KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 16.10.1996
KOM(96) 487 endg.

MITTEILUNG DER KOMMISSION

AN DEN RAT, DAS EUROPÄISCHE PARLAMENT,
DEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS
UND DEN AUSSCHUSS DER REGIONEN

Illegale und schädigende Inhalte im Internet

INHALTSVERZEICHNIS

EINLEITUNG

Als Verkörperung der Konvergenz der Industriebereiche Telekommunikation, Informatik und Informationsinhalte und als Haupttriebkraft dieser Konvergenz hat Internet sich in den letzten Jahren als ***einer der wichtigsten Bausteine der globalen Informationsinfrastruktur*** und als ***wesentlicher Katalysator für die Informationsgesellschaft in Europa*** etabliert. Mit seiner in der Geschichte der Kommunikationstechnik einmaligen Wachstumsrate erreicht Internet heute etwa 60 Millionen Benutzer in 160 Ländern; die Zahl verdoppelt sich jährlich. Die bekannteste Anwendung, das World Wide Web, dessen Protokolle in Europa entwickelt wurden, wird schnell das Standardmedium für Informationsveröffentlichung und elektronischen Handel; die ungefähr 10 Millionen Sites weltweit im Jahr 1995 bedeuten einen Zuwachs um 1600 % gegenüber dem Vorjahr. Unter dem Impuls dieses raketenhaften Anstiegs und der schnellen Entwicklung von einem Behörden-/Hochschulnetz zu einer umfassenden Kommunikations- und Handelsplattform revolutioniert das Internet gegenwärtig viele ***Wirtschaftsbereiche***, da eine ***kraftvolle, schnell anwachsende Internet-Wirtschaft"*** entsteht. Zugleich übt das Internet auch einen ***gewaltigen Einfluß im gesellschaftlichen, kulturellen und Bildungsbereich*** aus: Es verleiht Bürgern und Ausbildern Macht, senkt die Barrieren bei der Schaffung und Verteilung von Informationsinhalten, bietet universalen Zugang zu immer reicheren Quellen für digitale Information.

Entsprechend diesen Möglichkeiten sind die Internet-Inhalte in ihrer großen Mehrzahl für Informationszwecke zur völlig legitimen (und oft äußerst produktiven) geschäftlichen oder privaten Nutzung gedacht. Doch wie bei jeder anderen Kommunikationstechnologie, vor allem im Anfangsstadium der Entwicklung, sind auch im Internet schädigende oder illegale Inhalte zu finden, oder es wird für kriminelle Tätigkeiten mißbraucht. Das ist statistisch gesehen nicht von großer Bedeutung, betrifft jedoch viele verschiedene Bereiche, für die auf einzelstaatlicher und internationaler Ebene unterschiedliche rechtliche Regelungen und Instrumente gelten:

- Nationale Sicherheit (Anleitungen zur Herstellung von Bomben, zur illegalen Herstellung von Drogen oder für terroristische Tätigkeiten);
- Jugendschutz (mißbräuchliche Marketingformen, Gewalt, Pornographie);
- Schutz der Würde des Menschen (Aufstachelung zum Rassenhaß oder Rassendiskriminierung);
- wirtschaftliche Sicherheit (Fälschung, Anleitungen zur Fälschung von Kreditkarten);
- Informationssicherheit (Hacking);
- Schutz der Privatsphäre (unberechtigte Weitergabe personenbezogener Daten, elektronische Belästigung);
- Schutz des guten Rufs (Verleumdung und rechtswidrige vergleichende Werbung);
- geistiges Eigentum (unzulässige Weitergabe urheberrechtlich geschützter Werke, z. B. von Software oder Musik).

Beim Internet überwiegen zwar bei weitem die Vorteile, die negativen Aspekte sind jedoch nicht zu übersehen. Es stellen sich dringende Fragen von öffentlicher, politischer, kommerzieller und rechtlicher Bedeutung. Diese Probleme fanden ihren Niederschlag: Bei den politischen Erörterungen in der Europäischen Union wurde in letzter Zeit betont, daß Sofortmaßnahmen und konkrete Lösungen gebraucht werden.

