

Sperren und Blocken illegaler Inhalte im Internet

Rechtliche Rahmenbedingungen, technische Möglichkeiten und wirtschaftliche Auswirkungen

**Manuskript des am 30.01.2002 von Thomas Rickert auf der
Kongressmesse ONLINE 2002 gehaltenen Vortrages**

Sperren und Blocken illegaler Inhalte im Internet

Version 1.02

4. September 2002

eco Electronic Commerce Forum -
Verband der deutschen Internetwirtschaft e.V.

Arenzhofstr. 10
50679 Köln

Tel.: +49 (0) 221 - 70 00 48 - 0
Fax: +49 (0) 221 - 70 00 48 - 11

E-Mail: info@eco.de
<http://www.eco.de>

I. Rechtliche Grundlagen

Die Verpflichtung von Diensteanbietern zur Sperrung von Inhalten steht in engem Zusammenhang mit deren Haftung. Daher soll nachfolgend auf die rechtlichen Grundlagen für die Verantwortlichkeit von Internet Service Providern eingegangen werden:

In Deutschland hat der Gesetzgeber im Jahre 1997 mit dem Informations- und Kommunikationsdienstegesetz (IuKDG) Regelungen zur Verantwortlichkeit von Internet Service Providern aufgestellt. Dieses Gesetz stellte jedoch keine abschließende Kodifizierung dar, da die Länder nicht mit einer Regelung der Materie nur durch den Bund einverstanden waren. Als Folge finden sich nunmehr weitgehend gleichlautende Regelungen auch im Mediendienste-Staatsvertrag (MdStV) der Länder, was mit erheblichen Abgrenzungsproblemen der Anwendungsbereiche verbunden ist.

Mit der E-Commerce-Richtlinie sollte das Problem später auf europäischer Ebene einheitlich gelöst und die Rechtslage weiter geklärt werden. Leider hat die deutsche Umsetzung der Richtlinie im Gesetz zum Elektronischen Geschäftsverkehr (EGG) jedoch in Teilen einen Rückschritt mit sich gebracht. Zum Beispiel stellt der neue Gesetzeswortlaut im Gegensatz zum bisherigen nicht klar, dass eine Sperrung vom Diensteanbieter nur verlangt werden kann, sofern dies „technisch möglich und zumutbar“ ist. Wenngleich aus allgemeinen Grundsätzen folgt, dass auch ohne eine ausdrückliche Nennung dieser Voraussetzungen der Staat Unmögliches oder Unzumutbares vom Regelungsadressaten nicht verlangen kann, ist die Streichung unglücklich. Der Gesetzestext wäre mit der Klarstellung einfacher verständlich und die erheblichen Irritationen bei Providern wären vermieden worden.

Zudem hat die Neuregelung im EGG nichts am gleichzeitigen Fortbestehen des MdStV geändert.

Die Verantwortlichkeit der Diensteanbieter lässt sich gleichwohl wie folgt darstellen, wobei verschiedene Tatbestände je nach Art der erbrachten Leistungen greifen:

- Wer eigene Inhalte anbietet, beispielsweise eine eigene Website veröffentlicht, ist stets in vollem Umfang für die von ihm vorgehaltenen Informationen verantwortlich.
- Diensteanbieter sind für fremde Inhalte, die sie zur Nutzung bereithalten, nur dann verantwortlich, wenn sie von diesen Inhalten Kenntnis haben und nicht unverzüglich die Informationen entfernen oder den Zugang zu ihnen sperren. Diese Konstellation beschreibt typischerweise einen Anbieter von Webspace, der – um rechtliche Nachteile zu vermeiden – dann reagieren muss, wenn er von rechtswidrigen Inhalten erfährt, die einer seiner Kunden auf seinem System abgelegt hat.
- Für unveränderte fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, sind Diensteanbieter grundsätzlich nicht verantwortlich. Diese Regelung bezieht sich auf sogenannte Access-Provider, die lediglich ihre technische Infrastruktur bereitstellen, unter deren Zuhilfenahme der Kunde sodann Inhalte Dritter abrufen. Die Regelung stellt klar, dass auch eine kurzzeitige Speicherung, das Caching, bei Vorliegen bestimmter Parameter von dieser Privilegierung umfasst ist. Es sind dies unter anderem, dass keine Veränderungen der Informationen vorgenommen werden und unverzüglich gehandelt, das heißt die Informationen entfernt oder der Zugang zu ihnen gesperrt wird, sobald der Diensteanbieter Kenntnis davon erlangt, dass beispielsweise eine gerichtliche Sperrungsanordnung vorliegt.
- Die Beschränkung der Verantwortlichkeit von Vermittlern lässt jedoch die Möglichkeit unberührt, dass ein Gericht oder eine Behörde vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern.

