzelner, wird ein Eingriff in die Grundrechte aller (überwiegend unbescholtener) Nutzer von Telekommunikationsdienstleistungen angeordnet[151].

Grundsätzlich ist zudem in Entsprechung der Judikatur des VfGH festzuhalten, dass in einer von der Achtung der Freiheit geprägten Gesellschaft, ein Bürger ohne triftigen Grund niemandem Einblick zu gewähren hat, welchem Zeitvertreib er nachgeht, welche Bücher er kauft, welche Zeitungen er abonniert, was er ißt und trinkt und wo er die Nacht verbringt. Wird nun die Vorratsdatenrichtlinie tatsächlich umgesetzt, so wird es dadurch möglich, nachzuvollziehen, welche Internetseiten ein Nutzer besucht hat. Die Speicherung dieser Daten ist auch dann zulässig, wenn kein triftiger Grund vorliegt, weswegen schon aus diesem Grund ein Verstoß gegen Art 8 EMRK angenommen werden kann.

Vielfach wird (von den Befürwortern der Vorratsdatenrichtlinie) ins Treffen geführt, dass sich die gesellschaftlichen Bedingungen, insbesondere aufgrund der Terroranschläge, geändert hätten. Auch nach der Ansicht des EGMR sind in „außergewöhnlichen Situationen" intensive staatliche Eingriffe in den Telefonverkehr zulässig. Der EGMR führt allerdings nicht aus, was in einer derartigen Situation hinsichtlich der Ausgestaltung des Überwachungssystems die „beste Politik" sei. Der Staat dürfe jedenfalls nicht zu jedweder Maßnahme greifen. Darüber hinaus seien auch wirksame Maßnahmen gegen Mißbrauch einzurichten.

Die Eingriffsintensität im Fall der Vorratsdatenrichtlinie ist beachtlich, weil die Vorratsdaten aller Nutzer ohne konkretes Fehlverhalten gespeichert werden. Die Grundrechtsposition des Einzelnen ist umso intensiver betroffen, je weniger er einen solchen staatlichen Eingriff veranlaßt hat. Bei einer verdachtsunabhängigen Speicherung der Vorratsdaten, müssen die Grenzen der staatlichen Ermächtigung für diesen Grundrechtseingriff besonders eng gezogen und klar formuliert werden, auch wenn der in der Vorratsdatenspeicherung liegende Nachteil für den Einzelnen sich erst dann manifestiert, wenn dessen Daten abgerufen werden. Es wird daher gefordert, dass die ermittelten Daten nur dann verwertet werden, wenn die Verdachtslage gegen eine bestimmte Person besonders dicht oder die ihr vorgeworfene gerichtlich strafbare Handlung besonders schwer ist. Wenn nun aber § 102a TKG 2003 in der Fassung der

[151] *Otto/Seitlinger*, MR 2006, 227, mwN

Novelle auf § 17 SPG verweist, kann die Adäquanz des Grundrechtseingriff zumindest ernsthaft in Zweifel gezogen werden[152].

7.3.2. Geforderte Mindeststandards

Der Europäische Datenschutzbeauftragte anerkennt grundsätzlich, dass die Strafverfolgungsbehörden in den Mitgliedstaaten, insbesondere zur Bekämpfung von Terrorismus und anderen schweren Straftaten, über alle erforderlichen Rechtsinstrumente verfügen müssen. Weiters führt er aus, dass sich die gesellschaftlichen Bedingungen aufgrund von Terroranschlägen durchaus geändert haben. Dennoch darf dies nicht dazu führen, dass die Schutzstandards, die die Grundrechte einräumen, beeinträchtigt werden.

Der Europäische Datenschutzbeauftragte bezweifelt, dass – jedenfalls ohne zusätzliche Maßnahmen – die physische Sicherheit der Bewohner der Europäischen Union durch die Vorratsdatenspeicherung allein erhöht wird. Aufgrund der großen Datenbanken ist zu bezweifeln, dass die Strafverfolgungsbehörden leicht etwas finden, was sie in einem bestimmten Fall suchen.

Aus der Sicht des Europäischen Datenschutzbeauftragten ist die Vorratsdatenspeicherung von Daten nur dann geeignet und wirksam, wenn es auch effiziente Suchmaschinen gibt. Weiters fordert er eine Begrenzung der Speicherfristen, eine Sicherstellung, dass kein Zugang zu Inhaltsdaten möglich ist, eine Einschränkung der Gründe, die einen Zugang zu den Daten ermöglichen, einen effizienten Schutz der Datenbanken vor unzulässigen Zugriffen und eine Sicherstellung, dass die Daten nach Ablauf der Speicherfrist gelöscht werden[153].

