Schleswig-Holsteinischer Landtag
Umdruck 18/1146

HANS-BREDOW-INSTITUT
für Medienforschung an der Universität Hamburg

Bundesratsinitiative zur Stärkung der Freiheit und der Privatsphäre im Internet

Drucksache 18/195

Stellungnahme des Hans-Bredow-Instituts für den Innen- und Rechtsausschuss des Landtags Schleswig-Holstein

Hamburg, 26. April 2013

Inhalt

0 Allgemeines

Das Hans-Bredow-Institut wurde von dem Innen- und Rechtsausschuss des Landtags Schleswig-Holstein gebeten, zu der o.b. Beschlussvorlage umfassend Stellung zu nehmen. Angesichts der zahlreichen rechtlichen Grundsatzfragen, die von den Einzelpunkten berührt sind, konnte das Institut eine umfassende, alle rechtlichen Aspekte klärende Begutachtung im Rahmen einer einfachen Stellungnahme nicht übernehmen. Die folgenden Ausführungen beziehen sich nach einer erneuten, inhaltlich begrenzteren Bitte um Stellungnahme ausschließlich auf europarechtliche Aspekte der in der Drucksache aufgestellten Forderungen und Vorschläge (s. Umdruck 18/706).

Das Hans-Bredow-Institut bedankt sich für die Gelegenheit zur Stellungnahme. Der Gesetzgeber ist dabei aber nicht nur auf verfassungsrechtlicher Ebene in seiner Einschätzungsprärogative durch Übermaß- und in Fällen objektiv-rechtlicher Schutzpflichten durch Untermaßverbot eingeschränkt, er muss auch die europarechtlichen Vorgaben des Primär- und Sekundärrechts beachten. Dies führt bei den hier in Frage stehenden Forderungen jeweils zu der Frage, inwieweit sich die Umsetzung der Forderungen (noch) an EU-Recht orientieren, wo sie diese Vorgaben überragen und ein (ein grundsätzlich zulässiges) strengeres nationales Rechtsregime zur Folge haben und wo sie gegen die positiven EU-Vorgaben verstoßen.

1 Erstreckung der Haftungsbegrenzung des TMG auf Telekommunikationsdienste (z. b. offene Internetzugänge)

Die hier vorgetragene Forderung zielt auf eine Haftungsfreistellung von privaten Anbietern bei der Gestattung der Mitbenutzung ihres Internetzugangs durch Dritte ab: Anbieter öffentlicher WLAN-Internetzugänge sollen „für einen Missbrauch ihrer Dienste ebenso wenig verantwortlich gemacht werden können wie Anbieter öffentlicher Telefonzellen“ (Drs. 18/195, S. 3). Für die europarechtliche Einordnung dieses Vorschlag muss zunächst auf ein mögliches Missverständnis hingewiesen werden, das aus der Kombination der in Deutschland bestehenden gesetzlichen Anwendungsbereiche von TKG und TMG und der Anwendung der Grundsätze der Störerhaftung ergebenden Haftungsproblematik entstanden ist: Anbieter öffentlicher Telefonzellen haften für die übermittelten Inhalte schon deshalb nicht, weil das TMG in Gänze auf diese Dienste schlicht gar nicht anwendbar ist. Die in Telefonzellen angebotenen Leistungen sind reine Telekommunikationsdienste, auf die ausschließlich das TKG Anwendung findet. Damit scheidet auch die Anwendbarkeit des § 7 Abs. 1 TMG aus, der eine Verantwortlichkeit nach TMG überhaupt erst begründen würde.

Im Falle der Zurverfügungstellung eines Internetzugangs handelt es sich jedoch nicht ausschließlich um einen Telekommunikationsdienst, sondern auch um einen Telemediendienst

nach § 2 Abs. 1 Nr. 1 TMG, da der Diensteanbieter durch den Zugang („access providing“) immer auch den Zugang zu Telemedien vermittelt. Dass Zugangsanbieter dem Anwendungsbereich des TMG unterfallen sollen, ergibt sich ausdrücklich auch aus der Gesetzesbegründung. Damit wird das Access Providing sowohl vom Anwendungsbereich des TKG und des TMG umfasst. Das Anbieten von Internetzugängen untersteht somit einer Doppelregulierung. Eine Ausweitung der Haftungsprivilegien des TMG auf (reine) Telekommunikationsdienste erscheint angesichts dieser Sachlage nicht nur unnötig, sondern sogar kontraproduktiv, da durch eine explizite Haftungsprivilegierung eine grundsätzliche Haftungsmöglichkeit von TK-Diensteanbietern gerade erst geschaffen würde.