Wichtig ist zudem die Feststellung, dass sowohl nach der alten wie auch nach der neuen Regelung keine allgemeine Verpflichtung des Diensteanbieters besteht, proaktiv die von ihm gespeicherten oder übermittelten fremden Inhalte zu überwachen oder selbständig nach rechtswidrigen Inhalten oder Aktivitäten zu suchen.

Wir können die vorgestellten Regelungen an dieser Stelle auf folgende Kurzformel herunterbrechen:

Der Diensteanbieter soll für

- eigene Informationen stets die Verantwortung übernehmen und für
- fremde Inhalte lediglich dann zur Rechenschaft gezogen werden, wenn er auf diese aufmerksam gemacht wird und nichts unternimmt, obwohl er es zumutbar könnte.

Es dürfte Einvernehmen darüber bestehen, dass dieses Haftungssystem eine gerechte Lösung darstellt, da sie primär die Inhalteanbieter adressiert und lediglich bei Vorliegen weiterer Voraussetzungen die technischen Dienstleister haftbar macht.

II. Fallgruppen

Lassen Sie uns nun einige Konstellationen durchspielen, um Probleme und deren Auswirkungen aufzudecken, sowie nach Lösungsansätzen zu suchen. Wir werden in diesem Zusammenhang auch auf einige prominente Fälle zu sprechen kommen, von denen Sie möglicherweise gehört haben.

1. Inanspruchnahme des Inhalteverantwortlichen

Am wenigsten Probleme macht es, wenn ein rechtswidriger Inhalt in Deutschland zum Abruf gespeichert wird und der Inhalteverantwortliche bekannt ist. In diesem Fall kann der Verantwortliche unmittelbar zivil- und gegebenenfalls strafrechtlich zur Rechenschaft gezogen werden.

Der Umstand, dass man für das einzustehen hat, was man veröffentlicht, ist allerdings denjenigen, die rechtswidrige Inhalte veröffentlichen möchten, nicht verborgen geblieben. Die Folge ist, dass die Täter ihre Aktivitäten in Länder mit „schwächeren“ Rechtsordnungen verlegen und bedenkliche Inhalte immer weniger in Deutschland gespeichert werden. Sofern die Inhalte dennoch im Inland abgelegt sind, versuchen die Täter, ihre Identität zu verbergen. Kriminelle kommen in den seltensten Fällen ihrer Verpflichtung zur Veröffentlichung einer Anbieterkennzeichnung nach.

Entgegen einer bei Laien weit verbreiteten Auffassung ist auch die Tatsache, dass eine Homepage mit rechtswidrigen Inhalten über einen Domain Namen unter der für Deutschland stehenden Top Level Domain „.de“ abrufbar ist, kein Hinweis darauf, dass der Inhalteverantwortliche in Deutschland zu finden ist. Dies liegt daran, dass über eine „.de“-Domain auf einen Webserver in aller Welt referenziert werden kann. Man trifft häufig die Praxis an, dass „.de“-Domains – bei Nennung falscher Kontaktdaten im Rahmen der Registrierung - nur genutzt werden, um auf einen Server weiter zu leiten, der sich im Ausland befindet.

Selbst, wenn man wie ich die Auffassung vertritt, dass demjenigen, der eine solche Weiterleitung auf strafbare Inhalte veranlasst, die Inhalte wie eigene zugerechnet werden müssen, da er bewusst und zielgerichtet auf sie verweist, können die Verantwortlichen nur schwer gefasst werden.

Für die Strafverfolgungsbehörden besteht neben dem Auffinden der Täter jedoch das Problem, dass die meisten strafbaren Inhalte gerade nicht von Menschen produziert und veröffentlicht werden, die der deutschen Rechtsordnung unterliegen. Dies ist insbesondere dann misslich, wenn Äußerungsdelikte betroffen sind, hinsichtlich derer aus historischen Gründen in Deutschland besonders strenge Vorschriften gelten. Rechtsextremistische Äußerungen, die in Deutschland strafbar sind, sind in den USA durch das Recht der freien Meinungsäußerung geschützt und damit rechtmäßig. In dieser Konstellation scheidet gar eine Einschaltung der amerikanischen Kollegen aus.

