Materialien zu:

Version 0.9.3.1 beta
vom 6. Oktober 2002

Internet-Sperrungsverfügungen

Die Bezirksregierung Düsseldorf möchte es *Ihnen* unmöglich machen, rund 6000 ausländische Internet-Seiten anzuschauen.

DAVID
Deutsche Arbeitsgemeinschaft zur Verteidigung der Informationsfreiheit in Datennetzen
http://www.david-gegen-goliath.org/
david@david-gegen-goliath.org

„Regierungspräsident Büssow hat heute Vorwürfe der Zensur gegen sein Vorhaben, vier amerikanische Websites durch die nordrhein-westfälische Zugangs-Vermittler sperren zu lassen, entschieden zurückgewiesen. Diese Vorwürfe waren in der letzten Woche von den Magazinen Focus und Spiegel, dem Bundestagsabgeordneten Jörg Tauss, dem Chaos Computer Club, aber auch von Jörg Schieb (WDR) erhoben worden."

Aus einer Pressemeldung der **Bezirksregierung Düsseldorf**

Inhalt

Eine kurze Geschichte über den Umgang mit dem Internet

Einführung

Stefan Krempl zitiert aus einem Beitrag des Bundesverfassungsrichters Wolfgang Hoffmann-Riem im „Jahrbuch Telekommunikation und Gesellschaft 2002“:

„Neben das (alte) Grundrecht auf informationelle Selbstbestimmung tritt ein Grundrecht auf multimediale Selbstbestimmung und -entfaltung“, schreibt der Jurist. Dieses sei eingebettet in die „rechtlich geprägte Informationsordnung“. Dazu gehöre nicht nur das „Setzen von Schranken gegenüber der Ausübung von Kompetenzen des Staates oder von Freiheiten anderer Bürger. Erfasst werde auch der Schutz vor der „Informationsfilterung durch Private“, so Hoffmann-Riem unter Anspielung auf die um sich greifenden Versuche des Staats, Internet-Provider zum Filtern gewisser – etwa pornographischer oder sonst wie strafbarer Inhalte – aus dem Netz zu motivieren. Derlei Tun sei „begrifflich als Zensur“ bekannt, warnt der Bundesverfassungsrichter vor der Entstehung neuer Machtprobleme und einer „Art Geistespolizei“.

Stefan Krempl, in Telepolis
http://www.heise.de/tp/deutsch/inhalt/buch/13265/1.html

Als das Internet Anfang der 90er Jahre an Popularität gewann, versprach es vor allem Freiheit: Preiswerte Ausrüstung verschaffe Zugang zu einem alternativen sozialen Raum, in dem Informationen jeder Art frei fließen würden. Publizieren sei ebenso einfach wie Lesen.

Am Ende des Jahrzehnts hat sich die allgemeine Vorstellung vom Netz gewandelt: Nach dem Eroberungsfeldzug der Wirtschaft scheint vor allem das bequeme Einkaufen per Mausklick vom Sofa aus die eigentliche Bestimmung des Mediums zu sein. Die einstigen Freiheitsversprechen verwandelten sich in Chancen: Jeder könne nun für wenig Geld seinen eigenen Webshop eröffnen und am Internet-Boom teilhaben!

Inzwischen fließen zunehmend wichtige und persönliche Daten über das Netz, während gleichzeitig Überwachung und Kontrolle des Datenverkehrs zunehmen. Dadurch wird Netzwerk- und Software-Design zum politischen Thema. Wir nehmen uns diesem Thema an und setzten sich für den Erhalt der Informations- und Meinungsfreiheit im Internet ein.

Denn auf der einen Seite nimmt zwar die Nutzung des Internets als Vertriebs-, Kommunikations- und Unterhaltungskanals zu, gleichzeitig findet die kompetentere Diskussion über die Bedeutung des neuen Mediums, und auf welche Weise normative Wertevorstellungen transportiert werden, nur in kleinen Zirkeln statt, an der die exekutiven und legislativen Organe weitgehend unbeteiligt sind. Dem gegenüber steht eine Schar von Konsumenten, die sich einem Medium überantwortet, das sie nicht (mehr) versteht – und durch entsprechendes Interface-Design, sowie durch technische Hürden auch nicht verstehen kann.

Für die Informationsgesellschaft ist es unabdingbar, dass jeder das Recht hat, sich aus allen öffentlich zugänglichen Informationsquellen und Datennetzen unzensiert zu unterrichten.

Der populistische Ruf nach „Sperren“ von „nicht zulässigen“ Inhalten mag auf den ersten Blick sinnvoll und gut gemeint sein, ist schlussendlich aber kontraproduktiv und mit demokratietheoretisch äußerst bedenklich. Hinzu kommt die Frage, wer bestimmen soll, was „nicht zulässig“ sein soll. Die Erfahrungen der letzten Jahre zeigen, dass es zu viele Interessen(gruppen) gibt, die bedient werden wollen.

Niemand kann ernsthaft wollen, dass ein Provinzbeamter oder der Geschäftsführer eines Telekommunikations-Dienstleisters bestimmen soll, was die Menschen lesen dürfen und was nicht.

Rheinische Filter-geschichte(n)

Eine Zusammenfassung von Jörg-Olaf Schäfers

Jörg-Olaf Schäfers ist Student, Medienschaffender und Mitarbeiter bei ODEM.org

olaf@odem.org

Irgendwie hat man sich schon an sie gewöhnt: die Meldungen, in denen mit beständiger Regelmäßigkeit verkündet wird, dass die Anzahl der „Schund- und Schmutzseiten“ im Internet mal wieder gestiegen sei. Es sind ja auch durchaus beeindruckende Zahlen. Mal sind es 50% Anstieg, mal 100%, hin und wieder hat man es gar mit Verzehn- [1] bis Verhundertfachungen zu tun. Fast immer erreicht der Grad der Abscheulichkeiten mit einer neuen Meldung auch „eine neue, bisher unbekannte Qualität oder Dimension“. Man könnte meinen, man würde automatisch und ohne eigenes Zutun mit Neonazi-Propaganda und Kinderpornografie überflutet, sobald man online geht.

[1] http://www.teltarif.de/arch/2001/kw22/s5276.html

Selten hingegen findet man in den Berichten eine Relation zur Entwicklung des restlichen Internets oder Angaben, wie die Statistiken erhoben wurden. Kein Wunder: Wenn der Berliner Verfassungsschutz Ende des Jahres 2001 verkündet, die Zahl der Neonazi-Sites sei im letzten Jahr um rund 50 Prozent auf 1000 gestiegen, [2] wäre der ganze Schockeffekt dahin, wenn man gleichzeitig erwähnen würde, dass sich die Zahl der in Deutschland registrierten Domains um 250 Prozent erhöht hat. [3]

[2] http://news.zdnet.de/story/0,,t101-s2101811,00.html

[3] Verstehen Sie mich bitte nicht falsch, es geht nicht darum, real existierende Probleme unserer Gesellschaft zu verharmlosen, allerdings ist es sicher nicht minder wichtig - vor allem für die Beurteilung von Gegenmaßnahmen und ihrer Verhältnismäßigkeit - die Dimensionen nicht aus den Augen zu verlieren.

http://www.denic.de/DENICdb/stats/index.html

Auf entsprechende Meldungen bezieht sich Anfang des Jahres 2001 auch der Düsseldorfer Regierungspräsident Jürgen Büssow in einem „offenen Brief“ an die in „seinem“ Bundesland ansässigen Internet-Provider. [4] Büssows Behörde ist eigentlich für die Überwachung von Mediendiensten wie TV und Radio in NRW zuständig, ob das Internet auch in seinen Aufsichtsbereich fällt, ist umstritten – doch dazu an anderer Stelle. [5]

Es geht in diesem offenen Brief um rechtsradikale Webseiten im Internet. Neben einer möglichen rechtlichen Verantwortung als „Service-Provider“ oder „Content-Provider“, weist Büssow die angeschriebenen Dienstleister in diesem Schriftstück dezent und ohne weitere Ausführungen auf einen Abschnitt im Mediendienstestaatsvertrags (MdStV) hin, der, zumindest nach seiner Auffassung, „Internet-Access-Provider“, die „den Zugang zu ausländischen Internetservern, insbesondere aus den USA ermöglichen“, betreffen würde.

Für aufmerksame Beobachter der Netzszene war die Kombination „Büssow / Internet / MdStV“ damals nicht neu. Bereits im August des Jahres 2000 machte der Düsseldorfer Regierungspräsident kurz von sich Reden, als er laut Spiegel die Provider in Nordrhein-Westfalen aufforderte, sie sollten ihre „Online-Dienste“ (eine begriffliche Ungenauigkeit, die nicht gerade auf Kompetenz in Fachfragen schließen lässt) nach rechtsextremistischen Angeboten durchsuchen und diese

[4] Offener Brief an die Provider in NRW: http://www.bezreg-duesseldorf.nrw.de/cat/SilverStream/Pages/THEMEN_Beitrag.html?query=THBTR.ID%3d3101

[5] Näheres zu den juristischen Aspekten finden Sie im Aufsatz von Andreas Neumann ab Seite 30

gegebenenfalls sperren: „Büssow droht den Unternehmen Geldbußen von bis zu 500.000 Mark an, sollten Nazi-Parolen dennoch weiter verbreitet werden."[6]

Nun, Service-Provider, die „Webspace", also Rechnerkapazitäten im Internet vermieten oder verkaufen, oder Content-Provider, die selber Inhalte publizieren, sind eine Sache, Access-Provider, die ihren Kunden lediglich die Einwahl beziehungsweise den Zugang ins Internet anbieten, eine andere.

Laut Focus sollte der MdStV aber schon damals als Grundlage für ein Vorgehen gegen deutsche Access-Provider herhalten, die ihren Kunden lediglich einen Netzzugang anbieten, über den natürlich auch „unzulässige Inhalte" abgerufen werden können: „In solchen Fällen haften die deutschen Provider, über die der Kontakt zu den Internetseiten im Ausland hergestellt wird". Der Laie staunte und nickte womöglich, die Experten wunderten sich.

Wenn nicht freiwillig, dann per Zwang

Knapp 9 Monate später, im Mai 2001, wird die Situation ein wenig klarer. Auf einer Tagung der Medienaufsichtsbehörden in Düsseldorf sagt Büssow: Wenn es nicht gelänge, ausländische Inhalte-Anbieter oder Service-Provider „rassistischer oder rechtsextremer Seiten" zum Sperren von Angeboten zu bewegen, „müsse dies auf der Zugangs-Ebene geschehen." [7] Als rechtliche Grundlage für ein solches Vorgehen wurde abermals der MdStV angeführt.

Sprich: Wenn ein Anbieter eines Internetangebotes im Ausland auf Anfrage einer deutschen Behörde dieses nicht freiwillig sperrt oder entfernt und auch nicht dazu gezwungen werden kann, könne man deutsche Provider in die Verantwortung nehmen und diese per Verfügung und Bußgeldandrohung dazu bringen, ihren Kunden den Zugriff auf diese Inhalte zu sperren.

Genau diese Interpretation des MdStV ist unter Juristen allerdings umstritten, interessant ist dabei vor allem die Frage, ob Zugangs-Anbieter überhaupt einen Mediendienst im Sinne des Staatsvertrages anbieten .

Über den Sommer 2001 hinweg blieb die Lage zunächst ruhig, erst Anfang Oktober hörten die nordrhein-westfälischen Provider wieder von der Düsseldorfer Behörde. Es war eine Einladung,[8] über die sich kaum ein Provider gefreut haben dürfte. Man lud zur Anhörung nach Düsseldorf, um, so Stefan Krempel für das Netzmagazin Telepolis, die „Zugangsanbieter mit dem Stand der Filtertechnik vertraut machen und dadurch „sanften Druck auszuüben". [9] Die ersten Sperrungen standen auf der Tagesordnung.

Die Bezirksregierung Düsseldorf hatte vier Internetseiten ausgewählt, die nach ihrer Meinung nach deutschem Recht unzulässig seien und zu denen die angeschriebenen Provider ihren Kunden den Zugang sperren sollten. Die Auswahl erschien zuerst recht willkürlich, angesichts der auffallenden Plakativität der einzelnen Angebote wurden sie jedoch offenbar mit Bedacht gewählt. Die Nazi-Seiten sollten als Begründung für weitergehende Maßnahmen herhalten.

Dabei kam es zu einem peinlichen Patzer. Eine der vier Seiten war zu diesem Zeitpunkt schon gar nicht mehr existent: das Angebot des texanischen Service-Providers *front14.org*, der über seine Server rechtsextremistische Inhalte verbreitete, war bereits ohne Zutun aus Deutschland aus dem Netz verschwunden. Die Nummer 4 auf der Wunschliste der Bezirksregierung war die „Tasteless"-Seite *„This is rotten dot com" (http://www.rotten.com)*, der man sicherlich viel vorwerfen kann, allerdings wohl kaum rechtsextrem zu sein. Ein erster Versuchsballon, wie die Öffentlichkeit reagieren würde?

Aber hieß es nicht immer, es wäre technisch nicht möglich Inhalte im Internet effizient zu sperren? Und nun sollten Provider, von denen man eigentlich annehmen darf, sie wären über die technischen Belange ihrer tagtäglichen Arbeit bestens informiert, von der Bezirksregierung über den „Stand der Filtertechnik" informiert werden?

Taschenspielertricks

Tatsächlich, die Bezirksregierung hatte sich von den Firma Tricus Systemhaus aus Dormagen und der Webwasher AG aus Paderborn beraten lassen. Danach war die Behörde der festen Überzeugung „punktgenaue Filtermaßnahmen für deutsche Surfer" seien machbar, selbst so genannte Mirrors, also Kopien von Webangeboten auf neuen Servern, sollte eine wundersame Filtersoftware dank „automatischer Nachverfolgung" erkennen und in einer „zentralen Datenbank"[9] speichern.

Die Katze war also aus dem Sack, knapp 5 Jahre nachdem die Bundesanwaltschaft im Fall „xs4all" gescheitert war, die Verbreitung der Zeitschrift „Radikal" im Netz zu unterbinden, schickte sich erneut eine deutsche Behörde an, Webseiten im Ausland auf der Zugangsebene filtern zu lassen.

Doch zunächst blieb die Situation ruhig, zwar wurden die Absichten der Bezirksregierung auf einigen Mailinglisten [10] und in juristischen Fachforen kontrovers diskutiert, für die breite Netzöffentlichkeit waren die Sperrungen aber noch kein Thema. Dies sollte sich Mitte November ändern. Unmittelbar nach der Anhörung bei der Bezirksregierung in Düsseldorf wurde bekannt, dass sich bereits 12 Provider dem „sanften Druck" der Bezirksregierung nachgaben (man drohte mit Bußgeldern von 500.000 bis

1.000.000 DM) und sperrten den Zugriff auf die o.g. Webseiten, teilweise schon seit Oktober: die Einladung der Anhörung wurde als Sperrungsaufforderung missverstanden.

Doch statt der in Aussicht gestellten hochkomplexen Filtersysteme setzte man auf von der Bezirksregierung empfohlene Taschenspielertricks. Durch Manipulationen an den Provider-eigenen Nameservern (eine Art Telefonbuch für Internetadressen [11]) wollte man die Nutzer von den „unzulässigen Inhalten“ fernhalten. Jeder Nutzer, der fortan den URL (die „Adresse“ einer Webseite im Klartext, etwa „http://www.odem.org/“) einer der zu gesperrten Seiten in seinen Browser eintippte, sollte umgeleitet werden, da der Adresse im „Telefonbuch“ beim Provider eine falsche Nummer zugewiesen wurde.

Zweifelsohne eine Sperrmethode, die man völlig zu Recht als „Netzsperre für Fritzchen Doof“ [12] bezeichnen kann, ist sie doch bereits mit wenig Sachkenntnis zu umgehen [13]. Zum Beispiel durch Nutzung eines alternativen „Telefonbuchs“/ Nameservers.

Kritiker: Verfassungsmäßige Bedenken, populistischer Aktionismus und „Schaumschlägerei“

Noch während die ersten Filter aktiviert wurden, formierte sich heftiger Widerstand gegen die „rheinischen Sittenwächter“ [14]. Sierk Harmann, Rechtsexperte der Gruppe Artikel5 (http://www.artikel5.de) äußerte „verfahrens- wie verfassungsmäßige Bedenken“, die auch von Juristen wie dem Münchener Rechtsanwalt Thomas Stadler [15] und Prof. Dr. Thomas Hoeren vom Institut für Informations- , Telekommunikations- und Medienrecht der Universität Münster geteilt wurden [16]. Selbst Büssows Parteikollege, der medienpolitische Sprecher der SPD-Bundestagsfraktion, Jörg Tauss, warf der Bezirksregierung Düsseldorf in einer Pressemitteilung [17] „politischen Aktionismus“ und „Schaumschlägerei“ vor und wies, wie viele andere Internetexperten auch, auf die technischen Probleme des eigentlichen Vorhabens hin, der Etablierung einer halbswegs kontrollierbaren Filterinfrastruktur für „unzulässige Inhalte“. Deutliche Worte fand auch Harald Summa vom Electronic Commerce Forum, dem Verband der deutschen Internetwirtschaft (eco e.V.): „Die Provider werden zum Spielball ordnungswütiger Aufsichtsbehörden mit zweifelhafter Zuständigkeit“. Summa war es auch, der schließlich „eine endgültige Klärung der Haftungsfrage für Provider durch die Politik“ forderte [14].

Knapp 3 Wochen später, am 19.Dezember 2001, stellten die Firmen Webwasher.com AG, IntraNet GmbH und Bocatel GmbH und Co. KG in einem Strategiepapier [18] den so genannten „Filterpiloten“ vor, „ein kombiniertes Verfahren aus Routing und Filtertechnologien, [..] das die von der Bezirksregierung Düsseldorf geforderte technische Sperrung überflüssig machen soll.“ [19]. Was an einem kombinierten Verfahren aus „Routing- und Filtertechnologien“ nicht technisch sein sollte, verschwiegen die „Filterexperten“ allerdings.

Handelte es sich hier um die von der Bezirksregierung angekündigte Wunderwaffe gegen den „Schmutz und Schund“ im Internet?

Dies sollte in den kommenden Monaten ein Pilotversuch an der Universität Dortmund zeigen, auf den später noch eingegangen wird. Doch bleiben wir zunächst beim 19. Dezember, denn dieser hielt noch eine weitere Überraschung bereit:

In einer Presseerklärung [20] kündigte die Bezirksregierung an, zur „Herstellung von Rechtssicherheit“ nun die entsprechenden Sperrungsverfügungen erlassen zu wollen, auf deren Grundlage die Provider in NRW ihren Kunden den Zugriff auf die von der Bezirksregierung ausgewählten Inhalte sperren sollten. Doch schon zwei Absätze weiter in der gleichen Presseerklärung wird klar, dass man in Düsseldorf eigentlich an einer „Lösung“ des Problems ohne Beteiligung der eigenen Behörde interessiert war, kein Wunder, ist damit doch nicht zuletzt die von Harald Summa (eco e.V.) gestellte Haftungsfrage verbunden. Den schwarzen Peter möchte niemand gerne haben, vor allem wohl dann nicht, wenn man sich, wie die Bezirksregierung Düsseldorf, auf derart dünnen Eis bewegt.

Doch bis die nordrhein-westfälischen Provider die Sperrungsverfügung tatsächlich in den Händen hielten, sollten noch 2 weitere Monate vergehen. 2 Monate, in denen einige Anbieter, darunter die Ruhr-Uni Bochum [21] ihre Sperrungen wieder rückgängig machten, unter anderem wegen der fehlenden Rechtssicherheit und der Unzulänglichkeit der Maßnahmen.

In der Zwischenzeit versuchte Alvar Freude, Mitbegründer der Netzinitiative ODEM.org, das Treiben des Düsseldorfer Regierungspräsidenten durch eine Strafanzeige prüfen zu lassen [22]. In dem 38seitigen Schriftstück warf der Stuttgarter Medienkünstler und Internet-Experte den an den Sperrmaßnahmen beteiligten Providern, Filtertechnik-Anbietern und Hochschulen unter anderem Datenunterdrückung, Verletzung des Fernmelde- und Postgeheimnisses, sowie die Planung von Datenmanipulationen vor. Zwar wurden in einigen Fällen nicht einmal Ermittlungsverfahren aufgenommen und die Verfahren in den anderen Fällen nach einiger Zeit wieder eingestellt, dennoch konnte die Aktion aufgrund ihres Beitrags zur Sensibilisierung der Netzöffentlichkeit als Erfolg verbucht werden.

Anfang Februar 2002 war es dann endlich soweit: Die seit Oktober 2001 angekündigten Sperrungsverfügungen wurden verschickt. Die Anzahl der zu sperrenden Domains hatte sich von vier auf zwei verringert. Dass der rechte Service-Provider front14.org seit geraumer Zeit nicht mehr im Netz aktiv war, hatte nun offenbar auch die Bezirksregierung Düsseldorf gemerkt. Auch die Sperrung der umstrittenen, weil zwar fast durchweg geschmacklosen, aber nicht rechtsextremen Seite „rotten.com“ wurde nicht mehr verlangt. Zu deutlich waren die Proteste gegen eine drohende „Zensur“ des Internets, zumindest in diesem Punkt wurde der Vorstoß abgebrochen, generell „unzulässige Inhalte“ sperren zu wollen. Die Bezirksregierung konzentrierte sich nun wieder ganz auf den „Kampf gegen den Rechtsextremismus“.

Interessant war der Blick auf die in der Verfügung vorgeschlagenen „Sperrmethoden“. Die Bezirksregierung empfahl zur Sperrung immer noch die von Netzexperten als untaugliche beschriebene Nameserver-Manipulation, führte aber bereits zwei weitere Methoden an, die technisch weit komplexer waren und mit erheblichen Einschnitten in den Netzwerkverkehr der Provider verbunden gewesen wären, vom Material-und Zeitaufwand nicht einmal zu reden.

Eine weitere Überraschung fand sich auf Seite 10 der Sperrungsverfügung. Auch Internetsuchmaschinen, so war dort nachzulesen, die „systematisch fremde Inhalte erfassen, ordnen und z. T. kommentieren, dürften als Service-Provider gemäß § 5 Abs. 2 MdStV anzusehen sein“. Ein kleiner Absatz, der, wie auch der Rest der Verfügung, in den kommenden Wochen immer wieder aufgegriffen wurde. Als „völlig unverhältnismäßig“ bezeichnete so zum Beispiel Michael Ronellenfitsch, Professor für Öffentliches Recht an der Universität Tübingen, die drohenden Sperrungsverfügungen gegen Internet-Suchmaschinen [23].

„Der politische Aktionismus, den die Bezirksregierung Düsseldorf hier an den Tag legt, bleibt letztlich nur Schaumschlägerei.“

Jörg Tauss, MdB (SPD), Beauftragter für Neue Medien der SPD-BTF, 21.11.01
http://www.tauss.de/berlin/taeterverfolgen.html

Allerdings sollte man wissen, dass viele Suchmaschinen bereits aktiv in ihre Rankingmechanismen eingreifen, um möglicherweise „unzulässige“ Angebote zumindest nicht auf den ersten Ergebnisseiten einer Suchanfrage erscheinen zu lassen. Hin und wieder werden Webseiten von Suchmaschinen auch komplett für die Ergebnisliste gesperrt, sie bleiben dann zwar im Datenbestand („Index“) der Suchmaschine, können aber nicht mehr „gefunden“ werden. Im April wurde beispielsweise ein Fall bekannt, wo die Deutsche Bahn AG Suchmaschinen abmahnte, die den Zugriff auf die bereits erwähnten Webseiten der Zeitschrift „Radikal“ beim niederländischen Provider xs4all ermöglichten. Auch das von der Sperrungsverfügung der Bezirksregierung Düsseldorf betroffene rechtsextremistische „Portal“ *stormfront.org* ist für User, die das deutsche Interface der beliebte Suchmaschine Google benutzen, nicht mehr ohne weiteres zu finden [24]. Damit wird es inbesondere denjenigen, die sich nicht in der Nazi-Szene auskennen schwer, sich mit dieser kritisch auseinanderzusetzen.