Dennoch ist die Forderung einer Haftungsfreistellung im Hinblick auf die Gestattung der Mitnutzung eines Internetanschlusses grundsätzlich nachvollziehbar: Geschuldet ist der Eindruck der Ungleichbehandlung der in der Spruchpraxis der Gerichte entwickelten Grundsätze der sogenannten Störerhaftung. Folge der beschriebenen Doppelregulierung des Angebots von Internet-Zugängen ist die grundsätzliche Anwendbarkeit der Haftungsprivilegien für technische Dienstleister, wie sie sich aus den § 8 bis 10 TMG ergeben. Für das Access Providing enthält § 8 Abs. 1 TMG die entsprechende Verantwortlichkeitsbegrenzung: Danach sind Diensteanbieter „für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie 1. die Übermittlung nicht veranlasst, 2. den Adressaten der übermittelten Informationen nicht ausgewählt und 3. die übermittelten Informationen nicht ausgewählt oder verändert haben.“ Diese Voraussetzungen sind bei der Überlassung eines Internet-Zugangs grundsätzlich gegeben, so dass von einer bestehenden Haftungsprivilegierung bei Access Providing in der Regel auszugehen ist.

Die in der deutschen Rechtsprechung entwickelte Störerhaftung erkennt diese Haftungsprivilegierung des § 8 Abs. 1 TMG, unterscheidet die (straf- und ordnungsrechtliche) Verantwortlichkeit des technischen Dienstleisters für Rechtsverletzungen aber von seiner zivilrechtlichen Haftung auf Unterlassen gegenüber dem Verletzten: „Als Störer kann bei der Verletzung absoluter Rechte auf Unterlassung in Anspruch genommen werden, wer — ohne Täter oder Teilnehmer zu sein — in irgendeiner Weise willentlich und adäquat kausal zur Verletzung des geschützten Rechts beiträgt (...). Da die Störerhaftung nicht über Gebühr auf Dritte erstreckt werden darf, die nicht selbst die rechtswidrige Beeinträchtigung vorgenommen haben, setzt die Haftung des Störers nach der Rechtsprechung des Senats die Verletzung von Prüfpflichten voraus. Deren Umfang bestimmt sich danach, ob und inwieweit dem als Störer in Anspruch Genommenen nach den Umständen eine Prüfung zuzumuten ist (...)“ (BGHZ 185, 330). Diese Prüfpflichten sehen die Gerichte bei privaten Anbietern von Internetzugängen vor allem im Hinblick auf die Sicherung des Netzwerks und dem (dadurch bedingten oder vertraglichen) Ausschluss von Rechtsverletzungen durch Dritte: „Der Betrieb eines nicht ausreichend gesicherten WLAN-Anschlusses ist adäquat kausal für Urheberrechtsverletzungen, die unbekannte Dritte unter Einsatz dieses Anschlusses begehen. (...) Es ist nicht gänzlich unwahrscheinlich, dass unberechtigte Dritte einen unzureichend gesicherten WLAN-Anschluss dazu benutzen, urheberrechtlich geschützte Musiktitel im Internet in Tauschbörsen einzustellen. Die Unterlassung ausreichender Sicherungsmaßnahmen beruht auch auf dem Willen des Anschlussinhabers“ (BGHZ 185, 330).

Auf der Grundlage dieser Störerhaftungs-Rechtsprechung zu unzureichend gesicherten W-Lan-Netzen ist somit davon auszugehen, dass private Anbieter offener Internetzugänge für die Rechtsverletzungen Dritter, die über den Anschluss begangen werden, zumindest auf Unterlassung haften. In Kombination mit der Praxis vorgerichtlicher Abmahnungen und den entsprechenden Kostenersatzansprüchen des Abmahnenden ergibt sich somit ein erhebliches finanzielles Risiko für die Anbieter offener Internetzugänge. Die geforderte Erstreckung der Haftungsprivilegien des § 8 Abs. 1 TMG auch auf TK-Dienste würde angesichts dieser Rechtsprechung nicht zweckdienlich sein, da die Haftungsbegrenzung hier wohl gerade nicht für zivilrechtliche Unterlassungsansprüche zum Tragen käme. Der Grund für den Ausschluss der Haftung kommerzieller Zugangsanbieter, die selbstverständlich auch dem TMG unterfallen, ergibt sich entsprechend ebenfalls gerade nicht aus § 8 Abs. 1 TMG, sondern aus der in sich schlüssigen Begrenzung der Störerhaftung in diesen Fällen: Die dem Zugangsanbieter auferlegten Prüfpflichten finden dort ihre Grenze, wo diese dem Anbieter nicht mehr zumutbar sind. Dem Zugangsanbieter auf der Grundlage der bestehenden Spruchpraxis umfassende Prüfpflichten aufzubürden, hätte vielmehr „eine Überdehnung der Grundsätze der Störerhaftung zur Folge, die nach den Grundsätzen der Rechtsprechung des BGH in Bezug auf Dritte gerade nicht gerechtfertigt ist“ (LG Köln, MMR 2011, 833).