2. Inanspruchnahme des hostenden Providers

Konfliktträchtiger als die vorgenannte Fallgruppe, die die Providerlandschaft meistens nicht unmittelbar betrifft, ist die Inanspruchnahme des Providers, der rechtswidriges Material hostet, das heißt auf seinem System gespeichert hat und zum Abruf bereithält. Wir haben zuvor festgestellt, dass in dieser Konstellation der Provider erst dann haftet, wenn er Kenntnis von den Inhalten erlangt und dennoch nichts unternimmt, um die Inhalte zu entfernen oder zu sperren. Die Verschaffung der Kenntnis von diesen Inhalten kann durch jedermann erfolgen. Es ist daher nicht gewährleistet, dass Beschwerden oder Mitteilungen über Inhalte qualitativ hochwertig sind, das heißt sich wirklich auf rechtswidriges Material beziehen. Gleichwohl muss sich der Diensteanbieter damit beschäftigen, um Nachteile zu vermeiden. Schwerer wiegt jedoch die

Tatsache, dass der Diensteanbieter auch eine rechtliche Bewertung vornehmen muss. Die Prüfung, ob es sich um einen rechtmäßigen Inhalt handelt, der nicht gesperrt oder gelöscht werden muss oder um einen rechtswidrigen, der eben ein solches Verhalten erfordert, ist nicht immer ganz einfach. Der Provider ist hier oft in einer misslichen Lage, denn er steht vor der Entscheidung zwischen den folgenden Handlungsalternativen:

Er kann zum einen den Inhalt auf Zuruf aus dem Netz nehmen. Handelte es sich allerdings um einen rechtmäßigen Inhalt, so verhält sich der Provider gegenüber seinem Kunden vertragsbrüchig und sieht sich dessen Schadensersatzansprüchen ausgesetzt.

Trifft der Provider umgekehrt die falsche Entscheidung und sperrt einen rechtswidrigen Inhalt nicht, so läuft er Gefahr, straf- und zivilrechtlich dafür in Anspruch genommen zu werden.

Die wirtschaftlichen Auswirkungen in diesem Zusammenhang sind durchaus erwähnenswert. Eine Überprüfung von Inhalten auf ihre Rechtmäßigkeit ist zeitintensiv und kann häufig lediglich durch juristisch geschultes Personal erledigt werden. Verfügt ein Unternehmen nicht über eine eigene Rechtsabteilung, so schlägt eine Prüfung durch einen beauftragten Rechtsanwalt pro Fall oft selbst dann mit ca. 200 Euro netto zu Buche, wenn nur eine Erstberatungsgebühr abgerechnet wird.

Auf Möglichkeiten, wie hier die Verwaltungs- und Beratungskosten für die Provider gering gehalten werden können, kommen wir sogleich zu sprechen.

Zuvor möchte ich jedoch anmerken, dass das zuvor beschriebene Procedere des „Notice and Take Down“ recht gut funktioniert. Die Provider sind daran interessiert, keine strafbaren Informationen auf ihren Systemen vorzuhalten. Um Probleme mit Kunden einzudämmen, die Inhalte vorhalten, die sich in einer schwer auf ihre Rechtswidrigkeit zu beurteilenden Grauzone befinden, haben viele von ihnen eine Impressumspflicht in ihre Vertragsbedingungen implementiert. Wie bereits erwähnt, möchte derjenige, der bedenkliches Material ins Netz stellt, in der Regel unerkannt bleiben und wird seinen Klarnamen nicht preisgeben. Wird ein solcher Kunde bzw. sein Inhalt auffällig, so kann der Provider sich seiner leichter wegen der Verletzung der Impressumspflicht ohne nachteilige Folgen entledigen, als wegen der Inhalte als solche.

An seine Grenzen – auch im wörtlichen Sinne - stößt „Notice and Take Down“ jedoch oftmals, wenn der Host-Provider im Ausland sitzt.

3. Inanspruchnahme des Access-Providers

Die dritte und problematischste Konstellation ist die, in der ein Diensteanbieter lediglich Informationen durchleitet. Typischerweise bietet ein Provider hier seinen Kunden die Möglichkeit, sich in seine technische Infrastruktur einzuwählen und unter deren Nutzung auf das Internet zuzugreifen. Es handelt sich also weder um Inhalte, die der Provider selbst erstellt hat, noch solche, die Dritte bei ihm gespeichert haben und die er beispielsweise von seinen Festplatten löschen könnte.

