



WESTFÄLISCHE WILHELMS-UNIVERSITÄT
Institut für Informations-, Telekommunikations- und Medienrecht (ITM) zur ÖA 5.7.2010
- Zivilrechtliche Abteilung -
Prof. Dr. Thomas Hoeren

Deutscher Bundestag
Enquete-Kommission
Internet und digitale Gesellschaft

Ausschussdrucksache

17(24)004-A

zur ÖA 5.7.2010

30.6.2010

Leonardo-Campus 9

D-48149 Münster

Tel.: 02 51/83-3 86 00

Fax: 02 51/83-3 86 01

Email:

hoeren@uni-muenster.de

Münster, 30. Juni 2010

Stellungnahme zu rechtlichen Aspekten der Fragen der Fraktionen
zur Öffentlichen Anhörung der
Enquete-Kommission Internet und digitale Gesellschaft
am 5. Juli 2010

Vorbemerkung

Der folgende Text kann nur bruchstückhaft auf die Fragen der Enquete-Kommission antworten. Zum Teil fehlt dem Verfasser die Kompetenz, um die hochkomplexen Fragen etwa mit Bezügen zur Soziologie zu beantworten. Zum Teil sind die Fragen selbst bei rechtlichen Bezügen so weit gefaßt, daß ihre korrekte Beantwortung in einer Form, die noch für Zwecke einer Enquete-Kommission geeignet wäre, undenkbar wäre. Ich bitte daher um Entschuldigung für den fragmentarischen Charakter der weiteren Überlegungen. Auch auf Fußnoten wurde aus den genannten Gründen verzichtet. Die Fragen habe ich unabhängig und weisungsfrei beantwortet; ich gehöre keiner politischen Partei an.

Gesellschaftliche und mediale Auswirkungen der Digitalisierung

1. Wer nutzt digitale Medien und wie wird sich die Nutzung voraussichtlich weiterentwickeln? In welcher Weise und wie verändert die künftige Nutzung digitaler Medien die Wirtschaft in Deutschland, unsere Kultur und das Verhältnis bzw. die klassische Trennung von Arbeit und Freizeit? Was kann getan werden, um die anzunehmenden Auswirkungen des veränderten Mediennutzungsverhaltens positiv im Sinne von mehr Wertschöpfung, mehr Arbeitsplätzen und einer höheren Lebensqualität in Deutschland zu beeinflussen? (*Frage der CDU/CSU-Fraktion*)

2. Welche Auswirkungen hat das veränderte Mediennutzungsverhalten auf die Anbieter traditioneller Medien, auf den Stellenwert unterschiedlicher Medien und auf deren wirtschaftliche Entwicklung? Welche Kenntnisse und Fähigkeiten sollten wie gefördert werden, um jedem Einzelnen die Auswahl, die Einordnung und die Bewertung der im Internet nahezu unbegrenzt zur Verfügung stehenden Informationen zu ermöglichen? Was kann im nationalen und im internationalen Rahmen getan werden, um die Meinungsvielfalt und damit zugleich das Internet als freiheitliches Informationsmedium zu sichern? (*Frage der CDU/CSU-Fraktion*)

Gerade im Internet-Zeitalter muss das Grundrecht auf Information und Kommunikation abgesichert werden. Dabei geht es um Vielfalt, Freiheit, Zugangs- und Beteiligungsmöglichkeiten. Das Internet stellt ein anerkanntes Kommunikationsmedium dar.

Meinungsvielfalt bedeutet, dass es eine Vielzahl unterschiedlicher voneinander unabhängiger Informationsquellen gibt. Die Sicherung der Meinungsvielfalt stellt die wesentliche Voraussetzung für eine freie Meinungsbildung dar. Pluralität lässt sich durch möglichst wenig Regulierung erreichen. Wenn eine Regulierung erfolgen soll, dann muss sie auf ein Minimum beschränkt sein. Sie darf nur dort erfolgen wo sie tatsächlich Sinn macht.¹ Eine Schaffung technischer Sperren, etwa gegen kinderpornographische Inhalte, hat zur Folge,

¹ Vergleiche Diskussion um Kinderpornographie und die Sperrung von Websites.

dass Kommunikationsflüsse in einem weiten Ausmaß kontrolliert werden können und Begehrlichkeiten bezüglich verbotener oder unerwünschter Inhalte geweckt werden.² Dies ist umso bedenklicher, zumal die Wirksamkeit und Praktikabilität technischer Sperren von Experten stark bezweifelt wird.³ Gleichwohl lässt sich jedoch weltweit eine erhebliche Zunahme an Internet-Zensur verzeichnen.⁴ Vorreiter bei der Überwachung des Internets ist China mit der „Great Firewall“, die auch technologisch am weitesten entwickelt ist.

Nationale Alleingänge sollten vermieden werden, da diese ohnehin nicht praktikabel sind, beziehungsweise nur für deutsche Anbieter überhaupt denkbar sind. Um die Meinungsvielfalt und damit zugleich das Internet als freiheitliches Informationsmedium zu sichern, muss die Offenheit des Zugangs zu Information und Kommunikation gesichert werden. Der Zugang zu Informationen im Internet muss jedermann verfügbar sein. Manipulationen bei Suchhilfen müssen abgewehrt werden, Zensuren müssen vermieden werden und eine Angebotsvielfalt muss ermöglicht werden.

Suchmaschinen wie Google stehen in der Kritik.⁵ Google wird bereits als vorherrschende Meinungsmacht bezeichnet und damit verfüge das Unternehmen über ein Informationsmonopol.⁶ Google kann die Auswahl und Darstellung der vorhandenen Informationen nach Belieben manipulieren. Es stellt sich daher die Frage, ob Suchmaschinen wie Google die verfassungsrechtlich verankerte Meinungsbildungsfreiheit bedrohen.

Ziel sollte es sein, die Sozialverantwortung von Angeboten zur Information und Orientierung zu stärken. Das Prinzip der Selbstregulierung erscheint hier besser als eine Einzelsteuerung durch Kommunikationspolitik und entspricht dem Verfassungsrecht, denn staatliche Regulierung steht immer im Konflikt mit der gebotenen Staatsfreiheit für den Mediensektor. Das Recht sollte sich zurücknehmen und nur Rahmenbedingungen im Sinne von Spielregeln schaffen, innerhalb dessen der „Kampf der Meinungen“ stattfinden kann.

3. Wie verändern sich die Kommunikationsstrukturen der digitalen Gesellschaft und welche Konsequenzen oder auch Gefährdungen ergeben sich hieraus für die individuelle Kommunikation, die Öffentlichkeit, Journalismus und die politische Kommunikation und inwiefern müssen die Kommunikations- und Medienfreiheiten diesen Herausforderungen angepasst werden und welche neuen Formen der Teilhabe sind denkbar? (*Frage der SPD-Fraktion*)

² Marberth-Kubick, Der Beginn der Internet-Zensur – Zugangssperren durch Access-Provider, NJW 2009, S. 1792. Zu Internetsperren siehe auch die Ausführungen zu Abschnitt „Regulierung“ Frage 5.

³ <http://www.handelsblatt.com/technologie/it-internet/internet-sperre-teuer-und-wirkungslos;2215850>: „Das Internet lasse sich nicht sperren.“

⁴ Viefhues, Zunahme der Internet-Zensur, MMR aktuell 2010, 301163.

⁵ Zu Suchmaschinen siehe auch die Ausführungen zum Abschnitt „Regulierung“ Frage 4.

⁶ Danckert/Mayer, Die vorherrschende Meinungsmacht von Google - Bedrohung durch einen Informationsmonopolisten? MMR 2010, S. 219.

4. Welche Chancen bietet die digitale Gesellschaft für die Emanzipation der immer noch in vielen gesellschaftlichen Bereichen benachteiligten Frauen, welche Veränderungen des weiblichen Rollenbildes und klassischer geschlechtsspezifischer Zuschreibungen sind durch die Digitalisierung aller Lebensbereiche möglich und zu erwarten? (*Frage der Fraktion DIE LINKE.*)

Medienkompetenz

1. Welche Auswirkungen haben digitale (Unterhaltungs-)Medien auf die Persönlichkeitsentwicklung insbesondere auch im Vergleich zu anderen Medien? Welche Maßnahmen zur Verbesserung der Medienkompetenz in Familie und Gesellschaft sind geeignet, negativen Auswirkungen vorzubeugen? Wie und in welcher Weise kann der Bereich eLearning, das Lernen in der Schule, die Ausbildung von Lehrern und in Unternehmen von Mechanismen und Technologien insbesondere digitaler Unterhaltungsmedien profitieren? Können von digitalen Unterhaltungsmedien innovierende Impulse ausgehen? Welche sind dies und welche gesellschaftlichen Gruppen werden hiervon in besonderem Maße beeinflusst? (*Frage der CDU/CSU-Fraktion*)

2. Wie kann das Bewusstsein von Nutzern in Sozialen Netzwerken, insbesondere von Kindern und Jugendlichen, für die Sensibilität der eigenen Daten gestärkt werden? Sehen Sie diese Aufgabe primär im Bildungssystem oder sollten die Betreiber sozialer Netzwerke selbst dafür sorgen? Welche Bedeutung haben Soziale Netzwerke auf der Ebene lokaler/regionaler Gemeinschaften? Wie verändert die Nutzung sozialer Netzwerke herkömmliche Formen gesellschaftlichen Miteinanders und Aktivitäten, etwa in Vereinen, Parteien, Nichtregierungsorganisationen oder bei anderen sozialen Engagements? (*Frage der FDP-Fraktion*)

Wirtschaft und Arbeitswelt

1. Wie weit ist die Digitalisierung von Unternehmen und der Arbeitswelt bereits voran geschritten und wann wird sie abgeschlossen sein? Welche Tätigkeiten und Berufe werden unmittelbar, welche eher am Rand und welche überhaupt nicht erfasst? Welche Branchen werden von der Digitalisierung der Arbeit besonders profitieren, welche werden eher mit Herausforderungen konfrontiert sein? Wie wird sich Deutschland dabei im internationalen Wettbewerb entwickeln und beeinflusst die Digitalisierung der Arbeitswelt die Positi-

on Deutschlands als Technologiestandort positiv oder negativ? (*Frage der CDU/CSU-Fraktion*)

2. In welchem Maße prägen Produkte der ITK-Branche den Wandel zur digitalen Gesellschaft? Welche technologischen Entwicklungen stehen dabei im Mittelpunkt? Bei welchen dieser Technologien besitzt Deutschland in Wirtschaft und Wissenschaft im internationalen Vergleich besondere Kompetenzen und wie können diese ausgebaut werden? Wie wirken sich diese Technologien auf das Leben der Bürger, auf die Rolle des Staates und auf den Wirtschaftsstandort Deutschland aus und was kann getan werden, um staatliches Handeln transparenter zu machen sowie um neue unternehmerische Aktivitäten zu erleichtern? (*Frage der CDU/CSU-Fraktion*)

3. Welche Chancen und Herausforderungen ergeben sich in der digitalen Gesellschaft für Wirtschaft und Arbeit aus ökonomischer, arbeitsrechtlicher und gesellschaftlicher Perspektive (Stichworte hier: digitale Ökonomie, neue Selbständigkeit, digitale soziale Sicherheit, Mobilität und permanente Erreichbarkeit, Arbeitnehmerdatenschutz, etc.)? (*Frage der SPD-Fraktion*)

In der digitalen Gesellschaft ergeben sich für Arbeit und Wirtschaft viele Chancen aber auch einige Herausforderungen.

Wichtiger Aspekt ist der Arbeitnehmerdatenschutz.⁷ Die Einfügung des § 32 BundesdatenschutzG (BDSG) zum 1.9.2009 ist bereits Folge der jüngsten Datenschutzskandale, insbesondere aufgrund von Videoüberwachung am Arbeitsplatz, Bespitzelung und PC-Überwachung. Diese Einfügung kann aber noch nicht alle offenen Fragen in diesem Bereich klären.⁸ Deshalb sind weitere gesetzliche Regelungen wünschenswert. Zwar gibt es heute zu vielen Fragen des Beschäftigtendatenschutzes eine einzelfallbezogene Rechtsprechung der Arbeitsgerichte, die allerdings oft uneinheitlich ist. Spezielle gesetzliche Regelungen bestehen meist nicht. Sind Regelungen vorhanden, so finden sie sich über verschiedene Gesetze wie dem BDSG, Betriebsverfassungsg, TelekommunikationG (TKG) oder dem TelemedienG (TMG) verteilt. Deshalb wäre es sinnvoll, umfassende, allgemeingültige Regelungen für den Datenschutz am Arbeitsplatz zu schaffen, um die Rechtslage für Arbeitgeber und Beschäftigte gleichermaßen deutlich zu machen und mehr Rechtssicherheit zu erlangen. Dabei sollte unter anderem die Einwilligung des Beschäftigten auf einzelne Bereiche beschränkt werden, um dem ungleichen Machtverhältnis zwischen Arbeitnehmer und Arbeitgeber gerecht zu werden. Ebenfalls sinnvoll wäre eine ausdrückliche Regelung zur Korruptionsbekämpfung und Durchsetzung von Compliance-Anforderungen. Ferner sollte festgelegt werden, wann gesundheitliche Untersuchungen

⁷ Dazu siehe auch die Ausführungen zu Frage 5.