Diese kurze Einordnung der aufgestellten Forderung hat zweierlei gezeigt: Zum einen erscheint eine Erstreckung der Haftungsprivilegien des TMG auch auf (reine) Telekommunikationsdienste weder notwendig, noch hilfreich – ja sogar kontraproduktiv. Andererseits ist deutlich geworden, dass eine Klarstellung der Haftung oder Haftungsbegrenzung von privat angebotenen Internetzugängen medienpolitisch grundsätzlich nachvollziehbar erscheint. Letztere müsste dann aber in einer anderen Form erfolgen als vorgeschlagen, also etwa in Form eines ausdrücklichen Haftungsausschlusses der privat angebotenen Mitnutzung eines Internetzugangs, auch und vor allem im Hinblick auf Unterlassungsansprüche; eine bloße Erstreckung der bestehenden Haftungsprivilegierung des § 8 Abs. 1 TMG auf entsprechende Anbieter reicht angesichts der Unklarheiten bei der Reichweite der dort vorgesehenen Privilegierung gerade nicht aus. Ein entsprechender Vorschlag findet sich etwa in einem von der Digitalen Gesellschaft e.V. entwickelten Gesetzesvorschlag in BT-Drs. 17/11137, S. 4.

Interpretiert man die hier in Nr. 1 aufgestellte Forderung also in diesem Sinne als Forderung nach einem vollständigen, auch zivilrechtlichen Haftungsausschluss privater Internet-Zugangsanbieter, so trifft dies an zwei Stellen auf europarechtliche Zulässigkeitsfragen.

1.1 Anwendbarkeit der Vorgaben der E-Commerce-Richtlinie auf private Anbieter

Zum Einen ließe sich anführen, dass die für den Anwendungsbereich der E-Commerce-Richtlinie ausschlaggebenden „Dienste der Informationsgesellschaft“ ausschließlich solche sind, die kommerziell erbracht werden. Die beschriebenen Haftungsprivilegierungen des TMG, die ihre europarechtliche Grundlage in den Art. 12 bis 14 der E-Commerce-Richtlinie haben, wären dann europarechtskonform nicht auf privat erbrachte Telemediendienste anwendbar. Eine ausdrückliche Erstreckung der Haftungsbegrenzung auch auf private Anbieter würde damit

deutsche Anbieter haftungsrechtlich besser stellen, und gleichzeitig die Durchsetzung von Rechtsverletzungen in diesen Konstellationen erheblich erschweren bzw. unmöglich machen.

Die Gewerbelastigkeit des Begriffs des „Dienstes der Informationsgesellschaft“ ergibt sich zum Einen aus dem Wortlaut, wonach eine „Dienstleistung der Informationsgesellschaft (...) jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung“ ist (s. Art. 2 Buchstabe a) E-Commrece-Richtlinie i.V.m. Art. 2 Nr. 1 der Richtlinie 98/34/EG). Zum anderen ist der jedenfalls wirtschaftslastige Begriff dem binnenmarktdienlichen Zweck der Richtlinien geschuldet – es ging der EU gerade um die Herstellung eines „level playing fields“ für mitgliedstaatliche Wirtschaftsdienstleister. Die regelmäßige Entgeltlichkeit – wobei es sich nicht um ein Austauschverhältnis von Leistungen zwischen Anbieter und Nutzer handeln muss – und der Begriff des „Dienstes“ an sich deuten insoweit auf eine mögliche Einschränkung auf gewerblich erbrachte Dienste hin. So könnte die Gestattung der Mitnutzung des eigenen Internet-Anschlusses gerade kein „Dienst“ sein, der von einem Anbieter gegenüber einem Dritten erbracht wird, da dem privat handelnden Mitbürger die Nachhaltigkeit, wirtschaftliche Zweckorientierung und das dem Dienstbegriff innewohnende Mindestmaß an interner Organisation und Professionalität fehlt. Oder kurz: Es ist ein Gefallen, eine nette mitmenschliche Geste – kein „Dienst“. Folgte man dieser Sichtweise, wäre das private Angebot gerade nicht von dem Anwendungsbereich der E-Commrce-Richlinie erfasst. Die haftungsrechtliche Gleichstellung von Privatpersonen, die Internetzugänge zur öffentlichen Nutzung zur Verfügung stellen, und gewerblichen Diensteanbietern wäre damit nicht von der Richtlinie geregelt – stünde also einer entsprechenden Anwendungserweiterung der Haftungsprivilegien im deutschen Recht auch nicht entgegen, würde aber zu einem unterschiedlichen Begriffsverständnis des „Dienstes“ auf deutscher Ebene einer- und EU-Ebene andererseits führen.