Der so genannte Access-Provider stellt vielmehr vergleichbar einem Telefoniedienstleister lediglich Leitungen zur Verfügung, über die der Kunde Informationen bezieht, die er eigenverantwortlich ausgewählt hat. Man wird die Deutsche Telekom kaum dafür zur Verantwortung ziehen können, wenn anlässlich eines Telefonats eine strafbare Handlung – beispielsweise die Verabredung zu einem Verbrechen – vorgenommen wird. Ein weiteres gerne bemühtes Beispiel ist das der Verantwortlichkeit der Deutschen Bahn im Zusammenhang mit Drogen, die durch einen Fahrgast ins Inland transportiert werden. Auch hier ist die einhellige Reaktion, dass man der Deutschen Bahn als Transporteur hier weder die Durchsuchung eines jeden Fahrgastes zumuten noch eine Verantwortlichkeit für die unbewusste Mitwirkungshandlung konstituiert werden kann.

Bei Internetdienstleistern wird indes häufig eine abweichende Wertung vorgenommen.

Wir haben soeben die wesentlichen rechtlichen Grundlagen und einige damit in Zusammenhang stehende Probleme kennen gelernt. Insofern kann leicht darauf geschlossen werden, dass immer dann, wenn ein Täter nicht ermittelt oder nicht verfolgt werden kann, der Ruf danach laut wird, dass diejenigen, die rechtswidrige Materialien zu den Rechnern in die Wohnzimmer oder Büros der Bürger „transportieren“, dafür Sorge tragen sollen, dass derartiges abgestellt wird. Das ist vor dem Hintergrund verständlich, dass einige der Materialien, die im Internet abrufbar sind, auch nach der Auffassung überzeugter Vertreter des Rechts auf freie Meinungsäußerung nicht als schützens-, sondern verdammenswert eingestuft werden. Dies ist nicht zuletzt daran zu erkennen, dass die Mehrzahl der amerikanischen Provider, wenngleich aus Rechtsgründen keine Veranlassung dazu besteht, das Hosten rechtsextremistischer Propaganda ablehnt. Eine Folge ist, dass Neonazis nunmehr selbst als Provider auftreten und so Gesinnungsgenossen technische Plattformen zur Verbreitung ihres Gedankengutes zur Verfügung stellen. Eine weitere Folge ist jedoch, dass in dieser Konstellation kein technischer Diensteanbieter mehr angesprochen werden kann, um eine Sperrung oder Löschung rechtswidriger Materialien vornehmen zu lassen. Das Problem ist also nicht mehr da zu lösen, wo Inhalte ins Netz gestellt werden, sondern nur dort, wo sie vermittelt oder heruntergeladen werden.

Der aufmerksame Zuhörer hat bemerkt, dass ich soeben als Ansatzpunkt für Lösungen nicht nur auf die Access-Provider abgestellt habe, sondern auch auf den Ort, wo Internetinhalte heruntergeladen werden. Wir werden auf diesen Aspekt sogleich noch zurückkommen.

Zunächst jedoch verbleiben wir bei den Möglichkeiten und Auswirkungen des Sperrens von Internetinhalten durch Access-Provider.

Als Beispiel sei zunächst der „Radikal-Fall“ genannt. Bei einem niederländischen Provider wurde eine mit zweifelsfrei strafbaren Inhalten versehene Homepage gehostet. Es handelte sich um Beschreibungen, wie Anschläge auf die Bahn durchzuführen sind. Der Generalbundesanwalt rief in der Folge die Internetwirtschaft auf, die Inhalte zu sperren.

Die Internetwirtschaft folgte diesem Ruf in der Weise, dass die IP-Adresse des Webservers, auf dem die Inhalte abgelegt waren, gesperrt wurde. Das Problem war damit jedoch keinesfalls gelöst, sondern im Gegenteil vervielfacht. Die Internetgemeinde fasste das Anliegen der Bundesanwaltschaft als Versuch auf, das Internet zu zensieren. Die Folge war, dass von jetzt auf gleich die Inhalte auf unzähligen Rechnern „gespiegelt“ waren.

In einem weiteren medienträchtigen Fall wurde Yahoo von einem französischen Gericht verpflichtet, für französische Nutzer den Zugriff auf Angebote von Nazi-Memorabilia bei von dem Unternehmen ermöglichten Auktionen im Internet zu sperren.