Die Bezirksregierung lag also voll im Trend, als sie auch Internet-Suchmaschinen in den Fokus nahm. Vorreiter auf diesem Gebiet war allerdings das Mainzer Aufsichtsgremium jugendschutz.net, eine gemeinsame Einrichtung der Jugendministerien der Länder, die bereits seit 2 Jahren einen „Verhaltenscodex“ für Suchmaschinenbetreiber zu etablieren versucht, in dem unter anderem der Austausch von „Adress-“ und „Schlüsselwortlisten“ für „unzulässige“ und „jugendgefährdende Inhalte“ geregelt werden soll [25]. Suchmaschinen-Experten wie Stefan R. Müller bezeichnen dies als vollkommen unwirksam.

Doch nicht nur von Juristen wurde die Sperrungsverfügung der Bezirksregierung heftig kritisiert, immer breiter wurde die Front gegen die Düsseldorfer „Internetzensoren“. Abermals und in auffallend scharfer Form äußerte sich der medienpolitische Sprecher der SPD-Bundestagsfraktion Jörg Tauss zu den Vorgängen in Düsseldorf [26]. Ende Februar 2002 startete die Netzinitiative ODEM.org schließlich die Unterschriftensammlung „Erklärung gegen die Einschränkung der Informationsfreiheit“ [27] und konnte schon in den ersten Tagen mehr als 2000 Unterschriften sammeln. Zu den Erstunterzeichnern gehörten unter anderem die „Reporter ohne Grenzen“, der ICANN-Direktor und CCC-Sprecher Andy Müller-Maguhn, der Pressesprecher des virtuellen Ortsvereins der SPD Arne Brand und die Bundestagsabgeordneten Grietje Bettin (Bündnis 90 / Die Grünen), Angela Marquadt (PDS) und Jörg Tauss (SPD).

Mit der taz, die von „der neuen Wacht am Rhein“ schrieb [28], und dem Tagesspiegel, der von einem „Düsseldorfer Alleingang“ berichtete, fand das Thema nun auch außerhalb der Computerpresse Beachtung. Wenig später folgten Berichte in der Süddeutschen Zeitung, der Frankfurter Rundschau, der jungen Welt und beim Online-Ableger des Hamburger Magazins Spiegel.

Anfang April 2002 waren die Vorgänge in Düsseldorf sogar für eine ungewöhnliche Premiere verantwortlich. Erstmals in seiner 20jährigen Geschichte organisierte der Chaos Computer Club (CCC) zusammen mit ODEM.org und zahlreichen anderen Gruppierungen eine Straßendemonstration [29]. Rund 300 Computerfreaks folgten dem Ruf der „Chaoten“ und begaben sich begleitet von zahlreichen Ordnungshütern, die sich offenbar auf Schlimmeres vorbereitet hatten, auf einen friedlichen Umzug durch das sonnige Düsseldorf, der mit einer Kundgebung und anschließender Diskussion mit Vertretern der Bezirksregierung vor dem Dienstgebäude der Bezirksregierung endete. Das Medienecho war bemerkenswert, mehr als 60 Berichte in der regionalen und überregionalen Presse, im Hörfunk und Lokalfernsehen, selbst der Düsseldorfer Regierungspräsident schien überrascht.

Bemerkenswert waren aber auch vor allem die Statements, die Regierungspräsident Büssow und sein Stellvertreter Riesenbeck nach der Demostration in Gesprächen mit Pressevertretern und Teilnehmern abgaben. Wenn der Filterpilot im Einsatz sei, beabsichtige man jegliche „nicht zulässigen Inhalte“ zu sperren und wolle sich nicht nur auf rechtstremistische Angebote beschränken. Die Sperrung der zwei rechtsextremen Seiten sei relativ willkürlich und nur ein mit den zuständigen Stellen der anderen Bundesländern abgesprochener Versuchsballon. „Wenn ich das Milchtrinken verbieten will, muss ich erst mal ein oder zwei Flaschen beschlagnahmen“ [30].

Da war er also wieder, der ominöse „Filterpilot“, von dem man seit Ende letzten Jahres nichts mehr gehört hatte. Doch plötzlich, es war inzwischen Anfang Mai, brodelte es in der Gerüchteküche, aus den wie üblich gut informierten Kreisen war zu hören, dass die vermeintliche Wunderwaffe offenbar nicht so recht funktionieren wollte. Am 15. Mai ließ der Chaos Computer Club schließlich die Bombe platzen und verkündete, dass die „seit Februar laufenden Versuche der Sperrung von Internet-Inhalten durch eine „filterbasierte Zensurinfrastruktur [..] auf der technischen Ebene gescheitert“ seien [31]. Günter Schwichtenberg, Leiter des Hochschulrechenzentrums der Universität Dortmund und für den Test des Filterpiloten verantwortlich, bestätigte dies gegenüber dpa, die Pressemitteilung der Bezirksregierung folgte einen Tag später [32].

Aber auch das (vorläufige?) Scheitern des einstigen Vorzeigeprojektes, das von der Düsseldorfer Behörde seitdem wie ein verstoßener Sohn behandelt wird, konnte Büssow nicht von seinen Plänen abbringen, im Gegenteil. In einem Interview gab er sich gegenüber dpa entschlossen, das Scheitern eines zentralen Filtersystems „entbinde die Provider nicht von ihrer Pflicht keine strafbaren Inhalte zu verbreiten“: „Büssow sagte, dass bis zu 6000 Internet-Angebote für eine Sperrung in Frage kämen. Ziel sei es, die Verbreitung strafbarer Inhalte und das Geschäft mit Neonazi- Propaganda zu erschweren.“ [33] Den Unterschied zwischen Rundfunk und Internet haben die Mediaufseher immer noch nicht verstanden, die Transporteure sollen immer noch für den transportierten Inhalt haftbar gemacht werden. Wann wird die Telekom angewiesen, „nicht zulässige“ Telefonnummern im Ausland zu „sperren“?

Als Reaktion kündigte die Bezirksregierung an, umgehend mit der Bearbeitung der Widersprüche, die 38 der ursprünglich knapp 80 angeschriebenen Provider gegen die ergangene Sperrungsverfügung eingelegt hatten, zu beginnen. Doch bis die ersten Provider den Ablehnungsbescheid ihres Widerspruchs in den Händen hielten, sollten weitere zwei Monate vergehen [34]. In der Zwischenzeit stimmte die Bezirksregierung abermals das hohe Lied der Selbstregulierung an. Die Provider sollten doch bitte von sich aus und nach eigenem Ermessen filtern, ohne dass man sie jedes Mal per Sperrungsverfügung zwingen müsse. Verwunderlich, sollte der Regierungspräsident immer noch nicht bemerkt haben, dass diese Form der „Selbstregulierung“ für Provider recht uninteressant ist, man erinnere sich an die nun schon reichlich strapazierte Haftungsfrage der neu ernannten Hilfs-Sheriffs? Oder handelte es sich etwa um ein taktisches Manöver, um sich aus der Verantwortung zu ziehen? Der Bundesverfassungsrichter Wolfgang Hoffmann-Riem hat in der Zwischenzeit vor einer „Informationsfilterung durch Private“ gewarnt. [35]

Was hat die Bezirksregierung zu verbergen?

In der Zwischenzeit beantragte ODEM.org den Zugang zu Dokumenten, die im Zusammenhang mit den Sperrverfügungen stehen. Nach dem Informationsfreiheitsgesetz Nordrhein-Westfalen sind Behörden verpflichtet, auf Anfrage den Zugang zu den bei ihnen vorhandenen Informationen zu gewährleisten, und zwar unverzüglich, spätestens aber innerhalb eines Monats. Doch die Bezirksregierung dachte gar nicht daran, die betreffenden Dokumente herauszugeben. Einige der angeforderten Dokumente würden nicht existieren (und das obwohl der Regierungspräsident sie mehrfach zuvor öffentlich zitiert hatte), manche Erkenntnisse seien „nicht im dienstlichen Zusammenhang“ erlangt worden (obwohl sie aus einem Treffen in den Räumen der Bezirksregierung hervorgingen und diese in Pressemeldungen darauf einging) und würde daher daher auch nicht unter das Informationsfreiheitsgesetz [36] fallen. Die Ausreden der Bezirksregierung waren kreativ und interessant, aber nur wenig glaubwürdig. Die Rüge durch die Landesdatenschutzbeauftragte folgte auf dem Fuß, nur die angeforderten Dokumente wurden größtenteils auch Monate später noch nicht herausgegeben.

Das bisher letzte Kapitel der rheinischen Filtergeschichte(n) beschäftigt sich mit der kürzlich ergangenen „Anordnung des sofortigen Vollzugs der Sperrmaßnahmen“. Die plötzliche Eile verwundert. „Das Verfahren zieht sich schon über ein Jahr hin, und jetzt soll es plötzlich ganz schnell gehen“, sagte eco-Geschäftsführer Harald Summa.

„Wir können uns die besondere Eile nicht mit sachlichen oder juristischen Argumenten erklären, dahinter kann nur politisches Kalkül stecken.“ [37] Dass von den beiden Naziseiten so ganz plötzlich eine Gefahr für die freiheitlich-demokratisch Grundordnung unseres Landes ausgehen soll, ist auch nicht so recht begreiflich. Schon eher ist zu verstehen, wenn man kurz vor einem Kongress im eigenen Haus noch einmal punkten will und wird sogar vom Verfassungsschutz NRW verneint: „Der Einfluss von Lauck auf die bundesdeutsche Neonazi-Szene ist aufgrund seiner äußerst aggressiven nationalsozilistischen Grundhaltung eher marginal.“

[1] http://www.teltarif.de/arch/2001/kw22/s5276.html
[2] http://news.zdnet.de/story/0,,t101-s2101811,00.html
[3] http://www.denic.de/DENICdb/stats/index.html
[4] Offener Brief an die Provider in NRW: http://www.bezreg-duesseldorf.nrw.de/cat/SilverStream/Pages/THEMEN_Beitrag.html?query=THBTR.ID%3d3101
[5] Näheres zu den juristischen Aspekten finden Sie im Aufsatz von Andreas Neumann ab Seite 30
[6] http://www.heise.de/newsticker/data/jk-26.08.00-005/
[7] http://www.teltarif.de/arch/2001/kw22/s5276.html
[8] http://www.ccc.de/CRD/CRD20011004-NRWLAD.pdf
[9] http://www.telepolis.de/deutsch/inhalt/te/9902/1.html
[10] http://www.fitug.de/debate/0110/msg00557.html ff
[11] http://www.wdrmaus.de/sachgeschichten/internet
[12] http://www.telepolis.de/deutsch/inhalt/te/11175/1.html
[13] http://ccc.de/censorship/dns-howto/index.html
[14] http://www.telepolis.de/deutsch/inhalt/te/11225/1.html
[15] http://www.jurawelt.com/aufsaetze/5520
[16] http://www.odem.org/zensur/stellungnahme-prof-hoeren.pdf
[17] http://www.tauss.de/service/presse/nrwsperrungtaeterverfolgennichtinterent
[18] http://www.bocatel.de/Docs/2001-1219-Strategiepapier_Filtering1.pdf
[19] http://www.heise.de/newsticker/data/mur-20.12.01-001/
[20] http://www.bocatel.de/mitteilung_1.htm
[21] http://www.heise.de/newsticker/data/hod-31.01.02-002/
[22] http://odem.org/zensur/ sowie http://odem.org/zensur/anzeige/
[23] http://www.heise.de/tp/deutsch/inhalt/te/11864/1.html
[24] http://www.heise.de/telepolis/12948.html
[25] http://www.heise.de/newsticker/data/jk-12.07.02-007/
[26] http://www.tauss.de/service/presse/stellungnahmesperrungsverfuegung bzw. http://www.heise.de/newsticker/data/anw-20.02.02-009/
[27] http://odem.org/informationsfreiheit/erklaerung.html

[28] http://www.taz.de/pt/2002/02/21/a0170.nf/text
[29] http://www.politik-digital.de/text/netzpolitik/netzrecht/demo.shtml
[30] http://www.telepolis.de/deutsch/inhalt/te/12262/1.html
[31] http://www.heise.de/newsticker/data/anw-15.05.02-000/
[32] http://www.bezreg-duesseldorf.nrw.de/cat/SilverStream/Pages/presseframe?BeitragsID=7706
[33] http://www.heise.de/newsticker/data/cp-16.05.02-000/
[34] http://www.heise.de/newsticker/data/hod-23.07.02-000/
[35] Wolfgang Hoffmann-Riem: Informationsfreiheit; in: Kubicek, Klumpp, Büllesbach, Fuchs, Roßnagel (Hrsg): Innovation@Infrastruktur. Jahrbuch Telekommunikation und Gesellschaft 2002, Heidelberg 2002: Hüthig; Seite 81ff.
Siehe auch: http://www.heise.de/tp/deutsch/inhalt/buch/13265/1.html
[36] http://odem.org/informationsfreiheit/presse-ifg-bescheid.html und http://odem.org/informationsfreiheit/presse-ifg-bescheid.html
[37] http://www.heise.de/newsticker/data/hod-10.09.02-000/ und http://odem.org/material/verfuegung/vollzug.html
[38] Verfassungsschutzbericht des Landes Nordrhein-Westfalen 2001, S.104: http://www.im.nrw.de/inn/doks/vs/jb2001.pdf

„Es ist daher und wegen der mit der Sperrungsanordnung verbundenen Öffentlichkeitswirkung nicht abwegig, anzunehmen, dass die Sperrung dazu geführt hat, dass mehr Nutzer auf die illegalen Inhalte zugreifen können, als es ohne die Sperrung der Fall gewesen wäre. Entsprechend wurde Anfang Februar auf der Seite von Gary Lauck stolz verkündet, dass es im januar 3 Millionen zugriffe auf das Angebot gegeben habe.“

Jörg Tauss, MdB (SPD), Beauftragter für Neue Medien der SPD-BTF, 21.11.01
http://www.tauss.de/service/presse/stellungnahmesperrungsverfuegung

Grundsatz-Erklärung

der Bezirksregierung Düsseldorf

Weil Kinder „ungeeignete“ Webseiten sowieso nicht anschauen und wegklicken, sollten sie davor geschützt werden:

„Filter können ein wichtiges Hilfsmittel sein, besonders für jüngere Schüler. Kinder wissen oft noch nicht, auf welche Inhalte sie im Netz stoßen können, und sie erschrecken sich vielleicht, wenn sie »ungeeignete« Websites entdecken. Diese Kinder haben kein Interesse daran, sich solche Sites anzusehen, und darum sollten sie davor mit einem einfachen Filter geschützt werden.“

Julius Getz Mørk, 18, Schüler der Nesodden upper Secondary School in Nesoddtangen, Norwegen in einem Aufsatz über Internet-Filter

In: Marcel Machill, Felicitas von Peter (Hrsg.): Internet-Verantwortung an Schulen; Verlag Bertelsmann Stiftung, Gütersloh 2001 Seite 373

Zur Sperrung von rechtsextremistischen Internet-Seiten

von RD Jürgen Schütte

Im Februar 2002 hat die Bezirksregierung Düsseldorf als Aufsichtsbehörde nach dem Mediendienste-Staatsvertrag und dem Teledienstgesetz die Zugangs- (Access-) Provider in Nordrhein-Westfalen zur Sperrung von zwei rechtsextremistischen Internet-Angeboten aufgefordert.

In diesen Angeboten, die über amerikanische Host-Provider verbreitet werden, wird zu Hass und Gewalt gegen Juden, Ausländer und Menschen anderer Herkunft und Rasse aufgerufen. Das friedliche Zusammenleben aller Menschen in der Bundesrepublik Deutschland wird in Frage gestellt und bekämpft, indem Vorurteile, Zwietracht, Misstrauen sowie kämpferische Feindschaft gegen Teile der Bevölkerung propagiert werden.

Die nationalsozialistische Rassenideologie wird in diesen Angeboten zu Propagandazwecken verbreitet, der Holocaust wird geleugnet oder glorifiziert. Die Geschichte des nationalsozialistischen Terrorregimes wird umgeschrieben und gefälscht.

In menschenverachtender Weise werden Nachbildungen von Zyklon-B-Dosen, oder „Seife Marke Auschwitz“ zum Kauf angeboten.

Wenn solche Angebote jederzeit im Internet abgerufen werden können, wird der Eindruck vermittelt, neonazistische Inhalte seien gesellschaftsfähig.
Es gibt aber keinen allgemeinen Informationsanspruch auf menschenverachtende Inhalte.

Der in allen Bundesländern geltende, im Jahre 1997 beschlossene Mediendienste-Staatsvertrag erklärt Angebote, die gegen Strafgesetze verstoßen, den Krieg verherrlichen, die Menschenrechte verletzen, geeignet sind Kinder und Jugendliche sittlich schwer zu gefährden, für unzulässig.

Die zwei zu sperrenden Angebote sind unzulässig, weil sie nicht nur die Menschenwürde verletzen, den Krieg verherrlichen, jugendgefährdend sind, sondern insbesondere den Tatbestand Volksverhetzung nach § 130 Strafgesetzbuch erfüllen.
In jedem anderen Medium, ob Zeitungen, Zeitschriften, Film, Fernsehen, Tonträger etc. sind diese Angebote nach den geltenden Gesetzen der Bundesrepublik Deutschland unzulässig und verboten.

Der Mediendienste-Staatsvertrag verpflichtet die Aufsichtsbehörden der Länder zur Sperrung oder Untersagung von unzulässigen Angeboten. Den Behörden wird dabei kein Ermessensspielraum eingeräumt. Da mehr als 90 % der von deutschen anonym bleibenden Content-Providern verantworteten rechtsextremistischen Inhalte über ausländische (insbesondere amerikanische) Host-Service-Provider im Internet verbreitet werden, sieht der Mediendienste-Staatsvertrag als einzig verbleibende Lösung die Verpflichtung der Access-Provider zur Sperrung vor.

Auf die Möglichkeit der Inanspruchnahme der Zugangsprovider zu verzichten, bedeutet nicht nur ihre gesetzlich vorausgesetzte Mitverantwortung für die Verbreitung dieser Inhalte zu ignorieren.
Die staatlichen Aufsichtsbehörden würden darüber hinaus ihren Verpflichtungen nicht gerecht und müssten sich zu Recht vorwerfen lassen, das ihnen Mögliche gegen den zunehmenden Rechtsextremismus im Internet nicht unternommen zu haben.

Dass Sperrungen bei den Zugangs-Providern die rechtsextremistischen Inhalte nicht – wie es wünschenswert wäre – aus dem Internet verbannen, wußten auch die Gesetzgeber. Trotzdem ist es sinnvoll solche Sperrungen vorzusehen, weil dadurch die Verbreitungslogistik der vernetzten rechtsextremistischen Szene gestört wird.

Die gegenwärtigen Sperrungen beweisen, dass die rechtsextremistische Szene gezwungen ist, zu reagieren. So sehen sich die gesperrten rechtsextremistischen Provider z. T. gehalten, ihre verbotenen Inhalte auf weitere Seiten – mit einem anderen Domain-Namen – zu spiegeln.
Technische Anleitungen werden verbreitet, um für die Nutzer durch Manipulation ihres Rechners die Sperrungen zu umgehen.
Nicht zuletzt massive Drohungen gegen Beschäftigte der Aufsichtsbehörde sprechen dafür, dass die rechtsextremistische Internetszene getroffen wurde.

Wer bei dieser Sachlage Sperrungen deswegen ablehnt, weil sie keine 100%ige Zugangsbehinderung bewirken können, folgt einer technokratischen Funktionslogik, die die Wirkungen staatlicher Ge- und Verbote verkennt.

Straßenverkehrszeichen z. B. werden auch nicht deswegen abgeschafft, weil ihnen oft genug zuwider gehandelt wird.

Würden alle Provider in der Bundesrepublik Deutschland die unzulässigen rechtsextremistischen Angebote sperren, wären diese faktisch für 70 – 80 % der Nutzer nicht mehr erreichbar.
Mit der Vorgabe, rechtsextremistische Inhalte im Internet nicht zuzulassen, vollzieht der Mediendienste-Staatsvertrag europäisches Recht. Die in allen EG-Staaten verbindliche E-Commerce-Richtlinie gibt den Gesetzgebungskörperschaften der Mitgliedsstaaten vor, Hass und Gewalt im Internet zu verbieten (Artikel 3 Absatz 4 a, 1. E-Commerce-Richtlinie des Europäischen Parlaments und Rates vom 08.06.2000).

Konkrete Verbote sind auch in Frankreich verhängt worden. So wurde die Fa. Yahoo verurteilt, Auktionen von Nazi-Memorabilien für französische Nutzer aus ihrem Angebot herauszunehmen (Tribunal de Grande Instance de Paris, 20. Nov. 2000, No. RG 00/05308). Ende Oktober 2001 hat ein französisches Gericht festgestellt, dass die dortigen Zugangs-Provider materiell zur Sperrung eines rechtsextremistischen Content- und Service-Providers aus den USA verpflichtet sind (http://www.heise.de/newsticker/data/fr-01.11.01-000/)

Sperrungen von unzulässigen Internet-Angeboten haben nichts mit diktatorischen Zensurmaßnahmen zu tun. Sperrungen in einem Rechtsstaat, wie der Bundesrepublik Deutschland, sind transparent, nicht diskriminierend und vor allen Dingen anfechtbar und korrigierbar vor den unabhängigen Verwaltungsgerichten und evtl. sogar vor dem Bundesverfassungsgericht. Es dürfte Ausdruck einer Unschärfe im Differenzierungsvermögen mancher Diskussionsteilnehmer sein, hier Parallelen zu den Diktaturen im Iran oder in China zu konstruieren.

Es ist daran zu erinnern, dass mit Bestehen der Bundesrepublik Deutschland, die Gesetzgebung immer wieder deutlich gemacht hat, dass strafbare rechtsextremistische Propaganda nicht zur tolerierbaren Alltagskultur gehört.

Insofern gibt es aus historischen Gründen Unterschiede zum amerikanischen Freiheits- und Verfassungsverständnis. Die Bundesrepublik Deutschland ist nach dem II. Weltkrieg bewußt in antifaschistischer Tradition aufgebaut worden. Das Bekenntnis zur Menschenwürde, das Widerstandsrecht und das Fortgelten der Vorschriften über die Entnazifizierung sind verfassungsrechtlicher, zahlreiche spezifische Strafvorschriften repressiver Ausdruck dieser Tradition.

Die Bundesrepublik Deutschland versteht sich als wehrhafte Demokratie, die den Feinden der Freiheit, der Demokratie und des Rechtsstaats nicht noch einmal die Möglichkeit einräumen will, durch den Missbrauch von Freiheitsrechten, die freiheitlich demokratische Grundordnung abzuschaffen.

Eine Demokratie ist dem Minderheitenschutz verpflichtet. Bezogen auf den Rechtsextremismus entsteht dadurch die staatliche Pflicht, die Aggression zu bekämpfen und mögliche Opfer zu schützen. Wer rechtsextremistische Inhalte im Internet zulassen will, duldet rechtswidrige Taten und liefert ethische und religiöse Minderheiten der aggressiven neonazistischen Haßpropaganda aus. Der Rechtsextremismus verschafft sich durch das Internet seinen gesellschaftlichen Resonanzboden, obwohl es kein on-line-Recht gibt, das nicht brereits off-line Gültigkeit hat.

