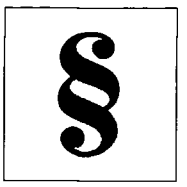


Das INTERNET: ein rechtsfreier Raum?

Rigo Wenning

"Das INTERNET: ein rechtsfreier Raum?" ist eine nicht nur im "Usenet" häufig gestellte Frage. Manche behaupten auch, daß das Internet eher eine geordnete Anarchie sei. In der Presse liest man dieser Tage sehr viel über "Internet". Die Beiträge kommen aus berufener und weniger berufener Feder. "Internet" ist eben ä la mode und in aller Munde. Aber was ist das überhaupt: "Internet" und "Usenet"? Allein die genaue Erklärung dieser beiden Begriffe wäre einen eigenen Artikel wert. In den Tageszeitungen wird Internet als "das" weltweite Computernetz bezeichnet, in dem mittlerweile über 3 Millionen Computer miteinander verbunden sind[1]. Man wird dem Phänomen "Internet" wohl eher gerecht, wenn man es als weltweite Verbindung vieler Teilnetze beschreibt. Es gibt Firmennetze, Universitätsnetze und private Anbieter[2] etc. Technisch gesehen besteht das Internet aus sogenannten Großrechnern, die über eine Standleitung miteinander verbunden sind. Um jeden Großrechner herum gibt es dann mehrere Computernetze, von denen aus der PC oder ein Unternetz bei Bedarf die Dienstleistungen aller international miteinander verbundenen Computer abfragen kann. Man unterscheidet "Clients" und "Server". Als "Server" werden solche Computer bezeichnet, die eine Dienstleistung anbieten, die man auch von einem entfernten Rechner abfragen kann. Als "Client" werden solche Computer bezeichnet, die in der Lage sind, die angebotenen Dienste abzurufen. Ein Computer kann gleichzeitig "Client" und "Server" sein. (Die Unterscheidung zwischen "Client" und "Server" hat ihre Entsprechung auf der Software-Seite.)

Am Anfang war das Pentagon ...

Die Entwicklung des Internet geht auf das amerikanische Pentagon zurück. Damals suchte man nach Wegen, die strategische Kommunikation mit den in der ganzen Welt verteilten Stützpunkten der USA zu gewährleisten. Man bediente sich dazu der Satelliten- und Telekommunikationstechnik. Kernstück ist ein an der Universität von Berkeley entwickeltes Protokoll, das es einem Computer ermöglicht, die von anderen Computern übermittelten Daten zu erkennen. Ein Protokoll ist eine Vereinbarung zwischen den Nutzern, wie Daten übertragen werden. Das Protokoll (TCP/IP) des Pentagon erwies sich als außerordentlich leistungsfähig. In den siebziger Jahren wurde die Technik dann zur zivilen Nutzung freigegeben. Die Universitäten waren mit die ersten, die über diesen neuen Weg kommunizierten. Ihnen folgten die großen internationalen Konzerne. Durch die Verbindung der Universitätsnetze mit den großen Firmennetzen von IBM & Co. entstand das, was heute als Internet bezeichnet wird. Der große Boom begann aber erst Ende der achtziger Jahre. Heute wird das Internet mehr und mehr auch von Privaten genutzt, die Dienstleistungen aller Art anbieten und nachfragen[3]. Die Welt wird kleiner und damit die Probleme der internationalen Kooperation größer. Die deutschen Behörden sind gegenüber dem ausländischen Anbieter praktisch machtlos, denn er unterliegt nicht ihrer Hoheitsgewalt; internationale Maßnahmen dauern lange.

"Usenet" – eine Teilmenge des Internet

"Usenet" ist eine thematische Teilmenge des Internet. Es bezeichnet den Teil des Netzes, der zum allgemeinen Austausch von Nachrichten und Meinungen genutzt wird, kurz *News* genannt. Hier gibt es nicht nur das Internet, sondern auch andere Netze, wie Fido, Maus, Zerberus etc.. Zum Internet gehören außerdem die Dienste World-Wide-Web (abgekürzt WWW), E-Mail, FTP und IRC. Es gibt noch weitere Dienste, wie Telnet[4] und Wais[5], auf die hier aber nicht weiter eingegangen werden soll. Diese einzelnen Dienste müssen (sehr) kurz beschrieben werden, um ihre rechtliche Dimension zu erhellen.

Assessor Rigo Wenning ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Strafrecht, Strafprozeßrecht, Kriminologie und Strafrechtsvergleichung an der Universität des Saarlandes.

---

1 Der Spiegel 20/1995 oder Online, *http://spiegel.nda.net/nda/spiegel/*. Die Zahl der verbunden Computer nimmt bis dato ständig zu und kaum jemand hat einen Überblick, wieviele Computer tatsächlich verbunden sind.

2 Die privaten Anbieter lassen sich wiederum in große und kleine Anbieter aufteilen. Das reicht von der Mailbox (z. B. Fido) bis zum internationalen Verkehr (z. B. X-Link).

3 Als private Anbieter, die auf eine breite Konsumentenschicht zielen, seien u.a. Compuserve, X-Link, Saar-Link, America-Online (aol.com) und dialup.fr genannt.

4 Mit Telnet kann man sich in entfernte Rechner einloggen. Der eigene Computer wird dann zum Terminal des entfernten Hosts.

5 Wais (*Wide area information system*) durchsucht weltweit Wais-Datenbanken nach einem bestimmten Begriff.

Die Internet-Dienste: "World Wide Web" (WWW)...

WWW ist ein Hypertextsystem, das Dateien auf entfernten Computern ansteuern kann. Dabei können Text, Bilder und Ton übertragen werden[6]. Auf dem Bildschirm wird ein farblich gekennzeichneter Textteil oder ein sensitives Bild *(clickable map)* angezeigt. Man klickt mit der Maus auf den gewünschten, farblich unterlegten Beitrag. Durch den dahinterstehenden Zeiger wird nun ein Prozeß in Gang gesetzt. Der eigene Computer verbindet sich mit dem im Zeiger angegebenen Rechner und ruft dort die gewünschte Seite auf. Dabei ist ohne explizite Angabe im Text für das geübte Auge lediglich aufgrund der (in der Statuszeile eingeblendeten) Adresse erkennbar, in welchem Land der entfernte Computer liegt[7]. Die so aufgerufene Seite enthält Eigenes und oftmals weitere Verweise auf andere entfernte Seiten. Wird von der gefundenen Seite ein weiterer Verweis gewählt, verbindet uns nicht der entfernte Rechner weiter, sondern der eigene Computer baut nun eine Verbindung zu der in der entfernten Seite angegebenen Fundstelle auf. Die Anbieter von Informationen müssen *Server* sein, der Nachfrager braucht ein Programm (hier *Browser* genannt), das die Informationen verstehen kann[8]. Diese Reise um die Welt bezeichnet man im Cyberjargon als "Surfen" des Internet.

News...

