

# **Ist die Speicherung dynamischer IP-Adressen von Kunden, die einen Flatrate-Vertrag haben, durch Access Provider zulässig?**

**Dennis Jlussi**

*cand. iur. an der*

*Gottfried Wilhelm Leibniz Universität Hannover*

*Diese Arbeit wurde mit dem Absolventenpreis 2007 der Deutschen Stiftung für Recht und Informatik (DSRI) ausgezeichnet.*

## **Auszug**

*Diesen Auszug veröffentlicht der Autor unter einer Creative Commons Lizenz.*



*Der Lizenztext ist abrufbar über*

*<http://creativecommons.org/licenses/by-nc-nd/2.0/de/>.*

## Inhalt

<b>Abbildungsverzeichnis .....</b>	<b>14</b>
<b>Abkürzungsverzeichnis .....</b>	<b>15</b>
<b>Zusammenfassung.....</b>	<b>18</b>
<b>Abstract .....</b>	<b>19</b>
<b>Literatur- und Quellenverzeichnis .....</b>	<b>20</b>
<b>A. Einführung .....</b>	<b>28</b>
<b>I. Gesellschaftliche Relevanz .....</b>	<b>28</b>
<b>II. Jüngste Entwicklung in Rechtsprechung und Praxis .....</b>	<b>30</b>
<b>III. Herangehensweise .....</b>	<b>31</b>
<b>B. Grundlagen.....</b>	<b>34</b>
<b>I. Zentrale Begriffe.....</b>	<b>34</b>
<b>1. Dynamische IP-Adresse .....</b>	<b>34</b>
a) Allgemeines .....	34
b) Zuteilung von IP-Adressen .....	35
<b>2. Access Provider .....</b>	<b>36</b>
a) Allgemeines .....	36
b) Reseller .....	37
<b>3. Flatrate.....</b>	<b>37</b>
<b>4. Terminologie im Datenschutz .....</b>	<b>38</b>
a) Grundbegriffe des Umgangs mit Daten.....	38
b) Speichern und Löschen.....	39
<b>II. Access Provider als Telekommunikations- und     Telemediendiensteanbieter .....</b>	<b>39</b>
<b>1. Telekommunikationsdiensteanbieter .....</b>	<b>40</b>
a) Literatur und Rechtsprechung.....	40
b) Bundesnetzagentur .....	40
c) Gemeinschaftsrechtlicher Hintergrund.....	41
d) Stellungnahme .....	42
<b>2. Telemediendiensteanbieter.....</b>	<b>43</b>
a) Access Provider als Vermittler .....	43
b) Schichtenmodell.....	44
c) Abgrenzung bei Kombinationsangebot .....	45
aa) Gemeinschaftsrechtlicher Hintergrund.....	45
bb) Klärung durch das Telemediengesetz? .....	46
d) Diskussion.....	47
aa) Keine schematische Anwendung des OSI-Modells im Recht	48
bb) Systematik des TMG .....	49
cc) Richtlinienkonformität .....	49
dd) Ergebnis.....	50
e) Bewertung.....	50

<b>C. Die IP-Adresse und ihr rechtlicher Schutz</b> .....	<b>51</b>
<b>I. Europäisches Recht</b> .....	<b>51</b>
<b>1. Unionsgrundrechte</b> .....	<b>51</b>
a) Achtung des Privat- und Familienlebens .....	51
b) Schutz personenbezogener Daten .....	51
<b>2. Marktfreiheiten</b> .....	<b>52</b>
a) Betroffene Marktfreiheiten .....	52
b) Funktion des Internet zur Verwirklichung der Freiheiten .....	52
c) Stellungnahme.....	53
<b>3. Sekundärrecht</b> .....	<b>54</b>
a) Datenschutzrichtlinie .....	54
b) Datenschutzrichtlinie für elektronische Kommunikation.....	55
<b>4. Internationales Binnenmarktrecht</b> .....	<b>56</b>
a) Europäische Menschenrechtskonvention .....	57
aa) Allgemeines.....	57
bb) Artikel 8 .....	57
b) Datenschutz-Konvention .....	57
<b>II. Deutsches Recht</b> .....	<b>58</b>
<b>1. Grundrechte</b> .....	<b>58</b>
a) Informationelle Selbstbestimmung .....	59
aa) Entstehung.....	59
bb) Inhalt und Schranken .....	59
b) Fernmeldegeheimnis.....	59
aa) Historische Entwicklung.....	59
bb) Inhalt und Schranken .....	60
c) Verhältnis der Grundrechte zueinander.....	61
<b>2. Einfachgesetzlicher Schutz</b> .....	<b>61</b>
a) Datenschutzrecht .....	61
aa) Verbotsprinzip mit Erlaubnisvorbehalt .....	61
bb) Datenvermeidung und Datensparsamkeit .....	61
b) Telekommunikationsrecht .....	62
aa) Telekommunikations-Datenschutz.....	62
bb) Schutz juristischer Personen.....	62
c) Telemedienrecht .....	63
d) Europäische Menschenrechtskonvention.....	63
<b>III. Die IP-Adresse als personenbezogenes Datum</b> .....	<b>64</b>
<b>1. Bestimmbarkeit des Teilnehmers</b> .....	<b>64</b>
<b>2. Bestimmbarkeit des Nutzers</b> .....	<b>64</b>
<b>IV. Die IP-Adresse als Verkehrsdatum</b> .....	<b>65</b>
<b>1. Definition und Funktion</b> .....	<b>65</b>
a) Legaldefinition .....	65
b) Entstehung von Verkehrsdaten .....	66
aa) Prinzip der Verkehrsdaten in der Telefonie .....	66
bb) Übertragbarkeit der Prinzipien auf das Internet .....	67
<b>2. Bewertung im Hinblick auf Auskunftsbegehren</b> .....	<b>69</b>
a) Klare Einordnung.....	69

b) Unterscheidung zwischen den Daten und Auskunft .....	69
aa) Widersprüchlichkeit .....	70
bb) Stellungnahme .....	71
<b>V. Die IP-Adresse als Standortdatum? .....</b>	<b>72</b>
<b>1. Einordnung als Standortdatum .....</b>	<b>72</b>
<b>2. Rechtsfolgen der Einordnung .....</b>	<b>73</b>
a) Möglicher Widerspruch .....	73
aa) Mobile Anschlüsse .....	73
bb) Dienst mit Zusatznutzen .....	74
cc) Mögliche Rechtsfolge .....	74
b) Diskussion .....	74
aa) Änderung des Wortlauts gegenüber der TDSV .....	74
bb) Verstoß gegen Sparsamkeitsgebot .....	75
c) Gemeinschaftsrechtlicher Hintergrund .....	75
d) Stellungnahme .....	75
<b>VI. Erhebung und Löschungspflicht .....</b>	<b>76</b>
<b>1. Erhebung und Speicherung für die Verbindung .....</b>	<b>76</b>
<b>2. Löschungspflicht mit Erlaubnisvorbehalt .....</b>	<b>76</b>
<b>D. Erlaubnis für die Speicherung .....</b>	<b>77</b>
<b>I. Einwilligung .....</b>	<b>77</b>
<b>1. Abschließende Regelung im TKG .....</b>	<b>77</b>
<b>2. Grundrechtliche Abwägung .....</b>	<b>78</b>
a) Privatautonomie .....	78
b) Schutz des Kommunikationspartners .....	78
c) Veräußerlichkeit von Grundrechten .....	78
d) Beschränkung der Privatautonomie .....	79
<b>3. Gemeinschaftsrechtlicher Hintergrund .....</b>	<b>79</b>
<b>4. Stellungnahme .....</b>	<b>79</b>
<b>II. Vermarktung, Gestaltung und Dienste mit Zusatznutzen .....</b>	<b>80</b>
<b>1. Vermarktung und Gestaltung .....</b>	<b>81</b>
<b>2. Dienste mit Zusatznutzen .....</b>	<b>81</b>
<b>III. Speicherung zur Entgeltermittlung und -abrechnung .....</b>	<b>82</b>
<b>1. Ermittlung und Abrechnung .....</b>	<b>82</b>
<b>2. Nachweis der Richtigkeit .....</b>	<b>83</b>
a) Streit über die Richtigkeit .....	83
b) Praktische Bedeutung und Beweiskraft .....	83
c) Beweislast .....	84
d) Speicherung der IP-Adresse zum Nachweis? .....	84
<b>3. Einzelverbindungs nachweis .....</b>	<b>84</b>
a) Einzelverbindungs nachweis bei Internet-Flatrate? .....	84
b) IP-Adresse im Einzelverbindungs nachweis? .....	85
c) Zulässigkeit der Speicherung .....	86
<b>4. Abrechnung mit anderen Diensteanbietern .....</b>	<b>86</b>
a) Fremde Diensteanbieter .....	86
b) Diensteanbieter ohne eigenes Netz .....	87
<b>5. Leistungsermittlung .....</b>	<b>88</b>

