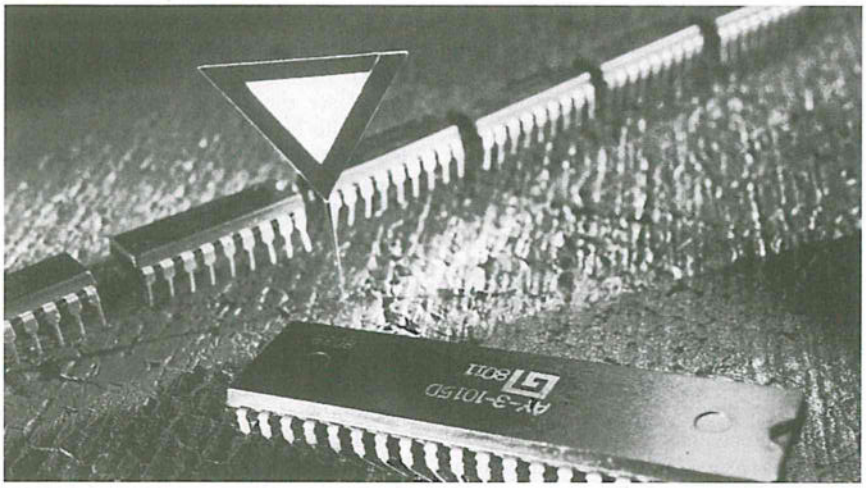

Spielwiese Internet – brauchen wir den Rasenmäher?

Jürgen Dierlamm

Was dürfen Nutzerinnen und Nutzer des globalen Internets[1] der restlichen Netzwelt mitteilen? Kann man die Veröffentlichung einer Meinung im Internet verbieten oder aber denjenigen zur Verantwortung ziehen, der die Möglichkeit schafft, dort Meinungen zu äußern bzw. abzulegen? Darf der Staat auf dieser „Spielwiese der freien Meinungsäußerung" mit Zensur[2] oder Verboten arbeiten und so den „Rasenmäher" einsetzen und die Schicht des „extremen Wuchers" einfach kappen?

Als Regel für die Benutzung des Internets diente seit Beginn des Austausches von Meinungen über dieses Medium die sogenannte „Netiquette". Sie ist als freiwillige Selbstkontrolle, als „Spielregel" verwendbar, juristisch aber als Rechtsquelle nicht zu verwenden. Fast jeder WWW-Universitätsserver verweist auf die Netiquette[3], jeder Provider schafft solche Regeln, die privaten meist in Form von Allgemeinen Geschäftsbedingungen (AGB). Hier wird vor der Nutzung klargestellt, wann und bei welchen Verstößen eine Sperrung des Zugangs erfolgt. Wer sich mit einem Modem und dem Vertrag eines Providers versorgt hat, kann seine Meinung in der Netzwelt verbreiten. Strafrechtlich verantwortlich dafür ist er selbst. Aber der Provider, der die Meinungskundgabe ermöglicht, schafft ja erst die Gelegenheit zu Straftaten – was ihm nebenbei auch noch Geld einbringt. Daher ist er auch für die Verbreitung von Meinungen verantwortlich.[4] Die Ängste der Provider vor strafrechtlich Relevantem im Bereich ihres Angebots sind berechtigt: Zwar kann meist leicht festgestellt werden, wer den betreffenden Text abgelegt hat. Die User, die einen Zugriff besitzen, müssen sich bei der Nutzung von News-Seiten mit einer E-Mail-Adresse ausweisen, und die Anbieter von WWW-Seiten können solche auch nur gegen entsprechende Rückversicherung abgeben. Allerdings kann E-Mail über einige Provider trotzdem anonym versendet werden.

Pornographie und Rechtsradikalismus

Weiterhin ist denkbar, sich bei einem Provider unter einer falschen Identität einen Zugang zu besorgen, solange die „normale" Post irgendeinen Briefkasten findet und die Rechnungen für den Dienst bezahlt werden. Ebenfalls kann man Internet-Programme, die E-Mail oder News versenden, über die wahre Identität täuschen, wie dies auch bei der Kopfzeile von Fax-Geräten möglich ist, oder aber öffentlich zugängliche PCs nutzen.