⁸ Erfurth, Der „neue“ Arbeitnehmerdatenschutz im BDSG, NJOZ 2009, S. 2914.

zulässig sind und welche Fragerechte dem Arbeitgeber zustehen. Inzwischen gibt es dazu einen neuen Gesetzesentwurf des Bundesinnenministeriums, der einen eigenen Unterabschnitt „Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses“ mit 14 Ziffern zum § 32 BDSG vorsieht.⁹

Netzwerkportale wie Xing oder Facebook bieten die Möglichkeit berufliche Kontakte zu knüpfen und zu pflegen. Sie funktionieren wie eine große, ausführliche Datenbank für Visitenkarten. Unternehmen können gezielt nach potentiellen Arbeitnehmern suchen und sich von Bewerbern ein umfassendes Bild machen. Die Herausforderung an diesen sozialen Netzwerken ist, dass Sicherheit und Datenschutz oftmals unzureichend sind.¹⁰ Daneben ist sehr problematisch, dass die Nutzer viel zu sorglos mit den eigenen Daten in sozialen Netzwerken umgehen und sich der Gefahren gar nicht bewusst sind. Möglich wäre es, die einschlägigen Gesetze wie TMG und BDSG zu überarbeiten, um den Schutz von persönlichen Daten und Informationen in sozialen Netzwerken zu gewährleisten. Durch die Überarbeitung können die Anbieter zu umfassender Aufklärung ihrer Nutzer und zum Einsatz datenschutzfreundlicher Technologien angehalten werden.

Eine weitere Chance für die Arbeit und Wirtschaft bietet die Telearbeit. Unter Telearbeit werden verschiedene Arbeitsformen zusammengefasst, bei denen Mitarbeiter zumindest einen Teil der Arbeit außerhalb der Gebäude des Arbeitgebers, vorzugsweise zu Hause, verrichten. Oftmals werden die Arbeitsergebnisse dabei dem Arbeitgeber über digitale Kanäle übermittelt. Diese Art von Arbeit ermöglicht es Beruf und Familie besser zu vereinbaren, da ein Teil der Arbeit von zu Hause aus verrichtet werden kann. Die Vorteile für Arbeitgeber sind bessere Qualität, stärkere Bindung der Mitarbeiter an das Unternehmen, ein besseres Image und Kosteneinsparung. Allerdings bringt die Telearbeit auch einige Herausforderungen mit sich. Der Arbeitgeber steht vor dem Problem der Sicherheit im Internet. Mit der zunehmenden Übertragung von wichtigen Daten über Telekommunikationsverbindungen wird es auch für die Firmen wichtig, diese Daten zu schützen, da auch die Angriffe darauf zunehmen werden. Dies erfolgt sowohl im Eigeninteresse der Firma (interne Produktions- oder Verwaltungsdaten), als auch im Rahmen des gesetzlich vorgeschriebenen Datenschutzes personenbezogener Daten (Mitarbeiter- oder Kundendaten). Analog dazu ist auch die Datensicherung bei vielen verteilten Lagerungsstellen viel schwieriger als an einem zentralen Ort.

4. In welchem Umfang bedarf es eines Ausbaus der bisherigen Kommunikations-Infrastruktur, um den zukünftig zu erwartenden Verkehrsmengen gerecht zu werden? In welchem Umfang wird das Verkehrsvolumen in der festnetzgestützten bzw. mobilen Kommunikation in welchen Zeiträumen anwachsen? (*Frage der FDP-Fraktion*)

⁹ <http://www.iitr.de/iitr-veroeffentlicht-internen-entwurf-eines-gesetzes-zur-regelung-des-beschaefigtendatenschutzes-arbeitnehmerdatenschutz.html>.

¹⁰ <http://www.heise.de/newsticker/meldung/Verbraucherzentrale-raet-zu-Verzicht-auf-Facebook-972308.html>; <http://www.heise.de/newsticker/meldung/Facebook-Chef-verspricht-mehr-Datenschutz-1006048.html>.

5. In welcher Art haben sich Arbeitswelt und Arbeitsbedingungen für Menschen und Gesellschaften durch das Internet verändert, welche Vor- und Nachteile sehen Sie in diesen Veränderungen und welchen Mitbestimmungs- und Regelungsbedarf sehen Sie für den Schutz von Arbeitnehmerinnen und Arbeitnehmern im digitalen Zeitalter? (*Frage der Fraktion DIE LINKE.*)

Durch das Internet haben sich die Arbeitswelt und Arbeitsbedingungen für Menschen und Gesellschaft grundlegend verändert. So sind durch das Internet neue Formen der Erwerbstätigkeit entstanden und der Arbeitsmarkt selbst ist transparenter geworden. Darüber hinaus führt das Internet allerdings auch dazu, dass die Grenzen zwischen Beruf und Privatleben immer mehr verschwimmen.

Arbeitgeber haben den Vorteil, dass sie sich über die verschiedenen sozialen Netzwerke ein umfassendes Bild von den einzelnen Bewerbern machen können. Daneben funktionieren Netzwerkportale wie XING wie eine große, ausführlichere Datenbank für Visitenkarten. Personalverantwortliche können schnell und gezielt potentielle Arbeitnehmer suchen, da unter anderem Berufserfahrung, derzeitige Position und Fähigkeiten einer Person für alle Mitglieder einsehbar sind. Netzwerkportale schaffen zudem die Voraussetzungen berufliche Kontakte zu knüpfen und über einen langen Zeitraum mühelos zu pflegen.

Überdies bietet das Internet die Möglichkeit der Telearbeit. Telearbeit bietet viele Vor- und Nachteile für beide Seiten. Für den Arbeitnehmer kommt es zu einer Verbesserung der Vereinbarkeit von Familie und Beruf, für junge Mütter werden zahlreiche Jobs attraktiver, es entstehen flexiblere Arbeitszeiten, und die Pendlerwege verkürzen sich. Allerdings können Schwierigkeiten wie soziale Isolierung, Raumprobleme oder Abkoppelung vom Betriebsgeschehen entstehen. Der Arbeitgeber wiederum profitiert von einer stärkeren Bindung der Mitarbeiter an das Unternehmen, einem besseren Image und von Kosteneinsparung, begegnet allerdings auch Problemen wie einem schlechteren Gruppenzusammenhalt, Verlust der Identifikation mit dem Unternehmen und Datenschutz- und Datensicherheitsproblemen.

Problematisch bei all diesen Veränderungen sind vor allem die rechtlichen Aspekte. Der Datenschutz spielt insbesondere bei sozialen Netzwerken und Jobportalen eine bedeutende Rolle. Hierbei muss sichergestellt werden, dass ein zufriedenstellendes Maß an Datenschutz erreicht wird und dass dieser von allen Seiten gewahrt wird. Zudem ist dafür zu sorgen, dass die Gesellschaft sensibler mit ihren Daten umgeht und die Gefahren von freizügiger Datenpreisgabe ernst nimmt.

Daneben muss für ausreichende Sicherheit im Internet gesorgt werden, damit z.B. Telearbeit problemlos bewerkstelligt werden kann. Auch müssen ausreichende und brauchbare Regelungen für den Online-Handel geschaffen beziehungsweise die existierenden Regelungen verbessert werden, damit ausreichend Rechtssicherheit geschaffen wird. Außerdem müssen arbeitsrechtliche Unsicherheiten geklärt werden. In wieweit ist die private

Nutzung des Internet auf der Arbeit erlaubt?¹¹ Mit welchen Konsequenzen muss gerechnet werden? Wann ist eine Kündigung aufgrund dessen wirksam?

Regulierung

1. Welche Herausforderungen und möglicherweise auch Gefährdungen bringt die Informations- und Kommunikationsinfrastruktur der digitalen Gesellschaft mit sich und wo besteht hier politischer oder rechtlicher Handlungsbedarf (Stichworte hier: Zugang, Breitband, Rechtsdurchsetzung, Netzverwaltung und -kontrolle, Netzneutralität, Verantwortlichkeiten, etc.)? (*Frage der SPD-Fraktion*)

Der Begriff der Netzneutralität¹² wird unterschiedlich verstanden. Fraglich ist, inwieweit der Begriff auch den reinen Zugang zum Netz umschreibt. Ist der Begriff auch so zu verstehen, liegt jedenfalls eine Ungleichbehandlung im Ausbau des Netzes vor. So ist bis heute eine Verbreitung auf dem Land unzureichend gesichert. Dies liegt zunächst an den technischen Gegebenheiten. Gerade der Ausbau von VDSL Netzen kann so nicht ausreichend sein und es findet seit Jahren eine Schuldzuweisung der Bundesnetzagentur zu den Telekommunikationsanbietern und zurück statt. So bleibt es fraglich, ob das optimistische Ziel eines Breitbandausbaus bis zum Ende des Jahres 2010 in allen noch nicht erreichbaren Gebieten möglich ist. Die Kosten für einen Ausbau gerade der weitaus schnelleren Next Generation Networks (NGN) kostet Geld. Das langfristige Investitionsvolumen wird auf 30 - 50 Mrd. Euro geschätzt.¹³

Die Versteigerung von Frequenzen aus der digitalen Dividende war hier ein erster Schritt. Durch die neu nutzbaren Frequenzen könnte die LTE-Technik weiter vorangetrieben werden. Es muss beobachtet werden, ob die Versorgung in ländlichen Gebieten weiter vorrangingt oder ob hier regulierend eingegriffen werden muss. Nachteil am momentanen Aufbau eines LTE-Netzes ist es jedoch, dass hier nur die großen Mobilfunkanbieter eine Chance haben. Neue und vor allem kleinere Unternehmen sind im Bereich des Aufbaus eines solchen Netzes ohne eine vergleichbare Chance.

Im Zusammenhang mit der Regulierung sollte sich auch gefragt werden, ob nicht die Dienste-Anbieter mit in den Ausbau einbezogen werden sollten. Betrachtet man den Netztraffic weltweit, so macht alleine Youtube 5% des weltweiten Datenverkehrs aus. Inwieweit eine Beteiligung in der Praxis umgesetzt werden kann ist jedoch fraglich. Davon abgesehen, müsste hier auch eine internationale Regelung gefunden werden. Eine auf Deutschland begrenzte Regelung hätte kaum eine Möglichkeit der Durchsetzung.

Versteht man den Begriff der Netzneutralität im Rahmen der Definition „jedes Bit ist gleich“ geht es um das Problem der ungehinderten Weiterleitung von Daten. Gerade mit dem Ausbau von NGN werden eine Kontrolle und eine Priorisierung von Datenpakete

¹¹ BAG, MMR 2006, S. 94; LAG Rheinland-Pfalz, MMR 2010, S. 430.

¹² Dazu siehe auch die Ausführungen zu Frage 4.

¹³ Ufer, Netzneutralität zerstört auf Dauer die Netzstabilität, MMR 2010, S. 13

einfacher. Datenpakete lassen sich nahezu beliebig verlangsamen oder sperren. Eine Offenheit des Internets wäre dadurch nicht mehr gegeben. Zwar dürfen Anbieter von Netzen prinzipiell selber entscheiden, was mit ihrem Netz geschieht, jedoch gehört das Internet heute schon zu einer kommunikativen Grundversorgung. Eine Versorgung mit Internetdiensten sollte deshalb für jeden Bürger sichergestellt werden. In den USA wird der Streit um rechtliche Vorgaben im Zusammenhang mit der Netzneutralität mit deutlich größerer Schärfe als in Europa geführt. Dies hängt auch mit anderen rechtlichen Gegebenheiten in Europa und in Deutschland zusammen. In Europa bleibt bei bestimmten Marktbeeinträchtigungen immer noch die Möglichkeit im Rahmen des Kartell- und des Telekommunikationsrechts regulierend einzugreifen. Eine zusätzliche gesetzliche Verankerung ist jedoch trotzdem angebracht. Die bisherigen Stellungnahmen der EU Kommission zu dieser Thematik genügen nicht. Die EU Kommission hat in ihrem Policy Statement vom 13.11.2007 von einer größeren Transparenz gegenüber dem Verbraucher gesprochen. Verbraucher sollen danach bei Verträgen regelmäßig aufgeklärt werden, wann und weshalb ein Anbieter den Internetzugang verlangsamt. Dies wird jedoch nicht ausreichen. Ein Vorschlag in diese Richtung wäre auf der Regulierungsebene eine „Must-Carry“ Regelung aufzunehmen, die vergleichbar mit denen im Rundfunkrecht sein könnte. Diese könnten genutzt werden um Provider dazu zu bewegen jedenfalls alle für die Öffentlichkeit notwendigen Dienste gleichmäßig zu verbreiten.

Im Zusammenhang mit der Netzverwaltung¹⁴ muss beobachtet werden, ob die Umgestaltung innerhalb der ICANN, weg von einer Aufsicht der US Regierung, hin zu einem international besetzten Ausschuss den erwünschten Erfolg verspricht. Gerade hier ist zu beachten, dass trotz des Rückzugs der US-Regierung durch einen Vertrag mit der Internet Assigned Numbers Authority (IANA) immer noch eine Aufsicht der US-Regierung über die Root Zone besteht. Es sollte darauf hingearbeitet werden, dass auch die IANA unter eine internationale Aufsicht gestellt wird.

