

Recht und Cyberspace

Eine Einführung in einige rechtliche Aspekte des Internets

Ausgangsthesen

I. Einleitung

Cyberspace - ein neues Rechtsgebiet? Alle reden über das Internet, und die Juristen sollten mitreden. Der folgende Beitrag soll hier bei der Orientierung helfen und auf einige aus der Sicht des Rechts bedeutsame Fragen hinweisen, ohne dass ich dabei eine erschöpfende oder auch nur vollständige Darstellung der Probleme behaupten will.

II. Cyberspace - was ist das?

Um was geht es überhaupt?

Als Begriff aus einem Science-Fiction-Roman ist 'Cyberspace' sicherlich schillernder und griffiger als das technisch-scheppernde Wort 'Internet'. Die beiden oft gleich gesetzten Begriffe sind jedoch letztlich wenig konkret und werden häufig undifferenziert gebraucht. Was heisst denn schon "im Cyberspace" oder "auf dem Internet"?

Denkbar ist, Cyberspace als eigenständigen 'Ort' zu begreifen, wo es Substrukturen wie kommerzielle On-line-Anbieter, Computer Bulletin Board Systems (BBS), private Systeme, Newsgroups auf dem Usenet, Homepages auf dem World Wide Web und Computernetzwerke gibt.

Man kann sich dem Phänomen Cyberspace aber auch über die dort vorzufindenden Aktivitäten nähern. Zu nennen sind hier E-mail, die Nutzung von Public Messaging Systems, Austausch von Software und allgemein Datenübertragung, Electronic Publishing, Unterhaltung im weitesten Sinne, direkte Kommunikation, die Nutzung durch Bildungs- und Forschungseinrichtungen sowie allgemein kommerzielle Anwendungen.

III. Rechtliche Problemfelder

Rechtliche Fragen im Zusammenhang mit dem Internet betreffen eine Vielzahl von Rechtsgebieten: in dem Maße, in dem das Internet Teil des Alltages wird, wird es auch Teil des Rechtsalltages. Dementsprechend kann ich hier nur eine Auswahl von rechtlichen Fragestellungen ansprechen, wobei sich schon über die Auswahl und die Abgrenzung der Bereiche sicherlich gut streiten lässt.

Einen Problembereich Datenschutz und Persönlichkeitsrecht nenne ich als erstes.

Datenschutz ist schon seit längerem als 'modernes' computerspezifisches rechtliches Problem im Zusammenhang mit der Hacker-Subkultur erkannt.

Die technische Fortentwicklung des Datenschutzes (Verschlüsselung von Daten) hat mittlerweile zu neuen rechtlichen Problemen geführt. Vielfach wird befürchtet, dass elektronische Deckmäntel, die eigentlich dem Datenschutz dienen sollen, von Rechtsbrechern zur Verschleierung ihrer Identität missbraucht werden können und damit Datenschutz bieten (Stichwort 'elektronisches Vermummungsverbot').

Überhaupt stellen sich neue Fragen um den Begriff der Identität. Der rechtliche Schutz von Identität im Cyberspace (Namensrechte und Warenzeichenrechte) wie überhaupt der Begriff der Identität im Cyberspace sind (noch) fließend.

Spezifische Probleme von Rechtsgeschäften im Cyberspace gewinnen mit der zunehmenden Kommerzialisierung des Cyberspace an Bedeutung. Die zu erwartenden Schwierigkeiten lassen sich an den Beispielen der Willenserklärung im Cyberspace sowie Schriftform und Unterschrift im Cyberspace erläutern.

Ein eigenständiger Problembereich ist das geistige Eigentum im Cyberspace, wo blitzartige Vervielfältigung und Verteilung den Schutz von Werken zunehmend erschweren.

Das Recht der freien Rede im Cyberspace, die Meinungsäußerungsfreiheit im Cyberspace, ist ein besonders heftig diskutiertes Problemfeld. Dabei geht es im wesentlichen um die Frage nach der zulässigen Kontrolle von Meinungsäußerungen, was letztlich zu der Frage führt, wessen Werte im Cyberspace maßgeblich sein sollen. Neue Fragen stellen sich hier auch um den Presse- und Rundfunkbegriff.

IV. Cyberspace als neuer Rechtsraum - die vierte rechtliche Dimension?

Eine nähere Betrachtung der Rechtsprobleme führt fast immer zu der Feststellung, dass die spezifische Problematik des Regelungsgegenstandes Cyberspace in seinem grenzüberschreitenden Charakter liegt, der sich einseitig-nationalen Regelungen entzieht.

Die vor diesem Hintergrund vielfach geäußerte (Fehl-)vorstellung, Cyberspace sei ein rechtsfreier Raum, legt zunächst einmal eine Bestandsaufnahme bestehender Regeln formaler und materieller Natur nahe.

Dabei ist zunächst auf die vielfältigen formalen (technischen) Regeln einzugehen, die als technische Standards weltweit das Internet erst möglich machen und in bestimmten Verfahren erzeugt werden. Im Bereich der materiellen Regeln sind die Netiquette und die Benutzungsregeln der Anbieter anzusprechen.

Obwohl auch das Internet auch heute schon durchaus Regeln unterliegt, ist doch die Frage nach dem Regelungsbedarf ganz offenkundig nicht ohne Berechtigung. Dementsprechend sind nationale Gesetzgeber bereits tätig geworden, so dass sich Regelungsansätze und Regelungsversuche vergleichen lassen.

Weg von diesen unilateralen Regelungsanstrengungen weist der Weg, Cyberspace als eigenständigen Rechtsraum zu begreifen und von dieser Konzeption ausgehend rechtliche Lösungen vorzuschlagen.

Ebenfalls von der Einsicht in die Beschränktheit nationaler Regelungsmöglichkeiten getragen, aber konkreter an herkömmlichen Vorstellungen vom Recht orientiert, ist dagegen die

Überlegung, die sich stellenden Probleme durch internationales Recht auf der Ebene des Völkerrechts anzugehen.

V. Besseres Recht durch Cyberspace?

Cyberspace bedeutet für das Recht nicht nur mehr oder weniger lösbare neuartige Probleme, sondern auch eine Chance.

Dies bezieht sich einmal auf den eher technischen Aspekt der Effizienz im Sinne einer Optimierung der juristischen Arbeit.

In einem abstrakteren Sinne können sich positive Aspekte aber auch ergeben durch erhöhte Entscheidungstransparenz und verbesserte Ereignistransparenz.

VI. Zusammenfassung und Ausblick

Aus der zunehmenden Verbreitung computergestützter Kommunikation ergeben sich zahlreiche neuartige Rechtsprobleme. Aufgrund der besonderen Struktur des Cyberspace, wo territoriale Grenzen kaum noch Sinn machen, genügen herkömmliche Rechtsstrukturen den Erfordernissen eines Rechts des Cyberspace nicht mehr. Einfache Lösungen sind nicht in Sicht. Lösungsansätze könnten sich einmal darauf richten, Cyberspace als eigenständigen Rechtsraum zu begreifen und, davon ausgehend, die rechtliche Autonomie im Cyberspace zu fördern, in deren Rahmen sich Regeln eigenständig ausbilden könnten und die durch schiedsgerichtliche Streitschlichtungsmechanismen zu ergänzen wäre. In eine andere Richtung geht der Vorschlag, Cyberspace auch rechtlich zu internationalisieren und mit Hilfe der etablierten Instrumente einer internationalen Konvention, verbunden mit der Errichtung einer zuständigen Internationalen Organisation, rechtlich zu fassen.

Jeder Lösungsversuch in diesem Bereich ist verknüpft mit dem schwer vorhersehbaren Fortschritt der Technik. Für das Recht bietet diese technische Entwicklung jedoch durchaus auch Entwicklungs- und Verbesserungsmöglichkeiten. Fest steht jedenfalls, dass die Entwicklung in diesem Bereich nicht aufgehalten werden kann und dass die computergestützte Kommunikation Sinnbild für eine sich fundamental wandelnde, zunehmend interdependente Welt ist.

Das Recht wird sich dieser Entwicklung letztlich nicht entziehen können.

I. Einleitung

Cyberspace - ein neues Rechtsgebiet? Wenn die soziale Relevanz eines Phänomens in direktem Zusammenhang mit der rechtlichen Relevanz steht, ist dies heute fraglos mit ja zu beantworten: Alle reden über das Internet, und die Juristen sollten mitreden. Der folgende Beitrag soll hier bei der Orientierung helfen und auf die aus der Sicht des Rechts bedeutsamen Fragen hinweisen. Dabei wird im wesentlichen die amerikanische und, in geringerem Umfang, auch die französische Diskussion rezipiert werden.

Warum die USA und Frankreich?

Für die USA lässt sich das einfach begründen: Das Internet ist eine amerikanische Erfindung. Dort existiert bereits umfangreiche Literatur in Fachzeitschriften und Monographien, es findet eine intensive Diskussion der sich stellenden Probleme in der Fachwelt aber auch in der Öffentlichkeit statt.

Frankreich dagegen ist wie das übrige Europa bemüht, den Anschluss an die Entwicklung in den USA nicht zu verlieren. Allerdings hat man in Frankreich seit Anfang der Achtziger Jahre mit dem Minitel-System Erfahrungen damit sammeln können, was für (Rechts)probleme mit einem in der Bevölkerung verbreiteten und häufig genutzten internaktiven Computersystem auftreten können.

Zunächst ist zu klären, was eigentlich Cyberspace bedeutet und welche Aktivitäten dort vorzufinden sind, bevor auf rechtliche Probleme und mögliche Lösungen eingegangen werden kann. Abschließend soll ein Ausblick auf die Möglichkeiten angedeutet werden, die das neue Medium für die Anwendung des Rechts selbst bietet.

II. Cyberspace - was ist das?

Der Begriff Cyberspace entstammt der Mitte der achtziger Jahre erschienenen preisgekrönten Novelle *Neuromancer* von William Gibson¹, die äußerst einflussreich auf die Computer- und Telekommunikationszene war, weswegen sich als Sammelbegriff für die Netzwerke untereinander verbundener Computer und den daraus entstandenen Kommunikationsraum die Bezeichnung Cyberspace² durchgesetzt hat³. Die Handlung der Novelle spielt in einer Zukunft, in der das menschliche Bewusstsein unmittelbar an einen Computer angeschlossen werden kann und auf diesem Wege Zugang zu einer virtuellen Welt (der Matrix im Cyberspace) erlangt wird, die keine Entsprechung in der wirklichen, physischen Welt hat, sondern nur in der Vorstellung der angeschlossenen Teilnehmer existiert. Obwohl heute noch Tastatur und Bildschirm zwischen Cyberspace und Mensch stehen, erscheint gleichwohl die durch Vernetzung von Computern entstandene Welt zunehmend als eigenständige Dimension, insofern dem Cyberspace aus *Neuromancer* ähnlich.

Ihren Anfang nahm die Entwicklung in einem militärischen Kommunikationssystem, das Anfang der 70er Jahre zur Verbindung von militärischen und zivilen Forschungsstellen in den USA errichtet wurde, dem Arpanet⁴. Vor allem gedacht zur Übermittlung von Forschungsdaten, erwies sich die beiläufig mögliche Übermittlung von elektronischen Botschaften - Elektronische Post (E-mail) -, eigentlich nur ein Nebenprodukt der Forschung, als großer Erfolg und wurde zum Ausgangspunkt für neue Arten der Kommunikation. Im Laufe der Zeit wurden zunehmend rein zivile Forschungsstellen an das System angeschlossen und das Arpanet durch das Internet abgelöst, welches heute Millionen von Teilnehmern in aller Welt verbindet⁵. Ergänzt wurde die Entwicklung der Forschungsnetzwerke durch die Vielzahl von kleinsten privaten Computernetzwerken, sog. Bulletin Board Systems (BBS, s.u.), die - oft nur einen Personal Computer umfassend, durch Computermodem⁶ und Telefonleitungen mit anderen PCs verbunden - sich wie kleine Inseln begreifen lassen, die im Laufe der Zeit untereinander verknüpft wurden und schließlich den Zugang zum Internet gefunden haben⁷.

¹ W. Gibson, *Neuromancer*, 1984.

² Das Wort bezieht sich auf den Begriff Cybernetics (Kybernetik), der 1948 von dem Mathematiker Norbert Wiener geprägt wurde. Im französischen Sprachraum wird gelegentlich der Begriff cyberspace benutzt, s. etwa A. Dufour, *Internet (Que sais-je?)*, 1996.

³ Zur Frage, inwieweit diese neue Entwicklung auch die Tätigkeit des Juristen verändern wird E. Katsh, *Digital Lawyers: Orienting the Legal Profession to Cyberspace*, 55 *University of Pittsburgh Law Review* 1141 (1994); s. auch unten Fußn. 20 zu *LEXIS Counsel Connect*. Für die deutsche Entwicklung M. Hartmann, *Legal Data Banks, the Glut of Lawyers, and the German Legal Profession*, 27 *Law & Society Review* 421 (1993).

⁴ ARPA (Advanced Research Project Agency), eine Einrichtung des U.S.-Verteidigungsministeriums, die 1957 in Erwiderung der sowjetischen Sputnik-Erfolge gegründet worden war, wollte durch die Vernetzung von Forschungsstellen nicht zuletzt auch die Kosten für die Kommunikation der Forschungsstellen untereinander senken; vgl. H. Rheingold, *The Virtual Community*, 1993, S. 70 ff. Zur historischen Entwicklung s. auch T. Piette-Coudol/A. Bertrand, *Internet et la Loi*, 1997 und Dufour (o. Fußn. 2), S. 25 ff.

⁵ Bei seiner Errichtung im Jahre 1981 betrug die Zahl der angeschlossenen Systeme 213, die genaue Teilnehmerzahl heute kennt niemand, einig ist man sich jedoch in der Einschätzung, daß die Zahl in den letzten Jahre förmlich explodiert ist. Anfang 1995 wurden für das Internet Teilnehmerzahlen zwischen 30 und 40 Millionen genannt, in manchen Ländern betrug der Zuwachs an Teilnehmern Anfang der 90er Jahre in drei Jahren über 1000%, s. P. Elmer-De Witt, *Welcome to Cyberspace*, *TIME Spring 1995 (Special Issue)*, S. 9.

⁶ Modem steht für Modulator/Demodulator und ermöglicht die Übermittlung von Computerdaten über normale Telefonleitungen an einen anderen Computer mit Modem.

⁷ Das Netzwerk der BBS, Fidonet, wurde Ende der 80er Jahre durch ein gateway mit dem Internet verbunden, Rheingold, (o. Fußn. 4), S. 139.

Oft wird allgemein von On-line-Kommunikation "im Internet" gesprochen. Technisch handelt es sich beim Internet lediglich darum, dass verschiedenste Computer über ein gemeinsames sogenanntes Protokoll⁸ gewissermaßen die gleiche Sprache sprechen. Obgleich das Internet letztlich nur das Datenaustauschprotokoll ist, auf das man sich geeinigt hat, ist doch die Vorstellung, dass es irgendwo die 'Leitungen des Internet' gibt, nicht abwegig. Die Computerkommunikation erfolgt zum Teil über normale Telefonleitungen, in der Regel gibt es jedoch ein nationales "Rückgrat" von Hochgeschwindigkeitsverbindungen, in den USA etwa das NSFNet⁹, das sechs Hochleistungsrechner sowie über 290 lokale Hochschulrechner und einige regionale Netzwerke miteinander verbindet. An die Datenautobahn des NSFNet sind national kleinere Netzwerke über gates (Schleusen), oftmals eben über normale Telefonleitungen, angeschlossen - gewissermaßen Landstraßen und Feldwege. In den meisten Ländern findet sich eine vergleichbare Struktur mit einem Hochleistungsnetzwerk, an das kleinere Netzwerke und Einzeleinrichtungen angeschlossen sind. Die verschiedenen Hochleistungsnetzwerke sind wiederum über das Internet Protokoll miteinander verbunden, wodurch sich der Ausspruch vom Internet als weltumspannendem Netzwerk der Netzwerke erklärt.

Geblichen ist vom militärischen Ausgangspunkt nach wie vor die dezentrale Struktur, und dies ist außerordentlich bedeutungsvoll für die rechtlichen Fragestellungen. Die Grundidee für das Arpanet stammte seinerzeit von RAND¹⁰, einem Thinktank für Szenarios eines thermonuklearen Krieges, aus einem Entwurf für ein Kommunikationssystem, das auch Atomschläge so weit wie möglich überleben können sollte, weil es keine die Kommunikation organisierende Zentrale des Systems gab und die Botschaften nicht als ganzes auf einem Wege verschickt wurden. Erreicht wurde die dezentrale, extrem widerstandsfähige Struktur durch die Technik des Package switching. Package switching bedeutet, dass Botschaften gewissermaßen in elektronische Pakete zerlegt werden, die sich - mit Individualisierungsmerkmalen versehen - jeweils ihren eigenen Weg durch die Verbindungen zum Adressaten suchen. Stoßen einzelne Pakete auf ihrem Weg auf ein Hindernis, so suchen sie sich eine Umleitung. Beim Adressaten angekommen, werden die Pakete wieder zu einer Nachricht zusammengesetzt. Der Vorteil dieser Methode ist die geringe Verwundbarkeit der Informationsübermittlung: wenn etwa bei einem Atomschlag weite Teile des Datennetzes ausfallen, bleibt die Informationsübermittlung gleichwohl noch möglich. Außerdem gibt es keine Zentrale, deren Zerstörung auch die Zerstörung des Kommunikationssystems bedeuten würde¹¹. So gibt es auch heute keine Internetzentrale, wo das Internet kontrolliert oder gar abgeschaltet werden könnte. Aufgrund der technischen Struktur des Internet lässt sich noch nicht einmal sagen, auf welchen Leitungen die verschiedenen Teile einer Botschaft zum Empfänger gelangen. George Orwells Vision der Zukunft, die Vorstellung vom 'Großen Bruder', der staatlichen Autorität, die alles überwacht und die oft mit neuen Technologien verbunden wird, hat sich hier gerade nicht erfüllt¹²: es gibt keinerlei mit Zwangsmitteln ausgestattete Kontrollinstanz für das Internet und die Idee geographischer Grenzen macht für das Internet und für Cyberspace nur noch wenig Sinn. Belegt wird dies eindrucksvoll dadurch, dass Informationen über Ereignisse wie das Massaker von Tianamen, den Golfkrieg, die Putschs in Moskau und den Krieg im früheren Jugoslawien über Cyberspace an allen

⁸ Transmission Control Protocol/Internet Protocol (TCP/IP), seit 1983 in Gebrauch.

⁹ Das NSFNet soll in absehbarer Zeit durch ein noch leistungsfähigeres Netz namens NREN ersetzt werden.

¹⁰ Rheingold (o. Fußn. 4), S. 7.

¹¹ S. im einzelnen Rheingold (o. Fußn. 4), S. 74.

¹² Katsh (o. Fußn. 3), S. 1160.

Zensurbemühungen vorbei nach außen gelangen konnten¹³. Zensur wird technisch als Schaden interpretiert und umgangen¹⁴.

Cyberspace, in seiner heutigen Struktur letztlich ein Produkt des Kalten Krieges, lässt sich damit begreifen als ein öffentlicher oder sozialer Raum neuen Typs¹⁵. Die Zukunft richtet sich auf den Information Superhighway, die Super-Datenautobahn, auf der sowohl die Quantität als auch die Geschwindigkeit der Datenübertragung neue Dimensionen erreichen werden. Visionäre sehen für diese Zukunft das Einkaufen von Zuhause aus und das interaktive Fernsehen als alltägliche Selbstverständlichkeit, Rechnungen werden in dieser Zukunft elektronisch bezahlt und Parlamente vom Computer aus elektronisch gewählt. Kennzeichnend für diese Zukunft wird jedenfalls sein, dass die klaren Grenzen zwischen Rundfunk/Fernsehanbietern, Telefonbetreibern und Computernetzwerkanbietern zunehmend verschwimmen, weil alle diese Dienste im wesentlichen auf dem gleichen Übermittlungsweg in digitaler Form zum Benutzer gelangen¹⁶.

¹³ Rheingold (o. Fußn. 4), S. 130 (Tianamen), S. 185 (IRC aus Kuwait und Israel im Golfkrieg).

¹⁴ Dies ist ein in der Computergemeinde oft zitierter Ausspruch, Rheingold (o. Fußn. 4), S. 7.

¹⁵ Zum Begriff des sozialen Raums, s. J. Habermas, Faktizität und Geltung, 1992, S. 436 f. In der Qualität als öffentlicher Raum liegt einer der vielen Unterschiede zu herkömmlichen Medien: Auch telefonische Kommunikation ist grenzüberschreitend, aber in der Regel wird sie von Person zu Person zu erfolgen, dies ist im Cyberspace, der die Möglichkeit eröffnet, eine große Menge von Personen in aller Welt zu erreichen, anders.

¹⁶ Zur künftigen Entwicklung mit zahlreichen weiteren Nachweisen s. The Message in the Medium: The First Amendment on the Information Superhighway, 107 Harvard Law Review 1062, 1067 ff. (1994). Skeptisch C. Stoll, Die Wüste Internet - Geisterfahrten auf der Datenautobahn, 1996.

1. Substrukturen

Heutzutage finden sich im Cyberspace im wesentlichen die folgenden Substrukturen¹⁷:

a) Kommerzielle On-line-Anbieter:

Hier stehen auf Großrechnern von Privatanbietern (wie etwa CompuServe, T-Online oder America Online) Tausenden von Nutzern - in der Regel gegen monatliche Gebühren - jeweils personalisierte Konten (account) zur Verfügung, zu denen man mittels eines Benutzernamens (username) und eines Kennwortes (password) Zugang erlangt, und über das man damit - theoretisch zumindest - alleinige Kontrolle hat. Daneben werden dem Nutzer meist eine Vielzahl von Anwendungen geboten; üblich sind dabei elektronische Post (E-mail), Datenbanken, Sammlungen von Computerprogrammen (Software), elektronische Diskussionsrunden, elektronische Kommunikation in Echtzeit mit anderen Anwendern, aktuelle Nachrichten. Manche Systeme eröffnen sogar die Möglichkeit des elektronischen Einkaufens. Nicht zuletzt bieten diese Dienste meist Zugang zum Internet. Die Popularität dieser Dienste ist im Steigen begriffen, auch wegen ihres hohen Freizeitwertes. Nicht selten verbringen Anwender täglich Stunden damit, mit anderen oder dem Anbietersystem zu kommunizieren und schaffen so einen neuen sozialen Raum¹⁸.

b) Computer Bulletin Board Systems (BBS):

BBS sind gewissermaßen die Taschenausgabe der kommerziellen On-line-Anbieter, allerdings nicht im Sinne einer Kopie, sondern einer eigenständigen Basisbewegung¹⁹. Wenn auch die Abgrenzung zwischen den beiden oft schwerfällt²⁰, so lässt sich sagen, dass BBS oft von einem handelsüblichen PC mit nur einer Telefonleitung betrieben werden, mit einer sehr kleinen Zahl von Anwendern, die sich per Modem in diesen PC einwählen. Oft ist der Zugang zum jeweiligen BBS gratis, weil der System Operator (Sysop), der den Haupt-PC betreut, das ganze System als Hobby betreibt. BBS bieten meist E-mail, elektronische Schwarze Bretter und Zugang zum Internet. Da BBS extrem einfach zu errichten sind, hat sich eine Vielzahl von spezialisierten BBS entwickelt. Von exotischen Fachthemen bis zu Neonazi-BBS reicht das Spektrum, so dass wohl mit Recht das BBS als das Massenkommunikationsmittel mit der geringsten Zugangsschwelle in der Geschichte der Menschheit beschrieben wurde (Ralph

¹⁷ Die folgende Übersicht stützt sich auf die Darstellung bei Cavazos/Morin, *Cyberspace and the Law*, 1994, S. 2 ff.

¹⁸ Eine Art Vorläufer waren hier die Kommunikationsdienste der 80er Jahre wie BTX in Deutschland oder Minitel in Frankreich. Zur Sonderstellung des französischen Minitel-Systems Rheingold (o. Fußn. 4), S. 220 ff. Vgl. auch Proissl, *Gefangen im eigenen Netz*, *Die Zeit* v. 14.6.96, S. 29. Obwohl in Frankreich die für Internet-Anfänger meist beeindruckende Pizza- oder Flugticketbestellung vom heimischen Computer aus schon längst Alltag ist, hat Frankreich doch den Anschluß an das Internet fast versäumt, nicht zuletzt wegen der Inkompatibilität von Minitel und Internet.

¹⁹ Zu BBS s. Rheingold (o. Fußn. 4), S. 131 ff. In Deutschland ist in diesem Zusammenhang der Begriff mail-box weit verbreitet.

²⁰ Ein bekanntes Beispiel für ein sehr großes BBS ist das in Kalifornien gegründete regionale Netz WELL (Whole Earth 'Lectronic Link), das seit 1992 auch Zugang zum Internet bietet, s. dazu Rheingold (o. Fußn. 4), S. 17 ff. Zwischen BBS und On-line Anbieter steht auch das juristische Diskussionsforum Lexis Counsel Connect (LCC) das in den U.S.A. bereits 16.000 zahlende Mitglieder zählt. Dort finden Diskussionen von Fachleuten aus der juristischen Wissenschaft ebenso wie aus der juristischen Praxis zu verschiedenen Rechtsgebieten und verschiedenen rechtspolitischen Fragen statt, s. Katsh (o. Fußn. 3); s. auch cconnect@reach.com.