<b>IV. Speicherung zur Fehler- und Störungsbeseitigung .....</b>	<b>89</b>
1. <b>Offensichtlichkeit der Störung?</b> .....	<b>89</b>
2. <b>Verhältnismäßigkeit</b> .....	<b>90</b>
3. <b>Ergebnis</b> .....	<b>90</b>
<b>V. Bekämpfung von Leistungserschleichungen .....</b>	<b>91</b>
1. <b>Telekommunikationsrecht</b> .....	<b>91</b>
2. <b>Telemedienrecht</b> .....	<b>91</b>
3. <b>Abgrenzung</b> .....	<b>92</b>
4. <b>Rechtswidrige Inhalte als rechtswidrige Inanspruchnahme?</b> ..	<b>92</b>
<b>VI. Speicherung zur Gewährleistung der ICT-Sicherheit.....</b>	<b>93</b>
1. <b>Bedeutung der IP-Adresse für die Gewährleistung von     ICT-Sicherheit.....</b>	<b>93</b>
2. <b>ICT-Sicherheit als Erlaubnistatbestand?.....</b>	<b>94</b>
a) <b>Telemedienrecht</b> .....	<b>95</b>
b) <b>Telekommunikationsrecht</b> .....	<b>95</b>
<b>VII. Speicherung aufgrund von Auskunftspflichten .....</b>	<b>96</b>
1. <b>Bestehende Auskunftspflichten</b> .....	<b>96</b>
a) <b>Auskunftspflichten im Urheberrecht</b> .....	<b>96</b>
b) <b>Andere Auskunftspflichten</b> .....	<b>97</b>
2. <b>Auskunftspflichten als Erlaubnistatbestand?</b> .....	<b>97</b>
a) <b>Das schwedische Öffentlichkeitsprinzip</b> .....	<b>97</b>
b) <b>Rechtsprechung und Literatur</b> .....	<b>98</b>
c) <b>Stellungnahme</b> .....	<b>98</b>
3. <b>Änderungen durch das TKG-Änderungsgesetz?</b> .....	<b>100</b>
4. <b>Änderungen durch die Durchsetzungsrichtlinie</b> .....	<b>101</b>
a) <b>Durchsetzungsrichtlinie und Umsetzung</b> .....	<b>101</b>
b) <b>Erlaubnistatbestand durch die Umsetzung der         Durchsetzungsrichtlinie?</b> .....	<b>101</b>
aa) <b>Ziele der Richtlinie</b> .....	<b>102</b>
bb) <b>Schadensersatzanspruch</b> .....	<b>102</b>
cc) <b>Vorabentscheidungsersuchen</b> .....	<b>102</b>
dd) <b>Stellungnahme</b> .....	<b>102</b>
<b>VIII. Speicherung im Rahmen der Telekommunikationsüberwachung .....</b>	<b>103</b>
1. <b>Rechtsgrundlagen der TK-Überwachung</b> .....	<b>103</b>
a) <b>TK-Überwachung im Strafprozessrecht</b> .....	<b>103</b>
b) <b>Telekommunikationsüberwachung im Gefahrenabwehrrecht</b> ..	<b>104</b>
c) <b>TK-Überwachung zu geheimdienstlichen Zwecken</b> .....	<b>104</b>
2. <b>TK-Überwachung als Erlaubnistatbestand?</b> .....	<b>104</b>
<b>IX. Speicherung für IP-Billing.....</b>	<b>105</b>
1. <b>IP-Billing als Zahlungsmethode</b> .....	<b>105</b>
2. <b>Einwilligung</b> .....	<b>106</b>
3. <b>§ 97 Abs. 6 TKG</b> .....	<b>106</b>
4. <b>Stellungnahme</b> .....	<b>107</b>
<b>X. Unverzügliche Löschung .....</b>	<b>108</b>
1) <b>Unverzüglichkeit</b> .....	<b>109</b>

<b>2) Zumutbarkeit und Güterabwägung .....</b>	<b>110</b>
<b>E. Anstehende Umsetzungen.....</b>	<b>112</b>
<b>I. Umsetzung der Cybercrime Konvention .....</b>	<b>112</b>
<b>1. Gegenstand der Konvention.....</b>	<b>112</b>
a) Strafprozessuale Maßnahmen.....	112
b) Materieller Anwendungsbereich .....	113
<b>2. Umsetzung der Konvention .....</b>	<b>114</b>
a) Ratifikationsstand unter den Mitgliedsstaaten der EU.....	114
b) Umsetzung in Deutschland .....	114
aa) Umgehende Sicherung .....	114
bb) Herausgabebeanordnung.....	115
cc) Verkehrsdatenerfassung in Echtzeit.....	115
<b>II. Umsetzung der Data Retention Richtlinie.....</b>	<b>115</b>
<b>1. Gegenstand der Richtlinie.....</b>	<b>115</b>
<b>2. Umsetzung der Richtlinie .....</b>	<b>116</b>
<b>3. Formelle und materielle Bedenken.....</b>	<b>117</b>
a) Formelle Bedenken .....	117
b) Materielle Bedenken .....	118
c) Stellungnahme.....	119
<b>F. Resümee .....</b>	<b>121</b>

## Abbildungsverzeichnis

Abbildung 1: IP-Pakete und Vermittlung über den Access Provider .....	36
Abbildung 2: Das OSI Schichtenmodell.....	44
Abbildung 3: Entstehung von Verkehrsdaten bei Telefongesprächen .....	66

## Abkürzungsverzeichnis

a.A.	andere Ansicht
a.a.O.	am angegebenen Ort
Abb.	Abbildung
ABl.	Amtsblatt der Europäischen Union (vor 2003: Amtsblatt der Europäischen Gemeinschaften)
Abs.	Absatz
Anm.	Anmerkung
ABMG	Autobahnmautgesetz
AG	Amtsgericht / Aktiengesellschaft
Art./Artt.	Artikel (Singular/Plural)
Aufl.	Auflage
BB	Betriebsberater
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BFH	Bundesfinanzhof
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BK	Beschlusskammer (der Bundesnetzagentur)
BR-Drs.	Bundesrats-Drucksache
BT-Drs.	Bundestags-Drucksache
Bundesnetzagentur	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
CR	Computer und Recht
ders., dies.	derselbe, dieselbe(n)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSRL	Datenschutzrichtlinie
DSRLeK	Datenschutzrichtlinie für elektronische Kommunikation
DTAG	Deutsche Telekom AG
DuD	Datenschutz und Datensicherheit
E	Entscheidungssammlung
EC	European Community
ECRL	E-Commerce-Richtlinie
EG	Europäische Gemeinschaft(en) <i>mit Artikelangabe:</i> Vertrag zur Gründung der Europäischen Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
EL	Ergänzungslieferung

EMRK	Europäische Menschenrechtskonvention (Konvention zum Schutze der Menschenrechte und Grundfreiheiten)
EU	Europäische Union <i>mit Artikelangabe:</i> Vertrag über die Europäische Union
EuGH	Gerichtshof der Europäischen Gemeinschaften
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWG	Europäische Wirtschaftsgemeinschaft
f., ff.	folgend, fortfolgend
Fn.	Fußnote
FS	Festschrift
G10	Artikel-10-Gesetz
GG	Grundgesetz für die Bundesrepublik Deutschland
GRC	Grundrechtecharta (Charta der Grundrechte der Europäischen Union)
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GSM	Global System for Mobile Communications
h.M.	herrschende Meinung
Hrsg.	Herausgeber
IANA	Internet Assigned Numbers Authority
ICT	Information and Communications Technology
IP	Internet Protocol
i.S.d.	im Sinne des
ISDN	Integrated Services Digital Network
ISO	Internationale Organisation für Normung
i.V.m.	in Verbindung mit
J Bus Ethics	Journal of Business Ethics
JZ	Juristen Zeitung
K&R	Kommunikation und Recht
KG	Kammergericht
LG	Landgericht
lit.	litera (Buchstabe)
LNCS	Lecture Notes in Computer Science
MDSStV	Mediendienste-Staatsvertrag
MMR	MultiMedia und Recht
MR	Medien und Recht
MSN	Multi Subscriber Number
m.w.N.	mit weiteren Nachweisen
NCC	Network Coordination Centre
NdsGVBl.	Niedersächsisches Gesetz- und Verordnungsblatt
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NSOG	Niedersächsisches Sicherheits- und Ordnungsgesetz
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
ö	( <i>vorangestellt</i> ) österreichisch
OGH	Oberster Gerichtshof (der Republik Österreich)
OLG	Oberlandesgericht

OSI	Open Systems Interconnection
PoP	Point of Presence
RADIUS	Remote Authentication Dial-In User Service
RDV	Recht der Datenverarbeitung
RefE	Referentenentwurf
RegE	Regierungsentwurf
RegTP	Regulierungsbehörde für Telekommunikation und Post
resp.	respektive
RIPE	Réseaux IP Européens
RL	Richtlinie
Rn.	Randnummer
RP	Regierungspräsidium
RR	Rechtsprechungs-Report
RStV	Rundfunkstaatsvertrag
S.	Seite
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TDDSG	Teledienstdatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikations-Datenschutzverordnung
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung
TKV	Telekommunikations-Kundenschutzverordnung
TMG	Telemediengesetz
u.a.	unter anderem / und andere
u.ä.	und ähnliches
UrhG	Urheberrechtsgesetz
USA	United States of America
vgl.	vergleiche
Vorbem.	Vorbemerkung
WDR	Westdeutscher Rundfunk
ZAP	Zeitschrift für die Anwaltspraxis
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik

## Zusammenfassung

Die Speicherung von dynamischen IP-Adressen durch Access Provider ist ein rechtlich, rechtspolitisch und gesellschaftlich diskutiertes Thema, insbesondere im Hinblick auf die nicht anlassbezogene Vorratsdatenspeicherung. Access Provider sind TK-Diensteanbieter; zugleich erfordert insbesondere das Gemeinschaftsrecht, sie auch als Telemediendiensteanbieter zu klassifizieren. Für die Erhebung, Verwendung und Löschung von IP-Adresszuordnungen gelten daher die besonderen Datenschutzbestimmungen des TKG und des TMG.

Da die dynamische IP-Adresse ein Verkehrsdatum ist und dem Fernmeldegeheimnis unterliegt, muss der Access Provider die Zuordnung grundsätzlich unverzüglich nach dem Verbindungsende löschen. Eine darüber hinausgehende anlassbezogene Verwendung ist nur bei Missbrauchsverdacht und mit Einwilligung des Teilnehmers auch für den Einzelverbindungs-nachweis und IP-basierte Zahlungssysteme zulässig; Abrechnungszwecke, Auskunftspflichten des Access Providers und die Datensicherung können hingegen die Speicherung nicht rechtfertigen. Die Vorratsspeicherung ist unzulässig; daran ändert auch der Blick auf das europäische Recht nichts, weil die Richtlinie zur Vorratsspeicherung formell und materiell rechtswidrig ist.