Im Rahmen der Rechtsdurchsetzung ist die Behauptung das Internet sei ein rechtsfreier Raum nicht richtig. So sind viele Regelungen innerhalb des TMG, sowie innerhalb des UrheberG grundsätzlich geeignet Rechtsverstöße im Internet zu verfolgen. Problematisch ist allerdings die tatsächliche Durchsetzung des Rechts im Internet. Gerade auf der Rechtsfolgenseite wird über neue Maßnahmen diskutiert. Dies zeigen bspw. Überlegungen eine „Three-Strikes-Out“-Regel¹⁵ einzuführen. Diese begegnen allerdings größten grundrechtlichen Bedenken und erscheinen zudem nicht verhältnismäßig. Auch wenn in Deutschland eine „Three-Strikes“ Regelung derzeit nicht geplant ist, sollte auch verhindert werden, dass eine solche Regelung durch die Hintertür eingeführt wird. Werden, wie es bspw. im Rahmen des ACTA-Abkommen¹⁶ überlegt wird, verschärfte Haftungsregeln für Provider eingeführt, könnten diese dazu gezwungen werden, Vertragsbestimmungen so anzupassen, dass Internetzugänge blockiert und gekündigt werden. Auch eine „Two-Strikes-Out“ Regel ist rechtlich bedenklich. Zunächst werden innerhalb dieser Methode Provider zur eigenen Überprüfung ihrer Kunden gezwungen. Sie werden so als Ermitt-

¹⁴ Dazu siehe auch die Ausführungen im Abschnitt „Internationale Strukturen“ Frage 3.

¹⁵ Dazu siehe auch die Ausführungen zu Frage 5.

¹⁶ Dazu siehe auch die Ausführungen zu Frage 5 sowie im Abschnitt „Internationale Strukturen“ Frage 1.

lungshelfer eingesetzt. Auch die nach zwei Vergehen geplante Übergabe eines Berichtes des Providers an ein neu geschaffenes Gremium ist datenschutzrechtlich, wie prozessrechtlich stark bedenklich.

Gefährdungen bringen auch die immer neuen Formen der Ausnutzung von Kundendaten. Kann der Kunde nun immer und überall online sein, so wird er im nächsten Schritt auch immer auffindbar sein. Viele Anwendungen, bspw. Google Buzz, greifen inzwischen auf ortsbezogene Daten zurück, die diese für personalisierte Werbung in die Dienste einbeziehen können. Durch die Kombination von Netzwerkzugriff und GPS-Daten wird nun eine permanente Standortbestimmung möglich. Ein Schutz dieser Standortdaten und die Verhinderung der Aufzeichnung von Bewegungsprofilen muss das Ziel rechtlicher Vorgaben sein.

2. Welche Herausforderungen gehen mit der Digitalisierung und der weltweiten Vernetzung einher und wo besteht rechtlicher Anpassungsbedarf (Rechtsdurchsetzung, Konvergenz der Medien – Konvergenz des Rechtes, Urheberrecht, Informations- und Datenrecht, Persönlichkeitsrechte, etc.)? (*Frage der SPD-Fraktion*)

Die Herausforderungen der (weltweiten) Vernetzung und Digitalisierung sind unübersehbar. Ausgangspunkt der Herausforderungen ist, dass Inhalte über das Internet schnell und weltweit und zu jeder Zeit abgerufen werden können. Durch die Digitalisierung sind ganz neue Verbreitungsmöglichkeiten entstanden. Dies gilt für beinahe alles, was digitalisiert werden kann. Zu diesen Inhalten gehört bspw. urheberrechtlich geschütztes Material, wie Fotos, Filme, Musik, Software (Büroanwendungen und Computerspiele etc.), literarische Texte usw. Diese können alle digitalisiert hochgeladen werden und über das Internet verbreitet werden. Bei urheberrechtlich geschützter Musik und Filmen geschieht dies oftmals über sog. Tauschbörsen im P2P-System. Diejenigen, die dadurch an diesen Werken Urheberrechtsverletzungen begehen sehen sich professionellen Abmahnern gegenüber, die vielfach überhöhte Schadensersatzforderungen (insb. Anwaltskosten) eintreiben wollen. Neben dem Urheberrecht sind allerdings auch andere Immaterialgüterrechte betroffen. Hierzu zählen vor allem die Marke und das Patent. Über das Internet gibt es viele neue Vertriebsmöglichkeiten für gefälschte Produkte. Hier wurde in den letzten Jahren stets plakativ von Produktpiraterie gesprochen. Der Vertrieb gefälschter Produkte über das Internet stellt einen Unterfall davon dar. Vertrieben werden können diese Produkte z.B. über Online-Auktionen, wie eBay. Hinsichtlich der Marke gibt es zudem noch weitere Probleme: Zunächst kann eine fremde Marke als sog. Google-Adword eingesetzt werden. Dabei sichert sich ein direkter Konkurrent bestimmte Marken als Suchbegriff bei Google. Des Weiteren treten Probleme im Verhältnis Marke und Domain auf. Aber auch Meinungen können digitalisiert verbreitet werden. Dies geschieht einerseits über Plattformen, wie Gästebücher und Foren, andererseits durch Bewertungsportale (z.B. spickmich.de). Hierbei kann es zu erheblichen Verletzungen des grundrechtlich geschützten Allgemeinen Persönlichkeitsrechts kommen, wenn sich die Meinungen auf eine bestimmte Person beziehen und diese diskreditieren bis hin zu strafrechtlich relevanten Beleidigungen, üblen Nachreden und Verleumdungen. In diesen Rahmen gehört auch der Upload von Fotos

ohne Einverständnis der betroffenen Person, z.B. Nacktbilder usw. Immer wieder in der Diskussion steht auch die Preisgabe von persönlichen Daten im Internet, bzw. deren Schutz vor dem Zugriff Dritter, sei es nur zu Werbezwecken (Spam) oder sogar für strafrechtliche Vorhaben (z.B. Phishing). Besonders im Fokus stehen hier die sozialen Netzwerke StudiVZ, Facebook, Xing usw. Aber auch die Suchmaschinen, v.a. Google sammeln und speichern im großen Stil persönliche Daten von ihren Nutzern, um individuelle Werbung erstellen zu können.

Rechtlicher Anpassungsbedarf hinsichtlich der Rechtsdurchsetzung von Immaterialgüterrechten wurde bereits von der EU gesehen. Während die materielle Seite der Immaterialgüterrechte bereits durch unterschiedliche Richtlinien europaweit harmonisiert wurde, gab es eine solche Harmonisierung bzgl. der Durchsetzung dieses Sonderrechtsschutzes früher nicht. Dies hat sich durch die Enforcement-Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums¹⁷ aus dem Jahre 2004 geändert. Darin ist eine umfangreiche Harmonisierung der zivilrechtlichen Rechtsfolgen einer Verletzung eines Sonderrechts geregelt worden. Außerdem sind in der Enforcement-Richtlinie viele neue Wege der Beweiserlangung und -sicherung vorgesehen (z.B. Auskunft, Besichtigung). Die Richtlinie wurde mit dem Durchsetzungsgesetz 2008 in deutsches Recht übertragen.¹⁸ Mittel zu einer wirksamen Rechtsdurchsetzung der Sonderrechte sind demzufolge reichlich vorhanden. Hierzu gehören allerdings nur die technischen Schutzrechte (z.B. Patent), die Marke und das Urheberrecht. Die Umsetzung in deutsches Recht erfolgte für jedes Sonderrecht gesondert. Im Hinblick darauf, dass die Verletzungshandlungen gerade über das Internet immer vergleichbarer werden, wäre zu wünschen gewesen, einen Allgemeinen Teil des Geistigen Eigentums zu schaffen. Dies hätte zu einer besseren Übersichtlichkeit der Regelungen über die Rechtsdurchsetzung geführt.

Nicht von der Enforcement-Richtlinie beeinflusst werden das Allgemeine Persönlichkeitsrecht und der Datenschutz. Bei Verletzungen des Allgemeinen Persönlichkeitsrechts ist der Verletzte auf die allgemeinen Rechtsbehelfe des BGB angewiesen. Es gibt hier eine sehr umfangreiche und weit gereifte Kasuistik, so dass eine Neuregelung nicht erforderlich erscheint. Das BDSG regelt den Datenschutz auf Bundesebene. Hier gab es im Jahre 2009 drei Novellen. Diese haben allerdings nicht zu einer Vereinfachung des Datenschutzes geführt. Insb. die Änderungen zur Zulässigkeit personalisierter Werbung sind kompliziert mit vielen Ausnahmetatbeständen versehen (§ 28 BDSG).

Ein weiteres Problem ist die Haftung bei der Verletzung von Immaterialgüterrechten. Wie gesagt, werden bspw. viele Urheberrechtsverletzungen über P2P-Tauschbörsen von Jugendlichen begangen. Anschlussinhaber sind jedoch zumeist deren Eltern. Daher ist auch die IP-Adresse, über die die Verletzung begangen wird, den Eltern zugeordnet. Sie werden als erstes in Anspruch genommen. Ähnlich verhält es sich bei der fahrlässig verursachten Ausnutzung eines fremden eBay-Zugangs durch einen Dritten. Jüngst sorgte ein

¹⁷ Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29.4.2004.

¹⁸ Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums vom 7.7.2008, BGBl. I 2008, S. 1191.

Urteil des BGH zur mangelnden Sicherung eines WLAN-Anschlusses für Aufsehen.¹⁹ All diesen Fällen ist gemeinsam, dass die Rechtsprechung unter bestimmten Umständen von einer sog. Störerhaftung ausgeht. Das bedeutet, dass hier neben dem eigentlichen Täter der Verletzung auch ein Dritter, der bildlich gesprochen die Mittel bereitgestellt hat, haftet. Dabei handelt es sich um reines „Case-Law“, das im Bereich des Immaterialgüterrechts komplett von den Gerichten entwickelt. Hier wäre es wünschenswert, zu einer Kodifikation der Voraussetzungen der Störerhaftung zu kommen, bzw. Überlegungen anzustellen, inwieweit diese auch gesetzlich einzuschränken wäre.

Anpassungsbedarf besteht zudem beim sog. Fliegenden Gerichtsstand im Zusammenhang mit Rechtsverstößen im Internet. Dieser wird aus § 32 Zivilprozessordnung (ZPO) hergeleitet und ist eine Ausnahme von dem Grundsatz, dass stets am Wohnsitz des Beklagten geklagt werden muss (§ 13 ZPO). Nach § 32 ZPO ist für unerlaubte Handlungen dasjenige Gericht zuständig, in dessen Bezirk die Handlung begangen wurde. Bei Rechtsverstößen über das Internet, z.B. Urheberrechtsverstößen wäre demnach theoretisch jedes Gericht in Deutschland zuständig, da die Rechtsverletzung überall begangen worden sein kann. Dies wird durch die Rechtsprechung dahingehend eingeschränkt, dass zuständig nur dasjenige Gericht ist, an dessen Ort das Internetangebot bestimmungsgemäß abzurufen ist. Dies bleibt allerdings ungenau. So ist einer unerlaubte öffentliche Zugänglichmachung urheberrechtlich geschützter Werke theoretisch überall bestimmungsgemäß abzurufen. Es kommt daher häufig zu einer – bis zur Grenze des Rechtsmissbrauchs reichenden – Benachteiligung des Beklagten, die so im Hinblick auf die Grundregel des § 13 ZPO nicht vorgesehen ist. Der Fliegende Gerichtsstand in § 32 ZPO stammt aus einer Zeit, als es das Internet mit seinen Verbreitungsmöglichkeiten noch nicht gab. Bei Verletzungen von Immaterialgüterrechten sollte deshalb eine Regelung gefunden werden, die den Fliegenden Gerichtsstand ausschließt.

3. Wie haben sich die Rolle und die Gestaltungsmöglichkeit des Verbrauchers durch die Digitalisierung verändert. Wie haben sich die Nutzungsformen des Internets in den letzten Jahren gewandelt und welche Veränderungen erwarten Sie innerhalb der nächsten 5 bzw. 10 Jahren? Wie kann man Verbraucher/innen effizienter im Hinblick auf neue Formen von Internet-„Abzocke“ schützen (z.B. bei Phishing, Internetabofallen etc.)? Wie wirken die Transparenzanforderungen und Informationspflichten für Internetprovider? Droht hier eine Informationsüberflutung oder ist der Weg steigender Informations- und Impressumspflichten für Webanbieter weiterhin sinnvoll? (*Frage der FDP-Fraktion*)

Um den Verbraucher vor Abzocke im Internet – insbesondere im Bereich der Kostenfallen – zu schützen, ist es notwendig, bestehende gesetzliche Regelungen anzupassen. Nur bei klaren rechtlichen Vorgaben kann den betrügerisch agierenden Internetanbietern Einhalt geboten werden.

Gegen Internetabofallen könnte die sogenannte „Button-Lösung“ Abhilfe schaffen. Danach soll der Vertrag über eine Ware oder Dienstleistung immer erst dann zustande

¹⁹ BGH, Urt. v. 12.5.2010, Az. I ZR 121/08.

kommen, wenn der Verbraucher ein Bestätigungsfeld anklickt, welches unmissverständlich auf die Zahlungspflicht hinweist. Unmissverständlich heißt in diesem Zusammenhang, dass der Preis für das Angebot direkt auf oder unter dem Bestellbutton stehen muss oder zumindest ein anderer klar formulierter Passus die Entgeltlichkeit des Angebots hervorhebt. Bisherige Tricks der Internetanbieter, die Kosten in einem Link zu verstecken, der auf weitere Informationen verweist und oftmals nur am unteren Bildschirmrand nach dem Herunterscrollen in identischer Farbe eingeblendet wird, wären mit diesem Modell nicht mehr möglich.