Nader)²¹. Großen Raum nimmt auf den BBS auch der Tausch von - oftmals urheberrechtlich geschützten - Computerprogrammen ein. Die Sysops haben erheblichen Spielraum was die Ausgestaltung der BBS angeht, insbesondere im Hinblick auf Zugang und Teilnahmeregeln.

c) Private Systeme:

Eine Vielzahl von Systemen schließlich wird ausschließlich privat von Unternehmen oder Institutionen (u.a. Universitäten) errichtet und ist grundsätzlich nichtöffentlich. Solche Privatnetze bieten oft die klassischen BBS-Funktionen an oder aber eröffnen Zugang zu speziellen Datenbanken, zum Teil auch zum Internet.

d) Newsgroups auf dem Usenet:

Ähnlich wie die BBS erinnert das Usenet an ein schwarzes Brett, wobei Usenet lediglich ein Programm ist, das es ermöglicht, auf dem Internet E-mail Nachrichten nicht an eine einzelne Adresse, sondern gewissermaßen an ein schwarzes Brett zu einem bestimmten Thema zu schicken, wo die Nachricht von einer unbegrenzten Zahl von Lesern eingesehen werden kann²². Mittlerweile ist dies eines der größten Foren im Cyberspace mit zwischen 14.000 und 17.000 Newsgroups. Die On-line-Anbieter, BBS oder private Systeme, die Zugang zum Internet bieten (Internet-Provider), treffen für ihre Nutzer jeweils eine Auswahl von meist wenigen tausend Newsgroups.

e) Homepages auf dem World Wide Web (WWW):

Auch das WWW ist nur ein auf dem Internet fußendes Programm bzw. Protokoll und nicht etwa ein Anbieter²³; mit Hilfe von browsern (Navigationsprogrammen) werden homepages - gewissermaßen virtuelle Schaufenster - über eine Adresse mit dem Format <http://www.anwender> angesteuert, wo sich von Unternehmen über Institutionen bis zu Privatpersonen Anwender mit Informationen oder Produkten präsentieren können²⁴. Der Zugang zu einer solchen Homepage kann ganz oder teilweise von der Eingabe eines Kennwortes abhängig gemacht werden. Verbreitung und Qualität der Präsentation in Bild und Ton nehmen hier ständig zu²⁵.

²¹ S. Reid/Hume, Bulletin-Boards Make for Cut-rate Media Moguls, Chicago Tribune vom 8.12. 1991, S. C8.

²² Usenet Newsgroups beginnen meist mit einem von 8 Kürzeln: soc., news., talk., misc., sci., comp., rec., und alt. (letzteres steht für alternative Newsgroups, die - meist ohne jede Moderation - besonders wenig Regeln unterworfen sind), woran sich weitere, das Thema der Gruppe näher bezeichnende Kürzel anschließen.

²³ Die Entwicklung des WWW und der damit verbundenen Programmiersprache HTML wird im wesentlichen betreut durch ein Konsortium der Forschungseinrichtungen CERN, INRIA und MIT, s. <http://www.w3.org>.

²⁴ Zahlreiche Tageszeitungen können auf diesem Wege gelesen werden, auch deutsche Rechtsfakultäten sind mit Homepages auf dem WWW zu finden: die Humboldt-Universität Berlin etwa unter <http://www.rewi-hu-berlin.de>, die juristische Fakultät der Universität Saarbrücken zeigt auf <http://www.jura.uni-sb.de> u.a. Pressemitteilungen der obersten Bundesgerichte.

²⁵ Von 500 Anbietern in Herbst 1993 bis zu über 10.000 ein Jahr später, E. Katsh, Law in a Digital World, 1995, S. 39. Die Homepages erreichen teilweise bereits Fernsehqualität, mit der Übertragung bewegter Bilder beginnt sich die Grenze zu anderen Medien aufzulösen. Entwicklungen wie die Programmiersprache Java verbessern Interaktivität und Anwenderfreundlichkeit des WWW. Das VRML-Projekt (Virtual Reality Modeling Language) soll die Dreidimensionalität des WWW bringen, siehe <http://www.vrml.org>.

f) Computernetzwerke:

Computernetzwerke bestehen aus einzelnen Computern, die die Fähigkeit besitzen, untereinander Informationen auszutauschen. Alle oben beschriebenen Systeme können Bestandteil eines Netzwerkes sein. Das weltweit wichtigste Netzwerk ist das Internet. Verschiedene Programme bzw. Protokolle erleichtern die Kommunikation zwischen den vermittels Internet verbundenen Systemen²⁶. Erwähnenswert ist neben dem Internet das Fidonet, ein Netzwerk im wesentlichen von BBS²⁷. Wie bereits erwähnt, sind Netzwerke vielfach dezentral organisiert und von keiner Zentralgewalt kontrollierbar, vielmehr herrscht in diesen Netzwerken eine überraschend effektive Anarchie.

²⁶ Telnet erlaubt den Zugang vom jedem beliebigen Computer in der Welt, der an das Internet angeschlossen ist (node) zu jedem anderen node, als ob man an einem Terminal arbeitet, das unmittelbar an den angewählten Computer angeschlossen ist. Telnet existiert seit 1972, vgl. RFC 318, <http://ds.internic.net/rfc/rfc318.txt>, RFC 854 <http://ds.internic.net/rfc/rfc854.txt>, RFC 855 <http://ds.internic.net/rfc/rfc855.txt>, STD 8. Das File Transfer Protocol (FTP) erlaubt es, Daten Files (wie etwa mit Textverarbeitungsprogrammen erstellte Textdateien, aber auch schlicht Software) auf dem Internet zu versenden. FTP existiert seit 1973, vgl. RFC 454 <http://ds.internic.net/rfc/rfc454.txt>, RFC 959 <http://ds.internic.net/rfc/rfc959.txt>, STD 9. E-mail Programme schließlich ermöglichen das Versenden und Empfangen elektronischer Post. Gopher oder World Wide Web (WWW) sind Programme bzw. Protokolle, die mit Hilfe von Zugriffsprogrammen benutzerfreundlich Zugang zu von Anbietern bereitgehaltenen Informationen bieten.

²⁷ Fidonet arbeitet im Gegensatz zum Internet nicht in Echtzeit, d.h. es besteht keine permanente Verbindung, die Verbindung wird erst hergestellt wenn erforderlich.

2. Aktivitäten

Oft werden die Begriffe Cyberspace, Internet, E-mail etc. synonym verwandt und die Abgrenzung zwischen dem, was man im virtuellen Raum tun kann und der Frage, wo man es tun kann, übersehen. Daher im folgenden ein kurzer Überblick über mögliche Aktivitäten im Cyberspace, wobei zu beachten ist, dass diese Aktivitäten meist nicht an eine der oben beschriebenen Substrukturen gebunden sind: so lässt sich etwa E-mail sowohl von einem kommerziellen On-line-Anbieter aus, wie auch von einem BBS oder einem privaten System aus versenden (zusammenfassend spricht man auch von Internet-Providern).

a) E-mail:

Die Übermittlung von elektronischer Post, für die sich der Begriff Electronic Mail (E-mail) durchgesetzt hat²⁸, stellt wohl die wichtigste Aktivität dar. Dabei werden wie im realen Briefverkehr zwischen Individuen Texte ausgetauscht; der am Computer erstellte Briefftext wird an den mit der typischen E-mail Adresse individualisierten Empfänger gesandt; dieser findet den Brief dann in seinem elektronischen Briefkasten vor, wenn er sich das nächste Mal in das System begibt. Auf dem Internet bedeutet eine Adresse mit dem Format "benutzer@computer.system", dass die Botschaft an ein Computersystem mit der Kennung "computer.system" weitergeleitet wird und dort dann im elektronischen Briefkasten von "benutzer" abgelegt wird. In einem On-line-Dienst oder einem BBS ist der mögliche Adressatenkreis oft auf die jeweiligen Systemnutzer beschränkt. Ist das System jedoch Teil eines Netzwerkes oder mit einem Netzwerk verbunden, wird dieser Kreis erheblich erweitert. E-mail weist gegenüber herkömmlicher Post erhebliche Vorteile auf; so kann etwa ein E-mail vom Empfänger durch Tastendruck weitergesandt werden, die Adressatenzahl ist beliebig wählbar. Gleichwohl kann auch bei umfangreichem Verteiler immer noch individuell geantwortet werden, da Zustelldauer (meist nur wenige Minuten) und -kosten sehr gering sind. Oft können den Botschaften Text-, Bild- oder sonstige Datendateien "angehängt" werden. Verbreitet sind auch mailing lists; dabei werden E-mail-Beiträge zu einem bestimmten Thema abonniert.

b) Public Messaging Systems:

Hierbei wird eine elektronische Botschaft zu einem bestimmten Thema gewissermaßen an ein öffentlich zugängliches elektronisches schwarzes Brett geheftet, eine message base oder auch newsgroup, wo andere Benutzer diese dann lesen können und ihrerseits in elektronischen Botschaften reagieren, woraus sich dann eine ganze Folge von Texten zu einem bestimmten Thema ergibt (thread). Newsgroups verbinden meist Nutzer aus voneinander völlig unabhängigen Systemen. In manchen Messaging Systemen gehen die Botschaften vor der Veröffentlichung an einen Moderator, der in der Regel die Diskussion steuert und moderiert. Usenet, ein verbreitetes Messaging System, das in erster Linie über Internet funktioniert, kennt jedoch keine solche Moderation, d.h. jeder Beitrag auf dem Usenet kann grundsätzlich von allen Usenet-Nutzern zur Kenntnis genommen werden.

²⁸ E-mail Adressen enthalten immer das '@' (lies: at) Zeichen und haben meist das Format user@computer.system, Grundlage hierfür ist das Domain Name System (DNS), es handelt sich dabei um eine handlichere Fassung der IP-Adressen, einer 32 bit-Zahlenreihe.

c) Software, Datenübertragung:

Cyberspace eröffnet die Möglichkeit, umfangreiche Computerprogramme und -dateien in kürzester Zeit zu transferieren. Auf BBS werden Programme oft nach strengen Regeln geradezu wie eine Währung gehandelt. Spezielle Programme wie Archie helfen dabei, Software auf dem Internet zu lokalisieren.

d) Electronic Publishing:

Ist ein Verleger herkömmlicherweise darauf angewiesen, neben den Produktionsstätten auch einen Vertrieb zur Verfügung zu haben, so ermöglichen On-line-Systeme und Computernetzwerke auch Einzelnen mit begrenzten Ressourcen, einen großen Adressatenkreis zu erreichen. Zahllose elektronische Publikationen (zines) existieren mittlerweile. Das Abonnement kommt denkbar einfach durch ein E-mail an den Herausgeber zustande, worauf dann die jeweilige Ausgabe der Publikation direkt in den elektronischen Briefkasten des jeweiligen Nutzers gesandt wird. Es finden sich dabei Publikationen, die in Papierform gar nicht existieren ebenso wie elektronische Ausgaben herkömmlicher Printmedien, letztere zunehmend auf dem World Wide Web.

e) Unterhaltung:

Neben den üblichen Computerspielen und elektronischen Versionen etwa der bekannten Brettspiele finden sich im Cyberspace auch komplexe interaktive Rollenspiele, sogenannte MUDs (Multiuser Dungeons).

f) Direkte Kommunikation (chat):

Schließlich existiert die Möglichkeit zum (fast) Echtzeitdialog via Bildschirm zwischen unbegrenzt vielen Teilnehmern. Auf dem Internet etwa finden sich unter der Bezeichnung IRC (Internet Relay Chat) sogenannte Kanäle zu verschiedenen Themenkreisen, auf denen ständig lebhaft diskutiert wird. Fortgeschrittenere Systeme ermöglichen es, aus der Gruppendiskussion in "privatere Räume" auszuweichen, wo die Kommunikation nur in einem ausgesuchten Teilnehmerkreis stattfindet. Auf dem Internet ist mit dem Talk-Programm (fast) Echtzeit-Kommunikation von Bildschirm zu Bildschirm möglich. Die großen On-line-Dienste bieten oft Vorträge von Gastrednern an, an die elektronisch Fragen gerichtet werden können, so dass sich elektronische Dialoge entwickeln.

Auch Sprachübertragung ist heute über das Internet möglich. Von der israelischen Firma Vocaltec²⁹ im Frühjahr 1995 erstmals - allerdings noch in mäßiger Übertragungsqualität - demonstriert, hat sich die Technik in diesem Bereich mittlerweile so weit entwickelt, dass schon von einer Revolution gesprochen wird. Auch bei dieser Erfindung standen militärische Nutzungsmöglichkeiten am Anfang. Auch hier ergeben sich neue rechtliche Fragen: In den USA hat die America's Carriers Telecommunications Association (ACTA) im Frühjahr 1996 die zuständige Aufsichtsbehörde für den Fernspreverkehr, die Federal Communications

²⁹ <http://www.vocaltec.com>.

Commission (FCC), angerufen, um ein Verbot der neuen Technologie zu erreichen³⁰. In Deutschland stellen sich hier Rechtsfragen im Zusammenhang mit dem Telefonmonopol - immerhin ist mit diesen Programmen per Internet weltweites 'Telefonieren' fast gratis oder zum Ortstarif für die Einwahl zum nächsten Internet-Node möglich. Zum Teil wird argumentiert, die Sprachübertragung per Internet falle nicht in den Bereich des Telefonmonopols, weil keine verzögerungsfreie Echtzeitkommunikation stattfindet, da die Sprache in Datenpaketen zerlegt verschickt wird³¹.

Der nächste Schritt in der technischen Entwicklung des Internet ermöglicht Sprach- UND Bildübertragung, die Kommunikation findet dann nicht mehr über die per Tastatur eingegebenen Texte statt wie bei Talk oder IRC, sondern wie beim Bildetelefon von Angesicht zu Angesicht³².

g) Bildungs- und Forschungseinrichtungen:

Neben dem Zugang zu den Katalogen der großen Bibliotheken dieser Welt vom heimischen Schreibtisch aus, erschließt sich über Cyberspace die ganze Fülle existierender Datenbanken zu bestimmten Fachgebieten³³.

h) Kommerzielle Anwendungen:

Die Welt der Unternehmen ist dabei, Cyberspace zu entdecken. Elektronisches Einkaufen wird immer selbstverständlicher werden, Handelsbeziehungen finden elektronisch statt, Geschäftskorrespondenz wird elektronisch abgewickelt, Kundenbetreuung erfolgt ebenfalls auf elektronischem Wege. Sobald eine Einigung über ein Zahlungssystem³⁴ im Internet erzielt worden ist, wird dieser Bereich an Bedeutung noch zunehmen.

³⁰ Antrag vom 4. März 1996. Gegen die durch den Antrag beabsichtigte Beschränkung des 'telephonierens' auf dem Internet hat sich darauf eine Interessengruppe konstituiert, die Voice on the Net Coalition, vgl.

<http://www.von.org>, vgl. auch N. Tortello/P. Lointier, Internet pour les Juristes, 1996, S. 16 f.

³¹ S. im einzelnen Borchers, Vom blechernem Reden zum großen Geschäft, Die Zeit v. 16.8.1996, S. 54

³² Vgl. dazu etwa das CU-Seeme-Projekt an der Cornell University, <ftp://cuseeme.cornell.edu/pub/CU-seeMe>.

³³ In den U.S.A. etwa bieten LEXIS-Nexis und Westlaw den Juristen nationale und internationale Gerichtsentscheidungen sowie Fachaufsätze im Volltext, <http://nex.lexis.nexis.com>.

³⁴ Dazu s. Perritt, CyberPayment Infrastructure, 1996 Journal of Online Law, article 6, s. <http://www.wm.edu/law/publications/jol/>.

III) Rechtliche Problemfelder

1. Datenschutz und Persönlichkeitsrecht³⁵

a) *Datenschutz*

Die Frage, wie Daten vor unbefugter Benutzung bzw. unbefugtem Zugriff zu schützen sind, hat in Zusammenhang mit der Entstehung der sogenannten Hacker-Subkultur bereits frühzeitig öffentliches Aufsehen erregt und den Gesetzgeber strafrechtliche Sanktionen³⁶ für diese neue Art von Kriminalität formulieren lassen. Der Begriff Hacker stand zunächst für jemanden, der sich lediglich Zugang zu einem Computersystem verschaffte um es zu erkunden. Dieser ursprüngliche Idealismus bzw. dieses Ethos ist im Verschwinden begriffen, Hacker werden zunehmend mit Datendiebstahl und ähnlichen Delikten in Verbindung gebracht³⁷.

Probleme bereiten hier immer noch Uneinheitlichkeiten in den Sanktionsmechanismen³⁸ und die praktische Verfolgung von Straftaten. Da sich "Handlungen" im Cyberspace oft nicht ohne weiteres einer realen Person zuordnen lassen, wird das Aufspüren eines Eindringlings in ein Computersystem häufig nur bis zu einem bestimmten Telefonanschluss möglich sein, von dem aus der Täter gearbeitet hat, und dem es häufig gelingt, auch diese Spur zu verwischen³⁹. Neben diesen Verfolgungsschwierigkeiten, die oftmals dadurch ergänzt werden, dass in den Verfolgungsbehörden menschliche und technische Ressourcen hinter denen der Straftäter zurückbleiben⁴⁰ (vgl. etwa für die USA den Fall *Steve Jackson Games Inc. v. United States Secret Service*⁴¹), ergeben sich für Straftaten im Cyberspace erhebliche

³⁵ Zu Information und 'Privacy' s. allgemein O. H. Gandy Jr., *The Panoptic Sort*, 1993.

³⁶ Für die Bundesrepublik s. etwa das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität aus dem Jahre 1986.

³⁷ Zu Hackern s. S. Levy, *Hackers: Heroes of the Computer Revolution*, 1984, S. 23 f.; M. P. Dierks, *Electronic Communications and Legal Change: Computer Network Abuse*, 6 *Harvard Journal of Law and Technology* 307, 309 (1993); zur Frage, wie "hacken" ohne Schädigungsvorsatz und daraus resultierenden Schaden zu würdigen ist, s. *United States v. Morris*, 928 F.2d 504, 509 (2d Cir.), und 112 S. Ct. 72 (1991). In Deutschland machte bereits Ende der 80er Jahre der Fall Hans Heinrich Hübner Schlagzeilen, der gegen Geld an den KGB (allerdings wertlose) Daten verkaufte, s. T. Ammann u.a., *Hacker für Moskau*, 1989. In diesem Zusammenhang ist auch die Cyberpunk-Bewegung zu erwähnen, die stark beeinflusst durch Gibsons Roman (s.o.) den Versuch unternimmt, gewaltsam Ungleichheiten beim Zugang zum Cyberspace zu beseitigen, s. K. Hafner/J. Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, 1991, zum gesamten Thema auch B. Sterling, *The Hacker Crackdown*, 1992.

³⁸ M. P. Dierks (o. Fußn. 37), S. 330, weist darauf hin, daß die gleiche Handlung im Cyberspace bereits innerhalb der U.S.A. zu unterschiedlichen strafrechtlichen Würdigungen gelangen kann, weil dort Strafrecht nicht in der Kompetenz der Bundesgewalt liegt. Beispielfhaft sei hier erwähnt der Fall niederländischer Hacker, die im Jahre 1991 in U.S.-Militäreinrichtungen eindringen, ohne dafür in den Niederlanden belangt werden zu können; J. Markoff, *Dutch Computer Rogues Infiltrate American Systems with Impunity*, *New York Times* vom 21.4. 1991, Section 1, Part 1, S. 1.

³⁹ Dierks (o. Fußn. 37), S. 333.

⁴⁰ Bezeichnenderweise wurde in den U.S.A. der jahrelang flüchtige Hacker Kevin Mitnick letztlich mit Hilfe eines anderen Hackers gestellt, s. *New York Times* vom 16.2. 1995, S. A1, zu Mitnick vgl. auch Hafner/Markoff (o. Fußn. 37), S. 13-137.

⁴¹ 816 F.Supp 432 (W.D.Tex. 1993), s. dazu auch Cavazos/Morin (o. Fußn. 17), S. 22 ff. und Tortello/Lointier (o. Fußn. 30), S. 138. Dokumente über die Sondertelephonlinien für die landesweite Notrufnummer waren über das Internet bekannt geworden, der Secret Service nahm daraufhin eine Hausdurchsuchung bei Steve Jackson vor,

Beweisschwierigkeiten aus der besonderen Struktur des Cyberspace⁴². Der Fall Jackson belegt allerdings auch, dass der Datenschutz nicht nur von privaten Hackern bedroht wird, sondern dass auch staatlichen Stellen Grenzen gesetzt sein müssen. Die dem Grundrechtsschutz dienenden Beweisgewinnungs- und Beweisverwertungsverbote des Strafprozessrechts dürften hier im wesentlichen Anwendung finden. Das Gericht entschied im Fall Jackson, dass der Secret Service durch die systematische Durchsichtung der gesamten E-mail Korrespondenz von Jackson den Electronic Communications Privacy Act (ECPA) verletzt hatte. Jackson bekam 50.000 US-Dollar Schadensersatz zugesprochen; jeder, dessen E-mails bei der Durchsichtung gelesen worden waren, war zu 1000 US-Dollar Schadensersatz berechtigt. Zur Abgrenzung von Datenschutz und Tatenschutz.

Obwohl die Qualität der Sicherung von Daten ständig zugenommen hat, stellt Sicherheit in Computernetzen noch immer ein Problem dar⁴³. Gerade E-mail wird, was Schutz vor unbefugtem Einblick angeht, immer noch als extrem unsicher eingestuft⁴⁴. Angesichts der zunehmenden Computerisierung etwa von Bankgeschäften ist dies sicherlich durchaus ein besorgniserregender Befund, wobei allerdings die Gefahr oft überzeichnet wird⁴⁵.

In einem gewissen Sinne ist es schlechthin unausweichlich, dass Computernetzwerke durchlässiger sind als ein verschlossener stählerner Aktenschrank⁴⁶. Genauso unvermeidbar ist, dass die Vernetzung von Computern die Verbreitung sogenannter Computerviren vereinfacht. Diese Kosten stehen den positiven Aspekten einer zunehmenden Computerisierung bis zu einem gewissen Grad nahezu unvermeidbar gegenüber.

Neben dem Schutz von Daten vor Zugriff durch Unbefugte tritt die Frage, was Befugte mit den ihnen zugänglich gemachten Daten anfangen dürfen. Sie ist rechtlich kaum geklärt. Technisch ohne weiteres möglich und mittlerweile durchaus verbreitet ist die Sammlung von Daten durch Anbieter über das Netzverhalten von Nutzern⁴⁷. Die Entwicklung eines diesbezüglichen Problembewusstseins und entsprechender Vorsicht der Nutzer bei der Preisgabe von Informationen würde bereits einiges zur Verbesserung der Situation beitragen.

dieser hatte mit der Veröffentlichung der Dokumente jedoch nichts zu tun und erreichte im anschließenden Rechtsstreit eine Entschädigung.

⁴² Dierks (o. Fußn. 37), S. 334 weist etwa daraufhin, daß im Cyberspace in der Regel weder Augenzeugen noch Fingerabdrücke existieren. S. auch Bär, CR 1995, 158 und 227; 489.

⁴³ S. dazu J. Quittner, Cracks in the Net, TIME vom 27.2. 1995, S. 34 ff.

⁴⁴ S. dazu J. I. Schiller, Secure Distributed Computing, Scientific American, November 1994, S. 72; zu Datenmißbrauch im Cyberspace s. Dierks (o. Fußn. 37). Zur Sicherheit von WWW-Homepages s. T. Hardy, The Ancient Doctrine of Trespass to Web Sites, Journal of Online Law, Article 7 <http://www.wm.edu/law/publications/jol>.

⁴⁵ Von einer Übertreibung der Gefahren in quantitativer Hinsicht und einer Fehleinschätzung in qualitativer Hinsicht spricht etwa Dierks (o. Fußn. 37), S. 319 ff.

⁴⁶ Katsh (o. Fußn. 3), S. 1163.

⁴⁷ Das Center for Democracy and Technology in Washington hat eine Demonstration auf seiner Homepage eingerichtet, die illustriert, welche Datenspur der Nutzer unbewußt beim 'Surfen' auf dem WWW hinter sich läßt. <http://www.cdt.org/privacy/>.

b) Tatenschutz?

Eine andere rechtliche Problematik ergibt sich in neuerer Zeit daraus, dass die Entwicklung des Computers vom Daten- zum Kommunikationsträger das Interesse des Staates nach sich zieht, diese Kommunikation zumindest in einigen begründeten Fällen auch überwachen zu können. Zu erinnern ist hier daran, dass Anleitungen zur Herstellung einer Bombe wie sie in den USA das Federal Building in Oklahoma City zerstörte, auf dem Internet zirkulieren, was belegt, dass potentielle Täter im Bereich politisch motivierter Straftaten Cyberspace als Kommunikationsraum längst entdeckt haben⁴⁸. Die Neonazi-Szene im deutschsprachigen Raum etwa hat sich mit dem sogenannten Thule-Netz ein eigenes BBS geschaffen⁴⁹. Hier stellen sich im einzelnen schwierige Fragen der Abwägung zwischen Verfolgungsinteressen des Staates und Rechten des Einzelnen.

Das neue Telekommunikationsgesetz des Bundes⁵⁰ verpflichtet beispielsweise Diensteanbieter dazu, den Sicherheitsbehörden aktuelle Kundendateien automatisiert zugänglich zu machen (§ 87 Absatz 2). Den Sicherheitsbehörden sind die Auskünfte zur Erfüllung ihrer gesetzlichen Aufgaben zu erteilen, eine Generalklausel, die praktisch kaum kontrollierbar sein dürfte⁵¹.