Mit News (also Nachrichten) wird eine Technik beschrieben, der das sogenannte NNTP-Protokoll zugrunde liegt[9]. Auch hier handelt es sich um eine Client-Server Architektur. Bekannt ist dieser Dienst durch die Verbindung von Mailboxen unter dem Namen BBS[10]. Am besten kann man sich diesen Dienst als weltweites "schwarzes Brett" vorstellen. Da es aber nicht nur ein interessantes Thema zu diskutieren gibt, wurden mehrere "schwarze Bretter" geschaffen. Im Deutschen heißt die Bezeichnung für eine Newsgroup denn auch "Brett". Auf dem News-Server des Rechenzentrums[11] der Universität des Saarlandes sind zur Zeit ca. 3.300 solcher "Bretter " verfügbar[12]. Der Administrator des News-Servers kann wählen, welche der von anderen News-Servern angebotenen Newsgruppen er abonniert. Der Klient hat dann die Wahl, aus diesem Angebot wiederum die ihn interessierenden Bretter auszusuchen[13]. Man kann nun die Nachrichten in der angewählten Gruppe lesen, eine Nachricht in das Brett einspeisen, oder eine dort schon vorhandene Nachricht kommentieren. Die News-Server sind untereinander verbunden und tauschen die von Klienten aufgespielten Nachrichten, je nach gewählter Verteilung, weltweit untereinander aus. Mittels News können auch Bilder übertragen werden, wenn man die Nachricht vorher durch ein bestimmtes Verfahren *(uuencode)* behandelt hat.

E-Mail...

E-Mail, die elektronische Post im Internet, bedarf eigentlich kaum noch einer Erklärung. Natürlich ist auch hier die Übertragung von Bildern und Programmen im Binärformat möglich[14]. Über Mail-Listen wird eine Verteilung ähnlich wie bei den News erreicht, allerdings ist hier der Adressatenkreis überschaubar[15].

File Transfer Protocol (FTP)...

FTP ist die Abkürzung für *File Transfer Protocol.* Das ist einer der "Urdienste" des Internet und wie TELNET als Standardbefehl im Betriebssystem UNIX enthalten. Heute gibt es diesen Dienst als Zusatzprogramme auch für fast alle anderen Betriebssysteme. FTP ermöglicht es, jede Art von Datei von einem Computer (FTP-Server) auf den eigenen Rechner zu kopieren. Dies wird vor allem zur Verteilung von Shareware-Programmen genutzt. Man findet aber auch die verschiedensten Texte, wie Gesetzestexte und Erläuterungen, FAQ (Frequently Asked Questions) genannt.

---

6 Multimedia ist ein zur Zeit vielbeschworener Begriff.

7 Es sei denn, auf der aufgerufenen Seite ist der Ort vermerkt, was immer üblicher wird.

8 Gebräuchlich sind vor allem Mosaic und Netscape, aber es gibt auch andere. Diese WWW-Klienten gibt es für viele verschiedene Betriebssysteme wie Unix, Linux, Macintosh, Windows und OS/2. Alle Programme werden als Shareware vertrieben, wobei Netscape neuerdings von dieser Linie abweicht. Erhältlich sind die Programme auf den meisten FTP-Servern: z. B. ftp.rz.uni-sb.de. Die deutsche Version der Virtual Law Library, einer Sammlung juristischer Seiten im WWW, gibt es unter http://www.jura.uni-sb.de/

9 News-Server werden deshalb auch oft als NNTP-Server bezeichnet.

10 Bulletinboard-System, was wiederum mit schwarzem Brett übersetzt werden kann.

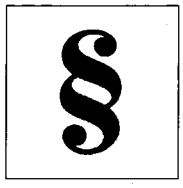
11 sie sehen schon, es gibt mehrere News-Server in Saarbrücken.

12 Wieviel Gruppen es gibt, läßt sich kaum ermitteln. Es existieren News-Server mit mehr als 4.000 verschiedenen Gruppen.

13 Der Befehl heißt "subscribe" oder "unsubscribe"

14 gebräuchlich sind die Verfahren: BinHex, MIME und uuencode-uudecode

15 oder kann zumindest überschaubar gehalten werden.



... und "Internet Relay Chat" (IRC)

IRC (Internet Relay Chat) ist eine direkte Kommunikation. Man wählt sich in den nächstgelegenen IRC-Server[16] ein und hat dort eine Liste von Gruppen[17], in denen gerade diskutiert wird. Entweder man macht eine eigene Gruppe auf, oder man beteiligt sich an einer Diskussion in einer bestehenden Gruppe. Alles was ein Teilnehmer tippt und abschickt erscheint nun auf dem Bildschirm aller anderen Teilnehmer der Gruppe. Dieser Dienst ist einer Telefonkonferenz vergleichbar. Je nach gewähltem Server ist die Verteilung unterschiedlich. Das kommt darauf an, mit welchem Teilnetz der angewählte Server verbunden ist[18].

Was alle Dienste eint und trennt

Trotz ihrer Unterschiedlichkeit haben die Dienste eines gemeinsam, sie übertragen Informationen. In einem ersten Schritt wird auf die allgemeinen Probleme des Rechts beim Übergang zur internationalen Informationsgesellschaft einzugehen sein. In einem zweiten Schritt muß dann den Besonderheiten der einzelnen Dienste Rechnung getragen werden. Gibt es bei News keinen fest umrissenen Benutzerkreis, so ist eine Mail-Liste an einen bestimmten (bestimmbaren) Personenkreis gerichtet. Kann bei IRC jeder interaktiv teilnehmen, beschränkt sich die Nutzung im WWW oftmals auf das Ansehen oder Lesen einer Seite.

Rechtliche Probleme: (Internationales) "Netlaw"? Internet-Polizei?

Im Gefolge der Internet-Euphorie sind nun einige Probleme sichtbar geworden, die mit der eigenen Qualität des Mediums zusammenhängen. Einerseits sind den Nutzern die einschlägigen Normen oft unbekannt, andererseits sind bestehende Normen durch den technischen Fortschritt anpassungsbedürftig geworden. Die Schwierigkeiten entstehen auch dadurch, daß das Internet ursprünglich nicht für kommerzielle Anwendungen konzipiert war. Wie oben schon erklärt, war das Ziel ursprünglich der für den Netzteilnehmer kostenlose und schnelle Informationsaustausch. Finanziert wurde das Gesamtnetz durch die beteiligten Netzbetreiber. Dementsprechend stößt z. B. der Austausch von Shareware bisher auf wenig Probleme[19]. Zur Zeit werden deswegen die Rufe nach einer Durchnormierung des Internet lauter[20]. Wichtig ist jedoch vor allem, daß dem internationalen Charakter des Netzes Rechnung getragen wird. Jede nationale Lösung wird zu unbefriedigenden Lösungen, oder schlimmer zu Verwerfungen im Recht führt[21]. Festzuhalten bleibt, daß Information zwar mittelbar ein enormes Bedrohungspotential haben kann, unmittelbar aber nicht zu einem Eingriff in die körperliche Unversehrtheit führt.