## **Abstract**

The processing of data about dynamically assigned IP addresses by internet access providers is an issue that is being widely discussed in aspects of law, politics and civil rights, especially concerning blanket retention of that data. Access providers are telecommunication service providers; at the same time, especially considering European law, they are to be classified as telemedia service providers. Therefore, for collection and processing of IP address assignments, both the Telecommunications Act and the Telemedia Act are relevant.

As any IP address assignment is traffic data and therefore protected by the constitutional secrecy of telecommunications, data about the assignments have to be erased forthwith after the connections are terminated. Further retention can only be justified for individual data, namely for the purposes of prevention of abuse and, with the subscriber's consent, also for itemised bills and IP-based billing services. General billing, any obligations to give information, and data security are not justifications for retention. Traffic data retention is illegal and cannot be justified by the EC Data Retention Directive, as the directive is void by law in form and content.

## Literatur- und Quellenverzeichnis

**Aust, Sascha**

IP-Adressen schneller gelöscht – Internetprovider speichern Verbindungsdaten von Flatratennutzern nur noch wenige Tage, Hannoversche Allgemeine Zeitung vom 22. Februar 2007, S. 14.

**Bär, Wolfgang**

Auskunftsanspruch über Telekommunikationsdaten nach den neuen §§ 100g, 100h StPO, MMR 2002, S. 358-364.

*ders.*

Anmerkung zur Entscheidung LG Ulm, MMR 2004, S. 187-188.

*ders.*

Anmerkung zur Entscheidung LG Frankfurt/Main, MMR 2004, S. 339-343.

*ders.*

Anmerkung zur Entscheidung LG Stuttgart, MMR 2005, S. 626-627.

**Bleich, Holger**

Aufbewahrungsverbot, c't 15/2005, S. 32.

**Bosse, Rolf / Richter, Thomas / Schreier, Michael**

Abrechnung mit IP-Adressen, CR 2007, S. 79-84.

**Breyer, Jonas**

Vorratsspeicherung von IP-Adressen durch Access Provider, DuD 2003, S. 491-495.

**Breyer, Patrick**

Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005.

*ders.*

Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal 2005, S. 365-375.

**Bundesbeauftragter für den Datenschutz und die Informationsfreiheit**  
(Hrsg.)

Website des BfDI, Bonn, <http://www.bfdi.bund.de>.

**Burhoff, Detlef**

Auskunft über Telekommunikationsverbindungsdaten, ZAP 2002, Fach 22, S. 359-360.

**Business Software Alliance** (Hrsg.)

Website der Business Software Alliance, München, <http://www.bsa.de>.

**Busse-Muskala, Dominika und Veit**

Die Berücksichtigung europäischer Vorgaben bei der Abgrenzung eigener und fremder Informationen nach dem TDG, JurPC Web-Dokument 30/2005, <http://www.jurpc.de/aufsatz/20050030.htm>.

**Callies, Christian / Ruffert, Matthias (Hrsg.)**

EUV/EGV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, Kommentar, 3. Aufl., München 2007 (zitiert Callies/Ruffert – *Bearbeiter*).

**Czychowski, Christian**

Auskunftsansprüche gegenüber Internetzugangsp Providern „vor“ dem 2. Korb und „nach“ der Enforcement-Richtlinie der EU, MMR 2004, S. 514-519.

**Dietrich, Ralf**

Rechtsprechungsbericht zur Auskunftspflicht des Access-Providers nach Urheberrechtsverletzungen im Internet - Anmerkung zu LG Flensburg, GRUR-RR 2006, 174, GRUR-RR 2006, S. 145-147.

**Dix, Alexander**

Vorratsspeicherung von IP-Adressen?, DuD 2003, S. 234-236

**Eckhardt, Jens**

Kommentar zum Urteil des LG Darmstadt, K&R 2006, S. 293-296.

**Einzinger, Kurt / Schubert, Agnes / Schwabl, Wolfgang / Wessely, Karin / Zykan, David**

Wer ist 217.204.27.214? Access-Provider im Spannungsfeld zwischen Auskunftsbegehrliehkeiten der Rechteinhaber und Datenschutz, MR 2005, S. 113-118.

**Elbel, Thomas**

Die datenschutzrechtlichen Vorschriften für Diensteanbieter im neuen Telekommunikationsgesetz auf dem Prüfstand des europäischen und deutschen Rechts, diss. iur., Berlin 2005.

**Echenbach, Jürgen / Niebaum, Frank**

Von der mittelbaren Drittwirkung unmittelbar zur staatlichen Bevormundung, NVwZ 1994, S. 1079-1082.

**Europarat, Vertragsbüro (Hrsg.)**

Website des Vertragsbüros des Europarates, Straßburg, <http://conventions.coe.int>.

**Fisahn, Andreas**

Ein unveräußerliches Grundrecht am eigenen genetischen Code, ZRP 2001, S. 49-54.

**Forgó, Nikolaus / Feldner, Birgit / Witzmann, Martin / Dieplinger, Simone** (Hrsg.)

Probleme des Informationsrechts, Wien 2003.

**Fröhle, Jens**

Web Advertising, Nutzerprofile und Teledienstedatenschutz,  
München 2003.

**Geppert, Martin / Piepenbrock, Hermann-Josef / Schütz, Raimund / Schuster, Fabian** (Hrsg.)

Beck'scher TKG-Kommentar, 3. Aufl., München 2006  
(zitiert BeckTKG – *Bearbeiter*).

**Gercke, Marco**

Analyse des Umsetzungsbedarfs der Cybercrime Konvention - Teil 2:  
Die Umsetzung im Bereich des Strafverfahrensrechts,  
MMR 2004, S. 801-806.

**Gesellschaft für deutsche Sprache** (Hrsg.)

Wörter, die Geschichte machten – Schlüsselbegriffe des  
20. Jahrhunderts, Gütersloh/München 2001.

**Grabitz, Eberhard** (Begründer) / **Hilf, Meinhard** (Hrsg.) /

**Wolf, Manfred** (Hrsg.)

Das Recht der Europäischen Union, Band III, Sekundärrecht:  
EG-Verbraucher- und Datenschutzrecht, Loseblatt, Stand 30. EL,  
München 2006.

**Grote, Elisabeth**

Die Telekommunikations-Kundenschutzverordnung,  
BB 1998, S. 1117-1120.

**Heidrich, Joerg**

Die T-Online-Entscheidung des RP Darmstadt und ihre Folgen,  
DuD 2003, S. 237-238.

**Heise, Christian und Ansgar / Persson, Christian** (Hrsg.)

Heise Online, Hannover, <http://www.heise.de>.

**Hoeren, Thomas / Sieber, Ulrich** (Hrsg.)

Handbuch Multimedia Recht, Loseblatt,  
Stand 16. EL, München 2006 (zitiert Hoeren/Sieber – *Bearbeiter*).

**IDG Business Media** (Hrsg.)

Tecchannel, München, <http://www.tecchannel.de>.

**International Federation of the Phonographic Industry, Deutsche Landesgruppe** (Hrsg.)

Website der deutschen Phonoverbände, Berlin, <http://www.ifpi.de>.

**Jandach, Thomas**

Identität und Anonymität bei der elektronischen Kommunikation, in  
*Taeger, Jürgen / Wiebe, Andreas* (Hrsg.): Informatik-Wirtschaft-Recht –

Regulierung der Wissensgesellschaft – Festschrift für Wolfgang Kilian,  
S. 443-461.

**Johnston, Steven R.**

The Impact of Privacy and Data Protection Legislation on the Sharing  
of Intrusion Detection Information, LNCS 2212/2001, S. 150-171.

**Kazemi, Robert**

Anmerkung zur Entscheidung des AG Darmstadt,  
MMR 2005, S. 636-637.

*ders.*

Anmerkung zur Entscheidung des BGH, MMR 2007, S. 37-38.

**Kemmitt, Helen / Mögelin, Chris**

Data Protection and Privacy, in *Scherer, Joachim (Hrsg.)*,  
Telecommunication Laws in Europe, 5. Aufl., Haywards Heath 2005,  
S. 112-124.

**Kilian, Wolfgang**

Europäisches Wirtschaftsrecht, 2. Auflage, München 2003.

**Kitz, Volker**

Die Auskunftspflicht des Zugangsvermittlers bei Urheberrechts-  
verletzungen durch seine Nutzer, GRUR 2003, S. 1014-1019.

**Klaß & Ihlenfeld Verlag (Hrsg.)**

Golem.de – IT-News für Profis, Berlin, <http://www.golem.de>.

**Klein, Eckart**

Grundrechtliche Schutzpflicht des Staates, NJW 1989, S. 1633-1640.

**Koenig, Christian / Loetz, Sascha / Neumann, Andreas**

Telekommunikationsrecht, Heidelberg 2004.

**Köcher, Jan / Kaufmann, Noogie**

Anmerkung zur Entscheidung LG Hamburg, MMR 2005, S. 61-62.

*dies.*

Speicherung von Verkehrsdaten bei Internet-Access-Providern,  
DuD 2006, S. 360-364.

**Köster, Oliver / Jürgens, Uwe**

Haftung professioneller Informationsvermittler im Internet - Eine  
Bestandsaufnahme nach der Novellierung der Haftungsregelungen,  
MMR 2002, S. 420-425.

**Krasemann, Henry**

Besprechung des Beschlusses des Landgerichts Frankfurt am Main  
vom 15.05.2003 (Az.: 5/6 Qs 47/03) und des Beschlusses des  
Landgerichts Frankfurt am Main vom 21.10.2003 (Az.: 5/8 Qs 26/03),  
JurPC Web-Dokument 140/2004,  
<http://www.jurpc.de/aufsatz/20040140.htm>.

**Lepperhoff, Niels / Tinnefeld, Marie-Theres**

Aussagewert der Verkehrsdaten – Aspekte der Sicherheitspolitik, des Datenschutzes und der Wirtschaft, RDV 2004, S. 7-11.

**Leutheusser-Schnarrenberger, Sabine**

Vorratsdatenspeicherung – Ein vorprogrammierter Verfassungskonflikt, ZRP 2007, S. 9-13.

**Linke, Thomas**

Anmerkung zur Entscheidung des OLG Hamburg, MMR 2005, S. 456-458.