Neben der Frage nach der Rechtsgrundlage für das "Abhören" von Computerkommunikation ergeben sich Probleme aus der Tatsache, dass - anders als etwa beim realen Gespräch oder beim leitungsgebundenen Telefongespräch - wegen der technischen Entwicklung im Bereich der Kodierungsprogramme schon technisch der Staat möglicherweise gar nicht mehr in der Lage ist, im Cyberspace "abzuhören"⁵². Der U.S.-amerikanische Geheimdienst NSA (National Security Agency) hatte zunächst versucht, diesen Trend durch den Escrowed Encryption Standard zu steuern: Der Clipper Chip (bzw. der Capstone Chip) sollte als Standard-Verschlüsselungsmechanismus für alle Telekommunikation Sicherheit gegen jegliches Abhören bieten, mit Ausnahme von Abhören durch befugte Regierungsstellen wie dem FBI, die gewissermaßen einen elektronischen Zweitschlüssel erhalten hätten⁵³. Die Idee scheiterte daran, dass die Computergemeinde mit dem PGP-Programm (Pretty Good Privacy) von Phil Zimmermann konterte⁵⁴, einem außerordentlich leistungsfähigen, gratis ausgegebenen Verschlüsselungsprogramm, zu dem die Regierung eben keinen "Nachschlüssel" besitzt. Diskutiert wird nun, ob der Staat eine Art elektronisches Vermummungsverbot erlassen kann, wonach elektronische Kommunikation für den Staat grundsätzlich lesbar sein muss⁵⁵. In Russland sind bestimmte Verschlüsselungsmechanismen schlichtweg verboten⁵⁶, die USA

⁴⁸ Vgl. dazu New York Times vom 25.4. 1995, S. A21.

⁴⁹ Nach Erkenntnissen des Bundesamtes für Verfassungsschutz sind allein 1994/95 14 Mailboxen neu eingerichtet worden, von denen im April 1996 12 als aktiv galten. Das Thule-Netz ist mittlerweile in Deutschland flächendeckend, s. BT-Drucksache 13/4350, Antwort der Bundesregierung, Neue Organisations- und Aktionsformen der rechtsextremen Szene, S. 6. Allgemein s. Schröder, Neonazis und Computernetze, 1995.

⁵⁰ vgl. Bundestags-Drucksache 13/3609.

⁵¹ S. im einzelnen Ruhmann, Das Geheimnis der dritten Leitung, Die Zeit v. 10.5.1996.

⁵² Zur Angst der Behörden davor, die Kontrolle über die elektronische Kommunikation zu verlieren s. A. M. Froomkin, The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 University of Pennsylvania Law Review 595, 630 ff. (1995); laut FBI spielt elektronisches Abhören eine Rolle in durchschnittlich 2200 Fällen pro Jahr, ebd. S. 631. Für Deutschland s. etwa Bundestags-Drucksache 13/4105, Antwort der Bundesregierung, Sicherheit der Informationstechnik und Kryptierung.

⁵³ Nachweise bei Froomkin (o. Fußn. 52), ähnlich auch ein Vorstoß des FBI, Digital Telephony Proposal, Cavazos/Morin (o. Fußn. 17), S. 31.

⁵⁴ Cavazos/Morin (o. Fußn. 17), S. 30 f.

⁵⁵ Dazu grundsätzlich Froomkin (o. Fußn. 52), S. 709.

⁵⁶ S. Kuner, NJW-CoR 1995, 413.

verbieten (zumindest in der Theorie) noch immer den Export von Verschlüsselungssoftware. In Frankreich unterliegt Verschlüsselung diversen Restriktionen⁵⁷.

Solche Verbote sind jedoch bereits im Ansatz verfehlt: Solange Cyberspace nationale Grenzen überwindet, die Verschlüsselung ihrerseits jedoch unüberwindbar ist, kann ein nationales elektronisches Vermummungsverbot schon gar nicht wirksam durchgesetzt werden. Zwar wird der grenzüberschreitende Aspekt dieser Fragen mittlerweile erkannt. Die staatlichen Stellen, die der NSA entsprechen (auf deutscher Seite das Bundesamt für Sicherheit in der Informationstechnik, BSI) pflegen folgerichtig regelmäßig multilateralen internationalen Erfahrungsaustausch⁵⁸. Ausdruck der Einsicht in die Notwendigkeit von staatenübergreifenden, einvernehmlichen Regelungen ist auch, dass etwa auf der Ebene der OECD zwischen den USA und Europa über einheitliche Regelungen verhandelt wird. Offen ist ohnehin die Frage, ob nicht doch bestimmte Dienste wie die NSA (die über eine eigene Chipherstellung verfügt) durch den Einsatz nachrichtendienstlicher Mittel entweder Hardware oder Verschlüsselungssoftware vor dem Vertrieb preparieren (lassen) können bzw. unmittelbar am Erfinder von Verschlüsselungsprogrammen ansetzen und so einzelnen Staaten der Zugang zu Daten ohnehin gesichert ist⁵⁹.

Solange jedoch die Entwicklung der Verschlüsselungstechnik nicht unter lückenloser staatlicher Kontrolle steht, kann auch eine intensive Kooperation der Staaten wenig ausrichten. Nachdem es heute dank privat entwickelter Programme möglich erscheint, verschlüsselte Daten so zu versenden, dass sogar die Tatsache der Verschlüsselung unerkannt bleibt, indem etwa Textdateien in dem Datenmeer einer Photodatei versteckt sind, wird teilweise sogar die völlige Freigabe der Verschlüsselungstechnik erwogen⁶⁰.

Da das Verbot von Kryptographie sich schon wegen der mit der Datensicherheit verknüpften Weiterentwicklung der kommerziellen Nutzungsmöglichkeiten des Internet und der hier wirkenden Interessen nicht durchhalten lässt, richtet sich die Diskussion nun darauf, dass Anwender zwar Verschlüsselung benutzen dürfen, jedoch ihre elektronischen Schlüssel unabhängigen Einrichtungen (*Trusted Third Parties, Trustcenter*) überlassen⁶¹. Auch die Entwürfe zu einem deutschen Kryptographie-Gesetz gehen in diese Richtung⁶², wobei noch nicht absehbar ist, ob nicht auch hier der aussichtslose Versuch unternommen werden wird, den zuständigen Sicherheitsbehörden eine elektronische Hintertür offenzulassen⁶³. Mit jeder Standardisierung der Verschlüsselungsmöglichkeiten wird allerdings auch das staatliche Drängen auf Kontrollmöglichkeiten wieder zunehmen.

⁵⁷ Einzelheiten bei Piette-Coudol/Bertrand, (o. Fußn. 4), S. 76 ff. und Tortello/Lointier (o. Fußn. 30), S. 141 ff. Dies gilt auch nach dem Gesetz vom 26. Juli 1996.

⁵⁸ Bundestags-Drucksache 13/1405, S. 2.

⁵⁹ Vgl. Lauscher im Datenreich, Der Spiegel 36/1996, S. 194 ff.

⁶⁰ Zur Verschlüsselung der Verschlüsselung durch das Program Stego s. Siegele, Talent für beides, Die Zeit v. 14.6f.96, S. 70, s. auch <http://www.fqa.com/romana>.

⁶¹ Siehe dazu Piette-Coudol/Bertrand, (o. Fußn. 4), S. 98. Zur Bedeutung von Trusted Third Parties für die ökonomische Entwicklung des Internet s. A. M. Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, 75 Oregon Law Review 49 (1996).

⁶² Siehe Borchers, Der Kampf um die Schlüsselgewalt, Die Zeit v. 14.6.96, S. 70.

⁶³ Siehe Big Brother bald auch im Internet. Bund will Verschlüsselungsprogramme für Computer verbieten - es sei denn, die Behörden dürfen mitlesen, Tageszeitung v. 24.12.96, S. 4.

c) Identität

Schließlich stellen sich datenschutzrechtliche Fragen im Zusammenhang mit dem Phänomen, dass die Identität einer Person im Cyberspace von anderen mit dieser Person Kommunizierenden anders als in der echten Welt nicht ohne weiteres nachprüfbar ist, sondern die Annahme einer bestimmten Identität im Cyberspace auf der nicht ohne weiteres nachprüfaren Identitätsbehauptung eines Kommunikationspartners beruht⁶⁴. Dies bedeutet etwa, dass sich im Cyberspace ein Mann ohne weiteres für eine Frau ausgeben kann und umgekehrt⁶⁵, ein Minderjähriger als volljährig usw., dass aber auch eine Vielzahl von Personen im Cyberspace als eine einzige Person auftreten kann. Dass sich hier Probleme ergeben, wenn Rechte und Rechtsfähigkeit an die Personenqualität geknüpft sind, liegt auf der Hand. Denkbar ist aber auch, hier auf lange Sicht interessante neue Formen von juristischen Personen entstehen zu sehen, eine rechtsfähige juristische Cyberspace-Person etwa⁶⁶.

Eng verknüpft mit der Problematik der Identität im Cyberspace ist auch das elektronische Namensrecht⁶⁷: Firmennamen und Warenzeichen sind als Namen im Cyberspace bisher nicht geschützt, so musste etwa BMW feststellen, dass die Adresse bmw.com bereits von einer kalifornischen Firma belegt war, ähnliches wiederfuhr McDonalds. Zu großen Problemen führt hier der Umstand, dass die Internet-Adressen national vergeben werden, dann aber weltweit gelten⁶⁸.

Die völlige Verschleierung der Identität ermöglichen sogenannte Re-mailer. Dabei werden E-mail-Nachrichten durch einen Computer aller Identifikationsmerkmale entkleidet und dann weitergesandt, der elektronische Brief wird gewissermaßen in einen neuen Umschlag gesteckt⁶⁹. Der Empfänger kann nur erkennen, dass die Nachricht von einem Re-mailer kommt. Manche Re-mailer bewahren immerhin die Daten der ursprünglichen Absender der Briefe auf. Hierbei stellt sich die Frage, inwieweit solche Re-mailer unter bestimmten Umständen gezwungen werden können, die Identität bestimmter Nutzer zu enthüllen. Auch hier klingt die Problematik vom elektronischen Vermummungsverbot an, dies ist jedoch nur eine der Fragen im Zusammenhang mit dem hier zentralen Aspekt des Grundrechts auf freie Meinungsäußerung⁷⁰. Allerdings sollte man sich vor Augen halten, dass die anonyme Kommunikation auch positive Aspekte bietet; so erklärt sich der Erfolg von Newsgroups, auf denen etwa Opfer von Kindesmisshandlungen Menschen in der gleichen Lage vorfinden, zum großen Teil aus der Möglichkeit, die eigene Identität nicht offenbaren zu müssen. Von daher wäre zu überlegen, inwieweit die Cyberspace-Identität oder Anonymität nicht auch rechtlichen Schutz verdient. Aufsehen hat in diesem Zusammenhang ein Fall erregt, bei dem

⁶⁴ Zu Identität und Anonymität im Cyberspace s. G. P. Long III, Who are you? Identity and Anonymity in Cyberspace, 55 University of Pittsburgh Law Review 1177 (1994).

⁶⁵ Dazu s. D. Sagan, Sex, Lies and Cyberspace, Wired, Januar 1995, S. 78 ff.

⁶⁶ Ähnlicher Vorschlag bei L. Rose, NetLaw, 1995, S. 60 ff. ("virtual corporation").

⁶⁷ Siehe allgemein Piette-Coudol/Bertrand, (o. Fußn. 4), S. 93 ff. und Kur, CR 1996, 590.

⁶⁸ Für weitere Beispiele vgl. "Was Dein ist, gehört mir", Der SPIEGEL 20/1995, S. 206 ff. und Too many loopholes in the Net?, The Economist vom 1.7. 1995, S. 15. Die Scientology-Organisation etwa hat gegenüber einem Verwender der Adresse www.scientologie.org und der die Domainnamen in den USA verwaltenden Einrichtung (InterNIC) ein Urheberrecht auf den Begriff Scientology in allen Schreibweisen geltend gemacht, vgl. Baumgärtel, Scientology gegen Scientologie, Die Tageszeitung v. 15.8.1996, S. 12. Für die Linie der Rechtsprechung in Deutschland vgl. die Entscheidung des LG Mannheim in CR 1996, 353.

⁶⁹ Zu anonymen Servern s. Long (o. Fußn. 64), S. 1183 Fußn. 28.

⁷⁰ Der U.S.-Supreme Court hat bereits 1960 festgestellt, daß die Teilnahme am öffentlichen Diskurs auch anonym möglich sein muß Talley v. California, 362 U.S. 60 (1960).

der bekannteste Re-mailer, der in Finnland ansässige anon.penet.fi⁷¹-Dienst durch die finnische Polizei gezwungen wurde, die Identität eines Users zu offenbaren, gegen den die amerikanische Scientology-Organisation in den USA wegen Verletzung von Urheberrechten prozessierte⁷².

Die völlige Auflösung der Identität im Cyberspace droht von Re-mailern, die nicht nur erlauben, die eigene Identität zu verbergen, sondern auch die eigene Identität durch eine beliebige andere Identität zu ersetzen, ohne dass der Empfänger einen Anhaltspunkt dafür hat, dass die Botschaft gar nicht vom angegebenen Absender stammt. Hier allerdings können elektronische Signaturen u.ä. eine gewisse (Rechts-)Sicherheit gewährleisten.

⁷¹ Gegründet im November 1992, mit bis Januar 1994 über 50.000 Nutzern. In Wired, Juni 1994, S. 370 ff. findet sich ein Interview mit Johan Helsinghuis, dem Betreiber von anon.penet.fi. Im September 1996 wurde die Einstellung des Betriebs von anon.penet.fi gemeldet, s. Die Zeit v. 13.9.1996, S. 78.

⁷² Vgl. "Was Dein ist, gehört mir", Der SPIEGEL 20/1995, S. 204; zu diesem Verfahren s. auch unten Fußn. 106.

2. Rechtsgeschäfte im Cyberspace

Auch im Bereich des an der physischen Welt orientierten Zivilrechts sind Probleme zu erwarten. Wenn mit der Einigung auf ein Abrechnungssystem bzw. kompatible Zahlungsmittel ('Cybercash') die letzten Schranken für die Kommerzialisierung des Cyberspace fallen⁷³, wird die damit verbundene verstärkte Nutzung des Internet im Rechtsverkehr zwischen Privaten diese Probleme verstärkt hervortreten lassen.

Die künftigen Schwierigkeiten sind vielfältiger Natur: Eine spezifisch mit der Kommerzialisierung verbundene Frage wird sich beispielsweise im Bereich der steuerlichen Erfassung (indirekte Besteuerung) des Cyberhandels stellen⁷⁴. Absehbar sind neue Fragen, die Vertragspflichten berühren: So hat etwa der U.S. Court of Appeals in Chicago entschieden, daß es eine Rechtspflicht geben kann, sich im Internet zu informieren (hier: Wertpapiergeschäfte)⁷⁵. Teilweise wird im privatrechtlichen Bereich ein ähnlicher Quantensprung für das elektronische Zeitalter erwartet, wie der, der durch die Möglichkeit, Verträge zu drucken (man denke nur an das sog. Kleingedruckte) eingetreten ist⁷⁶.

Weniger futuristisch erscheinen die Probleme, die sich im Zusammenhang mit den (formalen) Grundlagen des Zivilrechts stellen. Damit ist nicht gemeint das Problem, dass von unterschiedlichen Rechtssystemen aus Rechtsgeschäfte getätigt werden (Käufer in Deutschland, Verkäufer in den USA mit einem Lieferanten in Frankreich): hier kann bei fehlenden Parteiabsprachen wohl größtenteils auf das Instrumentarium des Internationalen Privatrechts zurückgegriffen werden, um zu ermitteln, welche Regeln für Leistungsstörungen, Gewährleistung, Verjährung usw. gelten sollen. Vielmehr bedarf es in Teilbereichen einer Anpassung des von den Rechtsordnungen für den alltäglichen Rechtsverkehr zwischen Privaten zur Verfügung gestellten formalen Instrumentariums, welches für das Zeitalter der elektronischen Kommunikation teilweise keine adäquaten Lösungen bietet. Dieser Aspekt wird im Folgenden anhand zweier Beispiele veranschaulicht: Erstens das Beispiel der Willenserklärungen durch E-mail und deren Zugang⁷⁷. Zweitens die Problematik von Schriftformerfordernissen und damit verwandten Fragestellungen (Unterschriften, Urkunden im Zivilrecht)⁷⁸.

⁷³ S. dazu Heuser, Marktplatz Internet, Die Zeit v. 10.5.1990, S. 17. Perritt (o. Fußn. 34) unterstreicht insgesamt die Bedeutung wirksamer Kryptographie als Voraussetzung für den Handel über das Internet. Regierungen und Banken dagegen fürchten um ihre Hoheitsrechte, s. Siegele, Wie werden wir morgen bezahlen?, Die Zeit v. 18.10.1996, S. 88.

⁷⁴ Piette-Coudol/Bertrand (o. Fußn. 4), S. 65, dies allerdings keine originär zivilrechtliche Frage.

⁷⁵ 67 F.3d 605, 7th Cir. 1995.

⁷⁶ Katsh, (o. Fußn. 25), S. 114 ff, dazu auch E. Eisenstein, The Printing Press as an Agent of Change I, 1979.

⁷⁷ Vgl. S. Heun, CR 1994, 595; Melullus, MDR 1994, 109; Burgard, AcP 195 (1995), 74; zum elektronischen Vertrag s. auch Cavazos/Morin (o. Fußn. 17), S. 40 ff.

⁷⁸ Vgl. S. Heun, CR 1995, 2.

a) Willenserklärung im Cyberspace

Grundelement der Rechtsgeschäftslehre ist die Willenserklärung, verstanden als Äußerung eines auf die Herbeiführung eines bestimmten Rechtserfolges gerichteten Willens. Eine elektronische Willenserklärung liegt dann vor, wenn sich Erklärender und Empfänger gleichermaßen eines elektronischen Mediums, etwa im Cyberspace, bedienen. Die Problematik des Zugangs einer solchen Willenserklärung illustriert, dass Anpassungen der überkommenen Regelungen erforderlich sind.

Im Gegensatz zur telefonischen Kommunikation⁷⁹ fehlt für die elektronische Willenserklärung eine gesetzliche Regelung. Gleichwohl lässt sich im Wege der Analogie ohne weiteres die Einwegkommunikation (E-mail, BBS) zu den Erklärungen unter Abwesenden - das Bild vom elektronischen Briefkasten legt diese Analogie bereits nahe - die Dialogkommunikation (Echtzeitkommunikation, etwa IRC) zu den Erklärungen unter Anwesenden rechnen⁸⁰: Schließlich werden statt Sprache (Telefon) lediglich Zeichen benutzt⁸¹.

Der häufigste Fall elektronischer Kommunikation wird im Bereich der Erklärungen unter Abwesenden liegen⁸². Hier gelten Willenserklärungen als zugegangen, wenn sie so in den Bereich des Empfängers gelangt sind, dass dieser unter normalen Umständen die Möglichkeit zur Kenntnisnahme hat⁸³. Was aber im elektronischen Zeitalter als Bereich des Empfängers anzunehmen ist, in dem die Kenntnisnahme möglich ist, erscheint fraglich.

Teilweise wird vertreten, dass das Übertragungsrisiko bis zum Ende des jeweiligen Übertragungsweges reichen soll. In aller Regel ist dieses Ende eine Telefonanschlussdose⁸⁴. Zugang liegt demnach auch dann vor, wenn Speicherung oder Ausdruck fehlschlagen, weil der Empfänger für die Funktionstüchtigkeit der von ihm bereitgestellten Einrichtungen verantwortlich sein soll⁸⁵. Wird eine Willenserklärung in einem System auf Abruf gespeichert (etwa E-mail), soll bereits mit der Möglichkeit des Zugriffes auf die Daten Empfang zu bejahen sein, so dass Zugang ab dem Zeitpunkt anzunehmen ist, zu dem der Empfänger üblicherweise Daten abrufen, wobei von einem Abruf mindestens einmal täglich wohl ausgegangen werden darf⁸⁶. Unklar bleibt hier allerdings, warum der Empfänger das Risiko fehlerhafter Übermittlung vom Abrufspeicher tragen muss: vermehrt findet Abruf etwa von E-mail nicht mehr von einem unmittelbar dem Computer mit Abrufspeicher angeschlossenen Terminal statt, sondern vom PC über Modem und Telefonleitung. Dies geschieht oft nicht einmal vom eigenen Gerät, sondern von öffentlichen Computern aus. Zugang wäre nach obiger Argumentation etwa dann zu bejahen, wenn eine elektronische Willenserklärung zwar im Abrufspeicher bereitstünde, der Nutzer jedoch wegen eines Ausfalles der Telefonleitungen keine Chance hätte, sich in den Großcomputer einzuwählen. Spätestens hier löst sich die

⁷⁹ Nach \square 147 Abs. 1 S. 2 BGB gelten hier die Regeln für die Erklärung unter Anwesenden.

⁸⁰ Heun (oben Fußn. 77), S. 597; eine Ausnahme für die Dialogkommunikation stellt der Fall dar, in dem auf einer Seite eine Computeranlage in den Dialog eingeschaltet ist, wie etwa bei einem Geldautomaten, dort wird man Erklärung unter Abwesenden annehmen müssen, Heun (oben Fußn. 77), S. 597 m.w.N.

⁸¹ Heun (o. Fußn. 77), S. 598.

⁸² Heun (o. Fußn. 77), S. 598.

⁸³ Palandt/Heinrichs, \square 130 Rz. 5.

⁸⁴ Heun (o. Fußn. 77), S. 598, a.A. Kuhn, Rechtshandlungen mittels EDV und Telekommunikation, 1991, S. 95, 99, 104.

⁸⁵ Heun (o. Fußn. 77), S. 599.

⁸⁶ Heun (o. Fußn. 77), S. 599 m. w. Nachw.

Analogie zum herkömmlichen Briefkasten auf, wenn sich Möglichkeit zur Kenntnisnahme einer Willenserklärung und Herrschaftsbereich nicht mehr decken.

Überlegenswert scheint vielmehr der Weg, sich zum Nachweis des Zugangs oder auch nur des Zugangszeitpunktes (Widerruf einer Erklärung unter Abwesenden ist nach § 130 Abs. 1 S. 2 BGB noch bis zum Zugang möglich, so dass der Bestimmung des Zugangszeitpunktes durchaus Bedeutung zukommt) der Informationen zu bedienen, die die Computerkommunikation ohnehin beinhaltet. Bei E-mail etwa erscheint die mit jeder Nachricht verbundene Protokollierung des Sendewegs einschließlich der Sende- und Empfangszeit als geradezu ideale Lösung: An Stelle von Mutmaßungen über Zugangszeitpunkte, verbunden mit der Verteilung von Übermittlungs- und Zugangsrisiken, mit denen sich das herkömmliche Zivilrecht in Ermangelung von Alternativen begnügen musste, ermöglicht die moderne Technik eine genaue Bestimmung des Zugangs⁸⁷. Sicherheit vor einseitiger Manipulation lässt sich durch entsprechende technische Vorkehrungen erzielen.

⁸⁷ Ein Beispiel aus dem E-mail-Bereich dafür, wie elektronische Kommunikation protokolliert wird: Hier wurde ein E-mail von A. Sender (E-mail Adresse asender@computer.edu) an Joe User (E-mail Adresse juser@machine.de) am 1. Januar 1998 um 13.06 gesandt und ist bei Joe User am selben Tag um 19.08 eingegangen: Return-Path: Received: by machine.de (Smail0.4.71.1) from computer.edu (100.007.007.00) with smtp id ; Thu, 1 Jan 1998 19:08:19 Received: from Toshiba Satellite.computer.edu (slipp8-13.computer.edu) by computer.edu with SMTP (1.00.007.08/15) id AA987654321; Thu, 1 Jan 1998 13:06:34 Date: Thu, 1 Jan 1998 13:06:34 Message-Id: <2.2.16.19970112130936.26873982@pop.computer.edu> X-Sender: asender@computer.edu X-Mailer: Windows Eudora Pro Version 4.0 Mime-Version: 1.0 Content-Type: text/plain; charset="us-ascii" To: Joe User From: A. Sender Subject: Hallo. Zuzugeben ist, daß Sendeprotokolle dort, wo Benutzer die entsprechenden Endgeräte selbst programmieren können - wie etwa Telefaxgeräte -, ohne zusätzliche Vorkehrungen nicht weiterhelfen; vgl. auch OLG München CR 1994, 98 f.; Heun (o. Fußn. 77), S. 599.

b) Schriftform und Unterschrift in Cyberspace

Willenserklärungen werden im Rechtsverkehr häufig schriftlich fixiert. Schrift existiert auch in Cyberspace noch, allerdings wird Schrift nicht mehr auf Papier oder einem anderen physisch wahrnehmbaren Medium aufgezeichnet, sondern in kodierter Form übermittelt. Damit stellen sich Rechtsfragen zum Beispiel im Hinblick auf den zivilrechtlichen und zivilprozessualen Urkundenbegriff, wonach Urkunden verkörperte Gedankenäußerungen in Schriftzeichen sind, als auch im Hinblick auf die Unterschrift, die eine Urkunde im Rechtsverkehr individualisiert⁸⁸.

Das elektronische Dokument unter den Begriff der Urkunde zu fassen, bereitet bereits deshalb Schwierigkeiten, weil der Ausgangspunkt hier das physisch wahrnehmbare Dokument ist, das ohne Hilfsmittel wie Bildschirm oder Drucker wahrgenommen werden kann⁸⁹. Dies ist bei der elektronischen Willenerklärung gerade nicht der Fall, sie wird nur durch den Bildschirm oder über den Ausdruck erst wahrnehmbar. Streiten lässt sich auch darüber, ob elektronische Dokumente durch Speicherung auf bestimmten Speichermedien überhaupt als eine Verkörperung der in dem Dokument enthaltenen Gedankenerklärung aufgefasst werden können⁹⁰.