Strafrechlicher Schutz der Daten im Netz (?)

Ist der Bundesrepublik eine Information mißliebig, die in einem anderen Staat noch geduldet wird, so stellt sich vor allem die Frage nach der Verbreitung von Schriften i.S.d. § 11 Abs. 3 StGB. Für das BTX-Verfahren hat das OLG-Stuttgart[22] entschieden, daß ein Datenträger einem Bildträger i.S.v. § 11 Abs. 3 StGB gleichzustellen ist. In der Verbreitung via BTX liege auch ein "Zugänglichmachen" der pornographischen Inhalte des Datenträgers i.S.v. § 184 Abs. 1 Nr. 2 StGB. Beispiele für pönalisierte Informationen im Netz gibt es genug. Das geht von der Nazi-Propaganda über Information zu Drogen[23] und Pornographie[24] bis zur Anleitung zum Bau einer Bombe[25]. Oder man wählt z. B. einen Hypertext-

---

16 Für Saarbrücken ist das irc.rz.uni-karlsruhe.de

17 Die Diskussionsgruppe wird bei IRC 'channel' genannt.

18 siehe dazu die ausführlichen Erklärungen bei Corinne Villemin-Gacon, http://depinfo.u-bourgogne.fr/ADELIMI/Maitrise/villemin/IRC.html

19 Die sich hier stellende Problematik der Verteilung von Computerviren durch Shareware wird dadurch entschärft, daß man gleichzeitig Anti-Virus Programme im Netz erhält. Wer diese Anti-Virus Programme trotz Netzteilnahme nicht nutzt, muß sich zumindest den Vorwurf der Fahrlässigkeit machen lassen. Anti-Virus Programme liegen auf den meisten FTP-Servern zum kopieren bereit: z. B. ftp.rz.uni-sb.de oder ftp.mcafee.com

20 Vgl statt vieler Koch, Netlaw ante portas, NJW CoR 1995, 259, der allerdings sehr allgemein bleibt.

21 Die Forderung nach internationalen Regelungen wurde schon 1985 von Ulrich Sieber aufgestellt: De la nécessité d'une législation internationale contre la fraude informatique in Droit de l'informatique, numéro spécial, La fraude informatique, 1985, zitiert nach Devèze, Juris-Classeur pénal, Art. 462-2 ä 462-9 n 5. (Original an der Universität nicht verfügbar) Neuere Aufsätze: Der strafrechtliche Schutz der Information, ZStW 1991, 779-795; Computer Crimes and Other Crimes against Information Technology. Commentary and Preparatory Questions, Revue Internationale de droit pénal, Heft 1, 1993, 67-78.

22 OLG Stuttgart vom 27.08.1991, Az: 5 Ss 560/90, NStZ 1992, 38 (ST).

23 siehe http://www.paranoia.com/drugs/. Dieser Host informiert aber eher über Drogen.

24 Klemens Polatschek (kp@zeit.de), Finger weg vom Sauladen, in der "Zeit" vom 14. Juli 1995, der zu Recht vor einer Verfolgungshysterie auf diesem Gebiet warnt.

25 "Ich will Bomben bauen. Bringt es mir bei. – Muß Internet polizeilich überwacht werden?", Welt am Sonntag vom 28.05.1995.

Prävention?

Verweis[26] an und wird innerhalb von ca. 3 Minuten von einem Server in den USA über alle möglichen Drogen und deren Preise in verschiedenen Teilen der Welt informiert[27].
Prävention ist im Netz besonders schwierig zu bewerkstelligen, weil ein wirksamer Schutz zum Erliegen des Netzverkehrs führen würde. Die Information kann bei einer Filterung ohne weiteres aus einem anderen Land von einem anderen Server her angeboten werden, weil sich die Filterung eher auf die Herkunft als auf den Inhalt beziehen muß. Eine Filterung des Inhalts würde schon an der Masse der übertragen Information scheitern[28]. Außerdem hindert auch die Möglichkeit der Kompression und geringfügigen Änderung der Daten die reine Inhaltsanalyse. Die Information braucht nicht einmal neu geschrieben zu werden. Sie wird per FTP in Minuten einmal um die Welt transportiert und irgendwo anders aufgelegt. Den interessierten Nutzern läßt man eine Nachricht zukommen, wo die Information nun zu finden sei. Dies kann per Mail oder auch in den News geschehen[29]. Darüber hinaus ist die Verteilung mittels verschlüsselter Nachrichten nicht kontrollierbar[30].

Repression?

Auch Repression scheitert oft an der Internationalität des Datenverkehrs. Jeder Nutzer kann nun ohne große Anstrengung die nationalen Regelungen umgehen und sich die Information auf einem Server außerhalb besorgen. Eine Pönalisierung des Nutzers erscheint nicht wünschenswert. Es wäre im übrigen verfehlt, das Internet auf die Verteilung gefährlicher oder mißliebiger Information zu reduzieren.

Vertragsabschluß über das Netz? Kommerzialisierung des Internet

Rechtliche Probleme treten auch bei dem Versuch der Kommerzialisierung des Internet auf. Es werden wohl in Zukunft immer mehr Verträge über Internet geschlossen werden. Damit wird auch der private Konsument mehr und mehr international tätig. Das bedeutet, daß dem internationalen Privatrecht und den verschiedenen internationalen Abkommen zum Privatrecht eine immer größere Bedeutung zukommen wird. Der Anfang ist hier mit Schaffung des einheitlichen Wiener Kaufrechts von 1980[31] gemacht. Das Abkommen wurde bisher von ungefähr 40 Staaten ratifiziert[32]. Außerdem ist das CISG nach Art. 1 Abs. 1 lit. b auch dann anzuwenden, wenn die Regeln des internationalen Privatrechts zur Anwendung des Rechts eines Vertragsstaates führen[33]. Es ist daher eine brauchbare Grundlage für die Abwicklung des Kaufrechts im Internet. Probleme stellen sich allerdings insoweit, als im Internet oftmals immaterielle Güter verkauft werden, die auch über das Netz lieferbar sind. Mit viel Auslegungsaufwand wird daher zur Zeit versucht, Software unter den Sachbegriff *(marchandises, goods)* des CISG zu subsumieren[34]. Damit wäre zumindest das Problem der Haftung für Softwarefehler und der Software anhaftende Viren auf eine solide Grundlage gestellt[35]. Über die Vollstreckung einer solchen Entscheidung ist damit aber noch nichts gesagt.
Eine internationale Vereinheitlichung bestimmter Kernbereiche des Zivilrechts würde der zur Zeit herrschenden Unsicherheit der Netzteilnehmer über die zu befolgenden Regeln entgegenwirken und einen wichtigen psychologischen und rechtlichen Hemmschuh der

---

[26] Als Hypertext bezeichnet man Textstellen, die farblich oder sonst unterlegt sind und auf eine andere Stelle verweisen. Der versteckte Verweis kann auch auf eine andere Datei zeigen. Diese Datei kann im Internet mit Hilfe des sogenannten World-Wide-Web auch auf einem entfernten Computer in einem anderen Land liegen.