Bislang bewegen sich die Betreiber derartiger Vertragsfallen in einer rechtlichen Grauzone. Die rechtliche Situation im Fernabsatzrecht sieht derzeit so aus, dass Preisangaben nicht direkt sichtbar auf der ersten Seite des Angebots platziert werden müssen. Ausreichend ist es nach der Rechtsprechung, wenn die Schritte bis zur Information (über den Preis) mittels zweier Klicks erreicht werden können. Strengere Vorgaben für die Preisangaben gelten nach der Preisangabenverordnung (PAngV) nur für Anbieter, die mit Preisen werben. Doch auch nach diesen Vorgaben ist es zulässig, dass die Kosten erst nach einem Klick sichtbar gemacht werden. Diese Regelungen bestärken Internetanbieter darin, die Entgeltlichkeit ihrer Angebote zu verschleiern.

Die Rechtsprechung hat in zahlreichen Urteilen gegen die Abofallenbetreiber entschieden und deutlich gemacht, dass entweder mangels Vertragsschluss überhaupt kein Zahlungsanspruch begründet wird oder dieser jedenfalls durch Anfechtung zum Erlöschen gebracht werden kann, so dass theoretisch eine „Button-Lösung“ zur Rechtsdurchsetzung nicht erforderlich wäre. Allerdings muss sich der Verbraucher auch der fehlenden Zahlungspflicht bewusst sein und entsprechende gerichtliche Schritte nach Erhalt eines Abmahnschreibens einleitet, um seine Rechte durchzusetzen bzw. im Falle eines fehlenden Zahlungsanspruchs die Zahlungsaufforderung zu ignorieren. In der Realität lassen sich zahlreiche Verbraucher aber durch die Schreiben, die in der Regel von Abmahnanwälten aufgesetzt werden, derart einschüchtern, dass sie oftmals sofort auf die Mahnung zahlen. Die bestehenden gesetzlichen Regelungen müssten daher zum Schutze des Verbrauchers so geändert werden, dass Anbieter explizit verpflichtet werden, die etwaigen Kosten unmittelbar auf der ersten Seite ihres Angebots deutlich hervorzuheben. Klare Regelungen hinsichtlich Layout, Schriftfarbe und Position des Zustimmungsfensters sind unumgänglich. Verbraucher würden dann aus ihrer im Internet eingeschränkten Aufmerksamkeit aufschrecken, weil sie plötzlich mit dem für sie wichtigsten Entscheidungsparameter, nämlich der Kostenpflicht, konfrontiert würden. Sie könnten sich dann bewusst und vor allem nachweislich für oder gegen die entgeltliche Leistung entscheiden.

Von einem weiteren eigenständigen nationalen Gesetz, welches unabhängig von der Systematik der bisherigen Regelungen steht, ist dagegen dringend abzuraten. Gerade im Bereich der Pflichten für Diensteanbieter bei Internetangeboten gibt es bereits zahlreiche Normen, so dass ein weiteres Gesetz die – ohnehin – schon unübersichtliche rechtliche Lage weiter verschlimmern würde. Vielmehr bedarf es einer Vereinfachung der bestehenden Regelungen, damit jeder einzelne Verbraucher erkennen kann, welche Rechte ihm zustehen. Vereinfachung heißt in diesem Zusammenhang eine grundlegende Überarbei-

tung der gesetzlichen Systematik im Bereich der Verbraucherschützenden Vorschriften.

Ein weiteres Problem der Internetabzocke tritt bei elektronischen Geldtransaktionen in Form von Phishing und Pharming auf. Ziel ist es dabei, Legitimationsdaten von Bankkunden (PIN und TAN) ohne deren Wissen zu erlangen und für illegale Transaktionen zu missbrauchen. Rechtliche Unsicherheit besteht in diesem Bereich dahingehend, ob dem Kunden in bestimmten Fällen ein Mitverschulden aufgebürdet werden kann oder ob die kontoführende Bank stets für den Vermögensschaden gegenüber dem Bankkunden in vollem Umfang haftet. Hier sollte es klare gesetzliche Vorgaben geben, die den einzelnen Kontoinhaber von der Verantwortlichkeit freistellen, es sei denn, ihm ist grob fahrlässiges Verhalten zuzuschreiben. Die Einordnung der Pflichten zwischen Bank und Kunden beim Online-Banking ist dabei entscheidend für die Zuordnung von Risiken und für die Haftungsverteilung. Eine Pflicht des Kunden könnte sicherlich das Einspielen regelmäßiger Sicherheitsupdates für das Betriebssystem und die verwendete Software sein. Banken sollten verpflichtet werden, über die Gefahren elektronischer Geldtransaktionen aufzuklären und Warnungen herauszugeben, PIN und TAN niemals auf telefonische Anforderung oder per Mail herauszugeben. Um der missbräuchlichen Verwendung von Passwörtern und anderen Identitätsmerkmalen vorzubeugen, hilft nur eine Sensibilisierung der Kunden für dieses Thema.

Die Transparenzanforderungen und Informationspflichten für Internetprovider verfolgen vorrangig den Zweck, Vertrauen der Verbraucher im elektronischen Geschäftsverkehr zu schaffen. Für Internetprovider bedeutet die Einhaltung der zahlreichen Vorschriften einen hohen zeitlichen und finanziellen Aufwand. Es ist aber nicht davon auszugehen, dass durch die Vorschriften die Geschäfte im E-Commerce-Bereich gehemmt werden. Ganz im Gegenteil boomt der Markt der Online-Angebote auch weiterhin. Allerdings führen die zahlreichen nationalen und europäischen Bestimmungen, welche nicht in einem Gesetz einheitlich geregelt wurden, zu einer solchen Unübersichtlichkeit im Hinblick auf die Informationspflichten, dass es für den einzelnen Diensteanbieter äußerst schwierig ist, den Überblick zu wahren und alle Pflichten gesetzestreu zu erfüllen. Am 18.5.2010 trat noch eine weitere Rechtsnorm – die Dienstleistungs-Informationspflichten-Verordnung – in Kraft. Problematisch ist, dass die Inhalte, die auf eine größere Transparenz der Dienstleistungsangebote abzielen, nicht in das TMG aufgenommen wurden, wo auch die PAngV dem Adressatenkreis besser hätte zugeordnet werden können. Eine Änderung der gesetzlichen Systematik wäre an dieser Stelle notwendig gewesen, um der fehlenden Überschaubarkeit entgegenzuwirken. Verbraucherschützende Vorschriften nützen dem einzelnen Verbraucher nicht, wenn dieser nicht mehr überblicken kann, welche Rechte ihm überhaupt zustehen. Von einer Stärkung des Verbraucherschutzes, in der Weise wie sie durch die einzelnen Vorschriften bezweckt wird, kann wohl nicht ausgegangen werden. Einen echten Nutzen hätten Verbraucher und auch Unternehmen erst, wenn das gesamte Verbraucherschutzrecht so weit wie möglich vereinheitlicht würde. Dabei muss national darauf geachtet werden, dass bestehende gesetzliche Regelungen vereinfacht und in einem Gesetz zusammengefasst werden, um die bestehenden Pflichten für Unternehmer und die Rechte der Verbraucher für alle Beteiligten transparenter zu machen. Steigende Informationspflichten führen nicht zu einer Informationsüberflutung, sofern sie nicht in

zahlreichen gesetzlichen Regelungen verstreut werden. Im Bereich der Abofallen zeigt sich, dass bestehende Regelungen sogar verschärft werden müssen, um einen angemessenen Verbraucherschutz zu ermöglichen. Was zu einer Informationsüberflutung führt, ist vielmehr die Masse an Bestimmungen, die im Gesetz ohne jede Systematik geregelt wird.

4. Bringt das Internet andere oder neue Monopolpotentiale mit sich und stellen diese ggf. Rechtssetzung und Politik vor neue Herausforderungen? Auf welche Weise kann der politische Gestaltungsspielraum in Bezug auf die Bildung von auch transnationalen Monopolen ausgeschöpft werden? (Stichworte: Netz,- Suchneutralität, crossmediale Konzentration etc.) (*Frage der Fraktion BÜNDNIS90/Die Grünen*)

Beim Themenkomplex „Internet“ besteht die Gefahr des Missbrauchs einer marktbeherrschenden Stellung auf verschiedenen Ebenen. Als Grundlage für den Zugang zum Internet nutzen die Zugangsanbieter für die sog. „Letzte Meile“ vielerorts die Kabelleitung der Telekom. Das Zugriffsrecht auf diese Leitungen stellt eine wichtige Voraussetzung für das wirtschaftliche Überleben der einzelnen Anbieter und für einen fairen Wettbewerb dar. Die Kontrolle dieses Zugriffsrechtes muss daher auch in Zukunft sichergestellt sein. Neue Aspekte sind hier aufgrund der tiefgreifenden Veränderungen im Bereich des Internetzugangs über Kabelanbieter und bei der Vermischung von Rundfunk (TV) und Internet zu berücksichtigen. Weiterentwickelte Technologien in der Datenkompression und der Ausbau der Breitbandverbindungen ermöglichen die Übertragung von Bewegtbildern, Fernsehprogrammen und fernsehähnlichen Diensten über das Internet; TV-Geräte mit integriertem Internetanschluss lassen die Grenzen zwischen Rundfunk und Internet weiter verwischen. Es wird daher immer wichtiger, den erheblichen Markt exakt zu definieren. Die Regulierung der Bundesnetzagentur (BNetzA) wird auch auf lange Sicht weiter notwendig sein, um hier für alle Diensteanbieter Chancengleichheit und freien Wettbewerb zu ermöglichen.

Im Bereich der Datenweiterleitung im Internet ist die Entwicklung der NGN weiter zu beobachten. Eine Priorisierung von Datenpaketen und Anwendungen muss unter dem Stichwort „Netzneutralität“²⁰ kritisch hinterfragt werden. Nach Meinung der EU-Kommission wird der Wettbewerb zwischen den Anbietern automatisch für eine Neutralität des Netzes sorgen. Sollte dies nicht der Fall sein, müssten die Anbieter auf Basis der Zugangsrichtlinie zur Neutralität verpflichtet werden.

Im Hinblick auf die zur Nutzung des Internets verwendete Software, insbesondere des Browsers, haben in den letzten Jahren bereits mehrfach Eingriffe der Regulierungsbehörden auf EU-Ebene stattgefunden. Neben dem bei Microsoft-Betriebssystemen mitgelieferten Browser „Internet Explorer“ wird in Zukunft bei der Installation des Betriebssystems eine Auswahl aus verschiedenen Alternativen angeboten. Für den Nutzer sind die Unterschiede eher marginal, alle verbreiteten Browser befinden sich auf einem hohen Niveau und der Umstieg auf ein anderes Produkt kann heute problemlos erfolgen. Die starke Marktposition von Microsoft wird hier in Zukunft weiter abnehmen.

²⁰ Dazu siehe auch die Ausführungen zu Frage 1.

Monopolgefahren bestehen jedoch bei diversen Angeboten im Internet. Zunächst sind hier die Suchmaschinenbetreiber in ihrer Funktion als Gatekeeper zu nennen, quasi als Schlüsselportale zum Internet.²¹ Ohne Suchmaschinen kann der Nutzer die Flut von Informationen, die das Internet ihm bietet, nicht verwerten. Unter allen Anfragen an Suchmaschinen hat Google in Europa einen Anteil von über 80%. Dies ist unter mehreren Gesichtspunkten bedenklich. Der Platz in der Trefferanzeige bei Google entscheidet darüber, ob ein Unternehmen, ein Internetangebot oder ähnliches im Internet überhaupt wahrgenommen wird. Große Teile der Benutzer fragen nur die ersten Seiten einer Ergebnisliste ab, weitere Ergebnisse sind praktisch bedeutungslos. Da Google die Parameter, aus denen die Ergebnisse gebildet werden, nicht offenlegt, lässt sich ein Missbrauch an dieser Stelle nicht ausschließen. Daneben sei darauf hingewiesen, dass Google durch den großen Anteil aller Suchanfragen weltweit als einziges Unternehmen in der Lage ist, Entwicklungen und Bedürfnisse in bestimmten Bereichen festzustellen und diese Ergebnisse zu vermarkten. So war es Google z.B. anhand der Suchanfragen in Europa möglich, bereits im Vorfeld den deutschen Sieg beim Eurovision Song Contest vorauszusagen. Auch auf dem Feld der Online-Werbeanzeigen liegt Google unangefochten vorne, so dass die Preisentwicklung für Anzeigen im Rahmen der Google-Suche beobachtet werden muss.

Die Vergangenheit hat gezeigt, dass Suchmaschinenbetreiber oft nach einer gewissen Zeit wieder als Standard abgelöst wurden. Allerdings erscheint es höchst fraglich, ob sich diese Erkenntnisse auch auf Google übertragen lassen. Die Position von Google ist gefestigt, die Werbeumsätze sind beträchtlich. Google ist durch verschiedene Angebote nicht nur im Internet breit aufgestellt. Google hat daher auch die finanziellen Möglichkeiten, in neue Technologien zu entwickeln und seine Position auszubauen. Microsoft hat mit der Übernahme von Yahoo den Weg zu einem Konkurrenten für Google eingeschlagen. Man wird jetzt abwarten müssen, wie sich der Markt für Suchmaschinen entwickelt, welche Schritte Google zur Verteidigung seiner Position einleiten wird und welche Maßnahmen der Gesetzgeber gegebenenfalls dagegen treffen kann.