Auch die Datenschutzgruppe erkennt an, dass sich die Gesellschaft infolge der mit der terroristischen Bedrohung einhergehenden Gefahr und Risiken verändert hat. Sie nimmt zur Kenntnis, dass manche Daten gelegentlich für bestimmte Ermittlungen nützlich sein können und zu Recht verwendet werden[154]. Sie fordert allerdings bestimmte Mindestanforderungen (safeguards), die eingehalten werden müssen. Im einzelnen fordert die Datenschutzgruppe insbesondere[155], dass

1. die Datenspeicherung nur zu spezifischen Zwecken gespeichert werden. Der Begriff „schwere Straftat" müßte einerseits klar definiert werden und jede weitere Verarbeitung andererseits durch besondere Schutzvorkehrungen ausgeschlossen oder streng begrenzt werden.

2. Zugang zu den Daten dürfen nur bestimmte Strafverfolgungsbehörden erhalten. Dies zum Zwecke der Ermittlung, Feststellung und Verfolgung der in der Vorratsdatenrichtlinie genannten Straftaten. Eine Liste der Strafverfolgungsbehörden muß veröf-

[152] *Feiel*, jusIT 2008/46, 97
[153] Stellungnahme des europäischen Datenschutzbeauftragten zur Vorratsdatenrichtlinie, RZ 9 ff, C 298 vom 29. November 2005
[154] Art 29 Datenschutzgruppe, WP 113
[155] Art 29 Datenschutzgruppe, WP 119

fentlicht werden. Ferner müssen alle Datenabrufe protokolliert und die Aufzeichnungen den Datenschutzbehörden zu Kontrollzwecken zur Verfügung gestellt werden.

3. Es sollen so wenig Daten wie möglich auf Vorrat gespeichert werden.

4. Bei der Ermittlung, Feststellung und Verfolgung der in der Vorratsdatenrichtlinie angeführten Straftaten dürfen die dabei auf Vorrat gespeicherten Daten nicht ausgewertet werden, etwa zum Zwecke der Feststellung des Reise- und Kommunikationsverhaltens von Personen, die von den Strafverfolgungsbehörden nicht zum Kreis der Verdächtigen gezählt werden.

5. Der Zugang zu den Daten muß grundsätzlich in jedem Einzelfall von einer Justizbehörde ordnungsgemäß genehmigt werden, es sei denn, in einem Mitgliedstaat ist die Möglichkeit des Datenzugriffs bereits gesetzlich geregelt und unterliegt der Aufsicht durch eine unabhängige Instanz.

6. Betreiber öffentlicher elektronischer Kommunikationsdienste oder Betreiber öffentlicher Kommunikationsnetze dürfen Daten, die gemäß der Vorratsdatenrichtlinie allein zu Zwecken der öffentlichen Ordnung gespeichert wurden, nicht für andere (z.B. ihre eigenen) Zwecke auswerten.

7. Betreiber haben getrennte Systeme einzurichten, so dass Systeme, in denen Daten zu Zwecken der öffentlichen Ordnung gespeichert werden von jenen Systemen getrennt werden, die Betreiber für ihre geschäftlichen Zwecke verwenden.

8. Die allgemeinen Anforderungen der Vorratsdatenrichtlinie müssen durch Mindeststandards ergänzt werden, die genau regeln, welche technischen und organisatorischen Sicherheitsvorkehrungen die Anbieter treffen müssen.

Meines Erachtens sind sowohl der Europäische Datenschutzbeauftragte als auch die Art 29 Datenschutzgruppe zu nachgiebig, indem sie zwar Mindestanforderungen an die Vorratsdatenrichtlinie stellen, allerdings zum Preis einer (weiteren) Aushöhlung der Grundrechte. Dies wird aus meiner Sicht dazu führen, dass die Hemmschelle, Eingriffe in die Grundrechte vorzunehmen, weiter sinken wird. Ich gehe davon aus, dass Kriminelle und Mitglieder terroristischer Gruppen sich auf die Vorratsdatenrichtlinie einstellen werden. Dies wird dazu führen, dass an der „Schraube" noch fester gedreht wird und weitere Kontrollmaßnahmen, die Hand in Hand mit einer Grundrechtseinschränkung gehen werden, erlassen werden.