Ziel staatlicher Regulierung im Internet ist die für alle sonstigen Medien geltende und bewährte Selbstregulierung.
Die an die Allgemeinheit gerichtete Nazipropaganda im Internet in Form von Schrift, Ton und Bild unterscheidet sich nicht von der Propaganda in Form von Büchern, Schallplatten und Filmen. Wenn staatliche Maßnahmen dazu beitragen, dass die Regeln, die im Zeitschriften-, Buch-, Tonträgerhandel im Rundfunk und Fernsehen gelten und zumeist eingehalten werden, sich auch im Internet durchsetzen, dann hat staatliche Ordnungspolitik ihr Ziel erreicht.

„Herr Büssow ist als selbsternannter Internet-Saubermann auf einem privaten Kreuzzug und zielt in erster Linie auf die medienwirksame Verwertung seines moralisch sicherlich heren Anliegens.“

Jörg Tauss, MdB (SPD), Beauftragter für Neue Medien der SPD-Bundestagsfraktion am 30. Mai 2002
http://www.tauss.de/service/presse/buessowheute6000morgen600000/

Ein Versuchsballon mit gefährlichem Flugziel

von Florian Steglich und Alvar C.H. Freude

Florian Steglich studiert Politikwissenschaft und Soziologie in Mainz und ist Mitarbeiter bei ODEM.org

Alvar C.H. Freude ist Diplom-Kommunikations-Designer, Medienkünstler, Internet-Entwickler und Initiator von ODEM.org

http://alvar.a-blast.org/

„Wenn ich das Milchtrinken verbieten will, muss ich erst mal ein oder zwei Flaschen beschlagnahmen.“

Mit diesen Worten gab Hans-Jürgen Riesenbeck, Vizepräsident der Bezirksregierung Düsseldorf, am 6. April 2002 einen Ausblick auf die weiteren Pläne seiner Behörde.

Die zwei Websites, die die Bezirksregierung *Ihnen* vorenthalten möchte, sind demnach nur der Anfang. Gary Lauck und die Stormfront-Seite dienen zur Etablierung einer weitreichenden Filter-Infrastruktur. Um dies durchzusetzen, die gesellschaftliche Ächtung des Rechtsextremismus mißbraucht. Wer die Entwicklung der letzten Jahre aufmerksam verfolgt hat realisiert schnell, wieviele Interessengruppen auf ein umfangreiches Filtersystem warten.

Auf der Bundeskonferenz der Regierungspräsidenten im Mai 2001 präsentierte der Düsseldorfer Amtsträger Jürgen Büssow seinen Kollegen Statistiken über mehr als 1500 „nicht-zulässige“ Internet-Seiten, die seine Bezirksregierung innerhalb von 27 Monaten mit dem Meldeformular auf ihrer Website gesammelt hatte[1]. Laut einer dpa-Meldung vom 16. Mai diesen Jahres kommen für den Regierungspräsidenten gar 6000 Seiten für eine Sperrung in Frage. Die Vermutung, dass es bis zum Mai des nächsten Jahres zu einer weiteren Vervierfachung dieser „Schwarzen Liste“ kommen könnte, ist nicht vollkommen abwegig.

[1] http://www.brd.nrw.de/cat/pdf/2268bundes_rpk_top2.pdf

Es geht nicht um die Meinungsfreiheit von Kriminellen

Niemand bezweifelt, dass einschlägige extremistische Webseiten sich nicht auf dem Boden unseres Grundgesetzes bewegen, sondern nicht selten gegen die freiheitlich-demokratische Grundordnung agitieren. Aber gerade aus diesem Grunde stellt sich die Frage, ob der Rückbau von Grundrechten die richtige Maßnahme ist, diesen Gefahren zu begegnen.

Wenn die Meinungsfreiheit missbraucht wird, kann sie eingeschränkt werden. So steht es im Grundgesetz und so geschieht es, wenn ein Autor (Content-Provider) von deutschem Boden aus strafbewehrte Inhalte ins Netz stellt. Im Falle unzulässiger Internet-Inhalte aus dem Ausland geht es aber nicht um die Meinungsfreiheit des Anbieters, sondern vorrangig um das Recht des „Sich-informieren-Dürfens" des Konsumenten, also die Informationsfreiheit oder Rezipientenfreiheit der Bürger, ebenso wie die Arbeit von Forschung und Lehre. Nicht beim Urheber setzen Sperrungen und Filter an, sondern beim Rezipienten – die beanstandeten Informationen sind weiterhin vorhanden.

Den hohen Stellenwert der Informationsfreiheit auch und gerade im Kontext einer ausländischen Quelle hat das Bundesverfassungsgericht bereits festgeschrieben. Im Fall „Einfuhrverbot / Leipziger Volkszeitung" (BVerfG 27, 71) konkretisierten die obersten deutschen Richter das Recht, sich aus „allgemein zugänglichen Quellen ungehindert zu unterrichten". „Ungehindert" bedeutet demnach frei von staatlicher Abschneidung, Behinderung, Lenkung, registrierung und sogar „frei von unzumutbarer Verzögerung". Das Recht, sich zu unterrichten, umfasst dabei explizit nicht nur die schlichte Entgegennahme, sondern auch das aktive Beschaffen von Informationen. Damit ist zugleich ein wichtiger Unterschied zwischen Medien wie dem Rundfunk und Medien wie dem Telefon oder Internet angesprochen. Das Netz ist Individualkommunikation, der Nutzer nicht passiver Empfänger der Informationen, sondern aktiv Abrufender.

Eine Sperrung von bestimmten Inhalten ist deshalb keineswegs verfassungskonform, sondern verstößt gegen Artikel 5 GG. Die Frage der Informationsfreiheit erachtet das Dezernat 21 der Bezirksregierung aber offenbar für nicht relevant.

Yahoo!, der neue französische Access-Provider

In einer aktuellen Pressemitteilung vom 13. September 2002 bezieht sich die Bezirksregierung auf zwei ähnliche Fälle, die die französische Justiz beschäftigten: Im einen Fall klagten Anti-Rassismus-Organisationen wegen Nazidevotionalien auf den US-Auktionsseiten von Yahoo.com gegen Yahoo.fr, im anderen Fall wurde der französische Providerverband AFA vor Gericht geladen, der den Zugang zur rechtsextremistischen Seite front14.org sperren sollte. Die Bezirksregierung schreibt in dieser Pressemitteilung beide Urteile der Firma Yahoo zu und macht diese Portalseite mal eben zum französischen Access-Provider.

Wer dies liest, den beschleichen bereits leise Zweifel, ob die Aufsicht über das Medium Internet bei der Düsseldorfer Behörde in den richtigen Händen liegt. Wenn Regierungsdirektor Schütte aber die mangelnde Wirksamkeit der Sperrungen mit Analogien zur Straßenverkehrsordnung zu entkräften sucht, offenbart er ein grundlegenderes Unverständnis für die Problematik im globalen Netz kollidierender Rechtsauffassungen. Ein Unverständnis, das wesentlich gravierendere Auswirkungen hat als einige Schnitzer in Pressemitteilungen.

Eine Diskussion findet nicht statt

Die Bezirksregierung sucht nicht den Dialog. Sie verweigert die Herausgabe von Unterlagen nach dem Informationsfreiheitsgesetz NRW und handelte sich damit eine Rüge der Landesbeauftragten für das Recht auf Information ein (für Details siehe auch http://odem.org/informationsfreiheit/ifg-bescheid.html – der überwiegende Teil der Dokumente fehlt noch heute). Sie illustriert ihre Grundsatzerklärung mit den widerlichsten Beispielen der Nazi-Sites und tabuisiert so eine Diskussion, die angesichts der ungeheuren Konsequenzen einer bundesweiten Umsetzung der Sperrverfügungen dringend nötig ist. Wer sich gegen die Pläne aus der Düsseldorfer Cecilienallee ausspricht, ist in der Defensive.

Wir brauchen eine sachliche und sachverständige Debatte über den Sinn und die Folgen zentraler wie dezentraler Netzfilter. Was wir nicht brauchen, sind emotionalisierende Rauchbomben, kurzfristige und oberflächliche Lösungen.

Strapaziert und doch notwendig: Medienkompetenz

Letztlich führt kein Weg vorbei am vielbemühten, aber selten mit Inhalten unterfütterten Begriff der Medienkompetenz. An der Fähigkeit, souverän mit technischen Geräten umzugehen, diese zu verstehen und zu beherrschen, anstatt sich von ihnen beherrschen zu lassen, fehlt es nicht nur der sogenannten Generation @. Daran fehlt es auch in den Kreisen der politischen Entscheidungsträger. Medienkompetenz muß mehr sein als wöchentliche 45 Minuten Textverarbeitung auf dem Stundenplan und eine @brd.nrw.de-Mailadresse.

Waffenscheinpflicht für Serverzugang

von Dr. Michael Charlier

Zuest erschienen am 19. Mai 2001 in der Frankfurter Rundschau

Michael Charlier ist Kulturwissenschaftler und Webwriter

http://www.charlier.de/

Wer auch bei Reizthemen kühlen Kopf bewahrt, stellt sich vielleicht einmal die Frage, was das eigentlich bedeutet, wenn z.B. der Düsseldorfer Regierungspräsident Büssow mit dem Alarmruf an die Öffentlichkeit geht, die Zahl der rechtsradikalen Sites im Internet habe sich in den letzten fünf Jahren mehr als verzehnfacht. Höchste Zeit also, jeden denkbaren Druck auf die Provider auszuüben, den Zugang zu diesen Sites zu sperren.

Weiß der Chef der obersten Aufsichtsbehörde nicht, daß es vor fünf Jahren, im Mai 1996, gerade einmal 18 619 deutsche Domains gab? Im Mai 2001 sind es nach Statistik[1] des DENIC weit über 4,4 Millionen. Natürlich kann man daraus nicht ableiten, das Internet sei in diesen 5 Jahren um exakt das 236-fache gewachsen – aber der Aufschrei des Aufsehers verliert doch etwas an Überzeugungskraft.

[1] http://www.denic.de/DENICdb/stats/domains_simple.html

Und dann sei doch einmal in aller Bescheidenheit die Frage gestellt, wer eigentlich bestimmt, was eine rechtsradikale Site ist, die sich nicht mehr auf die im Grundgesetzt garantierte Freiheit der Meinungsäußerung berufen kann. Daß der Umgang mit diesen Freiheitsgarantien im Rechtsstaat nicht so einfach ist, wie es der Ruf nach dem kurzen Prozess gerne hätte, sieht man ja an den Demonstrationen der NPD und nicht nur der: Die Polizeipräsidenten verbieten, die Verfassungsgerichte lassen zu. Wie soll denn die „schwarze Liste" zustandekommen, die 15 Jugendminister der EU-Staaten gefordert[2] haben, um den Providern zu sagen, welche Server sie bedienen dürfen und welche nicht?

[2] http://www.heise.de/newsticker/data/em-29.05.01-000/

Selbstmord aus Angst vor dem Tode?

Werden in Zukunft nur die Seiten abgeschaltet, die dumm genug sind, Hakenkreuz zu zeigen? Oder auch schon eine Seite der Jungen Union mit dem „Kinder statt-Inder"-Slogan? Reicht mein Anruf beim Provider, die Türkenwitze auf *http://www.meinvaterhatdoenerbudeoderwas.de/* entsprächen nicht meinem Geschmack, um das vom Netz zu nehmen? Bei wem kann sich der Autor beschweren? Das Internet dürfe kein rechtsfreier Raum sein, verlangt Büssow.[3] Aber als rechtsstaatsfreien Raum sähe er es schon gerne?

[3] http://www.heise.de/newsticker/data/em-28.05.01-000/

Den Verdacht wenigstens muß sich der SPD-Abgeordnete Peter Paul Gantzer nicht gefallen lassen: Er fordert eine staatliche Zertifizierung[4] für jeden, der etwas im Netz veröffentlichen will. Rechtlich ganz klar geregelt: Es ist alles verboten, was nicht ausdrücklich erlaubt ist. Waffenscheinpflicht für Serverzugang.

[4] http://www.heise.de/newsticker/data/dal-16.05.01-000/

Meinungsfreiheit ist ein schwieriges Ding, und ja: damit sind auch Risiken verbunden. Aber ist das ein Grund zum Selbstmord aus Angst vor dem Tode?

„Es muss nicht gleich eine »Bankrotterklärung staatlicher Souveränität« bedeuten, wenn man in Kauf nimmt, dass zwar manche Dinge im Internet auch für Deutsche zugänglich sind, die hierzulande verboten sind, aber dass dafür auch eine überstaatliche Meinungsfreiheit erhalten und gefördert wird, die letztlich der Demokratisierung der Weltgesellschaft dient."

Florian Rötzer in Telepolis
http://www.heise.de/tp/deutsch/inhalt/te/11306/1.html

Juristische Perspektive(n)

„Die netzseitige zentrale Filterung beim Access-Provider mithilfe einer eigenen Filterinfrastruktur – etwas demokratietheoretisch bedenklicheres kann man sich kaum vorstellen“

Jörg Tauss, MdB (SPD), Beauftragter für Neue Medien der SPD-Bundestagsfraktion am 30. Mai 2002
http://www.tauss.de/service/presse/buessowheute6000morgen600000/

Zusammenfassung einschlägiger Veröffentlichungen

von Andreas Neumann

Andreas Neumann ist Jurist und Mitglied im Redaktionsteam von artikel5.de

Weitere Informationen: http://andreasneumann.de/

Die Möglichkeit von Sperrungsanordnungen gegen Internet-Zugangsvermittler („Access-Provider“[1]) wurde schon bald nach Inkrafttreten des Mediendienstestaatsvertrags (MDStV) und des Teledienstegesetzes (TDG) in der Rechtswissenschaft diskutiert. Mangels praktischer Relevanz verstummte diese juristische Diskussion jedoch weitgehend, bis die Pläne der Bezirksregierung Düsseldorf zum Erlass von auf § 22 Abs. 2, 3 MDStV bzw. § 18 Abs. 2, 3 MDStV alter Fassung (a. F.) gestützten Sperrungsverfügungen bekannt wurden und die Debatte neu entfachten.

Nachfolgend soll, ohne Anspruch auf Vollständigkeit und insbesondere unter Verzicht auf die Einbeziehung der (vereinzelten) monographischen Abhandlungen zu diesem Thema, versucht werden, den Inhalt der einschlägigen Veröffentlichungen in einigermaßen chronologischer Reihenfolge kurz zusammenzufassen. Die Darstellung fokussiert dabei auf diejenigen Aspekte, die für die rechtliche Bewertung von Sperrungsanordnungen gegenüber Access-Providern von besonderer Relevanz sind. Sie zeigt, dass die Rechtswissenschaft noch weit von einer einheitlichen Linie hinsichtlich der Möglichkeit, der Voraussetzungen und der Rechtsgrundlage solcher Sperrungsanordnungen entfernt ist.

Auch wenn die Autoren sich in der Regel auf die alte Fassung des MDStV und dessen § 18 Abs. 2, 3 beziehen, wird im Folgenden auf die neue Fassung des MDStV und den in der Sache identischen § 22 Abs. 2, 3 verwiesen.

[1]
Es sei an dieser Stelle darauf hingewiesen, dass dieser Begriff verkürzend ist, da er nicht deutlich macht, wozu der Zugang vermittelt wird. Dennoch – und obwohl die in der Sache nicht gebotene Verwendung englischsprachiger Begriffe sprachästhetisch zumindest zweifelhaft ist – soll angesichts seiner Gängigkeit in dem hier diskutierten Bereich im Folgenden auf diesen Terminus zurückgegriffen werden.

Allgemeine Beiträge zu Sperrungsanordnungen

„(ein) Versuch (...), auch auf solche Angebote Einfluss zu nehmen, die außerhalb der Bundesrepublik auf einem Server gespeichert sind“

Vesting, Thomas: Kommentar zu § 18 MDStV, in: Roßnagel (Hrsg.), Recht der Multimedia-Dienste, Loseblattsammlung, Grundwerk, 1999:

Im Rahmen seiner Kommentierung zu § 18 MDStV a. F., dem heutigen § 22 MDStV, hält Vesting Aufsichtsmaßnahmen auch gegen Access-Provider für möglich. Dies gelte jedoch nur, soweit Maßnahmen gegenüber Inhalteanbietern und „Service-Providern“ zur Sperrung von Angeboten keinen Erfolg versprechen, und betreffe insbesondere Fälle, in denen die Angebote auf Servern außerhalb der Bundesrepublik Deutschland gespeichert sind. Während dem begrenzenden Kriterium der technischen Möglichkeit keine nennenswerte praktische Bedeutung zukomme, seien solche Maßnahmen jedoch am normativen Element der Zumutbarkeit zu messen, das eine Abwägung zwischen der Belastung des Anbieters und dem durch die Verbreitung des Inhalts bedrohten oder verletzten Rechtsgut erfordert. In einer abschließenden Würdigung bezeichnet Vesting die kommentierte Vorschrift allerdings angesichts der seiner Ansicht nach nicht hinreichend komplexitätsgerechten Regulierung als „Produkt und Ausdruck eines ‚neoliberalen‘ Zeitgeistes, dem offensichtlich die Grundeinsichten liberalen Denkens abhanden gekommen sind“.

„Anwendung des MDStV auf Access-Provider findet (...) im Gesetz keine Stütze“

Koenig, Christian / Loetz, Sascha, Sperrungsanordnungen gegenüber Network- und Access-Providern, CR 1999, 438:

Online unter: *http://www.artikel5.de/sperrungsanordnungen.html*

Nach der Auffassung von Koenig und Loetz bieten Access-Provider zwar keinen Teledienst an, unterfallen aber aufgrund § 3 Nr. 1 TDG als Zugangsvermittler dem Begriff des Diensteanbieters. Sperrungsmaßnahmen im Sinne des § 5 Abs. 4 TDG a. F. ließen sich jedoch nicht gegen Access-Provider richten. Dies ergebe sich u. a. daraus, dass sich inkrimierte Inhalte regelmäßig auf ausländischen Servern befinden und von daher die Gefahr der im Widerspruch zur Gesetzessystematik stehenden Inanspruchnahme von Access-Providern für das Verhalten Dritter in einer Vielzahl von Fällen bestehe. Maßnahmen gegen Access-Provider kommen nach Auffassung der Autoren lediglich als die Inanspruchnahme von Nichtstörern in Betracht, für welche allerdings strengere Eingriffsvoraussetzungen gelten und die zugleich einen Ausgleichsanspruch für den Nichtstörer zur Folge haben können. Gänzlich ausscheiden müssten hingegen Maßnahmen auf Grundlage des § 22 Abs. 3 MDStV, da der rein wirtschaftliche Vorgang der Datenübermittlung ohne Bezug zum übermittelten Inhalt ausschließlich in den bundesrechtlichen Regelungsbereich falle. Des Weiteren bestünden gegenüber an Access-Provider gerichtete Sperrungsanordnungen aber auch erhebliche gemeinschaftsrechtliche Bedenken, da sie zu einer faktisch diskriminierenden Beschränkung der primärrechtlich gewährleisteten Dienstleistungsfreiheit führen.

[Zu: Das Internet ist kein rechtsfreier Raum]:

„(...) aber es ist ein Raum, in dem verschiedene Rechtssysteme auf neue Weise kollidieren können. Die Lösung kann vernünftigerweise nicht darin bestehen, dass alle souveränen Staaten ihr nationales Recht auf die ganze Welt ausdehnen, was für das Internet bedeuten würde, dass es entweder eine Unzahl ineinander verschachtelter Blockade- und Filterschichten oder überwachter Grenzen auf Seiten der Zugangsprovider oder der Content-Anbieter geben müsste.“

Florian Rötzer in Telepolis
http://www.heise.de/tp/deutsch/inhalt/te/11306/1.html

„schwierige Fragen im Hinblick auf die Verhältnismäßigkeit“

Zimmermann, Andreas: Polizeiliche Gefahrenabwehr und das Internet, NJW 1999, 3145:

Zimmermann hält die Haftungsprivilegierungen des TDG und des MDStV für unbeachtlich im Hinblick auf ordnungsbehördliche Maßnahmen, was für den Bereich der Teledienste auch von § 5 Abs. 4 TDG a. F. bestätigt werde. Für den Bereich der Mediendienste stelle § 22 Abs. 3 MDStV außer Streit, dass unter den dort normierten engen Voraussetzungen auch bloße Zugangsanbieter grundsätzlich als Adressaten einer Sperrungsanordnung in Betracht kommen. Im Bereich der Teledienste komme eine Inanspruchnahme etwaiger Zugangsanbieter nur als Nichtstörer in Betracht. Damit sind nach Auffassung Zimmermanns Sperrungsanordnungen gegenüber Zugangsanbietern überhaupt nur möglich, wenn Maßnahmen gegenüber dem jeweiligen Inhalte- oder „Serviceanbieter“ keine Aussicht auf Erfolg haben. Dies könne beispielsweise der Fall sein, wenn sich diese Anbieter im Ausland befinden. In der anschließenden Betrachtung der durch eine Sperrungsanordnung gegenüber Access-Providern aufgeworfenen Verhältnismäßigkeitsfragen verweist Zimmermann zunächst auf die technischen Ausweichmöglichkeiten der Nutzer. Diese würden regelmäßig zu erheblichen Problemen im Hinblick auf die Geeignetheit solcher Anordnungen führen. Bei der Beurteilung der Erforderlichkeit gelte es insbesondere auch zu berücksichtigen, gegenüber wie vielen Nutzern der in Rede stehende Eingriff wirksam wird, und ob nicht die Möglichkeit besteht, nicht alle, sondern nur einzelne Internet-Dienste zu sperren. Im Rahmen der Angemessenheit stellt Zimmermann beispielhaft auf die Anordnung der Installation von Proxy-Servern bei Zugangsanbietern ab. Eine solche Maßnahme sei zwar nicht von vornherein und generell unzumutbar. Es müsse insoweit jedoch auch berücksichtigt werden, dass die Einrichtung und kontinuierliche Anpassung eines solchen Systems einen erheblichen technischen Aufwand bedeute, und dass überdies zur Verhinderung von Umgehungen derartige Verpflichtungen allen in Deutschland tätigen Zugangsanbietern auferlegt werden müssten.

„Ich will mir nicht vorschreiben lassen, welche Räume ich im Internet betreten kann und welche nicht.“

Angela Marquardt, MdB (PDS), medien- und technologiepolitische Sprecherin, Mitglied Unterausschuss Neue Medien

„gewisse Zweifel an der Geeignetheit einer solchen Maßnahme“

Schuhmacher, Dirk: Sperrungsverpflichtungen für Access-Provider bezüglich des Zugangs zu Webseiten mit rechtswidrigen Inhalten:

Online unter: *http://www.dfn.de/service/ra/checkliste/SperrungAccessProvider.html*

Schuhmacher hält eine auf das Polizei- und Ordnungsrecht gestützte Verfügung gegen Access-Provider zur Sperrung bestimmter WWW-Seiten grundsätzlich für möglich. Allerdings sei die Geeignetheit einer solchen Maßnahme zweifelhaft. Überdies müsse der Access-Provider wohl als Nichtstörer gelten, so dass eine Sperrungsanordnung nur unter engen Voraussetzungen möglich sei. Schließlich sei aber auch zu beachten, dass bei der Vielzahl der im Internet vorhandenen rechtswidrigen Inhalte eine Vielzahl von Sperrungsverfügungen zu erwarten sein könnte. Die dadurch bedingte ständige Erweiterung und Verwaltung der Listen der gesperrten Seiten und Server könne aber zu einem unzumutbaren Aufwand auf Seiten der Access-Provider führen und überdies erhebliche Leistungseinbußen bei der Abwicklung des Datenverkehrs zur Folge haben.