Elektronischen Dokumenten aus diesen Gesichtspunkten heraus von vornherein die Urkundeneigenschaft abzusprechen⁹¹, greift in Anbetracht der zu erwartenden Entwicklung der Bedeutung von Cyberspace-Kommunikation jedoch wohl zu kurz. Irgendwann in der Zukunft muss es auch möglich sein, beispielsweise ein elektronisches Testament zu errichten, was derzeit noch am Erfordernis der eigenhändig geschriebenen und unterschriebenen Erklärung gemäß § 2247 BGB scheitert.

Unabhängig davon, ob Schriftform zwingend vorgeschrieben ist oder nicht, werden durch die Verneinung einer Urkundeneigenschaft elektronische Willenserklärungen und Abschlüsse von elektronischen Verträgen rechtlich erheblich benachteiligt. Schriftformerfordernisse sollen den Rechtsteilnehmer meist vor möglichen Gefahren eines Rechtsgeschäfts warnen, die Urkundeneigenschaft erzeugt dann eine gesteigerte Vertrauenswürdigkeit eines Dokumentes. Neben dieser Warnfunktion steht allgemein die Beweisfunktion. In zivilprozessualer Sicht betrifft die Beweisproblematik jeden Vertrag unabhängig von einem materiell-rechtlichen Schriftformerfordernis, kommt es doch im Rechtsverkehr häufig darauf an, Vertragsschluss und Vertragsinhalt zu beweisen. Hierzu ist dem Vertragspartner eines elektronischen Vertrages der Urkundenbeweis verwehrt. Jedoch bietet die elektronische Kommunikation durchaus technische Möglichkeiten, die genannten Bedürfnisse des Rechtsverkehrs zu bedienen: Beispielsweise kann die Beweisfunktion der Urkunde unter Erweiterung des herkömmlichen Urkundenbegriffes auf die elektronisch verkörperte Gedankenerklärung durch besonders schwer manipulierbare Speichermedien erzielt werden⁹².

⁸⁸ Zum Urkundenbegriff s. Thomas/Putzo, ZPO, Rdnr. 1 vor \square 415. Schriftformerfordernisse für bestimmte Willenserklärungen oder Verträge richten sich nach \square 126 BGB, wonach die Urkunde vom Aussteller eigenhändig durch Namensunterschrift oder notariell beglaubigtes Handzeichen unterzeichnet werden muß. Die Folge bei Nichteinhaltung dieser Bestimmung ist Nichtigkeit, \square 125 BGB.

⁸⁹ Heun (o. Fußn. 78), S. 3.

⁹⁰ Heun (o. Fußn. 78), S. 3 m. w. Nachw.

⁹¹ So Heun (o. Fußn. 78), S. 3.

⁹² Heun erwähnt hier die Beispiele des gesicherten Chips oder der nur einmal beschreibbaren Platte (WORM-Disk), Heun (o. Fußn. 78), S. 3; zu denken ist auch an eine Verschlüsselung, die jede Änderung des Textes erkennen läßt, wie etwa die hash-Funktion, bei der ein Dokument in eine numerische Darstellung übertragen wird, so daß Änderungen sofort erkennbar sind, s. näher dazu Cavazos/Morin (o. Fußn. 17), S. 42.

Die Unterschrift kann bei elektronischen Dokumenten nicht in der herkömmlichen Form erfolgen: Denkbar ist hier, sie durch eine faksimilierte Unterschrift oder durch eine individualisierte elektronische Kennung (elektronische Signatur⁹³) zu ersetzen. Zwar ist im Zusammenhang mit Telefax-Dokumenten die faksimilierte Unterschrift von den Gerichten entgegen dem Gesetzeswortlaut von § 126 BGB ("eigenhändig") anerkannt worden⁹⁴, jedoch wird gegen eine elektronische Signatur geltend gemacht, dass sie "kein vollständiges Funktionsäquivalent"⁹⁵ darstelle und dass im Rechtsverkehr die Gleichsetzung von Codeeingabe und eigenhändiger Unterschrift bewusstseinsmäßig noch nicht erreicht sei⁹⁶.

Was elektronische Signaturen betrifft, so ist in Deutschland der Gesetzgebungsbedarf durchaus erkannt. Das Multimedia-Gesetz vom August 1997 (siehe unten) sieht digitale Signaturen vor⁹⁷. Dabei sollen, ähnlich wie bei der Verschlüsselung (siehe oben), vertrauenswürdige Dritte (Trusted Third Parties), bei denen die Authentizität einer elektronischen Unterschrift durch Abgleich mit den dort vom Unterzeichner hinterlegten Daten überprüft werden kann, eine wichtige Rolle spielen⁹⁸. In den USA existieren bereits praktische Erfahrungen mit gesetzlich geregelten elektronischen Unterschriften/Signaturen (Utah Digital Signature Act)⁹⁹.

Zusammenfassend läßt sich feststellen, dass es durchaus Möglichkeiten gibt, das Recht an die neuen technischen Gegebenheiten anzupassen. Allerdings ist wieder darauf hinzuweisen, daß - in den gewählten Beispielen - der Ansatz am Zugangsbegriff des BGB oder am Urkundsbegriff der ZPO oder die Einführung einer elektronischen Signatur in Deutschland nur bedingt sinnvoll sind, wenn andere Rechtssysteme andere Regelungen vorsehen¹⁰⁰, weil mit der zunehmenden Nutzung des Internet der die Grenzen der Rechtsordnungen überschreitende Geschäftsverkehr weiter zunehmen wird: Der Umstand, daß Cyberspace außerhalb jeder geographischen, politischen oder jurisdiktionellen Grenze liegt, führt dazu, dass - neben den natürlich stets möglichen eindeutigen Parteiabsprachen - dauerhaft eine befriedigende Lösung in diesem Bereich nur in internationalen Standards zu finden sein dürfte¹⁰¹.

⁹³ Heun (o. Fußn. 78), S. 6 m. w. Nachw.

⁹⁴ BGH NJW 1989, 589, s. allgemein Wolf, NJW 1989, 2592.

⁹⁵ Heun (o. Fußn. 78), S. 6.

⁹⁶ Heun (o. Fußn. 78), S. 6, s. dort auch zum Sonderfall des \square 416 ZPO, der nach h.M. keine eigenhändige und handschriftliche Unterschrift erfordert.

⁹⁷ Vgl. auch Bundestags-Drucksache 13/4105, Antwort der Bundesregierung, Sicherheit der Informationstechnik und Kryptierung, vgl. auch Borchers, Der Kampf um die Schlüsselgewalt, Die Zeit v. 14.6.96, S. 70.

⁹⁸ Vgl. auch Piette-Coudol/Bertrand, (o. Fußn. 4), S. 98. Zur Bedeutung von Trusted Third Parties für die ökonomische Entwicklung des Internet s. A. M. Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, 75 Oregon Law Review 49 (1996).

⁹⁹ Utah Code 46-3-101 bis 46-3-504, eine gesetzliche Regelung von 1995, s. auch <http://www.law.vill.edu/~perritt/utahdsig.asc>. Auch die American Bar Association hat einen Entwurf in diesem Bereich vorgelegt, Information Security Committee, Electronic Commerce and Information Technology Division, ABA, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Electronic Commerce (Draft October 1995), s. http://www.law.vill.edu/vls/student_home/courses/computer-law/abaguid.htm.

¹⁰⁰ Für eine U.S.-amerikanische Sicht der Zugangsproblematik bei elektronischen willenserklärungen s. Cavazos/Morin (o. Fußn. 17), S. 40.

¹⁰¹ Im Ergebnis auf eindeutige Parteiabsprachen verweisend auch Cavazos/Morin (o. Fußn. 17), S. 41. Auch die sonst bei Konflikten zwischen Rechtssystemen hilfreiche Disziplin des Internationalen Privatrechts stößt in Anbetracht der Tatsache, daß sich Cyberspace nicht geographisch verorten läßt, auf gewisse Grenzen.

3. Geistiges Eigentum im Cyberspace

Die On-line mögliche blitzartige Vervielfältigung und Verteilung von Werken erschwert den Schutz geistigen Eigentums zunehmend¹⁰². Lösungsansätze für die Zukunft liegen hier in einer weiteren Internationalisierung des Urheberrechts¹⁰³, zum anderen in Fonds-Systemen (ähnlich der GEMA), wobei aus den Einnahmen der On-line-Anbieter und der Soft- und Hardwareproduzenten in einen Fonds gezahlt würde, aus dem Urheber von Werken für die Nutzung ihrer Werke entschädigt werden könnten (Entkoppelung von Urheberrecht und Schutzobjekt¹⁰⁴).

Im Mittelpunkt der geltendes Recht betreffenden Rechtsfragen stand bisher die Frage, inwieweit ein Anbieter von Diensten für Urheberrechtsverletzungen eines Nutzers (mit)haftet. In *Playboy Enterprises, Inc. v. Frena*¹⁰⁵ entschied ein U.S.-amerikanisches Gericht, dass ein BBS-Betreiber für die Verbreitung von Playboy-Fotografien über das BBS urheberrechtlich haften müsse. Der Betreiber Frena hatte allerdings Kenntnis davon, dass Nutzer eingescannte Fotografien aus der Zeitschrift Playboy verbreiteten. Anders noch die Entscheidung in *Cubby v. Compuserve*, wo Compuserve nicht für den Inhalt von Kommunikation verantwortlich gemacht wurde¹⁰⁶.

Zwischen der urheberrechtlichen Verantwortlichkeit eines Betreibers für von Nutzern unter Verstoß gegen Urheberrechte verbreitete Inhalte und der strafrechtlichen Verantwortlichkeit der Betreiber für von Nutzern verbreitete Inhalte bestehen gewisse Parallelen: der Betreiber kann die Überwachung der Tätigkeiten der Nutzer letztlich nicht vollständig gewährleisten. Der Rückgriff auf Anbieter bei Rechtsverletzungen ist danach nur möglich, wenn diesem die Rechtsverletzung ausnahmsweise wegen positiver Kenntnis zurechenbar und die Verhinderung der Rechtsverletzung zumutbar möglich ist.

¹⁰² Zum gesamten Problembereich vgl. D. L. Burk, Patents in Cyberspace: Territoriality and Infringement on Global Computer Networks, 68 Tulane Law Review 1 (1993). Die Software-Industrie kämpft bereits seit Jahren in ihrem Bereich gegen die Verletzungen des Urheberrechts durch Raubkopien von Programmen an, s. dazu A. L. Clapes, Software, Copyright and Competition, 1989. S. auch Mark A. Lemley, Dealing with Overlapping Copyrights on the Internet, University of Dayton Law Review 1 (1997); J. Littman, Reforming Information Law in Copyright's Image, 22 University of Dayton Law Review (1997); N. Elkin-Koren, A democratic approach to copyright in Cyberspace, 14 Cardozo Arts & Entertainment Law Journal 215 (1996); K. Aoki, (Intellectual) Property and Sovereignty, Notes Toward a Cultural Geography of Authorship, 48 Stanford Law Review 1293 (1996).

¹⁰³ Vgl. dazu die Berner Übereinkunft, der auch die Bundesrepublik beigetreten ist, BGBl II 1965, 1213) und die Arbeit der WIPO (Weltorganisation für geistiges Eigentum), s. auch D. Hatch, Better Late than Never: Implementation of the 1886 Berne Convention, Cornell International Law Journal 1717 (1989); nicht zu vergessen auch Entwicklungen im Rahmen des GATT bzw. der WTO (Agreement on Trade-related Aspects of Intellectual Property Rights, including Trade in Counterfeit Goods), s. dazu *Lehmann*, CR 1996, 2.

¹⁰⁴ Vgl. dazu die Praxis beim Softwareverkauf (Übertragung einer Nutzungslizenz statt Eigentumsübertragung). Zur Gestrigkeit des objektbezogenen Urheberrechts m. w. Nachw. zu neuen Ansätzen Katsh (o. Fußn. 25), S. 215 ff.

¹⁰⁵ 839 F. Supp., 1552 (M.D. Fla. 1993).

¹⁰⁶ 776 F. Supp. 135 (S.D.N.Y. 1991), s. dazu E. J. Naughton, 81 Georgetown Law Journal 409, 435 ff. (1992); s. in diesem Zusammenhang auch das Verfahren *Religious Technology Center, Bridge Publications v. Netcom*, Dennis Erlich, Tom Klemesrud, Clearwood Data Services, Az. C-95-20091 RHW, in dem die Scientology-Organisation wegen nicht autorisierter Veröffentlichung von Scientology Informationen einen On-Line-Dienst-Anbieter vor dem U.S. District Court Northern District of California San Jose Division verklagte; im Rahmen dieses Verfahrens wurde auch erstmals der bekannteste Re-mailer anon.penet.fi von den finnischen Behörden zur Preisgabe einer Identität gezwungen, s. Text zu Fußn. 72, vgl. auch "Was Dein ist, gehört mir", *Der SPIEGEL* 20/1995, S. 204.

Daraus folgt, dass der Ansatz entweder beim einzelnen Nutzer oder - im Urheberrecht - bei der Urheberrechte berührenden Tätigkeit (kopieren, vervielfältigen) erfolgen muss¹⁰⁷. Die Entwicklung in diesem Bereich wird möglicherweise einmal dazu führen, dass kostenlose Informationen im Internet seltener werden. Dafür besteht andererseits eine gewisse Aussicht darauf, dass dann auch mehr hochwertigere Informationen verfügbar gemacht würden.

¹⁰⁷ S. dazu Siegele, Der Dämon Copyright, Die Zeit v. 23.8.1996, S. 66 sowie die Erwiderung von Horst, Von Dämonen keine Spur, Die Zeit v. 13.9.1996, S. 78; siehe auch das Weißbuch der US-Regierung (US-Patentamt), <http://www.uspto.gov/web/ipni>.

4. Das Recht der freien Rede und Cyberspace - Wessen Werte? Wer kontrolliert?

In den USA wird die Frage der Meinungsäußerungsfreiheit im Cyberspace immer wieder heftig diskutiert¹⁰⁸; vielleicht ist dies gar die umstrittenste Rechtsfrage zu Cyberspace. Die hier berührten Probleme des Verfassungs- und des Strafrechts stellen sich in modifizierter Form auch anderswo:

Ebenso wie in den USA wird auch in Deutschland das Grundrecht auf freie Meinungsäußerung als "in gewissem Sinn die Grundlage jeder Freiheit überhaupt"¹⁰⁹ aufgefasst. Das Grundgesetz garantiert in Art. 5 Abs. 1 GG jedem das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten. Art. 5 Abs. 2 GG nennt als Schranken die Vorschriften der allgemeinen Gesetze, die gesetzlichen Bestimmungen zum Schutze der Jugend und das Recht der persönlichen Ehre. Die elektronische Datenübermittlung (elektronisch übermittelte Worte oder Bilder) ist wohl grundsätzlich als von Art. 5 GG umfasst anzusehen¹¹⁰. Fragen im Hinblick auf Schutzbereich und Schranken ergeben sich jedoch in anderer Hinsicht:

¹⁰⁸ S. dazu etwa *The Message in the Medium: The First Amendment on the Information Superhighway*, 107 *Harvard Law Review* 1062 (1994); C. R. Sunstein, *The First Amendment in Cyberspace*, 104 *Yale Law Journal* 1, (1995).

¹⁰⁹ BVerfGE 7, 198 [208] (Lüth-Entscheidung) unter Berufung auf Benjamin Cardozo.

¹¹⁰ Nach überwiegender Auffassung ist jedenfalls die elektronische Textübertragung geschützt, v. Münch/Wendt, GG, Art. 5 Rdnr. 15; ohnehin soll die Aufzählung "Wort, Schrift und Bild" lediglich als Aufzählung von Beispielen gelten, h.L., Maunz/Dürig/Herzog/Scholz, GG, Art. 5 Rdnr. 73; Hoffmann-Riem, in: AK, Art. 5 Rdnr. 25.

a) Wer kontrolliert?

Grundrechte schützen prinzipiell nur vor Eingriffen durch den Staat, die öffentliche Gewalt; eine Drittwirkung des Grundrechts der Meinungsäußerungsfreiheit besteht grundsätzlich nicht im Verhältnis der Einzelnen untereinander¹¹¹.

Schwierigkeiten bereitet hier die Tatsache, dass Private gelegentlich auf Veranlassung staatlicher Stellen die Meinungsäußerungsfreiheit beschränken. Aufsehen erregte in Deutschland die Maßnahme des On-line-Dienstes Compuserve, Ende 1995 nach Ermittlungen der Münchener Staatsanwaltschaft weltweit allen Kunden den Zugang zu 200 bestimmten Newsgroups zu sperren, die angeblich sexuellen Inhalt hatten¹¹². In diesem Fall ging die Staatsanwaltschaft der Einspielung von Kinderpornografie über Compuserve nach; allerdings nahm Compuserve die folgende Sperrung der 200 Newsgroups wohl freiwillig vor. Es kam zu harschen Zensurvorwürfen durch Kunden, insbesondere amerikanische Nutzer fühlten sich durch deutsche Behörden bevormundet und verließen den Anbieter.

In diesem Zusammenhang sind auch die Ermittlungen der Staatsanwaltschaft Mannheim gegen T-Online zu erwähnen, weil über T-Online der Zugang zu Neonazipropaganda (Ernst Zündel) auf dem WWW möglich war. Sperrmaßnahmen von T-Online blieben in der Folge wirkungslos, weil in den USA die fraglichen WWW-Seiten von Verfechtern der Redefreiheit allgemein zugänglich gemacht wurden¹¹³. Dies geschah auch mit dem in Frankreich verbotenen, genau deswegen dann aber in den USA auf dem Internet verbreiteten Buch des ehemaligen Mittelmeer-Arztes Claude Gubler, *Le Grand Secret*¹¹⁴, wobei hier allerdings eine staatliche Maßnahme (Verbot der Verbreitung) unmittelbar gegen das Buch erfolgt war. In Großbritannien forderte Scotland Yard im Sommer 1996 durch ein Schreiben an über 140 Anbieter zur Sperrung des Zugangs zu 133 WWW-Sites und Newsgroups auf, deren Inhalt als illegal bezeichnet wurde¹¹⁵.

Die Liste der Beispiele von Aktivitäten in- und ausländischer Behörden lässt sich fortsetzen mit den Maßnahmen der Bundesanwaltschaft gegenüber Anbietern, die den Zugang zur Zeitschrift RADIKAL ermöglichen¹¹⁶. Eine neue Dimension hat dabei die Ermittlungstätigkeit deutscher Staatsanwaltschaften durch die Ermittlungen der Berliner Staatsanwaltschaft gegen Nutzer erreicht, die lediglich über einen Link auf ihrer Homepage die Verbindung zum Anbieter von RADIKAL in den Niederlanden ermöglichen¹¹⁷.

Allen diesen Fällen ist gemeinsam, dass die Verfolgungsbehörden, offenkundig von Fehlvorstellungen über die Natur des Internet geleitet, effektive Verbote von Inhalten für möglich halten und dementsprechend Anbieter rechtliche Konsequenzen in Aussicht stellen, wobei diese Ankündigung von möglichen Rechtsfolgen die Anbieter bereits zu beschränkenden Maßnahmen gegenüber den Nutzern durch Sperrung des unmittelbaren Zugriffs auf Inhalte veranlasst. Regelmäßig führt dies in der Folge aber zur Replizierung der fraglichen Inhalte außerhalb des Einflussbereichs der Verfolgungsbehörde (im Ausland) und

¹¹¹ S. etwa Pieroth/Schlink, Grundrechte, Staatsrecht II, 10. Aufl. (1994), Rdnr. 186 ff.

¹¹² S. dazu D. Borchers, Ein Elefant im Sauladen, Die ZEIT vom 12.1.1996, S. 70.

¹¹³ Angst vor der Anarchie, Der Spiegel 13/1996, S. 137.

¹¹⁴ M. Bullinger, JZ 1996, 385 m. w. Nachw.

¹¹⁵ Siehe dazu Piette-Coudol/Bertrand, (o. Fußn. 4), S. 116.

¹¹⁶ Hablützel, Radikal verboten, Die Tageszeitung v. 12.9.1996, S. 12.

¹¹⁷ Fall der ehemaligen stellvertretenden Bundesvorsitzenden der PDS, Angela Marquardt, siehe T. Baumgärtel, Juristisches Neuland, Die Tageszeitung v. 30.1.1997, S. 12.

zu publicityträchtiger Medienberichterstattung über den Fall und die beanstandeten Inhalte, die letztlich für den Nutzer doch über Umwege erreichbar bleiben.

Die einzige rechtlich und auch tatsächlich erfolgversprechende Strategie erscheint dagegen darin zu bestehen, dass die Behörden sich auf physisch fassbare oder tatsächliche Sachverhalte beschränken. Die Ermittlungstätigkeit sollte sich daher beispielsweise auf die Weitergabe von Datenträgern oder Ausdrucken mit aus dem Internet stammenden beanstandeten Inhalten konzentrieren, bzw. auf den Besitz von Inhalten auf Datenträgern (bereits der Besitz von Kinderpornografie ist in Deutschland zum Beispiel strafbar). Anknüpfungspunkte für diese Ermittlungen (Namen und Adressen) könnten bei hinreichender Sachkunde der Ermittlungsbehörden durchaus im Cyberspace gefunden werden. Diese Strategie könnte sich verbinden mit der unmittelbaren Bekämpfung, Aufklärung und Ermittlung bei On-line 'Handlungen' im Cyberspace: Wenn also Kinder in für sie eingerichteten 'Plauderecken' durch Erwachsene belästigt werden, müssten die Verfolgungsbehörden davon benachrichtigt werden können und dann unverzüglich, noch On-line, die Beobachtung und Identifizierung dieser Erwachsenen versuchen.

Meinungskontrolle wie sie durch Private (Sysops auf BBS oder On-line-Diensten) im Sinne der genannten Beispiele vorgenommen wird¹¹⁸ und bei der öffentliche und private Kommunikation förmlich zensiert wird, erscheint zunächst nicht als grundrechtsrelevantes Problem, solange die staatliche Veranlassung - wie etwa im Fall der Münchener Staatsanwaltschaft gegen Compuserve - informell bleibt und Anbieter voraussetzenden Gehorsam leisten oder aber gar keine konkrete staatliche Maßnahme vorliegt¹¹⁹.

Rechtlich steht vielmehr die Frage der Verantwortlichkeit der Anbieter für Inhalte im Vordergrund, durch die mittelbar eine Verpflichtung der Anbieter zur Inhaltskontrolle entsteht. Die Fallgestaltung kann sich dabei aus dem Strafrecht, dem Urheberrecht oder sonstigen Rechtsgebieten ergeben, die bestimmte Meinungsäußerungen erfassen. Die Schwierigkeit für den Anbieter ist dabei, dass er außerhalb der von ihm selbst produzierten Inhalte aus technischen Gründen nur beschränkt übersehen kann, welche Inhalte von seinen Nutzern anderen Nutzern angeboten werden bzw. welche Inhalte von Dritten über das Internet seinen Nutzern zugänglich sind.

Die Verunsicherung der Anbieter über die Reichweite ihrer Verantwortlichkeit wirkt sich teilweise auf die wirtschaftliche Entwicklung im Bereich der Anbieter aus. In Frankreich ist ein erster Versuch, mehr Rechtssicherheit zu erzeugen, zunächst gescheitert: Beabsichtigt war, den Anbietern durch bestimmte technische (Angebot von Filtergeräten an Nutzer) und inhaltliche (Erstellung von inhaltlichen Kriterien durch eine autorité administrative indépendante, den CSA mit Unterstützung des CST) Vorgaben die Möglichkeit zu geben, sich bei Einhaltung dieser Vorgaben von weitergehender Verantwortung freizuzeichnen. Hintergrund war auch hier die Ermittlungstätigkeit der Staatsanwaltschaft gegen Anbieter¹²⁰. Diese Bestimmungen sind jedoch vom Conseil Constitutionnel im Sommer 1996 für

¹¹⁸ Naughton (o. Fußn. 106), S. 417, nennt hier neben Compuserve und Prodigy, America Online und das WELL vertrauen dagegen auf die Selbstkontrolle des Diskurses durch die Nutzer.

¹¹⁹ Siehe in diesem Zusammenhang für Deutschland auch das Beispiel des Internet-Anbieter Verbandes ECO, der Anfang 1997 nach einer polizeilichen Durchsuchung bei EINEM Provider ALLEN angeschlossenen Anbietern eine unverzügliche Entscheidung über die prophylaktische Sperre aller *.erotica und *.sex newsgroups empfahl, siehe "Verhältnismäßige Maßnahmen", Die Tageszeitung v. 6.2.1997, S.12.

¹²⁰ Nach Ermittlungen einer polizeilichen Spezialeinheit (DZpartement informatique-Électronique de l'Institut de Recherche Criminelle de la Gendarmerie (ICRG)) wurden Anfang 1996 die Anbieter WorldNet und FranceNet wegen Verbreitung und Übertragung von Kinderpornographie angeklagt, s. im einzelnen Tortello/Lointier (o. Fußn. 30), S. 130 f.

verfassungswidrig erklärt worden, weil eine Verwaltungseinheit, nämlich der CSA, die Reichweite von Grundrechten bestimmt hätte, was jedoch der Kompetenz des parlamentarischen Gesetzgebers vorbehalten ist¹²¹.