Gegen dieses Verständnis spricht aber die Sichtweise, die im Umkehrschluss davon ausgeht, dass eine derartige Unterscheidung zwischen privaten und gewerblichen Zugangsvermittlungen anhand der grundlegenden Zielsetzung der Haftungsprivilegierungen gerade nicht davon abhängig gemacht werden kann, ob es sich bei dem Dienst um einen gewerblich erbrachten handelt: Ansonsten wäre ein gewerblicher Dienstleister, der einen Dienst aus wirtschaftlichen Interessen und regelmäßig mit Gewinnerzielungsabsicht verfolgt letztlich haftungsrechtlich besser gestellt als ein privater Anbieter, der gerade keine wirtschaftlichen Interessen mit der Diensteerbringung verfolgt, wobei beide Anbietertypen vergleichbare Kontroll- und Prüfmöglichkeiten haben. Für eine entsprechende Erstreckung des Anwendungsbereichs der E-Commerce-Richtlinie spricht auch ihr Erwägungsgrund 18 (Schmidt-Bens, CR 2012, 828, 831). Eine abschließende Klärung kann im Rahmen dieser Stellungnahme nicht erfolgen, eklatante Verstöße gegen EU-Recht sind auf den ersten Blick aber in der expliziten Anwendbarkeit der Haftungsprivilegien auch auf private Anbieter von Internet-Zugängen jedenfalls nicht zu erkennen.

1.2 Erweiterung der Privilegierung auch auf Unterlassungsansprüche

Eine Erweiterung der Privilegierungen des TMG auf einen Ausschluss von Unterlassungsansprüchen berührt daneben die Richtlinienvorgabe aus Art. 12 Abs. 3 E-Commerce-Richtlinie, der die Möglichkeit unberührt lässt, dass „ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern." Mit Rekurs auf Art. 12 Abs. 3 kann man der Ansicht sein, dass Unterlassungsansprüche durch die entsprechenden Umsetzungsvorschriften der Mitgliedsstaaten bei einer Eins-zu-Eins Umsetzung der Vorgaben der Richtlinie (für Deutschland: § 8 TMG) systematisch gerade nicht ausgeschlossen werden. Andererseits überlässt die E-Commerce-Richtlinie den Mitgliedstaaten bei der Umsetzung der Richtlinie an dieser Stelle ausdrücklich einen Spielraum. Es lässt die Möglichkeit „unberührt", geltend gemachte Unterlassungsansprüche gerichtlich oder behördlich durchzusetzen. Das wiederum schließt – jedenfalls auf Grundlage dieser konkreten Richtlinienvorgabe – nicht aus, dass einzelne Mitgliedstaaten den Haftungsausschluss auch auf Unterlassungsansprüche erstrecken. (vgl. Schmidt-Bens, CR 2012, 828, 832) Mit Blick auf die E-Commerce-Richtlinie allein spricht insoweit im ersten Zugriff nichts gegen eine gesetzgeberische Erweiterung der Privilegien auf eine auch Unterlassungsansprüche umfassende Haftungsfreistellung privater Zugangsanbieter. Inwieweit dagegen andere EU-Vorgaben einem entsprechenden Vorhaben entgegenstünden, kann im Rahmen der Stellungnahme nicht abschließend geklärt werden (s. etwa Art. 9 Abs. 1 Buchstabe a und Art. 11 der Enforcement-Richtlinie, wonach die Mitgliedstaaten sicherzustellen haben, dass die zuständigen Gerichte die Möglichkeit haben, auf Antrag des Antragstellers auch einstweilige Maßnahmen gegen eine Mittelsperson anzuordnen, deren Dienste von einem Dritten zwecks Verletzung eines Rechts des geistigen Eigentums in Anspruch genommen werden). Unbenommen bleibt daneben die Prüfung der Konsequenzen einer entsprechenden Haftungsfreistellung für die nationalrechtlichen Vollzugsmöglichkeiten und deren Effektivität bei der Geltendmachung und Durchsetzung von Ansprüchen aus Persönlichkeitsrechten, Datenschutzrechten und Urheberrechten im Falle von Rechtsverletzungen; hier treffen den Gesetzgeber ggf. grundrechtliche Vorgaben in Form objektiv-rechtlicher Gewährleistungsgehalte, die der nationale Gesetzgeber nicht unberücksichtigt lassen darf.