„Access-Provider (sind) (...) im Grundsatz taugliche Adressaten von Aufsichtsmaßnahmen“

Hornig, Michael: Möglichkeiten des Ordnungsrechts bei der Bekämpfung rechtsextremistischer Inhalte im Internet, ZUM 2001, 846

Online: *http://www.jurawelt.com/download/aufsaetze/zum-artikel.pdf*

Hornig weist zunächst darauf hin, dass Sperrungen auf Grundlage des § 22 Abs. 3: MDStV nur als Ultima Ratio in Betracht kommen. Auch angesichts der Schwierigkeit, die Sperrungen technisch auf die inkrimierten Inhalte zu beschränken, sei mit Sperrungsanordnungen behutsam umzugehen. § 22 Abs. 3 MDStV sei allerdings keine Subsidiarität der Inanspruchnahme des Access-Providers zu entnehmen. Vielmehr bestimme sich die Möglichkeit, Maßnahmen gegen diesen (und nicht gegen den Inhalteanbieter oder denjenigen, der den rechtswidrigen Inhalt für diesen speichert) zu ergreifen, ausschließlich nach dem Verhältnismäßigkeitsprinzip. Insoweit sei vor allem auch der Gedanke der Effektivität ordnungsrechtlichen Handelns zu berücksichtigen, der es durchaus erlauben könne, Ordnungsmaßnahmen auch gegen nachrangig oder sogar nicht verantwortliche Personen zu richten. Dieser Gesichtspunkt sei insbesondere dann relevant, wenn sich die eigentlich verantwortlichen Personen im für die Ordnungsbehörden unerreichbaren Ausland befinden. Damit seien Access-Provider grundsätzlich taugliche Adressaten von

Aufsichtsmaßnahmen auf Grundlage des § 22 Abs. 2, 3 MDStV, obwohl hierbei aber auch die technischen Besonderheiten der Internet-Kommunikation berücksichtigt werden müssten.

> **Anmerkung:** Der Beitrag besteht zu einem großen Teil aus (wertvollen) rechtspolitischen und soziologischen Erwägungen. Auf weichenstellende rechtsdogmatische Fragen, wie insbesondere die Anwendbarkeit des Mediendienstestaatsvertrags auf Access-Provider, wird indes nicht eingegangen, die Möglichkeit, Sperrungsanordnungen gegen Access-Provider auf § 22 Abs. 2, 3 MDStV zu stützen, vielmehr unterstellt.

Beiträge zu Sperrungsanordnungen mit Bezugnahme auf die Verfügungen der Bezirksregierung Düsseldorf

„Die von der Bezirksregierung Düsseldorf ins Auge gefasste Konstruktion (...) ist fehlerhaft."

Hoeren, Thomas: Stellungnahme zur geplanten Sperrungsverfügung der Bezirksregierung Düsseldorf (Anhörung am 13.11.2001):

Online: *http://odem.org/zensur/stellungnahme-prof-hoeren.pdf*

In seiner Stellungnahme bezweifelt Hoeren bereits die Einordnung der in Rede stehenden WWW-Seiten als Mediendienste. Vielmehr spräche viel dafür, dass es sich um Teledienste handele und daher mit § 22 Abs. 3 MDStV die falsche Rechtsgrundlage gewählt wurde. Darüber hinaus seien reine Access-Provider aber auch bereits keine Diensteanbieter im Sinne des MDStV. Des Weiteren sei zu berücksichtigen, dass die Sperrung der WWW-Seiten einerseits erheblichen sachlichen und personellen Aufwand erfordert, andererseits aber leicht umgangen werden könne, so dass sie den Access-Providern nicht zumutbar sei. Außerdem werfe insbesondere der Einsatz von Proxy-Servern erhebliche Folgeprobleme mit Blick auf das allgemeine Persönlichkeitsrecht, das Fernmeldegeheimnis und ggf. auch die Wissenschaftsfreiheit der Nutzer auf. Diese Überlegungen seien im Übrigen auch zu berücksichtigen, wenn man die Sperrungsanordnung auf das allgemeine Ordnungsrecht stützen wollte. Qualifiziere man die Access-Provider dabei als Nichtstörer, komme überdies ein Entschädigungsanspruch in Betracht.

„Sperrungsverfügungen (...) werfen (...) bereits mit Blick auf die Informationsfreiheit verfassungsrechtlich intrikate Probleme auf"

Neumann, Andreas, Ordnungsrechtliche Sperrungsverfügungen und die Informationsfreiheit nach Art. 5 Abs. 1 S. 1 2. Alt. GG:

Online: *http://www.artikel5.de/artikel/sperrunginffreiheit.html*

In diesem Aufsatz wird ausschließlich darauf hingewiesen, dass die Sperrungsverfügungen in den Schutzbereich des Grundrechts der Informationsfreiheit eingreifen. Die Ausführungen der Bezirksregierung Düsseldorf lassen dabei nach Ansicht des Verfassers erkennen, dass die Bezirksregierung vermutlich einer grundsätzlich falschen Auffassung von Tragweite und Bedeutung dieses Grundrechts anhängt.

„Die selbsternannten Repräsentanten der angeblichen Internetgemeinde (können sich) immer noch nicht mit der Geltung staatlichen Rechts (...) abfinden."

Mankowski, Peter, Die Düsseldorfer Sperrungsverfügung – alles andere als rheinischer Karneval, MMR 2002, 277:

In seinem MMR-Editorial weist Mankowski den gegen die Sperrungsanordnungen erhobenen Vorwurf der Zensur zurück. Auch gebe es kein Grundrecht auf passive Informationsfreiheit. Darüber hinaus sei es auch richtig, die Access-Provider in die Pflicht zu nehmen, da diese einerseits den Profit aus der Zugangsvermittlung realisieren wollten, die Lasten jedoch der Allgemeinheit aufbürdeten. Die Sperrungsanordnungen der Bezirksregierung Düsseldorf verursachen nach Auffassung Mankowskis auch weder große Kosten noch Mühen und seien daher verhältnismäßig. Es stehe zwar sicher zu erwarten, dass die Betreiber der inkrimierten WWW-Seiten zu Umgehungsmaßnahmen greifen werden. Dies dürfe jedoch nicht zur Kapitulation von Staat und Gesellschaft führen. Vielmehr sei es durchaus möglich, jedenfalls für das Normalpublikum ohne Sonderwissen den Zugang zu den inkrimierten Seiten zu sperren. Unklar sei im konkreten Fall lediglich, ob der MDStV eine rechtfertigende Eingriffsermächtigung „erhält" (sic!).

> **Anmerkung:** Das Editorial ist nicht nur – wie es für diese Textform durchaus üblich und angemessen ist – in hohem Maße polemisch, es ist auch in hohem Maße angreifbar. Den Vorwurf der Zensur, gegen den sich Mankowski entschieden wendet, hat in der wissenschaftlichen Fachdiskussion, soweit ersichtlich, niemand erhoben. Neben diese juristische

Spiegelfechterei treten aber erhebliche fachliche Angriffsflächen. Wer behauptet, es gebe „kein Grundrecht auf passive Informationsfreiheit, also auf Zugriff auf bestimmte Informationsquellen“, sieht sich nicht nur der sprachlogischen Frage ausgesetzt, warum er einen (notwendig aktiven) Zugriff auf bestimmte Informationsquellen mit dem Begriff der „passiven Informationsfreiheit“ bezeichnet. Er dürfte überdies die Reichweite der in Art. 5 Abs. 1 S. 1 Alt. 2 GG garantierten Informationsfreiheit verkennen, die in den Worten des Bundesverfassungsgerichts neben der aktiven Informationsbeschaffung gerade „auch die schlichte Entgegennahme von Informationen“ schützt. Aus rechtsdogmatischer Sicht ungenau wirkt schließlich der Hinweis, dass WWW-Seiten kein Mittel der Individualkommunikation seien und daher „kein Briefgeheimnis für sich beanspruchen können“. Niemand hält ernstlich das Briefgeheimnis für einschlägig – vielmehr wird das ebenfalls in Art. 10 GG garantierte Fernmeldegeheimnis als betroffene Grundrechtsgarantie in Betracht gezogen.

„Alternativen zur Inanspruchnahme der Access-Provider stehen nicht zur Verfügung“

Schütte, Jürgen, Sperrung von Internet-Seiten mit verbotenem Inhalt – Und es geht doch ..., NJW 23/2002, III:

Das NJW-Editorial von Schütte, Regierungsdirektor im Dienste der Bezirksregierung Düsseldorf, zeichnet in erster Linie die Vorgänge nach und benennt die unterschiedlichen Positionen. Für den Fall, dass die Gerichte die derzeit bekannten technischen Sperrmethoden generell für ungeeignet halten sollten, sieht Schütte die Frage der Verfassungskonformität des MDStV gestellt, da der Staatsvertrag bzw. seine Verfasser davon ausgehe/ausgingen, dass es auch notwendige und rechtmäßige Sperrungen bei den Zugangsanbietern geben könne.

„Anordnungen gegenüber Access-Providern zur Sperrung rechtsradikaler Webangebote (sind) regelmäßig als nicht verhältnismäßig einzustufen“

Stadler, Thomas, Sperrungsverfügung gegen Access-Provider, MMR 2002, 343:

Online: *http://www.jurawelt.com/aufsaetze/5520*

Stadler hält § 22 MDStV grundsätzlich für verfassungswidrig, da die Vorschrift gegen den Verfassungsgrundsatz der Polizeifestigkeit der Presse verstoße, wenn man, im Gegensatz zu den Landesgesetzgebern, den Pressebegriff des Art. 5 Abs. 1 S. 2 GG richtigerweise auf alle im Internet veröffentlichten Inhalten erstreckt, denen eine gewisse publizistische Relevanz zukommt. Aufgrund der Bestimmung des Geltungsbereichs in § 2 MDStV/TDG unterfallen Access-Provider darüber hinaus nach Auffassung Stadlers nicht dem MDStV (und auch nicht dem TDG), so dass schon aus diesem Grund Sperrungsanordnungen gegen Access-Provider nicht auf § 22 Abs. 3 MDStV gestützt werden könnten. Doch selbst, wenn man anderer Ansicht sei, könne auf § 22 MDStV jedenfalls nicht zur Sperrung des Zugangs zu Telediensten zurückgegriffen werden. Bei der Untersuchung der Verhältnismäßigkeit der von der Bezirksregierung Düsseldorf angesprochenen Sperrungsmaßnahmen stellt Stadler zunächst fest, dass dieses Vorgehen mit Blick auf die korrekte Ermessensausübung zweifelhaft ist und jedenfalls zur Rechtswidrigkeit des gesamten Sperrungsbescheids führen muss, sobald auch nur eine der von der Bezirksregierung angebotenen Maßnahmen unverhältnismäßig ist. Anschließend verneint Stadler die Verhältnismäßigkeit aller drei Handlungsoptionen: Eingriffe am DNS-Server des Access-Providers seien leicht zu umgehen und daher nicht geeignet, den Sperrungszweck zu erreichen. Die Blockade von IP-Adressen verhindere auch den Zugang zu einer Vielzahl nicht rechtswidriger Angebote und sei überdies ebenfalls sehr einfach zu umgehen. Und der Einsatz von Proxy-Servern erfordere nicht nur einen erheblichen technischen Aufwand und führe zu spürbaren Leistungseinbußen, sondern erfasse überdies nicht lediglich den Zugang zu Mediendiensten und sei schon deshalb rechtswidrig. Darüber hinaus tragen die Sperrungsverfügungen der Bezirksregierung Düsseldorf nach Ansicht Stadlers dem durch sie betroffenen Grundrecht der Informationsfreiheit und den Interessen der Allgemeinheit nicht hinreichend Rechnung, was seinerseits dazu führe, dass Anordnungen gegenüber Access-Providern zur Sperrung rechtsradikaler WWW-Angebote regelmäßig nicht verhältnismäßig seien. Schließlich weist Stadler auch noch darauf hin, dass den Access-Providern im Falle der Inanspruchnahme durch eine Sperrungsanordnung jedenfalls ein Entschädigungsanspruch zustehe.

„Man stelle sich einmal das Szenario vor, dass ein Access-Provider womöglich täglich aufgefordert wird, Hunderte von Seiten mit verbotenen Inhalten zu sperren und ebenso viele mit zwischenzeitlich zulässigem Content zu entsperren.“

Tobias H. Strömer, Rechtsanwalt, Düsseldorf
http://www.heise.de/newsticker/data/hod-13.11.01-000/

„Die Sperrungsverfügungen (waren) im konkreten Fall verhältnismäßig“

Greiner, Arved, Sperrungsverfügungen als Mittel der Gefahrenabwehr im Internet, CR 2002, 620:

Obwohl Greiner die sonstigen Voraussetzungen des § 22 Abs. 2, 3 MDStV im Falle der Sperrungsverfügungen der Bezirksregierung Düsseldorf als gegeben ansieht, hält er die Internet-Zugangsvermittlung für einen dem TKG unterfallenden Telekommunikationsdienst, so dass nach seiner Auffassung gegen Access-Provider nicht auf Grundlage des MDStV eingeschritten werden kann. Greiner hält jedoch Maßnahmen auf Grundlage der polizei- und ordnungsrechtlichen Generalklausel für möglich. Die Sperrungsverfügungen der Bezirksregierung sind des Weiteren seiner Auffassung nach geeignet, da sie den Zugriff auf die zu sperrenden Angebote wenigstens erschweren, und erforderlich. Bei der Prüfung der Angemessenheit bemängelt Greiner, dass die Bezirksregierung in diese Prüfung eine Vielzahl von einschlägigen Grundrechten (Meinungsfreiheit der Inhalteanbieter, Informationsfreiheit und Fernmeldegeheimnis der Nutzer) nicht eingestellt habe. Im Ergebnis rechtfertige aber im konkreten Fall das öffentliche Interesse an der Bekämpfung der zu sperrenden Inhalte diese Grundrechtseingriffe.

> **Anmerkung:** Die Güterabwägung im Rahmen der Prüfung der Angemessenheit fällt bei Greiner sehr knapp und apodiktisch aus. Ob man angesichts des von ihm bejahten Eingriffs in das Fernmeldegeheimnis jeden Nutzers wirklich von einer „insgesamt eher als gering einzuschätzenden Eingriffsintensität“ sprechen kann, scheint eher fraglich, insbesondere wenn man ähnliche Konstellationen ins Auge fasst (vgl. etwa § 100g Abs. 2 StPO).

„Die Sinnfrage bleibt (...) nach wie vor virulent.“

Spindler, Gerald / Volkmann, Christian, Die öffentlich-rechtliche Störerhaftung der Access-Provider, K & R 2002, 398:

Die Autoren gehen davon aus, dass Internet-Zugangsvermittlung zwar kein Tele- oder Mediendienst ist, Access-Provider aufgrund § 3 Nr. 1 TDG/MDStV jedoch Dienstean-bieter im Sinne des TDG bzw. MDStV sind. Sperrungsverfügungen gegen Access-Provider seien damit je nach dem konkreten Inhalt, zu dem der Zugang vermittelt wird, entweder auf § 22 Abs. 2, 3 MDStV oder auf die polizeiliche Generalklausel zu stützen. In letzterem Falle gelte es jedoch zu beachten, dass Access-Provider nur als Nichtstörer in Anspruch genommen werden können, also insbesondere nur im Ausnahmefall und nur zur Beseitigung von Gefahren für bedeutsame Rechtsgüter. Diese Einschränkungen müssen Spindler und Volkmann zufolge aufgrund der zugrunde liegenden verfassungsrechtlichen Wertungen auch im Anwendungsbereich des § 22 Abs. 3 MDStV berücksichtigt werden. Damit seien u. a. strenge Anforderungen an die Unmöglichkeit oder Aussichtslosigkeit von Maßnahmen gegen Content- und Host-Provider zu stellen. Bei Inlandssachverhalten dürften Sperrungsanordnungen generell unzulässig sein. Darüber hinaus bestehe eine Pflicht zur Entschädigung der in Anspruch genommenen Access-Provider.
Bei der Prüfung der Verhältnismäßigkeit von Sperrungsanordnungen bejahen die Autoren deren Geeignetheit und Erforderlichkeit. Im Rahmen der Untersuchung der Angemessenheit nennen sie zunächst die von den Sperrungsanordnungen tangierten Grundrechte (Berufs- und Eigentumsgrundrecht der Access-Provider, Meinungs- und Pressefreiheit der Inhalteanbieter, Informationsfreiheit der Nutzer). Der Eingriff in diese Grundrechte sei jedoch bei der Sperrung von kriegsverherrlichenden oder volksverhetzenden Inhalte verfassungsrechtlich gerechtfertigt. Allerdings dürfe der Eingriff nicht auch zur Sperrung des Zugangs zu legalen Inhalten führen. Die Blockade von IP-Adressen müsse daher ausscheiden. Die Installierung von Proxy-Servern, insbesondere aber zielgerichtete Sperrungen einzelner Webseiten sowie der Ausschluss von Domains am DNS-Server könnten hingegen angemessene Maßnahmen sein. Aus allgemeinen Erwägungen sei den Behörden jedoch nahezulegen, bei der Verfügung von Sperrungen größere Zurückhaltung zu üben.

„Elektronische Medien [...] bilden [...] einen Ausdruck gesellschaftlicher Grundüberzeugungen und sind ein Teil der Antwort auf die Frage, in was für eine Gesellschaft wir leben wollen. Freie Medien und Meinungsvielfalt sowie die freie, selbstbestimmte Kommunikation von Bürgerinnen und Bürgern sind kein Luxus, den wir uns leisten. Beides ist vielmehr die Voraussetzung für ein freies, offenes, pluralistisches und auch demokratisches Gemeinwesen.

.“

Jörg Tauss, MdB (SPD), Beauftragter für Neue Medien der SPD-Bundestagsfraktion am 13. Juni 2002
http://www.tauss.de/service/dokumente/texte/medienordnungtauss/

Der Widerspruchsbescheid zur Düsseldorfer Sperrungsverfügung:

Anmerkungen

von Rechtsanwalt Thomas Stadler

Thomas Stadler ist Rechtsanwalt in Freising

Gegen die Sperrungsverfügungen der Bezirksregierung Düsseldorf vom 06.02.2002 haben insgesamt 38 Provider Widerspruch eingelegt. Diese Widersprüche hatten aufschiebende Wirkung, mit der Folge, dass die Sperrungsanordnungen gegen die widersprechenden Provider nicht vollzogen werden konnten.

Da die Bezirksregierung zugleich Widerspruchsbehörde ist, hat sie zwischenzeitlich – beginnend Ende Juli 2002 – Widerspruchsbescheide erlassen, mit denen die Widersprüche erwartungsgemäß als unbegründet zurückgewiesen worden sind. Gegen diese Widerspruchsbescheide steht den betroffenen Providern nunmehr die Klage zum Verwaltungsgericht offen. Die Bezirksregierung hat einen Musterwiderspruchsbescheid ins Netz gestellt, weshalb davon auszugehen ist, dass an alle betroffenen Provider wortgleiche Bescheide versandt worden sind und auf die jeweilige Widerspruchsbegründung nicht einzeln eingegangen wurde.v

Die Bezirksregierung hat ihre Ausführungen aus dem Ausgangsbescheid in einigen Punkten ergänzt, verarbeitet aber gleichwohl nicht alle juristischen Kritikpunkte, die in der Diskussion der letzten Monate vorgebracht worden sind.

Interessant ist vor allem, dass die Behörde nunmehr auch die Möglichkeit in Betracht zieht, dass es sich bei den zu sperrenden Angeboten nicht um Medievndienste handelt. Die Bezirksregierung sah sich außerdem veranlasst, den Begriff der Sperrung nochmals näher zu betrachten, nachdem des öfteren die Ansicht vertreten worden ist,

Maßnahmen gegen den Access-Provider seien bereits im Wvcortsinne keine Sperrung. Auffällig ist zudem der Versuch, die Argumentation zur Rechtmäßigkeit der Sperrungsmaßnahmen nunmehr auf Eingriffe am DNS-Server zu beschränken, während die Ausgangsbescheide noch ausdrücklich die Blockade von IP-Adressen sowie den Einsatz von Proxy-Servern als Instrument der Sperrung genannt hatten und den Providern insoweit die Wahl gelassen wurde.

1. Ermessensspielräume könnten zu rechtswidrigen Sperrungen führen

Die zuletzt geschilderte Vorgehensweise ist deshalb problematisch, weil einerseits Teile der der Behörde obliegenden Ermessensentscheidung dem Provider überlassen werden und andererseits alle drei Sperrungsalternativen rechtmäßig sein müssen, da andernfalls die Gefahr besteht, dass sich der Provider, dem die Auswahl überlassen wurde, gerade für diejenige Variante entscheidet, die rechtswidrig ist.

Die Bezirksregierung meint im Widerspruchsbescheid demgegenüber, die Ansicht, sie würde Teile ihrer Ermessensentscheidung den Providern überlassen, sei vom Gesetzeswortlaut nicht gedeckt. Da sich die allgemeinen Grundsätze der pflicht- und ordnungsgemäßen Ermessensausübung regelmäßig nicht aus dem Wortlaut der Eingriffsnorm ergeben, sondern vielmehr Ausfluss des Grundsatzes der Gesetzmäßigkeit der Verwaltung sind, ist der Einwand der Behörde erstaunlich.

Der Wortlaut von § 18 Abs. 2 MDStV a.F. (§ 22 Abs. 2 n.F.) besagt, dass die Aufsichtsbehörde die zur Beseitigung des Verstoßes erforderlichen Maßnahmen trifft und insoweit insbesondere die Untersagung und Sperrung von Angeboten anordnen kann. Bereits der Gesetzeswortlaut zeigt daher überdeutlich, dass der Bezirksregierung ein sog. Auswahlermessen zukommt. [1] Dies bedeutet, dass die Behörde unter mehreren in Betracht kommenden zulässigen Maßnahmen grundsätzlich eine bestimmte auszuwählen und anzuordnen hat. [2] Die Bezirksregierung hat aber lediglich eine Art Vorauswahl getroffen und die endgültige Festlegung der Sperrmaßnahme dem Provider überlassen. Die Behörde geht damit jedenfalls das Risiko ein, dass ihr Verwaltungsakt nicht mehr bestimmt genug ist. Außerdem muss, wenn wie im konkreten Fall dem Provider die Auswahl zwischen drei Möglichkeiten überlassen bleibt, sichergestellt sein, dass jede der drei Alternativen für sich betrachtet rechtmäßig ist. Ist nur eine der drei Varianten rechtswidrig, so kann die Verfügung insgesamt nicht mehr rechtmäßig sein, da stets die Möglichkeit besteht, dass sich der Provider im Rahmen der ihm überlassenen Auswahl für die rechtswidrige Variante entscheidet.

Es ist aus diesem Grunde nicht ausreichend, wenn die Bezirksregierung im Widerspruchsbescheid dahingehend argumentiert, dass jedenfalls die DNS-Sperrung rechtmäßig sei.

In diesem Zusammenhang ist vor allem folgende Passage des Widerspruchsbescheids hervor zu heben: „Da die DNS-Sperrung zielgenau ist und durch sie nur das konkret gesperrte Internet-Angebot unzugänglich gemacht wird, besteht auch nicht die Gefahr, dass andere, rechtmäßige Angebote gesperrt werden."

Die Bezirksregierung gibt in dieser Passage zu erkennen, dass ihr offenbar bewusst geworden ist, dass die ebenfalls von ihr vorgeschlagenen Maßnahmen der IP-Blockade und des Einsatzes von Proxy-Servern diese zielgenaue Unterbindung einzelner Inhalte nicht gewährleisten, sondern bei diesen Maßnahmen vielmehr die Gefahr besteht, dass in großem Umfang andere, rechtmäßige Angebote ebenfalls blockiert bzw. mitgesperrt werden.

