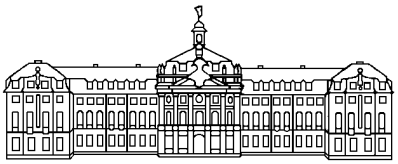

WESTFÄLISCHE WILHELMS-UNIVERSITÄT MÜNSTER
Institut für Informations-, Telekommunikations- und Medienrecht (ITM)
- Öffentlichrechtliche Abteilung -
Direktor: Prof. Dr. Bernd Holznagel, LL.M.

Stellungnahme für die öffentliche Anhörung „Von der Industrie- zur Wissensgesellschaft: Wirtschaft, Arbeitswelt und Recht, Privatisierung und Patentierung von Wissen“ Montag, 8. Oktober 2001

Ich beschränke meine Stellungnahme auf die Fragen 2.17. bis 3.4. und 3.6. bis 3.9. Zu Frage 3.10. ist auf die BT-Drucksachen zur Anhörung des Unterausschuss Neue Medien des Deutschen Bundestages „Expertengespräch Cyber-Crime / TKÜV“ am Donnerstag 05. Juli 2001 zu verweisen.

2. Von der Industrie zur Wissensgesellschaft: Auswirkungen, Probleme und Handlungsfelder in Bezug auf die Arbeitswelt und die Bildungssysteme

2.17. Skizzieren Sie die wichtigsten Merkmale der so genannten „Digitalen Spaltung“ (digital divide) in Nutzer und Nichtnutzer der neuen IuK-Technologien auf nationaler, europäischer und internationaler Ebene. In welchem Zusammenhang steht der digital divide dabei mit anderen gesellschaftlichen Indikatoren wie allgemeiner sozialer Kontext, wirtschaftliche Situation, Bildungsniveau u.a.?

Als Digital Divide wird die Spaltung derjenigen in der Gesellschaft, die Zugang zu Informationen und neuen Technologien haben, von denjenigen, die hierbei außen vor bleiben, bezeichnet. „Negatives Charakteristikum“ des Digital Divide ist es vor allem, dass die Vorzüge des Internet nicht von jedermann in gleicher Weise genutzt werden. Das Internet ist derzeit ein Medium, das immer noch überwiegend – wenngleich auch in

einem abnehmenden Maße – von jungen, gut ausgebildeten und gut verdienenden Menschen in Anspruch genommen wird. Der Digital Divide ist ein international – jedoch in unterschiedlichem Maße – zu beobachtendes Phänomen.

Deutschland liegt bei der Internetnutzung im internationalen Vergleich zurück. So liegt der Anteil der Bevölkerung mit einem privaten Internetzugang mit derzeit 38,8 Prozent (ARD/ZDF Online-Studie 2001, Stand: Mai/Juni 2001) unter dem europäischen Durchschnitt. Gegenüber den USA ist der Rückstand noch deutlicher: Mehr als doppelt so viele Menschen sind dort bereits an das weltweite Datennetz angeschlossen.

Ein Ausschluss vieler aus der Cyberwelt ist nicht akzeptabel, wenn immer mehr der vom Staat oder von der Wirtschaft angebotenen Dienstleistungen online abgewickelt werden. Die Abwendung eines „digital divide", einer Aufspaltung der Bevölkerung in einen Teil, der die neuen digitalen Techniken nutzt, und in einen Teil, der sie nicht nutzt oder ihnen gar ablehnend gegenüber steht, ist heute eine zentrale Herausforderung für Politik, Wirtschaft und Wissenschaft.

Die Ursachen des digital divide sind vielfältig und stehen in unmittelbarem Zusammenhang mit gesellschaftlichen und wirtschaftlichen Faktoren. Zunächst lässt sich hier eine bestimmte Technikscheu oder gar Technikfeindlichkeit als typische E-Barrier anführen. Oft fehlt es auch einfach an dem notwendigen Internet-Know-How und der Möglichkeit, sich dies ohne zu hohen Kosten- und Zeitaufwand anzueignen. Daher ist es für viele Menschen gar nicht abschätzbar, inwiefern sie die Onlineangebote für ihre Interessen optimal einsetzen könnten. Ihnen fehlen die nötigen Fertigkeiten, mit der Zugangstechnologie und dem neuen Medium umzugehen. Ursächlich für diesen Missstand ist die oftmals komplizierte Bedienungsweise der Technik sowie der Umgang mit den Inhalten des Mediums. Das Internet bietet eine unüberschaubare Fülle an Informationen und Webseiten, so dass sich Ungeübte leicht in dem Medium „verlieren" und durch dessen Vielfalt abgeschreckt werden können. Notwendig sind daher gezielte Schulungsmaßnahmen, die Grundfertigkeiten im Umgang mit dem Internet vermitteln. Diese Ausbildung mit und an dem Medium muss bereits in der Schule beginnen.

Das Internet wird auch noch nicht in allen sozialen Schichten gleichermaßen intensiv genutzt. Noch immer ist der Internet-Nutzer überwiegend männlich, hat eine höhere Bildung und verdient ein überdurchschnittliches Einkommen.

Von zentraler Bedeutung dürften schließlich die vergleichsweise hohen Telefonkosten sein, die derzeit für die Internetnutzung anfallen. Diese Kosten wirken sich unmittelbar zeitabhängig auf die Internetkosten aus. In Europa mangelte es insbesondere lange an günstigen Pauschaltarifen für die Internetnutzung. Erfahrungen aus anderen Ländern

belegen, dass durch eine pauschalisierte Abrechnung der Internetgebühren die Nutzungsintensität gesteigert werden kann. Zudem wird für die Teile der Bevölkerung, die bislang noch keinen Internetzugang hatten, ein Anreiz geschaffen, da dann die von der tatsächlichen Inanspruchnahme unabhängigen Kosten klar kalkulierbar sind. Hemmend auf die Verbreitung des Internet in Deutschland wirken sich auch die Preise für die Hardware aus. Derzeit ist für einen Internetzugang ein vollwertiger Personal-Computer mit entsprechender Kommunikationshardware notwendig.

Als Hindernisse einer vermehrten Internetnutzung lassen sich darüber hinaus das mangelnde Vertrauen in die Sicherheit und Verlässlichkeit von Onlinetransaktionen sowie die Befürchtung anführen, dass persönliche Daten „abgehört" und missbraucht werden. Dieser Gesichtspunkt hat gerade in den letzten Wochen sicher wieder an Bedeutung gewonnen. In der Cyberworld gibt es zahlreiche Instrumente, die das Ausspionieren von persönlichen Daten erleichtern (mobile Agenten oder Cookies) und die Auswertung von Datenbeständen (Datamining) optimieren können. Viele Verbraucher haben daher die Befürchtung, dass von ihnen Persönlichkeitsprofile erstellt werden, die später zu ihrem Nachteil z.B. für gezielte Werbeaktionen eingesetzt werden. Eine moderne Datenschutzgesetzgebung hat neben der Sicherung des Rechts auf informationelle Selbstbestimmung auch die Aufgabe, Vertrauen zu schaffen und für Nutzerakzeptanz zu sorgen. Auch können die Unternehmen selbst „Gütesiegel" einführen, mit denen sie einen sensiblen Umgang mit persönlichen Daten garantieren.

Die Akzeptanz des Internet insbesondere bei älteren Menschen wird auch durch die Dominanz von Angeboten in fremden Sprachen und Kulturen im Netz behindert. So sind derzeit ca. 77 Prozent aller Internetseiten in englischer Sprache verfasst, lediglich 2,3 Prozent aller vorhandenen Internetseiten sind auf Deutsch. Da Länder- und Sprachgrenzen im Internet nicht existieren und die Gewichtung nicht gezielt verändert werden kann, bietet sich eine noch stärkere Regionalisierung und Bündelung von Angeboten des eigenen Kultur- und Sprachkreises an. Dies könnte durch Werbung für Suchmaschinen, die auf deutsche Angebote spezialisiert sind, oder durch die Einrichtung besonderer Portale geschehen. Auch hier könnten staatliche Institutionen als Vorbild vorangehen und z.B. die Zugänglichkeit ihrer Angebote durch die Errichtung eines Deutschland.de-Portals verbessern. Die Programme der öffentlich-rechtlichen Rundfunkanstalten könnten mit solchen Angeboten verzahnt werden.

Diese Faktoren führen insgesamt dazu, dass der Anteil der Internetnutzer in den einzelnen Bevölkerungsgruppen divergiert. Die Teilnahme am Internet ist abhängig von den klassischen Faktoren Alter, formaler Bildungsgrad und Berufstätigkeit. Ein Durchbruch des Internet in allen Bevölkerungsschichten dürfte erst erfolgen, wenn mit der Konvergenz der Endgeräte die Handhabung des Internet so leicht wird wie die

Handhabung einer Fernbedienung und vor allem, wenn die Noch-Nicht-Nutzer den realen Nutzwert des Mediums für sich erkennen.

2.18. Welche Erkenntnisse gibt es hinsichtlich der unterschiedlichen Nutzungsweise der neuen IuK-Techniken durch Männer und Frauen? Welche spezifischen Unterschiede gibt es, welche Ursachen haben diese und welche aktuellen Entwicklungstendenzen sind zu berücksichtigen?