2 Verpflichtung zur Entfernung von Informationen nur bei vollstreckbarem Gerichtsurteil

Zunächst ist im Hinblick auf die Forderung in Nr. 2 der Drs. 18/195, dass Anbieter von Durchleitungs- oder Speicherdiensten erst bei Vorlage einer gerichtlichen Anordnung Löschungs- oder Sperrungspflichten treffen, anzumerken, dass eine etwaige Verantwortlichkeit ab Kenntnis für den Bereich von reinen Durchleitungsdiensten nicht existiert. Reine technische Infrastrukturdienstleister und Access Provider haften grundsätzlich nicht für die durchgeleiteten Inhalte (s. oben). Eine Klarstellung ist hier insoweit nicht erforderlich.

Für den Bereich der „Speicherdienste“ rekurriert die Forderung hier auf die Grundfrage, inwieweit ein national ausgestaltetes bzw. einfachgesetzlich konkretisiertes Notice-and-Takedown-Verfahren nach der Richtlinie möglich ist. Hier ist Art. 14 E-Commerce-Richtlinie einschlägig, der die Mitgliedstaaten dazu verpflichtet („stellen sicher“), dass Host Provider für die im Auftrag eines Nutzers gespeicherten Informationen nicht verantwortlich sind, sofern der „Anbieter (...) keine tatsächliche Kenntnis von der rechtswidrigen Tätigkeit oder Information (hat), und, in Bezug auf Schadenersatzansprüche, (...) er sich auch keiner Tatsachen oder Umstände bewusst (ist), aus denen die rechtswidrige Tätigkeit oder Information offensichtlich wird“. Hat er diese Kenntnis, so muss er allerdings unverzüglich tätig werden, um die Information zu entfernen oder den Zugang zu ihr zu sperren. Mit einer auf mitgliedstaatlicher Gesetzesebene etablierten Eingrenzung des Kenntnisbegriffs auf solche Fälle, in denen zunächst eine gerichtliche Anordnung vorliegen muss, würde insbesondere die Umsetzungspflicht im Hinblick auf offensichtlich rechtswidrige Fälle verletzt werden. Sie erscheint vor diesem Hintergrund jedenfalls für derartige Sachverhalte nicht europarechtskonform.

3 Begrenzung proaktiver Maßnahmen der Verhinderung zukünftiger Rechtsverletzungen

Der in Nr. 3 geforderte gesetzliche Ausschluss privatpolizeilicher Überwachungspflichten ist bereits europarechtlich normiert, wenn Artikel 15 E-Commerce-Richtlinie den Mitgliedstaaten verbietet, „Anbietern von Diensten im Sinne der Artikel 12, 13 und 14 keine allgemeine Verpflichtung“ aufzuerlegen, „die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen.“ Ihre Umsetzung findet diese Vorschrift in § 7 Abs. 2 S. 1 TMG. Eine ausdrückliche gesetzliche Regelung ist insoweit nicht notwendig, andererseits jedenfalls auch nicht gemeinschaftsrechtswidrig.