Ist einmal der erste Schritt getan, fällt der nächste Überwachungsschritt umso leichter. Es ist unschwer auszumalen, was passieren wird, sollte ein nächster Terroranschlag in Europa - der sich auch mit der Vorratsdatenspeicherung nicht verhindern lassen wird - stattfinden[156].

7.4. Grundrecht auf Datenschutz

[156] Stellungnahme der ARGE DATEN - Österreichische Gesellschaft für Datenschutz im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 21. Mai 2007

Der Vollständigkeit halber soll hier auch das Grundrecht auf Datenschutz Erwähnung finden. Aufgrund der oben angestellten Überlegungen zum Anwendungsvorrang des Gemeinschaftsrechts gegenüber entgegenstehendem innerstaatlichen Recht (mit eingeschlossen dem Verfassungsrecht), kann die Vorratsdatenrichtlinie, beziehungsweise die innerstaatliche Umsetzung in österreichisches Recht, nicht am Maßstab des DSG 2000 geprüft werden.

Die Verfassungsbestimmung des § 1 DSG 2000 regelt das Grundrecht auf Datenschutz, wonach jedermann Anspruch auf die Achtung seines Privat- und Familienlebens, auf Geheimhaltung seiner personenbezogenen Daten hat, soweit ein schutzwürdiges Interesse daran besteht. Personenbezogene Daten sind gemäß § 4 Z 1 DSG 2000 Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. Weil es nach dem DSG 2000 irrelevant ist, in welcher Form, beziehungsweise auf welchen Datenträgern Daten gespeichert werden, und Verkehrs- und Standortdaten bestimmten Personen zugeordnet werden können, sind (oder besser wären) die Bestimmungen des DSG 2000 auch auf die Novelle des TKG 2003 anwendbar[157].

Gemäß § 1 Abs 2 DSG 2000 sind Beschränkungen des Grundrechts auf Datenschutz nur zulässig, (a) wenn die Verwendung von personenbezogenen Daten im lebenswichtigen Interesse des Betroffenen liegt oder (b) mit seiner Zustimmung erfolgt oder (c) zur Wahrung überwiegender berechtigter Interessen eines anderen, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art 8 Abs 2 ERMK genannten Gründen notwendig sind. Derartige Gesetze dürfen gemäß § 1 Abs 2 DSG 2000 die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

Die Vorratsdatenspeicherung ist daher auch im Hinblick auf das DSG 2000 problematisch. Jedenfalls wäre gemäß des DSG 2000 eine Vorratsdatenspeicherung grundsätzlich unzulässig. Eine Einschränkung des Grundrechts ist zwar nicht ausgeschlossen, aber wiederum nur dann zulässig, wenn entweder lebenswichtige oder öffentliche Interessen den Grundrechtsschutz überwiegen, weswegen auf die obigen Überlegungen(zu Art 8 EMRK) hingewiesen wird.

7.5. Der Schutz des Fernmeldegeheimnisses

Ebenso der Vollständigkeit halber, wird das Grundrecht auf Schutz des Fernmeldegeheimnisses beleuchtet. Das Fernmeldegeheimnis ist in Art 10a StGG normiert. Das Grundrecht schützt die Vertraulichkeit der über Fernmeldeanlagen (Telefon, Fernschreiber, Funk, sonstige Datenübertragungen) vermittelten und nicht zur Kenntnisnahme durch Dritte bestimmten Kommunikation[158]. Das Fernmeldegeheimnis darf gemäß Art 10a StGG nicht verletzt werden. Ausnahmen von der Bestimmung des

[157] *Otto/Seitlinger,* MR 2006, 227, mwN
[158] *Berka*, Lehrbuch Grundrechte, RZ 297

vorstehenden Absatzes sind nur auf Grund eines richterlichen Befehles in Gemäßheit bestehender Gesetze zulässig.

Strittig ist, ob das Fernmeldegeheimnis auch Verkehrsdaten sowie Standortdaten umfaßt oder ob nur Inhaltsdaten durch das Fernmeldegeheimnis geschützt sind. Nach der Judikatur des OGH umfaßt das Fernmeldegeheimnis nicht nur Kommunikationsinhalte, sondern auch Vermittlungsdaten[159]. In der Lehre wird dies überwiegend anders gesehen, wonach der verfassungsrechtliche Schutz des Fernmeldegeheimnisses auf die Inhalte der Kommunikation zu beschränken ist. Begründet wird dies im Wesentlichen aus der Entstehungsgeschichte. Art 10a StGG sei aus der älteren Gewährleistung des Briefgeheimnisses heraus entwickelt worden[160].