[27] Der Server heißt http://www.paranoia.com/ und liegt in den USA. Seine Spur konnte vom CIP-Raum der Juristen aus nur bis nach Texas verfolgt werden.

[28] Durch eine gutgehende Mailbox laufen täglich ca. 450 MB an Daten. Das entspricht 9 m Papier im Bücherregal oder 130.000 Seiten (Quelle: Josef Dietl, josef@greenie.muc.de). Multipliziert man dies mit der Anzahl der existierenden Mailboxen, dann ergibt das eine nicht mehr überschaubare Menge. Eine technische Aufbereitung zur Kontrolle würde das Netz in erheblichem Umfang verlangsamen.

[29] Zum Problem der anonymen Postings in den "News" weiter unten.

[30] Siehe dazu unten zur Kryptographie.

[31] Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenkauf Vom 11. April 1980, BGBl. 1989 II S. 588, im folgenden mit CISG abgekürzt. Der Text ist dreisprachig erschlossen bei http://www.jura.uni-sb.de/

[32] siehe zum Stand der Ratifikationen Claude Witz, Les premières applications jurisprudentielles du nouveau droit uniforme de la vente internationale, L.G.D.J. Paris 1995

[33] Claude Witz, L'entrée en vigueur de la Convention des Nations Unies du 11 avril 1980 sur les contrats de vente internationale de marchandises, übersetzt ins Japanische von Munehide Nisbizawa, in: "Kiorin-Shakaikagaku-Kenkyu" (Revue des Sciences Sociales de Kiorin), Tokyo 1989, Vol 5, n 2, Seite. 1 bis 10.

[34] Frank Diedrich, Autonome Auslegung von Internationalem Einheitsrecht – Computersoftware im Wiener Kaufrecht, Baden-Baden 1994 m.w.N.

[35] Matthias Brandi-Dohrn, Haftung und Gewährleistung bei EDV-Produkten, CR 1993, 473.

kommerziellen Entwicklung beseitigen. Nationale Regelungen schaffen hier eher eine weitere Verunsicherung. Dies gilt ganz besonders für Fragen des Urheberrechts. Zwar ist mit der Berner Konvention[36] eine internationale Grundlage vorhanden, diese ist aber bezüglich der durch die Technik geschaffenen Anforderungen anpassungsbedürftig geworden. Welchen urheberrechtlichen Schutz genießen beispielsweise News-Postings? Die Programme sehen bei einer Anmerkung an einen bestehenden Artikel bisher standardmäßig vor, daß die zu kommentierende Nachricht vollständig in die Anmerkung kopiert wird und dann verändert werden kann. Eine Kenntlichmachung erfolgt durch sogenanntes "quoten", d. h. jeder Zeile des anzumerkenden Artikels wird ein Zeichen, beispielsweise ">", vorangestellt. Gewisse Schwierigkeiten wird auch der Übergang von einem zum anderen Medium bereiten. Als Beispiele können die Verwendung von privaten E-Mails, von Artikeln aus dem "Usenet" und WWW-Seiten bei der Erstellung von Zeitungsartikeln durch Dritte genannt werden. Aus elektronischen Nachrichten wird wieder Papier.

Gefahren bei der "elektronischen Bezahlung" Sicherheit durch Verschlüsselungsverfahren

Es ist zwar möglich, Informationen über weite Strecken schnell zu transportieren, aber die Möglichkeiten der Bezahlung solcher Informationen hinken bis dato der Entwicklung des kommerziellen Informationsangebots hinterher[37]. Bisher wird vielfach die Nummer einer Kreditkarte verlangt. Die Leistung wird erst nach erfolgter Zahlung erbracht. Das ist jedoch ein risikoreiches Unterfangen, weil diese Nummer im Klartext über das Netz gespielt und an vielen "Gateways" mitgespeichert wird. Dabei ist die Möglichkeiten des "Mithörens" im Netz noch nicht in Betracht gezogen. Es kann außerdem keine Kontrolle darüber stattfinden, ob die Kreditkartennummer tatsächlich von dem Eigner der Kreditkarte kommt, denn es gibt weder eine sichere Adresse noch eine Identitätsfeststellung. Schließlich und endlich kann sich der Karteninhaber auch nicht der ordnungsgemäßen Verwendung seiner Kartennummer sicher sein, weil er seinen Vertragspartner nicht kennt und auch nicht eindeutig identifizieren kann.

Ein Professor im virtuellen Dialog mit sich selbst

Zwar hat jeder Internet-Teilnehmer eine eigene Adresse[38]. Die Adresse ist jedoch nicht vor Manipulationen geschützt. Prof. Dr. Buchmann[39] erzählte auf dem EDV-Gerichtstag 1995 von einer lustigen Internet-Diskussion in den News. Man konnte eine Nachricht eines bekannten amerikanischen Professors lesen, die seiner bisherigen Meinung diametral entgegenstand. Der gleiche Professor dementierte kurz darauf diese Nachricht und verwickelte sich anschließend in eine heftige Diskussion mit sich selbst. Dahinter standen einige Studenten, die dem System vorspiegelten, eben jener Professor zu sein. Sie veröffentlichten Nachrichten in den News unter seinem Namen.

(P)retty (G)ood (P)rivacy

Eine eindeutige Identifizierung ist im Internet nur mit kryptographischen Public-Key Verfahren ä la PGP[40] möglich. Die Bedeutung dieser Technik wurde auch im Report der "Gruppe" der europäischen Kommission anerkannt[41]. Dem amerikanischen Professor wäre die "Selbsterfahrung" erspart geblieben, wenn der News-Server nur unterzeichnete Nachrichten angenommen hätte. Das Verfahren dazu verläuft wie folgt: Bei Public-Key Verfahren wird ein privater und ein öffentlicher Schlüssel erzeugt[42]. Mit dem privaten Schlüssel kann unser Professor nun die Nachricht unterschreiben. Nur wenn die Unterschrift sich mit seinem öffentlichen Schlüssel entschlüsseln läßt, ist man sicher, daß die

---

36 Berner Übereinkunft vom 09. September 1886, in Deutschland gültig in der Pariser Fassung vom 24.07.1971, BGBl. 1973 II, S. 1069. Siehe dazu das Buch Daniel Remer and Robert Dunaway, Legal Care for Your SOFTWARE, A Step-by-Step Legal Guide for Computer Software Writers, Programmers and Publishers, http://www.island.com/LegalCare/ Genaue Fundstelle: http://www.island.com/LegalCare/Chapter13/Chapter13.html#RTFToC22

37 siehe dazu den Bangemann-Report einer Gruppe der Europäischen Kommission auf Anfrage des Rates: http://www.earn.net/EC/bangemann.html

38 Damit ist nicht notwendig seine E-Mail Adresse gemeint, sondern die IP-Nummer seines Rechners. Sobald der Teilnehmer aber aufgrund einer öffentlichen Kennung (z. B. bei aol.com oder dialup.fr von Minitel aus) eine Maschine nur zeitweilig nutzt, ist diese Adresse wertlos.