**Malek, Klaus**

Strafsachen im Internet, Heidelberg 2005.

**Di Martino, Alessandra**

Datenschutz im Europäischen Recht, Berlin 2004,  
<http://www.whi-berlin.de/documents/whi-paper1504.pdf>.

**Meyer, Jürgen (Hrsg.)**

Charta der Grundrechte der Europäischen Union (Kommentar),  
2. Aufl., Baden-Baden 2006 (zitiert MeyerGRC – *Bearbeiter*).

**Meyer-Ladewig, Jens**

Europäische Menschenrechtskonvention,  
Kommentar, 2. Aufl., Baden-Baden 2006.

**Michelfelder, Diane**

The moral value of informational privacy in cyberspace,  
Ethics and Information Technology 2001, S. 129-135.

**Mühlbauer, Peter**

Wer die Verbindungsdaten speichert, Telepolis 16.01.2007,  
<http://www.heise.de/tp/r4/artikel/24/24446/1.html>.

*ders.*

Wer die Verbindungsdaten speichert (und das Gegenteil behauptet),  
Telepolis 24.01.2007,  
<http://www.heise.de/tp/r4/artikel/24/24496/1.html>.

**Nachbaur, Andreas**

Standortfeststellung und Art. 10 GG – Der Kammerbeschluss des  
BVerfG zum Einsatz des „IMSI-Catchers“, NJW 2007, S. 335-337.

**Ohlenburg, Anna**

Der neue Telekommunikationsdatenschutz - Eine Darstellung von Teil  
7 Abschnitt 2 TKG, MMR 2004, S. 431-440.

**Penders, Jacques**

Privacy in (mobile) telecommunications services, Ethics and  
Information Technology 2004, S. 247-260.

**Pfeiffer, Gerd** (Hrsg.)

Karlsruher Kommentar zur Strafprozessordnung, 5. Aufl.,  
München 2003 (zitiert KKStPO – *Bearbeiter*).

**Pincus, Laura B. / Johns, Roger**

Private Parts: A Global Analysis of Privacy Protection Schemes and a  
Proposed Innovation for Their Comparative Evaluation,  
J Bus Ethics 1997, S. 1237-1260.

**Pocar, Fausto**

New Challenges for International Rules against Cyber-Crime,  
European Journal on Criminal Policy and Research 2004, S. 27-37.

**Pollach, Irene**

A Typology of Communicative Strategies in Online Privacy Policies:  
Ethics, Power and Informed Consent, J Bus Ethics 2005, S. 221-235.

**Rieß, Peter** (Hrsg.)

Löwe/Rosenberg – Die Strafprozessordnung und das  
Gerichtsverfassungsgesetz, Band 2: §§ 72-136a, 25. Aufl., Berlin 2004  
(zitiert Löwe/Rosenberg – *Bearbeiter*).

**Roßnagel, Alexander** (Hrsg.)

Handbuch Datenschutzrecht, München 2003.

**Sankol, Barry**

Die Qual der Wahl: § 113 TKG oder §§ 100g, 100h StPO? - Die  
Kontroverse über das Auskunftsverlangen von Ermittlungsbehörden  
gegen Access-Provider bei dynamischen IP-Adressen,  
MMR 2006, S. 361-365.

**Schild, Hans-Hermann**

Die Richtlinie über die Verarbeitung personenbezogener Daten und  
den Schutz der Privatsphäre im Bereich der Telekommunikation,  
EuZW 1999, S. 69-74.

*ders.*

Vom Dreigestirn zum Zweigestirn? - Ein Beitrag zum sprachlichen  
Babylon nach dem zukünftigen neuen TMG und dem 9. RÄStV,  
MMR 2007, Heft 2, S. V-VI.

**Schmitz, Peter**

Anmerkung zur Entscheidung des OLG Hamburg,  
MMR 2000, S. 615-617.

*ders.*

Inhalt und Gestaltung von Telekommunikationsverträgen,  
MMR 2001, S. 150-158.

*ders.*

Anmerkung zur Beurteilung des RP Darmstadt,  
MMR 2003, S. 214-216.

**Schramm, Marc**

Staatsanwaltschaftliche Auskunft über dynamische IP-Adressen,  
DuD 2006, S. 785-788.

**Schuster, Fabian (Hrsg.)**

Vertragshandbuch Telemedia, München 2001.

**Schütz, Raimund**

Anmerkung zur Regulierungsverfügung der RegTP,  
MMR 1999, S. 557-568.

**Sieber, Ulrich / Höfninger, Frank Michael**

Drittauskunftsansprüche nach § 101a UrhG gegen Internetprovider zur  
Verfolgung von Urheberrechtsverletzungen, MMR 2004, S. 575-585.

**Simitis, Spiros (Hrsg.)**

Bundesdatenschutzgesetz (Kommentar), 6. Aufl., Baden-Baden 2006  
(zitiert Simitis/Bearbeiter).

**Spindler, Gerald (Hrsg.)**

Vertragsrecht der Internet-Provider, 2. Aufl., Köln 2004.

*ders.*

Anmerkung zur Entscheidung des OLG Frankfurt/Main,  
MMR 2005, S. 243-245.

**Spindler, Gerald / Schmitz, Peter / Geis, Ivo**

Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz,  
Kommentar, 1. Aufl., München 2004.

**Splitzgerber, Andreas / Klytta, Joanna**

Auskunftsansprüche gegen Internetprovider, K&R 2007, S. 78-85.

**Steele, Jonathan**

Data Protection: An Opening Door? The Relationship between  
Accessibility and Privacy in Sweden in an EU Perspective,  
Liverpool Law Review 2002, S. 19-39.

**teltarif.de Onlineverlag (Hrsg.)**

teltarif.de, Berlin, <http://www.teltarif.de>.

**Ulmer, Claus / Schrief, Dorothee**

Datenschutz im neuen Telekommunikationsrecht – Bestandsaufnahme  
eines Telekommunikationsdienstleisters zum aktuellen Entwurf des  
Telekommunikationsgesetzes, RDV 2004, S. 3-7.

**Vassilaki, Irini**

EU-Richtlinie zur Vorratsspeicherung: Aufklärung von Straftaten oder  
Aushöhlung von Grundrechten, MMR 2006, Heft 2, S. XIII

**Volkemann, Christian**

Anmerkung zur Entscheidung des VG Düsseldorf,  
CR 2005, S. 893-894.

**Waldenberger, Arthur**

Teledienste, Mediendienste und die „Verantwortlichkeit“ ihrer  
Anbieter, MMR 1998, S. 124-129.

**Westdeutscher Rundfunk (Hrsg.)**

Website der Redaktion Quintessenz, Radio WDR 2,  
<http://www.wdr.de/radio/wdr2/quintessenz>.

**Westphal, Dietrich**

Die neue EG-Richtlinie zur Vorratsdatenspeicherung – Privatsphäre  
und Unternehmerfreiheit unter Sicherheitsdruck,  
EuZW 2006, S. 555-560.

**Wiebe, Andreas**

Anmerkung zur Entscheidung des OGH, MMR 2005, S. 827-830.

**Wikimedia Foundation (Hrsg.)**

Wikipedia – Die freie Enzyklopädie, St. Petersburg (USA),  
<http://de.wikipedia.org>.

**Wuermeling, Ulrich / Felixberger, Stefan**

Fernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz,  
CR 1997, S. 230-238.

*Die Internet-Quellen wurden sämtlich im Februar/März 2007 gesichtet.*

“There’s no place like 127.0.0.1“  
Fortune Cookie<sup>1</sup>

## A. Einführung

### I. Gesellschaftliche Relevanz

Erläuterungen darüber, wie sehr das Internet im „Informationszeitalter“ Lebens-, Konsum- und Kommunikationsgewohnheiten der Menschen – oder kurz: die Welt – verändert hat, wirken heute bereits nahezu großväterlich; jedenfalls ist das Internet ein Schlüsselbegriff des vergangenen Jahrhunderts.<sup>2</sup>

Das gilt jedoch nicht für den Datenschutz: Die Diskussion über den Datenschutz im Allgemeinen und über den Schutz der IP-Adresse im Besonderen ist aus zweierlei Hinsicht in jüngerer und jüngster Zeit gesellschaftlich relevant geworden:

Erstens haben die Terroranschläge vom 11. September 2001 in den USA eine weltweite und noch immer andauernde Sicherheitsdiskussion ausgelöst; in Europa hat sich diese Diskussion nach den weiteren Terroranschlägen am 11. März 2004 in Madrid und am 7. Juli 2005 in London verschärft. Die „westliche Welt“ befindet sich in einem anhaltenden Dilemma zwischen der Verteidigung ihrer Grundwerte und Errungenschaften gegen Terroristen und dem Erhalt ihrer Grundwerte und -rechte bei ebendieser Verteidigung. Praktisch überall sind strengere Überwachungsmaßnahmen beschlossen worden, auch hinsichtlich der elektronischen Kommunikation. Andere Formen von schwerer Kriminalität, insbesondere der Handel mit Kinderpornografie über das Internet, tragen ebenso dazu bei, den Ruf nach einer stärkeren Überwachung von elektronischer Kommunikation laut werden zu

---

<sup>1</sup> Fortune Cookies (Glückskekse) sind ein beliebtes Gimmick bei textbasierten Terminalservern: Bei jedem Login wird dem Benutzer eine „Weisheit“ angezeigt wie in einem Glückskeks. Der genannte Fortune Cookie ist angelehnt an den (in echten Glückskekse zu findenden) Spruch „There is no place like home“: 127.0.0.1 ist die IP-Adresse für eine Verbindung (*loopback*) zum eigenen Rechner (*localhost*).