Folgt der österreichische Gesetzgeber aber der Judikatur des OGH, hätte dies zur Folge, dass die gemäß Art 5 Abs 1 der Vorratsdatenrichtlinie zu speichernden Daten auch vom Fernmeldegeheimnis umfaßt sind. Weil ein Eingriff in das Grundrecht auf Schutz des Fernmeldegeheimnisses nur auf Grund eines richterlichen Befehles in „Gemäßheit" bestehender Gesetze zulässig ist, bedarf eine generelle Anordnung zur Vorratsdatenspeicherung ohne richterlichen Befehl einer Umsetzung im Verfassungsrang[161].

8. Kosten

8.1. Allgemeines

Die Richtlinie zur Vorratsdatenspeicherung sieht keine Pflicht zur staatlichen Entschädigung der betroffenen Unternehmen vor und überläßt diese Frage den Mitgliedstaaten. Ebensowenig sieht der Entwurf der Novelle zum TKG 2003 eine Kostenersatzpflicht zugunsten der betroffenen Unternehmen vor.

8.2. Wirtschaftliche Auswirkungen

Die wirtschaftlichen Auswirkungen sind indes beachtlich. Der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres geht von enormen Belastungen für die europäische Telekommunikationsindustrie aus. Kosten würden insbesondere im Zusammenhang mit der Anpassung der Systemtechnik zur Generierung und Speicherung der Daten, der Anpassung der betrieblichen Abläufe zur sicheren Archivierung der Daten sowie der Bearbeitung und Auswertung von Anfragen der Sicherheitsbehörden erwachsen. Der hierfür erforderliche Investitionsaufwand im Bereich der klassischen leitungsvermittelten Telefonie läge nach Schätzungen verschiedenster größerer Unternehmen innerhalb der Mitgliedstaaten bei € 180 Mio im Jahr pro Unternehmen mit jährlichen Betriebskosten bis zu € 50 Mio. Der Geschäftsbetrieb kleinerer und mittlerer Unternehmen sei sicher gefährdet. Nach Schätzungen würden im Bereich des Internets die

[159] *Feiel*, jusIT 2008/46, 97, mwN
[160] *Kunnert*, Der sicherheitspolizeiliche Griff nach Telekommunikationsdaten, in *Jahnel*, Jahrbuch Datenschutzrecht und E-Government 08, 83 (120)
[161] *Feiel*, jusIT 2008/46, 97

Belastungen den Investitionsaufwand im Bereich der klassischen leitungsvermittelten Telefonie um ein Vielfaches übersteigen[162].

Die Deutsche Vereinigung für Datenschutz e.V. zitierte im September 2004 den Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. in Berlin[163], der den Aufwand mit einem hohen zweistelligen Millionenbetrag je Unternehmen beziffert hatte, und die Deutsche Telekom, die von Investitionskosten in Höhe von € 180 Mio und jährlichen Mehrkosten von € 40 Mio ausgegangen war[164].

Die Telekom Austria geht in ihrer Stellungnahme im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 21. Mai 2007 von Mehrkosten in der Höhe von mindestens € 4,5 Mio aus. Die Telekom Austria fordert daher, den Gesetzesentwurf um eine entsprechende Kostenabgeltung zugunsten der betroffenen Betreiber zu ergänzen[165].

Der österreichische Gesetzgeber hält in den Gesetzesmaterialien fest, dass mit der Novelle des TKG 2003 die Telekommunikationsbetreiber verpflichtet werden, Verkehrs- und Standortdaten, die beim Erbringen von Kommunikationsdiensten erzeugt oder verarbeitet werden, für Zwecke der Strafverfolgung zu speichern. In den Gesetzesmaterialien wird weiters festgehalten, dass diese Speicherverpflichtung ausschließlich Daten betrifft, die bereits derzeit für Verrechnungszwecke gespeichert werden. Mehrkosten könnten daher allenfalls deswegen entstehen, weil einerseits die Speicherung nunmehr anders strukturiert werden muß, um Anordnungen der Strafverfolgungsbehörden entsprechen zu können und andererseits durch die Befolgung der Anordnung selbst[166].