Im Hinblick auf die Medienkonzentration steht für den Zugang zu ausführlichen Informationen und Nachrichten im Internet ein breites Feld an Angeboten bereit. Anbietern aus verschiedenen Medienfeldern sind dabei vertreten. Man kann sich z.B. direkt bei seinem Internetzugangsanbieter informieren, etwa über das Zugangportal von T-Online. Die Nutzer können daneben Angebote der verschiedenen Printverlage nutzen, z.B. bild.de oder spiegel.de, oder sie können sich über Suchmaschinen selbst die benötigten Informationen beschaffen. Dazu gibt es auch noch die Internetauftritte von TV-Sendern, die zusätzlich mit umfangreichen Mediatheken die Grenzen zwischen den Medien, insbesondere zwischen Rundfunk und Internet, überschreiten. Die Entwicklung in diesem Punkt hat gerade erst begonnen, zurzeit ist die Konzentration der Medien nicht so fortgeschritten, dass ein Eingriff notwendig erscheint.

²¹ Dazu siehe auch die Ausführungen im Abschnitt „Gesellschaftliche und mediale Auswirkungen der Digitalisierung“ zu Frage 1.

Der Handel im Internet ist breit aufgestellt. Die Entwicklung erscheint positiv, neben den großen Händlern wie Amazon, eBay oder ähnlichen besteht auch eine große Auswahl an kleineren Händlern. Da auch daneben noch die Möglichkeit des Kaufs im Ladengeschäft besteht, ist eine Monopolbildung hier auf absehbare Zeit nicht zu erwarten. Eine Gefahr könnte jedoch bei dem Internetangebot von eBay für private Nutzer bestehen. Da Kleinanzeigen in Zeitungen und vergleichbare Angebote weiter rückläufig sind, muss beobachtet werden, wie eBay seinen hohen Marktanteil nutzt und wie sich die Preise für private Nutzer entwickeln.

5. Sehen Sie rechtliche Maßnahmen der letzten Jahre, die den freiheitlichen Charakter des Internets bereits kontraproduktiv beschränkt haben oder geeignet sind, den freiheitlichen Charakter des Internets zu verändern? Welche netzpolitischen Verfehlungen hat es in den letzten 5 bis 10 Jahren gegeben? (*Frage der Fraktion BÜNDNIS90/Die Grünen*)

Der freiheitliche Charakter des Internets wird vor allem durch Maßnahmen beeinträchtigt, die zu einer Filterung der Internetinhalte²² führen. Hierbei ist zunächst das inzwischen zwar verabschiedete allerdings nicht angewendete Zugangerschwerungsgesetz zu nennen. Dies sah eine Sperrung von Webseiten mit kinderpornographischen Inhalten durch die Access-Provider vor. Die Inhalte werden bei einer derartigen Sperrung aber nicht gelöscht, sondern sind nach der leichten Umgehung weiterhin im Internet verfügbar. Zudem ist zu befürchten, dass derartige Sperren von Vertretern der Unterhaltungsindustrie für eigene Zwecke eingesetzt werden.²³ Der Schritt zu einer „Zensur“ ist nicht weit, wenn eine Speerinfrastruktur erst einmal eingerichtet ist. Inzwischen hat sich aber in der Politik zu Recht der Grundsatz „Löschen statt Sperren“ durchgesetzt,²⁴ der nun auch vom Europäischen Parlament verfolgt wird.²⁵

Weiterhin sind auch Versuche zu nennen, eine Haftung der Access-Provider herbeizuführen. So wurde versucht, die Access-Provider in einem ordnungsbehördlichen Verfahren bzw. gerichtlich dazu zu verpflichten, den Zugang zu bestimmten rechtswidrigen Inhalten zu sperren. Zunächst ging es hierbei um Pornographie, inzwischen aber auch um urheberrechtswidrige Inhalte, was die Relevanz der o.g. Befürchtung unterstreicht. Die Gerichte lehnten eine solche Haftung der Provider aber meist ab, da entsprechende Maßnahmen nicht wirksam und zudem nicht zumutbar sind.²⁶

²² Dazu siehe auch die Ausführungen zum Abschnitt „Gesellschaftliche und mediale Auswirkungen der Digitalisierung“ Frage 2.

²³ Zur Lage in Großbritannien: <http://www.heise.de/newsticker/meldung/Grossbritannien-Webseiten-Sperre-soll-Internetsperren-ergaenzen-947437.html>.

²⁴ Vgl. <http://www.heise.de/newsticker/meldung/Bundesrat-streitet-ueber-Linie-zu-Websperren-auf-EU-Ebene-992072.html>; <http://www.heise.de/newsticker/meldung/CDU-plaedierte-fuer-Loeschen-vor-Sperren-im-Kampf-gegen-Kinder pornos-1004976.html>.

²⁵ <http://www.heise.de/newsticker/meldung/EU-Parlament-formuliert-Grundsätze-zur-Netzpolitik-1023466.html>.

²⁶ Zu rechtsradikalen Inhalten: VG Düsseldorf, MMR 2003, S. 205; OVG Münster, MMR 2003, S. 348; zu pornographischen Inhalten: OLG Frankfurt, MMR 2008, S. 166; LG Kiel, MMR 2008, S. 123; LG Frankfurt, MMR 2008, S. 344; LG Düsseldorf, MMR 2008, S. 189; LG Düsseldorf, MMR 2008, S. 349; zu urheberrechtswidrigen Inhalten: LG Hamburg, MMR 2009, S. 506; LG Hamburg, Urt. v. 12.3.2010, Az. 308 O 640/08; LG Hamburg, B. v. 6.5.2010, Az. 310 O 154/10, dazu

Generell kann ein zu scharfes Haftungsregime auch zu einer Gefährdung des freiheitlichen Charakters des Internets führen. Zu denken ist hier insbesondere an die Betreiber von Foren oder Weblogs, denen die Gerichte zum Teil exorbitante Prüfungspflichten auferlegen, die kaum zu erfüllen sind.²⁷ Als Reaktion darauf können sich daher zahlreiche Betreiber dazu veranlasst sehen, den Betrieb ihrer Angebote aus Angst vor rechtlichen Konsequenzen einzustellen. An dieser Stelle sind klare gesetzliche Vorgaben erforderlich um den Gerichten eine Handlungsleitlinie zur Seite stellen zu können.

Ebenfalls ein sehr bedenklicher Trend sind Bestrebungen, die Access-Provider durch sog. Three-Strikes-Out-Regelungen²⁸ zu Erfüllungsgehilfen der Unterhaltungsindustrie zu machen. So gibt es in Frankreich seit kurzem ein Gesetz, nach dem Urheberrechtsverletzern für bis zu einem Jahr der Internetanschluss abgeschaltet werden kann.²⁹ Auch in Großbritannien gibt es derartige Pläne.³⁰ Höchst bedenklich ist zudem das Anti-Counterfeiting Trade Agreement (ACTA-Abkommen)³¹, das seit 2007 von der EU, den USA, Japan und sechs weiteren Staaten hinter verschlossenen Türen verhandelt wird. Ziel des ACTA-Abkommens ist u.a. die Eindämmung der Verletzung des geistigen Eigentums. Wegen der mangelnden Transparenz und Befürchtungen unter anderem über die Durchsetzung etwa von Internetsperren gegen Urheberrechtsverletzer gab und gibt es heftige Diskussionen um dieses Abkommen. In einem nun veröffentlichten Entwurf ist das Three-Strikes-Modell zwar nicht mehr vorhanden.³² Dennoch ist größte Vorsicht angesagt, dass nicht über die Hintertür internationaler Abkommen Verpflichtungen für den deutschen Gesetzgeber geschaffen werden, die später nicht mehr rückgängig gemacht werden können.

6. Wie beurteilen Sie die Veränderung des Charakters des Internets als einem in Nutzung und Zugang freiheitlichen, offenen Medium unter der Maßgabe seiner fortschreitenden Einhegung, Zensur und Regulierung und damit einhergehenden Zerstörungen von Innovationspotentialen, und wie beurteilen Sie Forderungen, dass das Internet als Universaldienst gelten sollte, der unter die öffentliche Daseinsvorsorge fiele? (*Frage der Fraktion DIE LINKE.*)

<http://www.heise.de/newsticker/meldung/Pirate-Bay-nach-Breitseite-der-Filmindustrie-offline-2-Update-1001516.html>.

²⁷ Etwa LG Hamburg, MMR 2009, S. 580; LG Hamburg, Urt. v. 31.3.2009, Az. 325 O 69/09; OLG Hamm, NJW-RR 2010, S. 189; AG München, MMR 2008, S. 782; aber auch OLG Zweibrücken, MMR 2009, S. 541; OLG Hamburg, ZUM 2009, S. 417.

²⁸ Dazu siehe auch die Ausführungen zu Frage 1.

²⁹ <http://www.heise.de/newsticker/meldung/Franzoesisches-Gesetz-fuer-Internetsperren-tritt-in-Kraft-894248.html>; <http://www.heise.de/newsticker/meldung/Frankreich-Internetsperre-fuer-Urheberrechtsverletzer-gebilligt-837138.html>.

³⁰ <http://www.heise.de/newsticker/meldung/Grossbritannien-Webseiten-Sperre-soll-Internetsperren-ergaenzen-947437.html>. Die Bundesjustizministerin hat in ihrer Berliner Rede zum Urheberrecht vom 14.6.2010 ein derartiges Modell abgelehnt.

³¹ Dazu etwa <http://iri-blog.info>; siehe auch die Ausführungen zu Frage 1 sowie im Abschnitt „Internationale Strukturen“ Frage 1.

³² <http://www.heise.de/newsticker/meldung/Analyse-ACTA-liefert-noch-viel-Stoff-fuer-Diskussionen-984590.html>.

Nach Art. 87f GG muss der Bund im Bereich der Telekommunikation flächendeckend angemessene und ausreichende Dienstleistungen gewährleisten. Dementsprechend ist auch ein Ziel des TKG die Sicherstellung einer flächendeckenden Grundversorgung mit Telekommunikationsdiensten (Universaldienstleistungen) zu erschwinglichen Preisen (§ 2 Abs. 2 Nr. 5 TKG). Als Universaldienst sind bislang u.a. der Anschluss an ein öffentliches Telefonnetz an einem festen Standort und der Zugang zu öffentlichen Telefondiensten an einem festen Standort bestimmt (§ 78 Abs. 2 TKG). Das Internet, bzw. präziser, der Zugang zum Internet wird dort nicht ausdrücklich als Universaldienst genannt. Allerdings ist über einen analogen bzw. digitalen Telefonanschluss ein Zugang zum Internet jederzeit möglich. Mit der Frage kann daher nur gemeint sein, ob ein breitbandiger Internetanschluss zum Universaldienst gehören soll.

Dies kann nur befürwortet werden. Mit der zunehmenden Verbreitung von Breitbandanschlüssen werden zahlreiche Informationsangebote auch entsprechend ausgerichtet, so dass sie ohne einen breitbandigen Anschluss praktisch nicht genutzt werden können. Neben diesem eher die Bürger und deren Teilhabe am kulturellen und gesellschaftlichen Leben im Internet betreffenden Aspekt, spielen vor allem wirtschaftliche Gesichtspunkte eine bedeutende Rolle. Gerade in Unternehmen sind breitbandige Internetanschlüsse zwingend erforderlich. Dies ist vor allem in der heutigen arbeitsteiligen Wirtschaftswelt mit zahlreichen Outsourcing-Aktivitäten von erheblicher Bedeutung. Durch das sog. Cloud Computing müssen die Unternehmen nicht selber große Serverfarmen kaufen, sondern können entsprechende Rechenkapazitäten bei anderen Dienstleistern mieten, deren Server dadurch deutlich besser ausgelastet sind. Um die zu verarbeitenden Daten transportieren zu können, sind erhebliche Bandbreiten erforderlich. Aber auch die Umstellung des leitungsvermitteltes Telefonnetzes auf ein paketbasiertes Telefonnetz erfordert hohe Bandbreiten. Von dem Vorhandensein breitbandiger Anschlüsse hängen deshalb nicht zuletzt auch Standortentscheidungen von Unternehmen ab. Unternehmen in Regionen ohne einen derartigen Anschluss haben daher extreme Standortnachteile. Die Aufnahme eines Breitbandanschlusses in den Universaldienst kann daher nur befürwortet werden.

Eine weitere Frage ist dann die der konkreten Bandbreite. Dabei ist zum einen der Stand der Technik zu berücksichtigen. Zum anderen wird bei Universaldienstleistungen nur eine Grundversorgung und nicht der Ausbau einer optimalen Infrastruktur verlangt. Momentan werden am Markt bereits Anschlüsse mit bis zu 100 MBit/s angeboten. Der Großteil der Anschlüsse verfügt allerdings nur über eine Bandbreite von 1 – 6 MBit/s. Als Universaldienst ist momentan sicherlich eine Bandbreite von 2 MBit/s angemessen, die sich aber an den technischen Fortschritt anpassen muss. So sieht die digitale Agenda“ der EU-Kommission vor, dass 2020 alle Europäer einen Anschluss von mindestens 30 MBit/s und die Hälfte der Haushalte über Leitungen mit 100 MBit/s verfügen soll.³³

Digitale Spaltung

³³ <http://www.heise.de/newsticker/meldung/EU-Kommission-praesentiert-digitale-Agenda-1003476.html>.