Das Verhältnis von Frauen und Männern bei der Internetnutzung hat sich seit zunehmender Verbreitung des Mediums stark geändert. Während vor fünf Jahren überwiegend Männer online waren, richteten in den vergangenen Jahren vermehrt Frauen einen Internetanschluss ein. So sind heute die männlichen Internetnutzer im Durchschnitt schon 39 Monate im Netz, die weiblichen erst seit 28 Monaten. Noch immer sind Internet-NutzerInnen aber vorwiegend männlich, wobei aber der Frauenanteil in den letzten Jahren deutlich gesteigert werden konnte. Der Frauenanteil liegt derzeit bei 41 Prozent aller Onlinenutzer. Demgegenüber sind bereits 59 Prozent der Männer online (ARD/ZDF-Onlinestudie 2001). Ursache dieses Phänomens dürfte vor allem die Technikscheu und mangelndes Internet-Know-How bei Frauen sein. Dennoch ist zu erwarten, dass sich die Internetnutzung durch Männer und Frauen – insbesondere in der heranwachsenden Generation – weiter annähert. Spezielle Schulungsmaßnahmen für Frauen können hierzu beitragen.

2.19. Welche Risiken birgt die digitale Spaltung der Gesellschaft allgemein und insbesondere für die wirtschaftliche Entwicklung? Welche Gegenmaßnahmen sind sinnvoll oder sogar erforderlich, um die digitale Spaltung zu überwinden oder zumindest zu verringern?

Die Nutzung des Internet durch breite Bevölkerungskreise und damit die Vermeidung eines „digital divide" ist eine wichtige Voraussetzung dafür, dass die Bundesrepublik den Wandel von einer Industrie- zu einer Wissens- und Informationsgesellschaft vollzieht und hierbei nicht in einen schwer aufholbaren Entwicklungsrückstand etwa zu den Vereinigten Staaten, Skandinavien und Großbritannien gerät. Wirtschaftliche Transaktionen werden zukünftig in erheblichem Maße im Internet stattfinden. Dies zeigt sich vor allem an der Geschwindigkeit, mit der Produkte und Dienstleistungen im Netz angeboten und abgewickelt werden. Aber E-Mail-Dienste, Diskussionsforen sowie

Wahlen und Abstimmungen via Internet bieten auch Perspektiven einer neuen Art von Kommunikation in der Demokratie. In diesem Bereich gewinnen die neuen Informations- und Kommunikationstechniken ebenfalls zunehmend an Bedeutung und sollten mittelfristig ausgebaut werden. E-Government kann so zu einem Mittel gegen Partei- und Politikverdrossenheit werden. Hinzu kommt, dass sich die neuen Medien schon jetzt für die dringend benötigte Verwaltungsmodernisierung einsetzen lassen. Steuererklärungen, die Anmeldung eines neuen Wohnsitzes, die Bestellung von Tickets für eine kommunale Veranstaltung – all dies kann online abgewickelt werden.

In den westlichen Demokratien gibt es eine lange Tradition, für eine angemessene Versorgung der Bevölkerung mit Kommunikationsdiensten und die hierfür erforderliche Infrastruktur zu sorgen. So fordert das Bundesverfassungsgericht für den Rundfunksektor in ständiger Rechtsprechung, dass die unerlässliche Grundversorgung durch öffentlich-rechtliche Anstalten gewährleistet werden muss. Diese Aufgabe umfasst technische Aspekte ebenso wie die „Preisgestaltung" und die Gewährleistung inhaltlicher Programmqualität. Im Bereich der Telekommunikation hat der Staat einen Infrastruktursicherungsauftrag, zu dessen Erfüllung er ebenfalls durch verfassungsrechtliche Vorgaben (Art. 87 f GG) verpflichtet ist. Hier geht es primär darum, Sprachtelefonie und Übertragungswege flächendeckend und zu einer bestimmten technischen Qualität anzubieten.

Diese Gewährleistungen müssen vom Grundanliegen her in das digitale Zeitalter übertragen werden. An einem überzeugenden Gesamtkonzept hierfür fehlt es jedoch noch. Vorzugswürdig erscheint ein funktionaler Ansatz, der dynamisch weiterentwickelt werden kann. Er muss diejenigen Dienste definieren, die für die Versorgung der Bevölkerung unerlässlich sind, und darf nicht von vornherein auf die Festlegung bestimmter Übertragungstechniken oder Anbietergruppen beschränkt sein. Eine Politik, die sich dem Ziel der Schaffung einer Informationsgesellschaft für alle verpflichtet fühlt, wird dabei vor allem die folgenden Prinzipien in Rechnung stellen müssen:

Verfügbarkeit

Die erforderlichen Dienste müssen in jeder Region des Landes verfügbar sein. Die Bürger sollten eine größtmögliche Auswahl unter den verschiedenen Übertragungswegen und Endgeräten haben. Staatliche Initiativen könnten in diesem Zusammenhang auch technische Systeme (Endgeräte, Set-Top-Boxen, Übertragungsplattformen) unterstützen, die für die Angebote aller Wettbewerber „offen" sind.

Erschwinglichkeit

Die Angebote sollen zu erschwinglichen Preisen nutzbar sein. Für gewisse Gruppen in der Gesellschaft kann es dabei notwendig sein, die Internetkosten für ausgewählte Dienste überproportional zu senken, um die Zugangsraten zu maximieren.

Qualitätssicherung

Schon die Vorgaben für die Grundversorgung mit Rundfunk oder die Universaldienstverpflichtung im Bereich der Sprachtelefonie zeigen, dass eine E-Versorgung auch eine qualitative Dimension aufweisen muss. Dies gilt sowohl in Bezug auf die Art der angebotenen Dienste (z.B. aus den Bereichen Erziehung, Gesundheit und öffentliche Sicherheit) wie auch im Hinblick auf die Schnelligkeit und Bandbreite der Übertragungswege. Darüber hinaus muss gewährleistet sein, dass Onlinetransaktionen sicher und unter Wahrung datenschutzrechtlicher Grundsätze abgewickelt werden können.

Medienkompetenz

Die Umsetzung der zuvor genannten Prinzipien muss Hand in Hand mit der Schaffung und Verbesserung von Medienkompetenz erfolgen. Auch muss auf die neuen Möglichkeiten des Internet durch öffentlichkeitswirksame Aktionen aufmerksam gemacht werden.

2.20. Welche Maßnahmen, die eine Förderung der IuK-Nutzung für bestimmte gesellschaftliche Gruppen zum Ziel haben, gibt es und wie bewerten Sie deren Erfolgsaussichten? Welche weiteren Maßnahmen halten Sie für sinnvoll?

Public Access Points

In Anlehnung an die Vorschläge des Ministerkomitees des Europarates kann die Versorgung gerade sozial schwächerer Bevölkerungsgruppen mit neuen Informationsdiensten auch in der Bundesrepublik Deutschland durch so genannte „Public Access Points" verbessert werden, also öffentliche Stellen, an denen dem einzelnen die Internetnutzung ermöglicht wird. Die nähere Ausgestaltung des verfassungsrechtlichen Infrastruktursicherungsauftrages nach Art. 87 f Abs. 1 GG

nimmt § 17 TKG vor. Danach sind Universaldienstleistungen ein Mindestangebot an Telekommunikationsdienstleistungen für die Öffentlichkeit, für die eine bestimmte Qualität festgelegt ist und zu denen alle Nutzer unabhängig von ihrem Wohn- oder Geschäftsort zu einem erschwinglichen Preis Zugang haben müssen. Als derartige Universaldienstleistungen sind gem. § 17 Abs. 1 Satz 2 TKG insbesondere Telekommunikationsdienstleistungen zu bestimmen, die den Bereichen des Sprachtelefondienstes und des Betreibens von Übertragungswegen zuzuordnen sind. Welche konkreten Dienste nun in der Bundesrepublik im Rahmen des Universaldienstes angeboten werden müssen, legt wiederum die von der Bundesregierung auf Basis von § 17 Abs. 2 TKG erlassene Telekommunikations-Universaldienstverordnung fest. § 1 der Verordnung nennt derzeit den Sprachtelefondienst in einem digital vermittelnden Netz mit einer bestimmten Bandbreite im Teilnehmeranschlussbereich sowie zugehörigen ISDN-Leistungsmerkmalen. Außerdem sind verschiedene Telekommunikationsdienst-leistungen anzubieten, die in unmittelbarem Zusammenhang mit dem Sprachtelefondienst stehen, wie Auskunftsdienste, Teilnehmerverzeichnisse und öffentliche Telefonstellen. Darüber hinaus gilt das Angebot bestimmter leitungsgebundener Übertragungswege als Universaldienstleistung. Es erscheint allerdings zweifelhaft, ob das in der Universaldienstverordnung festgeschriebene Mindestangebot heute noch ausreicht. Möglicherweise haben sich die an einen Universaldienst zu stellenden qualitativen Anforderungen dergestalt geändert, dass auch neue Informations- und Kommunikationsdienste wie der kostengünstige, breitbandige Zugang zum Internet in den staatlichen Gewährleistungsauftrag fallen. Angesichts der zunehmenden Bedeutung des Internet ist es de lege ferenda zunächst erwägenswert, „Public Access Points" – vergleichbar der flächendeckenden Bereitstellung von öffentlichen Telefonstellen an allgemein und jederzeit zugänglichen Standorten – in den Umfang des Infrastruktursicherungsauftrages mit einzubeziehen. Außerdem könnte die Versorgung der Schulen mit Internetterminals in den Kanon der Universaldienstverpflichtungen aufgenommen werden.