Sie werden sich möglicherweise fragen, warum dieser Fall nicht in der vorgenannten Kategorie der Inanspruchnahme für den hostenden Provider erwähnt wurde, wenn nicht sogar in der erstgenannten, wenn man der Auffassung ist, dass eine Auktion einschließlich der von Kunden gemachten Angebote als eigener Inhalt des Anbieters einer Auktion anzusehen ist.

Dieser Einwand ist vollkommen berechtigt. Aufgrund der Tatsache, dass es hier oftmals in der Diskussion zu Vermengungen der Problemkreise kommt, soll der Fall dennoch angesprochen werden. Es handelt sich in der Tat nicht um einen Fall der Sperrung von Inhalten durch Access-Provider, sondern um die Verhinderung des Zugriffs auf bestimmte Inhalte durch einen begrenzten Personenkreis. Der Grund ist darin zu sehen, dass das französische Gericht lediglich eine Entscheidung treffen konnte, die sich territorial auf Frankreich bzw. französische Nutzer bezieht. Die weltweit angebotenen Inhalte von Yahoo, Inc., konnten daher nicht angegriffen werden, zumal diese – wie bereits oben erwähnt – beispielsweise in den USA nicht rechtswidrig sind. Es lag daher an Yahoo, proprietäre Angebote einer länderspezifischen Sperrung zu unterziehen.

Yahoo, Inc., hat in dieser Situation die Not zur Tugend gemacht, einige der Artikel mit weltweiter Wirkung gelöscht und im übrigen eine Kostenpflicht für das Auktionsangebot eingeführt und durch Vertragsbedingungen dafür gesorgt, so dass sich das Problem damit von selbst erledigte. Ein Filtern von Internetinhalten erfolgte nicht.

Erwähnenswert ist noch, dass ein amerikanisches Gericht zwischenzeitlich ausdrücklich festgestellt hat, dass das französische Urteil aufgrund des 1st Amendment in den USA keine Anwendung findet. Das französische Gericht hatte es sich nämlich nicht nehmen lassen, neben der ausgesprochenen Verpflichtung auch eine Aufforderung an Yahoo, Inc. auszusprechen, derartige Inhalte nicht zu verbreiten.

In einem weiteren Fall, der ebenfalls in Frankreich seinen Ursprung findet, wurden französische Access-Provider von der Organisation „J'accuse“ verklagt, den Zugang zu dem Webangebot unter „www.front14.org“ zu sperren. Es handelt sich um rechtsradikale Inhalte. Diese Klage ist inzwischen abgewiesen worden. Eine Sperrverpflichtung wurde nicht ausgesprochen.

Bemerkenswert ist, dass schweizer Internet Service Provider zwischenzeitlich einer gleichlautenden Sperrungsaufforderung durch die Organisation „Kinder des Holocaust“ nachgekommen waren. Die Folge waren wiederum etliche Spiegelungen der Inhalte. Derzeit und möglicherweise dauerhaft hat sich jedoch auch das Problem um „www.front14.org“ erledigt. Dem Vernehmen nach wurde die Homepage entweder durch Hacker korrumpiert oder aus wirtschaftlichen Gründen von den Betreibern eingestellt.

Letztlich wollen wir auf die Ereignisse in Düsseldorf zurückkommen. Wie bereits erwähnt, hatte der Regierungspräsident Büssow unter Berufung auf seine Zuständigkeit als Aufsichtsbehörde nach § 18 Abs. 1 MdStV mehr als 50 Access-Provider in Nordrhein-Westfalen zur Sperrung von vier Internetpräsenzen aufgefordert.

Im Rahmen der Diskussion um diese Sperrungsaufforderung wurden die bestehenden technischen Ansätze zur Durchführung von Sperrungen und ihre Wirksamkeit ebenso wie die Auswirkungen auf die Internetindustrie erörtert.

Es handelt sich im Wesentlichen um drei verschiedene Herangehensweisen zur Sperrung:

- Manipulation des DNS

Das Verfahren setzt beim Domain Name System an, welches im Rahmen der Adressierung von Netzelementen im Internet zum Einsatz kommt. Diese werden über so genannte IP-Adressen, 4 Byte lange numerisch Zeichenfolgen, angesprochen. Da diese Ziffernfolgen nur schwer merkbar sind, wurde das Domain Name System eingeführt, das es Internetnutzern ermöglicht, leichter merkbare Domain Namen zu verwenden. Diese Domain Namen werden – für den Nutzer unbemerkt - nach Eingabe in das Adressfeld der Navigationssoftware durch Abfrage von Nameservern, einem Telefonbuch vergleichbar, in die zugehörige IP-Adresse aufgelöst. Sodann sorgt der Browser für eine Ansprache dieser IP-Adresse. Die Manipulation bewirkt, dass die nach Internet-Standards anzusprechenden Nameserver nicht „befragt“ werden, sondern für die beanstandeten Seiten falsche Informationen eingepflegt werden mit der Folge, dass Abrufversuche von zu sperrenden Internetangeboten scheitern.