1. Welche Chancen und welche möglichen Gefährdungen bringt die digitale Gesellschaft aus soziologischer Perspektive und für den Einzelnen wie für die Gesellschaft und wo besteht hier Handlungsbedarf in den Bereichen Bildung und Medienkompetenz, Daten-, Informations- und Verbraucherrecht, auch um der neuen digitalen Spaltung der Gesellschaft entgegenzuwirken? (*Frage der SPD-Fraktion*)

2. Stellt sich die Frage einer „gerechten Verteilung“ von Rechten an Informationen im Verhältnis zum „Interesse der Gesellschaft“ an einem freien Zugang zu Informationen? Ist die mögliche „Digitale Spaltung“ ein Phänomen, das eher durch staatliches/politisches Handeln abgeschwächt werden kann (so wie z.B. das Zurückdrängen des Analphabetismus durch eine staatliche Bildungs-/Schulpflicht) - oder wird es sich eher ohne staatliche Eingriffe abschwächen (so wie z.B. im Rundfunkbereich - wo wir bei Fernsehgeräten einen Verbreitungsgrad von nahezu 100% haben). (*Frage der FDP-Fraktion*)

Information ist ihrer Natur nach frei verfügbar und auf Verbreitung angelegt. Sie eignet sich daher nur schlecht zur Begründung von Ausschließlichkeitsrechten. Solche Rechte können vielmehr nur sinnvoll begründet werden, wenn ein besonderer Grund für die Gewährung von Ausschließlichkeitsrechten besteht und insofern auch ein klares, nach außen hin eindeutiges Kriterium für die Zuordnung besteht. In dubio pro libertate – jeder Zweifel an der Rechtfertigung eines Informations-Rechtes geht zu Gunsten der Informationsfreiheit. Im Übrigen erweist sich das Immaterialgüterrecht als die Magna Charta der Informationsgesellschaft und damit auch des Informationsrechts. Aufgrund der Tatsache, dass das Bürgerliche Gesetzbuch mit der Fokussierung auf Sachen und Rechten den Bedürfnissen der Warengesellschaft entspricht, ist das bürgerliche Recht als zutiefst überaltet zu bezeichnen. Schon bei Dienstleistungen erweist sich diese klassische Kodifikation des 19. Jahrhunderts als brüchig; auf Informationen kann das BGB nicht reagieren. Hier kommt statt dessen dem Immaterialgüterrecht eine zentrale Bedeutung zu, schützt es doch den Schöpfer und Erfinder mit seinen Ideen sowie für die originelle Auslese und Zusammenstellung von Musik-, Text- oder Bildinformationen. Dabei ist zu beachten, dass Kreativität und Innovation in Auseinandersetzung mit und unter Verwendung von bestehenden Traditionen entsteht. Aus diesem universellen Kulturerbe kann grundsätzlich jeder frei Nutzen ziehen; die Ergebnisse seines Wirkens gehören daher grundsätzlich auch wieder diesem Erbe an. Das Immaterialgüterrecht ist folglich nicht der Grundsatz, sondern die rechtfertigungsbedürftige Ausnahme.

Bedingt durch den Übergang der Waren- und Dienstleistungsgesellschaft hin zu einer Informationsgesellschaft sind Wissen und Informationen marktfähige, wertvolle Güter geworden, um deren Verwertung zahlreiche juristische Konflikte grassieren. Auf der Seite der Rechteinhaber bzw. der Inhaber der relevanten Informationen ist deshalb im Rahmen der nach wie vor rasanten Entwicklung der Softwareindustrie und des Internets sowie vergleichbarer Technologien der Wunsch nach einer Zuweisung von Eigentumsrechten an

Ideen und Inhalten und deren effektive Durchsetzung in das Blickfeld der Öffentlichkeit gelangt. Gleichzeitig besteht aber natürlich auch auf der Kehrseite der Medaille ein Interesse der Öffentlichkeit daran, in unserem informationstechnologischen Zeitalter möglichst unkompliziert und ohne rechtliche Hindernisse auf die weltweit vorhandenen und (theoretisch auch) verfügbaren Informationen zuzugreifen.

Dieser Zielkonflikt wird nach derzeitiger Rechtslage in Deutschland so gelöst, dass die Inhaber von Informationen zwar Schutzrechte für diese erlangen können, allerdings nur unter Beachtung gewisser Interessen der Öffentlichkeit. Auch unterliegen diese Schutzrechte Beschränkungen, wenn ein erhöhtes Interesse der Allgemeinheit an einem (teilweise) freien Zugang zu den Informationen und ihrer Nutzung besteht. Als Schutzregime für Informationen ist dabei insbesondere das Immaterialgüterrecht interessant, namentlich Gesetze wie das Patentgesetz, das Marken- sowie das Urhebergesetz.³⁴

Nach wie vor lässt sich zu dieser Frage aber konstatieren, dass das Spannungsfeld bisher durch den Gesetzgeber zwar reguliert wurde, dies aber gerade vor dem Hintergrund der sprunghaften Entwicklungsschritte in den neuen Medien noch nicht in befriedigender und abschließender Art und Weise geschehen ist. Zu mannigfaltig sind die Konflikte, die sich in diesem Bereich neu stellen oder auch mit anderen Facetten wieder auftauchen.

Als eines der sicherlich prägnantesten Beispiele sei hier die bereits seit Jahren schwelende Debatte um Privatkopien, illegale Downloads und die Kulturfltrate genannt.³⁵ Diese Diskussion geht letztendlich auf genau jene, als Verteilungsgerechtigkeitsproblem empfundene Situation zurück: Es besteht Unzufriedenheit sowohl auf der Seite der Rechteinhaber, welche sich in einer Vielzahl von Fällen in ihren vermögenswerten Ausschließlichkeitspositionen verletzt sehen, als auch von Seiten der Internetnutzer, denen sich die Gründe für die Kriminalisierung von Downloads aus dem Internet nicht erschließen kann und will.

Ein weiteres aktuelles Beispiel ist die Debatte um das geplante Leistungsschutzrecht für Verlage: Hierbei geht es um das Problem, dass in Zeiten des Internets der alte Satz „Die Nachrichten von heute interessieren morgen schon keinen mehr“ nicht mehr gilt; vermehrt greifen andere Anbieter auf die Online-Angebote von Presseverlagen in einer Art und Weise gewerblich zu, die über das bloße Verlinken weit hinausgeht. Die Verleger sehen darin ein Ausnutzen ihrer Leistungen, in die sie investieren mussten. Sie wehren sich daher mit der Forderung nach einem eigenen Leistungsschutzrecht, vergleichbar mit den bereits im Urhebergesetz bestehenden Leistungsschutzrechten, wie dem Recht der Datenbankhersteller gem. §§ 87a ff. UrheberG.³⁶ Diese Begehrlichkeiten gehen aber bereits jetzt schon so weit, dass die Forderung gestellt wird, auch kleinste „Textschnipsel“, wie

³⁴ Siehe weiterführend zu den Problemen des Urheberrechts in der digitalen Gesellschaft *Lehmann*, Die Krise des Urheberrechts in der digitalen Welt, in: Festschrift für Loewenheim, München 2009, S. 167 ff. sowie die „Berliner Rede zum Urheberrecht“ der Bundesjustizministerin vom 14.6.2010.

³⁵ Exemplarisch zur juristischen Dimension der Idee „Kulturfltrate“ *Roßnagel/Jandt/Schnabel*, Kulturfltrate – Ein verfassungsrechtlich zulässiges alternatives Modell zur Künstlervergütung?, MMR 2010, S. 8.

³⁶ Siehe hierzu <http://www.netzpolitik.org/2010/verleger-leistungsschutzrecht-soll-sprache-monopolisieren>.

die Vorschau bei Suchmaschinenergebnissen, in den Schutzbereich dieses Leistungsschutzrechtes einzubeziehen.³⁷ Auf Seiten der Öffentlichkeit besteht in dieser Diskussion daher die durchaus begründete Sorge, dass die aufkeimende neue Informationslandschaft und die Vernetzung von Informationen massiv behindert werden wird. Es ist die Rede von einer Gefahr der „Monopolisierung von Sprache im Internet“.³⁸

Gerade letzteres Beispiel zeigt, dass Bedarf besteht, sich mit diesem Spannungsfeld vor dem Hintergrund der neuen Möglichkeiten, die das Internet und die Digitalisierung seit geraumer Zeit eröffnen, auseinanderzusetzen, alte gesetzliche Strukturen aufzubrechen, sie neu zu überdenken und kreativ und zukunftsweisend in eine von möglichst allen Seiten als befriedigend empfundene Richtung zu verändern.

3. Welche Herausforderungen sehen Sie durch die fortschreitende Digitalisierung aller Lebensbereiche für die Gesellschaft und den Gesetzgeber, und welche Maßnahmen erachten Sie für nötig, um allen Menschen, egal ob jung oder alt, reich oder arm, eine umfassende gleichberechtigte Teilhabe an dieser Entwicklung zu ermöglichen? (*Frage der Fraktion DIE LINKE.*)

4. Welche neuen Formen von Inklusion und Exklusion in Deutschland und der Welt hat das Internet hervorgebracht und welche Maßnahmen auf welchen Ebenen bedarf es, um die digitale Spaltung in Deutschland und weltweit zu verhindern bzw. abzubauen? (*Frage der Fraktion BÜNDNIS90/ Die Grünen*)

Datenschutz

Welche Bedeutung hat der Schutz personenbezogener Daten im Internet auch im Vergleich mit dem Datenschutz in der analogen Welt, welche Entwicklungen können Sie erkennen und wie bewerten Sie diese? (*Frage der Fraktion DIE LINKE.*)

Personenbezogene Daten (§ 3 Abs. 1 BDSG) sind besonders sensible Daten, weil sie einen Rückschluss auf die dahinterstehende natürliche Person zulassen. Gerade das Internet birgt im Vergleich zur analogen Welt größere Gefahren, dass solche Daten an Unbefugte gelangen oder dem Betroffenen schaden können. Die Veröffentlichung im Internet eröffnet einen weltweiten Zugang zu den Daten und macht deren Löschung kaum effektiv möglich. Zwar kann ein Betreiber Daten von der Internetseite nehmen, doch sind sie regelmäßig in Internet-

³⁷ Siehe <http://www.heise.de/newsticker/meldung/Leistungsschutzrecht-soll-Snippets-erfassen-1025613.html>.

³⁸ Ausführlich dazu *Kreutzer*, <http://carta.info/15635/leistungsschutzrecht-fuer-verlage-mehr-schaden-als-nutzen>. Allgemein zum Leistungsschutzrecht für Verleger siehe die Ausarbeitung der Wissenschaftlichen Dienste des Bundestages, abrufbar unter <http://irights.info/fileadmin/texte/material/045-09-A-LeistungsschutzrechtevonZeitungs.pdf>.

archiven weiterhin auffindbar.³⁹ Was einmal im Netz veröffentlicht ist, bleibt auch dort. Zudem ist die Nutzerschaft unsichtbar. Oft fehlt ein Überblick, welche Daten im Internet kursieren. Die persönlichen Daten werden dem eigenen Wirkungskreis entzogen, was ein nicht mehr kalkulierbares Risiko für den Betroffenen zur Folge haben kann und dem informationellen Selbstbestimmungsrecht des einzelnen widerspricht. Eine Schädigung der persönlichen und beruflichen Reputation kann folgen. Jedoch geht es nicht nur um die Gefahren, die durch die Verbreitung von persönlichen Daten entstehen, sondern auch darum, dass der unkontrollierbarer Datenfluss im Internet die Möglichkeit eröffnet, Persönlichkeitsprofile zu erstellen und damit einen tiefen Einblick in die Persönlichkeit zu nehmen.⁴⁰ Die Gefahr des Internet besteht also in seiner Intransparenz und in der wachsenden Verselbstständigung der Datennutzung.

Zu beobachten ist, dass dem Datenschutz in der digitalen Welt eine immer größere Bedeutung zukommt. Digitale Datensammlungen werden immer wichtiger und die Eingriffe immer schwerer. Dies lässt sich an den stetig wachsenden Mitgliederzahlen sozialer Netzwerken festmachen, die immer mehr zu einem festen Bestandteil des Alltags werden und eine Flut von Daten über ihre Nutzer beherbergen. Die Bedeutung des Datenschutzes wird darüber hinaus auch am Beispiel der Vorratsdatenspeicherung deutlich, die das Bundesverfassungsgericht (BVerfG) als einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt“ wertete.⁴¹ Auch die durch die Datenschutzskandale in jüngster Zeit⁴² veranlassten drei BDSG-Novellen verdeutlichen die Bedeutung des Datenschutzes. Allerdings reformierten diese Novellen lediglich kleine Teile. Zu überdenken ist insbesondere die freie und informierte Einwilligung als zentrales Regulativ für den Schutz des Rechts auf informationelle Selbstbestimmung. So ist fraglich, ob durch die Einführung des Opt-In-Verfahrens in § 28 Abs. 3 BDSG eine echte Freiwilligkeit im Internet gewährleistet wird,⁴³ wenn bei den Internetnutzern nicht die nötige Sensibilisierung für die Relevanz des Schutzes ihrer persönlichen Daten besteht und angesichts der die Netzkommunikation prägenden Flut von Daten ein Überschauen der Folgen einer autonomen Entscheidung für die Datenpreisgabe durch den Nutzer kaum möglich ist.