Ausbildungsmaßnahmen und weitere Nutzungsanreize

Flankierend ist das Internet-Know-How in allen Bevölkerungskreisen zu steigern. Zukünftig wird es eine wichtige Aufgabe etwa des öffentlich-rechtlichen Rundfunks und der Volkshochschulen sein, Kenntnisse im Umgang mit den neuen Medien zu vermitteln. Weitere Nutzungsanreize ließen sich schaffen, indem z.B. eine online eingereichte Steuererklärung oder eine via Internet durchgeführte Anmeldung zu einer kostenpflichtigen kommunalen Veranstaltung mit einer Prämie vergütet werden. Zudem wären Steuererleichterungen für PC-Hersteller zu erwägen, die in besonderer Weise für Behinderte und ältere Menschen tauglich sind. Die Aufmerksamkeit der Bevölkerung für

Fragen der Mediennutzung ließe sich schließlich durch einen nationalen Internettag steigern. Auch ist an die Schaffung eines Fonds (Digital Citizen Fonds) zu denken, mit dem der Zugang zu bestimmten Diensten (z.B. Gesundheitsangeboten) für ausgewählte gesellschaftliche Gruppen finanziert wird.

Senkung der Nutzungskosten

Um das Wachstum der Internet-Wirtschaft zu beschleunigen und in den vollen Genuss seiner positiven gesamtwirtschaftlichen Auswirkungen zu kommen, muss die Internetnutzung vor allem für jedermann finanziell erschwinglich sein. Es kann die Senkung der Internetkosten durch eine alternative Abrechnungs- und Vergütungsmethode erfolgen. Eine quantitative Steigerung und qualitative Verbesserung der Internetnutzung durch Wirtschaft und Bevölkerung ist möglich, wenn die Kosten sich nicht länger nach der zeitlichen Länge der Verbindung richten, also taktgebunden nach Gebühreneinheiten berechnet werden. Als neues Tarifmodell kommen hier so genannte Flatrates in Betracht. Dies sind taktunabhängige monatliche Nutzergebühren, bei denen der Kunde Internetdienste gegen Entrichtung eines Festpreises zeitunabhängig, d.h. ohne Entstehung getakteter Telefonkosten je Verbindungsdauer, nutzen kann. Erfahrungen aus den USA haben gezeigt, dass eine Flatrate die Internetnutzung erheblich intensiviert. Auch in Deutschland gibt es bereits Versuche, derartige Preismodelle einzuführen. Ein echter Durchbruch ist hier allerdings noch nicht erfolgt. Entweder sind die monatlichen Kosten immer noch zu hoch, oder die Angebote sind mit weiteren Verpflichtungen verbunden, beispielsweise der gleichzeitigen Inanspruchnahme anderer Dienste des Anbieters. Regulatorische oder zumindest politische Maßnahmen des Staates können hier geeignetere Rahmenbedingungen schaffen.

Wettbewerb der Netze

Zur Übermittlung von Daten aus dem Internet dient in Deutschland derzeit beinahe ausschließlich die analoge Nutzung des schmalbandigen Fernsprechnetzes oder die digitale Datenübertragung via ISDN-Technik. Die Übertragung dauert dabei zum einen wegen der begrenzten Bandbreite sehr lange, zum anderen fehlt der Wettbewerb zwischen verschiedenen Infrastrukturen.

Qualität und Quantität der Internetnutzung lassen sich einerseits durch Ausbau und Aufrüstung des herkömmlichen Fernsprechnetzes verbessern, indem über die bereits vorhandenen Telefonleitungen „Always-On"-Internetzugänge mittels DSL-Technik (Digital Subscriber Line) flächendeckend etabliert werden. Auf diese Weise lässt sich die Übertragungskapazität des gängigen Telefon-Kupferkabels auf ein Vielfaches der

bisherigen ISDN-Bandbreite von 64 Kilobit pro Sekunde steigern. So sind bei ADSL (Asymmetric Digital Subscriber Line) schon heute Downstreamgeschwindigkeiten von bis zu acht Megabit pro Sekunde möglich, dem 125fachen einer einfachen ISDN-Verbindung. Digital Subscriber Lines sind als pauschal abgerechnete Standleitungen konzipiert und lassen somit die Einwahlprozedur entfallen. Auch erfordert diese alternative Form des Zugangs vom Online-Nutzer ein Minimum an Investitionsaufwand und garantiert durch die digitale Übertragungstechnik hohe Datenraten.

Eine leistungsfähige Alternative zur Übertragung via analogem oder digitalem Telefonnetz liegt auch in der Verbreitung des Internet über das Breitband-(Fernseh)Kabelnetz. Im breitbandigen Netz können Internetangebote aufgrund einer Minimierung der Übertragungszeiten erheblich komfortabler genutzt werden. Zudem wird die Verbreitung neuartiger, auf größere Kapazitäten und Schnelligkeit angewiesener Dienste möglich. Hinzu kommt, dass in diesem Netz ebenfalls kein taktgebundener Tarif, sondern ein monatlicher Pauschalpreis berechnet wird. Die Bundesrepublik befindet sich hier zudem in einer äußerst günstigen Ausgangslage, da bereits über 60% der Haushalte an das Kabelnetz angeschlossen sind. Für eine effiziente Nutzung dieser Infrastruktur sollte das Netz als offene Plattform ausgestaltet sein und alle Dienste und Angebote diskriminierungsfrei übertragen. Für die Internetverbreitung via Kabelnetz ist lediglich ein Rückkanal erforderlich, um die bidirektionale Datenübertragung zu ermöglichen, und das Netz muss insgesamt leistungsfähiger gemacht werden, was bei einem gewissen Investitionsaufwand aber technisch ohne weiteres möglich ist. Problematisch erscheint allerdings, dass das gesamte deutsche Breitbandkabelnetz ursprünglich im Eigentum der Deutschen Telekom AG stand. Es bleibt abzuwarten, ob sich mit der Veräußerung des Kabelnetzes an dritte Netzbetreiber (z.B. Callahan und Liberty Media) nunmehr echter Wettbewerb zu anderen internetfähigen Netzen einstellen wird.

Noch im Entwicklungsstadium befindet sich die Datenübertragung über das Stromnetz. Erste Versuche lieferten jedoch sehr gute Ergebnisse, was die Übertragungsgeschwindigkeit und die Zuverlässigkeit betrifft. Wenn weiterhin mit Hochdruck an der Entwicklung einer solchen alternativen Zugangsform gearbeitet wird und ein marktfähiges Produkt entsteht, bietet der Internetzugang über das in jedem Haushalt verfügbare Stromnetz eine wertvolle Alternative zu den bisherigen Zugangsmöglichkeiten.

Maßnahmenbündelung in einer Task Force „Informationsgesellschaft für alle:"

Schon gegenwärtig gibt es zahlreiche staatliche Initiativen, um die Internetnutzung zu erhöhen und eine Informationsgesellschaft für alle zu schaffen. Jedoch sind diese

Aktivitäten häufig nur unzureichend aufeinander abgestimmt. Gerade in der Bundesrepublik ist der Koordinierungsbedarf wegen der unterschiedlichen Bund-Länder-Kompetenzen besonders hoch. Daher erscheint es sinnvoll, diese Fragen in einer die verschiedenen Ministerien übergreifenden Task Force „Informationsgesellschaft für alle" aufzuarbeiten. Hierbei sollte es sich um eine offene Arbeitsgruppe handeln, die gemeinsam mit der Wissenschaft die zentralen Problemstellungen abarbeitet. Sie könnte bei einem E-Beauftragten der Bundesregierung angesiedelt sein. Dieser müsste verpflichtet werden, jährlich über den Fortschritt Deutschlands auf dem Weg in die Informationsgesellschaft zu berichten. In einem solchen Gremium wäre auch zu ermitteln, inwiefern eine intensive Zusammenarbeit zwischen der Bundesrepublik und anderen europäischen Staaten in diesem Bereich anzustreben ist. Aufgabe der Task Force wäre es neben der kurz- und mittelfristigen Umsetzung eines bestimmten Maßnahmenkataloges schließlich, langfristige Visionen und Strategien für die weitere Entwicklung der Informationsgesellschaft zu formulieren, um die Gefahr eines deutschen Rückstands auf diesem Gebiet auf lange Sicht zu bannen.

3. Von der Industrie- zur Wissensgesellschaft: Auswirkungen, Probleme und Handlungsfelder in Bezug auf Recht und Cyberlaw

3.1. Wo sehen Sie die wesentlichen Anforderungen an das Recht? Wie ist der Stand und wo liegen die wesentlichen Probleme?