<sup>2</sup> *Gesellschaft für deutsche Sprache (Hrsg.)*, Wörter die Geschichte machten, S. 142f.; danach ist auch „Datenverarbeitung“ ein Schlüsselbegriff des 20. Jahrhunderts (S. 91f.), nicht jedoch „Datenschutz“.

lassen. Tatsächlich sind die rechtlichen Möglichkeiten für die staatliche TK-Überwachung seit der Einführung des G10 im Jahr 1968 stetig ausgedehnt, aber fast nie zurückgenommen worden.<sup>3</sup>

Zweitens haben die Inhaber von geistig-gewerblichen Schutzrechten den politischen und gesellschaftlichen Druck gegen „Raubkopien“<sup>4</sup> und „Piraterie“ erheblich verschärft. Durch Kampagnen wie „Raubkopierer sind Verbrecher“<sup>5</sup> haben sie sich öffentliche Aufmerksamkeit geschaffen. Die *Business Software Alliance* gibt für das Jahr 2002 in Deutschland einen Schaden allein durch illegale Softwarekopien von einer Milliarde Euro an,<sup>6</sup> die deutschen Phonoverbände sprechen für den Bereich der Musik von einer „dreistelligen Millionenhöhe“.<sup>7</sup> Die Rechteinhaber wünschen sich effektive Möglichkeiten, um gegen „Raubkopierer“ vorzugehen; dazu gehört auch und gerade die Auskunft der Access Provider über die Person hinter einer ermittelten IP-Adresse.

Bei alledem ist das Problembewusstsein der Bürger eher gering. Wer nichts zu verbergen hat, kann auch nichts gegen die Verwendung seiner Daten haben, solange mit den Daten kein offensichtliches Schindluder getrieben wird, lautet eine verbreitete Auffassung.<sup>8</sup> Das mag auch daran liegen, dass die informationelle „Kräfteverteilung“ zwischen dem Access Provider und seinem Kunden ungleichmäßig ist:<sup>9</sup> Der Kunde hat häufig weder technische Kenntnisse darüber, was gespeichert werden kann, noch rechtliche Kenntnisse darüber, was genau gespeichert werden darf; selbst Nachfragen beim Access Provider können falsch beauskunftet werden.

---

<sup>3</sup> P. Breyer, *Die systematische Aufzeichnung...*, S. 25f., m.w.N.

<sup>4</sup> Der Begriff ist üblich, aber tendenziös: Eine illegale Kopie anzufertigen, hat mangels Drohung oder Gewalt nicht einmal im übertragenen Sinne etwas mit einem Raub nach § 249 StGB zu tun.

<sup>5</sup> Vgl. <http://www.hartabergerecht.de>, eine Initiative der Kino- und Filmwirtschaft.

<sup>6</sup> *Business Software Alliance*, <http://www.bsa.org/germany/piraterie/auswirkungen.cfm>.

<sup>7</sup> *International Federation of the Phonographic Industry*, Pressemitteilung vom 24.01.2007, <http://www.ifpi.de/news/news-822.htm>.

<sup>8</sup> *Michelfelder*, *Ethics and Information Technology* 2001, 129, [130].

<sup>9</sup> So auch *Pollach*, *J Bus Ethics* 2005, 221 [224] für das Verhältnis Kunde-Onlineshop. *Jandach*, FS Kilian, S. 443, unterscheidet bei der Qualität der Anonymität im Internet deswegen zwischen der, die nur im Verhältnis zum Kommunikationspartner besteht und der, die auch gegenüber dem Access Provider besteht.

Es sitzen daher sowohl die Access Provider als auch der Staat zwischen den Stühlen: Die Access Provider sind einerseits ihren Kunden zum Schutz ihrer jeweiligen Daten verpflichtet und andererseits kommen Ermittlungsbehörden und Rechteinhaber auf sie zu mit Auskunftsbegehren, die sie nur erfüllen können, wenn sie die Daten, die sie beauskunften sollen, zunächst einmal überhaupt speichern. Der Staat wiederum will einerseits notwendige (und darüber hinaus publikumswirksame) Maßnahmen gegen Kriminalität und Terrorismus treffen, soll aber andererseits die Privatautonomie der Bürger schützen, indem er das informationelle Kräfteungleichgewicht ausgleicht.

## II. Jüngste Entwicklung in Rechtsprechung und Praxis

Aufsehen erregt haben vor allem Entscheidungen des AG<sup>10</sup> und des LG<sup>11</sup> Darmstadt gegen T-Online. Nachdem das *RP Darmstadt*<sup>12</sup> als zuständige Aufsichtsbehörde (§ 38 BDSG)<sup>13</sup> die Beschwerde eines Kunden von T-Online darüber, dass das Unternehmen die ihm dynamisch zugewiesenen IP-Adressen speicherte, abschlägig beurteilte, begehrte dieser von T-Online im Klageweg die Unterlassung der Speicherung und bekam vom AG im wesentlichen Recht; das LG hat im Berufungsverfahren den Tenor im wesentlichen bestätigt.

Der *BfDI* hält das Urteil des LG Darmstadt für allgemeingültig.<sup>14</sup> Gleichwohl findet es in der Praxis keine breite Beachtung: Bei einer journalisti-

---

<sup>10</sup> *AG Darmstadt*, MMR 2005, 634, m. Anm. *Kazemi*.

<sup>11</sup> *LG Darmstadt*, GRUR-RR 2006, 173; das Urteil ist rechtskräftig, der *BGH* (MMR 2007, 37, m. Anm. *Kazemi*) hat die Beschwerde gegen die Nichtzulassung der Revision als unzulässig zurückgewiesen.

<sup>12</sup> *RP Darmstadt*, MMR 2003, 213, m. Anm. *Schmitz*.

<sup>13</sup> Eigentlich war das RP wegen § 89 Abs. 4 TKG a.F. (§ 115 Abs. 4 TKG n.F.) sachlich unzuständig; zuständig wäre der *BfDI*; *Schmitz*, Anm. zu *RP Darmstadt*, MMR 2003, 214 [215]; wohl auch *Dix*, DuD 2003, 234 [235]. Zur Einschlägigkeit des TKG sogleich.

<sup>14</sup> *BfDI*, Speicherung von IP-Adressen bei Flatrate-Verträgen, [http://www.bfdi.bund.de/clin\\_029/nn\\_530308/DE/Themen/Kommunikationsdienst\\_eMedien/Internet/Artikel/SpeicherungVonIP-AdressenBeiFlatrate-Vertraegen.html](http://www.bfdi.bund.de/clin_029/nn_530308/DE/Themen/Kommunikationsdienst_eMedien/Internet/Artikel/SpeicherungVonIP-AdressenBeiFlatrate-Vertraegen.html); das Urteil als solches entfaltet subjektive Rechtskraft freilich nur *inter partes*, § 325 Abs. 1 ZPO.

schen Umfrage<sup>15</sup> um den Jahreswechsel 2006/2007 unter sechzig Access Providern haben zwölf Unternehmen eingeräumt, die dynamisch zugewiesene Adresse mit einer Zuordnung zum Kunden zu speichern, dreißig Unternehmen verweigerten die Auskunft.

Die Zahl von achtzehn Access Providern, die angaben, nicht zu speichern, welchem Kunden sie welche IP-Adresse zuordneten, hat sich nach Reaktionen von Lesern, die Kunden dieser Provider sind und wegen Urheberrechtsverletzungen anhand der IP-Adresse ermittelt und sodann abgemahnt wurden, noch einmal relativiert:<sup>16</sup> Einige Unternehmen mussten einräumen, bei der Umfrage falsche Angaben gemacht zu haben, andere gaben an, sie würden zwar nicht die dynamische IP-Adresse speichern, aber „andere Daten“, die eine Ermittlung des Vertragskunden anhand der bei der DTAG gespeicherten IP-Adresse ermöglichten.

Die DTAG hat – mit technischer Wirkung auch für ihre Reseller – angekündigt, die gespeicherten IP-Adressen nunmehr nur noch sieben Tage zu speichern, anstatt, wie vorher, bis zu achtzig Tagen.<sup>17</sup> Hintergrund dessen ist eine mit der Wirtschaft und dem Referat für TK-Datenschutz bei der *Bundesnetzagentur* abgestimmte Auffassung des *BfDI*, die Speicherung bis zu 14 Tagen zuzulassen.<sup>18</sup> Die nunmehr von 80 auf sieben Tage verkürzte Speicherungsfrist ist von der Medienindustrie als „Zumutung“ für den Schutz geistig-gewerblicher Schutzrechte bezeichnet worden.<sup>19</sup>

### III. Herangehensweise

Zunächst muss geklärt werden, welches Recht für die Speicherung von IP-Adressen einschlägig ist: Das Telekommunikations- oder das Telemedien-

---

<sup>15</sup> *Mühlbauer*, Wer die Verbindungsdaten speichert, Telepolis 16.01.2007.

<sup>16</sup> *Mühlbauer*, Wer die Verbindungsdaten speichert (und das Gegenteil behauptet), Telepolis 24.01.2007.

<sup>17</sup> *Aust*, Hannoversche Allgemeine Zeitung vom 22.02.2007, S. 14; *Heise Online*, T-Online speichert IP-Adressen nur noch sieben Tage, 20.02.2007, <http://www.heise.de/newsticker/meldung/85609>.

<sup>18</sup> Vgl. auch die Schilderung des *AG Darmstadt*, MMR 2005, 634 [635]; dass diese Auffassung Bestand hat, hat die *Bundesnetzagentur* d. Verf. am 05.03.2007 mitgeteilt.

<sup>19</sup> *Heise Online*, Einwöchige Speicherung für Verbindungsdaten als „Zumutung“ kritisiert, 14.03.2007, <http://www.heise.de/newsticker/meldung/86686>.

recht? Selbst wenn diese Unterscheidung *im Ergebnis* keinen Unterschied machen würde,<sup>20</sup> müsste sie dennoch für eine dogmatisch einwandfreie Beurteilung erfolgen. Die Frage, welches Recht anwendbar ist, stellt sich auch deshalb, weil das TKG – trotz einiger Modernisierungen – noch immer auf Telefonie als klassische Form der Telekommunikation fokussiert ist und daher wichtige Fragen der Internet-Kommunikation nur schwer erfassen kann.<sup>21</sup> Darüber hinaus wird zu zeigen sein, dass sich durchaus Unterschiede hinsichtlich der ins einfache Recht hineinstrahlenden einschlägigen Grundrechte ergeben<sup>22</sup> und gerade die jüngsten Gesetzgebungen die Abgrenzung im Detail verändert haben.