Der Nachteil liegt insbesondere darin, dass durch die Verwendung alternativer Nameserver die Sperrung umgangen werden kann und darüber hinaus auch unbedenkliche Inhalte gesperrt werden, wenn auch solche Inhalte auf dem Server mit dem gleichen Namen abgelegt sind.

- Access-Listen bei Routern

Hier wird ein Zugriff auf zu sperrende Inhalte durch einen Eingriff in das Routing verhindert. Die Abfrage von Informationen im World Wide Web erfolgt durch Senden und Empfangen von Datenpaketen, deren Vermittlung durch Router bewerkstelligt wird. Im Vorgriff auf die Zustellung eines Datenpaketes arbeiten nach diesem Verfahren die Router Listen ab und leiten an solche IP-Adressen keine Pakete weiter, die auf den Listen geführt werden.

Der Nachteil ist, dass alle Dienste und damit auch alle WWW-Seiten auf dem gelisteten Host betroffen sind. Zudem kommt es ab einer bestimmten Länge dieser Listen zu massiven Performanceeinbußen.

- Einsatz von Proxy-Servern

Anfragen zu bestimmten Webangeboten werden im Rahmen dieses Konzeptes lediglich dann weitergeleitet, wenn ein beim Provider installierter Proxy-Server dies zulässt.

Probleme dürften insbesondere hinsichtlich der Performance bei größeren Datenvolumina auftreten. Zudem kann die Wirkung des Proxies ausgehebelt werden, wenn die Daten über einen standardmäßig nicht verwendeten Port ausgetauscht werden. Zudem beeinträchtigen technische Probleme am Proxy-Server den gesamten Datenverkehr und damit auch unbedenkliche Angebote. Sollen solche Risiken ausgeschlossen werden, so müssen äußerst kostenträchtige hochperformante Systeme eingesetzt werden.

Im Hinblick auf die wirtschaftlichen Auswirkungen derartiger Maßnahmen habe ich keine Berechnungen angestellt, da eine verlässliche Quantifizierung ohnehin nicht möglich sein dürfte. Die Dimension der Belastung des Wirtschaftszweiges lässt sich jedoch leicht abschätzen, wenn man bedenkt, dass es in Deutschland 85 nationale Backbone-Betreiber und etwa 3000 regionale Betreiber, das heißt ISPs, POPs und Wiederverkäufer gibt.

Zu anfallenden Hardwarekosten, die schon bei kleineren Anbietern leicht fünfstelligen Beträge erreichen dürften, kommen als wesentlicher Faktor die Kosten der Pflege des Systems. In diesem Zusammenhang ist zu bedenken, dass sich die Sperrungsaufforderung aus Düsseldorf lediglich auf vier Internetpräsenzen bezog. Dies ist jedoch allenfalls als Testballon zu verstehen. Sollte die geforderte Sperrung dieser Homepages durch Access-Provider durchgeführt werden, so muss davon ausgegangen werden, dass einige hundert weitere Seiten beanstandet werden. Die Anzahl der zu sperrenden Adressen wird sich sodann noch vervielfachen. Die Erfahrung lehrt, wie oben bereits angerissen, dass zu erwarten ist, dass die gesperrten Angebote gespiegelt werden. Dazu kommt, dass diejenigen, die ihr Gedankengut verbreiten wollen, ohne weiteres IP-Adressen und URLs verändern werden, um die Sperrung auszuhebeln. Schließlich sind solche Adressen wieder aus der Liste der zu sperrenden Angebote zu löschen, deren Inhalte zur Unbedenklichkeit hin verändert wurden. Der administrative Aufwand ist immens. Die Personalkosten dürften insbesondere kleine Unternehmen unzumutbar belasten.