8.3. Rechtsprechung des VfGH

Obgleich daher der österreichische Gesetzgeber in den Erläuterungen anerkennt, dass ein Privatrechtsträger staatliche, im öffentlichen Interesse liegende Aufgaben der Strafrechtspflege, übernimmt, hat er keine Kostenersatzpflicht im Gesetzesentwurf vorgesehen. Der VfGH hob am 27.02.2003 § 89 Abs 1 letzter Satz des Telekommunikationsgesetz, BGBl. I Nr. 100/1997, als verfassungswidrig auf, weil diese Bestimmung keine Kostenersatzpflicht vorgesehen hatte, obwohl eine staatliche Aufgabe auf ein privates Unternehmen überwälzt worden war[167].

---

[162] Bericht des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres, Europäisches Parlament, vom 31.05.2005; ähnlich: Stellungnahme des Europäischen Datenschutzbeauftragten zur Vorratsdatenrichtlinie, RZ 68, C 298 vom 29. November 2005 (bis zu € 150 Mio/Jahr für die Vorratsspeicherung und € 50 Mio/Jahr an Betriebskosten)

[163] http://www.bitkom.org/

[164] Deutsche Vereinigung für Datenschutz e.V., Hintergrundinformationen zur Pressemitteilung vom
30. September 2004

[165] Stellungnahme der Telekom Austria im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 21. Mai 2007

[166] Die Gesetzesmaterialien zur Novelle des TKG 2003 sind abrufbar unter:
http://www.parlinkom.gv.at/PG/DE/XXIII/ME/ME_00061/pmh.shtml

[167] G37/02 ua

Der VfGH führte in dieser Entscheidung aus, dass die Überwachung des Fernmeldeverkehrs im Zuge der Strafverfolgung nach den verfassungsrechtlichen Wertungen grundsätzlich Sache des Bundes ist, der den mit der Strafverfolgung verbundenen Aufwand, soweit er Gebietskörperschaften trifft, zu tragen hat. Wenn Überwachungskosten, die an sich vom Bund zu tragen sind, auf private Unternehmen überwälzt werden, so ist der Gesetzgeber gehalten, den Verhältnismäßigkeitsgrundsatz zu beachten. Es ist daher einerseits eine Abwägung der Höhe der den Privaten erwachsenen Kosten und andererseits die Kriterien, die eine besondere rechtliche und wirtschaftliche Beziehung begründen, vorzunehmen. Zu diesen Kriterien gehören unter anderem die Eingrenzbarkeit und damit die konkrete Kalkulierbarkeit der vom Privaten zu erbringenden Leistungen, die wirtschaftliche Zumutbarkeit des Aufwandes für den einzelnen Unternehmer, ein allfälliges Interesse, das nicht bloß die Allgemeinheit, sondern auch die betroffenen Unternehmer selbst an den im Rahmen der Mitwirkung zu erbringenden Leistungen haben, und eine allfällige zusätzliche Gefährdung, die gerade vom Betrieb des Unternehmens ausgeht und der durch die vom Unternehmen verlangte Mitwirkung entgegengewirkt werden soll.

Auch wenn nach der Rechtsprechung des VfGH die Inpflichtnahme privater Betreiber von Telekommunikationsdiensten für die Überwachung des Fernmeldeverkehrs und die Bereitstellung entsprechender Einrichtungen eine sachlich gerechtfertigte und daher verfassungsmäßige Mitwirkungspflicht Privater an einer staatlichen Aufgabe darstellen kann, so ist dennoch auch bei der Regelung der Kostentragung der Verhältnismäßigkeitsgrundsatz zu beachten. Budgetäre Gründe allein bilden jedenfalls keine ausreichende sachliche Rechtfertigung für eine vom Gesetzgeber getroffene (beziehungsweise fehlende) Kostentragungsregelung.

8.4. Stellungnahmen im Begutachtungsverfahren

Ins gleiche Horn stoßen die Industriellen Vereinigung und die ISPA. Die Industriellenvereinigung vermißt im Entwurf der Novelle des TKG 2003 eine Kostenabgeltung zugunsten der betroffenen Unternehmen und wendet ein, dass der Entwurf eine Reihe zusätzlicher Verpflichtungen für die Telekommunikationsbetreiber vorsieht, womit erhebliche Mehrkosten im öffentlichen Interesse begründet würden, denen allerdings kein wirtschaftlicher Nutzen gegenüberstünde. Die Mehrkosten seien laut der Industriellenvereinigung allerdings noch nicht abschätzbar, weil zunächst die bereits angekündigte Änderung der Überwachungsverordnung abgewartet werden müßte.

Jedenfalls würde infolge des Umstandes, dass der Entwurf eine Speicherdauer von sechs Monaten vorsieht, für die Netzbetreiber ein weiterer Kostenfaktor entstehen. Eine zusätzliche finanzielle Belastung für die (betroffenen) Unternehmen würde aufgrund der im Entwurf vorgesehenen Sicherungsmaßnahmen nach § 102a Abs 3 und 4 TKG entstehen[168].