Sodann wird zunächst zu zeigen sein, wodurch dynamische IP-Adressen (und deren Zuordnung zu einem bestimmten Kunden) eigentlich vor einer Speicherung geschützt sind. Jeder kann tun und lassen – also auch speichern und löschen – was er will, solange er nicht die Rechte anderer verletzt, Art. 2 Abs. 1 GG. Damit die Titelfrage nicht mit einem lapidaren „warum denn nicht?“ beantwortet werden kann, müssen diese Rechte anderer zunächst untersucht und aufgezeigt werden, wie das deutsche und das europäische Recht die Internetnutzer grundsätzlich davor schützen, dass die Access Provider die Zuordnung der dynamisch vergebenen IP-Adresse speichern; dazu gehört auch die Einordnung der dynamischen IP-Adresse in die einschlägigen Datenkategorien.

Danach muss geprüft werden, wann und inwieweit dieser Schutz durchbrochen werden kann. Die Interessen der Allgemeinheit, der Access Provider und bestimmter Dritter müssen im Lichte des deutschen und europäischen Rechts gegen die durch die Schutzvorschriften geschützten Interessen der Kunden abgewogen werden. Die rechtliche Systematik gebietet hierbei eine sequentielle Betrachtung der verschiedenen denkbaren Erlaubnistatbestände; diese soll jedoch nicht auf die in der Rechtsprechung entschiedenen

---

<sup>20</sup> So *Dix*, DuD 2003, 234 [235].

<sup>21</sup> So auch *Ulmer/Schrief*, Datenschutz im neuen Telekommunikationsrecht, RDV 2004, 3 [6].

<sup>22</sup> So auch *Ohlenburg*, MMR 2004, 431 [431].

Aspekte beschränkt, sondern um neue technische und rechtliche Aspekte erweitert werden.

Bei der Frage, ob eine Speicherung der dynamisch vergebenen IP-Adresse mit Kundenzuordnung zulässig ist, sind zwei grundlegend verschiedene Arten der Speicherung zu unterscheiden: Bei der anlassbezogenen Speicherung werden die an einen vorher *bestimmten* Kunden vergebenen IP-Adressen gespeichert, während bei der Vorratsspeicherung *alle* Zuordnungen von IP-Adressen gespeichert werden. Ohne den Ausführungen im Einzelnen vorgreifen zu wollen, ist evident, dass die anlassbezogene Speicherung von Daten eines bestimmten Kunden im Rahmen der allgemeinen Verhältnismäßigkeit weit weniger problematisch erscheint als die Speicherung der Daten aller Kunden auf Vorrat; daher werden Schwerpunkte vor allem hinsichtlich der Vorratsspeicherung gesetzt und für die individuelle Speicherung nur dort, wo es besondere Spannungsverhältnisse gibt.

Am 24.02.2007 ist das TKG-Änderungsgesetz<sup>23</sup> in Kraft getreten, am 1.03.2007 das Telemediengesetz.<sup>24</sup> Da die Änderungen im Hinblick auf verschiedene Teilaspekte der Fragestellung bisher weitgehend ungeklärt sind, wird auch insoweit auf die Änderungen ausführlich einzugehen sein.

---

<sup>23</sup> Gesetz zur Änderung telekommunikationsrechtlicher Vorschriften vom 18. Februar 2007, BGBl. I S. 106.

<sup>24</sup> Art. 1 des Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste vom 26. Februar 2007, BGBl. I S. 179; zum Inkrafttreten vgl. die Bekanntmachung des *Bundesministeriums für Wirtschaft und Technologie*, BGBl. I S. 251.

## E. Anstehende Umsetzungen

Für Deutschland stehen zwei Umsetzungen von Völker- resp. Europarecht an, die die Verwendung von Verkehrsdaten betreffen, nämlich die Cybercrime Konvention des Europarates und die Data Retention Richtlinie der EG.

### I. Umsetzung der Cybercrime Konvention

#### 1. Gegenstand der Konvention

Das Übereinkommen über Computerkriminalität des Europarates<sup>263</sup> vom 23.11.2001 (*Cybercrime Konvention*) war der erste multilaterale Vertrag über die Bekämpfung von Computerkriminalität.<sup>264</sup> Die Cybercrime Konvention setzt einen internationalen Rahmen für die Staaten zur Bekämpfung von Computerkriminalität sowohl im materiellen Strafrecht als auch im Strafprozessrecht.<sup>265</sup> Das Übereinkommen betrifft nur die Kommunikation mittels Computersystemen. Ausführliche und umfangreiche Erläuterungen zur Cybercrime Konvention finden sich im *Explanatory Report*<sup>266</sup> des Europarates.

#### a) Strafprozessuale Maßnahmen

Die Konvention sieht unter anderem die Erhebung und Verwendung von Verkehrsdaten für strafprozessuale Zwecke vor:

Gemäß Art. 16 müssen die Vertragsstaaten Maßnahmen treffen, um die umgehende Sicherung von Computerdaten – einschließlich Verkehrsdaten – zu ermöglichen, um die Daten vor einer Löschung zu bewahren. Diese Verpflichtung gilt auch, wenn Diensteanbieter mehrerer Staaten beteiligt sind; dann müssen die Daten auch weitergegeben werden (Art. 17). Die Vorschriften beziehen sich allerdings nur auf bereits erhobene und gespei-

---

<sup>263</sup> Konventionen des Europarates können internationales Binnenmarktrecht bilden, siehe oben C I 4.

<sup>264</sup> *Pocar*, European Journal on Criminal Policy and Research 2004, 27 [30].

<sup>265</sup> Ebendort.

<sup>266</sup> *Vertragsbüro des Europarates*,  
<http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

cherte Daten; Verpflichtungen zur Vorratsspeicherung ergeben sich daraus nicht.<sup>267</sup>

Art. 18 sieht Auskunftsanordnungen durch Behörden über Bestandsdaten vor. Ob dies Bestandsdaten umfasst, die nur unter der Verwendung von Verkehrsdaten ermittelt werden können, bleibt offen.<sup>268</sup> Die Auskunftspflichteten sollen dadurch jedenfalls nicht zur Speicherung verpflichtet werden.<sup>269</sup>

Die Vertragsstaaten müssen gemäß Art. 20 Abs. 1 die erforderlichen Maßnahmen zu treffen, um Verkehrsdaten in Echtzeit zu erheben und aufzuzeichnen; ihnen bleibt die Wahl, ob sie zur technischen Umsetzung die Diensteanbieter zur Erhebung und Speicherung verpflichten oder dazu, die Erhebung und Speicherung durch die zuständigen Behörden zu ermöglichen. Die Erhebung und Speicherung soll jedoch nicht vorratsweise, sondern jeweils auf bestimmte strafrechtliche Ermittlungen und Verfahren gerichtet sein.<sup>270</sup>

### **b) Materieller Anwendungsbereich**

Die Maßnahmen sind verpflichtend anzuwenden in Bezug auf alle mit Computern begangenen Straftaten nach nationalem materiellem Strafrecht (Art. 14 Abs. 2 lit. b), wobei sich die Vertragsstaaten zur Sanktionierung mehrerer Tatbestände durch ihr nationales materielles Strafrecht verpflichten, darunter verschiedene Formen von Computersabotage und -betrug sowie Urheberrechtsverletzungen (in „gewerblichem Ausmaß“), Kinderpornografie (Artt. 2 bis 10) und Rechtsradikalismus (Zusatzprotokoll<sup>271</sup>). Die Staaten, die Verkehrsdaten wie Kommunikationsinhalte schützen, können sich die Anwendung der Echtzeiterfassung auf bestimmte Katalogstraftaten vorbehalten; ebenso ist grundsätzlich eine Beschränkung

---

<sup>267</sup> *Explanatory Report*, Abs. 150, mit ausdrücklichem Hinweis auf Flatrates.

<sup>268</sup> Zu dem Streit siehe oben C IV 2.

<sup>269</sup> *Explanatory Report*, Abs. 181.

<sup>270</sup> Ebendort, Abs. 216.

<sup>271</sup> Zusatzprotokoll zum Abkommen über Computerkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art vom 28.01.2003.

auf öffentliche TK-Netze möglich (Art. 14 Abs. 3).<sup>272</sup> Die individuelle Anwendung der Maßnahmen steht auch unter ausdrücklichem Vorbehalt der Menschenrechte und Grundfreiheiten des nationalen Rechts und der EMRK sowie der Verhältnismäßigkeit (Art. 15).<sup>273</sup>

## 2. Umsetzung der Konvention

### a) Ratifikationsstand unter den Mitgliedsstaaten der EU

Die Konvention wurde (u.a.) von sämtlichen Mitgliedsstaaten der EU unterzeichnet, jedoch bisher nur von Bulgarien, Dänemark, Estland, Frankreich, Litauen, den Niederlanden, Rumänien, Slowenien, Ungarn und Zypern ratifiziert.<sup>274</sup>

### b) Umsetzung in Deutschland

Den materiellen Umsetzungsbedarf will die Bundesregierung durch das von ihr eingebrachte *Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität*<sup>275</sup> erfüllen; die prozessrechtliche Umsetzung soll gemeinsam mit der Umsetzung der Data Retention Richtlinie (dazu sogleich) erfolgen und zeitgleich mit der Umsetzung der prozessrechtlichen Vorgaben soll die Ratifikation erfolgen.<sup>276</sup>

#### aa) Umgehende Sicherung

Die Umsetzung der Artt. 16f. müsste es ermöglichen, die Access Provider durch behördliche Anordnung zu verpflichten, auf die automatische Löschung bestimmter IP-Adresszuordnungen zu verzichten. Dies würde vom Access Provider einen aktiven Eingriff in seine Datenverarbeitung erfordern,<sup>277</sup> und müsste, um nicht völlig leerzulaufen, für diesen die Speicherung und Nicht-Löschung der zugeordneten IP-Adresse rechtfertigen.