Möglicherweise können der finanzielle Aufwand minimiert und die technischen Schwächen der vorgenannten Lösungen aufgefangen werden. Zumindest wurde dies durch ein Konsortium von Unternehmen anlässlich eines von der Bezirksregierung eingesetzten Arbeitskreises in Aussicht gestellt. Das vorgeschlagene Konzept würde eine Poollösung darstellen, so dass der administrative Aufwand lediglich an einer zentralen Stelle entstünde. An der Universität Dortmund soll diese technische Lösung im Rahmen eines Pilotprojektes aufgesetzt und einige Monate lang evaluiert werden. Es bleibt abzuwarten, ob das System in technischer Hinsicht skaliert.

Wichtiger als der technische Ansatz erscheint mir jedoch eine rechtliche und politische Betrachtung zu sein.

In vielen Fällen, in denen öffentlich die Sperrung von Inhalten im Internet gefordert wurde, hat dies zu einer heftigen Diskussion on- wie offline geführt. Die Folge war, dass den beanstandeten Homepages eine kostenlose und nachhaltige Werbung verschafft wurde und diese insbesondere bei Jugendlichen eine besondere Attraktivität erlangten. Zum Teil fanden sich im Internet mit Hyperlinks versehene Listen von Internetpräsenzen mit strafbaren Inhalten.

Dazu kommt, dass im Zeitpunkt der Manuskripterstellung noch keine Sperrverfügung gegen die Access-Provider erlangt ist und gefragt werden muss, welchen Inhalts diese sein kann. Zum Teil wird die Auffassung vertreten, dass es der

Bezirksregierung schon an der erforderlichen Zuständigkeit fehle. Die Frage, ob und in welchem Umfang die Bezirksregierung die berufene Stelle zum Erlass derartiger Verwaltungsakte ist, erscheint mir hier aber vor dem Hintergrund vernachlässigenswert, dass jedenfalls eine Kompetenz als Aufsichtsbehörde im Bereich der Mediendienste zugunsten der Bezirksregierung bestehen dürfte.

Wenn nun aber eine Ermächtigungsgrundlage für die Bezirksregierung besteht, dann muss ein Verwaltungsakt die Aufforderung an die Access-Provider konkret bestimmen, indem beispielsweise ein URL oder eine IP-Adresse genannt wird. Ändert sich diese – und die Erfahrung zeigt, dass ein „Location-Hopping“, wie ich es nennen möchte, durchaus in kurzen Intervallen von wenigen Tagen vorgenommen wird -, dann läuft die Verfügung leer. Es dürfte schnell zu einem Wettlauf zwischen Kriminellen und Behörden kommen, um eine Aktualität der Verfügungen zu gewährleisten. Man muss also fragen, ob dies ein Ansatz ist, der erfolgversprechend ist oder ob nicht ein Gesichtsverlust für die erlassende Behörde das Ergebnis ist. Wenn indes die Verfügung zum Inhalt haben sollte, dass dem Access-Provider lediglich die im Zeitpunkt des Erlasses aktuelle Fundstelle genannt wird und sodann das Monitoring bei Änderungen dem Access-Provider überlassen wird, dürfte diese einer gerichtlichen Überprüfung nicht standhalten. Dies stellte nämlich einen Bruch mit dem Grundsatz dar, dass Provider eine proaktive Prüfung von Internetinhalten gerade nicht vornehmen sollen und dürfte zudem unverhältnismäßig sein.

Wenn nun aber lediglich punktuelle und damit nicht nachhaltige Verfügungen erlassen und dynamische Regelungen nicht rechtmäßig durchgesetzt werden können, stellt sich die Frage nach anderen und freiwilligen Ansätzen in Kooperation mit der Internetwirtschaft.

Hier ist insbesondere die Stärkung von Medienkompetenz zu nennen, die bei Eltern genauso ansetzen muss wie in Schulen, damit ein verantwortlicher Umgang mit diesem recht neuen Medium erlernt und das Augenmerk auf „gute“ Inhalte gelenkt wird.

Zudem wird man - egal durch welches technische Mittel – die Verbreitung und den Austausch rechtswidriger Materialien im Internet ebenso wenig unterbinden können wir „offline“. Es kann also ohnehin nur darum gehen, die Räume für illegale Machenschaften im Internet einzuengen und deren Sichtbarkeit, insbesondere für Kinder und Jugendliche, die eines besonderen Schutzes bedürfen, zu minimieren. Dies kann effizienter durch andere Mechanismen als eine Sperrung erfolgen.