Insgesamt zeigt sich, daß die Frage nach den Grundstrukturen des Datenschutzrechts zu stellen und deren Adäquanz zu prüfen ist. Paßt das Datenschutzrecht mit seiner Bindung an den Personenbezug für digitale Verarbeitung von Geodaten, IP-Adressen etc? Müßte nicht der Personenbezug als Prüfkriterium aufgegeben und statt dessen eine übergreifende Informationsordnung geschaffen werden, wie dies Wilhelm Steinmüller, der Nestor des Datenschutzrechts, schon 1970 forderte?

Green IT

³⁹ Zur internationalen Zuständigkeit bei persönlichkeitsrechtsverletzenden Inhalten in Online-Archiven siehe BGH, NJW 2010, S. 1752.

⁴⁰ Härting, Datenschutz im Internet - Gesetzgeberischer Handlungsbedarf, BB 2010, S. 839, 840.

⁴¹ BVerfG, NJW 2010, S. 833 Rn. 210.

⁴² Vgl. Bundesbeauftragter für Datenschutz und Informationsfreiheit (BfDI), 22. Tätigkeitsbericht 2007–2008, S. 16.

⁴³ Kutscha, Mehr Datenschutz - aber wie?, ZRP 2010, S. 112.

Wie lässt sich über das Bestehende hinaus ganzheitliche nachhaltige Green-IT realisieren (Stichworte: öffentliche Beschaffung, Entsorgung, Arbeitsbedingungen, Produktionsketten)? (Frage der Fraktion DIE LINKE.)

Internationale Strukturen

1. Das „Internet“ ist ein von nationalstaatlichen Grenzen unabhängiges Medium. Wenn man betrachtet, dass es zum einen Länder wie Deutschland gibt, die eine sehr hohe Regeldichte haben (Jugendschutz, Datenschutz, Verbraucherschutz) und zum anderen solche Länder, in denen solche Vorgaben von untergeordneter Bedeutung sind - welches „Regel“-Modell wird sich langfristig eher durchsetzen? Gibt es innovative Regelungs- und Kooperationsansätze, die es dennoch in dem internationalen Kontext erlauben, wirksam gestaltenden Einfluss auf Entwicklungen im Internet zu nehmen? (Frage der FDP-Fraktion)

Den Nationalstaaten stehen zwei regulatorische Grundkonzepte zur Verfügung, um auf den internationalen „Sachverhalt Internet“ zu reagieren: einerseits die autonom-nationale Rechtsetzung, und andererseits die grenzüberschreitende Regelung, Rechtsdurchsetzung und Kooperation. Das kooperative, transnationale Konzept kommt bislang vorwiegend in wirtschaftlichen Sachgebieten zur Anwendung, da es wirtschaftspolitisch geboten ist, den grenzüberschreitenden Handel zu fördern und Handelsbarrieren abzubauen. Das erstgenannte, national-autonome Konzept dagegen kommt traditionell bei elementaren ordnungspolitischen und ethischen Themen zur Anwendung.

Das wichtigste transnationale Kooperationsgefüge, die Europäische Union, ist – auch nach dem Vertrag von Lissabon – immer noch ganz vornehmlich eine Wirtschaftsgemeinschaft. Die Wirtschaftspolitik ist das Vehikel der europäischen Integration. Wesentliche Teile nationaler Regelungsgewalt in wirtschaftlichen Fragestellungen wurden von den Mitgliedstaaten unwiderruflich auf die Union übertragen. Jedoch enden die Befugnisse der Gemeinschaft regelmäßig bei den ordnungspolitischen Kernfragen und bei übergeordneten nationalen Interessen (sog. *ordre public*). Beispielsweise beschränken die europäischen (wirtschaftlichen) Grundfreiheiten nicht das Recht der Mitgliedstaaten, ordnungspolitische Kernbereiche autonom zu regeln. Die Arbeitnehmerfreizügigkeit aus Art. 45 Abs. 3 AEU, das Niederlassungsrecht aus Art. 49 AEU und die Freiheit des Kapital- und Zahlungsverkehrs aus Art. 63 AEU tasten nicht das Recht der nationalen Gesetzgeber an, Vorschriften zum Schutz der öffentlichen Ordnung, Sicherheit oder Gesundheit zu erlassen. Die Maßnahmen zum Schutz dieser Rechtsgüter sind wertungsabhängig, betreffen grundlegende Aufgaben der nationalen Staatsgewalt und unterliegen daher mit gutem Grund keinen europarechtlichen Beschränkungen.

Die „personenschützenden“ Rechtsgebiete Jugendschutz, Datenschutz und Verbraucherschutz betreffen gesellschaftspolitische Kernfragen, so dass man davon ausgehen müsste,

dass sie tendenziell in der Autonomie der nationalen Gesetzgeber verbleiben. Gleichwohl hat in diesen Fragen – zweckmäßigerweise – eine Teilübertragung von Befugnissen auf die EU stattgefunden, wenn auch in unterschiedlichem Maße. Der Verbraucherschutz ist auf europäischer Ebene durch zahlreiche Rechtsakte zu einem guten Teil harmonisiert. Dies ist sinnvoll, denn der europäische Verbraucherschutz ist wirtschaftlicher Verbraucherschutz. Auch beim Datenschutz liegen elementare Regelungskompetenzen bei der EU, denn Art. 16 AEU (ehemals Art. 286 EG) gibt dem europäischen Gesetzgeber die Befugnis zum Erlass von Vorschriften über den Schutz personenbezogener Daten. Einzig für den Jugendschutz hat die Gemeinschaft keine zentrale Normgebungskompetenz. Der Jugendschutz wird lediglich als Randmaterie in bestimmten Gebieten mit geregelt, beispielsweise in der Richtlinie über audiovisuelle Mediendienste.

Es gibt in den drei elementaren ordnungspolitischen Bereichen Jugendschutz, Datenschutz und Verbraucherschutz kein „Regelungskonzept“, das gegenüber anderen Regelungssystemen eindeutig überlegen wäre und sich daher langfristig durchsetzen würde. Den Kampf der Regelungssysteme kennt man beispielsweise aus dem Wirtschaftsrecht: So bieten sich viele Staaten einen Wettlauf um die liberalsten gesellschaftsrechtlichen Regelungssysteme, um Gesellschaftsgründungen in ihren Territorien attraktiver zu machen. Auch geringe Steuersätze können ein Werkzeug im Wettbewerb der Staaten um Kapitalzuflüsse sein. In den Bereichen Jugendschutz, Datenschutz und Verbraucherschutz wird es hingegen keinen Wettbewerb der Staatsgewalten um besonders niedrige („race to the bottom“) oder besonders hohe Schutzniveaus geben. Vielmehr sorgt sich jeder Staat um den Schutz und die Rechte seiner Bürger, die den jeweiligen Internetangeboten ausgesetzt sind.

Der nationale Gesetzgeber muss daher zunächst klären, inwieweit internationale Vorgaben bestehen. In den vorigen Abschnitten wurde bereits erläutert, dass der Verbraucherschutz stark, der Datenschutz teilweise und der Jugendschutz nur peripher gemeinschaftsrechtlich vorbestimmt sind. Sofern nationaler Spielraum/Freiraum besteht, stellt sich die Frage, welches Schutzniveau gewünscht wird. Soweit in den drei Rechtsgebieten nationale Gestaltungsspielräume oder -freiräume bestehen, wurde in der Bundesrepublik in der Tat ein im Vergleich zu anderen Staaten hohes Schutzniveau geschaffen. Schließlich muss erörtert werden, wie dieses Schutzniveau insb. auch gegen internationale Störfaktoren durchgesetzt werden kann. Besonders im Falle autonomer nationalstaatlicher Regelungen (wie beispielsweise im Jugendschutz), aber auch dort, wo die nationalstaatlichen Regelungen über verbindliche internationale Mindeststandards hinausgehen (wie beispielsweise die deutschen Vorschriften zum Datenschutz), ist die zentrale Frage, wie das nationale Schutzniveau gegen schädigende, sprich: rechtsverletzende internationale Einflüsse abgesichert werden kann. Sowohl im Hinblick auf den Jugendschutz, als auch den Datenschutz und den Verbraucherschutz erzeugt das Internet eine äußere Gefährdungslage. Das nationale Schutzniveau kann von Angeboten, die nicht dem Zugriff der deutschen Behörden unterliegen, unterlaufen werden.

Es gibt grundsätzlich zwei Ansätze, um auf diese internetspezifischen transnationalen Gefährdungslagen für das nationale Schutzniveau zu reagieren. So kann man das Internet

abschotten (mögliche Werkzeuge: Geotargeting und Sperrverpflichtungen) oder versuchen, durch internationale Kooperationen (mögliches Werkzeug: Staatsverträge) eine Rechtsdurchsetzung zu erleichtern.

Ein wesentliches, häufig unterbewertetes Werkzeug zur nationalen Rechtsdurchsetzung im Internet ist das sog. Geotargeting (Geolocation, Geolokalisation). Beim Geotargeting werden IP-Adressen den Nutzerstandorten zugeordnet, so dass bestimmte Angebote im Web für die jeweiligen Nutzer gezielt gesperrt oder verfügbar gemacht werden können.⁴⁴ Während in der allgemeinen Diskussion das Geotargeting früher oftmals als unzuverlässig abgetan wurde, ist heute weitgehend anerkannt, dass diese Methode eine hohe Wirksamkeit erreichen kann.⁴⁵ Deutsche Gerichte betrachten die Lokalisation zunehmend als zumutbares Mittel der territorialen Einschränkung von Internetangeboten.⁴⁶ Die Methode kann theoretisch auch dazu eingesetzt werden, Personen vor Angeboten zu „schützen“, die gegen bestimmte nationale Schutzvorschriften (zum Beispiel Jugendschutz, Datenschutz, Verbraucherschutz) verstoßen. Zusätzlich zur Methode des Geotargeting können die in Deutschland tätigen Provider theoretisch verpflichtet werden, bestimmte Angebote nicht zu verbreiten (Sperrverpflichtungen). Dass solche Verpflichtungen breite Ablehnung und Widerstand in der Bevölkerung hervorrufen können, zeigte allerdings das Beispiel des Zugangerschwerungsgesetzes.⁴⁷ In der Tat bergen Infrastrukturen für die Domain-Name-System (DNS)-Filterung die Gefahr des Fehlgebrauchs und Missbrauchs (Vorwurf der Zensur). Gleiches dürfte auch für das Geotargeting gelten, so dass bei der „Abschottung“ zur Sicherung des nationalen Schutzniveaus in jedem Falle sorgfältige Abwägungen erforderlich wären. Jede Art von Inhaltsbeschränkung im Internet erzeugt erfahrungsgemäß scharfen Gegenwind. Darüber hinaus ist die Vollstreckung von Verfügungen gegen ausländische Provider nach wie vor schwierig.⁴⁸

Ein bedeutsames Beispiel für die internationale Kooperation als Reaktion auf internetspezifische Gefährdungslagen sind die Entwürfe für das Anti-Piraterie-Abkommen „ACTA“⁴⁹, an dem sich zahlreiche große Industrienationen beteiligen wollen. Internationale Kooperationen sind die Alternative zur territorialen Abschottung, können gleichwohl in Sachen Eingriffsintensität ebenso heikel sein wie national begrenzte Sperrungen.

2. Wird dem Datenschutz in allen Bevölkerungsgruppen der gleiche Stellenwert eingeräumt oder ergeben sich insoweit Unterschiede (Alter, Bildungsniveau, Geschlecht, ethnische Herkunft etc.)? Gibt es ein Spannungsfeld zwischen dem persönlichen Bedürfnis nach Sicherheit in Anonymität und dem gesellschaftlichen Bedürfnis nach Sicherheit durch Offenheit? Wie bewerten Sie die Möglichkeiten die das neue Internetprotokoll IPv6 bezüglich der Priorisierung von Datenpaketen bietet - insbesondere im Hinblick auf das Prinzip

⁴⁴ Ausführlich *Hoeren*, Geolokalisation und Glücksspielrecht, ZfWG 2008, S. 229; *ders.*, Zoning und Geolocation - Technische Ansätze zu einer Reterritorialisierung des Internet, MMR 2007, S. 3.

⁴⁵ *Hoeren*, *ibid.*

⁴⁶ Aktuell OVG Münster, MMR 2010, S. 350; VGH München, NVwZ-RR 2009, S. 202.

⁴⁷ Dazu siehe auch die Ausführungen im Abschnitt „Regulierung“ Frage 5.

⁴⁸ Winkelmüller/Kessler, Territorialisierung von Internet-Angeboten – Technische Möglichkeiten, völker-, wirtschaftsverwaltungs- und ordnungsrechtliche Aspekte, GewA 2009, 181.