---

<sup>272</sup> *Explanatory Report* Abs. 143f..

<sup>273</sup> Ebendort, Abs. 145f.

<sup>274</sup> *Vertragsbüro des Europarates*,

<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=GER>,  
Stand 08.03.2007; Nicht-EU-Mitgliedsstaaten unberücksichtigt.

<sup>275</sup> BT-Drs. 16/3656.

<sup>276</sup> Dies hat das *Bundesministerium der Justiz* d. Verf. am 9.03.2007 mitgeteilt.

<sup>277</sup> *Gercke*, MMR 2004, 801 [802].

### ***bb) Herausgabeanordnung***

In Bezug auf Access Provider und von diesen zu beauskunftende Bestandsdaten stellt Art. 18 an das deutsche Recht keine Anforderungen, die nicht im Grunde bereits durch § 113 TKG erfüllt würden.<sup>278</sup> Nach Art. 18 muss der Access Provider Auskunft über die Daten erteilen, die sich in seinem Besitz oder unter seiner Kontrolle befinden, während § 133 TKG auf die von ihm erhobenen Daten abstellt; diese Unterscheidung dürfte aber im Hinblick auf die Fragestellung wenig praxisrelevant sein.

### ***cc) Verkehrsdatenerfassung in Echtzeit***

Eine Erfassung der Verkehrsdaten in Echtzeit, wie sie Art. 20 vorsieht, ist durch § 100a StPO im Rahmen der TK-Überwachung bereits vorgesehen.<sup>279</sup> Die Erfassung erfolgt dabei nach gemäß der TKÜV durch die zuständige Behörde und muss vom Access Provider „nur“ ermöglicht werden. § 100g StPO trägt eine Verkehrsdatenerfassung in Echtzeit nicht:<sup>280</sup> Aus der Pflicht zur unverzüglichen Beauskunftung zukünftiger Verkehrsdaten eine Pflicht zur vollautomatischen Beauskunftung in Echtzeit zu machen, wäre eine Umgehung der strengeren Vorschriften für die TK-Überwachung; eine Erfassung in Echtzeit stellt schon begrifflich eine Überwachung dar und nicht bloß eine Auskunft. Für die Umsetzung von Art. 20, sofern sie überhaupt gesondert erfolgt, gilt hinsichtlich der Speicherung der IP-Adressen nichts anderes als für die bestehende TK-Überwachung.<sup>281</sup>

## **II. Umsetzung der Data Retention Richtlinie**

### ***1. Gegenstand der Richtlinie***

Die Data Retention Richtlinie<sup>282</sup> der EG verpflichtet die EU-Mitgliedsstaaten, in ihrem jeweiligen nationalen Recht die Speicherung von

---

<sup>278</sup> Zu dem Streit, ob Namen „hinter“ dynamischen IP-Adressen auf Grundlage des § 113 TKG beauskunftet werden dürfen und müssen, oben C IV 2.

<sup>279</sup> Siehe oben D VII 2 c.

<sup>280</sup> A.A. *Gercke*, a.a.O. [806].

<sup>281</sup> Siehe oben D VIII.

<sup>282</sup> Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt  
(Fortsetzung auf nächster Seite)

Verkehrsdaten „auf Vorrat“, also ohne vorher individuell bestimmten Zweck, anzuordnen. Adressaten des nationalen Rechts sollen die Anbieter öffentlich zugänglicher Kommunikationsdienste und Betreiber öffentlicher Kommunikationsnetze sein; darunter fallen auch Access Provider.

Zu den zu speichernden Verkehrsdaten gehören insbesondere *„der Name und die Anschrift des Teilnehmers bzw. registrierten Benutzers, dem eine IP-Adresse, Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war“* (Art. 5 Abs. 1 lit. a Nr. 2 Ziffer iii) sowie *„Datum und Uhrzeit der An- und Abmeldung beim Internetzugangsdienst [...] zusammen mit der vom Internetzugangsanbieter einer Verbindung zugewiesenen dynamischen oder statischen IP-Adresse und die Benutzerkennung des Teilnehmers oder des registrierten Benutzers“* (lit. c Nr. 2 Ziffer i). Insoweit wird der von der DSRL eK errichtete Grundsatz der Löschung von Verkehrsdaten nach Verbindungsende völlig aufgegeben.<sup>283</sup>

Die Speicherfrist wird durch die Richtlinie auf einen Korridor zwischen sechs und 24 Monaten festgelegt (Art. 6). Die Richtlinie regelt ausschließlich die Speicherung der Daten und nicht ihre Verwendung; dies bleibt den Mitgliedstaaten vorbehalten (Art. 4).

## 2. Umsetzung der Richtlinie

Die Umsetzungsfrist für den für die Speicherung von IP-Adressen einschlägigen Bereich des Internetzugangs endet für Deutschland am 15. März 2009.<sup>284</sup>

Die Bundesregierung hat einen Referentenentwurf für die Umsetzung erstellt.<sup>285</sup> Gemäß § 110a Abs. 1 und 4 TKG<sup>RefE</sup> sollen die Access Provider

---

oder verarbeitet werden und zur Änderung der Richtlinie 2002/58/EG, ABl. L 105 vom 13.04.2006, S. 54-60.

<sup>283</sup> Stellungnahme des Europäischen Datenschutzbeauftragten, ABl. C 298 vom 29.11.2005, S. 1-12 [3].

<sup>284</sup> Art. 15 Abs. 3 Data Retention Richtlinie i.V.m. der Erklärung Deutschlands, ABl. L 105 vom 13.04.2006, S. 63.

<sup>285</sup> Bundesministerium der Justiz, Referentenentwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 8.11.2006, [http://www.humanistische-union.de/fileadmin/hu\\_upload/doku/vorratsdaten/de-](http://www.humanistische-union.de/fileadmin/hu_upload/doku/vorratsdaten/de-)

Verkehrsdaten für die Dauer von sechs Monaten speichern, nämlich die dem Teilnehmer für eine Verbindung zugewiesene IP-Adresse, eine eindeutige Anschlusskennung sowie den Zeitpunkt von Beginn und Ende der Verbindung. Nach Ablauf der Speicherfrist sollen nicht benötigte Daten binnen eines weiteren Monats gelöscht werden (§ 110b Abs. 2 TKG<sup>RefE</sup>).

### **3. Formelle und materielle Bedenken**

Gegen die Data Retention Richtlinie bestehen formelle und materielle Bedenken:

#### **a) Formelle Bedenken**

Die Richtlinie stützt sich formell auf Art. 95 EG. Dieser ist eine Generalkompetenz für die Rechtsangleichung zum Zweck der Funktionsfähigkeit des Binnenmarktes.<sup>286</sup> Er dient der Angleichung von nationalen Rechtsvorschriften, die durch ihre Unterschiedlichkeit die Verwirklichung der Marktfreiheiten behindern.<sup>287</sup>

Nach Auffassung des Richtliniengebers beeinträchtigen die rechtlichen und technischen Unterschiede für die Vorratsdatenspeicherung im Strafprozessrecht den Binnenmarkt für elektronische Kommunikation (Erwägungsgrund 6).

Irland hat vor dem EuGH auf Nichtigkeit der Richtlinie geklagt.<sup>288</sup> Ziel der Richtlinie sei nicht das Funktionieren des Binnenmarktes, sondern die Erleichterung der Strafverfolgung; die Richtlinie werde daher nicht von der Kompetenz aus Art. 95 EG und auch von keiner anderen Kompetenz des EG-Vertrages getragen. Allenfalls könne ein einstimmiger Rahmenbeschluss gemäß Artt. 31, 34 EU in Betracht kommen.<sup>289</sup>

---

[recht/bmj\\_2006.11.pdf](#) (das Ministerium selbst hat den Referentenentwurf nicht veröffentlicht).

<sup>286</sup> Callies/Ruffert-Kahl, Art. 95 EG Rn. 5.

<sup>287</sup> Ebendort, Rn. 13.

<sup>288</sup> EuGH Rechtssache C-301/06, ABl. C 237 vom 30.09.2006, S. 5.

<sup>289</sup> Tatsächlich gab es einen der Richtlinie ähnlichen Rahmenbeschlussentwurf (Ratsdokument 8958/04), der jedoch im November 2004 fallengelassen wurde, vgl. *Leutheusser-Schnarrenberger*, ZRP 2007, 9 [9].

Dem wird entgegengehalten, dass der EG zwar die Kompetenz für das Strafprozessrecht fehlt, dass sie aber insoweit strafprozessuale Richtlinien erlassen könne, wie diese nicht nur zum Abbau von Hürden auf dem Binnenmarkt erforderlich sind, sondern auch an binnenmarktrelevante und gemeinschaftsrechtlich geregelte Tätigkeiten – hier das Erbringen von TK-Diensten – anknüpfen.<sup>290</sup> Außerdem gehöre der TK-Datenschutz durch die DSRLeK zum gemeinschaftlichen Besitzstand, der nur durch gemeinschaftsrecht angetastet werden dürfe.<sup>291</sup>

### **b) Materielle Bedenken**

Neben den formellen gibt es auch erhebliche materielle Bedenken gegen die Richtlinie und ihre Umsetzung, wobei die Einwände nach deutschem Verfassungsrecht parallel zu denen auf europäischer Ebene nach der EMRK und den Unionsgrundrechten verlaufen.<sup>292</sup>

Bereits die Speicherung von Verkehrsdaten über mit ihr unmittelbar verbundenen Zwecke hinaus stellt einerseits einen Eingriff in das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG dar,<sup>293</sup> andererseits aber auch in die Berufsausübungsfreiheit der Access Provider.