Der wichtigste Aufhänger für Strafverfolgungsbehörden waren bislang komprimiert in News-Servern hinterlegte Fotos, die in einschlägigen Newsgroups zu finden waren. Die Fotos sind komprimiert, damit die spezielle Architektur der Datenübertragung im Internet sie nicht zerstören kann. Dann werden sie sie in Gruppen mit eindeutigen Namen wie etwa *alt.binaries.pictures.erotica.female* abgelegt. Strafrechtlich belangt werden müßten hier an erster Stelle die Verwalter der *alt*-Gruppen in den USA, und nicht etwa deutsche Provider, die nur weiterschalten.

Die Diskussion startete in Deutschland erst so richtig, als private Internet-Provider anfingen, die News-Seiten aus Amerika oder Deutschland anzubieten. Als die Firma Compuserve in Deutschland Fuß faßte, wurde auch das Usenet den zahlenden Kunden eröffnet. Da vorher keine Beschränkungen stattfanden, waren alle News-Foren lesbar, auch die mit eindeutig pornographischem Inhalt. Ähnliche Ermittlungsverfahren gegen die Deutsche Telekom AG („T-Online") und gegen America Online folgten, wobei z. T. auch die Verbreitung rechtsradikaler Propaganda Anlaß für das Tätigwerden der Staatsanwaltschaften war, wie Anfang 1996 wegen der WWW-Seiten des Neonazis Ernst Zündel.

Im Mittelpunkt der strafrechtspolitischen Diskussion steht die strafrechtliche Verantwortlichkeit der Internet-Provider.[5] Dabei wird bislang entweder eine strenge Verfolgung gefordert oder aber gar keine Handhabe gesehen, gegen die Provider vorzugehen. Beides stimmt so aber nicht.

Nach § 131 Strafgesetzbuch (StGB) ist die Verherrlichung oder Verharmlosung von Gewalt oder der Aufruf zum Rassenhaß strafbar. Gemäß § 86 StGB ist die Verbreitung von Propagandamitteln verfassungswidriger Organisationen verboten. Der § 184 StGB sieht vor, denjenigen zu bestrafen, der porno-

graphische Darstellungen, insbesondere solche mit Kindern, verbreitet oder zugänglich macht. Weiterhin ist eine Strafbarkeit wegen Beleidigung nach § 185 StGB denkbar. Strafrechtlich relevante Handlungen bzw. Unterlassungen[6] des Providers können das Zugänglichmachen der Informationen oder die Nichtsperrung von Teilen des Netzes sein. Das Problem hierbei ist der nach § 15 StGB erforderliche Nachweis des Vorsatzes des Providers, der etwa Pornos zugänglich macht. Zum Vergleich: Die Telekom etwa ist auch noch nicht dafür belangt worden, daß sie Telefonnummern der Anrufbeantworter von Neonazis ganz normal weiterschaltet.

Der Anwendung des bestehenden Strafrechts, das eine Nachzensur[7] ermöglicht, steht keinesfalls die Form der Darstellung von Meinungen oder Bildern im Internet entgegen: Der § 11 Abs. 3 StGB stellt Ton- und Bildträger sowie „andere Darstellungen" den in diesem Gesetz sanktionsfähigen Schriften gleich. Daher sind auch Bilder im Internet davon erfaßt.

Gleichwohl wird weiterer Handlungsbedarf gesehen: Im März 1986 wurde im Bundestag die strafrechtliche Verantwortlichkeit der Provider diskutiert (BT-Drucksache 13/4334). Es wurde darüber beraten, daß Provider und auch User sowohl gesetzlich zu schützen seien, aber auch Zugriffsmöglichkeiten des Staates bestehen müßten.