Anforderungen

Information und Recht

Es wurde und wird der Eindruck erweckt, in regulatorischer Hinsicht könne der Wandel von der Industriegesellschaft zur Informationsgesellschaft mit einem neuen „Cyberlaw" für das Internet bewältigt werden. Eine solche Sichtweise erfasst aber nicht die eigentliche Dimension des gesellschaftlichen Wandels, der mit der revolutionären Entwicklung der Informationstechnik verbunden ist.

Wenn es stimmt, dass Industrieanlagen, Operationssäle und Wohnhäuser mit Informationstechnik gesteuert werden, Information zu einem ubiquitären Gut wird, das an jedem Ort der Welt jederzeit verfügbar ist und die Menge an personenbezogenen Daten, die in staatlichen oder privaten Datenbanken gespeichert werden, ständig

zunimmt und immer unüberschaubarer wird. Dann kann es nicht nur darum gehen, (rechtliche) Spielregeln für den neuen Sozialraum, den Cyberspace, zu definieren. Vielmehr muss der „Informationierung" der Gesellschaft durch eine „Informationierung" des Rechts Rechnung getragen werden. Dies bedeutet zunächst, dass im ganz Grundsätzlichen untersucht werden muss, wie „Information" an sich zum Gegenstand des Rechts gemacht werden kann bzw. gemacht werden muss. Es stellt sich die Frage, inwieweit der vorhandene rechtliche Rahmen zu reformieren ist und ob – wie auf dem Deutschen Juristentag 1998 vorgeschlagen – ein „Informationsgesetzbuch" eine mögliche Antwort auf den Reformbedarf darstellen könnte.

Strukturen für einen Selbstschutz der Netzbürger

Das Staatsverständnis hat sich – augenfällig an Privatisierungstendenzen in allen Bereichen staatlichen Handelns – grundlegend geändert. Der Staat der Informationsgesellschaft erfüllt die staatlichen Aufgaben häufig nicht mehr selbst. Stattdessen übernimmt er eine Auffang- oder Gewährleistungsverantwortung dafür, dass Gemeinwohlziele durch den Beitrag privater Akteure erreicht werden. Daneben werden Steuerungsmöglichkeiten durch die zunehmende Globalisierung von der nationalstaatlichen auf die internationale Ebene verlagert. Schließlich wird der Staat in den globalen IuK-Netzen mit – nicht zuletzt technisch bedingten – „Ohnmachtserfahrungen" konfrontiert. Das Recht muss diesen Steuerungsverlusten (national)staatlicher Vorgaben Rechnung tragen bzw. der Staat muss seinen Steuerungsanspruch reduzieren. Dies bedeutet primär, dass der Staat Strukturen schafft, die seine Bürger zum Selbstschutz ertüchtigen. Betroffen sind insbesondere Bereiche wie Datenschutz, Schutz der Privatsphäre, Verbraucherschutz und IT-Sicherheit.

Rechtliche Rahmensetzung und Koregulierung

Auf der anderen Seite ist zu sehen, dass der (National-)Staat nach wie vor unter allen gesellschaftlichen Akteuren die alleinige Größe mit Neutralitätsanspruch bleibt, die – nicht zuletzt aufgrund des Gewaltmonopols – verbindliche, gemeinwohlorientierte, Entscheidungen durchsetzen kann. Das Recht der Informationsgesellschaft muss daher einen Rahmen und die grundlegenden Strukturen (Rahmen- und Strukturverantwortung) vorgeben. Aus der Beschränkung auf die Setzung rechtlicher Rahmenvorgaben folgte im Umkehrschluss, dass der Gesetzgeber auf übermäßige Detailregelungen verzichtet. Die in manchen Rechtsgebieten herrschende „Hyptertrophie des Rechts" muss beseitigt werden. Das Recht sollte einfacher werden.

Das Recht muss insbesondere die schnelle technologische Entwicklung adaptieren können. Hierzu kann es sinnvoll sein, rechtliche Regelungen regelmäßigen Evaluierungen (nach dem Vorbild des IuKDG) zu unterwerfen oder/und Gesetze mit „Verfallsdaten" zu versehen. Dabei sollte immer der Schutz der Verbraucher bzw. Nutzer im Vordergrund stehen. Dazu gehört auch, dass behördliche Strukturen und Zuständigkeiten– etwa im Rahmen von E-Government – transparenter bzw. überhaupt bekannt gemacht werden müssen: wer weiß schon, dass z.B. überwiegend die Bezirksregierungen über die Einhaltung des TDG wachen?

Sinnvoll erscheint es schließlich, das Konzept der Rahmengebung und Selbstregulierung um den von EU-Kommissionsmitglied ErkkiLiikanen vorgestellten Ansatz der Koregulierung zu ergänzen. Bei der Koregulierung arbeiten öffentlicher Sektor, Industrie und Verbraucherorganisationen zusammen, um praxisgerechte Regelungen für bestimmte Problembereiche (z.B. e-confidence, alternative Streitschlichtungsverfahren, Notice and take down-Verfahren, illegale Inhalte) zu erstellen. Dies könnte etwa so ablaufen, dass die Politik der Industrie und den Verbraucherorganisationen bestimmte Regelungsfelder vorgibt. In diesen Bereichen schlagen dann die privaten Player Richtlinien und Empfehlungen vor, wie der jeweilige Regelungsgegenstand (z.B. Notice and take down-Verfahren) einer Regulierung zugeführt werden könnte. Diese Vorschläge werden anschließend vom Gesetzgeber geprüft und in geeigneter Form rechtsverbindlich umgesetzt.

Globaler Minimalkonsens

Schließlich müssen – ggf. neue – Rechtsstrukturen bzw. Rechtssetzungmechanismen gefunden werden, die fähig sind, ein „globale Spielregeln" zu entwickeln, die in der Lage sind, die Unterschiede der verschiedenen Rechtstraditionen und –kulturen zu überwinden und in bestimmten Kernbereichen einen Minimalkonsens herzustellen. Die ordnungspolitischen Aufgaben und Ziele einer globalen Informations- und Kommunikationsregulierung sind im Grundsatz bereits aus der „Offline-Welt" bekannt: auch in einer globalen IuK-Kultur muss es um die Sicherung eines fairen Wettbewerbs, Datenschutz, den Schutz von Jugendlichen und Verbrauchern und die Gewährleistung von Meinungsvielfalt gehen – um nur einige Regelungsfelder zu nennen. Nicht die Regulierungsziele, sondern die Instrumente zu ihrer Erreichung müssen also an die neuen tatsächlichen Gegebenheiten angepasst werden.

Derzeitiger Stand

Auf nationaler Ebene ist das Recht, das im Cyberspace betroffen ist, schon in weiten Teilen an die neuen Verhältnisse angepasst worden (Beispiele: Elektronische Signaturen, Abschaffung von Rabattgesetz und Zugabeverordnung, Anpassung der Vergabeverordnung, Urheberrecht im Bereich der Datenbanken, Strafgesetzbuch, Fernabsatzgesetz) In der Überarbeitung befinden sich das Teledienstegesetz und das Teledienstedatenschutzgesetz (durch das Artikelgesetz zum Elektronischen Geschäftsverkehr), der Mediendienstestaatsvertrag, der Jugendschutz, das Verwaltungsverfahrensgesetz und das Urheberrecht. Außerdem befindet sich das neue Gesetz über den Schutz von zugangskontrollierten Diensten und Zugangskontrolldiensten im Gesetzgebungsverfahren.

Auf europäischer Ebene ist in den vorgenannten Bereiche durch eine Reihe von harmonisierenden Einzelmaßnahmen die Etablierung einer europäischen Marktordnung für den elektronischen Geschäftsverkehr bereits recht weit voran geschritten. Dies gilt insbesondere für Regelungsfelder wie den Datenschutz, Elektronische Signaturen, Verbraucherschutz und Elektronischer Geschäftsverkehr, und die grenzüberschreitende Rundfunkordnung, in denen die entsprechenden Europäischen Richtlinien bereits umgesetzt sind oder derzeit noch umgesetzt werden. Die Richtlinie über Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft wird wesentlich zur weiteren Harmonisierung im Bereich des Urheberrechts beitragen; die Umsetzungsfrist läuft hier bis Dezember 2002. In Bezug auf die Harmonisierung im Bereich der Vollstreckung in Zivilsachen vgl. unten **Frage 3.2.** Abgesehen davon, dass in bestimmten Einzelfragen noch weiterer Regelungsbedarf besteht, fehlt es an einer Harmonisierung vor allem im Wettbewerbsrecht, teilweise im Bereich des Jugendschutzes und im Strafrecht. In den letztgenannten Bereichen liegen bisher vornehmlich Kommissions-Mitteilungen (COM(96)487; COM(96)483; COM(2000) 890), aber noch keine Vorschläge für legislative Instrumente vor. Verbindliche, durchsetzbare Regelungen existieren hier praktisch noch nicht. Und auch von einem europaweiten oder gar globalen Cyber-Strafrecht kann noch längst nicht gesprochen werden. Hier wird jedoch die Cybercrime-Konvention des Europarates viele Lücken schließen.