Die ISPA ist der Dachverband der österreichischen Internet Service-Anbieter, der 1997 als Verein gegründet worden ist und als Interessenvertretung und Sprachrohr der ös-

[168] Stellungnahme der Industriellenvereinigung im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 18. Mai 2007

terreichischen Internet-Wirtschaft fungiert[169]. Die ISPA bringt vor, dass von der vorgesehenen Speicherverpflichtung nicht nur Daten betroffen seien, die ohnedies bereits zu Verrechnungszwecken gespeichert werden. Zudem würden Investitionskosten für sichere Systeme und Schnittstellen anfallen[170].

Sowohl die Industriellenvereinigung als auch die ISPA heben hervor, dass es sich bei der Vorratsdatenspeicherung letztlich um eine Maßnahme handelt, die im öffentlichen Interesse liegt, weil sie der Strafverfolgung dient und dadurch als der Teil der staatlichen Aufgaben vom Staat zu erfüllen sei. Beide heben die oben erwähnte Entscheidung des VfGH hervor und wünschen die gesetzliche Umsetzung dieses Erkenntnisses.

Die Datenschutzkommission kritisiert ebenfalls den Umstand, dass der Entwurf der Novelle zum TKG 2003 keine Kostenersatzpflicht des Bundes vorgesehen hat. Die Datenschutzkommission führt dazu in ihrer Stellungnahme aus, dass sie entsprechend des Art 9 der Vorratsdatenrichtlinie zur Vollziehung des neuen § 102a TKG 2003 berufen sein wird. Gemäß § 102a Abs 4 TKG 2003 haben die Anbieter und Betreiber öffentlicher Kommunikationsnetze zu gewährleisten, dass jede Anfrage und Übermittlung von Daten nach dieser Bestimmung protokolliert wird. Diese „Protokolldaten" sind auf Ersuchen der Datenschutzkommission dieser mitzuteilen. In diesem Zusammenhang kritisiert – und hält dies für inakzeptabel – die Datenschutzkommission, dass im Vorblatt zu den Erläuterungen unter „Finanzielle Auswirkungen" kein Resourcenbedarf für die Wahrnehmung dieser Aufgabe angemeldet worden ist[171]. Freilich kann hier nicht ins Treffen geführt werden, dass Kosten, die an sich vom Bund zu tragen sind, auf private Unternehmen überwälzt werden.

Das e-center ist ebenso der Ansicht, dass mit der Novelle des TKG 2003 Mehrkosten verbunden sein werden. Insbesondere wird die Einführung entsprechender Überwachungs- und Speicheranlagen, abhängig von der Größe des Providers, mit erheblichen Kosten verbunden sein. Ein großer Teil der Kosten wird allerdings auch durch die Anpassung innerbetrieblicher Prozesse notwendig werden. Dies wird vor allem Internet Service Provider betreffen, weil diese bislang keine Standort- und (abgesehen von statischen IP-Adressen) auch keine Verkehrsdaten speichern mußten[172].

Die Aufklärung strafbarer Handlungen durch Überwachung des Fernmeldeverkehrs bildet eine im öffentlichen Interesse gelegene staatliche Aufgabe, die aus Gründen der Effektivität eine Mitwirkung der Telekommunikationsdienstebetreiber erfordert, weil diese Betreiber infolge ihrer technischen Sachnähe die Überwachung am ehestens durchführen können. Ein öffentlich-rechtlicher Auftrag, bestimmte Daten zu speichern, diese für eine bestimmte Dauer vorrätig zu halten und auf staatliches Verlangen hin zugänglich zu machen, greift dann grundsätzlich in die Eigentumsgaran-

[169] http://www.ispa.at/index.php?id=6
[170] Stellungnahme der ISPA vom 21. Mai 2007
[171] Stellungnahme der Datenschutzkommission im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 23. Mai 2007
[172] Stellungnahme des europäischen Zentrum für e-commerce und internetrecht im Begutachtungsverfahren zum Entwurf der Novelle des TKG 2003 vom 15. Mai 2007

tie ein, wenn dieser Rechtsbefehl an ein vom Staat verschiedenes Rechtssubjekt gerichtet ist. Eine verfassungsmäßig einwandfreie Regelung erfordert daher, dass die Last derartiger Mitwirkungspflichten nicht unverhältnismäßig ist[173]. Die fehlende Auseinandersetzung des österreichischen Gesetzgebers mit der Kostenlast der privaten Kommunikationsdiensteanbieter, beziehungsweise die unterlassene Kostenersatzregelung zugunsten der betroffenen Unternehmen, ist aus meiner Sicht unverhältnismäßig.