Aber auch die sog. DNS-Sperrung kann bei näherer Betrachtung nicht als wirklich zielgenau bezeichnet werden. Die DNS-Sperrung beeinträchtigt neben dem WWW-Dienst auch den Maildienst der zu sperrenden Domain. Damit wird neben einem Tele- oder Mediendienst auch die Individualkommunikation via E-Mail unterbunden. Auch diesen „Nebeneffekt" hat die Bezirksregierung bisher außer Acht gelassen.

2. Bezeichnung als „Sperrung" wegen mangelnder Geeignetheit unzutreffend

Bemerkenswert ist außerdem die Tatsache, dass die Bezirksregierung nunmehr die Notwendigkeit sieht, den Begriff der Sperrung i.S.d. MDStV näher zu erläutern, um dann erwartungsgemäß zum Ergebnis zu gelangen, dass es sich bei den von ihr angeordneten Maßnahmen um Sperrungen im Sinne des Gesetzes handelt.

Interessant ist hierbei der von der Bezirksregierung gewählte Ausgangspunkt. Die Behörde geht davon aus, dass unter einer Sperrung nach dem allgemeinen Sprachgebrauch die Verhinderung des Zugangs zu dem verbotenen Angebot durch den jeweiligen Anbieter, zu verstehen sei. Dieser Ansatz legt es nahe, eine Sperrung zunächst nur dann anzunehmen, wenn der Content- oder Host- Provider das Angebot entfernt oder zumindest dafür sorgt, dass es grundsätzlich nicht mehr allgemein durch beliebige Nutzer des Web aufgerufen werden kann. Die Sperrung erfolgt also grundsätzlich durch einen Zugriff auf den speichernden Rechner und nicht dadurch, dass ein bloßer Access-Provider ein fremdes Angebot vor seinen eigenen Kunden versteckt. Da der Gesetzgeber in § 18 Abs. 2, Abs. 3 MDStV ausdrücklich aber auch Sperrungsmaßnahmen gegenüber Access-Providern als denkbar ansieht, ist der Bezirksregierung zumindest zuzugeben, dass man ihren Maßnahmen nicht allgemein den Charakter von Sperrungsverfügungen i.S.d. MDStV absprechen kann. Gleichwohl wird man ausgehend vom Wortlaut der Norm und dem allgemeinen Sprachverständnis zumindest hinsichtlich der Wirksamkeit einer solchen Maßnahme ein hohes Niveau verlangen müssen. Eine Maßnahme, die ohne nennenswerten Aufwand praktisch von jedermann zu umgehen ist, verdient die Bezeichnung als Sperrung nicht.

Auch wenn die Möglichkeit der Umgehung von Sperrungen nicht notwendigerweise die Rechtmäßigkeit einer Anordnung gegenüber einem Access-Provider in Frage stellt, so darf es andererseits aber auch nicht so sein, dass die Sperrungsmaßnahme beliebig, ohne größeren Aufwand umgangen werden kann. Dies scheint auch die Bezirksregierung so zu sehen, weshalb sie versucht, die z.B. vom CCC erläuterte Möglichkeit auf einen anderen DNS-Server zu wechseln, als für den Durchschnittsuser zu schwierig darzustellen. Es mag zwar sein, dass diese an sich sehr einfache Anleitung für eine Reihe von Internetnutzern immer noch zu schwierig ist, dennoch geht die Ansicht der Bezirksregierung, dass dies auf die Mehrzahl der Internetnutzer zutreffen würde, an der Realität vorbei. Wer mit den typischen Programmen, die heute üblicherweise auf einem durchschnittlichen Privat-PC vorhanden sind, einigermaßen umgehen kann, der ist auch ohne weiteres in der Lage, die eher triviale Anleitung zur Änderung des DNS-Servers umzusetzen. Man sollte zudem berücksichtigen, dass solche Maßnahmen wirkungslos bleiben, wenn unmittelbar die IP-Adresse eingegeben wird, oder der Nutzer einfach mittels der zahlreich vorhandenen Internet-By-Call-Anbieter einen anderen Zugang wählt. Wer die entsprechenden Inhalte also betrachten will, kann dies ohne größeren Aufwand auch dann tun, wenn sein Access-Provider den entsprechenden Eintrag am DNS-Server verändert hat. Die Umgehung einer Sperrung impliziert m.E. demgegenüber allerdings, dass eine zumindest nicht unbeträchtliche Hürde überwunden werden muss. Das trifft auf die von der Bezirksregierung als DNS-Sperrung bezeichnete Maßnahme nicht zu, weshalb man ihr bereits den Charakter einer Sperrung absprechen sollte.

3. Abgrenzung Mediendienste - Teledienste

Erwähnenswert ist schließlich auch, dass die Bezirksregierung nunmehr in Betracht zieht, dass die zu sperrenden Angebote evtl. doch keine Mediendienste sind, sondern auch Teledienste sein könnten. Die Bezirksregierung hält dies aber für unerheblich, da sie der Meinung ist, die Sperrungsanordnung in gleicher Weise auch auf § 14 OBG stützen zu können.

Die Bezirksregierung hält allerdings zunächst an der Auffassung fest, es würde sich bei den beanstandeten Angeboten „stormfront.org“ und „nazi-lauck-nsdapao.com“ um Mediendienste handeln. Begründet wird dies mit dem Argument, die beiden Angebote seien wie Zeitungen aufgebaut und journalistisch-redaktionell gestaltet. Wer sich die beiden Webangebote anschaut, wird sich ob dieser Thesen vermutlich verwundert die Augen reiben. Diese Inhaltsangebote entsprechen in ihrer formalen Aufmachung und Struktur einer Vielzahl anderer Websites. Es ist nicht erkennbar, dass die journalistisch-redaktionelle Gestaltung im Vordergrund steht. Würde man der Auffassung der Bezirksregierung folgen, müsste die Mehrzahl der Webinhalte als Mediendienste angesehen werden. Das Gegenteil ist freilich nach überwiegender Auffassung der Fall.

Dass die Bezirksregierung zudem als Sonderordnungsbehörde für die Überwachung der Einhaltung der Bestimmungen des Teledienstegesetzes (TDG) zuständig ist, mag sein. Diese Zuständigkeit verleiht ihr aber keine Kompetenz in diesem Bereich Sperrungsverfügungen zu erlassen.

Das TDG enthält anders als der MDStV (vgl. dort § 8 n.F.) weder Regelungen dazu, wann ein unzulässiges Angebot vorliegt, noch sieht es selbst die behördliche Anordnung von Sperrungsmaßnahmen vor. § 8 Abs. 2 S. 2 TDG (n.F.) stellt lediglich klar, dass Maßnahmen zur Sperrung nach den allgemeinen Gesetzen unberührt bleiben und verweist insoweit lediglich deklaratorisch – ohne eigenen Regelungsgehalt – auf die allgemeinen Vorschriften. Die Möglichkeit der Untersagung oder Sperrung von Telediensten nach dem allgemeinen Sicherheitsrecht stellt damit keine Maßnahme zur Einhaltung der Vorschriften des TDG dar, weshalb es insoweit bei den allgemeinen sicherheitsrechtlichen Zuständigkeitsregeln verbleibt. Die Bezirksregierung ist deshalb für die Anordnung der Sperrung von Telediensten nicht zuständig.

4. Beeinträchtigung der Informationsfreiheit

Die Bezirksregierung geht schließlich auch auf den grundrechtlich gewichtigsten Einwand der Beeinträchtigung der Informationsfreiheit nicht ein. Da der Schutzbereich der Informationsfreiheit betroffen ist, muss sich die Bezirksregierung zwingend mit der Frage auseinandersetzen, ob der von ihr insoweit vorgenommene Eingriff verfassungsgemäß ist. Dass dieser entscheidende Aspekt in der Widerspruchsbegründung ausgespart wird, ist angesichts des öffentlichen Protests [3] und der juristischen Diskussion [4] mehr als erstaunlich.

5. Fazit

Die Widerspruchsbegründung der Bezirksregierung wird so mancher Leser für stimmig und durchaus überzeugend halten. Dieser Eindruck konnte aber lediglich deshalb vermittelt werden, weil es die Bezirksregierung von vornherein vermeidet, sich mit einigen der gewichtigsten Gegenargumente auseinander zu setzen.

Man darf auf die zu erwartenden verwaltungsgerichtlichen Entscheidungen gespannt sein und darauf hoffen, dass diese auch höchstrichterlich überprüft werden.

1) So auch Vesting, in Roßnagel, Recht der Multimedia-Dienste, 4.Teil, § 18 Rn. 32.

2) Maurer, Allgemeines Verwaltungsrecht, 7. Aufl., § 7 Rn. 6

3) Die gegen die Sperrungsverfügung gerichtete „Erklärung gegen die Einschränkung der Informationsfreiheit“ wurde zwischenzeitlich von mehr als 13.000 Menschen unterzeichnet: http://odem.org/informationsfreiheit/

4) Vgl. hierzu Stadler, MMR 2002, 343 ff. und Neumann, Ordnungsrechtliche Sperrungsverfügungen und die Informationsfreiheit nach Art. 5 Abs. 1 S. 2 2.Alt GG.

„Eine relativ gefestigte Demokratie wie die unsere muss in der Lage sein,mit einem rechten Wählerpotenzial argumentativ umzugehen. Wir tun das nicht,setzen auf ein Verbot. Damit schafft man bloß Märtyrer – die offene Auseinandersetzung ist dem vorzuziehen.“

Günter Grass

Internet-Filter in der Praxis

von Alvar C.H. Freude

Alvar C.H. Freude ist Diplom-Kommunikations-Designer, Medienkünstler, Internet-Entwickler und Begründer von ODEM.org

http://alvar.a-blast.org/

Um die Kompetenz und Kritikfähigkeit der Anwender bezüglich des Alltags-Mediums Internet zu überprüfen, kontrollierten und manipulierten wir im Rahmen unserer Diplom-Arbeit insert_coin den Web-Datenverkehr an der Merz Akademie in Stuttgart. So verwandelten wir beispielsweise Suchmaschinen in Denunzier-Portale, veränderten aktuelle Meldungen auf Nachrichten-Sites; selbst Wörter in privater Email-Kommunikation, die über Web-Interfaces wie Hotmail abgerufen wurde, liefen durch unseren Filter. – Und niemand bemerkte es. Insgesamt haben wir über 600000 Manipulationen mit Hilfe unseres Filter-Systems vorgenommen.

Siehe auch: http://odem.org/insert_coin/

Im Wesentlichen sollten drei Fragestellungen analysiert werden:

1. Wie schwer ist es, ein umfangreiches und mächtiges Internet-Filter und -Manipulations-Systems zu entwickeln?

2. Fallen die Manipulationen den Manipulierten auf? Wie schnell fallen sie auf? Welche Gegenmaßnahmen der Opfer werden vorgenommen?

3. Wie reagieren die Betroffenen, wenn das Experiment aufgedeckt wird?

Zum Punkt der Schwierigkeit und des Aufwandes für die Erstellung eines umfangreichen Filter- und Manipulations-Systems lässt sich sagen, dass dies mit relativ wenig Aufwand möglich war. Wir haben es zu zweit innerhalb weniger Wochen geschafft, ein komplettes Systen auf die Beine zu stellen, das in der Lage ist, nahezu alle denkbaren Manipulationen durchzuführen. Mit Hilfe einiger Erweiterungen liesse es sich auch als transparente Filter-Lösung einsetzen, sprich: es wäre als verstecktes Filtersystem, das vom Anwender nicht ohne weiteres abgeschaltet werden kann, denkbar.

Die durchgeführtgen Manipulationen sind den Betroffenen im Prinzip nicht aufgefallen, und das obwohl wir massivste Veränderungen an den Webseiten, die sich die Nutzer anschauten, vornahmen. Durch einen einfachen Eingriff in die Einstellungen der Web-Browser-Konfiguration wurden alle von den Studenten abgerufenen Daten durch einen Computer geleitet, der unter unserer Kontrolle stand und der in Echtzeit eine Veränderung der Daten (in diesem Fall nur Webseiten).

Am erschreckendsten waren aber die Reaktionen der Betroffenen, nachdem wir bekannt gegeben haben, dass jeglicher Zugriff auf Webseiten durch unseren Filter geschleust wurden: es kam zu nahezu keiner Reaktion. Auch die (sehr einfache) Anleitung zum deaktiviren des Filters wurde nicht wirklich beachtet.

Dies führte dazu, dass auch drei Monate nach der Bekanntgabe immer noch auf über zwei Dritteln der von Studenten genutzten Computern unser Filter weiterhin eingestellt war.

Unser Experiment hat gezeigt, dass das Netz nicht „von Natur aus“ ein freies Medium ist, das niemand kontrollieren kann, und in dem Zensur und Kontrolle nicht vorgesehen und damit unmöglich sind. Mit im Vergleich zu den Auswirkungen relativ geringen Aufwand war es zwei Personen möglich, die Daten von über 200 Personen zu überwachen und ihnen beliebige Dinge unterzujubeln.

Gleichzeitig zeigt es aber auch, welche Gefahr in Filtersystemen stecken, vor allem von solchen, die zentral eingerichtet und gewartet werden.

Der vorliegende Text gibt nur einen sehr groben Überblick über ein Experiment, das im Rahmen der Diplomarbeit von Alvar C.H. Freude und Dragan Espenschied entstand.

Die Arbeit wurde 2001 mit dem Internationalen Medienkunstpreis 2001 vom Zentrum für Kunst und Medientechnologie in Karlsruhe (ZKM) und vom Südwestrundfunk (SWR) ausgezeichnet

Eine ausführliche Dokumentation der Arbeit kann im WWW unter der folgenden Adresse nachgelesen werden:

http://odem.org/insert_coin/

Sie können den Filter auch selbst mit Hilfe eine einfachen Browser-Einstellung ausprobieren. Details zu den Einstellungen finden Sie unter http://odem.org/insert_coin/experiment/proxy.html

Alternative: Selbstkontrolle, Rating, ICRA?

Wo es noch relativ leicht fällt, sich gegen staatliche Kontrolle zu wenden, macht das System der freiwilligen Selbstkontrolle auf den ersten Blick einen vernüftigeren Eindruck. Dennoch geht auch von diesen Bemühungen eine große Gefahr für die freie Meinungsäußerung im Netz aus, ganz zu schweigen von der Freiheit des Rezipienten, sich aus allen öffentlichen Quellen informieren zu dürfen. Dies hat letztendlich Auswirkungen darauf, wie das Netz sich in Zukunft weiterentwickelt und wie die Anwender damit umgehen. Bleibt es ein Kommunikations-Medium oder verkommt es zum Distributionskanal für Medieninhalte?

Das von der Bertelsmann Stiftung vorgeschlagene ICRA-System) vermittelt auf technischer Ebene den Eindruck, ein flexibles und mit Bedacht konstruiertes System sein. Jeder kann die eigenen Inhalte nach beliebigen Schemata selbst bewerten, zudem können sich Rating-Services bilden, die auch fremde Inhalte einteilen. Somit kann jede Information aus jedem nur erdenklichen Blickfeld bewertet werden – theoretisch.

Das Problem einer Kategoriesierung besteht im Internet noch viel mehr als bei klassischen Medien. Ist Kriegsberichterstattung nun gewaltverherrlichend und muss daher von Minderjährigen ferngehalten werden? Oder dürfen Nachrichten nicht gefiltert werden? Wenn ja, was sind dann Nachrichten und was ist beispielsweise Sensations-Journalismus? Was ist Ironie, was ernstgemeint? So einfach lässt sich das glücklicherweise nicht sagen, amerikanische Juristen sahen das im Fall von vote-auction jedoch anders. Vote-auction war eine Satire auf das US-Amerikanische Wahlsystem und stellte auf den ersten Blick eine Plattform zur Verfügung, bei der jeder seine Stimme für die Präsidentenwahl versteigern konnte. Bei genauerem Hinsehen konnte man schnell entdecken, dass alles nur ein Fake war. Ein Jurist forderte während einer Gesprächsrunde am 24. Oktober 2000 auf CNN tatsächlich, Satire müssen man kenntlich machen, so wie die Comics auf der letzten Seite einer Zeitung. Wie soll eine Filterung dieser Vorstellung nach ablaufen? Mit ein paar binären Kategorien lässt sich menschliche Kommunikation nicht einteilen.

Anders als bei einem Broadcast-Medium wie beispielsweise dem Kinofilm, das innerhalb eines Jahres eine endliche Anzahl Produkte erzeugt, entsteht im Netz täglich eine schlicht unüberschaubare Menge an Daten, die niemals vollständig nach auch nur irgendeinem Bewertungs-System eingeteilt werden könnte. Konversationen im Usenet, Einträge in Foren, Nachrichten, all das kann unmöglich bewertet werden.

Ein Filter-System, das nicht kategorisierte Inhalte durchlässt, ist sinnlos, weil dadurch eine Menge unerwünschte Inhalte unbehelligt blieben. Daher ist es aus Sicht der Filter-Software logisch, unbewertete Inhalte zu sperren.

Die einzigen Sites, die sich in allen populären Bewertungs-Schemen eintragen werden können, sind große kommerzielle Angebote. Alle anderen haben nicht die finanziellen Mittel, eine detaillierte Selbstbewertung vorzunehmen. Das Netz wird so zu einem homogenisierten, sauberen Distributionskanal für Mainstream-Ware.

Zudem verhindert eine freiwillige Selbstkontrolle keinesfalls staatliches Eingreifen. Ähnlich wie bei unbewertenen Inhalten können von einem Filter auch keine falsch bewerteten Inhalte akzeptiert werden. Stuft sich beispielsweise ein Porno-Anbieter zur Ankurbelung des Geschäfts als »tauglich ab 16 Jahren« ein, funktioniert der Filter nicht mehr wie gewünscht. Daher sind früher oder später Maßnahmen gegen falsche Bewertungen erforderlich. Eine andere Institution als der Staat könnte diese Kontrollfunktion kaum übernehmen.

Eine umfangreiche Auseinandersetzung mit dem Thema des Self-Rating oder der Selbsteinstufung ist unter der folgenden Adresse zu finden:
http://www.aclu.org/issues/cyber/burning.html

Die Idee für ein umfangreiches Selbstkontroll- und Filtersystem basiert auf der Angst der etablierten Medienkonzerne, mit dem Internet an Einfluss zu verlieren:

„Das neue Medium ist nicht mehr auf Vermittler wie Verlage, Sender, Zeitungen oder die Musikindustrie angewiesen. Im Internet wird eine „Massenkommunikation“ von Individuum zu Individuum möglich. Auf diese Entwicklung hin zur Nutzerkontrolle sind wir bisher nicht vorbereitet.

Wir müssen neue Regulierungsmechanismen entwickeln.“

Jens Waltermann, Marcel Machill (Hrsg.), Verantwortung im Internet, Selbstregulierung und Jugendschutz; Verlag Bertelsmann Stiftung, Gütersloh; Seite 9f

„O mein Herr, mir ist Gefängnis lieber als das, wozu sie mich einladen“

Von Dirk Eckert

Zuerst erschienen in Telepolis am 4. September 2002
http://www.telepolis.de/deutsch/inhalt/te/13186/1.html

Dirk Eckert ist Politikwissenschaftler und freier Journalist

Weitere Infos: http://www.dirk-eckert.de/

In einem Projekt der Harvard Law School ist jetzt erstmals dokumentiert worden, welche und wie viele Seiten des Internet in Saudi-Arabien nicht zu sehen sind

Im Königreich Saudi-Arabien ist das Internet nicht frei zugänglich. Seiten mit pornographischen Inhalten, zu Drogen, Alkohol, Bomben und Glücksspielen sowie Seiten, die „die islamische Religion oder die saudischen Gesetze und Verordnungen verletzen“, werden dort gesperrt. Verantwortlich hierfür ist die Internet Services Unit (ISU), eine Abteilung der King Abdulaziz City for Science & Technology (KACST), die in der Hauptstadt Riad einen Proxy betreibt, an den alle Provider des Landes angeschlossen sind. Sämtliche Datenströme, die in das Königreich fließen und wieder hinaus, laufen über diese eine Schaltstelle.

In einem Projekt der Harvard Law School ist jetzt erstmals dokumentiert worden, welche und wie viele Seiten des Internet in Saudi-Arabien nicht zu sehen sind. Von 64.557 getesteten Seiten waren 2038 in Saudi-Arabien gesperrt. Jonathan Zittrain und Benjamin Edelman vom Berkman Center for Internet and Society der Harvard-Universität haben sich für die Untersuchung mit Zustimmung der ISU in das saudi-arabische Internet eingeloggt. Aus ihrer Untersuchung folgern sie, dass die saudische Regierung ein „aktives Interesse“ daran hat, Seiten zu filtern, die explizit nichts mit Sexualität zu tun haben.

Zensiert werden etwa Inhalte aus den Bereichen Religion, Gesundheit, Bildung, Humor und Unterhaltung. Unter den gesperrten Seiten sind die Internetauftritte des Magazins „Rolling Stone“, des Anne-Frank-Hauses in Amsterdam, Warner Brothers Records, die Hisbollah, die israelische Armee sowie die Web-Seiten von amnesty international zu Saudi-Arabien. Auch 246 Seiten, die Yahoo in der Sparte Religion aufführt, sind in Saudi-Arabien nicht erreichbar: Im Einzelnen sind es in der Kategorie Christentum 67 Seiten, in der Kategorie Islam 45, bei Heidentum 22, bei Judentum 20 und bei Hinduismus 12.

Reagiert hat die ISU bisher nicht auf die Untersuchung bzw. die Vorwürfe aus Harvard. Kein Wunder, ist doch die Existenz des Filtersystems längst bekannt und oft kritisiert worden, etwa in einem Bericht von Human Rights Watch zur Zensur des Internets im Nahen Osten aus dem Jahr 1999. „Sie sind völlig offen mit dem, was sie tun und warum“, berichtete Jonathan Zittrain gegenüber dem „Boston Globe“.

Ich denke nicht, dass sie meinen, es müsste ihnen peinlich sein. Vielleicht denken sie jetzt anders, wo unsere Studie veröffentlicht ist.

Doch das ist zu bezweifeln, denn die Herrscher zwischen Rotem Meer und Persischem Golf sind sogar stolz auf ihr System. Die ISU preist das Verfahren auf der eigenen Homepage an, informiert die Nutzer bereitwillig über die Vor- und Nachteile des Verfahrens und rechtfertigt die Zensur u.a. mit Versen aus dem Koran:

O mein Herr, mir ist Gefängnis lieber als das, wozu sie mich einladen; und wenn Du nicht ihre List von mir abwendest, so könnte ich mich ihnen zuneigen und der Törichten einer sein. Also erhörte ihn sein Herr und wendete ihre List von ihm ab

heißt es bei Josef (12), Vers 33-34.

Dass ein Koran-Zitat herangezogen wird, um das Verhältnis zum Internet zu bestimmen, ist für Heinz Grotzfeld, Professor an der Universität Münster, nicht überraschend. Im Islam würde in solchen Fällen oft nach Parallelstellen gesucht, erläutert er. Die Auslegung des Koran sei in Saudi-Arabien bekanntermaßen „äußerlich und wörtlich“. Das theologische Problem, ob sich der Gläubige der Versuchung zu stellen hat oder besser im Gefängnis - und damit geschützt vor der Versuchung - zu leben

hat, sei auch im Christentum nicht endgültig geklärt, gibt der Islamwissenschaftler zu bedenken. Allerdings würden christliche Intellektuelle es in ihrer Mehrzahl für besser halten, sich der Versuchung zu stellen.

Auch wissenschaftliche Erkenntnisse führt die ISU an. Hier stellt sich das Land, in dem Frauen massiv diskriminiert werden, als Vorkämpfer gegen Männergewalt dar: Eine Studie von Cass Sunstein im „Duke Law Journal" habe gezeigt, dass bei strengen Gesetzen gegen Pornographie die Zahl der Vergewaltigungen zurückgehe. Und: Die US-Staaten Alaska und Nevada wären die beiden Bundesstaaten mit dem meisten pornographischen Material. Dort sei die Zahl der Vergewaltigungen bis zu acht Mal so hoch wie andernorts.