In diesem Zusammenhang zu nennen sind im Bereich der jugendgefährdenden Inhalte Client-basierte Lösungen, die in Abhängigkeit von Altersgrenzen nur den Abruf bestimmter Inhalte zulassen. Die Internet Content Rating Association (www.icra.org) stellt hier das aus meiner Sicht beste System bereit, das in der nahen Zukunft eine enorme Bedeutung gewinnen dürfte. Es basiert auf einem First Party Rating durch die Inhalteanbieter selbst, die ihre Inhalte nach bestimmten Kriterien (Nacktheit, Gewalt etc.) selbst klassifizieren und so genannte „content descriptors“ in den Quellcode der Seiten einpflegen. ICRA ermöglicht sodann Erziehungsberechtigten den Einsatz von Templates, die ziel- und altersgruppenabhängige den Zugriff auf bestimmte Internetinhalte – gegebenenfalls unter zusätzlicher Verwendung von Black- und Whitelists - beschränken.

Daneben unternimmt die Internetwirtschaft Anstrengungen, Inhalte dort zu bekämpfen, wo sie ins Netz gestellt werden und eine Verfolgung von Straftätern durch die zuständigen Strafverfolgungsbehörden zu ermöglichen. Zu diesem Zweck ist ein europäisches Netzwerk von Beschwerdhotlines eingerichtet worden. Die Internet Hotline Providers in Europe Association, kurz INHOPE (www.inhope.org), umfasst nach ihrer Gründung durch 8 nationale Hotlines im November 1999 mit Stand vom Dezember 2001 bereits 16 Mitglieder. Darunter sind auch assoziierte Mitglieder in den USA und Australien. Dieses Netzwerk ermöglicht eine sehr schnelle und effiziente Bekämpfung von kriminellen Inhalten, die nicht an den Ländergrenzen endet. In vielen Fällen sind strafbare Inhalte bereits einen oder zwei Tage nach der Weiterleitung einer Beschwerde an eine Partnerhotline nicht mehr im Internet abrufbar. eco betreibt mit dem Projekt ICTF (Internet Content Task Force) eine solche Beschwerdhotline, die über dessen Homepage (www.eco.de) oder direkt über www.ictf.de erreichbar ist. Es sei die Bemerkung erlaubt, dass eco Mitinitiator der Idee zu INHOPE war und insofern auch Gründungsmitglied der Organisation ist. Die ICTF nimmt im übrigen bei Beschwerden den angeschlossenen Providern die Prüfung

ab, ob bestimmte Inhalte rechtswidrig sind oder nicht und ermöglicht somit eine enorme Kostenersparnis.

Selbstredend wird im Rahmen dieser Kooperation der nationale rechtliche Kontext der einzelnen Hotlines und deren Beschwerdeordnungen respektiert, so dass keine Handhabe gegen Inhalte besteht, die im jeweiligen Land zulässig ist. Probleme entstehen somit wieder insbesondere im Bereich der Äußerungsdelikte. Es muss jedoch ohnehin gefragt werden, ob auf lange Sicht in einem internationalen Kontext die in Deutschland vorhandene strenge Reglementierung in diesem Bereich aufrecht erhalten werden kann und sollte.

Erlauben Sie letztlich noch den Hinweis auf den Aktionsplan der EU zur Schaffung eines sichereren Umfeldes im Internet hinzuweisen. Diesbezügliche Informationen finden sich unter www.saferinternet.org. Dieser Aktionsplan umfasst drei Handlungsstränge, nämlich den Aufbau eines Netzes von Hotlines – in diesem Kontext nimmt auch INHOPE und eco an dem Aktionsplan teil -, die Förderung von Aufklärungsprogrammen und die Förderung der Entwicklung von Filtersoftware. Erstaunlicherweise fördert der Aktionsplan eine Sperrung von Inhalten bei Access-Providern – soweit bekannt - nicht, wenngleich davon ausgegangen werden muss, dass den geistigen Vätern des Aktionsplans auch diese Handlungsoption bekannt war. Vor diesem Hintergrund ist die Frage erlaubt, ob in einem zusammenwachsenden Europa, welches Sperrmaßnahmen für alle Nutzer offensichtlich nicht als Werkzeug einsetzen möchte, ein nationaler Alleingang empfehlens- oder wünschenswert ist.

Lassen Sie mich mit Wunsch schließen, dass das Zusammenwirken verschiedener gesellschaftlicher Kräfte dazu führt, dass das Internet mehr und mehr zu dem wird, was es sein soll und auch schon ist: Ein Medium mit phantastischen Möglichkeiten zum Kommunizieren, Lernen, Spielen und Arbeiten – für jung und alt – überall auf der Welt.

RA Thomas Rickert