Anknüpfend an ihre Vorreiterrolle bei der technischen und ökonomischen Entwicklung des Internets waren die U.S.A. den Europäern bei der Etablierung einer Marktordnung für den Electronic Commerce um einiges voraus. Den Grundstein bildete insoweit ein Rahmenprogramm der U.S.-Regierung vom Juli 1997. Die U.S.-amerikanischen Ansätze unterscheiden sich durchweg durch ihren liberaleren Ansatz von den Europäischen Regulierungsinitiativen. Dies zeigt sich z.B. bei der elektronischen Signatur, wo die U.S.A. in ihrem „E-Sign Act" weitgehend auf technische Vorgaben für

elektronische Signaturen verzichtet hat. Von einer Harmonisierung der beiden Rechtskreise kann insgesamt nicht die Rede sein. Hier wird die teilweise noch ausstehende technische Standardisierung und Normierung eine entscheidende Rolle spielen. Die Frage, ob sich die U.S.-Lösung oder der Europäische Ansatz am Markt durchsetzen wird, kann deshalb derzeit nicht beantwortet werden.

Handlungsempfehlung:

Die Arbeit der internationalen technischen Standardisierungsgremien sollte im Sinne des Europäischen Ansatzes weiter gefördert werden, um möglichst schnell entsprechende Standards dem Markt zur Verfügung stellen zu können und somit das Europäische Modell global durchzusetzen.

Das Internet betrifft jedoch einen Wirtschaftsraum, der weit über die Grenzen dieser beiden Rechtskreise hinaus geht. Damit ist die Frage nach globalen Regelungen zum Electronic Commerce gestellt. Hier fällt auf, dass ernstzunehmende verbindliche Regelungsinitiativen bislang nur punktuell vorhanden sind. Dies gilt insbesondere für die traditionellen Player globaler Politik, allen voran die UNO. Über ihre Unterorganisationen hat sie sich zwar Teilen des zu bewältigenden Regelungsbedarfs angenommen, so etwa über die WIPO, in deren „Digital Agenda" den Fragen des weltweiten Schutzes von Urheberrechten und des geistigen Eigentums durch den WIPO Copyright Treaty (WCT) und den WIPO Performances and Phonogramms Treaty (WPPT), die überarbeitete Regelungen über den Schutz von Datenbanken und Computerprogrammen enthalten, nachgegangen wird. Auch sei auf den WIPO-Domain Name Process sowie das TRIPS der WTO verwiesen. Die UN-Handelsorganisation UNCITRAL schließlich erstellt ein – freilich unverbindliches – Modell-Gesetz für den Electronic Commerce. Insgesamt hat das Urheberrecht, selbst in Bereichen des Urheberpersönlichkeitsrechts, durch internationale Urheberrechtsverträge wie die Berner Übereinkunft bereits ein beachtliches Maß an Harmonisierung erreicht.

Auch OECD und G-8 sind hinsichtlich des globalen Electronic Commerce tätig geworden. Seitens der OECD gibt es eine ganze Reihe von – rechtlich unverbindlichen – Richtlinien, die sich mit Kryptografie, Datensicherheit und Verbraucherschutz beim elektronischen Geschäftsverkehr befassen. Die G-8-Gruppe dagegen hat sich insbesondere mit Fragen des Cybercrime auseinander gesetzt. Hierzu wurde schon 1996 die so genannte Carnegie-Gruppe für rechtliche und technische Fragen etabliert. Anlässlich ihres Gipfels in Berlin im Oktober 2000 haben die G-8-Staaten ihre einheitliche Position im Kampf gegen die internationale Computerkriminalität abermals bekräftigt. All diesen Maßnahmen fehlt jedoch die Verbindlichkeit. Sie wirken allenfalls

im Verhältnis zu den Mitgliedsstaaten, und auch diesen steht etwa bei der OECD ein Veto-Recht zu. Beachtet werden müssen auf der Ebene der weltweiten Regulierung allerdings auch die Initiativen von Industriezusammenschlüssen wie dem Global Business Dialogue on Electronic Commerce (dazu Frage 3.8). Sie sind zwar ebenfalls nicht in der Lage, aus eigener Kraft einen verbindlichen Marktrahmen zu etablieren. Schon aufgrund ihrer personellen Zusammensetzung – im Global Business Dialogue etwa finden sich die Führungskräfte von Konzernen wie Bertelsmann und AOL/Time Warner zusammen – sollte ihr Einfluss auf politische Entscheidungsprozesse aber nicht unterschätzt werden.

Wesentliche Probleme

Das eigentliche Problem liegt in der Rechtsdurchsetzung (dazu unten 3.2.) sowie der Harmonisierung des Rechts. Dabei müssen unterschiedliche Rechtstraditionen und -kulturen (etwa der angelsächsische Rechtskreis einerseits und das kodifizierte dem romanischen Rechtskreis entstammende kontinentaleuropäische Recht andererseits), divergierende Werteordnungen sowie verschiedene wirtschaftspolitische und staatstheoretische Ansätze miteinander in Einklang gebracht werden. Dies kann letztendlich nur auf einen Minimalkonsens in den wichtigsten Kernbereichen des Rechts hinauslaufen (s.o.).

3.2. Wie beurteilen Sie allgemein die Möglichkeiten und Probleme der nationalen, europäischen und auch internationalen Rechtsdurchsetzung in globalen Informations- und Kommunikationsnetzwerken?

Die Rechtsdurchsetzung im Cyberspace sieht sich mit folgenden Grundproblemen konfrontiert:

a) fehlendes Know How, Personal und Equipment bei den staatlichen Behörden;
b) mangelnde Identifizierung eines Rechtssubjektes;
c) Unsicherheit bei der Frage, welches Recht anwendbar ist;
d) komplizierte und langwierige Vollstreckung von gerichtlichen oder behördlichen Entscheidungen im Ausland;
e) unzureichende länderübergreifende Zusammenarbeit im Bereich von Ermittlungsmaßnahmen.

Ad a)

Der erstgenannte Punkt ist kein rechtliches Problem. Er dürfte jedoch vor allem in Bereichen wie dem Datenschutzrecht und der Strafverfolgung einer der Hauptgründe für Vollzugsdefizite sein.

Ad b)

Der zweite Punkt betrifft das Problem der Anonymität im Internet. Es existieren Anonymisierungstechniken, die die absolute Anonymität eines Internetnutzers gewährleisten können (Beispiel An.on – ein vom BMWi gefördertes Projekt des unabhängigen Datenschutzzentrums Schleswig-Holstein). Inwieweit diese von Kriminellen tatsächlich genutzt werden, ist jedoch unklar. Bei einer Studie über das Anonymisierungs-Projekt JANUS, an der der Verfasser beteiligt war, stellte sich jedenfalls heraus, dass der Anonymisierungsdienst nur sehr selten zu illegalen Zwecken verwendet wurde. Spektakuläre Fälle wie der Loveletter-Virus oder Mafiaboy, die aufgeklärt wurden, scheinen ebenfalls dafür zu sprechen, dass Anoymisierungsdienste die Arbeit der Behörden zwar erschweren aber nicht unmöglich machen. Demgegenüber ist der Nutzen, den die Anonymisierungsdienste für den Datenschutz und die Privatspähre im Cyberspace bieten, von erheblichem Wert. Forderungen, die „Anonymität des Internets" aufzuheben, sind deshalb mit größter Vorsicht zu genießen.

Handlungsempfehlungen:

1. ***Es sollte ein grundsätzliches Recht auf anonymen oder pseudonymen Zugang und Nutzung von Netzangeboten anerkannt werden (s. Mitteilung der EU-Kommission KOM(2000)890 endgültig, Ziff. 5.3.)***

2. ***Es sollte im Rahmen einer Studie geprüft werden, ob und in welchem Umfang Anonymisierungsdienste bei Cybercrime genutzt werden bzw. ob und falls ja, welche Delikte wegen der „anonymen" Verhältnisse im Internet nicht aufgeklärt werden können.***

Ad c)

Grundsätzlich finden auf Rechtsgeschäfte im Internet die Regelungen des Internationalen Privatrechts Anwendung. Vorrangig gelten völkerrechtliche Vereinbarungen wie z.B. das UN-Kaufrecht. Insgesamt ist die kollisionsrechtliche Situation im Internet für den Dienstanbieter und den Verbraucher oftmals unklar. Gerade im Bereich des Verbraucherschutzrechtes und Wettbewerbsrechtes tritt das sog. „Overspill-Risiko" hinzu: der Anbieter läuft Gefahr, einer Vielzahl von

Rechtsordnungen unterworfen zu sein. Dies führt im E-Commerce zu erheblicher Rechtsunsicherheit. Eine gewisse – auf das Gebiet der EU beschränkte – Lösung wird hier das Herkunftslandprinzip der E-Commerce-Richtlinie bringen. Zudem hat die EU-Kommission einen Vorschlag für eine Überarbeitung der Rom-Konvention von 1980 vorgelegt, um die Regelungen über die Anwendbarkeit des Rechts in Vertragsangelegenheiten an die Erfordernisse des E-Commerce anzupassen. Bis Ende 2001 wird zudem ein Kommissionsvorschlag für eine Verordnung über die Anwendbarkeit des Rechts in außervertraglichen Angelegenheiten erwartet (sog. Rom II Instrument), die u.a. die Probleme im Bereich des unlauteren Wettbewerbs lösen soll. Diesen Ansätzen fehlt bislang jedoch weitgehend ein Pendant auf internationaler Ebene.