Die amerikanische Rechtsprechung differenziert hier zunehmend: Nachdem in *Cubby v. Compuserve*¹²² festgehalten wurde, dass den Anbieter Compuserve keine Verantwortlichkeit für Inhalte traf (Hintergrund: Verantwortlichkeit für Verletzungen des Urheberrechts, siehe auch oben), musste dagegen der Anbieter Prodigy in *Stratton Oakmont v. Prodigy*¹²³ die Verantwortung für geschäftsschädigende Äußerungen eines Nutzers über das Unternehmen Stratton Oakmont als Herausgeber selbst tragen. Das Gericht argumentierte damit, dass Prodigy erstens durch die Zusicherung, am Wertesystem der amerikanischen Familie orientiert im Bereich des Anbieters Inhalte zu kontrollieren, zweitens durch die selbst ausdrücklich vorgezogene Parallele zur Zeitung sowie drittens durch die technischen und organisatorischen Maßnahmen zur Kontrolle von Inhalten ausdrücklich die Gewähr für die dem Nutzer zugänglichen erhältlichen Inhalte übernommen habe, was eine strenge Haftung rechtfertige, auch wenn tatsächlich eine absolute Kontrolle der Inhalte gar nicht möglich ist. Dagegen habe Compuserve in *Cubby v. Compuserve* gerade vorgetragen, die Inhalte nicht zu überprüfen. Das Gericht äußerte dabei die Erwartung, dass die strengere Haftung für Anbieter, die sich zu Inhaltskontrollen entschliessen, durch die Marktnachfrage ausgeglichen wird. Damit ist wohl gemeint, dass eine höhere Nachfrage seitens der an nicht zu beanstandenden Inhalten im Sinne des von Prodigy genannten Wertmaßstabes interessierten Kunden die durch strengere Haftung entstehenden Kosten finanziell kompensiert. Die Verantwortlichkeit der Anbieter wird in den U.S.A. durch den Communications Decency Act neu gefasst¹²⁴.

Zusammenfassend erscheint an die Grundsätze aus *Stratton* angelehnt die Verantwortlichkeit der Anbieter nur dann veranlasst, wenn der Anbieter sich in irgendeiner Form Inhalte zu eigen macht, wobei dies ausdrücklich oder auch konkludent erfolgen kann¹²⁵.

Zurück zum Problem der Grundrechtsdimension der Zensur durch private Anbieter: Zunächst hat hier im amerikanischen Verfassungsrecht die public forum doctrine zu neuen Fragen geführt: in seltenen Fällen haben die Gerichte einem an und für sich privaten Platz die Qualität als öffentliches Forum zugemessen, in dem die Meinungsäußerungsfreiheit nicht eingeschränkt werden darf. Diese Theorie steht in engem Bezug zur Theorie vom 'marketplace of ideas' beim Recht auf freie Rede, die sich wohl bis zu John Stuart Mill zurückverfolgen lässt und in neuerer Zeit durch Justice Oliver Wendell Holmes geprägt wurde. Justice Holmes in der Supreme Court Entscheidung *Abrams v. United States*¹²⁶ "the ultimate good desired is better reached by free trade in ideas [and] the best test of truth is the power of the thought to get itself accepted in the competition of the market". Formuliert wurde die public forum doctrine erstmals in *Hague v. Committee for Industrial Organization*

¹²¹ DŽcision no. 96-378 du 23 juillet 1996, Journal Officiel v. 27.7.1996, S. 11400; siehe auch Piette-Coudol/Bertrand, (o. Fußn. 4), S. 127 ff. Abgedruckt ist die Entscheidung bei Tortello/Lointier (o. Fußn. 30), Anhang Nr. 2.

¹²² Siehe o. Fußn. 106.

¹²³ Supreme Court of New York, Nassau County, 23 Media L. Rep. 1794.

¹²⁴ Siehe Text zu Fußn. 179.

¹²⁵ Ähnlich das Tribunal de Grande Instance de Paris, Ordonnance de rŽfŽrŽ du 12 juin 1996, Les Petites Affiches v. 10.7.96, S. 22 mit Anmerkung Maisl. in einer Klage der (UEJF) Vereinigung der jüdischen Studenten in Frankreich gegen 9 Anbieter, die den Zugang zu revisionistischen Angeboten ermöglichten. S. dazu auch Tortello/Lointier (o. Fußn. 30), S. 128 f.

¹²⁶ 250 U.S. 616, 630 (1919).

im Jahre 1939¹²⁷. Teilweise wird nun vertreten, dass die public forum doctrine auf Cyberspace anzuwenden sein soll, eben auf die von privaten, kommerziellen Anbietern geschaffenen "öffentlichen" Räume, womit gegenüber diesen Privaten das Recht der freien Rede geltend gemacht werden könnte¹²⁸. Die amerikanischen Gerichte haben diese Frage noch nicht abschließend entschieden¹²⁹.

Im deutschen Verfassungsrecht ist eine solche Drittwirkung nicht in Sicht; nach herrschender Ansicht umfasst Art. 5 Abs. 1 Satz 1 GG keinen Anspruch auf Verschaffung geeigneter Foren: Mit der Meinungsäußerungsfreiheit wird nur die Möglichkeit zur Meinungsäußerung eröffnet, nur die geistige Wirkmöglichkeit, nicht aber Erfolg der Meinungsäußerung und Erfolgsweg garantiert¹³⁰. Die ganze Dimension grundrechtsrelevanter Aspekte kann hier nicht ausgelotet werden; jedenfalls bleibt die Frage, wie in einer Welt, in der Meinungsäußerung und Kommunikation sich zu einem ganz überwiegenden Maße im Cyberspace abspielte, die Meinungsäußerungsfreiheit gegen willkürliche Zensur durch private Betreiber zu schützen wäre.

Zwar lässt sich dem entgegenhalten, dass auch in der heutigen Zeit "Zensur" insofern stattfindet, als dass nun einmal nicht jede Meinungsäußerung vom privaten oder auch öffentlichen Betreiber einer Rundfunk- oder Fernsehanstalt ausgestrahlt bzw. vom Herausgeber eines Printmediums abgedruckt werden muss. Dies wird jedoch durch den pluralistischen Aufbau von Rundfunk und Fernsehen aufgewogen¹³¹, wobei der Staat durch Lizenzvergabe regelnd eingreifen kann. Betätigung im Cyberspace ist jedoch nicht von solchen Lizenzen abhängig. Zum anderen bleibt dem Einzelnen, falls der Zugang zu Massenmedien nicht gelingt, dann immer noch die Möglichkeit, sich an die Straßenecke zu stellen, und seine Meinung zu verkünden. Was aber, wenn in der (fernen) Zukunft die Straßenecke, verstanden als physischer Ort der sozialen Interaktion, zunehmend unüblich wird, und soziale Interaktion sich dafür zunehmend im Cyberspace abspielt?

Berührt sind hier auch Aspekte der grundgesetzlich gewährleisteten Informationsfreiheit (Art. 5 Abs. 1 Halbsatz 2 GG)¹³². Zwar wird diese allgemein als Abwehrrecht gegen den Staat gesehen, weswegen der Staat nicht gezwungen ist, allgemein zugängliche Informationsquellen einzurichten¹³³. Allerdings ist denkbar, dass sich der objektiv-rechtliche Gehalt des

¹²⁷ 307 U.S. 496 (1939). Näheres zu dieser Theorie bei Cavazos/Morin (o. Fußn. 17), S. 69 ff.; Naughton (o. Fußn. 106), S. 419 ff. m. w. Nachw.

¹²⁸ Naughton (o. Fußn. 106), S. 428 ff., vgl. auch L. Grossman, *The electronic republic: the transformation of American Democracy*, 1995.

¹²⁹ Zur parallelen Problematik im Bereich des Kabelfernsehens s. die Entscheidung des Supreme Court im Fall *Turner Broadcasting System, Inc. v. Federal Communications Commission et al.* (114 S. Ct. 2445) vom Juni 1995, in der es um die Kontrolle geht, die durch die Kabelgesellschaften auf die inhaltliche Gestaltung der Programme ausgeübt wird. Die Entscheidung betont dabei, daß anders als früher bei der leitungs-freien Übertragung Ressourcenknappheit (Frequenzen) heute bei Kabel nicht mehr anzunehmen sei, läßt im Ergebnis jedoch viele Fragen offen, s. zum Turner-Fall auch Sunstein (o. Fußn. 108), S. 9 ff. oder N. W. Allard, *The Herbert Tenzer Memorial Conference: Copyright in the Twenty-First Century: Must Carry and the Courts: Bleak House, the Sequel*, 13 *Cardozo Arts & Entertainment Law Journal* 139 (1994)

¹³⁰ v. Münch/Wendt, GG, Art. 5 Rdnr. 19 m. w. Nachw.; Maunz/Dürig/Herzog/Scholz, GG, Art. 5 Rdnr. 63.

¹³¹ Vgl. Maunz/Dürig/Herzog/Scholz, GG, Art. 5 Rdnr. 65. Für die U.S.A. s. in diesem Zusammenhang die Entscheidungen des Supreme Court *Miami Herald Publishing Co. v. Tornillo*, 418 U.S. 241, 247 ff. (1974), *National Broadcasting Co. v. United States*, 319 U.S. 190 (1943).

¹³² Zur Gewährleistung der Informationsfreiheit auf internationaler Ebene s. etwa Art. 12 der Europäischen Menschenrechtskonvention. Vgl. auch die in den VN gescheiterte Draft Convention on Freedom of Information, UN Doc. A/5443 (1963). allgemein s. R. Pinto, *La liberté d'information et d'opinion en droit international*, Paris 1984.

¹³³ BVerwG, DÖV 1979, 102; B. Simma, *Grenzüberschreitender Informationsfluß und domaine réservé der Staaten*, 19 *Berichte der Deutschen Gesellschaft für Völkerrecht* 39 (1979).

Grundrechts in bestimmten Konstellationen zu einer Pflicht zur Offenhaltung des Kommunikationsprozesses und eines freien Informationsflusses verdichtet¹³⁴. Insbesondere wenn der Zugang zur elektronischen Kommunikation durch Marktentwicklungen in den Händen eines oder weniger privater Anbieter monopolisiert werden sollte¹³⁵, kann dies nicht ohne Folgen für die Pflicht des Staates bleiben, dem einzelnen Zugang zu Informationsquellen zu gewährleisten. Konkret könnte das bedeuten, dass - falls Cyberspace als Kommunikations- und Informationsraum einmal die Dimensionen erlangt oder übersteigt, die heute Presse, Rundfunk und Fernsehen einnehmen - der Staat für den Einzelnen die Zugangsmöglichkeit zum Internet außerhalb der kommerziellen On-line-Dienste schaffen muss¹³⁶.

In diesem Zusammenhang drängt sich der Vergleich mit der objektiv-rechtlichen Argumentation des BVerfG im Rundfunkbereich auf, wo die Funktion des Rundfunks als Medium und Forum öffentlicher Meinungsbildung im Vordergrund steht¹³⁷, und wo das BVerfG auf einer staatlicherseits zu gewährleistenden Grundversorgung besteht¹³⁸. Nicht verkannt werden darf jedoch dabei, dass für den Zugang zum Cyberspace eine wirklich neuartige Situation vorliegt, weswegen Bezugnahmen auf das Rundfunkrecht nicht ohne weiteres zulässig sind: Es ist nicht so, dass der Staat einen Regelungsbereich monopolisiert hat und sich Letztentscheidungen vorbehält. Selbst wenn der Staat regeln wollte, er könnte es nicht effektiv. Die einzig denkbare staatliche Einflussmöglichkeit liegt in der Gewährleistung des Zugangs zum Kommunikationsmedium, und hier liegt der Unterschied etwa zum Rundfunkbereich, wo der Staat einschränkende Entscheidungen sehr wohl auch durchsetzen kann. Im Cyberspace kann der Staat nur ein privates Monopol verhindern, es aber nicht durch ein staatliches Monopol mit entsprechenden Sicherungsmechanismen ersetzen.

¹³⁴ Vgl. Degenhardt, in: BK, Art. 5 Rdnr. 279 ff.

¹³⁵ Erinnerung sei in diesem Zusammenhang an die Verknüpfung des Betriebssystems Windows 95 mit einem On-Line-Dienst des Marktführers Microsoft, die auch die Kartellbehörden beschäftigt hat, S. Lohr, Microsoft is worried that the Justice Department may force a delay in Windows 95, New York Times vom 12.6. 1995, S. D3.

¹³⁶ Allerdings ließe sich aus Art. 5 GG wohl kein Anspruch auf Gratis-Zugang ableiten, vgl. BVerwGE 29, 214 (218). Zur Zugangsgewährleistung s. auch H. Kubicek, CR 1995, 370; vgl. auch die Gewährleistung des Art. 87f I GG. Der französische Telekommunikationsminister hat 1996 France-TZIŽcom angewiesen, den Nutzern Zugang zu Anbietern ihrer Wahl zum Ortstarif zu gewährleisten, Piette-Coudol/Bertrand, (o. Fußn. 4), S. 40.

¹³⁷ Pieroth/Schlink (o. Fußn. 111), Rdnr. 631 m. w. Nachw.

¹³⁸ BVerfGE 87, 181 (199), s. auch Maunz/Dürig/Herzog/Scholz, GG, Art. 5 Rdnr. 238 ff.

b) Presse- und Rundfunkbegriff

Im Zusammenhang mit der durch Art. 5 GG gewährleisteten Presse- und Rundfunkfreiheit ergeben sich neue Fragen, wenn aufgrund der technischen Entwicklung jeder sein eigener Herausgeber bzw. Programmdirektor sein kann: so wird der Begriff der Presse weniger fassbar werden; ob die elektronische Publikation, die ohne einen körperlichen Informationsträger auskommt, unter Presse fällt, erscheint in Anbetracht der üblichen Definitionen bereits sehr fraglich¹³⁹.

Denkbar wäre immerhin, den Rundfunkbegriff auf Cyberspace auszudehnen. In der weitesten Umschreibung umfasst Rundfunk die Verbreitung von Informationen für eine unbestimmte Vielzahl von Personen mittels physikalischer, insbesondere elektromagnetischer Wellen¹⁴⁰, womit jedoch bereits der interaktive Charakter der Kommunikation im Cyberspace nicht erfasst wird. In der Interaktivität des Mediums Cyberspace liegt nämlich (noch) der entscheidende Unterschied zu bisherigen Medien, wo der Einzelne im Wesentlichen die Rolle des passiven Verbrauchers innehat¹⁴¹.

Festzuhalten ist, dass der spezifische Charakter des Regelungsobjektes Cyberspace eine schematische Übertragung von rechtlichen Aspekten aus dem Bereich des Rundfunk- und Telekommunikationsrechts, wie sie vielfach unternommen wird, nicht zulässt¹⁴².

¹³⁹ Vgl. v. Mangoldt/Klein/Starck, GG, Art. 5 Rdnr. 38, "alle zur Verbreitung geeigneten und bestimmten Druckerzeugnisse und Informationsträger"; vgl. auch die einschlägigen Bestimmungen der Landespressegesetze wie § 7 NWPresseG.

¹⁴⁰ Pieroth/Schlink (o. Fußn. 111), Rdnr. 626; v. Münch/Wendt, GG, Art. 5 Rdnr. 58.

¹⁴¹ The Message in the Medium: The First Amendment on the Information Superhighway, 107 Harvard Law Review 1062, 1086 (1994). S. auch Bullinger, JZ 1996, 385 (387 f.).

¹⁴² In diesem Sinne auch die Berichterstatterin Falque-Pierrotin in ihrem Bericht an die französische Regierung, vgl. Piette-Coudol/Bertrand, (o. Fußn. 4), S. 81 und <http://www.telecom.gouv.fr/francais/activ/techno/missionint.htm>. Auszüge aus diesem Bericht sind abgedruckt bei Tortello/Lointier (o. Fußn. 30), Anhang Nr. 3.

c) *Wessen Werte?*

Die Meinungsäußerungsfreiheit ist unter dem Grundgesetz nicht schrankenlos gewährleistet, sondern findet ihre Schranken in den allgemeinen Gesetzen und im Recht zum Schutze der Jugend und der persönlichen Ehre. Wie das amerikanische Beispiel zeigt, handelt es sich bei der Entscheidung, bis zu welchen Grenzen Meinung toleriert wird und ab wo die freie Meinung das friedliche Zusammenleben so zu gefährden droht, dass die Meinungsäußerungsfreiheit hinter dem Interesse der Gemeinschaft am friedlichen Zusammenleben zurückstehen muss, um eine Wertentscheidung, die von Gesellschaft zu Gesellschaft unterschiedlich ausfallen kann. Diese Unterschiede sind hinzunehmen, da lediglich den Unterschiedlichkeiten der Gesellschaften Rechnung getragen wird. Fallen jedoch plötzlich, wie im Cyberspace, die geographischen Entfernungen und rechtlichen Grenzen weg, so ergeben sich neuartige unmittelbare Konflikte dieser unterschiedlichen Wertentscheidungen. Dazu zwei Fallbeispiele:

aa) Ein besonders deutliches Beispiel für die sich aus unterschiedlichen Wertvorstellungen ergebenden Konflikte bieten die verschiedenen auf dem Internet kursierenden Texte und Stellungnahmen zur sog. Auschwitzlüge (das Leugnen des deutschen Völkermordes an den Juden): Äußerungen, die in Deutschland von Strafe bedroht sind, werden in den USA vom Recht auf freie Meinungsäußerung geschützt¹⁴³. Dass es nicht weiterhilft, solche Konflikte sich selbst zu überlassen, belegt der Fall, in dem ein deutscher Sysop einen amerikanischen Diskussionsteilnehmer einer elektronischen Diskussionsrunde wegen seiner Thesen zu Auschwitz aus der Diskussion aussperrte, was wiederum zu heftigen Attacken aus den USA auf diesen Sysop führte, dem wegen angeblicher unzulässiger Beschneidung von Meinungsäußerungsfreiheit demokratiefeindliches Verhalten vorgeworfen wurde¹⁴⁴.

bb) Ein weiterer Konfliktbereich hat aus den USA den Weg hierher gefunden¹⁴⁵: Freie Rede und Pornografie¹⁴⁶; Jugendschutz vor pornografischen Veröffentlichungen. Auf dem Internet kursieren in Schrift- und Bildform pornografische Darstellungen aller Art¹⁴⁷. Fotografische Abbildungen können mittels eines Einlesegerätes (Scanners) in computerlesbare Form gebracht und dann über das Internet versandt werden. Zur Entschlüsselung dieser kodierten Bilder bedarf es lediglich eines dafür geeigneten Programms¹⁴⁸. Allerdings sollten die dazu erforderlichen Computerkenntnisse nicht unterschätzt werden. Man wird im Cyberspace nicht ganz zufällig auf harte Pornografie stoßen, sondern (noch) nur nach gezielter Suche. Die Frage, wie Jugendliche vor bestimmten Publikationen zu schützen sind, hat bisher wahrscheinlich noch jede Neuentwicklung im Bereich der Publikationstechnologie

¹⁴³ S. dazu die Supreme Court Entscheidungen *R.A.V. v. City of St. Paul*, 112 S. Ct. 2538, 2547 (1992); *Brandenburg v. Ohio*, 395 U.S. 444, 448 (1969); vgl. auch J. Stefancic/R. Delgado, *A Shifting Balance: Freedom of Expression and Hate-Speech Restriction*, 78 Iowa L. Rev. 737, 740 (1993), E. Stein, *History Against Free Speech: The New German Law Against "Auschwitz" - and Other - "Lies"*, 85 Mich. L. Rev. 277, 281 (1986).

¹⁴⁴ Es handelte sich um GerLine, ein deutschsprachiges Forum des amerikanischen Anbieters Compuserve, a. auch Focus vom 29.8. 1994, S. 140.

¹⁴⁵ S. o. Fußn. 112 der Fall der Zensur von Newsgroups durch Compuserve im Dezember 1995.

¹⁴⁶ Zur Frage, was in den U.S.A. in diesem Zusammenhang nicht mehr vom Recht der freien Rede erfaßt wird, grundlegend *Miller v. California*, 413 U.S. 15 (1973), hierin wird der örtliche community standard zum maßgeblichen Kriterium.

¹⁴⁷ Zu dieser Facette von Cyberspace, s. M. Rimm, *Marketing Pornography on the Information Superhighway*, 83 Georgetown Law Journal 1095 (1995), kritisch zu dieser Studie allerdings P. Lewis, *Hell has no fury like an Internet scorned*, New York Times vom 17.7. 1995, S. D5.

¹⁴⁸ Besonders häufig wird auf diesem Wege offenbar Kinderpornographie verbreitet, s. Long (o. Fußn. 64), S. 1183; s. auch D. Drewes, *Kinder im Datennetz*, 1995.

ausgelöst¹⁴⁹. Besondere Probleme ergeben sich aber aus dem Aufeinandertreffen der Nichtörtlichkeit von Cyberspace und örtlichen moralischen Standards, und in den USA jedenfalls bereitet dieser Aspekt den Verfolgungsbehörden erhebliche Probleme.

Erfolglos blieben die Behörden etwa im viel diskutierten Fall Baker¹⁵⁰, mehr Erfolg hatte man im Fall Robert und Carleen Thomas, einem kalifornischen Ehepaar, das in Kalifornien unbehelligt ein BBS zum Vertrieb pornografischer Abbildungen aller Art unterhielt: Thomas wurde nach Memphis im U.S.-Bundesstaat Tennessee gelockt und dort verhaftet, was nur möglich war, weil in den amerikanischen Südstaaten der Begriff der guten Sitten weitaus strenger ausgelegt wird als in Kalifornien¹⁵¹. In diesem Fall wurde eine mehrjährige Freiheitsstrafe verhängt¹⁵²; falls der Fall bis zum Supreme Court gelangt, ist ein Grundsatzurteil zu erwarten. Das Phänomen unterschiedlicher lokaler Moralverständnisse ist natürlich im Wesen eines Bundesstaates schon angelegt. Im Cyberspace treffen unterschiedliche Moralvorstellungen jedoch in ähnlicher Unmittelbarkeit aufeinander, wie es durch die relative geographische Nähe von staatlichen Untergliederungen in Bundesstaaten der Fall ist, ohne dass dies jedoch durch einen gemeinsamen Unterbau an Grundwerten, Grundideen oder auch nur an sozialer und staatlicher Organisation (wie etwa Bundesverfolgungsbehörden) ergänzt würde. Selbst da, wo aber die Verfolgung aufgrund hinreichender Rechtsgrundlagen grundsätzlich möglich ist, bleibt dennoch das Problem, dass es kaum eine wirksame Möglichkeit gibt, die Verbreitung bestimmter Inhalte wirksam zu verhindern. Beispielsweise sind die von Compuserve Ende Dezember 1995 gesperrten 200 Newsgroups problemlos über konkurrierende kommerzielle Anbieter oder auch die Server der Universitäten zu erreichen gewesen; selbst von Compuserve aus konnte, wer sich im Internet auskennt, weiterhin die 200 Newsgroups erreichen¹⁵³. Insgesamt ist festzuhalten, dass Jugendschutz bzw. Verhinderung von Gewaltpornografie auf dem Internet extrem schwierig zu realisieren sind. Darüber hinaus treten auch völlig neuartige Fragen auf, wie die nach der rechtlichen Behandlung von mit Hilfe künstlich erzeugter Computerbilder (Beispiel: morphing) hergestellter Pornografie: wie ist es zu bewerten, wenn etwa kinderpornografische Abbildungen gar keine Kinder abbilden, sondern lediglich Computerkreationen sind, und wie wäre strafrechtlich ein Softwarepaket zu würdigen, mit dessen Hilfe Nutzer gemorphte pornografische Abbildungen selbst herstellen können¹⁵⁴?

¹⁴⁹ In Frankreich hat man mit den sogenannten messageries roses auf Minitel, in einem gewissen Sinne ein lokaler Vorläufer des Internet, seit 1980 auch schon juristische Erfahrungen sammeln können, s. dazu Piette-Coudol/Bertrand, (o. Fußn. 4), S. 121 ff.

¹⁵⁰ Baker, Student an der Universität in Ann Arbor, hatte in der Newsgroup alt.sex.stories (eine unmoderierte Newsgroup) eine pornographische Gewaltdarstellung veröffentlicht, in der endlose sexuelle Mißhandlungen und Vergewaltigungen einer Frau, die schließlich zu deren Tode führen, beschrieben wurden. Es gelang nur über den Vorwurf einer interstate transmission of a threat eine Anklage zu formulieren. Baker hatte für den Namen des Opfers den Namen einer existierenden Frau gewählt und sich in seiner privaten E-mail Korrespondenz mit einem in Canada ansässigen Kommunikationspartner über die Umsetzung der Phantasien in die Wirklichkeit unterhalten. Baker wurde letztlich jedoch freigesprochen, s. *United States of America v. Abraham Jacob Alkhabaz a.k.a. Jake Baker and Arthur Gonda*, Az. 95-80106, U.S. District Court Eastern District of Michigan-SD 1995 vom 21.6. 1995. Nach deutschem Recht hätte Baker durchaus strafrechtlich belangt werden können.

¹⁵¹ S. TIME vom 3.7. 1995, S. 43.

¹⁵² *United States v. Thomas*, WD Tenn., July 28, 1994, *The Int. Comp. Lawyer*, Oktober 1994, S. 36; die Entscheidung des Court of Appeals (6th Circuit) in *The Cyberspace Lawyer*, April 1996, S. 30.

¹⁵³ S. Borchers (o. Fußn. 112).