4 Erstreckung des Fernmeldegeheimnisses auf die Nutzung von Telemediendiensten

Unabhängig von den rechtswissenschaftlichen Diskussionen der Schutzbereiche des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG und des vom BVerfG geprägten Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sind im Hinblick auf Forderung Nr. 4 auf europäischer Ebene einerseits Art. 8 Abs. 1 der Europäischen Grundrechtecharta, den Deutschland zu beachten hat und der gleichlautende Art. 16 Abs. 1 AEUV einschlägig: „Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten“. Nach Art. 8 Abs. 2 der EU-Grundrechtecharta dürfen diese Daten nur „nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede

Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken“. Daneben spielen auch Art. 7 der EU-Grundrechtecharta - „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation“ – und der bei der Auslegung von Grundrechten zu berücksichtigende Art. 8 Abs. 1 EMRK – „jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz“ – eine Rolle. Elektronisch gespeicherte Daten fallen dabei grundsätzlich unter den Begriff von „Korrespondenz“ (vgl. zur Beschlagnahme in einer Anwaltskanzlei EGMR v. 16.10.2007, 74336/01 Nr. 45 – NJW 2008, 3409 – Wieser u. Bicos Beteiligungs-GmbH/Österreich). Ein staatlicher Eingriff in dieses Recht ist gem. Art. 8 Abs. 2 EMRK nur rechtmäßig, „soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist 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“. Das Recht der Europäischen Union steht daher nicht im Widerspruch zu der Forderung in Nr. 4.

5 Ausdehnung des gesetzlichen Datenschutzes auf Internet-Protokoll- Adressen

Art. 2 a der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr besagt, dass „personenbezogene Daten alle Informationen über eine bestimmte oder bestimmbare natürliche Person (“betroffene Person”) sind; als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Danach liegen personenbezogene Daten vor, soweit eine Person bestimmbar ist. Bei der Frage, ob es sich bei IP-Adressen um personenbezogene Daten handelt und damit die entsprechenden Regelungen des BDSG auf sie anwendbar sind, kann der 26. Erwägungsgrund der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr herangezogen werden. Dem 26. Erwägungsgrund zufolge sollen „bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen“. Dies lässt sich so verstehen, dass es ausreicht, wenn ein Dritter den Personenbezug herstellen kann. Folglich erscheinen IP-Adressen europarechtlich immer als personenbezogene Daten, da zumindest der Access-Provider für den Zeitraum der IP-Adressdatenspeicherung eine solche Zuordnung vornehmen kann (vgl. die Stellungnahmen der Europäischen Art. 29-Gruppe: Opinion 4/2007 on the concept of personal data and the Opinion on data protection issues related to search engines, S. 15 f. und Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive), S. 8).

Damit stehen der in Nr. 5 geforderten Klarstellung keine europarechtlichen Vorschriften entgegen. Vielmehr gebietet die Datenschutz-Richtlinie sogar eine Auslegung der IP-Adressen als personenbezogene Daten. Inwieweit diese Sichtweise, die der ganz herrschenden Meinung der deutschen Rechtswissenschaft auch im Hinblick auf nationales Recht entspricht, einer ausdrücklichen gesetzlichen Konkretisierung bedarf, soll hier nicht vertieft behandelt werden.

6 Verbot der Erstellung von Nutzerprofilen

Die in Nr. 6 vorgeschlagene Änderung des derzeit in § 15 Abs. 3 TMG verfolgten Opt-Out-Ansatzes in einen Opt-In-Ansatz, bei der der Nutzer aktiv in die Bildung pseudonymer Persönlichkeitsprofile einwilligt, muss angesichts des bestehenden Einwilligungserfordernisses darin bestehen, dass die Einwilligung speziell in diese Form der Verarbeitung von Nutzungsdaten expliziter gemacht wird. Europarechtlich steht den Mitgliedstaaten hier derzeit ein Umsetzungsspielraum zu, der die Einführung erhöhter Anforderungen an die Einwilligung in das Anlegen von Nutzerprofilen umfasste.

Etwas anders ergäbe sich nach einem Inkrafttreten der derzeit diskutierten EU-Datenschutz-Grundverordnung, die zwar Widerrufsmöglichkeiten vorsieht (Art. 19 DS-GVO-Entwurf), aber keine speziell auf Profiling zugeschnittenen, erhöhten Anforderungen an die Einwilligung in die Datenverarbeitung vorsieht (s. Art. 20 DS-GVO-Entwurf).

7 Umsetzung der sog. „Cookie-Richtlinie“

Die Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz sollte bis zum 31.05.2011 in den EU-Ländern umgesetzt werden.

Der Bundestag nahm den im März 2011 veröffentlichten Entwurf zur Ergänzung des Telemediengesetzes (TMG) nicht an. Im Januar 2012 brachte die SPD-Fraktion einen neuen Entwurf ein, der aber im Ausschuss für Wirtschaft und Technologie mit den Stimmen der Regierungskoalition zurückgewiesen wurde. Dem Bundestag liegt ein von dem Land Hessen eingebrachter inhaltsgleicher Antrag momentan vor. Ob und wann über diese Gesetzesinitiative entschieden wird, steht nicht fest.