39 Buchmann ist Professor für Informatik an der Universität des Saarlandes und beschäftigt sich vorwiegend mit Kryptografie.

40 Pretty Good Privacy von Phil Zimmerman. Es gibt wegen des Exportverbots in den USA (dazu unten) eine amerikanische und eine europäische Version. Die europäische Version findet man auf der europäischen PGP-Homepage in Norwegen: http://www.ifi.uio.no/~staalesc/PGP/home.html

41 siehe Bangemann-Report a.a.O. Fußnote 37

42 Deswegen nennt man diese Verfahren auch asysmetrische Verschlüsselungsverfahren.

Nachricht wirklich von unserm werten Professor ist[43]. Ein Provider kann die Versendung der Nachricht nun von dieser Prüfung anhand einer Datenbank mit öffentlichen Schlüsseln abhängig machen. Wenn die Unterschrift nicht stimmt, wird die Nachricht nicht versandt. Diese Technik würde es auch erlauben, jemanden eindeutig als Urheber z. B. eines Vertragsangebots oder einer Annahme zu identifizieren, denn nur diese Person konnte mit ihrem privaten Schlüssel die Nachricht so generieren, daß sie mit dem öffentlichen Schlüssel dechiffriert werden kann[44]. Public-Key Verfahren werden inzwischen von Banken des Internet genutzt[45]. Auch die "normalen" Banken planen eine Sicherung ihrer Telebanking-Angebote mit Hilfe der asymmetrischen Kryptografie[46]. Legt jemand fahrlässig (oder grob fahrlässig) seinen privaten Schlüssel offen, dann sollte er dafür haften. Das ist im Prinzip nichts Neues, denn die Banken haben in ihren AGB die Haftung des Benutzers bei grob fahrlässigem Umgang mit Euroschecks und EC-Karte schon eingeführt[47]. Schon heute haftet derjenige, der seine PIN auf die EC-Karte schreibt[48]. Die Möglichkeiten des Verfahrens werden auch zivilprozessual eine erhebliche Bedeutung erlangen und zu größerer Sicherheit als das gängige Fax-System führen[49]. Gleichzeitig wird sich die Geschwindigkeit der Informationsübertragung erhöhen. Ob das aber zu einem schnelleren Prozeßverlauf führt, bleibt abzuwarten.

"Electronic Data Interchange" (EDI) im Geschäftsverkehr

Eine ebenfalls mit dem Internet zu noch brennenderer Aktualität gelangte Frage ist der Austausch von Geschäftsinformationen, auch unter dem Stichwort EDI[50] bekannt. Als Beispiel mag folgendes dienen: Weil Lagerkapazität Geld kostet, wird in der Industrie immer mehr auf Just-in-Time Zulieferung umgestellt. Teilweise werden heute schon bei Bedarf Nachbestellungen automatisch vom Computer des Produzenten an den Computer des Zulieferers übersandt. Diese Technik spart Geld, Zeit und Personal. Problematisch wird es jedoch, wenn Fehler auftreten. Die CCI, die *Chambre de Commerce International* in Paris hat deshalb einen Mustervertrag zu den EDI erstellt[51]. Nach dem Erfolg dieses Musters in der Praxis arbeitet nun auch UNCITRAL an einem entsprechenden Regelwerk, das dann nicht mehr gesondert vereinbart werden müßte[52].

Der Vorteil eines Transports der Daten über das Internet liegt in der Art der Abrechnung. Es wird üblicherweise nicht die Zeit der Kommunikation, sondern die anfallende Datenmenge berechnet. Ein weiteres Plus liegt darin, daß der kommerzielle Nutzer sich nicht um die Leitungen kümmern muß. Das ist Sache des Providers. Wird der Austausch von Daten so intensiv, daß sich eine eigene Standleitung rechnet, kann man das Internet wieder verlassen, oder die Leitung bei geringer Auslastung anderen zur Verfügung stellen. Benutzt man

---

43 zum Public-Key Verfahren siehe http://draco.centerline.com:8080/~franl/crypto/ und in deutscher Sprache: http://www.thur.de/ulf/krypto/;http://www.owl.de/pgp-friends.html

44 siehe zu dieser Problemstellung Rüßmann in seinem Beitrag zur Tagung "Moderne Elektroniktechnologie und Informationsbeschaffung im Zivilprozeß, Jahrestagung der Wissenschaftlichen Vereinigung für Internationales Verfahrensrecht e.V. vom 5.-8.04.1995 in Rostock" *(vgl. jur-pc 7/1995, S. 3212–3222)*; Alexander Roßnagel, Digitale Signaturen im Rechtsverkehr, NJW-CoR 1994, 96.

45 Genannt sei nur DigiCash, http://digicash.com/, das neuerdings auch eine niederländische Filiale hat (http://digicash.support.nl/). Die Bank arbeitet mit Public Key Verfahren;
siehe http://digicash.support.nl/ecash/about.html:
Ecash and security
When using ecash, your cash flows to it's destination over the Internet (or any other computer network). The open architecture of the Internet requires security measures to be taken against attempts by unfriendly third parties to intercept the digital money. Ecash provides the highest security possible by applying public key digital signature techniques. Additional security features of ecash include the protection of ecash withdrawals from your account with a password that is only known to you; not even to your bank.

46 Ekkehart Löhmann, Die elektronische Signatur in Kreditinstituten, Betriebswirtschaftliche Blätter 6/95.

47 Christof Harbeke vom Deutschen Sparkassen- und Giroverband, Neue Bedingungen für die Verwendung der ec-Karte, ZIP 1995, 250–255.

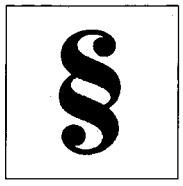
48 Schöne Beispiele bei Werner Paul, Hackerreport, NJW CoR 1995, 272 :-)

49 Mit Fax-System ist hier die aktuelle Methode gemeint, erst ein Fax zu schicken und den gleichen Schriftsatz später per "gelber" Post nachzureichen. Verwiesen sei hier auf Jörg W. Britz, wissenschaftlicher Mitarbeiter am Lehrstuhl Prof. Dr. Rüßmann, Universität des Saarlandes, der an einer Dissertation mit dem Arbeitstitel "Prozeßrechtlich Probleme der elektronischen Dokumentation und Telekommunikation" arbeitet. Siehe auch Rüßmann, Moderne Elektroniktechnologie und Informationsbeschaffung im Zivilprozeß, a.a.O (Fußnote 44).