¹⁵⁴ Zu diesen Fragen s. H. J. Reske, *Computer Porn a Prosecutorial Challenge*, ABA Journal December 1994, 40; vgl. auch Cavazos/Morin (o. Fußn. 17), S. 91, 99. In den U.S.A. kommt es darauf an, daß tatsächlich Minderjährige abgebildet sind, hier ergeben sich schwierige Beweisfragen, s. dazu bisher lediglich U.S. v. Nolan, 818 F.2d 1015 (1st Cir. 1987). Auch in Frankreich kommt es darauf an, daß zumindest das Ausgangsbild ein reelles Kind darstellt, zur "pŽdophilie virtuelle" Piette-Coudol/Bertrand, (o. Fußn. 4), S. 125 f.

Jugendschutz lässt sich im abgegrenzten Bereich der kommerziellen Anbieter durch bestimmte Filterprogramme verbessern¹⁵⁵. Auch für den direkt ans Internet angeschlossenen Teilnehmer wird es Filterprogramme geben, die bestimmte Wörter ausfindig machen und dann die Verbindung unterbrechen. Allerdings kann der Einsatz solcher Filterprogramme sowohl am Endgerät als auch beim On-line-Dienst nur begrenzt effektiv sein¹⁵⁶: Beim Endgerät, weil die Suche nach "Unwörtern" durch Verschlüsselung von Texten und Bildern und leichte Variation inkriminierter Suchworte ('sx' statt 'sex' etc.) leicht sabotiert werden kann; beim Anbieter, weil, solange der Anschluss ans Internet noch besteht, am Anbieter vorbei auf das Angebot im Internet zugegriffen werden kann. Auch Filterprogramme, die sich auf bestimmte Absenderadressen oder gar auf Absenderrechner abrichten lassen, bekommen regelmäßig nur mäßige Beurteilungen¹⁵⁷. Schließlich wird der Nutzen der Filterprogramme auch dadurch beeinträchtigt, dass im Bereich des Jugendschutzes neben dem statischen Element (Austausch von Dokumenten wie Bildern oder Texten) zunehmend auch das interaktive Element des Internet (On-line-Kontakte) zu Besorgnis Anlass gibt: wenn etwa im WWW eine "Plauderecke" für Kinder eingerichtet wird, die Pädophile zur Belästigung von Kindern nutzen¹⁵⁸.

Über Neonazi-Gedankengut und Pornografie hinaus lassen sich weitere Fallbeispiele für Wertkonflikte fast wöchentlich der Presse entnehmen: Zu denken sind hier an Bereiche wie das Recht der persönlichen Ehre (Beleidigungsdelikte und die presserechtliche Verantwortlichkeit in diesem Zusammenhang) und Äußerungen mit Bezug zur Religionsausübung. Abschätzig lästernde Bemerkungen über den thailändischen König - in Thailand strafbar - in einer Newsgroup soc.culture.thailand veranlassten die thailändischen Behörden zu der Erwägung, diese Newsgroup landesweit sperren zu lassen¹⁵⁹. Im Iran ist heimischen Internet-Anbietern die Verbreitung bestimmter Newsgroups verboten¹⁶⁰. In Abu Dhabi wurde ein Internetclub gezwungen, außer Sex und Politik auch Religion aus den verfügbaren Angeboten zu streichen¹⁶¹.

¹⁵⁵ AmericaOnline bietet beispielsweise einen parental guide Schalter, der Kinder daran hindert, bestimmte Programme aufzurufen.

¹⁵⁶ Die Wirksamkeit solcher Programme hängt schließlich davon ab, daß sie auch benutzt werden und daß sie nicht von computerkundigen Minderjährigen umgangen werden. Die 200 von Compuserve im Dezember 1995 gesperrten Newsgroups wurden wohl auch durch ein Filterprogramm mit bestimmten Worten ermittelt, wodurch aber neben pornographischen Newsgroups auch eine Selbsthilfenewsgroup von Vergewaltigungsopfern ins Raster geriet, Borchers (o. Fußn. 112).

¹⁵⁷ Borchers, Hilflose Hüter, Die Zeit v. 12.7.1996, S. 58

¹⁵⁸ Zum Vorfall bei dem Computerspielhersteller Nintendo s. M. Dworschak, Nestbeschmutzer ausgeklinkt. Aufgrund seiner Bauweise trotzts das digitale Dorf allen Ordnungshütern, Die Zeit v. 19.1.1996, S. 15.

¹⁵⁹ Dworschak, (o. Fußn. 158), S. 16.

¹⁶⁰ Dworschak, (o. Fußn. 158), S. 16.

¹⁶¹ Die Zensur ist global, Die Tageszeitung v. 30.5.1996, S. 12.

IV. Cyberspace als neuer Rechtsraum - die vierte rechtliche Dimension?

Cyberspace in irgendeiner Form rechtlicher Regelung zu unterwerfen, stößt zunächst einmal auf die Schwierigkeit, dass die Nutzer nicht einer einzigen staatlichen Autorität unterworfen, sondern über die ganze Welt verteilt sind. Dazu kommen die durch technische Gegebenheiten gesetzten Grenzen: Niemand kontrolliert das Internet, man kann es nicht einfach abschalten. Selbst wenn man das Internet-Protokoll auf der Stelle abschaffte und die nationalen Hochleistungsdatenleitungen stilllegte, würden weiterhin Millionen von Menschen E-mail austauschen und an Newsgroups teilnehmen können¹⁶². Die BBS- Verbindungen über reguläre Telefonleitungen und das Usenet-System würden bleiben; man müsste schon den Telefonverkehr stilllegen, um diese Kommunikation zu unterbinden.

Die Durchsetzung von allgemeinen Regeln wird vor diesem Hintergrund häufig als schwierig bis unmöglich angesehen¹⁶³. Dennoch wird immer wieder über die verkürzte Analogie zu herkömmlichen Medien im Rundfunk- oder Telekommunikationsbereich die Möglichkeit der effektiven Regelung behauptet. Erforderlich ist jedoch eine differenzierte Betrachtungsweise. Insgesamt wird vor dem Hintergrund divergierender und häufig aussichtsloser Regelungsversuche oft gefragt, ob der Versuch, spezifische Regeln für Cyberspace festzusetzen, überhaupt unternommen werden soll, oder ob hier ein rechtsfreier Raum droht. Vor der Beantwortung dieser Frage empfiehlt es sich, zunächst Klarheit über bereits bestehende formale und materielle Regeln im Internet zu erzielen.

¹⁶² Rheingold (o. Fußn. 4), S. 109.

¹⁶³ Ein 1995 an der Yale Law School im Rahmen eines Cyberspace Law Seminars (Professor L. Lessig) durchgeführtes Experiment, bei dem die Seminarteilnehmer im Cyberspace im Rahmen einer Newsgroup interagierten, zeigte, daß bereits die Festlegung und dann Einhaltung einfachster Regeln innerhalb dieser homogenen Newsgroup mangels hierarischer Struktur und Durchsetzungsmöglichkeiten on-line kaum zu leisten war. Gegenbeispiel für die prinzipiell durchaus mögliche Konsensbildung und -durchsetzung ist hier allerdings das renaming des Usenet 1986, wo es gelang, das gesamte System des newsgroups neu zu organisieren, vgl. Dufour (o. Fußn. 2), S. 64.

1. Bestandsaufnahme: bestehende Regeln formaler und materieller Natur

a) Formale (technische) Regeln

Formale Regeln sind technische Standards wie die Übertragungsprotokolle und Übereinkünfte über das Format von Internet-Adressen. Gesteuert und überwacht wird die Regelentwicklung in diesem Bereich durch die Internet Society (ISOC), eine Vereinigung nach amerikanischem Recht mit Sitz in Reston, Virginia (USA), welche im Januar 1992 gegründet wurde¹⁶⁴ und mittlerweile über 5.000 Mitglieder zählt, die 125 Länder und 129 Organisationen repräsentieren. An der Spitze der ISOC steht das Board of Trustees mit einem Präsidenten. Unter dem Dach der ISOC betätigen sich verschiedene Ausschüsse, beratende Gremien und Länderabteilungen. Spezialisierte Vereinigungen unter dem Dach der ISOC sind mit bestimmten Aspekten der technischen Regeln betraut.

Die wichtigste dieser Vereinigungen dürfte das IAB (Internet Architecture Board) sein¹⁶⁵. Von hier aus wird nämlich die technische Entwicklung der Internet-Übertragungsprotokolle überwacht. Dies geschieht durch drei Unterorganisationen:

- Die Internet Assigned Number Authority (IANA), die für alle einheitlichen Nummern und Codes im Internet zuständig ist, insbesondere für die IP-Adressen diese Aufgaben teilweise an regionale Unterstrukturen (InterNIC für Nordamerika, RIPE mit Sitz in Amsterdam für Europa, AP-NIC für Asien-Pazifik) delegiert sind, die diese beispielsweise in Europa wiederum an Länder-NICs (Network Information Centers) delegiert haben.
- Die Internet Research Task Force (IRTF), mit dem Leitungsgremium der Internet Research Steering Group (IRSG), betreibt mittel- und langfristige Forschung zur Vorbereitung der Arbeit der IETF.
- Die Internet Engineering Task Force (IETF) unter Leitung der Internet Engineering Steering Group (IESG) schließlich arbeitet an der Verbesserung und Aktualisierung der aktuellen technischen Spezifikationen des Internet¹⁶⁶.

Die bedeutsamste Rolle kommt der IETF und ihrem originellen Verfahren zur Entscheidungsfindung zu. Die IETF ist ein loser Zusammenschluss von technischen Experten, dessen Mitgliedschaft man einfach durch Einzahlung einer Registrierungsgebühr und Verpflichtung zur Mitarbeit in den technischen Arbeitsgruppen erwirbt. Die IETF tritt dreimal jährlich zusammen, zweimal in den USA und einmal außerhalb der USA. Im Übrigen findet der Austausch über die Arbeit per E-mail statt. Dabei werden die Entwürfe als elektronische Dokumente unter der Bezeichnung Requests for Comments (RFCs), Einladungen zur Stellungnahme, ausgetauscht und auch öffentlich zugänglich gemacht. Die Treffen außerhalb der E-mail-Kommunikation waren von Anfang an vorgesehen, vor allem im Wissen darum,

¹⁶⁴ Piette-Coudol/Bertrand, (o. Fußn. 4), S. 9; siehe allgemein <http://www.isoc.org>, ein Organigramm mit allen Unterstrukturen findet sich bei Dufour, (o. Fußn. 2), S. 22.

¹⁶⁵ Siehe die Charta des IAB in RFC 1601 <http://ds.internic.net/rfc/rfc1601.txt>, sowie RFC 1160, <http://ds.internic.net/rfc/rfc1160.txt>, zum Aufbau des IAB. IAB stand vor der Eingliederung in die neugegründete ISOC 1992 für Internet Activities Board. Dieses IAB ersetzte 1993 das Internet Configuration Control Board (ICCB), das 1979 noch durch die ARPA (o. Fußn. 4) gegründet worden war, und zwar als direkter Nachfolger der 1972 ins Leben gerufenen Internet Working Group (INWG); zur Entwicklung im einzelnen s. Dufour (o. Fußn. 2), S. 29.

¹⁶⁶ Siehe hierzu allgemein RFC 1539, <http://ds.internic.net/rfc/rfc1539.txt>, s. auch <http://www.ietf.org> und <http://www.ietf.org/proceedings/directox.html>.

dass Entscheidungsfindung durch gelegentliche Treffen von Angesicht zu Angesicht enorm beschleunigt werden kann und effizienter wird. Das IETF gliedert sich in Funktionsbereiche und Arbeitsgruppen, deren Zusammensetzung variiert. Logistische Unterstützung erfährt das IETF durch das CNRI (Corporation for National Research Initiatives), finanzielle Unterstützung erfolgt teilweise durch die staatliche National Science Foundation. Die originelle Struktur des IETF als nicht-hierarchischer, loser Verbund von hauptberuflich anderweitig Tätigen erklärt sich aus der Tradition seit den Anfängen des Internet bzw. Arpanet als die Zahl der Nutzer nicht wesentlich größer war als die Zahl derjenigen, die sich gelegentlich zur Absprache über technische Standards trafen. Die Entscheidungsfindung über neue Standards erfolgt über Rough Consensus, ungefähren Konsens, der sich in den Reaktionen auf ein RFC ausdrückt. Über divergierende Lösungsvorschläge wird dabei keine Mehrheitsentscheidung herbeigeführt, statt einer Dezision wird vielmehr ein Konsens über eine Lösung gesucht, der über einen Protokoll-Entwurf, einen Proposed Standard, dann einen Draft Standard, jeweils durch RFCs begleitet, zu einem Internet Standard mit entsprechender Nummer führt¹⁶⁷.

¹⁶⁷ Näheres bei Dufour (o. Fußn. 2), S. 23.

b) Netiquette

Über die nur formalen Regeln hinaus gehen zunächst einmal diejenigen ungeschriebenen oder jedenfalls nicht einheitlich niedergelegten Regeln, die sich in der Grauzone zwischen Konventionen und materiellen Regeln bewegen.

Zu nennen ist hier zuerst die sogenannte Netiquette¹⁶⁸, die aus dem Bereich der Newsgroups auf dem Usenet stammt. Danach gilt etwa, dass Wörter in Großbuchstaben lautem Schreien entsprechen oder dass Äußerungen im Cyberspace grundsätzlich kurz zu halten sind. Etwas weiter gehen gewohnheitsmäßige Regeln, die beispielsweise die kommerzielle Nutzung bestimmter Bereiche des Cyberspace nicht zulassen. Hier ist zu erinnern an den Fall der Anwaltskanzlei Canter & Siegel aus Phoenix, die auf dem Usenet in über 5000 Newsgroups Werbung für ihre Dienste verbreitete, woraufhin Usenet-Nutzer mit Protest-E-mails an die Kanzlei in solcher Anzahl antworteten, dass deren E-mail lahmgelegt wurde und der Anbieter des Internet-Zugangs für die Kanzlei den Vertrag mit der Kanzlei wegen unverantwortlichen Verhaltens auf dem Internet und Verletzung der Netiquette auflöste¹⁶⁹.

Im Grenzbereich zwischen formalen und materiellen Regeln sind teilweise auch die bereits erwähnten RFCs anzusiedeln. Obwohl ganz überwiegend zur Diskussion und Festlegung von technischen Normen genutzt, finden sich auch materielle Aussagen unter den RFCs¹⁷⁰, die allerdings nicht in einem bestimmten festgelegten Verfahren wie im Bereich der technischen RFCs zu materiellen Standards führen. In diese Richtung zielt jedoch die Schaffung einer Internet Law Task Force (siehe unten).

¹⁶⁸ Ein fest umrissener Bestand an Regeln, die die Netiquette darstellen, läßt sich schwer ausmachen, da der Begriff oft auch allgemein als Bestand der Benimmregeln auf dem Internet betrachtet wird. Eine verbreitete Version findet sich etwa in RFC 1855, <http://ds.internic.net/rfc/rfc1855.txt>, oder in FYI 28, <ftp://ftp.ripe.net/rfc/fyi-index.txt>. Vgl. auch <http://www.fau.edu>. Siehe auch Dufour (o. Fußn. 2), S. 67 m. w. Nachw.

¹⁶⁹ S. Long (o. Fußn. 64), S. 1203 und P. H. Lewis, An Ad (Gasp!) in Cyberspace, New York Times vom 19.4. 1994, S. D1.

¹⁷⁰ vgl. etwa Internet Activities Board, RFC 1087 Ethics and the Internet, 1989; <http://ds.internic.net/rfc/rfc1087.txt>, s. auch RFC 1855 Netiquette Guidelines, 1995 <http://ds.internic.net/rfc/rfc1855.txt>.

c) Benutzungsregeln

Jenseits von rudimentären Regeln und Bräuchen, die jedoch erstaunlich effektiv durchgesetzt werden, indem etwa der elektronische Briefkasten eines Regelverletzers durch Unmengen von E-mails oder eine einzige riesige Datensendung unbrauchbar gemacht wird, finden sich in abgrenzbaren Bereichen, meist bei den kommerziellen On-line-Diensten, aber auch zunehmend bei Universitäten, sehr detaillierte Regeln in Gestalt von Benutzungsregeln, die bei kommerziellen Anbietern im Benutzungsvertrag mit dem Anbieter enthalten sind. Manche Anbieter überprüfen durch elektronische Filter aufgrund solcher Regeln sämtliche Botschaften, auch Privatpost, auf Unwörter, um das Verbot bestimmter unerwünschter Inhalte durchzusetzen¹⁷¹. Teilweise werden im Rahmen der Benutzungsregelungen auch schon Streitschlichtungsmechanismen festgelegt. Das kommerzielle juristische On-line-Diskussionsforum LEXIS Counsel Connect (LCC) etwa bietet einen On-line "Cybercourt", der Streitfragen um Benutzungsregeln klären soll (Beispiel: Streit um Anwendung und Auslegung der Benutzungsregel, wonach in bestimmten Diskussionsrunden Studenten nur "zuhören", d.h. Beiträge lesen dürfen, aktiv mit eigenen Beiträgen teilnehmen können nur Professoren).

¹⁷¹ Vgl. o. Fußn. 118.

2. Regelungsbedarf

Die Vorstellung vom völlig regelungsfreien Raum erweist sich bei näherem Hinsehen also als unzutreffend¹⁷². Gleichwohl zeigen die unter III. angedeuteten Probleme, dass über den gegenwärtigen Zustand hinaus eine Verrechtlichung des Cyberspace wünschenswert wäre. Dabei spielt auch die Überlegung eine Rolle, dass die derzeit gültigen Regelungen in Anbetracht der gewachsenen Bedeutung des Internet mittlerweile einer umfassenderen Legitimation bedürfen, als die ISOC oder private Anbieter sie vermitteln können: Auch die Festlegung nur formaler oder technischer Standards hat teilweise durchaus den Charakter einer politisch-gesellschaftlichen Grundentscheidung. Augenfällig ist dies im Bereich der technischen Standards für die Verschlüsselung¹⁷³.

Wie mehrfach erwähnt, lässt sich einseitig seitens eines einzelnen Staates wegen der technischen Struktur des Cyberspace wenig ausrichten¹⁷⁴. Mögliche Lösungsansätze müssten sich daher darauf richten, entweder Cyberspace als eigenständigen Rechtsraum anzuerkennen (Ausblendung des staatlichen Elementes) oder aber konzertierte internationale Regelungen zu finden (Ausblendung des unilateralen Elementes).

¹⁷² Dies hält auch der Rapport Falque-Pierrotin (o. Fußn. 142) ausdrücklich fest. Probleme entstehen teilweise nicht wegen fehlender Regelungen, sondern wegen einem Zuviel an (einander widersprechenden) Regelungen.

¹⁷³ So auch J. R. Reidenberg, *Governing Networks and Cyberspace Rule-Making*, 45 *Emory Law Journal* 411 (1996).

¹⁷⁴ Dazu der Rapport Falque-Pierrotin (o. Fußn. 142): "[U]ne démarche purement nationale est illusoire", "[A]ucune démarche univoque sera efficace".

a) Regelungsansätze und Regelungsversuche

Die oben angedeuteten Rechtsprobleme haben in jüngerer Zeit nationale Gesetzgeber tätig werden lassen (USA, Frankreich, Deutschland, Großbritannien, Canada, Australien)¹⁷⁵. Mittelpunkt ist dabei fast immer die Frage der Kontrolle von Inhalten bzw. der Verantwortlichkeit für Inhalte.

Dabei stehen sich verschiedene Konzeptionen gegenüber: zum einen der Ansatz, der auf die Selbstregelungskräfte setzt und diese lediglich flankiert, zum anderen ein eher traditioneller, auf staatliche Regelung vertrauender Ansatz. Wo der Staat regelnd eingreift, ist nochmals zu unterscheiden zwischen Regelungsversuchen, die bei den Nutzern ansetzen (Registrierungen, Computerbenutzungsverbote), und Regelungsversuchen, die auf Inhalte im Cyberspace abzielen (Verbot bestimmter Inhalte).

Registrierung und Verbot von Computernutzung wird zumindest in autoritären Regimen zu einem gewissen Erfolg führen, weil außerhalb des Cyberspace angesetzt wird. Einseitig seitens eines Staates bestimmte Inhalte auf dem Internet zu verbieten ist jedoch angesichts der Grenzenlosigkeit des Internet und der Replizierbarkeit von Inhalten außerhalb der Jurisdiktion eines Staates schlechthin aussichtslos.

In China und Singapur versuchen die Regierungen, über die Registrierung von Internet-Anschlüssen und durch technische Filter unerwünschte Inhalte zu unterbinden und erzielen damit wohl auch gewisse Erfolge¹⁷⁶. Weitere Begrenzungsversuche durch die Anordnung technischer oder sonstiger Maßnahmen werden für Saudi-Arabien, Vietnam, Thailand, Hong-Kong und den Iran berichtet¹⁷⁷.

Bei den Regelungsversuchen findet man oft eine repressive Tendenz, wobei diese nicht auf die notorischen autoritären Regime beschränkt ist. Verkannt wird dabei die mehrfach erwähnte Problematik, die darin besteht, dass sich das Regelungsobjekt der Regelung durch bloße Replizierung in einem anderen Staat entziehen kann. Man kann beispielsweise an in Deutschland verbotene Inhalte über Anbieter in den USA gelangen. Allerdings sollte dabei eines nicht verkannt werden: Regelungen werden selten ein Regelungsziel vollkommen erreichen; die lückenlos wirksame Unterbindung des Zugangs zu den verbotenen Informationen ist daher ohnehin kein realistisches Ziel einer solchen Regelung. Wenn jedoch Regelungen die Kosten (im übertragenen Sinne) für den Zugang zu bestimmten Inhalten auch nur erhöhen, wird die Nachfrage nach diesen Inhalten in jedem Falle sinken. Das bedeutet für

¹⁷⁵ Die französische Regierung hat 1996 mit dem Rapport Falque-Pierrotin eine instruktive Zwischenbilanz dieser diversen Gesetzgebungsbemühungen vorgelegt, aus denen für die französische Gesetzgebung entsprechende Schlüsse gezogen werden sollen, vgl.

<http://www.telecom.gouv.fr/francais/activ/techno/missionint.htm>. Der Bericht mündet u.a. in folgende Empfehlungen:

- Die Neuartigkeit des Internet erkennen
- Selbstkontrolle vor präventiver Kontrolle
- Verantwortlichkeiten von Akteuren klar festlegen
- Internationale Zusammenarbeit weiter vertiefen

Auszüge aus diesem Bericht sind abgedruckt bei Tortello/Lointier (o. Fußn. 30), Anhang Nr. 3. In Australien ist ebenfalls vor konkreten gesetzgeberischen Maßnahmen zunächst einmal durch die Australian Broadcasting Authority ein Bericht erstellt worden, Investigation into the Content of On-line Services, siehe <http://www.dca.gov.au/aba/olsrprt.htm>.

¹⁷⁶ Angst vor der Anarchie, Der Spiegel 13/1996, S. 138; Die Zensur ist global, Die Tageszeitung v. 30.5.1996, S. 12; zur Regelung in Singapur s. LINK <http://www.gov.sg/sba/netreg/regrel.htm>.

¹⁷⁷ Vgl. Piette-Coudol/Bertrand, (o. Fußn. 4), S. 47 und S. 116 f. m.w.Nachw.

das konkrete Beispiel, dass die Anzahl der deutschen Nutzer, die sich die Inhalte aus den USA besorgen, niedriger sein wird als die Anzahl der Nutzer, die sich die Inhalte ohne das Verbot verschafft hätten, da der Umweg über die USA mit Kosten (Aufwand, Umstände, gar echte Kosten) verbunden ist¹⁷⁸.

aa) Beispiel USA

In den USA etwa bedrohte ein Bundesgesetz, der Communications Decency Act (CDA)¹⁷⁹ vom Februar 1996, auch On-line-Anbieter mit Strafe, wenn sie unsittliches (indecent) Material verbreiteten¹⁸⁰. Das Gesetz wurde bereits kurz nach Inkrafttreten gerichtlich außer Vollzug gesetzt, weil der Begriff "indecent" nicht hinreichend bestimmt ist¹⁸¹. Der U.S. Supreme Court erklärte den CDA am 26. Juni 1997 teilweise für verfassungswidrig. Der CDA ist wegen seiner einschränkenden Tendenz Gegenstand heftiger Diskussionen gewesen. Die Entscheidung des Supreme Court wird hier möglicherweise richtungweisend sein für die Entscheidung über eine eher zurückhaltende oder eine eher kontrollorientierte Gesetzgebung auch in anderen Staaten¹⁸².

bb) Beispiel Deutschland

Zurückhaltend, aber auch realistisch erscheint vor diesem Hintergrund das Multimedia-Gesetz des Bundes in Deutschland (Gesetz über Informations- und Kommunikationsdienste, IuKDG¹⁸³), in Kraft seit 1. August 1997. Umstritten war zunächst schon die Gesetzgebungskompetenz zwischen dem Bund und den Ländern¹⁸⁴. Ein dann gefundener Kompromiss richtete sich darauf, dass die Länder Teleshopping, PayTV und Video-on-demand per Staatsvertrag regeln, On-line-Kommunikation dagegen in die Bundeskompetenz fällt. Die technische Entwicklung lässt hier schwierige Abgrenzungsfragen erwarten¹⁸⁵. Man wird dann mit der Abgrenzung nach Bezugsschwerpunkt arbeiten müssen (Beispiel: die interaktive On-line-Kommunikation mit einem PayTV-Anbieter über das entsprechende Zusatzgerät wird sich weiter dem Bereich des PayTV zuordnen lassen). Offen ist derzeit, ob Abgrenzungen, bei denen etwa WWW-Seiten mit redaktionellem Inhalt der Länderkompetenz zugeordnet werden, E-mails an die Betreiber dieser Homepage jedoch der Bundeskompetenz unterfallen, überhaupt praktikabel sind¹⁸⁶. Insgesamt wäre eine einheitliche Bundeskompetenz auch wegen der langfristig möglicherweise erforderlichen internationalen Absprachen sinnvoll. Grundsätzlich beabsichtigt die gesetzliche Regelung nicht, Internet-Anbieter für die Inhalte auf ihren Diensten verantwortlich zu machen, es sei denn, den Anbietern sind strafbare

¹⁷⁸ L. Lessig, The Zones of Cyberspace, 48 Stanford Law Review 1367 (1996), S. 1405 mit Hinweis auf Coase.