Ad d)

Das Europäische Zivilverfahrensrecht beruhte auf zwei Konventionen, nämlich dem Brüsseler Gerichtsstands- und Vollstreckungsübereinkommen und dem Luganer Gerichtsstands- und Vollstreckungsübereinkommen. Ergänzend war das Haager Zustellungsabkommen heranzuziehen. Im Jahr 2000 wurden im Bereich der justiziellen Zusammenarbeit in Europa einige Neuerungen eingeführt, die zu deutlichen Verbesserungen bei der Vollstreckung (zivil)gerichtlicher Entscheidungen führen sollten. Für den Bereich des E-Commerce ist hierbei insbesondere die Verordnung (EG) Nr. 244/2001 des Rates vom 22. Dezember 2000 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (EuGVVO-Brüssel I) von Bedeutung, die am 1. März 2002 in Kraft treten wird. Ergänzt wird diese Verordnung durch die Verordnung (EG) Nr. 1348/2000 des Rates vom 29. Mai 2000 über die Zustellung gerichtlicher und aussergerichtlicher Schriftstücke in Zivil- oder Handelssachen in den Mitgliedstaaten, die am 31. Mai 2001 in Kraft getreten ist.

Die vorstehenden Verordnungen bilden die Grundlage für die internationale und grenzüberschreitende Forderungsbeitreibung in der Europäischen Union und haben auch Auswirkungen auf den grenzüberschreitenden Rechtsverkehr mit Drittstaaten. Gleichwohl fehlen auf internationaler Ebene vergleichbare Ansätze.

Handlungsempfehlung zu c) und d):

Auf internationaler Ebene sollten die Arbeiten der United Nations Commission on International Trade Law (UNCITRAL) forciert werden und ggf. ein Abkommen erarbeitet werden, dass die Vorgaben der E-Commerce Richtlinie, der Brüsseler Konvention und der Rom bzw. Rom II Konvention – jedenfalls für den Bereich des E-Commerce – auf globalem Level anderen Staaten zugänglich macht.

Ad e)

Im Bereich der Strafverfolgung waren die Rechtshilfeverfahren bislang vor allem auf bilaterale Kooperationen beschränkt. Am 29. Mai 2000 hat der Justiz- und Innenrat der EU das Europäische Rechtshilfeabkommen verabschiedet. Dieses Abkommen wird eine effektivere polizeiliche Zusammenarbeit bei Ermittlungen ermöglichen. Die Cybercrime-Konvention des Europarates baut zum Teil auf diesem Abkommen auf. Es kann erwartet werden, dass beide Regelungswerke die Rechtshilfeverfahren in Strafsachen insgesamt deutlich vereinfachen und beschleunigen werden. Auf internationaler Ebene haben zudem die G-8 bereits im Jahr 1997 die Arbeitsgruppe High Tech-Kriminalität eingerichtet. In deren Rahmen wurde eine „24h-Kontakttruppe" gegründet, die auf der Grundlage von zwei – rechtlich unverbindlichen – Regelwerken recht effektiv Rechtshilfe betreibt. Die Mitgliedsstaaten sind bestrebt, den Kreis der beteiligten Staaten über die G-8 auszudehnen und arbeiten auch mit internationalen Organisationen wie Interpol und dem Europarat zusammen. Insgesamt scheint dieser Bereich der faktischen Rechtshilfe schon weiter fortgeschritten zu sein als dies oftmals von der Öffentlichkeit wahrgenommen wird. Freilich darf nicht übersehen werden, dass noch ein erheblicher Bedarf an Harmonisierung im materiellen Strafrecht und bei den strafprozessualen Eingriffsbefugnissen besteht. Hier wird jedoch die Cybercrime-Konvention weitere Lücken schließen.

3.3. Welche Probleme stellen sich hinsichtlich des Wettbewerbsrecht? Welche Anforderungen ergeben sich für den Datenschutz, den VerbraucherInnenschutz, die Datensicherheit, der IT-Sicherheit und den Schutz der Privatsphäre und wie beurteilen Sie den Stand auf nationaler, europäischer und internationaler Ebene?

Verglichen mit anderen Ländern sind in Deutschland im Bereich des Wettbewerbsrechts, des VerbraucherInnenschutzes, des Datenschutzes Regeln vorhanden, die ein relativ hohes Schutzniveau etablieren. Während im Bereich des Datenschutzrechtes auf europäischer Ebene inzwischen ein einigermaßen einheitliches Schutzniveau implementiert wurde, kann hiervon im Bereich des Wettbewerbsrechtes keine Rede sein. Hier stellt sich das Problem, dass durch Regelungen wie das Herkunftslandprinzip der E-Commerce-Richtlinie ein „Race to the bottom" – eine Harmonisierung auf geringstem Level – einsetzen wird. Letztendlich könnte hieran eine materielle Harmonisierung im Bereich des Wettbewerbsrechts scheitern. Der VerbraucherInnenschutz liegt zwischen diesen beiden Polen, da die EU sich dieses Themas bereits 1992 angenommen hatte und die Fernabsatzrichtlinie von 1997 EU-weit umgesetzt wurde. Zudem wurde mit der „Entschließung des Rates über die

Verbraucherdimension der Informationsgesellschaft" im Jahre 1999 diese Thematik erneut in den Fokus der Harmonisierungsbemühungen der EU genommen. Es wird erwartet, dass ein Richtlinienvorschlag zum VerbraucherInnenschutz bei Finanzdienstleistungen im Fernabsatz bis Ende 2001 angenommen wird.

Auf internationaler Ebene sind trotz entsprechender Empfehlungen der OECD (vgl. oben **Frage 3.1.**) entsprechende Harmonisierungsbemühungen in allen drei Bereichen bislang nicht von Erfolg gekrönt. Allerdings ist davon auszugehen, dass zumindest im Bereich des Datenschutzrechts durch die Regelungen der EU-Datenschutzrichtlinie über den Datentransfer in Drittstaaten ein gewisser Regulierungsdruck auf andere Länder ausgeübt werden wird, der u.U. zu einer Anhebung des dortigen Schutzniveaus führen könnte (vgl. auch **Frage 3.9.**). Andererseits lässt sich – nicht zuletzt durch die aktuellen Entwicklungen im Bereich der Terrorismus-Bekämpfung – auf internationaler Ebene die Tendenz beobachten, dass verfassungsrechtliche Garantien zum Schutz der Privatsphäre und der personenbezogenen Daten im Cyberspace zunehmend zur Disposition gestellt werden, um vermeintlich bestehende Bedürfnisse der Sicherheits- und Strafverfolgungsbehörden zu befriedigen. Auf europäischer Ebene ist der datenschutzrechtliche Rechtsrahmen erneut in Bewegung geraten: die EU-Kommission hat eine neue Richtlinie zum Datenschutz für Kommunikationsdienste vorgeschlagen, die noch vom EU-Parlament angenommen werden muss.

Im Bereich der Daten- bzw. IT-Sicherheit ist der bisherige primär technikzentrierte Blickwinkel zu erweitern. IuK-Systeme sind sozio-technische Systeme, deren Sicherheit von den jeweiligen Anwendungsfeldern und den Menschen, die sie bedienen, abhängen. Hier sollten verstärkt interdisziplinäre Forschungsprojekte gefördert werden, die die entsprechenden Wechselwirkungen untersuchen. Die Verwundbarkeit der Informationsgesellschaft an sich muss zum Gegenstand der nationalen und internationalen Forschung gemacht werden (Stichwort: Schutz kritischer Infrastrukturen). Insoweit dürfte der Ansatz des Information Society Technologies Programme (IST) der EU als zu kurz greifend anzusehen sein.

Informationstechnologie ist keine monolithische Technologie wie z.B. Atomtechnik. Damit ist unklar, ob sie ebenso wie letztere in einem eigenen Gesetz geregelt werden kann. Durch ihre vielfältigen Einsatzmöglichkeiten im Zusammenhang mit anderen Technologien bspw. in der Prozessteuerung von Atomanlagen, ist aber zu überlegen, ob mittelfristig nicht ein IT-Sicherheitsgesetz sinnvoll sein könnte oder aber bestehende Technikgesetze ergänzt werden müssen. Auf nationaler Ebene sollte deshalb der gesamte sicherheitstechnische Regelungsrahmen überprüft werden, um festzustellen, wo Defizite in Bezug auf Einsatz und Verwendung von IuK-Technik bestehen.

Der Erlass eines Rechtsrahmens für Elektronische Signaturen ist zwar ein wesentlicher Bestandteil für eine IT-Sicherungsinfrastruktur und erhöht die IT-Sicherheit des E-Commerce. Es sind jedoch weitergehende Maßnahmen in Erwägung zu ziehen, um IuK-Systeme sicherer zu machen. Hierzu zählt u.a. die Förderung von Open Source Produkten, die eine Überprüfung des Patentrechts erfordert, sowie Überlegungen, ob eine spezielle zivilrechtliche Haftung für Software- und Hardwarefehler eingeführt werden sollte.