Neue Welt, neue Gesetze

Am 1. August trat das Telekommunikationsgesetz (TKG) in Kraft. Dies gilt für alle Betreiber von Kommunikationsdiensten, also für Provider wie für die Mobiltelefonteilnehmer. Es sieht in § 8 vor, daß die Betreiber die Namen und Benutzerdaten auf ihre Kosten in Datenbanken zur Verfügung halten müssen und der sog. Regulierungsbehörde zur Verfügung zu stellen haben. Alle Daten werden im Falle eines Mißbrauches der Behörde bekannt gegeben. Dagegen haben vor allem die Grünen im Bundestag datenschutzrechtliche Bedenken erhoben. Seinem Regelungsbereich nach ist das Gesetz jedoch weitgehend auf die Mobiltelefonbetreiber zugeschnitten. Das gewünschte Multimediagesetz ist dies noch nicht.

Schon bisher mußten Mailbox-Betreiber nach der Fernmelde-Überwachungsverordnung (FÜV) im Falle von strafprozessualen Überwachungsmaßnahmen den Fernmeldeverkehr im Klartext zur Verfügung stellen. Das Bundesforschungsministerium hält im Bereich der Internet-Dienste die heute bestehenden Gesetze für nicht ausreichend und plant neue, spezielle Regelungen. Verfassungsrechtlich umstritten ist dabei die Einordnung der Internet-Dienste als Rundfunk oder Presse i. S. d. Art. 5 Grundgesetz (GG).[8] Sie ist nicht zuletzt entscheidend für die Frage, ob der Bund überhaupt eine Gesetzgebungskompetenz in diesem neuen Bereich hat. Legt man den Diensten die Funktion von Rundfunk und Presse zugrunde, so wird die Verbreitung von Daten durch die Provider wohl als Presse einzuordnen sein und damit dem Bund eine Rahmenkompetenz zukommen. Das Gesetz des Bundes zur Regelung der Rahmenbedingungen für Informations- und Telekommunikationsdienste (IuKDG) liegt nun in einem Referentenentwurf mit Stand vom 2. Juni 1996 vor. Es enthält u. a. ein Gesetz über die Teledienste (TDG) sowie eines über digitale Signaturen (SiG). Das TDG gilt nach § 2 explizit nicht für diejenigen Anbieterinnen und Anbieter, die unter das TKG fallen. Damit steht fest: für das Internet sollen eigene Regeln gelten. Das TDG stellt sicher, daß der Staat an die Daten des Users im Falle der Strafverfolgung herankommt. Das SiG regelt den Umgang mit Kryptographie.[9]

Die Diskussion in den USA ist unserer schon einen Schritt „voraus". So wurde der „Communications Decency Act" geschaffen, ein Gesetz, das Freiheits- oder Geldstrafe für die Verbreitung anstößiger Inhalte im Internet androht. Das Gesetz ist im Juni 1996 vom Court of Appeals for the Third Circuit aber für verfassungswidrig erklärt worden, worüber nun der oberste Gerichtshof der USA abschließend zu befinden hat.[10]

Die gesetzlichen Beschränkungen der Meinungsfreiheit im Internet stießen in den USA auf massiven Protest: die *blue ribbon campaign*[11] der Electronic Frontier Foundation in den USA soll allen, die einen freien Austausch von Meinungen im Internet garantiert haben wollen, als gemeinsames Forum dienen. Erkennungszeichen ist eine blaue Schleife, angelehnt an die rote Schleife der Solidaritätsbewegung für HIV-Infizierte. Die Initiatorinnen und Initiatoren dieser Idee fordern eine absolute Freiheit im Internet. Es würde der Idee des Netzes zuwiderlaufen, wenn hier Regeln für die Kommunikation geschaffen werden würden.