Abschließend ist daher festzuhalten, dass die Novelle des Telekommunikationsgesetzes 2003 auch aus diesem Blickwinkel betrachtet problematisch erscheint. Infolge des durchaus vergleichbaren Sachverhaltes, der der Entscheidung des VfGH zu G37/02 zugrunde gelegen ist, kann davon ausgegangen werden, dass auch die Novelle des Telekommunikationsgesetzes – so sie je in Kraft treten sollte – verfassungswidrig ist. Die Vorratsdatenspeicherung erfolgt nicht zu Gunsten privater Unternehmen, sondern dient ausschließlich der Erfüllung öffentlicher Aufgaben.

9. Zusammenfassung

Die mit der Vorratsdatenrichtlinie und deren Umsetzung in die Rechtsordnungen der Mitgliedstaaten der Europäischen Gemeinschaft normierte generelle und vor allem anlasslose Pflicht zur Speicherung von Verkehrs- Stamm- Zugangs- und Standortdaten, die zumindest eine aussagekräftige Datensammlung ergeben und es ermöglichen Bewegungsprofile aller Nutzer zu erstellen, ist ein exzessiver Eingriff in das Grundrecht auf Achtung des Privat- und Familienlebens, der einer Verhältnismäßigkeitsprüfung aus meiner Sicht nicht standhalten kann. Aufgrund der Vorratsdatenspeicherung werden Daten aller Nutzer von Telekommunikationsdienstleistungen gespeichert, die (überwiegend) keine Veranlassung zu derartigen Verfolgungshandlungen gesetzt haben. Die Vorratsdatenspeicherung führt dazu, dass alle Nutzer als potentiell schuldig oder zumindest als grundsätzlich verdächtig betrachtet werden, eine strafbare Handlung begangen zu haben. Im Ergebnis wird die Unschuldsvermutung damit in ihr Gegenteil verkehrt.

Auch wenn keine Inhaltsdaten gespeichert werden (dürfen), läßt die Vorratsdatenspeicherung Rückschlüsse auf Art und Intensität von Beziehungen, Interessen, Gewohnheiten und Neigungen und nicht zuletzt auch auf den jeweiligen Kommunikationsinhalt zu und vermitteln – je nach Art und Umfang der angefallenen Daten – Erkenntnisse, die an die Qualität eines Persönlichkeitsprofils heranreichen.

Es ist freilich ein hehres und legitimes Ziel sowie ein berechtigtes Interesse des Staates, beziehungsweise des europarechtlichen Gesetzgebers, seine Bürger vor Kriminalität und Terrorattacken bestmöglich zu schützen. Dies kann aber nur als Rechtfertigung herangezogen werden, insoweit an der Eignung der Vorratsdatenspeicherung, Kriminalität und Terrorattacken zu verhindern, keine Zweifel bestehen. Gerade dies ist al-

[173] *Feiel*, jusIT 2008/46, 97, mwN

lerdings keineswegs der Fall. Es ist davon auszugehen, dass sich Kriminelle und Terroristen rasch auf die Vorratsdatenspeicherung einstellen und Anonymisierungstechniken entwickeln werden. Schon jetzt könnten Kriminelle und Terroristen anonym über Prepaid Dienste oder öffentliche Telefonzellen, die aufgrund der Universaldienstrichtlinie (2002/22/EG) wohl sobald nicht aus dem Straßenbild verschwinden werden, Straftaten und Terrorattacken verabreden. Zudem könnte auch über Internet E-Mail ein derartiges Verbrechen anonym bis zur Ausführung geplant werden.

Zudem ist es kaum einzusehen, dass durch den Verweis auf § 17 SPG auch Fahrlässigkeitsdelikte dem Regime der Vorratsdatenspeicherung unterliegen. Hier hätte der österreichische Gesetzgeber zumindest – und ohne inhaltlich gegen die Umsetzungspflicht zu verstoßen – auf § 17 StGB zurückgreifen müssen.