50 *Electronic Data Interchange*

51 Ian Walden, EDI-Austauschvereinbarungen, CR 1994, 1.

52 Gregor Heinrich, UNCITRAL und EDI-Einheitsrecht, CR 1994, 118.



aber das Internet, dann stellen sich die teilweise oben schon erwähnten Sicherheitsprobleme aufgrund der mangelnden Identifikationsmöglichkeit. Hinzu kommen jetzt natürlich noch Industriespionage und Sabotageakte. Das erfordert nicht nur ein ausreichendes Sicherheitsmanagement am eigenen Host, sondern auch Sicherheit bei der Übertragung. Der deutsche Gesetzgeber geht scheinbar von der Notwendigkeit einer verschlüsselten Übersendung aus, wenn er in § 202a StGB nur die Daten schützt, die besonders gegen unberechtigten Zugang gesichert sind[53].

Verschlüsselung im Internet: Die Lage in Deutschland ...

Die Wichtigkeit und Nützlichkeit von kryptographischen Methoden ist nach alledem evident. Doch die Medaille hat zwei Seiten, denn die Verschlüsselung mit Hilfe des RSA-Algorithmus ist so sicher, daß auch ein für die Strafverfolgung wichtiges Abhören von Kommunikation nur sehr schwer möglich ist. Als einzige Möglichkeit verbleibt ein Lauschangriff auf den Computer des Täters, um so den Schlüssel zu erfahren. Durch die Fernmeldeüberwachungsverordnung[54] hat die Bundesregierung versucht, der Verschlüsselungstechnik im Bereich des Mobilfunks Herr zu werden. Im deutschen Internet regt sich allerdings Widerstand gegen diese Regelung, wenn sie denn auf das Netz und seine Mailboxen anwendbar wäre[55]. Da nach einer Entscheidung des BVerfG[56] der Begriff der Fernmeldeanlage nicht nur die bei der Entstehung des Fernmeldeanlagengesetzes bekannten Arten der Nachrichtenübertragung umfaßt, sondern auch neuartige Übertragungstechniken, sofern es sich um körperlose Übertragung von Nachrichten in der Weise handelt, daß diese am Empfangsort "wiedergegeben" werden, gehört zum "Fernmeldewesen" auch die digitale Nachrichtenübertragung. § 1 FÜV beschränkt den Anwendungsbereich auf Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind. Nur wenn der Nachrichtenaustausch im Internet nicht öffentlich wäre, würde die Verordnung nicht anwendbar sein. Festmachen könnte man dies an der Notwendigkeit einer Zugangskennung für Computer, die am Internet teilnehmen. Dies würde jedoch beispielsweise dem öffentlichen Charakter von News und Anonymous-FTP[57] widersprechen.

Die genaue Umsetzung der Verordnung im Internet steht vor vielen ungelösten Problemen. Wie soll der Betreiber einer Fernmeldeanlage, also im Internet der Service-Provider, die Verordnung umsetzen? Er ist dazu außerstande, denn er kann die Möglichkeit zum Abhören an seinen Schnittstellen nicht gewährleisten. Wie will ein Provider verhindern, daß die Nutzer kryptographische Verfahren verwenden? Soll er nur noch Nachrichten weiterleiten, die unverschlüsselt sind? Das letztere erscheint bei der Masse der übertragenen Information undurchführbar, weil der Provider erst abgrenzen müßte, ob es sich um eine verschlüsselte Nachricht oder die Übertragung einer binären Programm- oder Bilddatei handelt. Und was passiert eigentlich, wenn der Provider die in der FÜV geforderte Schnittstelle aus den oben genannten Gründen nicht zur Verfügung stellen kann? Darf er dann seine Dienste nicht mehr anbieten? Wenn dem so wäre, müßte die Regierung wohl alle Universitätszentralrechner vom Netz nehmen. Man sieht, daß die FÜV an der Realität des Internet vorbeigeht. Die wirklich anstehenden Fragen werden durch die FÜV nicht beantwortet. Ein Interessenausgleich mit dem in Art. 10 GG ausgedrückten Bedürfnis nach Privatsphäre wurde nicht herbeigeführt. Es scheint, als sei sich der Verordnungsgeber der enormen Auswirkungen einer solchen Regelung auf das Netz nicht bewußt gewesen. Die Problematik des Eingriffs in die Privatsphäre wird das BVerfG in diesem Zusammenhang wohl noch öfter beschäftigen[58].

... in den USA

Auch international sind die kryptographischen Verfahren nicht unumstritten. In Amerika gilt kryptographische Software als "Munition" und unterliegt strengen Exportbeschrän-

---

53 Jung in Nomos-Kommentar zum StGB, § 202a Rn. 6; Dreher/Tröndle § 202a StGB Rn. 7a.

54 Verordnung über die technische Umsetzung von Überwachungsmaßnahmen des Fernmeldeverkehrs in Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind (Fernmeldeverkehr-Überwachungs-Verordnung-FÜV) vom 18. Mai 1995 (BGBl. I S. 722); dazu Dirk Fox, Hört ab die Signale, c't 7/95: Lauschangriff.

55 siehe dazu Ulf Moeller, http://www.thur.de/ulf/ m.w.N.

56 BVerfG, BVerfGE 46, 120–160 = DB 1978, 92–92 = NJW 1978, 313–317.

57 Als 'Anonymous-FTP' wird die Möglichkeit bezeichnet, sich anonym auf einen FTP-Server einzuloggen, der beispielsweise Shareware enthält. Die Netiquette verlangt, daß der Nutzer FTP oder "anonymous" als Login-Name und seine eigene E-Mail Adresse als Paßwort benutzt.

58 Siehe zu insbesondere den Beschluß vom 5. Juli 1995 – 1 BvR 2226/94, http://www.jura.uni-sb.de/Entscheidungen/BVerfG.html.

kungen nach ITAR[59]. Dies gilt auch für Software, die Schnittstellen für Verschlüsselungssoftware enthält. Zur Zeit wehrt sich die "Netzgemeinde" gegen den "Decency act"[60], der die Benutzung von kryptographischer Software innerhalb der USA reglementieren soll[61]. Erste Erfolge wurden bereits erzielt. Der Senat hat den Gesetzentwurf vorerst fallen gelassen.

... in Frankreich

In Frankreich ist Verschlüsselung durch das Gesetz 90-1170 vom 29.12.1990 de facto verboten[62]. Zwar kann man sich die Verschlüsselung nach vorheriger Hinterlegung des Schlüssel von der DISSI[63] genehmigen lassen, diese Genehmigung ist aber nach geltender Praxis nur großen Unternehmen und Banken vorbehalten[64]. Zur Authentifizierung dürfen kryptographische Verfahren nach vorheriger Anmeldung benutzt werden[65]. Das hat teilweise erstaunliche Auswirkungen. So werden Textverarbeitungsprogramme wie WordPerfect ohne den normalerweise enthaltenen Paßwortschutz für Textdateien geliefert, weil mit dieser Option die Datei verschlüsselt wird. Nutzer dürften theoretisch in Frankreich die Version 1.1N des Netscape WWW-Browser nicht benutzen, weil er die Übertragung von verschlüsselter Information erlaubt. Erkennbar ist die Verschlüsselung bei Netscape[66] nur daran, daß in der Statuszeile der normalerweise getrennte Schlüssel zusammenwächst.