Insgesamt kann die Forschungs- und Entwicklungstätigkeit im Bereich der IT-Sicherheit, die schließlich das Fundament der Informationsgesellschaft darstellt, weder auf nationaler noch auf europäischer Ebene als angemessen angesehen werden.

Handlungsempfehlung:

IT-Sicherheit muss dringend stärker als förderungswürdiges Forschungsfeld angesehen werden. Dabei ist nicht nur nach technischen Sicherheitslösungen zu suchen, sondern die Verwundbarkeit der Informationsgesellschaft muss als interdisziplinäres Forschungsthema begriffen werden.

3.4. Wie beurteilen Sie die tatsächlichen Gefährdungspotenziale durch Kriminalität in Informations- und Kommunikationsnetzen bzw. durch illegale Aktivitäten, die mittels IuK-Netzwerken oder allgemein computergestützt durchgeführt werden?

Kriminalität im Internet umfasst eine Vielzahl verschiedener Delikte. Zu unterscheiden ist zwischen Delikten, bei deren Begehung sich der Täter des Computers lediglich als eines „virtuellen Tatwerkzeugs" bedient, die aber auch außerhalb von technischen Informations- und Kommunikationsnetzen begangen werden können. In solchen Fällen wird das Netz also nur zur Vorbereitung von Straftaten genutzt. Dies sind z.B. Delikte wie Pornografie, Volksverhetzung, der Verbreitung extremistischer Propaganda, dem illegalen Verkauf von Waffen, Betäubungsmitteln und Medikamenten. Eine gesonderte Statistik bezüglich dieser Delikte im Hinblick auf die Begehung mittels Computernetzen wird in der polizeilichen Kriminalstatistik nicht erhoben. Eine seriöse Einschätzung zum Gefährdungspotenzial und der Bedeutung dieses Bereiches der Kriminalität ist somit nicht ohne weiteres möglich.

Daneben existiert eine Vielzahl von Delikten, die sich gegen die Sicherheit des Netzes an sich oder von vernetzten Rechnern oder von auf Rechnern vorhandenen Daten

richten. Dazu zählen die Tatbestände des Computerbetrugs (§ 263a StGB), der Datenveränderung (§ 303a StGB) sowie der Computersabotage (§ 303b StGB), des Ausspähens von Daten (§ 202a StGB), des Urheberrechts (UrheberrechtsG) sowie der verwandten Leistungsschutzrechte (MarkenG, § 17 UWG, GebrauchsmusterG, GeschmacksmusterG, KunsturheberrechtsG, PatentG) und der Softwarepiraterie. Wie die polizeiliche Kriminalitätsstatistik zeigt, ist in den letzten zehn Jahren in diesem Bereich ein stetiger Anstieg der Fallzahlen zu verzeichnen. Hierbei ist zu beachten, dass nach einhelliger Auffassung zudem für jedes der genannten Delikte ein erhebliches Dunkelfeld besteht.

Polizeiliche Kriminalstatistik

Jahr	§ 263a StGB	§§ 303a, b StGB	§ 202a StGB	UrhG, LeistungsschutzR	Private Softwarepiraterie	Gewerbl. Softwarepiraterie
1990	787	95	77	5.423		
1991	1.003	122	58	3.400	1.036	
1992	2.009	88	67	2.180	542	
1993	2.247	137	103	3.201	501	
1994	2.754	188	165	2.459	267	89
1995	3.575	192	110	2.844	363	120
1996	3.588	228	933	2.362	192	187
1997	6.506	187	213	3.504	546	772
1998	6.465	326	267	3.025	362	289
1999	4.774	302	210	5.444	972	1.252
2000	6.600	513	513	k.A.	k.A.	k.A.

(Quelle: Bundesinnenministerium, http://www.bmi.bund.de)

Auch für die zukünftige Entwicklung ist eher mit einer Zunahme der IuK-Kriminalität zu rechnen. Dies liegt beispielsweise für den Bereich der Datenspionage und der Datenveränderung daran, dass ein Ausspähen von Daten mittels weitverbreiteter Tools ohne größeren technischen Aufwand einfach durchgeführt werden kann, wenn der

vermeintlich Betroffene nicht angemessene Sicherheitsvorkehrungen trifft. Für solche Arten von Attacken stehen im Internet frei zugänglich bzw. auf CD-ROM käuflich erhältlich eine große Anzahl von Hacker-Werkzeugen zur Verfügung, so dass häufig kein großes Know-how mehr erforderlich ist, sondern Angriffe durch einfaches Anklicken in menügesteuerten Hacker-Tools gestartet werden können.

Mit der steigenden Anzahl der Taten korrespondiert der wirtschaftliche Schaden, der durch Angriffe auf IuK-Netze hervorgerufen wird. So kann ein weltweit verbreiteter Computervirus wie der „Loveletter-Virus" weltweit einen Schaden in Milliardenhöhe hervorrufen. Neben diesem unmittelbar hervorgerufenen wirtschaftlichen Schaden wird zusätzlich das Vertrauen der Nutzer in die Sicherheit der IuK-Systeme unterminiert, was deren Entwicklung hemmt und somit ebenfalls einen mittelbaren wirtschaftlichen Schaden hervorruft.

Auch wenn die vorgelegten Statistiken belegen, dass die Datennetzkriminalität in den vergangenen Jahren stetig zugenommen hat, so ist hinsichtlich der Erwägung neuer Strafbestimmungen oder der Ausweitung der gesetzlichen Eingriffsbefugnisse zur Strafverfolgung zu berücksichtigen, dass der Missbrauch der Datennetze im Vergleich zu deren legaler Nutzung lediglich einen verschwindenden Ausschnitt bildet. Zudem ist zu bedenken, dass die Zahl der Internet-Nutzer alleine in Deutschland in den letzten fünf Jahren um einen vierstelligen Prozentbetrag (von 5,9 Mio. in 1996 auf 113,14 Mio. in 2001, d.h. um fast 2000%) gestiegen ist und damit deutlich über der Zuwachsrate der Fallzahlen liegt.

Zusammenfassend lässt sich damit feststellen, dass Cybercrime zwar in der Tat eine grundlegende Bedrohung für die Informationsgesellschaft darstellt. Zuverlässige empirische Daten über die hierdurch verursachten Schäden fehlen aber weitgehend. Ebenso fehlen Studien über das tatsächliche Verletzlichkeitspotential der Informationsgesellschaft, das aus der Abhängigkeit von IuK-Systemen resultiert.

Soweit es um die Bekämpfung von internetgestützer Kriminalität geht, für die die IuK-Systeme nicht Angriffsziel, sondern Medium sind, sollte eine sorgfältige Abwägung zwischen den Interessen der sog. Bedarfsträger, den Sicherheits- und Strafverfolgungsbehörden, sowie den Rechten der Nutzer vorgenommen werden. Hierbei ist auch zu berücksichtigen, dass Überwachungsmaßnahmen gegen Täter, die ihre Kommunikation durch Verschlüsselung oder durch Steganographie schützen, von vorneherein aussichtslos sind. Bei Delikten, die sich demgegenüber gegen IuK-Systeme an sich richten, nützen Überwachungsmaßnahmen ohnehin nur wenig. Hier sollten präventive Maßnahmen zum Schutz der IT-Systeme und zur Absicherung der

Informationsinfrastruktur im Vordergrund der Kriminalitätsbekämpfung stehen. Die Europäische Kommission hat zu dieser Problematik einen Diskussionsprozess zwischen Providern, Strafverfolgungs- und Datenschutzbehörden auf der Grundlage der Mitteilung der EU-Kommission zu einem europäischen Politikansatz für die Sicherheit der Netze und Informationen vom 06. Juni 2001 initiiert.

Handlungsempfehlungen:

1. ***Bevor strafrechtliche Eingriffsbefugnisse erweitert und Vorhaben wie z.B. die TKÜV oder die Umsetzung der Cybercrime-Konvention des Europarates realisiert werden, sollten mindestens die Ergebnisse der Studie des Max-Planck-Insituts für ausländisches und internationales Strafrecht über die Effektivität der Telekommunikationsüberwachung, die voraussichtlich im Frühjahr 2002 vorgestellt werden, abgewartet, eingehend geprüft und berücksichtigt werden.***

2. ***Ferner sollte geprüft werden, inwieweit die heutigen, bereits 1986 mit dem 2. Wirtschaftskriminalitätsbekämpfungsgesetz eingeführten, materiell-rechtlichen Strafvorschriften ausreichend sind, die potentiell möglichen Delikte des Cybercrime aufzunehmen, oder um neue Straftatbestände ergänzt werden müssen.***

3. ***Es sollten Studien initiiert werden, die empirische Daten über das tatsächliche Verwundbarkeitspotential der Informationsgesellschaft liefern.***

3.6. Wie beurteilen Sie den Stand der internationalen Harmonisierung des Rechts und welche weiteren Schritte halten Sie diesbezüglich für erforderlich? Wie bewerten Sie insbesondere die Möglichkeiten technischer Lösungsansätze zur effektiveren Rechtsdurchsetzung in IuK-Netzen?