Internetanschlüsse für Universitäten und Forschungseinrichtungen gibt es in Saudi-Arabien seit 1994. 1999 wurden dann die ersten Provider zugelassen. Dabei kann jeder auf den Seiten der ISU Domain-Namen zur Sperrung empfehlen bzw. beantragen, bestehende Sperrungen wieder aufzuheben. Letzteres geht freilich nur mit freiem Zugang zum Netz - hier ist das System in sich widersprüchlich. Tatsächlich kann jeder, der sich die teureren Einwahlgebühren leisten kann oder will, über ausländische Provider ins Netz gehen und dort die verbotenen Seiten einsehen.

An der Entwicklung des Internets in Saudi-Arabien waren auch deutsche Wissenschaftler und Programmierer beteiligt. Die Deutsche Gesellschaft für Technische Zusammenarbeit (GTZ) und das Rechenzentrum der Universität Mannheim (RUM) gewannen 1997 eine entsprechende saudische Ausschreibung. Diplom-Ingenieur Franz-Josef Jochem von der Universität Mannheim räumt denn auch ein, dass die technischen Einrichtungen für die Seiten-Sperrung von den Deutschen installiert wurden. Das sei eine „Frage der Abwägung" gewesen, die auch unter den Wissenschaftler viel diskutiert worden sei, sagt er. Letztlich habe aber die Aussicht auf eine Verbesserung der Kommunikationsmöglichkeiten überwogen, sagt Jochem. Er ist sich sicher: „Informationen lassen sich nicht aufhalten."

„Die Harvard-Wissenschaftler Edelman und Zittrain beschäftigen sich mit staatlichen Filtermaßnahmen und versuchen jeweils die genaue Situation zu erkunden. Bisher galt ihr Interesse in erster Linie den Maßnahmen in totalitären Staaten beziehungsweise Ländern, deren Regierungen von einem religiösen Wertesystem geprägt sind. Nach den jüngsten Ereignissen richtet sich ihr Interesse nun auf Nordrhein-Westfalen."

intern.de: Saudi-Arabien, China, Nordrhein-Westfalen
http://www.intern.de/news/3458.html

„Zu Hause bin ich bereits auf bedenkliche Websites gestoßen, war aber aufgrund des Computertrainings in der Schule in der Lage, damit umzugehen: Ich habe die Websites einfach weggeklickt. [...]In meiner Familie herrscht Übereinstimmung darüber, dass man solche [Hass-] Sites einfach nicht besucht und wir diskutieren über die Gründe dafür."

Simon Proffitt, 13, Schüler der Netherhall School in Cambridge, Großbritannien
in einem Aufsatz über Internet-Filter

In: Marcel Machill, Felicitas von Peter (Hrsg.): Internet-Verantwortung an Schulen;
Verlag Bertelsmann Stiftung, Gütersloh 2001
Seite 374f.t

Die Gesellschaft für technische Zusammenarbeit (GTZ) lobt die Einführung des Internet in Saudi-Arabien als „gewaltigen Schritt" nach vorne. Erstmals hätten die Bürger Zugriff auf Informationen aus aller Welt, argumentiert ein Mitarbeiter. Tatsächlich, das ergab auch die Harvard-Studie, können die Saudis unzensiert durch die CNN-Seiten surfen. Der Zensur gibt der GTZ-Mitarbeiter wenig Chancen: „Die Inhalte im Netz ändern sich zu schnell". Und was das Blockieren einzelner Seiten betrifft: Das werde in anderen Ländern, darunter Deutschland, ebenso praktiziert. Auch dort sperrten Provider Seiten mit pornographischen oder antisemitischen Inhalten. „In Saudi-Arabien wird das exzessiver betrieben. Es ist aber nicht einzigartig."

Dass Seiten mit antisemitischen Inhalten in Saudi-Arabien gefiltert werden, hat die Harvard-Studie indes nicht ergeben. Die Gefahr, die Jonathan Zittrain sieht, ist, dass das Internet von einem globalen und grenzenlosen Netzwerk in viele verschiedene nationale Netze verwandelt wird. Jedenfalls, wenn das saudische Beispiel Schule macht.

Wasserbetten nur für Volljährige

US-Bürgerrechtsgruppen warnen vor technisch unausgereifter Filtertechnologie im Internet – doch die wahre Gefahr droht gerade bei technischer Perfektion.

von Konrad Lischka

Zuerst erschienen am 27. September 2000
in der Berliner Zeitung

Konrad Lischka ist freier Journalist

Weitere Infos:
http://www.konradlischka.de

Sherril Babcock mag ihren Namen. Einige Computer aber nicht. Als die Anwältin aus Los Angeles sich beim Online-Dienst Blackplanet.com registrieren wollte, hieß es lapidar, ihr Nachname sei „nicht akzeptabel". Blackplanet.com setzt Filtersoftware ein, um „anstößige" Inhalte zu blockieren. An Babcocks Namen stört sich niemand – außer dem Filter, der den Begriff „cock" (englisch für Schwanz) darin erkennt.

Bürgerrechtsgruppen in den USA laufen Sturm gegen solche Filtersoftware im Internet. Organisation Digital Freedom Network hat als Protest den „Foil the Filters" Wettbewerb ausgeschrieben. Bis zum Montag konnten Benutzer Fehlurteile von Filterprogrammen einschicken. Heute werden die Preise verliehen: Eine Mütze des britischen Städtchens Scunthorpe, ein Buch von Emily Dickinson und ein Souvenir aus Linz.

Für Antifilter-Aktivisten sind die Preise alles andere als seltsam: Ein Bewohner von Scunthorpe beschwerte sich bei der DFN, seine eMails würden oft blockiert. Grund: Filter erkennen im Ortnamen „cunt" (Gegenstück zu „cock"). Bei Schriftstellerin Emily Dickinson stören sich manche Filter am vermeintlichen „dick" (Synonym für „cock").

Mark Rotenberg von der US-Bürgerrechtsorganisation Electronic Privacy Information Center betont: „Die Menschen denken bei Filtern nur an Sexseiten, dabei wird alles mögliche zensiert. In manchen Bibliotheken erhält man keine Informationen über Bücher von Anne Sexton".

In der Tat versagen manche Filter bedenklich. Der amerikanische Internetprovider FamilyClick verwendet I-Gear von Symantec. Bürgerrechtsaktivist Bennett Haselton veröffentlicht auf der seiner Website Peacefire.org von FamilyClick blockierte Seiten. Beispiele: ein Bericht der Pekinger US-Botschaft über das AIDS-Problem in China, ein Artikel über die Verfolgung Homosexueller im Dritten Reich, ein Essay zur Reaktion Israels auf den Anschlag bei den Olympischen Spielen 1972.

Eine anderer Test Bennett Haseltons ergab für den Filter Surfwatch eine theoretische Fehlerquote von 82 Prozent. Unter den blockierten Domains fand sich unter anderem ein Anbieter von Wasserbetten und eine Kosmetikfirma, die betont, in „christlichem Besitz" zu sein.

Noch schlechter schnitt die Software BAIR bei Tests des US-Computermagazins Wired ab. Laut Hersteller Exotrope soll das Programm Bilder mit sexuellen Inhalten erkennen. Bei Wired hingegen blockierte das Programm Fotos von Snoopy, Booten, Sonnenuntergängen, Hunden und sogar der Wired Nachrichtenredaktion. Als unbedenklich für Minderjährige wurden hingegen Aufnahmen von Gruppensex eingestuft.

Das mögen technische Kinderkrankheiten sein, doch sind sie einmal gelöst stellt sich immer noch die Frage: Was soll eigentlich gefiltert werden? Und vor allem: Wer darf das bestimmen?

In zahlreichen Staaten blockieren Filterprogramme gezielt politische Inhalte. In Saudi-Arabien beispielsweise den Zugang den sogenannten Yahoo-Clubs, einer Art Diskussionsforum. Angeblich wegen pornographischer Inhalte. Weltweit schränken 45 Staaten laut einem Bericht der Organisation Freedom House den Internetzugang ein.

Auch das Engagement privater Unternehmen wie Bertelsmann im Bereich Filtertechnik muss nicht zwangsläufig uneigennützig sein. Darauf wies Andy Müller-Maguhn, Sprecher des Chaos Computer Clubs, in einem Interview mit dem Netzmagazin telepolis hin: „Ich habe keinen Zweifel, dass man hier ein aus wirtschaftlichen Kontrollgelüsten motiviertes Filtersystem mit der Argumentation ‚zum Wohle der Gesellschaft' der Politik schmackhaft machen will." Abseits von Verschwörungstheorien führen die Auseinandersetzungen um Napster und DeCSS vor Augen, welche Interessen Medienkonzerne an Filtersoftware haben könnten.

Ende April berichtete der angesehen Publizist Brian Livingston, die von AOL eingesetzte Software Cyber Patrol würde nach politischen Vorlieben filtern. So sei im „Kids

only“ Modus der Zugriff im aufs Republican National Comitee möglich, der aufs Democratic National Comitee hingegen verwehrt. „Young Teens“ könnten zwar auf die Seiten von Waffenherstellern und der National Rifle Association zurückgreifen, die Angebote der Initiativen „Stop Gun Violence“ und „Safer Guns“ seien hingegen gesperrt.

Diese Entwicklungen zeigen, dass das blindes Vertrauen auf Technik der falsche Weg ist. Rechtsprofessor Lawrence Lessing warnt in seinem Buch „Code“, dass das Internet zu einem enormen Kontrollsystem werden könnte, wenn solches Vorgehen sorgfältige Gesetzgebungsprozesse ersetzt.

Technik liefert nicht Antworten auf gesellschaftliche Fragen. Die 65,4 Prozent der 14 bis 17jährigen, die laut einer aktuellen Emnid-Unfrage nichts mit dem Begriff „Holocaust“ anzufangen wissen, haben das gewiss nicht fehlender Zensur im Internet zu verdanken.

Während eines Prozesses um Naziinhalte kritisierte Philippe Guillaton, CEO von Yahoo France das bloße Vertrauen auf Filter: „Stellen sie sich vor, wir könnten umsetzten, was hier von uns verlangt wird. Dann kämen morgen Richter aus jedem Land der Welt zum einem Anbieter und würde verlangen, er soll dies und jenes löschen, weil es in ihrem Land nicht zu akzeptieren sei. So funktioniert das Netz nicht. Es basiert auf dem Verantwortungsbewusstsein der Nutzer.“

Der Vorsitzende des Komitees für Cyberrecht der US-Anwaltskammer sieht eine internationale Körperschaft, die einheitliche, globale Prinzipien für Internet-Rechtssprechung festsetzt als einzige Lösung: „Es ist, als wären wir auf dem Mars gelandet. Wir müssen neue Regeln etablieren und die Leute daran gewöhnen, nach ihnen zu handeln.“

Etwas Zeit bleibt noch, denn Filtertechnik ist alles andere als perfekt. Sherril Babcock konnte sich letzten Endes doch bei Blackplanet.com registrieren – und dem Alias „Babpenis“.

„Es wäre zu wünschen, daß Deutschland für die Entwicklung des Internet mehr beizutragen hat als die Strafverfolgung von Access-Providern, die für die übermittelten Inhalte nicht verantwortlich sind.“

Prof. Dr. Ulrich Sieber im Plädoyer für Felix Somm

„Regierungspräsident Büssow hat heute Vorwürfe der Zensur gegen sein Vorhaben, vier amerikanische Websites durch die nordrhein-westfälische Zugangs-Vermittler sperren zu lassen, entschieden zurückgewiesen. Diese Vorwürfe waren in der letzten Woche von den Magazinen Focus und Spiegel, dem Bundestagsabgeordneten Jörg Tauss, dem Chaos Computer Club, aber auch von Jörg Schieb (WDR) erhoben worden.“

Pressemeldung der Bezirksregierung Düsseldorf

Sperrungen im Internet

Eine Systematische Aufbereitung der Zensur-Diskussion

von Kristian Köhntopp, Marit Köhntopp und Martin Seeger

Veröffentlichung am 14.05.97, für das Bundesministerium für Bildung und Forschung (BMBF)

Kristian Köhntopp ist Diplominformatiker und arbeitet als freiberuflicher Consultant für heterogene Datennetze und Rechnersicherheit

Marit Köhntopp ist Diplominformatikerin und arbeitet beim Landesbeauftragten für den Datenschutz Schleswig-Holstein als Referentin in den Bereichen „Neue Medien und Informationstechnologien" sowie „Technikfolgenabschätzung"

Martin Seeger ist Diplominformatiker und Geschäftsfuehrer der NetUSE Kommunikationstechnologie GmbH. Das Unternehmen beschäftigt sich mit der Internet-/Intranet-Technologie und der Sicherheit von Rechnern in Netzen

Zusammenfassung

Wie alle anderen Medien wird auch das Internet zur Verbreitung von beispielsweise rechtsradikalen oder kinderpornographischen Informationen mißbraucht. Dies hat in letzter Zeit den Ruf nach einem staatlichen Eingriff laut werden lassen, um zentrale Sperrungen bestimmter Inhalte zu erreichen.

Die Autoren halten einen solchen Schritt fuer nicht angemessen. Zum einen haben bisher alle technischen Ansätze zur Realisierung versagt. Strukturelle Überlegungen lassen vermuten, daß dies auch in Zukunft der Fall sein wird. Auf der anderen Seite haben Sperren stets Auswirkungen auch auf Bereiche, deren Sperrung nicht beabsichtigt ist. Diese Nebenwirkungen sind um so schwerwiegender, je wirksamer die Sperren sein sollen.

Dezentrale Lösungsansaetze koennen dem Nutzer die Möglichkeit geben, im eigenen Bereich selbstverantwortlich Inhalte zu filtern. Bewertungen von Inhalten durch nichtstaatliche Organisationen können dazu füehren, daß der Bewertungsmechanismus zur Durchsetzung fragwürdiger Interessen mißbraucht wird. Um diesem Risiko entgegenzuwirken, ist es unverzichtbar, daß nicht nur die Bewertungsmaßstäbe, sondern auch die Bewertungen selbst vollständig offengelegt werden.

Jede Art von staatlicher Regulierung treibt die Kosten in die Höhe. Es ist abzusehen, daß der Versuch, Inhalte im Internet zu bewerten, sehr personalintensiv sein wird. Bereits heute sind die Kommunikationskosten am Standort Deutschland wesentlich höher als bei konkurrierenden Nationen wie den USA. Regulierungen können daher zu einem Standortnachteil führen.

Was soll mit einer Sperrung erreicht werden?

Bevor man über technische Maßnahmen zur Sperrung von Inhalten im Internet und die Chancen ihrer Realisierung reden kann, muß man sich darüber klar werden, welche Ziele man mit einer solchen Sperrung erreichen möchte. Mögliche Ziele sind:

- Law Enforcement: Man moechte verhindern, daß nach den Kriterien einer nationalen oder regionalen Rechtsordnung strafrechtlich relevantes Material für die Subjekte dieser Rechtsordnung erreichbar ist bzw. von ihnen veröffentlicht werden kann, und zwar auch dann, wenn der Ort der Veröffentlichung außerhalb des Durchsetzungsbereiches dieser Rechtsordnung liegt. Traumziel wäre es, das Begehen solcher Straftaten technisch unmöglich zu machen.
- Indecency: In den USA wurde mit dem *communication decency act* (*CDA*) in seinen verschiedenen Formulierungen und Gesetzesvorlagen versucht, eine noch weitergehende Regelung zu etablieren: Es sollte verboten werden, Material ueber Datennetze zugänglich zu machen, das *indecent* ist, d.h. nach den Grundsätzen der jeweils herrschenden Moraldefinition ungehörig, obszön oder in anderer Weise störend (zu Free Speech siehe z.B. The Electronic Frontier FoundationEFF, http://www.eff.org).
- Jugendschutz: Nur Minderjährigen (Kindern und Jugendlichen) soll der Zugang zu bestimmten Materialien verwehrt werden, während Volljährigen weiterhin die gesamten Inhalte des Internet zugänglich bleiben sollen.
- Rating: Für jeden Teilnehmer im Netz soll weiterhin frei definierbar sein, welches Material empfangen/nicht empfangen werden soll, aber es soll eine Bewertungsstruktur geschaffen werden, die es jedem Konsumenten in eigener Verantwortung ermöglicht, seine Präferenzen anzugeben (kein Sex/viel Sex, keine Gewalt/Blood and Splatter, politisch links/politisch rechts, konform mit den Vorstellungen der katholischen Kirche/islamisch korrekt) und nur noch den Ausschnitt aus dem Internet wahrzunehmen, der diesen selbstgewählten Filter passieren kann.
- Nichtregulation: Jeder Netzteilnehmer soll freien Zugriff auf alle angebotene Information haben. Sogar die Existenz von Bewertungskriterien Dritter wird als

schädlich angesehen und die Bildung einer Bewertungsinfrastruktur nicht gefördert bzw. sogar behindert.

Welche Dienste werden betrachtet?

Unter der Bezeichnung *Inhalte im Internet* wird in der Regel eine ganze Reihe von Diensten subsumiert, die technisch vollkommen unterschiedlich realisiert werden und administrativ zu großen Teilen disjunkte Strukturen aufweisen. Allen Diensten ist lediglich gemeinsam, dass ihnen das Datenübertragungsprotokoll TCP/IP zugrunde liegt.

Man muß mindestens die beiden folgenden Dienste unterscheiden:

- WWW, World Wide Web: Das World Wide Web ist der graphisch ansprechendste Dienst des Internet. Es handelt sich um Server, die auf die Anfrage eines Benutzers Seiten beliebigen Inhaltes an das Darstellungsprogramm (*Browser*) auf seinem Rechner ausliefern. Der Zugriff auf diese Seiten erfolgt in der Regel mit Hilfe des HyperText Transport Protocol (*HTTP*). Dieses Protokoll erfordert keine Identifizierung oder Authentisierung des Abrufers und des Anbieters; die Daten werden im Klartext und nicht fälschungssicher übermittelt.
- Eine optional einsetzbare Modifikation von HTTP übermittelt Anfragen und Antworten mit Hilfe des Verschlüsselungsverfahrens *Secure Socket Layer* (*SSL*). Bei diesem Verfahren muß sich mindestens der Anbieter gegenüber dem Abrufer identifizieren. Weiterhin ist sichergestellt, daß die Verbindung nicht im Klartext abhörbar ist (Dritten wird nicht bekannt, welche Anfragen gestellt wurden oder welche Inhalte die ausgelieferten Seiten haben) und daß Inhalte nicht durch Dritte während der Übertragung unerkannt verfälscht werden können.

  Die abgerufenen Seiten bestehen aus Formatierungsanweisungen der *HyperText Markup Language* (*HTML*) und optional weiteren Bild-, Ton- oder Videodaten. Bei kleineren Servern liegen die abrufbaren Seiten häufig statisch als vorgefertigte und unverändert ausgelieferte Dateien auf der Festplatte vor. Größere Server erzeugen die Seiten jedoch oftmals dynamisch in Abhängigkeit von der Identität des Abrufers, seiner Netzadresse, seiner bevorzugten Landessprache (im Browser konfigurierbar), dem vom Abrufer verwendeten Browsertyp, der Uhrzeit des Abrufs oder anderen Kriterien, die frei progammierbar sind. Es ist also nicht sichergestellt, daßzwei aufeinanderfolgende Abfragen derselben Seite identische Antworten ergeben.

  Falls die Seiten aus einer Datenbank dynamisch erzeugt werden, kann sich der Datenbestand des Webservers durch die Updates der Datenbank ständig aendern. Dies ist zum Beispiel der Fall bei Katalogsystemen fuer Onlinehandel (Preis- und Produktupdates, Änderungen im Lagerbestand mit Auswirkungen auf die Lieferbarkeit usw.), bei Nachrichtenagenturen mit Anschluß an Presse- und Tickerdienste und bei Webverzeichnissen und Suchmaschinen, die einen Volltextindex für Seiten generieren und eine Recherche nach Inhalten erlauben.

  Grundsätzlich ist der Datenbestand im Web als höchst dynamisch anzusehen: Neue Versionen von Seiten lassen sich zu sehr geringen Kosten erzeugen und in Verkehr bringen. Der elektronische Charakter des Mediums im Zusammenhang mit der zentralen Datenhaltung (es sind keine verteilten Kopien einer Seite auf Stand zu bringen) begünstigen weiterhin eine sehr hohe Auflagenfrequenz.

- USENET News: Das USENET ist ein verteiltes System vom Diskussionsforen (*Newsgroups*). Es handelt sich um ein teilweise zusammenhängendes Netz von Servern, von denen jeder eine Auswahl von Artikeln zum Abruf bereithält. Die Artikel sind in der Regel in thematisch gegliederten Diskussionsforen in der Reihenfolge des Eingangs abgelegt. Leser können eine Verbindung zum netztopologisch am günstigsten gelegenen Server aufbauen und Artikel nach Diskussionsforen und Eingangsdatum selektiert abrufen.
- Leser können grundsätzlich auf jeden gelesenen Artikel antworten (*to follow up on an article*) oder unabhängig eigene Artikel auf dem Server ablegen (*posten*, von engl. *to post a notice*). Der Server wird dann seine Nachbarserver darüber informieren, daßer einen neuen Artikel vorrätig hat, und den Artikel ggf. an seine Nachbarserver replizieren (*to feed an article to a neighboring system*). Diese verbreiten den Artikel dann wieder an ihre Nachbarn usw. (*flood fill algorithm of USENET*). Nach einigen Stunden existieren Hunderttausende von Kopien dieses Artikels auf der gesamten Welt. Die Vernetzung der Server ist hochredundant; Unterbrechungen in Serverstrecken haben in der Regel keine oder nur lokal meßbare Auswirkungen auf Verfügbarkeit oder Transportgeschwindigkeit der Artikel.

  Um Platz zu gewinnen, werden die jeweils ältesten Artikel nach einiger Zeit gelöscht. Die genaue Zeitspanne bis zur Löschung hängt von der individuellen Konfiguration des Servers und seiner Platzsituation ab, liegt aber in der Regel nicht über 14 Tagen. Es existieren jedoch auch einige Newsarchive, die Diskussionen über mehrere Jahre hinweg abspeichern und diesen Datenbestand durch weitgehende Recherchemöglichkeiten erschliessen (z.B. Google im Newsmodus: *http://groups.google.com/*).

  Dadurch, daß jeder Leser auf beliebige Artikel direkt und ohne redaktionelle Bearbeitung antworten kann, entspinnen sich in der Regel unmoderierte, öffentliche

Diskussionen zu allen möglichen Themen. Ein Großteil der Diskussionsforen wird global ausgetauscht. Daher ist die Zusammensetzung der Diskussionsrunden zufällig und international.

Die Kommunikation zwischen Leser und Server sowie die Kommunikation zwischen den Servern erfolgt in der Regel unverschlüsselt und ohne Identifizierung und Authentisierung der Leser oder der Autoren von Artikeln. Die Fälschung von Absenderadresse oder Herkunftspfad eines Artikels ist trivial und in einigen Diskussionsforen sogar üblich. Es existieren Konverter von E-Mail nach USENET News und Anonymous- sowie Pseudonymous-Server, die zum Teil mit kryptographisch starken Methoden die Identität des Absenders sowie seinen Aufenthaltsort im Netz zu verschleiern suchen. Einige Newsserver lassen Lese- und Schreibzugriff von jedermann und ohne Authentisierung zu (*open servers*); es ist Sache des Veröffentlichenden, seine Identität in einem Artikel offenzulegen oder nicht.