Zweifelhaft ist, ob dieser Eingriff gerechtfertigt ist; dafür müsste er sich bei einer Güterabwägung als verhältnismäßig erweisen. Von dem Eingriff ins Fernmeldegeheimnis durch die Richtlinienumsetzung sind alle Personen betroffen, die Teilnehmer oder Nutzer in TK-Netzen sind – also praktisch jedermann. In die Grundrechte der allermeisten Betroffenen wird dabei eingegriffen, ohne dass diese durch ihr Verhalten einen Verdacht begründet hätten.<sup>294</sup> Dem gegenüber steht die eventuell vereinfachte Aufklärung von Straftaten, die ganz überwiegend nur wirtschaftliche Interessen einzelner

---

<sup>290</sup> In Anlehnung an *EuGH* EuZW 2005, 632 [634f. Abs. 52], der der Gemeinschaft die Kompetenz für das Umweltstrafrecht zur Bewehrung der EG-Umweltvorschriften zugesprochen hat.

<sup>291</sup> Stellungnahme des Rechtsausschusses des Europäischen Parlaments, Plenarsitzungsdokument A6-0174/2006, S. 11-13; a.A. 130 Mitglieder des Deutschen Bundestages, BT-Drs. 16/1622, S. 5.

<sup>292</sup> *Leutheusser-Schnarrenberger*, a.a.O. [11].

<sup>293</sup> *BVerfGE* 85, 386 [398].

<sup>294</sup> *Leutheusser-Schnarrenberger*, a.a.O. [11].

berühren; über das Internet begangene oder geplante Kriminalität stellt keine Massenbedrohung dar.<sup>295</sup>

### c) Stellungnahme

Die formellen Einwände gegen die Richtlinie sind überzeugend. Es ist nicht erkennbar, dass unterschiedliche Vorschriften zur Vorratsdatenspeicherung den Binnenmarkt behindern: Die Bundesregierung geht von nur marginalen zusätzlichen Kosten für die TK-Diensteanbieter durch die Vorratsspeicherung aus,<sup>296</sup> die nicht geeignet sind, Verzerrungen auf dem Binnenmarkt auszulösen, wenn sie nur in einigen Mitgliedsstaaten anfielen und in anderen nicht. Überhaupt ist bereits der Harmonisierungsgrad der Richtlinie gering: Neben dem weiten Speicherfristkorridor von sechs bis 24 Monaten erlaubt Art. 12 den Mitgliedsstaaten, noch längere Fristen durch ihr nationales Recht anzuordnen.

Im übrigen hätte es im Sinne des Subsidiaritätsprinzips genügt, allenfalls festzulegen, welchen Bestimmungen TK-Unternehmen unterliegen, die ihre Dienste in einem anderen Mitgliedsstaat anbieten und nach welchem Recht bei innergemeinschaftlichen TK-Verbindungen zu verfahren ist.

Der Unterschied zu der EuGH-Rechtsprechung zum Umweltstrafrecht besteht darin, dass mit der Data Retention Richtlinie keineswegs Verstöße gegen gemeinschaftsrechtliche Vorschriften bewehrt werden sollen, sondern Rechtsverstöße, die außerhalb des gemeinschaftsrechtlich harmonisierten und harmonisierbaren Rechts liegen.<sup>297</sup> Allein die Ermöglichung der strafprozessualen Verfolgung knüpft an das harmonisierende Gemeinschaftsrecht an; dies genügt aber für eine Kompetenz aus Art. 95 EG nicht.<sup>298</sup>

---

<sup>295</sup> P. Breyer, *European Law Journal* 2005, 365 [369].

<sup>296</sup> RefE (Fn. 285), S. 7.

<sup>297</sup> Die deutliche Mehrzahl „schwerer Fälle wie organisierte Kriminalität und Terrorismus“ (Erwägungsgrund 9) liegt außerhalb national strafbewehrten Gemeinschaftsrechts.

<sup>298</sup> So auch *Westphal*, *EuZW* 2006, 555 [557] m.w.N.

Die Beurteilung der materiellen Verhältnismäßigkeit hängt wesentlich von der Frage ab, wie geeignet und erforderlich die Vorratsspeicherung von Verkehrsdaten ist. Wenn schwerste Straftaten, die durch wenige Personen begangen werden, tatsächlich nur ermittelt und aufgeklärt werden könnten, indem die Verkehrsdaten praktisch aller Bürger gespeichert werden, spräche viel für eine Vereinbarkeit der Richtlinie und ihrer Umsetzung mit den europäischen und deutschen Grundrechten. Allerdings haben zahlreiche Fahndungserfolge gezeigt, dass die Aufklärung von Straftaten im Internet auch mit den bestehenden rechtlichen und technischen Instrumenten möglich ist; in Irland soll die Vorratsspeicherung nach empirischen Erkenntnissen hingegen nicht zu einer signifikant höheren Aufklärungsquote geführt haben.<sup>299</sup> Danach sprechen, auch bei Berücksichtigung der Einschätzungsprärogative des Richtliniengebers, die besseren Gründe für die Annahme, dass die Richtlinie und ihre geplante Umsetzung materiell grundrechtswidrig sind.

---

<sup>299</sup> *Heise Online*, Schwere Bedenken gegen Neufassung der TK-Überwachung, 22.01.2007, <http://www.heise.de/newsticker/meldung/84033>; zu dem Umgehungsmöglichkeiten für Kriminelle *Vassilaki*, MMR 2/2006, XIII; für das Vereinigte Königreich vgl. Stellungnahme des *Europäischen Datenschutzbeauftragten*, ABl. C 298 vom 29.11.2005, S. 1-12 [3].

## F. Resümee

Die Vorratsspeicherung von dynamischen IP-Adresszuordnungen ist *de lege lata* unzulässig, sieht man von einer ganz kurzfristigen Speicherung zum Zweck der Missbrauchskontrolle und bis zur Auswahl noch für anlassbezogene Verwendung benötigter Datensätze ab.

Unverständlich ist daher die Praxis der Access Provider, die Daten für bis zu zwei Wochen auf Vorrat zu speichern; ebenso unverständlich ist die Billigung dieser Praxis durch die zuständige Aufsichtsbehörde, den *BfDI*, im Einvernehmen mit der *Bundesnetzagentur*, zumal das *LG Darmstadt* in seinem Urteil keineswegs erkennen lässt, dass es eine Speicherfrist in dieser Größenordnung für zulässig hält. Zwar ist die vom LG postulierte Löschung „*unmittelbar nach dem Ende der jeweiligen Verbindung*“<sup>300</sup> nicht in jedem Fall durchführbar, aber angesichts der verhältnismäßig einfachen und kostengünstigen Möglichkeiten, die Daten vollautomatisch zu verarbeiten und auch im Fall des Resale (wenigstens fast) in Echtzeit zu übermitteln und auszuwerten, sind ein bis zwei Wochen weit entfernt von dem, was als angemessen, zumutbar und „unverzüglich“ gelten kann.

Die Unzulässigkeit der Speicherung wirft, auch angesichts der lockeren Auskunftspraxis der Access Provider,<sup>301</sup> die Frage auf, was die erlangten Daten eigentlich wert sind für die anfragenden Verwertungsgesellschaften und Staatsanwaltschaften. Die Rechtsprechung<sup>302</sup> hat die prozessuale Verwertbarkeit von Informationen, die unter Verletzung des Fernmeldegeheimnisses oder des Allgemeinen Persönlichkeitsrechts erlangt wurden, ausgeschlossen; dies sollte nicht anders auch für IP-Adressen gelten, von

---

<sup>300</sup> *LG Darmstadt*, a.a.O. [371].

<sup>301</sup> *Mühlbauer*, Wer die Verbindungsdaten speichert (und das Gegenteil behauptet), *Telepolis* 24.01.2007.

<sup>302</sup> Zuletzt die „Vaterschaftstest-Entscheidungen“ *BVerfG* 1 BvR 421/05 vom 13.02.2007 ([http://www.bverfg.de/entscheidungen/rs20070213\\_1bvr042105.html](http://www.bverfg.de/entscheidungen/rs20070213_1bvr042105.html)) Rn. 92ff.; *BGH NJW* 2005, 497 [498f.] hinsichtlich der informationellen Selbstbestimmung; für das Fernmeldegeheimnis *OLG Stuttgart MMR* 2002, 746 [750]; *BFH NJW* 2001, 2118 [2119]; für das Recht am gesprochenen Wort in der Telekommunikation *BVerfG* E 106, 28 [44ff.].

deren Zuordnung nur Kenntnis erlangt werden konnte, weil diese unter Verstoß gegen den TK-Datenschutz (noch) gespeichert war.

Der Umgang mit der Zuordnung dynamischer IP-Adressen ist nicht zuletzt deswegen problematisch, weil das Telekommunikationsrecht, einschließlich seines besonderen Datenschutzrechts, noch immer sehr auf die klassische Telefonie zugeschnitten ist. Die technische Entwicklung der Telekommunikation auch im Recht nachzuvollziehen, ist dem Gesetzgeber trotz zahlreicher Novellierungen immer noch nicht gelungen, mit der Konsequenz, dass ein technisch trivialer, nicht besonders neuer und tagtäglich millionenfach auftretender Vorgang – die Zuordnung einer dynamischen IP-Adresse – in seiner rechtlichen Beurteilung noch immer Probleme bereitet.

Dabei stehen die nächsten Probleme in diesem Bereich bereits vor der Tür: Das neue Internetprotokoll IPv6 sieht vor, dass dynamische IP-Adressen nicht mehr vom Access Provider zugeteilt, sondern vom anwählenden Rechner sich selbst zugewiesen werden.<sup>303</sup> Die rechtliche Bewertung dieses Vorgangs dürfte weitere Fragestellungen aufwerfen.

Der europäische und der deutsche Gesetzgeber sind daher aufgefordert, dem technischen Konvergenzprozess der Medien (nicht nur) im Bereich der Telekommunikation auch rechtlich zu entsprechen und dabei den Datenschutz und das Fernmeldegeheimnis nicht aufzuweichen: Urheberrechtliche Vergehen im Bagatellbereich rechtfertigen dies nicht und für die Bekämpfung schwererer Kriminalität stehen ausreichend anlassbezogene Maßnahmen zur Verfügung.

---

<sup>303</sup> *Wikipedia*: IPv6, <http://de.wikipedia.org/wiki/IPv6#Autokonfiguration>.