Zudem verfügte aus meiner Sicht das Europäische Parlament und der Rat der Europäischen Union nicht über die Kompetenz zum Erlaß der Vorratsdatenrichtlinie. Auch aus der Geschichte der Richtlinie wird deutlich, dass im Vordergrund keineswegs die Harmonisierung von Rechtsvorschriften in den einzelnen Mitgliedstaaten gestanden hat, sondern die Bekämpfung der Kriminalität und des Terrorismus. Bereits der Rahmenbeschluss aus dem April 2004 ließ deutlich diese Intention erkennen. Weiters sind auch die Erwägungsgründe des Rahmenbeschlusses zumindest teilweise die gleichen wie jene der Vorratsdatenrichtlinie. In diesem Zusammenhang ist ferner festzuhalten, dass in manchen Mitgliedstaaten vor der Vorratsdatenrichtlinie überhaupt keine „einschlägigen" Rechtsvorschriften bestanden haben, weswegen der Terminus „Harmonisierung" verfehlt und unangebracht ist. Daraus folgt, dass das Ziel der Vorratsdatenrichtlinie, nämlich die Harmonisierung der Rechtsvorschriften in den Mitgliedstaaten, tatsächlich nur ein Vorwand ist. Es dürfte auch kein Zufall sein, dass ursprünglich auch ein Rahmenbeschluss zur Regelung dieser überaus strittigen Inhalte vorgesehen gewesen ist.

Ferner ist festzuhalten, dass staatliche Aufgaben, nämlich die Verhütung, Bekämpfung und Aufklärung der Kriminalität, durch die Vorratsdatenrichtlinie und deren Umsetzung in innerstaatliches Recht, auf die Schultern privater Unternehmen abgewälzt wird, wobei eine Kostenersatzpflicht zugunsten der betroffenen Unternehmen nicht vorgesehen ist. Die Anbieter öffentlicher Kommunikationsnetze und Telekommunikationsunternehmen sind für den Mißbrauch ihrer Dienste durch Straftäter wohl nicht verantwortlich zu machen. Die fehlende Kostenersatzpflicht des Bundes ist angesichts der Rechtsprechung des VfGH zweifellos unzulässig. Schließlich werden diese Mehrkosten wohl vom Konsumenten oder Steuerzahler getragen werden, je nachdem, ob noch eine Kostenerstattung nachgereicht wird oder nicht.

Insgesamt können die Bedenken, die schon beim Rahmenbeschluss vom 28. April 2004 bestanden (und geäußert) worden sind, auch durch die Vorratsdatenrichtlinie nicht entkräftet werden.

Letztlich ist zu fragen, wohin dieser einmal eingeschlagene Weg, der eine (weitere) Aushöhlung der Grundrechte nach sich zieht, führen wird. Diesen Gedanken will man

gar nicht zu Ende denken, möchte man nicht am Ende des Tages beim völligen Überwachungsstaat landen.

10. Danksagung

Danken möchte ich meinen Eltern, die mir ein tolles Leben und zwei erfolgreiche Studienabschlüsse ermöglichten; es ist nicht das erste Mal, dass sie mich in durchaus anstrengenden und zuweilen schwierigen Zeiten unterstützten. Dank schulde ich außerdem meiner Schwester Ingrid und ihrer Tochter Lena für Zuspruch und Unterstützung und dafür, dass die beiden eben die beiden sind.

Ebenfalls zu Dank verpflichtet bin ich ao. Univ.Prof. Dr. Dietmar Jahnel, der mich bei und während dieser Arbeit betreute.

Dank schulde ich ferner Barbara Ullram: für sorgfältiges Durchlesen, wohldurchdachte Kritik und Überarbeiten sämtlicher meiner Referate und Powerpoint Präsentationen für Vorträge, die ich während des Lehrgangs halten mußte. Mehr als einmal, hat sie mich besser aussehen lassen als ich bin.

Danken möchte ich außerdem Rudolf Habenbacher, der mir an einem trüben Novemberabend 2007 mit äußerster Geduld das Binärzahlsystem, sozusagen das „kleine Einmaleins“ und damit „Grundlegendes“, solange erklärte, bis ich es verstand. Nochmals danke, meine Prüfungsarbeit "Hardware" wurde mit Sehr Gut benotet. Dank gebührt auch seiner Freundin Renate Koch, die diesen Vortrag geduldig ertragen mußte.

Ebenfalls danken möchte ich den „www.theyoungdudes.com“ für jahrzehntelange treue Freundschaft.

Nicht zuletzt möchte ich Heinz Neuner und Greg Robbins danken, die immer an mich glaubten und nie müde wurden, mich darin zu bestärken, an mich selbst zu glauben. Ich danke Euch, Freunde!

Michael Binder im September 2008