Zur internationalen Harmonisierung des Rechts siehe bereits Fragen 3.1. und 3.2.

Technische Lösungsansätze

Verschiedene Autoren haben überzeugend dargelegt, dass der Wirkungsgrad der traditionellen Steuerungsinstrumente des Staates im Cyberspace erheblich reduziert ist, wenn diese auf bereits bestehende technische Verhältnissen „aufgepfropft" werden. Die

technischen Parameter der IuK-Systeme bestimmen maßgeblich in welchem Umfang bestimmte Steuerungsziele verwirklicht werden können. Zur Veranschaulichung: Im Internet können E-Mails ohne Probleme mitgelesen werden, weil die Architektur des Internet nicht darauf ausgelegt wurde, das IT-Sicherheitsziel „Vertraulichkeit" zu realisieren. Mit einer anderen technischen Gestaltung der Protokolle könnte dies verhindert werden. Ein weiteres Beispiel: Die Blockade bestimmter Inhalte bleibt oftmals erfolglos, weil „Zensur" vom Internet als Fehler betrachtet wird und blockierte Verbindungen einfach umroutet werden oder die blockierten Inhalte auf zahllose andere Server „gespiegelt" werden.

Deshalb ist die Funktion von Technik, im Internet Recht zu ermöglichen bzw. umzusetzen, stärker in den Blick zu nehmen. Gerade in Bereichen wie dem Datenschutz, dem Strafrecht, dem Jugendschutz, dem Urheberrecht und beim Schutz der Privatsphäre können technische Instrumente rechtliche Werte und Ziele fördern. Durch „vorlaufende" Technikgestaltung, die darauf achtet, dass rechtlich oder gesellschaftspolitisch erwünschte Ziele in IuK-Systeme implementiert werden, kann somit ein „Mehr" an Verfassungs- und Rechtsverträglichkeit des Cyberspace erreicht werden.

Handlungsempfehlungen:

1. ***Es sollte im Rahmen einer interdisziplinären Studie genauer untersucht werden, in welchen praktischen Bereichen derartige technische Lösung möglich sind und welche (rechtlichen) Ziele implementiert werden könnten und sollten.***

2. ***Ferner ist an die Förderung von interdisziplinären Projekten, bei denen Techniker und Juristen (sowie ggf. andere Disziplinen) gezielt Lösungen für geeignete Bereiche entwickeln, gedacht werden (nach dem Vorbild von VERNET des BMWi).***

3. ***In diesem Zusammenhang ist auch daran zu denken, den Handlungsauftrag und die Kompetenzen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) neu auszurichten und ggf. zu erweitern. Der bislang primär auf die technische Sicherheit gerichtete Fokus des BSI sollte erweitert werden und stärker die gesellschaftlichen Abhängigkeiten und sozialen Wechselwirkungen von und mit IuK-Systemen in den Blick nehmen.***

4. ***Schließlich sollte der staatliche Einfluss auf die Arbeit der technischen Standardisierungsgremien unter dem Blickwinkel „Recht durch Technik" intensiviert werden. Es könnte auch daran gedacht werden einen internationalen „staatlichen Beirat" zur ISOC – insbesondere zum Internet Architecture Board bzw. der Internet Engineering Task Force – ins Leben zu rufen, dessen Aufgabe noch genauer zu entwickeln wäre.***

3.7. Erläutern Sie die wesentlichen Handlungsfelder auf nationaler, europäischer und internationaler Ebene sowie den Stand der Verhandlungen und die Umsetzung.

Siehe vorangehende Antworten.

3.8. Welche Ziele hat der „Global Business Dialogue für E-Commerce", welche Erfahrungen wurden damit gemacht und welche Konsequenzen sind daraus zu ziehen?

Der Global Business Dialogue für E-Commerce wurde im Januar 1999 gegründet und ist das Resultat einer Initiative des ehemaligen EU-Kommissars für Telekommunikation, Martin Bangemann. An der Gründung beteiligten sich fast 100 der weltweit führenden Medien- und Technologieunternehmen.

Der Global Business Dialogue für E-Commerce verfolgt vor allem zwei Ziele: Zum einen befürwortet er die Schaffung weltweit einheitlicher, transparenter Normen für den elektronischen Geschäftsverkehr. Die Regulierung der für den E-Commerce relevanten Rechtsbereiche soll dabei nicht in erster Linie durch die einzelnen Nationalstaaten erfolgen. Der Global Business Dialogue für E-Commerce setzt stattdessen auf verstärkte Selbstregulierungsanstrengungen der Internet-Wirtschaft, da nur auf dem Wege der Selbstregulierung sichergestellt werden könne, dass die verabschiedeten Bestimmungen nicht singuläre nationale Interessen verfolgten.

Das zweite Ziel des Global Business Dialogue für E-Commerce besteht darin, das Vertrauen der Verbraucher und Netzbürger in die neuen Informations- und Kommunikationsmedien zu stärken. Zur Vertrauensbildung soll ein System eingesetzt werden, das E-Commerce-Anbieter, die einen hohen und überprüfbaren

Sicherheitsstandard anbieten und somit vertrauenswürdig sind, mit einem besonderen Gütezeichen kennzeichnet.

Die Bemühungen des Global Business Dialogue, auf dem Wege der Selbstregulierung einheitliche Regulierungsstandards für die globale Geschäftskommunikation zu entwickeln, sind begrüßenswert. Durch das Engagement der Anbieter wird ein flexibles Instrument zur Lösung der den E-Commerce betreffenden Rechtsprobleme geschaffen, das nicht an nationale Grenzen oder behördliche Verfahren gebunden ist.

Jedoch wird auch der E-Commerce nicht gänzlich ohne staatliche Regelungen auskommen. Nur der demokratisch legitimierte Gesetzgeber kann sicherstellen, dass die Interessen aller Mitglieder der Informationsgesellschaft bei der Internet-Regulierung hinreichend berücksichtigt werden. Der Gesetzgeber ist daher dazu aufgerufen, einen äußeren rechtlichen Rahmen für die Selbstregulierungsanstrengungen der Internet-Wirtschaft zu schaffen – Selbstregulierung und staatliche Regulierung also effektiv miteinander zu verzahnen.

Handlungsempfehlung:

Die Empfehlungen des GBD sollten von staatlicher Seite aufgenommen, geprüft und in Zusammenarbeit mit den Spitzenverbänden der deutschen Wirtschaft sowie den Verbraucherschutzverbänden (etwa in Form eines Public-Private-Partnership zwischen dem BMWi und den einschlägigen Verbänden) Richtlinien für Selbstregulierung erstellen. Vergleichbare Bemühungen laufen derzeit auf europäischer Ebene.

3.9. Welche Bedeutung hat das Datenschutzabkommen zwischen der EU und den USA und welche Probleme ergeben sich bei der Umsetzung?

Das Safe-Harbour-Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika ist für den transatlantischen elektronischen Geschäftsverkehr von herausgehobener Bedeutung. Ziel des Abkommens ist es, für personenbezogene Daten aus dem Gebiet der EU, die von U.S.-Unternehmen erhoben und/oder verarbeitet werden, ein Datenschutzniveau zu gewährleisten, das dem der EU-Datenschutzrichtlinie entspricht. Ein gleichwertiges Datenschutzniveau ist gem. Art. 25 Abs. 1 der Datenschutzrichtlinie die Grundvoraussetzung dafür, dass personenbezogene Daten aus dem Raum der EU von Nicht-Mitgliedsstaaten überhaupt verarbeitet werden dürfen. Will also ein amerikanischer E-Commerce-Anbieter

Kundendaten aus dem Bereich der Europäischen Union erheben oder verarbeiten, muss er seine Datenverarbeitung entsprechend den Safe-Harbour-Prinzipien gestalten.

Bei der Umsetzung des Safe-Harbour-Abkommens stellt sich vor allem als problematisch dar, dass das Abkommen bislang noch keine umfassende Akzeptanz seitens der US-Unternehmen erfahren hat. Lediglich 102 Unternehmen haben sich bislang auf die Safe-Harbour-Grundsätze verpflichtet (Liste abrufbar unter: http://web.ita.doc.gov/safeharbor/SHList.nsf). Des Weiteren mangelt es an effektiven Kontrollmechanismen. Das amerikanische Wirtschaftsministerium hat auf die Installation eines systematischen Aufsichtssystems über die Einhaltung der Safe-Harbour-Prinzipien verzichtet. Es ahndet nur solche Datenschutz-Verstöße, bei denen nachweislich ein Missbrauch von personenbezogen Daten erfolgt ist.

Handlungsempfehlung:

Die Mitglieder der EU sind daher gehalten, die Umsetzung der Safe-Harbour-Prinzipien durch amerikanische Unternehmen und Behörden kritisch zu beobachten. Wird von amerikanischer Seite aus dauerhaft kein hinreichendes Datenschutzniveau gewährleistet, so muss gegebenenfalls die Europäische Kommission erneut darüber entscheiden, ob durch das Safe-Harbour-Abkommen ein ausreichendes Datenschutz-Niveau sicherstellt wird oder ob zum Schutze personenbezogener Daten weitergehende Verabredungen zwischen der EU und den Vereinigten Staaten zu treffen sind.