Die Entscheidung über die von einem Server angebotenen Diskussionsforen obliegt in der Regel jedem einzelnen Serverbetreiber. Teilweise existieren Kataloge von offiziellen Newsgroups, diese sind jedoch in der Regel weder vollständig noch für irgendwen verbindlich. Name oder Überschrift einer Newsgroup haben nur den Charakter von Empfehlungen. Thematisch falsch eingeordnete Artikel (*off topic postings*) oder bewußt massenhaft in alle Newsgroups verbreitete Artikel (*spam*) machen einen festen Anteil aller Artikel aus.

Die Dienste *IRC* (*Internet Relay Chat*) und *E-Mail* (Private elektronische Post sowie halböffentliche Mailinglists als Diskussionsforen) wären ebenfalls zu betrachten, sollen hier aber im Interesse einer kompakten Darstellung nicht diskutiert werden, da sie weniger im Rampenlicht der öffentlichen Diskussion stehen. Die genannten Argumente gelten aber in ähnlicher Form auch dort. Es existieren weitere Dienste, die fuer die öffentliche Kommunikation in der Regel von geringerer Bedeutung sind (*telnet*) oder deren Diskussion keine neuen Aspekte zu Tage foerdern wuerde (*ftp*, siehe *http*).

Wie können zu sperrende Inhalte identifiziert werden?

Um Inhalte zuverlässig sperren zu koennen, ist es notwendig, diese Inhalte in irgendeiner Form zu identifizieren. Diese Identifizierung kann von unterschiedlicher Auflösung sein. Auf der Basis von IP-Adressen kann ein einzelner Rechner identifiziert werden. Ein solcher Rechner erbringt jedoch in der Regel eine Vielzahl von Diensten für mehrere unterschiedliche Anbieter. Webserver von IP-Providern bringen unter einer IP-Adresse teilweise die Angebote von Tausenden Inhaltsanbietern ins Netz, Rechner von Kleinprovidern bieten teilweise alle Dienste des Providers unter einer IP-Nummer an. Eine Sperrung von IP-Nummern trifft also außer den zu sperrenden Inhalten meist auch eine große Menge von Inhalten und Diensten, deren Sperrung nicht beabsichtigt ist.

Mit entsprechendem Mehraufwand können dienstspezifische Kennzeichen von einzelnen Einheiten des Angebotes identifiziert werden. Im World Wide Web ist dies der Name einer Seite (ihr *Universal Resource Locator*, *URL*), in den USENET News erfolgt die Identifizierung über die Message-ID einer einzelnen Nachricht oder den Namen einer Newsgroup. Für neu entstehende Dienste müssen dienstspezifische Methoden zur Identifikation einzelner Einheiten neu gefunden werden.

Die zu bewertenden Datenmengen sind riesig: Die Suchmaschine Altavista hatte im Mai 1996 schon 30 Millionen Webseiten in ihrer Volltextdatenbank gespeichert; im April 1997 betrug das Newsaufkommen mehr als 72 Gigabyte für etwa 5,4 Millionen Artikel (Statistik von Eunet Deutschland GmbH aus *de.admin.lists* vom 01.05.97).

Es bleibt das Problem, zu sperrende Inhalte aus der Menge aller Inhalte zu isolieren. Hier gibt es nur zwei grundsätzlich verschiedene Systeme:

- Die automatische Bewertung von Inhalten auf der Basis formaler Merkmale wie etwa dem Vorhandensein bestimmter Schlüsselworte.
- Die manuelle Bewertung von Inhalten durch den Anbieter oder Dritte nach bestimmten Kriterienkatalogen (*rating*).

Verfahren zur automatischen Bewertung von Inhalten aufgrund von Schlüsselworten scheitern bei Komponenten, die keinen Text enthalten (Audiodateien, Bilder oder Animationen) schon im Ansatz. Einige Online-Dienste (Prodigy, AOL) haben versucht, Diskussionen in dem IRC-Dienst ähnlichen Chaträumen aufgrund des Gebrauchs bestimmter Schlüsselworte bewerten zu lassen; die Ergebnisse waren wenig befriedigend. Einerseits waren normale Diskussionen über bestimmte Themen nicht mehr möglich: Eine Sperrung des Wortes *suck* erschwerte den Meinungsaustausch zu Staubsaugern in einem Haushaltsforum, eine Sperrung des Wortes *breast* behinderte Diskussionen über Brustkrebs oder Kochrezepte (Hühnerbrust), und die Webseiten von Frau Cindy Tittle Moore (tittle@netcom.com) wurden durch das Programm Cybersitter wegen ihres Namens gesperrt.

Andererseits veränderte die eigentliche Zielgruppe einfach ihr Vokabular, so daß die Sperrung auf diese Zielgruppe keine nennenswerte Auswirkung hatte. Auch andere automatisierbare Bewertungsmethoden vermögen nicht die Semantik der Inhalte zu erkennen. Wer solche formalen Sperrkriterien kennt, kann leicht die Darstellung

seiner Informationen je nach Bedarf an diese Kriterien anpassen, ohne die inhaltliche Aussage zu verändern. Das Kindersicherungsprogramm Cybersitter ist beispielsweise in der Lage, als offensive eingestufte Worte aus Webseiten herauszuschneiden. Durch geschickte Formulierung sind so Aussagen in ihr Gegenteil verkehrbar, wenn sie unter Cybersitter betrachtet werden (Nachricht von Bennett Haselton auf der Mailingliste *fight-censorship@vorlon.mit.edu*, Message-ID: <01IAZF6R8I0I8XKGCV@ctrvax.Vanderbilt.Edu>).

Verfahren und Standards zur Bewertung von Inhalten durch den Anbieter oder Dritte liegen für den Bereich des World Wide Web bereits vor, das System PICS (Platform for Internet Content Selection) ist dabei zur Zeit führend. PICS erlaubt die Installation frei definierbarer Bewertungsmaßstäbe mit einer beliebig feinen Auflösung. Bewertungen von URLs koennen von den Anbietern selbst oder durch Dritte erfolgen. Gängige Bewertungsmaßstaebe sind dabei etwa Gewalt, Sex oder unanständige Sprache, die Abstufungen reichen von digitalen 0-1-Skalen bis zu sehr fein abgestuften Systemen. Die Auswertung von PICS-Einstufungen kann entweder im Clientprogramm des Anwenders erfolgen (dies wird zur Zeit vom Microsoft Internet Explorer unterstuetzt) oder auf Routern auf dem Weg zum Empfänger (dies geschieht zur Zeit nicht).

Das Hauptproblem bei der manuellen Bewertung von Inhalten ist die große Menge der anfallenden neuen oder veränderten Seiten. Der Betreiber des Nachrichtenservers *www.msnbc.com* (Joint-Venture von NBC und Microsoft) hat die Bewertung seiner Beiträge auf der Basis des von Microsoft geförderten Bewertungsschemas RSACi für PICS eingestellt, da die Bewertung einzelner Beiträge zu aufwendig war und eine Pauschalbewertung des Servers nach den Regeln von PICS den Server fuer Minderjährige unzugänglich gemacht haette (Briefwechsel zwischen Irene Graham, Michael Sims, Stephen Balkam (RSAC Ratingaufsicht) und Danielle Bachelder (MSNBC Systembetrieb), zitiert in <3339dd1a.500215@mail.thehub.com.au> und <199703191314.IAA03203@arutam.inch.com> auf derselben Mailingliste).

Hinzu kommt, dass die Webseite abhängig vom Kontext des Abrufes unterschiedlich aussehen kann, so daß eine Bewertung nach dem PICS-System problematisch wäre. Gerade diejenigen Seiten, die die interaktive Komponente des Internet ausnutzen, könnten so wegen ihrer dynamischen Generierung aus der Bewertung herausfallen und wüerden damit in entsprechend konfigurierten Browsern und Suchmaschinen nicht mehr dargestellt.

Die Bewertung von Angeboten erfolgt im Rahmen von PICS derzeit durch private Organisationen. Die Möglichkeiten des Widerspruchs gegen eine bestimmte Einstufung sind dabei begrenzt. Insbesondere ist es für einen Bürger schwierig, ein korrektes Rating einzufordern, wenn die Ratingorganisation in einem fremden Land sitzt.

Im Prinzip liegt hier dasselbe Problem vor, das sich zur Zeit bei der Strafverfolgung ausländischer illegaler Angebote stellt, nur daß die Ressourcen und Beweislasten nun andersherum verteilt sind: Ein Anbieter muß nun bei falscher Einstufung beweisen, dass sein Angebot legal ist, und er muß dazu den schwierigen Weg der Durchsetzung von Ansprüchen im Ausland gehen. Im Vergleich zu einer Staatsanwaltschaft ist ein Anbieter von Webseiten dafür im Durchschnitt schlechter ausgebildet, und ihm stehen weniger Ressourcen zur Verfügung.

Weiterhin orientieren sich die Ratingorganisationen an Werten und kulturellen Maßstäben ihrer Nation. Die Übernahme ausländischer Bewertungen für deutsche Benutzer ist daher problematisch. Da jedoch keine deutsche Zugriffssoftware existiert, werden meist nur ausländische (speziell US-amerikanische) Ratingsysteme unterstützt.

Die meisten Ratingorganisationen dokumentieren ihre Ratings nicht oder nur sehr ungern. Zum Teil erfolgt noch nicht einmal eine Benachrichtigung des Bewerteten über die Bewertung seines Angebotes. Vollständige Verzeichnisse aller vergebenen Ratings werden meist mit der Begründung unter Verschluss gehalten, daß diese Verzeichnisse als Kataloge fuer Schmutz und Schund mißbraucht werden könnten. Bei den Programmen, die die Bewertungen von Webseiten Dritter nicht online beziehen, sondern als Datei auf der lokalen Festplatte installiert haben, ist diese Liste grundsätzlich verschlüsselt - und meistens auch veraltet. Auch gegenüber dem Benutzer solcher Software ist damit nicht offengelegt, welche Angebote ihm nicht mehr zugänglich sind.

Inzwischen existieren (illegal) entschlüsselte Versionen der Sperrlisten aller Hersteller von Programmen mit statischer, in Dateien gelieferter Sperrliste. Die Auswertung der Sperrungen hat bei allen Herstellern eine klare politische Agenda und persönliche Feindschaften dokumentiert. Beispielsweise wurden vielfach Angebote von *womens organizations*, Informationsangebote über Abtreibung und Angebote schwuler und lesbischer Gruppen zensiert. Es ist weiterhin üblich, Webseiten in die Sperrlisten aufzunehmen, die den Hersteller des Sperrprogramms kritisieren, die Sperrliste offenlegen oder allgemein gegen Rating argumentieren. Beim Hersteller des Programms Cybersitter geht dies so weit, daß bei installiertem Cybersitter alle Seiten nicht mehr abrufbar sind, in denen die Namen von Kritikern seines Programms erwähnt werden.

Mit welchen Mitteln kann eine Sperrung erreicht werden?

Sperrungen können auf unterschiedlichen Ebenen der Kommunikation ansetzen:

Um erfolgreich zu kommunizieren, müssen beide Kommunikationspartner eine physikalische Verbindung zueinander aufbauen. Dies kann eine Standleitung, eine Telefonleitung, eine Richtfunkstrecke oder eine andere Kommunikationsform sein. Eine normalerweise nicht praktikable Möglichkeit der Sperrung besteht darin, diese physikalische Kommunikation zu verhindern, indem man etwa einen Telefonanschluss sperrt oder bestimmte Telefonnummern nicht erreichbar schaltet, Standleitungen unterbricht oder Störsender in Richtfunkstrecken einbringt. Das Opfer der Sperrung verliert damit in der Regel alle seine Kommunikationsmöglichkeiten.

Im Internet wird meist keine homogene physikalische Verbindung verwendet, sondern diese Verbindung wird aus Teilstücken unterschiedlicher Technologie zusammengestückelt. An den Übergangspunkten zwischen den Teilstuecken befindet sich ein Router, der IP-Pakete von einem Teilstück zum nächsten hinüberhievt. Die Funktionalität des Routers wird dabei von den Adressen in den einzelnen IP-Paketen und seinen Routingtabellen gesteuert. In den Routingtabellen ist eingetragen, in welche Richtung der Router Pakete mit einer gegebenen Zieladresse weiterzuleiten hat. Die klassische Dienstleistung eines Providers besteht darin, einen Übergang zwischen einer Wählverbindung (Privatkunden) oder einer regionalen Standleitung (Firmenkunden) und einer oder mehreren Standleitungen in das Ausland zu bieten. Dem Provider ist dabei nicht bekannt, welche Dienste der Kunde in Anspruch nimmt oder welche Daten abgerufen werden.

Sperrungen können hier über Eingriffe in die Routingtabellen von Routern vorgenommen werden. Es ist beispielsweise leicht möglich, alle Pakete an bestimmte Zieladressen am Router verwerfen zu lassen (eine Route zu *erden*). Mit diesem Verfahren werden ganze Rechner unerreichbar: Bei der durch den DFN-Verein praktizierten Sperrung des Rechners mit dem Namen *www.xs4all.com* waren auf diese Weise die Webseiten von mehr als 6000 Anbietern nicht mehr abrufbar, es konnte keine Mail auf der Maschine www.xs4all.com eingeliefert werden, und auch alle andere Kommunikation des DFN-Vereins mit dieser Maschine wurde unterbunden.

Die Auswahl eines Dienstes erfolgt im TCP/IP-Protokoll in der Regel durch die Angabe einer TCP-Portnummer. Mit Hilfe dieser Portnummer könnte eine selektivere Sperrung eines Dienstes erfolgen. Beispielsweise sind einige Router in der Lage, nach entsprechender Konfiguration TCP-Verkehr fuer den Port 80 (HTTP) zu einer Zieladresse zu sperren, Verkehr auf Port 25 (Mail) zu derselben Adresse aber zu gestatten.

Mit Hilfe eines Vermittlungsrechners (*proxy*) oder anderer Firewallsoftware, denen die im Netzmodell höher liegenden Ebenen zugänglich sind, kann eine selektive Sperrung auf der Ebene von Dienstelementen (einzelnen Seiten, einzelnen Nachrichten) erreicht werden. Die Firewallsoftware muß herbei jedoch fuer jeden Dienst (WWW, News, Mail, IRC etc.) angepaßt werden. Solche Systeme sind in der Regel sehr aufwendig im Betrieb, da sie für die nutzenden Clients die volle Leistung aller durch den Client in Anspruch genommenen Dienste simulieren müssen. Mit steigender Zahl von Clients skalieren sich diese Systeme ausgesprochen schlecht. Trotzdem setzen einige totalitäre Staaten auf dieses System, um das Eindringen mißliebiger Inhalte in das Land zu erschweren: In China, Singapur und in den Golfstaaten läuft saemtliche Kommunikation mit dem Ausland durch staatlich betriebene Firewalls.

Sperrung von IP-Adressen und der Einsatz von Firewalls ist unter bestimmten Voraussetzungen kombinierbar, dadurch ist eine Entlastung der Firewallmaschine möglich: Anstatt die Route zu einer zu sperrenden Maschine zu erden, läßt man alle Routen zur zu sperrenden Maschine auf einen Firewall zeigen, der dann die Dienste der zu sperrenden Maschine überwacht. Diese Lösung ist je nach Art der zu sperrenden und zu simulierenden Dienste sehr aufwendig zu konfigurieren und zu warten. Zum einen setzt sie einen zentralen Übergangspunkt zwischen dem zu kontrollierenden deutschen Netz und dem Rest der Welt voraus. Zum anderen handelt es sich bei diesem Verfahren um einen klassischen *Man in the middle*-Angriff. Dadurch versagt das Verfahren bei aller stark verschlüsselten Kommunikation, die unempfindlich gegen solche Angriffe ist.

Grundsätzlich sind die Auswirkungen von Filtermechanismen auf die Systemleistung um so höher, je feiner die Granularität der Sperrungen ist und je größer die Liste der zu sperrenden Informationsquellen ist. Systeme wie PICS lassen sich nicht effizient an zentralen Stellen im Netz etablieren, sondern können nur dezentral funktionieren. Alle bisher diskutierten Verfahren der Sperrung setzen auf dritten Maschinen zwischen dem Anbieter der zu sperrenden Information und dem Abrufer an. Denkbar wäre auch eine Sperrung beim Anbieter der Information sowie eine Sperrung beim Abrufer. Dies setzt jedoch eine Kooperation des Anbieters bzw. Abrufers voraus.

Eine Sperrung beim Anbieter würde bedeuten, daß der Anbieter die zu sperrenden Inhalte entweder niemandem anbietet oder daß er sie nur bestimmten Personen nicht anbietet. Ein personenselektives Anbieten von Inhalten setzt selbst bei Kooperation des Anbieters voraus, daß der Anbieter den Abrufer einer Information zweifelsfrei identifizieren kann und daß ihm genaue und juristisch hieb- und stichfeste Entscheidungstabellen vorgelegt werden, die es ihm erlauben, automatisch zu entscheiden, wem er welche Inhalte ausliefern darf. Ein Identifikationsmechanismus, der das Geforderte leistet, existiert derzeit nicht einmal im Ansatz und ist auch nicht in absehbarer Zeit realisierbar. Insbesondere kann nicht aus der IP-Adresse oder dem Rechnernamen eines Absenders auf seine Identität oder seinen physikalischen Aufenthalt geschlossen werden: Deutsche Kunden von amerikanischen Online-Diensten erscheinen im Netz als aus den Vereinigten Staaten kommend. Ähnliches gilt für Mitarbeiter multinationaler Konzerne.

Eine Sperrung beim Abrufer würde bedeuten, daß die angebotenen Inhalte nach bestimmten Bewertungskriterien ausgezeichnet sind (*rating*, z.B. nach PICS) und daß der Abrufer selbst seine Software so konfiguriert, daß Seiten mit bestimmten Ratings nicht mehr abgerufen werden können. Eine Kooperation des Anbieters wäre hier wünschenswert, ist aber nicht notwendig, da die Bewertungen auch von Servern Dritter geliefert werden können.

Auf welche Weise können Sperrungen unterlaufen werden?

Für den Nutzer stellt sich eine Sperrung von Inhalten als Betriebsstörung dar. Er wird nach Wegen suchen, die ordnungsgemäße Funktion des Netzes wiederherzustellen, d.h. die Sperrung zu unterlaufen. Diese Motivation ist um so größer, je stärker sich der Benutzer durch die Sperrung behindert fühlt.

Bei einer Sperrung der physikalischen Kommunikation ist dies nur durch einen Wechsel des Mediums möglich: Wenn etwa ein Störsender in Betrieb genommen wird, wird man versuchen, auf das Telefonnetz auszuweichen und umgekehrt.

Bei einer Sperrung von bestimmten IP-Adressen stehen dem Benutzer mehrere Möglichkeiten offen, die Störung zu umgehen. Alle laufen darauf hinaus, den sperrenden Router vollständig zu umgehen (siehe auch Ulf Moeller: Internet-Zensur: Routingsperren umgehen):

- Der Benutzer wechselt den Internet-Anbieter, notfalls wird er Kunde bei einem ausländischen Provider. Er baut eine Telefonverbindung oder Standleitung zu diesem Provider auf und wickelt seine Kommunikation über diesen nichtsperrenden Provider ab. Der sperrende Router des lokalen Providers wird nicht mehr verwendet, die Sperre ist wirkungslos.
- Diese Situation tritt automatisch ein, wenn der Nutzer Mitarbeiter eines (multinationalen) Konzerns mit einem eigenen Konzernverbundnetz ist, das an mehreren Stellen (im Ausland) mit dem Internet verbunden ist.
- Der Benutzer wird Kunde bei einem zweiten, nichtsperrenden Internet-Anbieter, notfalls im Ausland. Er baut eine TCP/IP-Verbindung zu diesem Provider auf und läßt seine Anwendungen auf dem entfernten Rechner, ggf. im Ausland, ablaufen.
- Es gibt inzwischen eine Reihe von Providern, die solche Angebote routinemäßig anbieten. Die Palette reicht dabei von der Bereitstellung einzelner Dienste (Postboxen fuer E-Mail (z.B. • pobox.com), Webservices (z.B. • geocities.com) usw.) bis zu kompletten Exil-Logins (z.B. • c2.org, • acm.org, • xs4all.nl).

  Der sperrende Router des lokalen Providers sieht keine Kommunikation mit einer gesperrten Adresse, sondern nur Kommunikation mit dem entfernten Provider. Die Zugriffe auf die gesperrten Adressen erfolgen von dort, also erst hinter dem sperrenden Router. Die Sperre durch den Router wird wirkungslos.
- Der Benutzer wird Kunde bei einem zweiten, nichtsperrenden Internet-Anbieter, notfalls im Ausland. Er baut eine Mobile-IP-Verbindung zu diesem Provider auf, d.h. seine IP-Pakete werden in anderen IP-Paketen verpackt zum zweiten Internet-Anbieter geschickt, dort ausgepackt und eingespielt. Optional kann die Kommunikation zum zweiten Provider verschlüsselt erfolgen.
- In Linux müssen dazu die folgenden beiden Kommandos gegeben werden:

  Aktivierung des Interface tunl0 zum entfernten Anbieter myriad.ml.org

  ```
  > ifconfig tunl0 (your.ip.address) pointopoint myriad.ml.org
  ```

  Legen einer Route zu www.xs4all.nl ueber tunl0

  ```
  > route add www.xs4all.nl tunl0
  ```

  Für einen Beobachter erscheint der Nutzer als normaler Kunde des zweiten IP-Providers. Der sperrende Router des lokalen Providers sieht nur eine Verbindung zum entfernten zweiten Provider. Die Sperre ist wirkungslos. Mobile-IP ist ein Routineangebot fuer IP-Provider, die Geschäftskunden betreuen.

Der Anbieter der gesperrten Information kann Abrufer unterstützen, indem er ebenfalls versucht, die Sperre zu unterlaufen. Im Falle der Sperrung des Rechners www.xs4all.nl hat der gesperrte Anbieter die Internet-Adresse seines Rechners alle paar Minuten verändert. Sperrungen einer einzelnen Adresse wurden dadurch wirkungslos, statt dessen mußten ganze Teilnetze gesperrt werden (die Sperrung wurde noch unspezifischer, es wurden als Nebenwirkung noch mehr unbeteiligte Anbieter mitgesperrt).

Während die bisher diskutierten Möglichkeiten des Unterlaufens von Sperrungen unabhängig vom gesperrten Dienst waren, sind die folgenden Moeglichkeiten dienstspezifisch:

WWW

Ähnlich der erwähnten Veränderung der IP-Nummer eines Serverrechners kann auch die Adresse eines Angebotes auf einem Server automatisch verändert werden. Eine automatische Sperrung einzelner Angebote würde dadurch unterlaufen werden, und man müßte wieder den gesamten Rechner pauschal sperren. Dort greifen dann wieder die Methoden zum Unterlaufen einer Komplettsperrung.

Wenn zu einem Angebot eine Suchmaschine existiert, mit der alle Seiten eines Angebotes nach bestimmten Begriffen durchsucht werden können, ist eine einzelne Seite praktisch unter beliebig vielen Adressen zu bekommen (nämlich allen Begriffen, die den Text in der Suchmaschine finden). Eine Sperrung müßte hier zusätzlich den Zugriff auf die Suchmaschine verhindern.

Das Verfahren des indirekten Zugriffs, wie es unter Mobile-IP diskutiert wurde, läßt sich mit Veränderungen auch für WWW einsetzen: Mit Hilfe eines entfernten Webservers, der Zugriffe im Auftrag Dritter abwickelt (*Proxy-Server*), ist ein indirekter Abruf der Seite möglich. Da Proxy-Server mit Zwischenspeicher zur Beschleunigung von Zugriffen üblich sind, ist es in der Regel kein Problem, einen solchen dritten Server zu finden. Im Rahmen der Zensurdiskussion der letzten Monate sind mittlerweile im In- und Ausland auch schon Proxy-Server für solche Umgehungen explizit eingerichtet worden (etwa am MIT fuer chinesische Staatsbürger, die die Zensur im eigenen Land unterlaufen möchten).