... und anderswo

Die Liste ließe sich noch verlängern. In den Niederlanden ist ein entsprechender Gesetzentwurf nach massiven Protesten gescheitert[67]. Ein Ausgleich zwischen diesen widerstreitenden Interessen, dem kommerziellen Nutzen und dem Recht auf Privatsphäre einerseits und der Schwierigkeit der Strafverfolgung andererseits, ist bisher nicht gefunden. In Deutschland steht dieser Konflikt noch bevor. Es kann jedenfalls nicht als glücklich erachtet werden, wenn eine Reglementierung für das Netz sozusagen durch die Hintertür via FÜV eingeführt worden wäre, ohne eine vorangegangene politische Diskussion, in der die Vertreter der verschiedenen Interessen ausreichend zu Wort kommen können.

Spezielle Probleme: Die News

Bei den spezielleren Problemen soll zuerst auf die News eingegangen werden. Der provozierende Titel dieses Aufsatzes gibt die Überschrift einer im Februar diesen Jahres geführten Diskussion in den News[68] wieder. Wenn es international, also kompliziert wird, verweigern nicht nur Nicht-Juristen die Gefolgschaft. Deshalb wurde oft die Frage gestellt, welche Auswirkungen eine Nachricht hat, die weltweit verteilt wird. Müsse man sich nun *weltweit* an *alle* Gesetze halten? Es müsse doch entsprechende Regeln geben oder gebe es eine Anarchie im "Usenet"[69]? Wie weit reicht das deutsche Strafrecht für "Postings" zweifelhafter Qualität aus dem Ausland? In den News stellen sich hauptsächlich rechtliche Fragen, die im Zusammenhang mit schlechter Kinderstube stehen. Das sind vor allem die Straftaten des vierzehnten Abschnittes des StGB, also die Beleidigungsdelikte. Hier wird auch das Zivilrecht im Zusammenhang mit Unterlassungs- und Schadensersatzklagen wegen der Verletzung des Persönlichkeitsrechts relevant. Alle anderen Informationsdelikte sind, wenn auch in geringerem Ausmaß, ebenfalls zu finden.

---

59 Ulf Moeller, http://www.thur.de/ulf/krypto/verbot.html International Traffic in Arms Regulations (ITAR), zu finden unter URL: http://dcs.ex.ac.uk/~aba/itar.html siehe dazu auch die eingehende Beschreibung des bisherigen Streitstandes unter: http://www.cygnus.eom/~gnu/export.html und http://www.eff.org/pub/Privacy/ITAR_export/HTML/

60 zu finden unter : http://www.eff.org/pub/Censorship/Comm_Decency_Act/

61 siehe dazu Online den Kampf der EFF (Electronic Frontier Foundation), http://www.eff.org/ mit den neuesten Meldungen zu diesem Thema.

62 das Gesetz findet man unter URL: http://www.ens.fr/dmi/equipes_dmi/grecc/loi.html, ebenso das dazugehörige Ausführungsdecret (décret d'application) vom Dezember 1992. Anmerkung von Stephan Bortzmeyer, http://www.cnam.fr/Network/Crypto/

63 La Délégation Interministérielle pour la Sécurité des Systèmes d'Information (DISSI)

64 Siehe dazu Stephan Bortzmeyer, http://www.cnam.fr/Network/Crypto/

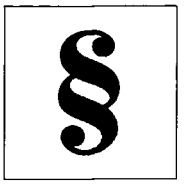
65 Ulf Moeller, http://www.thur.de/ulf/krypto/verbot.html; Stephan Bortzmeyer, http://www.cnam.fr/Network/Crypto/

66 In der Version für Windows, für die Puristen. Die Unix/Linux Version gibt beim Öffnen einen Hinweis auf die Verwendung von Kryptographie.

67 dokumentiert in http://www.xs4all.nl/~db.nl/english/Legal.html

68 Die Diskussion wurde in de.soc.recht geführt.

69 Fragen, die bei einer Diskussion "News – ein rechtsfreier Raum?" in de.soc.recht aufgetaucht sind. An dieser Stelle möchte ich alle erwähnen, deren Beiträge aus dem "Usenet" hier miteingeflossen sind. Es wären allerdings zu viele. So verweise ich pauschal auf die Gruppen de.soc.recht, de.comp.security, misc.legal.computing, misc.legal.moderated, fr.misc.droit, fr.network.internet etc.



Scientology vs. Parts of the Internet

Einige interessante Probleme sind im Zusammenhang des Streites der Scientology-Sekte mit einem Teil der Internet-Gemeinde aufgetaucht[70]. Scientology-Gegner hatten im Brett *alt.religion.scientology* gegen eben jene Sekte gewettert. Die Sekte nutzte nun eine Option des NNTP-Protokolls, um diese Nachricht weltweit zu löschen. Man nennt diese Technik Cancel-Messages. Der zu löschenden Nachricht wird eine zweite Nachricht hinterhergesandt, die die Identifikationsnummer der ersten Nachricht und den Befehl enthält, die erste Nachricht zu löschen. Man hat also die Chance, die ursprüngliche Nachricht noch zu erhalten, wenn man sie abruft, bevor die Cancel-Message den eigenen News-Server erreicht. In Deutschland dürfte diese Art der Selbstjustiz nach § 303a StGB strafbar sein[71]. Es wurde verschiedentlich andiskutiert, daß das 'Canceln' durch Notwehr gerechtfertigt sein könnte. Dem ist jedoch entgegenzuhalten, daß es dem Angegriffenen freisteht (nach Maßgabe der Verhältnismäßigkeit) wiederum eine eigene Anmerkung an die beleidigende Nachricht anzuhängen, die dann von den Interessierten gelesen werden kann. Bisher ungeklärt und für die Strafverfolgungsbehörden auch wahrscheinlich nicht zu bewältigen ist allerdings das Problem systematischer Löschungen vom Ausland aus. Das Problem könnte vielleicht technisch gelöst werden, indem man den Befehl zum automatischen Löschen auf dem News-Server sperrt. Hier ist jedoch noch viel Überzeugungsarbeit zu leisten.