⁴⁹ Dazu siehe auch die Ausführungen im Abschnitt „Regulierung“ Fragen 1 und 5.

der Netzneutralität? Stellt sich die Frage einer Neuordnung des Haftungsrechts im Hinblick auf Internet-Intermediäre (z.B. WLAN-Betreiber; Sharehoster; Admin-C; Access Provider)? Wie lässt sich eine Neuordnung international erreichen? (*Frage der FDP-Fraktion*)

Jeder Internetnutzer legt Wert darauf, dass seine Daten vertraulich behandelt werden. Er möchte sich möglichst anonym im Internet bewegen und keine Spuren hinterlassen. Log- und Verbindungsdaten sollen nicht gespeichert werden. Doch nicht jedes Bedürfnis nach Anonymität des Einzelnen ist im Einzelfall auch gerechtfertigt. Zu differenzieren ist hier vor allem im Hinblick auf die Verfolgung von Straftaten im Internet, die sich meist nur aufklären lassen, indem durch den Access-Provider gespeicherte Verbindungsdaten zum Täter führen. Eine Speicherung auf Vorrat ist nach dem Urteil des BVerfG⁵⁰ lediglich in seiner damaligen gesetzlichen Ausgestaltung verfassungswidrig. Die Vorratsdatenspeicherung selbst zum Zweck der Datennutzung durch staatliche Behörden, um schwere Straftaten zu ermitteln, festzustellen und zu verfolgen, ist hingegen legitim. Zugleich wird damit auch der Gesellschaft das Bedürfnis zugestanden, Daten zu speichern und beispielsweise zur Aufklärung von Straftaten wie Kinderpornographie zu nutzen. Aber auch ein Zugriff auf Daten zur zivilrechtlichen Inanspruchnahme beispielsweise bei Filesharing oder sonstigen Urheberrechtsverletzungen werden von der Gesellschaft als notwendig angesehen, um die unter dem Deckmantel der Anonymität im Internet begangenen Rechtsverletzungen zu ahnden. Wann das Recht des Einzelnen auf Anonymität und das Bedürfnis der Gesellschaft nach Sicherheit überwiegt, ist im Rahmen der Verhältnismäßigkeit zu beurteilen. Demnach gibt es ein Spannungsfeld zwischen dem persönlichen Bedürfnis nach Anonymität und dem gesellschaftlichen Bedürfnis nach Sicherheit durch Offenheit.

Zum Thema Netzneutralität siehe die Ausführungen im Abschnitt „Regulierung“ Fragen 1 und 4.

Provider sind die Hauptakteure im Internet. Zu ihnen gehören Access-Provider, Host-Provider und Content-Provider. Die rechtliche Verantwortlichkeit von Providern ist im TMG geregelt. Das TMG ist seit dem 1.3.2007 in Kraft und beruht auf der E-Commerce-Richtlinie (ECRL).⁵¹ In § 7 Abs. 1 unterscheidet das TMG zwischen fremden und eigenen Informationen. Diensteanbieter sind nach § 7 Abs. 1 TMG nur für eigene Inhalte nach den allgemeinen Gesetzen verantwortlich. Für fremde Informationen sind sie grundsätzlich nicht verantwortlich. Das bedeutet, dass der Betreiber für eigene Informationen haftbar gemacht werden kann, für fremde jedoch grundsätzlich nicht. Dabei reglementiert § 8 TMG diese Haftungserleichterung zu Gunsten der Access-Provider und §§ 9 und 10 TMG zu Gunsten der Host-Provider. Content-Provider haften in den meisten Fällen vollumfänglich, da sie regelmäßig eigene Inhalte zur Verfügung stellen. Für fremde Inhalte sollen auch Content-Provider nicht haften.

⁵⁰ BVerfG, NJW 2010, S. 833.

⁵¹ Richtlinie 2000/31/EG des Europäischen Parlamentes und des Rates vom 8.6.2000, ABl. EG Nr. L 178, S. 1 v. 17.7.2000.

Von der gesetzlichen Haftungsfreistellung nicht umfasst sind nach (falscher und europarechtswidriger) Auffassung des BGH Unterlassungs- und Beseitigungsansprüche. Das wird aus der Regelung des § 7 Abs. 2 S. 2 TMG gefolgert. Hierdurch wird durch die Hintertür doch eine Haftung der Provider für fremde Inhalte eröffnet. Diese Haftung läuft regelmäßig auf eine Überprüfung fremder Inhalte auf deren Rechtswidrigkeit und eine eventuelle Sperrung oder Löschung der fremden Inhalte durch die Provider hinaus. Im Vorgängergesetz des TMG, dem Teledienstegesetz (TDG) war ein Hinweis auf die technische Möglichkeit und wirtschaftliche Zumutbarkeit einer Sperrung enthalten. Ein solcher Hinweis fehlt im TMG. Das ist äußerst problematisch, weil daraus geschlossen werden könnte, dass Provider uneingeschränkt zur Sperrung rechtswidriger Inhalte verpflichtet sind, was zu einer ausufernden Haftung von Providern führen kann. Dieser ist dann u. U. zu einer umfassenden Prüfung der fremden Inhalte verpflichtet. Deutlich wurde das Problem der ausufernden Haftung in einem Urteil des OLG Hamburg⁵² zu markenrechtsverletzenden Angeboten bei eBay. Die Richter nahmen in diesem Urteil umfassende vorbeugende Prüfungspflichten des Auktionshauses an. Auch wenn der BGH⁵³ einen geringeren Prüfungsmaßstab anlegt, verdeutlicht dies die herrschende Unsicherheit in diesem Bereich. Zudem wird der in Art. 15 ECRL niedergelegte Grundsatz ausgehöhlt, nach dem Providern keine allgemeinen Überwachungspflichten auferlegt werden dürfen. Provider stehen aber nicht nur der Bewältigung der Überwachung von fremden Inhalten gegenüber, sondern befinden sich durch evtl. Sperrverpflichtungen zudem in einer Pattsituation. Sperrt der Provider die entsprechenden Inhalte nicht, haftet er gegenüber dem Rechteinhaber, der eine Verletzung geltend macht; Sperrt er einen zulässigen Inhalt, drohen ihm Schadensersatzforderungen seines Vertragspartners. Zudem können Überwachungspflichten vor allem bei Internetforen der grundgesetzlich geschützten Meinungsfreiheit entgegenstehen. Hinsichtlich des § 7 Abs. 2 S. 2 TMG ist mithin eine Änderung dringend erforderlich. So könnte die Norm um einen Hinweis auf die technische Möglichkeit und wirtschaftliche Zumutbarkeit einer Sperrung ergänzt werden, wie er bereits im TDG enthalten war.

Ein besonderes Problem stellt auch die Haftung für das Setzen von Hyperlinks bzw. das Betreiben von Suchmaschinen dar. Diese Dienste lassen sich nicht eindeutig einer Kategorie des TMG, also Access-, Host oder Content-Provider zuweisen. Hier könnte deshalb überlegt werden, die gesetzlichen Normen entsprechend zu ergänzen.

Neben der Haftung der Provider nimmt auch die Haftung des sog. Admin-C eine bedeutende Rolle im Haftungsrecht ein. Der Admin-C ist der bei der DENIC eingetragene administrative Ansprechpartner einer Domain. Seine Verantwortlichkeit ist nicht im TMG geregelt. Eine Haftung des Admin-C wird regelmäßig im Rahmen einer mittels einer Domain begangenen Namens-, Marken- oder Wettbewerbsverletzung diskutiert. Dabei ist die Rechtsprechung in diesem Bereich konträr. Während einige Gerichte eine Störerhaftung des Admin-C ablehnen⁵⁴, bejahte das OLG Koblenz kürzlich eine solche⁵⁵. Dies

⁵² OLG Hamburg, WRP 2008, S. 1569.

⁵³ BGH, NJW 2004, S. 3102.

⁵⁴ OLG Köln, MMR 2009, S. 48; OLG Düsseldorf, MMR 2009, S. 336; OLG München, MMR 2010, S. 261.

⁵⁵ OLG Koblenz, MMR 2009, S. 549.

führt zu einer enormen Rechtsunsicherheit in diesem Bereich. Allerdings ist mittlerweile ein Verfahren zur Haftung des Admin-C beim BGH anhängig (Az. I ZR 150/09). Es darf also auf eine höchstrichterliche Klärung in diesem Bereich gehofft werden. Eine Neuordnung erscheint daher gegenwärtig nicht notwendig.

Da das TMG auf der ECRL beruht, kann eine Neuordnung, soweit sie von der Richtlinie abweicht, nur aufgrund einer geänderten Richtlinie erfolgen. Die hier angeregte Neuordnung stimmt allerdings mit der Richtlinie im Wesentlichen überein, so dass eine internationale Neuordnung nicht erforderlich ist.

3. Bedarf es angesichts der Internationalität des Internets neuer oder internationaler Strukturen? (*Frage der Fraktion BÜNDNIS90/Die Grünen*)

In Großbritannien existiert seit 2002 eine zentrale Medienaufsichtsbehörde (Regulation and Wettbewerbsaufsicht) mit der Bezeichnung „Ofcom“ (Office of Communications), die Schweiz hat mit dem BAKOM (Bundesamt für Kommunikation) ebenfalls eine zentralisierte Behörde. In Deutschland hingegen sind die medien- und telekommunikationsrechtlichen Aufsichtsstrukturen nach wie vor zersplittert.⁵⁶ Bundesweite Aufsichtsstrukturen sind nach deutscher Verfassungslage schwer zu realisieren.⁵⁷ Sieht man von den unwahrscheinlichen Szenarien einer Verfassungsänderung oder einer staatsvertraglichen Lösung zur Schaffung einer zentralen deutschen Medienaufsichtsbehörde ab, wird die deutsche Medienregulierung auch in Zukunft vielgestaltig und dezentralisiert bleiben. Eine Bündelung der nationalen Befugnisse wäre aber der erste Schritt zur Zentralisierung der medienrechtlichen Aufsicht, der einer internationalen Zentralisierung voraus gehen sollte.

Die Schaffung internationaler Strukturen für die Medienaufsicht wäre aber auch aus anderen Gründen ein wenig erfolgversprechendes Vorhaben. Es ist allein schon fraglich, mit welchen Sachgebieten eine solche Behörde betraut sein sollte. Eine „europäische Kommunikationsbehörde“ mit vergleichbaren Befugnissen wie der Ofcom oder dem BAKOM müsste durch Änderungen der EU-Verträge mit ganz erheblichen Kompetenzen ausgestattet werden, die bislang aus gutem Grund bei den Mitgliedstaaten verblieben sind. Denn bei der Medienaufsicht geht es um viele unterschiedliche Sachgebiete, die schon für sich betrachtet erhebliche wirtschaftliche sowie gesellschaftspolitische Bedeutung haben, wie beispielsweise die Teilgebiete Telekommunikationsregulierung (Netzregulierung) und Rundfunkregulierung (Inhaltsregulierung). Jedes Teilgebiet müsste im Detail betrachtet werden.

Nach derzeitiger Kompetenzverteilung zwischen der Europäischen Gemeinschaft und den Nationalstaaten käme nur im Telekommunikationsrecht eine weitergehende Zentralisierung von Aufsichtskompetenzen, bis hin zur Schaffung zentraler Behörden, in Betracht. Mit den Richtlinien 2009/136/EG und 2009/140/EG wurde die Einrichtung eines neuen

⁵⁶ Holznapel/Ricke, Die Aufsicht im Internet - Wer hat noch nicht, wer will noch mal?, MMR 2008, S. 18.

⁵⁷ Thaenert, Nochmals zur Reform der Medienkontrolle durch den Zehnten Rundfunkänderungsstaatsvertrag, ZUM 2009, S. 131.

Gremiums Europäischer Regulierungsstellen für Telekommunikation (GEREK) beschlossen. Dem Gremium gehören die nationalen Regulierungsstellen aller 27 Mitgliedsstaaten an. Verbraucherrechte und ein fairer Wettbewerb sollen damit ausgebaut werden. Die GEREK löst die bisherige Gruppe europäischer Regulierungsstellen (ERG) ab, die als lose Gruppierung nationaler Regulierungsbehörden nur einstimmig handeln konnte und nicht in den EU-Regulierungsprozess eingebunden war. Das neue Gremium soll eine einheitliche Regulierung in ganz Europa sicherstellen und damit den Wettbewerb im Telekom-Binnenmarkt stärken.

Die Rundfunkregulierung hingegen ist, weil sie neben dem wirtschaftlichen auch einen starken kulturellen Hintergrund hat, nach wie vor überwiegend nationale Angelegenheit. Die Schaffung zentraler „Internetregulierungsbehörden“ oder internationaler Medienaufsichtsbehörden liegt also in weiter Ferne.

Eine andere Frage ist die Aufsicht über den Kern der technischen Infrastruktur des Internet, des Domain Name Systems (DNS).⁵⁸ Hier gab und gibt es anhaltende Diskussionen über eine Reform oder eine Ablösung der ICANN. Seit dem 1.10.2009 regelt der neue Vertrag mit dem US-Handelsministerium nun, dass ICANN sich regelmäßig mit internationalen Vertretern besetzten Gremien stellen muss. Dabei muss ICANN mindestens alle drei Jahre Rechenschaft über die Vertragsmäßigkeit seiner Arbeit ablegen.

⁵⁸ Dazu siehe auch die Ausführungen im Abschnitt „Regulierung“ Frage 1.