Da die Frist zur Umsetzung der Richtlinie abgelaufen ist, kommt grundsätzlich eine direkte Anwendung der Richtlinie in Betracht. Die Möglichkeit einer direkten Anwendung wird jedoch wohl daran scheitern, dass es sich bei den Streitfällen typischerweise um horizontale Konstellation handelt (Bürger-Betreiber), die unmittelbare Anwendung einer nicht umgesetzten Richtlinie aber grundsätzlich eine vertikale Konstellation (Bürger-Staat) erfordert. Darüber hinaus müsste die Richtlinie bürgerbegünstigend sein, was bei entsprechenden Datenschutzvorgaben fraglich erscheint: Zwar sind diese für den Nutzer aus Sicht der

informationellen Selbstbestimmung begünstigend, für die Nutzung von Diensten der Informationsgesellschaft können sich dadurch aber funktionale Nachteile ergeben; außerdem kann es sich auch bei den Diensteanbietern, die durch die Vorschrift belastet werden, um EU-Bürger handeln. Einer letztendlichen gesetzlichen Umsetzung der EU-Vorgaben steht das EU-Recht jedenfalls nicht im Wege, vielmehr fordert es sie sogar.

8 Information über die Dauer der Aufbewahrung der Daten

Der Nutzer wird nach dem Inkrafttreten der derzeit im Entwurfsstadium befindlichen Datenschutz-Grundverordnung, die gem. 288 AEUV unmittelbare Geltung in den Mitgliedsstatten entfalten wird, nach Art. 14 Nr. 1 c des Verordnungsentwurfs so lange einen Anspruch auf die Erteilung der Information haben, wie lange seine personenbezogenen Daten gespeichert werden.

Bisher allerdings geht der Vorschlag über das Schutzniveau der momentan Geltung entfaltenden Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr hinaus. Dies ist allerdings für die deutschlandweite Umsetzung des Vorschlages nicht schädlich, da es den Mitgliedstaaten, zumindest bis zum Inkrafttreten der unmittelbar geltenden Grundverordnung, frei steht, strengere Regelungen zu erlassen als die, die sie zur Befolgung der als verbindlich vorgegebenen Ziele einer Richtlinie umsetzen müssten.

9 Wirksames Kopplungsverbot im Hinblick auf die anonyme Nutzung von Telemedien

Das ursprünglich in § 12 Abs. 3 TMG a.F. vorgesehene Koppelungsverbot wurde im Rahmen der BDSG-Novelle 2009 in § 28 Abs. 3 a BDSG übernommen, aber in zweierlei Hinsicht geändert: Zum einen wurde die Anwendbarkeit auf Fälle der Einwilligung in Werbung oder Adresshandel i. S. d. § 28 Abs. 3 Satz 1 BDSG beschränkt. Für andere Verarbeitungszwecke gilt das Kopplungsverbot seitdem nicht mehr. Innerhalb des neu eingegrenzten Anwendungsbereichs wurde das Verbot dabei strenger gefasst als bisher. Wo vorher die Monopolstellung des Anbieters ausschlaggebend war, ist eine zwingende Kopplung jetzt bereits unzulässig, „wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist“.

Die in Nr. 9 beschriebene Forderung nach einem effektiven Kopplungsverbot würde die erneute Verbreiterung des Anwendungsbereichs bei gleichzeitiger Beibehaltung der verringerten Anwendungsvoraussetzungen erfordern. Gegen eine entsprechende Novellierung des Kopplungsverbots spricht aus Sicht der Datenschutzrichtlinie nichts – sie macht für diesen Bereich keinerlei konkretere Umsetzungsvorgaben. Bei kompromisslosen gesetzlichen Forderungen an die Art und Weise einer bestimmten Diensteerbringung müsste sich die nationale Rechtsvorschrift allerdings – neben den deutschen Grundrechten – grundsätzlich

auch an den Grundfreiheiten der EU messen lassen, hier insbesondere dem Grundsatz der Dienstleistungsfreiheit. Ob eine entsprechend novellierte Norm, die restriktivere Anforderungen an inländische Diensteanbieter zur Folge hätte, eine grundsätzlich zulässige Inländerdiskriminierung darstellte oder als eine europarechtlich problematische, die Dienstleistungsfreiheit unverhältnismäßig beschränkende Maßnahme zu bewerten wäre, hängt von der Ausgestaltung des Kopplungsverbots ab. Ein Aspekt der Beurteilung wird dabei vor allem sein, inwieweit ein entsprechend restriktives Kopplungsverbot erforderlich ist, wenn ein ähnlicher Effekt durch die Selbstregulierung des Marktes erzielt werden könnte.