Anonymes "Posten"

Ein weiteres Problem betrifft das anonyme "Posten" von Nachrichten in die News-Bretter. Es gibt in Finnland eine praktische Einrichtung mit Namen *anon.penet.fi*[72]. Nachrichten, die man per E-Mail dorthin schickt, werden mittels einer Nummer so anonymisiert, daß der Absender nicht mehr erkennbar ist. Anschließend wird die anonyme Nachricht in das gewünschte Brett der News weitergeleitet. Diese Technik wird vor allem bei Diskussionen mit sexuellem Inhalt benutzt[73]. Die Nützlichkeit und Erforderlichkeit der Anonymisierung ist in der "Netz-Gemeinde" fast durchgehend anerkannt[74]. Auch hier ist die virtuelle Welt durch Scientology sensibilisiert worden. Im Kampf der Scientology-Sekte gegen die Internet-Gemeinde[75] hatte ein Amerikaner namens Dennis Ehrlich Auszüge aus Büchern der Sekte als Beweis für die fragwürdigen Methoden der Sekte in die News gepostet. Mitglieder der Sekte klagten daraufhin wegen Verletzung des Urheberrechts. Mit Hilfe von Interpol und der finnischen Polizei wurde die Wohnung des Betreibers[76] von *anon.penet.fi* durchsucht. Julf Helsingius konnte die Polizei davon überzeugen, nur den einen Datensatz mitzunehmen und nur dessen Identität aufzudecken[77]. Dennoch dürfte das Vertrauen in

---

70 siehe zu den bisherigen Ereignissen: http://www.cybercom.net/~rnewman/scientology/home.html

71 § 303a StGB ist jedoch nach § 303c StGB nur ein Antragsdelikt.

72 näheres in Der Spiegel 20/1995 oder Online, http://spiegel.nda.net/nda/spiegel/

73 Man findet häufig anonyme Postings beispielsweise in de.talk.sex und ähnlichen Gruppen.

74 Diese Einsicht wurde aus einer Diskussion in fr.network.divers gewonnen. Die Archive dieser Gruppe können unter der URL http://www.loria.fr/news/ eingesehen werden.

75 siehe dazu Ron Newman, http://www.cybercom.net/~rnewman/scientology/home.html

76 Julf Helsingius, E-Mail: admin@anon.penet.fi

77 Die Originalnachricht (ohne Header) von Julf Helsingius lautete:
Organization: Anonymous contact service
Reply-To: an0@anon.penet.fi
Date: Sat, 18 Feb 1995 12:03:58 UTC
Subject: Anon.penet.fi compromised!
I am pretty shocked! Based on a request from Interpol, the Finnish police have gotten a search&seizure warrant on my home and the anon.penet.fi server, and gotten the real mail address of a user that has allegedly posted material stolen from the Church of Scientology. Fortunately I managed to prevent them from getting more than this one, single address.
There is going to be a very high-level public debate on how it is possible that a country that prides itself on honoring human rights and privacy very strongly has allowed this to happen. Maybe we can use the publicity to stop this from happening again.
*But in this situation, I find it pretty understandable that some of you might want all traces of your ID removed. I have now added the alias "remove@anon.penet.fi" to my server. If you want to be removed, just send a (possibly empty) message to that address. But I am hoping it won't be empty. I am hoping that you do outline *why* you have needed the server, and what you think about the actions of the Finnish authorities.*
*The messages will be anonymized using the normal anon.penet.fi procedure, and used to support the demand for a re-interpretation of the privacy laws in Finland. If you *don't* want to be removed, but still want to send a comment, you can use the addresses anon-support@lists.otol.fi (if you are 'for* keeping the server) and anon-against@lists.otol.fi (if you are *against* the server). If you want to be anonymous, use anon-support@anon.penet.fi and anon-against@anon.penet.fi.*
Julf (admin@anon.penet.fi)

diese Institution gesunken sein. Es bleibt aufzuklären, in welchen Fällen die Anonymität aufgehoben werden soll. Die Diskussion darüber findet in Deutschland bisher nur unter magerer Beteiligung der Juristen statt. Hier wäre eine Regelung, die natürlich keinen Einfluß auf Finnland haben kann, in Zukunft wünschenswert. Vorstellbar wäre eine Norm, die die Identitätsfeststellung an eine gewisse Schwere der Rechtsverletzung knüpft und die Entscheidung darüber dem Richter überträgt.

E-Mail: "Mail-Bomben"

Bei E-Mail stellt sich außer dem oben schon allgemein zur Verschlüsselung Gesagten das Problem der sogenannten "Mail-Bomben". Ein unliebsamer Zeitgenosse wird im Internet für eine ganze Weile dadurch mundtot gemacht, daß man ihm eine sehr sehr große Mail schickt (oder viele kleine). Dadurch wird seine Leitung zum Internet hin blockiert und er kann sich eine gewisse Zeit lang nicht mehr an Diskussionen beteiligen. Man bezeichnet Mail-Bomben auch als XI1-Bomben, weil der Source Code des Unix-Programms XI1 (R5) (ca. 60 MB) als Bombe recht beliebt war. Heute sind vielfach technische Schutzmaßnahmen getroffen.

WWW: Urheberrechtliche Fragen

Im WWW stellen sich hauptsächlich urheberrechtliche Fragen. Vor allem in den USA wurde die Frage aufgeworfen, ob ein Verweis im eigenen WWW-Dokument auf einen Host, der Raubkopien enthält, selbst eine Verletzung des Copyright darstellt[78]. Im deutschen Urheberrecht ist eine solche Ausweitung der Haftung jedoch nicht zu befürchten, weil nur eine Teilnahme an der Urheberrechtsverletzung zu einer Haftung des Teilnehmers führt. Allein der Verweis auf die Urheberrechtsverletzung eines anderen wird jedoch im deutschen Recht nicht als Teilnahme gesehen. Darüber hinaus wird im WWW die internationale Dimension des Internet besonders deutlich, denn die Verfolgung eines bestimmten Themas führt oft zu einer (elektronischen) Reise um die Welt.

Fazit

Abschließend läßt sich anmerken, daß viele Probleme unter Anwendung des geltenden Rechts lösbar sind. Eine Gesetzesflut wäre verfehlt und würde nur die Prosperität des Netzes hemmen. Probleme bereitet vor allem die internationale Dimension des Datenaustausches. Dem ist jedoch mit nationalen Lösungen nicht Herr zu werden. Gefragt ist vielmehr eine internationale Kooperation aller Staaten, die am Internet teilnehmen[79] oder teilnehmen wollen. Die "Internet-Gemeinde" hat es ihnen schon vorgemacht und verschiedene Regelwerke, genannt "Netiquette", entworfen, auf deren Einhaltung man immer wieder hingewiesen wird.

To find out more about the anon service, send mail to help@anon.penet.fi. Due to the double-blind, any mail replies to this message will be anonymized, and an anonymous id will be allocated automatically. You have been warned. Please report any problems, inappropriate use etc. to admin@anon.penet.fi.

78 Die Diskussion fand im April 1995 in den News in der Gruppe misc.legal.computing statt. Siehe auch Michael M. Lean, Queensland University of Technology, Copyright and the World Wide Web, http://www.scu.edu.au/ausweb95/papers/future/lean/ Die Endung ".au" macht deutlich, daß diese Seite aus Australien kommt.

79 eine sehr gute Übersicht der Topologie des Internet findet man auf dem WWW-Server der Rolling Stones, http://stones.com/imgs/mbone-topology.gif