Bei verschlüsselter Kommunikation (etwa mit dem in allen gaengigen Browsern eingebauten SSL-Support) entsteht ein nicht mehr in Echtzeit einsehbarer und nicht einfach verfälschbarer Kanal zwischen Server und Client. Fuer Dritte ist nicht erkennbar, welche Seiten abgerufen werden und welche Informationen sie enthalten.

News

Artikel in den USENET News liegen in zahlreichen Kopien auf Tausenden von Servern überall auf der Welt vor. Löschungen (*Cancel*) werden von vielen dieser Server nicht mehr ausgeführt, nachdem es seit einigen Jahren immer wieder zu gefälschten Löschaufforderungen von Saboteuren kam. Die großen Archive fuer USENET News (DejaNews und AltaVista) führen grundsätzlich keine Löschungen aus. Über Archivanfragen ist es daher in der Regel möglich, auch auf ältere und lokal nicht mehr verfügbare Texte zuzugreifen. Dabei gilt wie bei Suchmaschinen für Webseiten (siehe oben): Artikel sind nicht nur unter einer festen Bezeichnung abrufbar, sondern werden auch zu beliebigen im Artikel enthaltenen Stichworten gefunden.

Im Rahmen einer Untersuchung der bayrischen Staatsanwaltschaft wurde der Betreiber Compuserve aufgefordert, einige Newsgroups grundsätzlich nicht mehr bereitzustellen, da bei ihnen davon auszugehen sei, dass diese in Deutschland strafrechtlich relevante Inhalte enthielten. Die Leser dieser Gruppen beziehen diese jetzt direkt von anderen, nicht gesperrten Newsservern. Ausserdem gehen die Autoren von Artikeln für solche schlecht verbreiteten Newsgroups immer mehr dazu über, ihre Artikel zusätzlich in andere, thematisch unpassende, aber besser verbreitete Gruppen zu setzen. So kam es zum Beispiel anläßlich der Sperrung des Servers www.xs4all.nl wegen des Angebotes der verbotenen Zeitschrift Radikal, Ausgabe 154 zweimal zu je einem Posting der Komplettausgabe der Radikal in den Diskussionsforen de.soc.zensur (Diskussion ueber Zensur und Inhaltskontrolle) und de.org.politik.spd (Forum des virtuellen Ortsverbandes der SPD).

Da die Neueinrichtung von Newsgroups technisch automatisiert werden kann, kommt es vielfach zur Neueinrichtung schlecht verbreiteter Gruppen unter neuem Namen oder zum Angebot bekannter Gruppen unter Aliasnamen. So wurde die Gruppe de.talk.sex (Diskussionsforum ueber Sexualität) an einer deutschen Universität mehrere Jahre lang unter dem Namen de.soc.verkehr geführt, nachdem dort entschieden worden war, keine Gruppen mehr anzubieten, deren Bezeichnung den Begriff sex enthält.

Andere Effekte von Sperrungsversuchen

Jede Sperre kann unterlaufen werden, indem die gesperrte Information vielfach repliziert wird. Dann ist jedes Vorkommen dieser Information gesondert zu sperren. Dadurch werden die unangenehmen Nebenwirkungen der Sperrung vervielfacht, bis die Kosten fuer die Sperrung ihren Nutzen übersteigen. Im Falle der Sperrung von www.xs4all.nl wegen des Angebotes der verbotenen Radikal 154 existierten innerhalb kürzester Zeit über 40 Kopien der gesperrten Information. Die 6000 aus technischen Gründen mitgesperrten Anbieter wurden jedoch nicht repliziert. Bezüglich der angestrebten Wirkung wurde also eher das Gegenteil erreicht, während viele Anbieter durch die unbeabsichtigten Nebenwirkungen Verluste hinnehmen mußten.

Mit Hilfe der USENET News ist diese Replikation tausendfach automatisiert und mit minimalem Aufwand vorzunehmen. Aus diesem Grunde kam es nach der Sperrung von xs4all auch zu einer Verbreitung der Webseiten der Radikal in den News (die Webseiten der anderen 6000 Kunden von xs4all wurden nicht in die News eingespielt).

Alle Kommunikation mit Hilfe des TCP/IP-Protokolls ist konstruktionsbedingt eine individuelle Ende-zu-Ende-Kommunikation zwischen zwei Partnern. Selbst bei Be-

trachtung des Dienstes ist nicht erkennbar, ob die abgerufenen Informationen privater Natur sind (es ist möglich und für viele Anwender auch notwendig, ihre persönliche Post per WWW zu lesen) oder ob es sich um öffentliche Information handelt. Derartige Information kann sogar gemischt auf einer Webseite auftreten. Es ist zweifelhaft, inwieweit eine Kontrolle solcher Verbindungen durch unspezifisches Abhören (ohne richterlichen Beschluß) gestattet ist, selbst wenn dieses Abhören durch einen Roboter geschieht, der auf Schlüsselworte oder Ratings reagiert.

Nicht nur vom Standpunkt der Kontrolle der Bewerter, sondern auch vom Standpunkt des technischen Netzbetriebes ist eine Offenlegung aller Sperrungen unbedingt notwendig. Wenn Sperrungen von Rechnern oder einzelnen Angeboten massenhaft umgesetzt werden, ist für den einzelnen Systembetreiber genau wie für den einzelnen Anwender nämlich nicht mehr entscheidbar, ob eine technische Störung vorliegt, die zu beheben ist, oder ob eine inhaltlich begründete Sperrung vorgenommen wurde. Damit wird einer zuverlässigen Fehleranalyse durch die Betreiber von Netzen oder einzelnen Maschinen jede Grundlage entzogen, da aus dem Vorliegen einer Störung keine sichere Verhaltensvorschrift zu ihrer Behebung abgeleitet werden kann. Andererseits können offengelegte Sperrlisten natuerlich leicht als Kataloge fuer sexuell explizite oder gewalttätige Angebote mißbraucht werden. Eine Sperrung wäre dann eine Art Qualitaetssiegel. Offengelegte Sperrungen sind mit entsprechend modifizierten Programmen außerdem automatisiert umgehbar.

Modifikation des Internet

In dem heutigen Internet können Sperren nach den obigen Ausführungen also nicht oder nur mit unvertretbar hohen Kosten und Nebenwirkungen realisiert werden. Daraus ergibt sich die Frage, inwieweit das Internet modifiziert werden müßte, um effizientes Sperren von Inhalten zu erlauben.

Prinzipiell bieten Firewallsysteme (die von Unternehmen eingesetzt werden, um ihr Netz gegen unbefugtes Eindringen aus dem Internet zu schützen) einen Ansatz, effektive Sperren aufzubauen. Durch die Philosophie, nur solchen Daten das Passieren der Barriere zu gestatten, denen es explizit gestattet wurde, erzwingt man das Einhalten von Richtlinien.

Ähnliche Richtlinien müßten fuer die Nutzung der Internet-Dienste durch die Benutzer aufgestellt und ihre Einhaltung erzwungen werden. Dies kann durch die Verwendung der Firewalltechnologie als Barriere zwischen den Anwendern und dem Internet oder durch die Verwendung proprietärer Protokolle erzwungen werden. Entscheidend ist, daß Teilnehmer im Netz ausschließlich identifizierbar agieren koennen, daß nur freigegebene Dienste, Protokolle und Datenformate verwendet werden, daß die Verwendung kryptographischer Verfahren verboten wird und daß sämtliche Aktivitäten protokolliert werden. Durch diese Massnahmen soll sichergestellt werden, daß der Benutzer einer Sperre nicht mehr ausweichen kann durch Wechsel der Identität, des Protokolls oder durch Verschleierung der Daten.

Unabhängig von der Frage, ob ein solches Verfahren mit einem demokratischen Rechtsstaat vereinbar wäre, gibt es auch wirtschaftliche und technische Gründe, die dagegen sprechen: Ein solches Netz wäre zentralistisch gesteuert und könnte nur unter großem Zeit- und Kostenaufwand an veränderte Anforderungen angepaßt werden. Sämtliche Online-Dienste haben dieses Modell auf Druck ihrer kommerziellen Benutzer aufgegeben. Der administrative Overhead einer solchen Lösung auf nationaler Ebene wäre gewaltig. Ausserdem wuerde jede Beschraenkung kryptographischer Verfahren eine Nutzung des Internet zur Uebermittlung sensitiver Informationen beeinträchtigen.

Insgesamt könnte ein solches Modell katastrophale Standortnachteile mit sich bringen. Kommunikation ist eine Ressource, die in ihrer Bedeutung den Arbeitskräften oder der Verkehrsinfrastruktur in keiner Weise nachsteht. Auf der anderen Seite kann man, wie sich am Beispiel China zeigen läßt, selbst auf diese Art die Verbreitung unerwünschter Inhalte nur begrenzt unterbinden, denn für jede der oben genannten Massnahmen existieren wiederum Gegenmaßnahmen.

Bewertung

Eine zentrale Sperre von Inhalten im Internet läßt sich technisch nicht paßgenau vornehmen, ließe sich von den Benutzern bei Bedarf umgehen und wäre mit hohen Kosten verbunden (siehe auch Heimo Ponnath: Pornographie im Internet? Dichtung und Wahrheit, inside online 2/3 1996). Bedingt durch die globalen Datennetze zeigt sich hier der Paradigmenwechsel in den Aufgaben des Staates durch die Informationsgesellschaft, wie Alexander Rossnagel beschreibt (Alexander Rossnagel: Globale Datennetze: Ohnmacht des Staates - Selbstschutz der Buerger, ZRP 1997, Heft 1, 26-30). Die Ohnmachtserfahrung des Staates in der globalisierten Welt bedeutet jedoch nicht gleichzeitig eine Kapitulation vor den neuen Gefahren, sondern die modernen Informationstechnologien bergen vielfältige Möglichkeiten, daß der Buerger sich selbst schützen kann. Daraus erwächst die Verpflichtung für den Staat, Strukturen zu schaffen, die seine Bürger befähigen, ihre Interessen in der Welt der Netze selbstbestimmt zu schützen.

Hier bietet also die dezentrale Kontrolle und Filterung durch den Benutzer einen Lösungsansatz. Dazu müssen jedoch die Bewertungen durch Dritte (etwa nach dem PICS-System) transparent und nachvollziehbar sein. Beispielhafte Filterkonfigurationen können von einer Vielzahl von Interessengruppen vorgeschlagen werden; der Benutzer muß jedoch die Moeglichkeit haben, seine eigene Konfiguration individuell vorzunehmen oder anzupassen.

Ein universelles Rating wie PICS ist mit erhöhtem Zeitaufwand und zusätzlichen Kosten verbunden. Eine Reihe von Anbietern wird daher darauf verzichten. Den Ratingorganisationen kommt ein hohes Maß an Verantwortung zu, da jede Vorbewertung bereits zur Meinungsbildung der potentiellen Abrufer beiträgt und da absichtliche oder unabsichtliche Fehlbewertungen großen Schaden anrichten koennen. Geht es lediglich um die Gewährleistung eines Jugendschutzes im Internet, wäre es sehr viel billiger und unkritischer, wenn die Anbieter auf freiwilliger Basis ihre kindgerechten Materialien kennzeichneten und spezielle Kinderbrowser ähnlich dem TV-Kinderkanal nur solche Angebote darstellten (siehe The Net Labelling Delusion: Protection or Oppression).

Die Erfahrungen in den USA zeigen, daß Organisationen das Instrument der Bewertung von Inhalten für die Durchsetzung ihrer eigenen politischen Ziele unter dem Deckmantel des Jugendschutzes oder der Aufrechterhaltung der öffentlichen Moral mißbrauchen. Es ist zu verhindern, daß die Definition moralischer und gesellschaftlicher Werte in den Aufgabenbereich privater Organisationen übertragen wird. Durch eine Offenlegung der Bewertungsmaßstäbe und aller Bewertungen kann diese Gefahr des Mißbrauchs reduziert werden.

Danksagung

Wir danken Hannes Federrath und Andreas Pfitzmann von der Technischen Universitaet Dresden für zahlreiche Anregungen und Diskussionen, die zur Entstehung dieses Textes beigetragen haben.

„In politischer Perspektive fehlgeleitet und in rechtlicher Hinsicht unhaltbar“

Der Beauftragte für Neue Medien der SPD-Bundestagsfraktion, **Jörg Tauss**, kritisiert in deutlicher Form die Sperrungsverfügungen der Bezirksregierung Düsseldorf. In seiner Stellungnahme vom 20. Februar 2002 stellt Tauss fest, dass “das Vorgehen der Düsseldorfer Bezirksregierung sowohl in rechtlicher, technischer als auch in politischer Hinsicht untragbar” sei. Die von Regierungspräsident Büssow den Providern nahe gelegten Sperrmaßnahmen wie die leicht zu umgehende DNS-Umleitung und Proxy- oder Router-Lösungen überschreiten laut Tauss “die Schwelle von der Einzelfallmaßnahme in Richtung einer verfassungsrechtlich bedenklichen Schaffung einer präventiven Infrastruktur zur Inhaltekontrolle im Internet.” Eine zentrale Filterinstanz, wie sie von der Bezirksregierung geplant sei, sei aus demokratischer Sicht keinesfalls wünschenswert.Tauss, der die Entstehung der zugrundeliegenden und 1997 entstandenen “Multimedia-Gesetzgebung”, zu der auch der Mediendienstestaatsvertrag gehört, von Anfang an kritisch verfolgt und spricht nun von einer “Pervertierung des Mediendienste-Staatsvertrags”.

Der Volltext seiner Stellungnahme ist abrufbar unter der folgenden Adresse:

http://www.tauss.de/service/presse/stellungnvahmesperrungsverfuegung

Auch sein Parlamentskollege, der FDP-Abgeordnete **Rainer Funke**, rechtspolitischer Sprecher seiner Fraktion, verurteilte die Sperrverfügungen.Was „vordergründig als eine konsequente Reaktion der wehrhaften Demokratie“ erscheine, führe tatsächlich zu einer „tiefgreifenden Beeinträchtigung“ von Werten und Rechten, „ohne dass für den Kampf gegen den Rechtsextremismus etwas gewonnen ist.“ Zwar müssten die Feinde unserer Gesellschaft „mit allen rechtsstatlichen Mitteln und durch alle gesellschaftlichen Kräfte energisch bekämpft“ werden, untaugliche oder unverhältnismäßige Eingriffe in die im GG besonders geschützte Informations- und Pressefreiheit dürften dabei aber keine Rolle spielen.

Die medienpolitische Sprecherin der PDS-Fraktion im Bundestag, **Angela Marquardt,** lehnt „den EInsatz von Filtern zur Säuberung des Internet grundsätzlich ab“. Filter funktionierten nach der „Vogelstrauß-Methode“ und wer die anstößigen Seiten wirklich sehen wolle, der “wird sie auch finden”.

Martina Krogmann, Internet-Beauftragte betont die „Wichtigkeit eines funktionierenden Jugendschutzes“ auch und gerade im Internet, verurteilt jedoch „Maßnahmen, die deutsche Unternehmen belasten, ohne das Ziel auch nur annähernd zu erreichen“ als „völlig deplaziert“.

Bündnis 90/Die Grünen haben auf der Bundesdeliguertenkonferenz am 4. bis 5. Mai 2002 in Wiesbaden einen ähnlich grundsätzlichen Beschluß gefasst, der auch Eingang ins Wahlprogramm der Partei fand:

„Wir erkennen die Beduetung der informationsfreiheit als zentrale Voraussetzung für eine freie und möglichst gut informierte demokratische Öffentlichkeit an. Für die Leistungsfähigkeit eines demokratischen verfassungsstaates ist es notwendig, eine möglichst offene Kommunikationsstruktur zu erhalten. Deswegen lehnen wir zentrale Sperrungen von Webseiten ab. Diese sind technisch und demokratisch schwer zu kontrollieren und bergen mehr Gefahrenpotenziale als Nutzen für unsere Demokratie. Wir lassen uns nicht von populistischen Lösungen beeinflussen, die einen vermeintlichen Jugendschutz suggerieren. Stattdessen setzen wir auf Medienkompetenz und Selbstkontrolle.“

Erklärung gegen die Einschränkung der Informationsfreiheit

http://odem.org/informationsfreiheit/ (mit Unterschriften-Liste)

Am 8. Februar 2002 hat die Bezirksregierung Düsseldorf Sperrungsverfügungen gegen mehr als 80 Anbieter von Internet-Zugängen, sogenannte Access-Provider, erlassen. Die Bezirksregierung beruft sich dabei auf ihre Kompetenz als Landes-Aufsichtsbehörde für den gesetzlichen Jugendschutz und die »Ahndung von Ordnungswidrigkeiten« gemäß des Mediendienstestaatsvertrags.

Obwohl die Behörde für Mediendienste wie Videotext und nicht für Telekommunikationsdienste zuständig ist, wurden die Provider aufgefordert, zunächst zwei rechtsextremistische Domains in den USA für ihre Kunden unzugänglich zu machen. In der Praxis werden durch diese Sperrungen nicht nur die Websites blockiert, sondern es wird auch jegliche Kommunikation mit den Betreibern, beispielsweise via E-Mail, unterbunden. Ein zur Zeit in einem Pilotprojekt getestetes Filtersystem soll zukünftig nach einer »Schwarzen Liste« problematische Inhalte (beispielweise nach deutschen Gesetzen rechtswidrige oder jugendgefährdende) des ausländischen Internets in Deutschland sperren - wer diese Sperr-Liste führen soll und ob sie rechtsstaatlicher Kontrolle unterworfen sein wird, ist bislang nicht bekannt.

Gesellschaftlicher Rückschritt

Wir verurteilen das Vorgehen der Bezirksregierung Düsseldorf und weitergehende Pläne aus den folgenden Gründen:

Providerseitige Filtersysteme stellen unangemessene Eingriffe in Grundrechte dar

Der Artikel 5 des Grundgesetzes der Bundesrepublik Deutschland gibt allen Bürgern das Recht, sich ohne Beschränkung und frei aus allen zur Verfügung stehenden öffentlichen Quellen informieren zu dürfen. Diese Informationsfreiheit bildet das unverzichtbare Rückgrat einer informierten und wehrhaften Demokratie. Filtersysteme dienen dazu, Informationsquellen für Bürger unzugänglich zu machen. Dies sind Maßnahmen, die an totalitäre Staaten und »Feindsenderverbote« erinnern.

Wir sind entsetzt, dass die Einschränkung der Informationsfreiheit auch für Wissenschaft und Forschung gelten soll. So ist geplant, dass sich einzig Hochschulen durch Sondergenehmigungen den Filterungsmaßnahmen entziehen können – solche Regelungen wurden etwa in der DDR praktiziert. Betroffen sind auch Medienschaffende und Journalisten – ihnen ist es nicht mehr möglich, uneingeschränkt an Informationen zu gelangen, die zwar weiterhin vorhanden sein werden, aber nicht abgerufen werden können.

Diese Einschränkungen des Grundrechtes der Informationsfreiheit betrachten wir als gesellschaftlichen Rückschritt. Dieser wiegt deutlich schwerer als die mögliche Gefahr, die von problematischen Internet-Angeboten für einzelne oder unsere Demokratie ausgeht.

Nicht gegen Infrastrukturen, sondern gegen Inhalte vorgehen!

Das Internet ist ein Kommunikationsmittel. Es ist daher eher mit Telefon und Briefpost vergleichbar als mit Fernsehen und Rundfunk. Wie bei der Kommunikation mittels Telefon oder Brief sollte auch im Internet eine vertrauliche Kommunikation ohne behördliche Eingriffe die Regel sein. Mit Filtersystemen wird nicht gegen die Urheber illegaler Inhalte vorgegangen, sondern unmittelbar in die neutrale technische Infrastruktur der Kommunikation selbst eingegriffen.

Sperrungen verfehlen die Zielgruppe

Auch wenn die zur Zeit verfügten Maßnahmen mit EDV-Grundkenntnissen umgangen werden können, bedeuten sie und alle weiteren Bestrebungen doch erhebliche Eingriffe in Grundrechte. Die Sperrungen werden gerade bei der Zielgruppe ihre Wirkung verfehlen und im schlimmsten Falle zu einer Mystifizierung und Glorifizierung der Inhalte führen. Filtersysteme sind kontraproduktiv: Wer unerwünschte Inhalte im Internet nur ausblendet, handelt aktionistisch und entzieht sich der eigentlichen Herausforderung, gegen die Ursachen auf gesellschaftlicher Ebene vorzugehen.

Wir fordern aus diesen Gründen, providerseitige Filtersysteme als Mittel im Kampf gegen illegale und unerwünschte Internet-Inhalte auszuschließen. Wir fordern, stattdessen auf politischem Wege Lösungen zu finden und gegen die Urheber dieser Inhalte vorzugehen.

Setzen wir uns mit dem Problem auseinander, anstatt es auszublenden!

Impressum

DAVID

Deutsche Arbeitsgemeinschaft zur Verteidigung
der Informationsfreiheit in Datennetzen

http://www.david-gegen-goliath.org/

V.i.S.d.P:
Alvar c.h. Freude, alvar@ODEM.org
Ludwig-Blum-Straße 37, 70327 Stuttgart,
(07 11) 2 20 17 72; (01 79) 13 46 47 1
http://alvar.a-blast.org/

Mitarbeit und Unterstützung:

Artikel5.de
Die Blinde Kuh – Suchmaschine für Kinder
Chaos Computer Club e.V. (CCC)
FITUG e.V. Förderverein Informationstechnik und Gesellschaft
FoeBuD e.V.
Junge Liberale Nordrhein-Westfalen e.V.
mikro e.V.
ODEM.org
privatkopie.net
Quintessenz Verein zur Wiederherstellung der Bürgerrechte im Informationszeitalter
VIBE!AT Verein für Internet-Benutzer Österreichs
Virtueller Ortsverein der SPD (VOV)

Tim Bartel, Olaf Boos, Arne Brand, Dr. Michael Boettcher, Markus Borm, Dr. Michael Charlier, RA Jörg Eckhardt, Dragan Espenschied, Alvar c. h. Freude, Trixy Freude, Oliver Gassner, Igor Gilitschenski, Dr. Volker Grassmuck, Bettina Jodda, Christian Hammers, Prof. Dr. Peter A. Henning, Kurt Jaeger, Prof. Wolfgang Kleinwächter, Torsten Kleinz, Peter Kuhm, Stefan Lachmann, Tim Landscheidt, Wolfgang Leven, Andreas A. Milles, thomas molck, Stefan R. Müller, Andreas Neumann, Jens Ohlig, padeluun, Oliver Passek, Boris Piwinger, Silvan Rehberger, Rüdiger Rowold, Jörg-Olaf Schäfers, Andreas Schmidt,Michael Peter Schmidt, Burkhard Schröder, Moritz Schulte, Dr. Horst-Walter Schwager, Stefan Sels, RA Thomas Stadler, Florian Steglich, RA Tobias H. Strömer, Lars Weiler

Ich weiß, dass es hier sehr starke Einwände gibt, aber man kann die Technologie nicht verbannen oder Inhalte regulieren. Regulation ist Zensur: ein Erwachsener sagt dem anderen, was er machen oder sehen darf. Für mich ist diese Vorstellung schrecklich. Universalität ist der Schlüssel. Man muss alles im Web darstellen dürfen.

Tim Berners-Lee, Erfinder des World Wide Web

„So gerne wir die menschenverachtenden Neonazis mit ihren Hetzparolen daraus verbannt sähen, und so sehr wir es begrüßen, dass Nazi-Propaganda in Deutschland verboten ist, halten wir Zensurbestrebungen im Internet für einen Rückschritt im demokratischen Prozess. Die Auseinandersetzung damit ist zwingend."

SHOA-Projekt
http://www.shoahproject.org/links/links.htm