10 Anwendbarkeit der AGB-Kontrolle auf Datenschutz-Einwilligungsklauseln

Die Frage, ob Datenschutzhinweise der AGB-Kontrolle der §§ 305 ff. BGB unterliegen, hängt jeweils vom Einzelfall ab. Dabei kommt es einerseits darauf an, ob zu Beginn der Nutzung von Diensten die Voraussetzungen eines zivilrechtlichen Vertragsschlusses vorliegen, die Datenschutzklauseln Bestandteil der Allgemeinen Geschäftsbedingungen, also der vorformulierten Vertragsbedingungen sind bzw. bei Vertragsschluss geworden sind, wirksam in den Vertrag eingebracht wurden und andererseits, ob die dort gemachten Aussagen insbesondere der Inhaltskontrolle des § 307 BGB unterliegen können. Grundsätzlich aber ist jedenfalls von der Möglichkeit auszugehen, dass datenschutzbezogene Textteile der AGB auch der zivilrechtlichen Kontrolle unterliegen können (s. etwa BGH NJW 2010, 864). Soweit die Formulierung der Forderung Nr. 10 auf die Aufnahme der ausdrücklichen Anwendbarkeit der §§ 305 ff. BGB auf Datenschutzklauseln abzielt, erschiene dies grundsätzlich mit dem Europarecht vereinbar, soweit die Inhaltskontrolle dabei die spezialrechtlichen der Datenschutz-Richtlinie und der Klausel-Richtlinie beachtet. Allerdings würde eine Erweiterung des Anwendungsbereichs der §§ 305 ff. BGB auch auf Datenschutzklauseln außerhalb von AGB zum Einfallstor für eine entsprechende Inhaltskontrolle auch von Vorgaben, die nicht Bestandteil des Vertrags geworden sind, was sowohl auf Ebene des EU-Rechts als auch des nationalen Zivil- und Datenschutzrechts systemwidrig erscheinen würde.

Inwieweit eine entsprechende Klarstellung angesichts des akademischen Streits der rechtsdogmatischen Einordnung datenschutzrechtlicher Einwilligungen als rechtsgeschäftliche Willenserklärung oder als nicht rechtsgeschäftliche Erlaubnis des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung weiterführend erscheint, kann im Rahmen der Stellungnahme nicht abschließend bearbeitet werden. Hierzu bedürfte es eines umfangreicheren Gutachtens.

11 Zur Frage: Welche Dienstformen sind in ihrer Zuordnung als Telemediendienst, Telekommunikationsdienst oder telekommunikationsgestützter Dienst rechtlich besonders umstritten?

Die Frage der Zuordnung eines Dienstes unter den Anwendungsbereich von TMG oder TKG stellt sich insbesondere dort, wo eine Leistung verschiedene Aspekte einzelner Teildienste zu einem gesamten Dienst bündelt („hybride Dienste“) oder eine traditionell regulierte Nutzungsform über neue technische Plattformen elektronisch vermittelt wird („konvergente Dienste“). Beispiele für hybride Dienste sind etwa Onlinespiele, in deren Rahmen auch private Audiochats zwischen den Spielern möglich sind. Beispiele für konvergente Dienste sind unter anderem VoIP-Angebote, die Sprachtelefonie-Dienste über IP-basierte, offene Netzstrukturen ermöglichen. Wie oben gezeigt ist der Umstand der Doppelregulierung entsprechender Dienste durch die parallele Anwendbarkeit von TKG und TMG kein nationales Phänomen: Auch auf EU-Ebene kann die E-Commerce-Richtlinie neben den Vorgaben des TK-Richtlinienpakets auf entsprechende Dienste anwendbar sein. In diesen Fällen erfolgt weniger eine nicht gelingen wollende Einordnung des Gesamtdienstes unter eines oder beide Ordnungsregime, sondern werden die Einzelaspekte bzw. Teilbereiche der Dienste differenziert betrachtet. Diese differenzierte Diensteteilebetrachtung ermöglicht insoweit eine sachgerechte Anwendung der rechtlichen Vorgaben, erhöht aber gleichzeitig die Komplexität der Regelungsrahmens und erschwert die Einordnung und Nachvollziehbarkeit auf der Seite der Regelungsadressaten.