¹⁷⁹ 47 U.S.C. Section 223 (a) bis (h).

¹⁸⁰ Section 223 (a) (1) (B).

¹⁸¹ U.S. District Court Eastern District of Pennsylvania, American Civil Liberties Union et al. v. Janet Reno, Civil Action No. 96-963, Beschluß vom 15.2. 1996. Siehe auch <http://www.aclu.org/court/cdadec.html>, allgemein <http://www.eff.org>.

¹⁸² Zum CDA s. A. Lewine, Making Cyberspace Safe for Children(?): A First Amendment Analysis of the Communications Decency Act of 1996, 18 Hamline Journal of Public Law and Policy (1996). Die Entscheidung des Supreme Court (*Reno v. ACLU*) findet sich unter <http://www.findlaw.com/casecode/supreme.html>

¹⁸³ BGBl. I 1997, 1870; Wortlaut des Gesetzes unter <http://www.iid.de/rahmen/iukdgbt.html> und <http://www.bmbf.de/>. Die Begründungen finden sich unter

<http://www.uni.duesseldorf.de:80/WWW/Jura/netlaw/IuKDG-Begr.html>.

¹⁸⁴ Wegen der - behaupteten - Nähe zum Rundfunk beanspruchten die Länder die Länderkompetenz, geplant war in Anlehnung zum Rundfunk ein On-line-Staatsvertrag auf Grundlage des Btx-Staatsvertrages. Der französische Rapport Falque-Pierrotin (o. Fußn. 142) wertet den Ansatz der Länder als 'traditionell'.

¹⁸⁵ In den USA zeichnet sich bereits die "Vereinigung zweier Welten" ab, Schütte/Ludes, Auf dem Weg zum Computerfernsehen, Die Zeit v. 30.8.1996, S. 58.

¹⁸⁶ Vgl. dazu Hablützel, Internet unter Länderaufsicht?, Die Tageszeitung v. 14.11.1996, S. 13.

Inhalte bekannt und sie haben die technischen Möglichkeiten, den Zugang zu unterbinden¹⁸⁷. Vielmehr soll auch in diesem Bereich das das deutsche Presserecht prägende Prinzip der Selbstkontrolle wirken, nicht zuletzt weil man erkennt, dass absolute Zugangssperren kaum realisierbar sind. Die Bundesregierung nimmt damit eine andere Haltung ein als teilweise die Staatsanwaltschaften, sie hat jedoch abgelehnt, sich zu den Maßnahmen dieser Landesbehörden zu äußern¹⁸⁸. Im übrigen verweist die Bundesregierung auf die nach wie vor geltenden Bestimmungen des herkömmlichen Strafrechts, wo beispielsweise hinsichtlich der Verbreitung kinderpornografischer Schriften das Weltrechtsprinzip (§ 6 Nr. 6 StGB) gilt.

¹⁸⁷ Vgl. Bundestags-Drucksache 13/4800, Antwort der Bundesregierung, Kontrolle und Selektion von Telekommunikationsvorgängen, S. 2.

¹⁸⁸ Bundestags-Drucksache 13/4800, (o. Fußn. 187), S. 7.

b) Cyberspace als eigenständiger Rechtsraum

Bei der Diskussion um die künftige Entwicklung taucht immer wieder das Schlagwort vom Cyberspace als eigenständigem Regelungs- oder Rechtsraum auf¹⁸⁹. Dieser Ansatz führt die Konzeption, wie sie für die Erzeugung technischer Regeln im Laufe der Zeit gewachsen ist, konsequent weiter. Er vertraut auf die Selbstregelungsfähigkeit des Internet und seiner Nutzer. Diese den Staat bzw. die Staaten möglichst ausblendende Vorstellung einer community im Internet, die sich ihr Recht selbst schafft, wird vor allem in den USA vertreten, was sich aus der dortigen Gesellschaftskonzeption und dem Vertrauen in die Gestaltungskräfte der Individuen ohne den Rückgriff auf staatlichen Beistand erklärt.

Ausgangspunkt ist dabei die Frage nach der zuständigen Jurisdiktion für den Cyberspace, worauf die Antwort gegeben wird, dass die Lösung eine eigene Jurisdiktion des Cyberspace sein müsse. Zunächst ist nicht von der Hand zu weisen, daß viele Probleme, die sich im Zusammenhang mit Cyberspace ergeben, bei näherem Hinsehen in der Tat als Probleme der Jurisdiktion erscheinen: Wo ist Cyberspace? Welches Recht gilt? Wer entscheidet? Wer verfolgt? Eine mögliche Antwort hierauf ist, dass nur die Annahme einer eigenständigen Cyberspace-Jurisdiktion eine kohärente Lösung bietet.

Theoretisch bleibt zur Beantwortung dieser Fragen zwar die Anknüpfung an die reale Welt, an territoriale oder personale Kriterien, möglich: Wer im Cyberspace Kinderpornografie verbreitet und seine Wohnadresse oder Identität offenbart, kann von den Verfolgungsbehörden aufgespürt werden. Jedoch sind die sich stellenden rechtlichen Probleme eben keine reinen Vollzugsprobleme: Da die durchzusetzenden Ge- und Verbote bis auf wenige Ausnahmen, wie vielleicht das Verbot von Kinderpornografie¹⁹⁰, in den verschiedenen Jurisdiktionen unterschiedlich ausgestaltet sind, lassen sich mit dem Verweis auf die Vollzugsmöglichkeiten in der realen Welt nicht alle Fragen schlüssig beantworten. Eine solche herkömmliche Betrachtungsweise reduziert das Internet auf einen reinen Übertragungsvorgang, wo zwischen den rechtlich ausschließlich erheblichen geographischen Ausgangspunkten bestimmte Inhalte nur transportiert werden¹⁹¹ und es keine erkennbare Dimension zwischen diesen geographischen Ausgangspunkten gibt. Dies greift jedoch zu kurz.

Es bleibt jedenfalls das Problem des Konfliktes zwischen den sich widersprechenden nationalen Rechtsordnungen, in denen bestimmte religiöse oder politische Äußerungen hier strafbar sind, dort nicht, oder die Frage der Urheberrechtsverletzungen, die hier verfolgt werden, dort aber nicht interessieren usf.

Denkbar wäre hier, ähnlich wie im Internationalen Privatrecht (treffender die englische Bezeichnung: 'Conflict of Laws') ein personales oder territoriales Element zum Anknüpfungspunkt zu nehmen, um eine ausschließliche Zuständigkeit zu ermitteln. Dem lässt sich entgegenhalten¹⁹², dass die berührten rechtlichen Problemfelder eine solche Anknüpfung

¹⁸⁹ Vgl. dazu etwa D. Johnson/D.Post, Law and Borders - The Rise of Law in Cyberspace, 48 Stanford Law Review 1367 (1996): "taking Cyberspace seriously".

¹⁹⁰ Der Mißbrauch von Kindern in pornographischen Darstellungen dürfte in den meisten Rechtsordnungen in irgendeiner Form sanktioniert sein, vgl. etwa für Frankreich Artikel 227-23 des neuen Code Pénal: "Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image d'un mineur lorsque cette image présente un caractère pornographique est puni d'un an d'emprisonnement et de 300 000 F d'amende."

¹⁹¹ Johnson/Post (o. Fußn. 189), S. 1378.

¹⁹² Zu den Unlänglichkeiten der herkömmlichen, letztlich immer geographisch bezogenen Doktrinen zur Bestimmung der Jurisdiktion s. Johnson/Post (o. Fußn. 189), S. 1369 m.w.Nachw.

entweder überwunden haben (Strafrecht, Urheberrecht) oder aber absichtsvoll vermeiden. Ohnehin erscheint die Anknüpfung an das personale Element, konkret die Staatsangehörigkeit des jeweiligen Nutzers, praktisch problematisch in einem extrem flexiblen internationalen Datenstrom, in dem die Identität der Teilnehmer möglicherweise anonymisiert ist, wo Nachrichten für Regierungen unzugänglich verschlüsselt werden können und wo bereits der Zugriff auf die reale Person hinter der im Cyberspace agierenden Person nur begrenzt möglich ist. Territorial anzuknüpfen ist kaum möglich, da sich die Übertragungswege wegen der oben dargelegten störungsresistenten Technologie des Internet nicht linear beschreiben und damit auch nicht ermitteln lassen. An den "Sendeort" anzuknüpfen, an dem - etwa im WWW - Inhalte zur Verfügung gestellt werden, ist nicht ohne weiteres durchführbar, weil der Abruf von Inhalten oft zu temporären Kopien dieser Inhalte andernorts führt bzw. häufig aufgerufene Inhalte andernorts 'gespiegelt' werden und daher mehrfach existieren.

Die sich überschneidenden und dabei oft nicht durchsetzbaren Gebote und Verbote der einzelnen Rechtsordnungen ermöglichen keine effektive Kontrolle. Effektive Kontrolle ist jedoch ein denkbare Regelungsziel. Effektive Kontrolle des Cyberspace wäre nur dann möglich, wenn die Struktur des Cyberspace geändert würde. Einseitig von den einzelnen Rechtsordnungen aus kann effektive Kontrolle nicht gelingen.

Vor den Hintergrund der gegenwärtigen besonderen Natur des Cyberspace erscheint es daher folgerichtig, Cyberspace als eigenständigen, neuartigen Rechtsraum zu begreifen ("Cyberspace as a place")¹⁹³, der zunächst einmal außerhalb der diversen staatlichen Jurisdiktionen steht.

Die Annahme einer eigenständigen Cyberspace-Jurisdiktion sagt noch nichts darüber aus, wer in dieser Jurisdiktion Normen setzt und wie diese durchgesetzt werden¹⁹⁴. Teilweise wird hier die Auffassung vertreten, dass sich eigenständige effektive Rechtsinstitutionen ausbilden können¹⁹⁵.

aa) Rolle des Staates

Eine nicht vom Staat ausgehende oder aber - zumindest überwiegend - durch Staaten vermittelte (so lässt sich das Völkerrecht auffassen) Rechtsordnung anzunehmen, erscheint zunächst einmal befremdlich. Dazu wird jedoch argumentiert - und dieser Befund dürfte unstrittig sein -, dass die modernen Informationstechnologien bestimmte politische Auswirkungen zeitigen, die die Erosion der nationalen Souveränität in einer ökonomisch interdependenten Welt zumindest nicht aufhält¹⁹⁶. Möglicherweise etwas voreilig, aber im Ansatz nicht unbegründet ist die Feststellung, dass der Nationalstaat das adäquate Modell für das industrielle Zeitalter war, mitnichten aber für das informationelle Zeitalter geeignet ist¹⁹⁷. Und schließlich ist zuzugeben, dass bereits vor Entstehung der modernen Staaten Regeln entstehen konnten und auch Mechanismen sich ausprägten, die diesen Regeln zur Durchsetzung verhelfen.

¹⁹³ Johnson/Post (o. Fußn. 189), S. 1378.

¹⁹⁴ Johnson/Post (o. Fußn. 189), S. 1387.

¹⁹⁵ Johnson/Post (o. Fußn. 189), S. 1387.

¹⁹⁶ Zu den politischen Auswirkungen moderner Technologien s. W. B. Wriston, *The Twilight of Sovereignty*, 1992, der die Aushöhlung der nationalen Souveränität in Anbetracht grenzüberschreitender Informationsflüsse diskutiert. S. auch Burk (o. Fußn. 102), S. 49.

¹⁹⁷ Burk (o. Fußn. 102).

Allerdings wäre auch bei der Entwicklung eines eigenständigen Cyberspace-Rechts ohne staatliche Einflussnahme bei der Entwicklung dieses Rechts erforderlich, dass die Staaten diese neue Jurisdiktion respektieren. Dies bedeutet konkret, dass die Staaten Cyberspace als eigenständigen Rechtsraum anerkennen müssten, und damit mittelbar doch an der eigenständigen Cyberspace-Rechtsordnung durch die erforderliche Zurücknahme eigener Jurisdiktion mitwirken würden. Für die Ausgestaltung dieses Nebeneinander von souveränen (Staaten) und semi-souveränen Entitäten¹⁹⁸ im Cyberspace lassen sich bestimmte Aspekte aus den herkömmlichen Gewaltenteilungskonzepten entnehmen; ein Stichwort in diesem Zusammenhang ist Network Federalism¹⁹⁹.

bb) Struktur

Sollte sich ein eigenständiges Recht des Cyberspace entwickeln, so wird hinsichtlich der Struktur vermutet, dass es nicht hierarchisch organisiert wäre, sondern dass es an Konsens und Diskussion orientiert sein und als loser Verbund von Regeln und Konventionen wachsen würde, in dem eine freiwillige Schiedsgerichtsbarkeit Streitfälle schlichtet. Was dies genau heißen könnte, ist schwierig zu sagen: Als Vorbild für die Rechtsstruktur wird das Recht sich selbst autonom verwaltender Organisationen wie Kirchen oder Handelskammern genannt. Auch die Art und Weise, wie sich im Mittelalter Handelsbräuche entwickelt haben, stellt ein Beispiel dar für von staatlichem Einfluss freie Normentwicklung²⁰⁰. Dass das selbstregulierende Potential des Internet und seiner Nutzer nicht zu unterschätzen ist, belegt die Reorganisation der Usenet-Struktur (siehe oben II. 1. d) zu Newsgroups) im Jahre 1986, der eine mehrmonatige Diskussion und Konsensbildung der Nutzer vorausging²⁰¹. Von selbstregulierendem Potential zeugt allgemein das Verfahren zur Aufnahme einer neuen Newsgroup: Vorschläge für eine neue Diskussionsgruppe werden in RFDs (Requests for Discussion) vorgestellt. Darin werden Motivation des Vorschlags, Beziehung zu bestehenden Diskussionsgruppen sowie für die Diskussionsgruppe vorgesehene Themen erläutert. Zu einem bestimmten Zeitpunkt wird ein Abstimmungsauftrag, ein Call for Vote (CFV) auf dem Internet veröffentlicht, wonach die Nutzer ihre Stimme für oder gegen eine neue Newsgroup per E-mail abgeben. Damit eine neue Newsgroup als zugelassen gilt, sind mindestens 100 Ja-Stimmen mehr als Nein-Stimmen erforderlich, wobei mindestens zwei Drittel der abgegebenen Stimmen Ja-Stimmen sein müssen²⁰². Dieses Verfahren wird gerne als Beispiel für das demokratische Potential des Internet genannt, weil keine zentrale Entscheidungsinstanz über die Errichtung einer Newsgroup befindet, sondern die Nutzer selbst, wobei die Diskussion zur Ermittlung eines Kompromisses im Vordergrund steht, der dann durch die Abstimmung bestätigt wird²⁰³. Eine gewisse Parallele zum Verfahren im Bereich der technischen Standards (RFCs, rough consensus, siehe oben) ist unverkennbar.

cc) Rechtserzeugung

Der Übergang von der Konvention bzw. vom Brauch zum Recht ist in der Konzeption vom sich selbst regulierenden Cyberspace unscharf. Eine gewisse Verrechtlichung der Netiquette findet allerdings bereits heute statt in den Nutzungsverträgen (bzw. Nutzungsbedingungen) zwischen Nutzern und kommerziellen oder nicht-kommerziellen Anbietern. Eine

¹⁹⁸ So die Kategorie von Reidenberg (o. Fußn. 183) für Netzwerke im Cyberspace.

¹⁹⁹ Reidenberg (o. Fußn. 183).

²⁰⁰ T. Hardy, The Proper Legal Regime for Cyberspace, 55 University of Pittsburgh Law Review 993, 1019-1021 (1994); Johnson/Post (o. Fußn. 189), S. 1389.

²⁰¹ Vgl. dazu Dufour (o. Fußn. 2), S. 64.

²⁰² Im Frühjahr 1996 wurde beispielsweise die Errichtung einer Neonazi-Newsgroup mehrheitlich abgelehnt, s. Piette-Coudol/Bertrand, (o. Fußn. 4), S. 133.

²⁰³ Zum Verfahren mit weiteren Nachweisen Dufour (o. Fußn. 2), S. 66 f.

vergleichende Betrachtung dieser Nutzungsbedingungen wiederum ergäbe einen gewissen Bestand an 'Cyberrechtsgrundsätzen'.

Einen vielbeachteten konkreten Schritt auf dem Wege zur Entwicklung eines eigenständigen Rechts stellt das 1995 begonnene Projekt einer Internet Law Task Force (ILTF) dar, die mittlerweile in ILPF (Internet Law and Policy Forum) umbenannt wurde²⁰⁴. Diese soll im Rahmen der ISOC (siehe oben) ähnlich wie die IETF auf technischem Gebiet nun auf juristischem Gebiet Standards setzen. Beabsichtigt ist, die ILPF mit einem Sekretariat, einem Forum und diversen Arbeitsgruppen zu errichten. Das Vorhaben ist nicht ohne Kritik geblieben. Der Cook-report²⁰⁵ beanstandete im Juli 1996 vor allem die mangelnde Legitimation der ILPF-Mitglieder, deren Auffassungen nicht repräsentativ für die Internet-Gemeinde seien, und empfahl, die Aktivitäten des ILPF genau zu verfolgen, weil das dort bevorzugte governance model einer effektiven Kontrolle durch einige wenige Institutionen nicht den ursprünglichen Prinzipien des Internet entspreche.

Jedenfalls dürfte die ILPF durch die Verbindung mit den technische Standards vorgebenden Gremien und die Beteiligung von Anbieter-Unternehmen ein erhebliches Einflusspotential erreichen²⁰⁶.

dd) Streitschlichtung

Was die Streitschlichtung angeht, so könnten den kommerziellen und nicht-kommerziellen Anbietern des Cyberspace-Zugangs Jurisdiktionsbefugnisse gegeben werden, verbunden mit einer Art Schiedsklausel im Benutzungsvertrag mit dem Server. Als Beispiel dafür, wie Streitschlichtung hier aussehen könnte, kann das Beispiel des Cybercourt des juristischen kommerziellen Forums Lexis Counsel Connect gelten. In eine ähnliche Richtung geht das 1996 begonnene Projekt eines On-line-Schiedsgerichts Virtual Magistrate, das nicht an einen bestimmten Anbieter angebunden ist, sondern zur Streitschlichtung von jedem Nutzer angerufen werden kann. Die Schiedsrichter werden teilweise von der American Arbitration Association berufen²⁰⁷.

ee) Sanktion

Die Durchsetzung von Regeln würde erfolgen durch die Androhung des Ausschlusses vom Zugang zum Cyberspace durch den Anbieter²⁰⁸, die rechtsförmiger Überprüfung zugänglich wäre.

Bedenkenswert, wenn auch im Einzelnen nicht unproblematisch erscheinen im Bereich der umstrittenen Meinungsäußerung differenzierende Lösungen, die sich nicht sofort auf den Ausschluss vom Zugang zum Cyberspace und damit auf das Verbot einer Äußerung richten. Zu denken ist hier an Auflagen zur Gewährleistung von Gegenöffentlichkeit durch die On-line-Anbieter an ihre Kunden. Der wegen Verbreitung von Neonazi-Propaganda bekannt

²⁰⁴ Zur ILTF bzw. ILPF Piette-Coudol/Bertrand (o. Fußn. 4), S. 17 ff.

²⁰⁵ Die amerikanische Cook-Vereinigung beobachtet Aktivitäten auf dem Internet, siehe <http://pobox.com/cook/>.

²⁰⁶ Dies gilt umso mehr, als auch staatlicherseits eine Internet-Instanz gefordert wird, vgl. die diesbezügliche Empfehlung des Rapport Falque-Pierotin (o. Fußn. 142), abgedruckt bei Tortello/Lointier (o. Fußn. 30), Anhang Nr. 3, hier S. 267.

²⁰⁷ Grundlage der Schiedssprüche sollen allgemeine Rechtsprinzipien, equity und die Regeln der Netiquette sein, vgl. Tortello/Lointier (o. Fußn. 30), S. 20 f. Die erste Entscheidung des Virtual Magistrate vom 21. Mai 1996 findet sich unter <http://vmag.law.vil.edu:8080:doksys/96-0001/>.

²⁰⁸ Vgl. dazu T. Hardy, A new jurisdiction for cyberspace? A transcript of NEWJURIS, an electronic conference held September-October 1993, nicht veröffentlicht.

gewordene Ernst Zündel²⁰⁹ etwa muss auf seiner Homepage einen Querverweis zu einer Organisation anbieten, die über den Holocaust informiert (Nizkor²¹⁰). Auch Nizkor bietet (freiwillig) einen Querverweis zu Zündel.

ff) Realisierungschancen

Der selbstregulierenden Kraft des Internet zu vertrauen, führt weg vom rechtlichen Zentralismus. Dies entspricht der typischen Denkweise - übrigens auch was die Rolle des Staates angeht - im Common Law²¹¹.

Fraglich bleibt jedoch, ob angesichts der zu erwartenden Dimensionen des Cyberspace, verbunden mit seiner Ubiquität eine solche Rechtsentwicklung realistischerweise möglich ist²¹². Insbesondere bleibt das Problem, dass eine über die ganze Welt verteilte Gemeinschaft von Regelungsunterworfenen nur schwerlich einen Konsens selbst über wenige gemeinsame Grundregeln erzielen wird. Schließlich ist auch die hinter kommerziellen Anbietern stehende Wirtschaftsmacht problematisch, ginge es doch darum, die nähere Ausgestaltung von Grundrechtsausübung Privaten zu überlassen, nicht zuletzt weil im Bereich der kommerziellen weltweit tätigen Anbieter amerikanische Anbieter - und damit auch bestimmte Wert- und Rechtsvorstellungen - dominieren²¹³.

Der Haupteinwand gegen die Konzeption vom autonomen Recht ist jedoch ein anderer: Sie verkennt das Interesse der Staaten an der Beteiligung bei der Entwicklung von Normen im Bereich des Cyberspace.

Cyberspace als eigenständigen Regelungsraum anerkennen, heißt nicht zwangsläufig, diesen Regelungsraum als unabhängig anzuerkennen²¹⁴. Vielmehr spricht vieles dafür, dass die reale Welt die Kontrolle über die virtuelle Welt behalten wird²¹⁵. Insbesondere die ökonomischen Interessen und grundrechtsrelevante Fragen werden dafür sorgen, dass sich die virtuelle nicht allzuweit weg von der realen Welt entfernt. Dies wird auch durch das stetig zunehmende

²⁰⁹ Siehe oben Fußn. 113.

²¹⁰ Siehe <http://nizkor.almanac.bc.ca>.

²¹¹ Diesen Zusammenhang zwischen common law und Präferenz für Selbstregulierung beobachtet auch der Rapport Falque-Pierrotin (o. Fußn. 142) für den auf Selbstregulierung setzenden britischen Regelungsentwurf.

²¹² Ein origineller Beitrag zur empirischen Erforschung von Gewohnheitsrecht aus Sicht der ökonomischen Analyse des Rechts findet sich bei Robert Ellickson, *Order without Law: How Neighbors settle Disputes*, 1991. Ellickson untersucht dabei die für das Common Law typische dezentralisierte Rechtsentstehung am Beispiel der Regeln, die sich zwischen Viehzüchtern in einem abgelegenen Landstrich Kaliforniens für die Haftung bei Viehschäden entwickelt haben und faßt den Kenntnisstand über dezentralisierte Rechtsentstehung von informellen Normen zusammen. Ellicksons Ergebnis ist, daß Kooperation jenseits aller formellen Normen im Falle geringer materieller Schäden stattfindet. Das Kooperationsproblem läßt sich auch aus der Perspektive der Game Theory vor dem Hintergrund des Prisoner's Dilemma deuten (s. dazu etwa Fudenberg/Maskin, *The Folk Theorem in Repeated Games with Discounting and Incomplete Information*, 54 *Econometrica* 533 (1986)). Ellickson weist auch darauf hin, daß soziale Normen nur bis zu einer bestimmten Größe der jeweiligen Gesellschaft wirksam sind (Ellickson, a.a.O. S. 177 f., 182), und möglicherweise ist Cyberspace informellen Regelungsmöglichkeiten daher bereits entwachsen. Vielleicht würde hier die Unterscheidung zwischen einem öffentlichen und einem privaten Cyberspace weiterführen.

²¹³ Die anglo-amerikanische Dominanz dokumentiert sich bereits durch die im Cyberspace vorherrschende Sprache, kritisch dazu Cassen, *English spoken - muß das sein?*, *Le Monde Diplomatique* (dt. Ausgabe) v. Mai 1996, S. 5. Insgesamt geraten die kulturellen Auswirkungen des Cyberspace zunehmend ins Blickfeld, vgl. etwa German, *Politische (Irr-)Wege in die globale Informationsgesellschaft*, *Aus Politik und Zeitgeschichte B 32/96*, S. 16. Siehe dazu auch das Forschungsprojekt am Wissenschaftszentrum zu Berlin 'Kulturraum Internet', <http://www.duploxx.wz-berlin.de>.

²¹⁴ Darauf vereist zutreffend Lessig (o. Fußn. 178), S. 1405.

²¹⁵ Lessig (o. Fußn. 178), S. 1403.