Fazit: Die bestehenden Regeln genügen zur Verfolgung von Straftaten. Zum Schutz von Kindern und Jugendlichen müssen sich die Provider und die User technisch absichern. Grundsätzlich besteht daher kein Handlungsbedarf für weitere staatliche Eingriffe im Internet. Private Provider oder Mailboxen müssen sich des Inhalts ihres Angebotes bewußt sein. Den Usern sollte gesichert sein, daß die Mail in ihrer Box nicht von Leuten gelesen wird, für die sie nicht bestimmt ist, und daß ihre veröffentlichten Informationen von einer wachen Netzgemeinde gelesen werden.

Daher bedarf es keines Rasenmähers, um die sprießenden Meinungen im Internet für den Fall eines unkontrollierbaren Wildwuchses zu beschränken. Jeder Betreiber von Informationssystemen muß dem User die Folgen eines Verstoßes gegen die Netiquette und gegen geltendes Strafrecht klarmachen. Die Nutzerinnen und Nutzer müssen Verantwortung mit dem (nicht mehr ganz) neuen Medium Internet zeigen. Eine Ausweitung der (strafrechtlichen) Verantwortlichkeit des Providers könnte dazu führen, daß wohl auch viele „rechtmäßige" Informationen vom Provider „sicherheitshalber" nicht mehr bereitgehalten würden.

Keines Falles brauchen wir eine Internet-Polizei, die den Datenverkehr überwacht. Allerdings muß der Staat seine Strafverfolgungsbehörden mit Computer und Modem vewaffnen, um am Ball zu bleiben. Eine Zensur hat aber nicht stattzufinden!

Jürgen Dierlamm lebt als Referendar in Marburg und arbeitet dort an der Forschungsstelle für Rechtsinformatik der Philipps-Universität.

Anmerkungen:

1 Zur Einführung für Juristinnen und Juristen: Kröger / Clasen / Wallbrecht.
2 Vgl. dazu Knödler *JurPC* 257 ff.; allgemein Rath *FoR* 1/91, 18 ff.
3 Vgl. den Leitfaden zur verantwortungsvollen Nutzung von Datennetzen, „http://www.uni-marburg.de/hrz".
4 Jäger / Collardin *CR* 1996, 236 ff.
5 Vgl. Sieber *JZ* 1996, 429 ff., 494 ff.; Collardin *CR* 1995, 618 ff.
6 Ablehnend Sieber *JZ* 1996, 494, 506.
7 Die Nachzensur kann hier nicht erörtert werden; vgl. dazu Rath *FoR* 1/91, 18 ff.
8 Vgl. Bullinger *JZ* 1996, 385 ff. sowie jüngst den Bund-Länder-Kompromiß, *CR* 1996, 509 f., nach dem dem Bund in diesem Bereich die Rahmenkompetenz zukommt.
9 Zu den verfassungsrechtlichen Bedenken von Regelungen über die Verschlüsselung vgl. S. 131 in diesem Heft; die Entwürfe zum TDG und SiG liegen auf „http://www.rz.uni-duesseldorf.de/WWW/Jura/internet/".
10 Herberger *JurPC* 1996, 251.
11 „http://www.Eff.org/blueribbon.html".

Literatur:

Bullinger, Martin, Ordnung oder Freiheit für Multimediadienste, *Juristenzeitung (JZ)* 1996, 385 ff.
Collardin, Marcus, Straftaten im Internet, *Computer und Recht (CR)* 1995, 618 ff.
Herberger, Maximilian, „Communications Decency Act": Einstweilen angehalten, *JurPC* 1996, 251.
Jäger, Ulrike / Collardin, Marcus, Die Inhaltsverantwortlichkeit von Online-Diensten, *CR* 1996, 236 ff.
Knödler, Christoph, Zensur im Internet?, *JurPC* 1996, 257 ff.
Kröger, Detlef / Clasen, Ralf / Wallbrecht, Dirk, Internet für Juristen, Luchterhand 1996.
Rath, Christian, Mehr Zensur wagen?, *Forum Recht (FoR)* 1/91, 18 ff.
Sieber, Ulrich, Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen, *JZ* 1996, 429 ff., 494 ff.