Interesse der Staaten und der Öffentlichkeit am Internet belegt und hat damit zu tun, dass Cyberspace keine Nische für Eingeweihte und geistesverwandte Cybernauten mehr ist.

Die mehrfach erwähnte Nicht-Örtlichkeit und Nicht-Fassbarkeit des Cyberspace dürfte ein zentrales Argument für die Annahme eines eigenständigen Regelungsraumes sein. Daraus folgt jedoch nicht, dass Regelungen staatlicherseits nicht möglich sind, sondern dass Regelungen in anderer Art und Weise als sonst erfolgen müssen, wenn sie Wirkung erzielen sollen²¹⁶.

Hier ist zunächst an 'mittelbare' Regelungen zu denken: Die USA können nicht einseitig die Verschlüsselung weltweit verbindlich regeln. Aber die Subventionsvergabe für die Entwicklung bestimmter Technologien lässt sich ohne weiteres regeln²¹⁷.

Denkbare Ansatzpunkte für staatliche Einflussnahme sind jedoch durchaus viel unmittelbarer vorhanden: Wenn und soweit die Staaten gemeinsam vorgehen. Angesetzt werden kann nämlich auf der technischen Ebene, wie es im Kryptographie-Bereich (dort allerdings mit mäßigen Erfolg, nicht zuletzt aber wegen der Uneinigkeit der Staaten) bereits versucht wurde. Letztlich gilt, dass wer die Kontrolle über die Standards des Internet hat, letztlich die Kontrolle über die Inhalte hat. Vor diesem Hintergrund relativiert sich auch die These von der Offenheit bzw. Unkontrollierbarkeit des Cyberspace. Ist es nicht vielmehr so, dass die Offenheit des Cyberspace derzeit nur existiert, weil das 'Sozialkonstrukt' Cyberspace eben so angelegt ist²¹⁸? Dann käme es nun darauf an, dieses offene, unbeplante Rechtsgebiet zu 'beplanen'²¹⁹. Ob eine Veränderung dieses Sozialkonstrukts machbar ist, erscheint so gesehen nicht als grundsätzliche Frage, sondern als Frage nach der Regelungstechnik. Hier kommt das internationale Recht ins Blickfeld.

²¹⁶ Lessig (o. Fußn. 178), S. 1407.

²¹⁷ Beispiel bei Lessig (o. Fußn. 178), S. 1406.

²¹⁸ Lessig (o. Fußn. 178), S. 1408.

²¹⁹ Lessig (o. Fußn. 178) verwendet dieses Bild vom "Zoning", vgl. S. 1408 f.

c) Cyberspace und internationales Recht

Das traditionelle Instrumentarium des Völkerrechts bietet Möglichkeiten wie etwa eine internationale Konvention mit Errichtung einer zuständigen Internationalen Organisation, wenn es darum geht, weltweit verbindliche Regelungen zu erreichen (ohne dass dies auch weltweit einheitliche Regelungen bedeuten müsste). Das Völkerrecht ermöglicht grenzüberschreitende Regelungen, wie sie ein derart grenzenloses Medium wie das Internet zwingend erfordert; seine Hauptakteure, die Staaten, gewährleisten jedoch gleichzeitig eine gewisse Stabilität und damit Rechtssicherheit, wie sie die Konzeption des autonomen Cyberspace-Rechts bisher noch nicht bieten kann. Es fällt auf, dass die völkerrechtliche Option und Dimension in der amerikanischen Diskussion fast völlig ausgeblendet ist und die Debatte dort sich auf die Selbstregulierung des Internet konzentriert. Eine mögliche Erklärung dafür ist, dass aus amerikanischer Sicht eine völkerrechtliche Regelung zu sehr auf staatlich monopolisierte Kontrolle hinausläuft. Diese Sichtweise verkennt, dass auch im Bereich einer völkerrechtlichen Regelung über NGOs und IOs Akteure außerhalb der Staaten eine wichtige Rolle ausfüllen können.

Eine vom Völkerrecht ausgehende Regelung hätte zunächst den Vorteil, dass Vorgaben aus dem Bereich des internationalen Rechts, die nationalen Regelungen entgegenstehen, einfacher berücksichtigt werden könnten. Zu denken ist hier an Vorgaben aus dem Bereich GATT und WTO²²⁰.

Entscheidend wäre die möglichst globale Beteiligung an einer solchen internationalen Regelung²²¹. Probleme könnten sich hier ergeben aus dem informationellen Nord-Süd-Gefälle, in dem weniger entwickelte Staaten kein Interesse an einer gemeinsamen Regelung haben können, wenn sie ohne gemeinsame Regeln durch "Datendumping" im Sinne von laxeren Regelungen des Datengebrauches wenigstens etwas in den internationalen Datenverkehr eingebunden werden²²². Weiterhin setzt internationale Zusammenarbeit zur Lösung eines Problems normalerweise voraus, dass die beteiligten souveränen Staaten zur Lösung des Problems irgendwo innerhalb ihrer eigenen Grenzen ansetzen können, um diesen Ansatz dann durch internationale Zusammenarbeit zu ergänzen. Dies ist hier nicht ohne weiteres der Fall, weil Cyberspace, anders als etwa Rundfunk, unabhängig von staatlicher Lizenzierung existiert, sich staatlichen Maßnahmen leicht entziehen kann und sich aufgrund seines extra- oder infranationalen Charakters schwer fassen lässt. Schließlich ist fraglich, ob man sich über technische und formale Regeln hinaus auch auf materielle Normen verständigen könnte, würden hier doch wieder unterschiedliche Wertvorstellungen aufeinandertreffen²²³. Wo beispielsweise im Hinblick auf Kinderpornografie ein weltweiter Konsens immerhin vorstellbar ist, wird darüber hinaus über das Recht der freien Rede schwerlich Übereinstimmung erzielbar sein.

Dennoch zeigt der Fall Helsinghuis zwischen den U.S.A und Finnland²²⁴, dass internationale Zusammenarbeit - wenn sie denn zustande kommt - im Cyberspace Wirksamkeit entfalten

²²⁰ Vgl. Piette-Coudol/Bertrand (o. Fußn. 4), S. 64.

²²¹ Dies ist nicht völlig undenkbar, vgl. hierzu die Rechtsgrundlagen der internationalen fernmeldetechnischen Ordnung, insbesondere die Nairobi Konvention von 1982, BGBl II 1985, 425.

²²² Nord-Süd-Gefälle und Technologie-Transfer sind keine neuen Themen. Zum Nord-Süd-Gefälle in der informationstechnischen Entwicklung s. Burk (o. Fußn. 102), S. 51 m. w. Nachw., s. auch Renaud/ Torr□s, Internet - eine Chance für den Süden, *Le Monde Diplomatique* (dt. Ausgabe) v. 8.2.1996, S. 8.

²²³ Die vorsichtige Formulierung des Art. 19 des Internationalen Paktes über bürgerliche und politische Rechte (CCPR) (BGBl II 1973, 1534) über die Meinungsfreiheit deutet auf diese Schwierigkeiten hin.

²²⁴ S. oben Text zu Fußn. 71.

kann. Denkbar ist etwa, die sich im Bereich der kommerziellen und nicht-kommerziellen Anbieter ausgeprägten 'Cyberrechtsgrundsätze' zum Ausgangspunkt einer völkerrechtlichen Regelung zu nehmen.

Eine zu errichtende Internationale Organisation, die durchaus an bestehende Strukturen innerhalb der UN oder der ITU²²⁵ angegliedert werden könnte, wäre verantwortlich sowohl für formale (technische) Standards wie auch für materielle (rechtliche) Standards²²⁶. Hier könnten auch die existierenden Strukturen innerhalb der ISOC einbezogen werden.

Soweit eine möglichst globale Regelung (noch) nicht erreichbar ist, sollten wenigstens auf regionaler Ebene grenzüberschreitende Regelungsstrukturen genutzt werden. Für Europa bietet sich hier eine Zusammenarbeit im Rahmen der bestehenden Strukturen der EU bzw. EG an. Auf die vielfältigen Aktivitäten der EU bzw. EG, die Cyberspace betreffen, kann hier nicht im einzelnen eingegangen werden. Zusammenfassend lässt sich sagen, dass bisher eher Einzelaspekte (Urheberrechte, Telekommunikationsmärkte u.ä.) im Vordergrund standen. Einer umfassenden Regelung dürfte vor allem der Umstand entgegenstehen, dass die EG wegen des Prinzips der begrenzten Einzelermächtigung auf eine ausdrückliche Kompetenzzuweisung angewiesen ist. Eine solche existiert aber für einen Regelungsbereich Cyberspace bisher nicht. Weitere punktuelle Anknüpfungspunkte dürften sich aber sowohl im vergemeinschafteten Bereich der EG (Beispiel: Werbeverbote von Mitgliedstaaten, die auch WWW-Werbungen aus anderen Mitgliedstaaten erfassen, fallen unter Umständen unter das Verbot von Maßnahmen gleicher Wirkung wie mengenmäßige Beschränkungen im Sinne der nach Art. 30 EGV gewährleisteten Warenverkehrsfreiheit²²⁷) wie im intergouvernementalen Bereich (Beispiel: Zusammenarbeit in den Bereichen Justiz und Inneres) ergeben²²⁸.

²²⁵ Internationale Fernmeldeunion.

²²⁶ Ein Vorbild findet sich im Zusammenhang mit EDI-Austauschvereinbarungen (Electronic Data Interchange), der im Handels- und Industriebereich zunehmend an Bedeutung gewinnenden Form der Kommunikation, bei denen Absprachen über die Kommunikationsstruktur und rechtliche Rahmenvereinbarungen getroffen werden: Hier hat die Wirtschaftskommission der Vereinten Nationen für Europa (UN/ECE) unter Beteiligung diverser anderer internationaler Einrichtungen Einheitliche Verhaltensrichtlinien für den Austausch von Handelsdaten auf dem Wege der Datenfernübertragung (UNCID) formuliert (ECE-Dokument TRADE/WP.4/R.483, s. allgemein I. Walden, CR 1994, 1), die Grundlage für den von den VN formulierten UN/EDIFACT-Standard (United Nations/Electronic Data Interchange for Administration, Commerce and Transport) geworden sind. S. dazu W. Kilian, CR 1994, 657; s. dazu allg. B. Wright, *The Law of Electronic Commerce: EDI, Fax and E-mail Technology, Proof and Liability*, 1991. Ergänzend dazu existiert ein deutscher EDI-Rahmenvertrag, der u.a. Bestimmungen über die vertraglichen Beziehungen zwischen EDI-Partnern enthält (es finden sich hier Regeln zu Zugangsfragen und Haftungsklauseln sowie eine Schiedsklausel).

²²⁷ Ähnlich auch der Rapport Falque-Pierrotin (o. Fußn. 142).

²²⁸ Auf einem informellen Treffen der zuständigen Minister Ende April 1996 in Bologna wurde die Kommission beauftragt, wegen der transnationalen Natur des Internet einen Bericht zur Frage einer möglichen Rechtsangleichung oder einer völkerrechtlichen Regelung in diesem Bereich zu erstatten (französischer Vorschlag), vgl. *L'Europa indaga su Internet*, *La Stampa* vom 26.4. 1996, S. 23, zum französischen Vorschlag auch Tortello/Lointier (o. Fußn. 30), S. 135. Die französische Regierung betont dabei die Eigentümlichkeit des Internet, die den Vergleich mit anderen Medien nicht zulässt und unterstreicht, daß es weniger um eine konzertierte Regelung auf internationaler Ebene gehen kann als um eine Verständigung auf ein Minimum an gemeinsamen Prinzipien als Ausgangspunkt für einen "code de bonne conduite". Mittlerweile hat die Kommission sich in einer Mitteilung an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß sowie den Ausschuß der Regionen zu Kriminalität und Internet geäußert (<http://www2.echo.lu/legal/en/internet/content/communic.html>). Zu Aktivitäten auf Ebene der G7 s. H. Kubicek, CR 1995, 370. Vgl. auch die G7-Erklärung von Lyon vom 29. Juni 1996, Bulletin der Bundesregierung Nr. 59, S. 644, wonach über ethische und strafrechtliche Fragen der neuen Technologien nachgedacht wird.

V. Besseres Recht durch Cyberspace?

Internet und Cyberspace beschäftigen das Recht noch immer vorwiegend reaktiv, als neue Herausforderungen und Probleme, denen sich überkommene Rechtsbereiche anpassen müssen. Übersehen wird dabei leicht, dass Cyberspace auch für das Recht selbst eine Chance bedeutet, aktiv neue Ideen zu realisieren. Hier ist nicht der Ort, detaillierte Konzepte zu entwerfen, es kann nur auf einige Ansatzpunkte hingewiesen werden. Im übrigen hängt die Entwicklung hier von der Phantasie und Gestaltungsbereitschaft (auch) der Juristen ab.

Besseres Recht durch das Internet - dies zielt in einer utopischen Variante darauf ab, dass Menschen nicht mehr zur Wahl gehen, sondern per Internet abstimmen oder sich gar unmittelbar zu einzelnen Sachfragen äußern können. Eine solche 'TED-Demokratie'²²⁹ ist kurz- oder mittelfristig nicht zu erwarten. Dass Nüchternheit sich hinsichtlich der Gestaltungskraft der neuen Technologien empfiehlt und die diese Technologien begleitenden Umstände nicht übersehen werden dürfen, wird dadurch belegt, dass die subversive Wirkung neuer Technologien auf autoritäre Staaten bisher regelmäßig überschätzt worden ist. In China haben die Machthaber es bisher verstanden, durch Meldeauflagen für Internetzugänge, kombiniert mit Zugangsbeschränkungen und Strafandrohungen, das an sich doch schwer kontrollierbare Internet unter Kontrolle zu halten: indem nicht das Internet kontrolliert wird, sondern die Nutzer²³⁰.

Bei der Frage nach dem, was heute schon an Verbesserungen realisierbar wäre, ist auszugehen von den Vorteilen, die das neue Medium aufweist: Es vermag eine große Menge an Informationen dem Einzelnen zugänglich zu machen. Es ist zudem ein interaktives und schnelles Medium. Aus diesen drei Elementen Kapazität, Velozität, Interaktivität ergibt sich als Entwurf eines Ausgangspunktes für weitere Überlegungen folgendes:

²²⁹ TED ist ein in deutschen Fernsehsendungen häufig genutztes System zur Ermittlung von Zuschauermeinungen. Dabei können die Zuschauer durch Anwählen bestimmter Telefonnummern Zustimmung oder Ablehnung zu einer Frage signalisieren.

²³⁰ Zu China s. im einzelnen Bork, Surfer an der Leine, Die Zeit v. 2.8.1996, S. 25.

1. Effizienz - Optimierung der juristischen Arbeit

Kaum ein Bereich ist dermaßen auf die Verfügbarkeit aktueller Informationen angewiesen wie der juristische: Die aktuelle Gesetzgebung, die neueste Auflage eines Lehrbuchs, die aktuelle Rechtsprechung, der jährlich neu erscheinende Kommentar.

Folgerichtig wäre es, zur Befriedigung dieses Bedarfs an aktuellen Informationen moderne Informationstechnologie einzusetzen. Ansätze dazu bestehen auch in Deutschland durchaus, etwa in Gestalt des juristischen Informationssystems JURIS, einer GmbH, die fast völlig in staatlicher Hand liegt²³¹. Allerdings hält JURIS, möglicherweise gerade wegen der staatlichen Anbindung und Monopolstellung in Deutschland, immer noch keinem Vergleich mit den miteinander konkurrierenden, kostenintensiven amerikanischen kommerziellen juristischen Datenbanken Lexis und Westlaw stand, die insbesondere alle Zugriffe, gerade auch auf Zeitschriftenbeiträge, im Volltext ermöglichen. In Frankreich ist über Minitel schon seit längerem der Zugriff auf nationale und europäische Rechtsprechung möglich, allerdings auch hier nicht kostenfrei, obwohl die Unterhaltung der Datenbanken teilweise in staatlicher Hand liegt. Beim Übergang vom Minitel-System auf das Internet scheint hier eine gewisse Bewegung in die bisher ebenfalls weitgehende Monopolisierung der existierenden Datenbanken von Gerichtsentscheidungen zu kommen²³².

Ohne den Umweg über spezielle Datenbanken ist auch der Bezug von juristischen Informationen direkt an der Quelle denkbar: Für die Rechtsprechung ist der U.S. Supreme Court vorbildlich. Dort werden Entscheidungen binnen Stunden im Volltext über das Internet verfügbar gemacht²³³.

Soweit der Rechtsstaat sich auch dadurch bestimmt, dass er effektiv und effizient ist, kann das Internet Verbesserungen im Bereich der Effizienz ermöglichen. Denkbar ist in diesem Zusammenhang etwa die Zulassung elektronischer Schriftsätze bei den Gerichten sowie allgemein im Bereich der Justizverwaltung und der Verwaltung die Umstellung auf - zunächst wohl nur innerbehördlichen - elektronischen Schriftverkehr.

In Frankreich versucht die Anwaltschaft bereits diesen Aspekt des Internet für sich zu nutzen. Der Barreau de Paris (Anwaltskammer von Paris) bietet eine Anlaufstelle für den Rechtsuchenden²³⁴ und seinen Angehörigen darüber hinaus in einem zugangsbeschränkten Netz praktische und juristische Informationen²³⁵.

²³¹ Die Frage stellt sich, weswegen dieser quasi-öffentliche Dienst nicht allgemein kostenfrei erhältlich ist, eine Frage, die sich auch für die Datenbank zur Rechtsprechung des EuGH, CELEX, stellt, die aus öffentlichen Geldern unterhalten wird. JURIS besteht seit 1985, <http://www.juris-sb.de>.

²³² Vgl. Tortello/Lointier (o. Fußn. 30), S. 194.

²³³ <http://supct.law.cornell.edu/supct/>; vgl. auch das französische Projekt 'Les grands procès sur Infonie', wo Gerichtsverhandlungen fast on-line übertragen werden. Dieser Dienst ist allerdings noch nicht über das Internet erreichbar, s. dazu Tortello/Lointier (o. Fußn. 30), S. 19 f.

²³⁴ Möglicherweise stellen sich hier neue Rechtsfragen im Hinblick auf On-line Rechtsberatung und das Werbeverbot für Anwälte. Vgl. zu dieser Frage Tortello/Lointier (o. Fußn. 30), S. 233. Auch in Deutschland dürften die zunehmend verbreiteten WWW-Homepages von Anwälten teilweise im Hinblick auf das Werbeverbot nicht unproblematisch sein.

²³⁵ Später soll hier auch eine Zusammenarbeit mit der Gerichtsorganisation erfolgen, so daß etwa Verhandlungs- und Sitzungstermine on-line verfügbar sind. S. im einzelnen Tortello/Lointier (o. Fußn. 30), S. 198 f., s. <http://www.paris.barreau.fr/>.

2. Entscheidungstransparenz

Wo immer staatliche Entscheidungsprozesse ablaufen, von den Kommunen²³⁶ über die Länder²³⁷ und den Bund bis zur Europäischen Gemeinschaft, kann das Internet helfen, diese Entscheidungsprozesse für den Einzelnen durchschaubar zu machen: durch Offenlegung der Entscheidungsträger, der Entscheidungsgrundlagen, der Entscheidungsabläufe und der Entscheidungszeiträume.

Damit sind nicht gemeint die bereits existierenden Homepages von Ministerien oder sonstigen staatlichen Institutionen auf dem World Wide Web, denen vielfach neben Fotografie und Reden des Ministers oder Behördenleiters bestenfalls ein Organigramm des Ministeriums bzw. der Institution zu entnehmen ist.

Vielmehr ist zu fragen, warum der Einzelne eigentlich nicht per Internet den Sachstand seines Bau- oder sonstigen Genehmigungsantrages erfahren können soll oder warum nicht noch am Tag der Debatte die Verhandlungen gesetzgebender Körperschaften im Internet verfügbar sind oder warum es die Bundestags-Drucksachen nicht im Volltext auf dem Internet gibt²³⁸. Die Reihe von Beispielen lässt sich fortsetzen.

Dort, wo der Staat mit dem Bürger in einen Dialog tritt, kann das interaktive Element des Internet genutzt werden: Anhörung zu Behördenentscheidungen, Rückfragen zu Anträgen und Ähnliches. Interaktive Verwaltung könnte hier gleichbedeutend werden mit bürgernahe Verwaltung, die auf die Anliegen des Einzelnen eingeht.

Drei praktische Beispiele für bereits angedachte Konzepte:

- In Frankreich ist unter dem Namen AdmiNet auf die Privatinitiative eines Ministerialbeamten aus dem Industrieministerium hin ein erster Anstoß für eine Datenbank von aktuellen Regierungsdokumenten gegeben worden. AdmiNet ist nach einem Betriebsjahr 1996 wieder eingestellt worden. Der Ansatz wird jedoch weiterverfolgt: Mit Rundschreiben vom 15. Mai 1996²³⁹ hat der Premierminister den Ministerien aufgegeben, bis zum 31. Dezember 1997 ein Internet-Angebot zu errichten, wobei diese Angebote durch eine Kommission überprüft und koordiniert werden. Begleitend dazu soll die Documentation française ein Verzeichnis der Angebote und einen Führer durch die Angebote erstellen²⁴⁰.
- Sehr weitgehend ist das unmittelbar für Teilbereiche des besonderen Verwaltungsrechts (technisches Sicherheitsrecht) interessante, von der Konzeption her jedoch allgemein für interaktive Verwaltung vorbildhafte RuleNet-Project der amerikanischen Atombehörde (Nuclear Regulatory Commission)²⁴¹, in dem versucht wurde, durch computergestützte Kommunikation die Partizipation von Betroffenen bei der eigentlichen Normsetzung zu ermöglichen.

²³⁶ S. dazu Schütz, Am virtuellen Rathaus wird mit Vehemenz gebaut, Das Parlament v. 9./16.8.1996, S. 17.

²³⁷ S. etwa für Brandenburg das Ministerium für Wissenschaft, Forschung und Kultur unter <http://fh-brandenburg.de/mwfk/>.

²³⁸ Kritisch zu den (wie beim Deutschen Bundestag) auf eine Präsentation der Institution beschränkten Angeboten des französischen Senat und der Assemblée Nationale Tortello/Lointier (o. Fußn. 30), S. 191, unter Verweis auf eine entgegengesetzte Praxis in Spanien.

²³⁹ Journal Officiel v. 19.5.1996, abgedruckt bei Tortello/Lointier (o. Fußn. 30), Anhang Nr. 6.

²⁴⁰ Zu AdmiNet und den Vorgaben des Premierministers s. Tortello/Lointier (o. Fußn. 30), S. 186 ff.

²⁴¹ <http://nssc.llnl.gov/RuleNet/>.

- Interaktive und partizipatorische Elemente des Internet nutzbar machen soll auf der Ebene der Europäischen Gemeinschaften das Lexcalibur-System, das Professor Joseph H. H. Weiler (Harvard) vorgeschlagen hat²⁴². Ziel ist hierbei, durch Information des Einzelnen über Entscheidungsabläufe auf europäischer Ebene das vielbeklagte Demokratiedefizit zu reduzieren, wobei der gesamte Entscheidungsprozess innerhalb der EG per Internet unmittelbar einsehbar gemacht wird.

²⁴² Quelle, <http://www.iue.it/AEL/EP/Lex/index.html>.

3. Ereignistransparenz

In anderen Bereichen kann die Transnationalität des Internet rechtlich verwertet werden. Erste konkrete Ansatzpunkte gibt es hier im Bereich des internationalen Schutzes der Menschenrechte²⁴³. Hier kann durch schnelle und nur schwer zu unterbindende Verbreitung von Informationen über Menschenrechtsverletzungen durch autoritäre Regime die Effizienz der solche Menschenrechtsverletzungen verfolgenden internationalen staatlichen und nicht-staatlichen Organisationen (IOs und NGOs) gesteigert werden.

²⁴³ Ich danke Herrn Prof. Dr. Bruno Simma, München, für den diesbezüglichen Hinweis.

VI. Zusammenfassung und Ausblick

Aus der zunehmenden Verbreitung computergestützter Kommunikation ergeben sich zahlreiche neuartige Rechtsprobleme. Aufgrund der besonderen Struktur des Cyberspace, wo territoriale Grenzen kaum noch Sinn machen, genügen herkömmliche Rechtsstrukturen den Erfordernissen eines Rechts des Cyberspace nicht mehr. Einfache Lösungen sind nicht in Sicht. Lösungsansätze könnten sich einmal darauf richten, Cyberspace als eigenständigen Rechtsraum zu begreifen und, davon ausgehend, die rechtliche Autonomie im Cyberspace zu fördern, im deren Rahmen sich Regeln eigenständig ausbilden könnten und die durch schiedsgerichtliche Streitschlichtungsmechanismen zu ergänzen wäre. In eine andere Richtung geht der Vorschlag, Cyberspace auch rechtlich zu internationalisieren und mit Hilfe der etablierten Instrumente einer internationalen Konvention, verbunden mit der Errichtung einer zuständigen Internationalen Organisation, rechtlich zu fassen.

Jeder Lösungsversuch in diesem Bereich ist verknüpft mit dem schwer vorhersehbaren Fortschritt der Technik. Für das Recht bietet diese technische Entwicklung jedoch durchaus auch Entwicklungs- und Verbesserungsmöglichkeiten. Fest steht jedenfalls, dass die Entwicklung in diesem Bereich nicht aufgehalten werden kann und dass die computergestützte Kommunikation Sinnbild für eine sich fundamental wandelnde, zunehmend interdependente Welt ist.

Das Recht wird sich dieser Entwicklung letztlich nicht entziehen können.