Daher verabschiedete in allerjüngster Zeit, am 27. September 1996, der Telekommunikationsrat eine Entschließung, die sich mit der Verhinderung der Weitergabe illegalen Materials, vor allem von Kinderpornographie, im Internet beschäftigt. Der Rat nahm zur Kenntnis, daß die Kommission eine Mitteilung zu diesem Thema vorbereitet, und begrüßte diese Initiative. Angesichts des dringenden Handlungsbedarfs forderte der Rat die Kommission auf, ihre Arbeit fortzusetzen und rechtzeitig vor dem Telekommunikationsrat am 28. November Maßnahmenvorschläge zu unterbreiten.

Die Kommission ist sich der Bedeutung dieser Fragen voll bewußt, sie weiß, ***daß abgewogen werden muß zwischen der Sicherung des freien Informationsflusses und dem Schutz des öffentlichen Interesses***, so daß berechtigten Sorgen Rechnung getragen ist.

Bereits auf der informellen Ratstagung am 24. April 1996 in Bologna bezeichneten die europäischen Telekommunikations- und Kulturminister die Frage der illegalen und schädigenden Inhalte im Internet als sehr dringliche Angelegenheit. Es wurde die Ansicht vertreten, daß zwar einzelstaatliche Rechtsvorschriften für Internet gälten, daß jedoch in einem umfassenderen Rahmen Vereinbarungen getroffen werden müßten, um die spezifischen Probleme zu lösen, die sich bei diesem Netz der Netze" stellten. Die Kommission wurde daher beauftragt, die Probleme im Zusammenhang mit der schnellen Entwicklung von Internet zusammenzustellen und insbesondere die Frage zu behandeln, ob eine europäische oder internationale Regelung wünschenswert ist.

Die Weitergabe ***illegaler Inhalte*** im Internet fällt eindeutig in die ***Zuständigkeit der Mitgliedstaaten***, und diese müssen ***den geltenden Gesetzen Beachtung verschaffen. Was offline illegal ist, ist auch online illegal***, und es obliegt den Mitgliedstaaten, dies durchzusetzen. Da Internet jedoch stark dezentral und grenzübergreifend angelegt ist, sollten im Rahmen der Innen- und Rechtspolitik konkrete Maßnahmen zur Intensivierung der Zusammenarbeit zwischen den Mitgliedstaaten vorgeschlagen werden.

Die Präsenz illegaler und schädigender Inhalte im Internet hat eine ***direkte Auswirkung auf den Binnenmarkt***. So können insbesondere zum Schutz des öffentlichen Interesses getroffene Regelungen der Mitgliedstaaten für neue Internet-Dienste zu Wettbewerbsverzerrungen führen (z. B. durch stark voneinander abweichende Regelungen der Haftung der Internet-Dienstanbieter), den freien Verkehr mit diesen Diensten beeinträchtigen und zu einer erneuten Zersplitterung des Binnenmarkts führen. Wenn hier keine Lösungen gefunden werden, könnte ein Eingreifen der Gemeinschaft gerechtfertigt sein. Wie in jedem neuen, schnell wachsenden Industriesektor ist Rechtssicherheit die unabdingbare Voraussetzung für Investitionen,

für die Entwicklung eines wettbewerbsfähigen Internet-Dienstleistungssektors und für das Entstehen einer umfassenden, Internet-basierten Wirtschaft in Europa.

Das Internet in seiner Internationalität und Einzigartigkeit (äußerst dezentralisierter Aufbau, Kontrollresistenz, starke Automatisierung, globale Reichweite, umfassende Nutzung) wirft anerkanntermaßen neue, ganz spezifische Fragen auf. Diese Probleme machen innovative, spezifische Lösungen, die schnell realisiert werden sollten, und eine koordinierte Antwort auf internationaler und EU-Ebene unverzichtbar.

In Ergänzung dieser Initiative werden Fragen des Schutzes von Minderjährigen im engeren Sinn – als Teil der umfassenderen Frage der illegalen und schädigenden Inhalte – im *Grünbuch zum Jugendschutz und Schutz der Menschenwürde in den neuen audiovisuellen und Informationsdiensten* behandelt. Das Grünbuch verfolgt einen horizontalen Ansatz; es soll langfristige Überlegungen zu diesem Problem durch alle elektronischen Medien in Gang setzen.

Diese Mitteilung nimmt eine Beurteilung der Chancen von Internet vor, nennt unterschiedliche Ausformungen illegaler und schädigender Inhalte, stellt das technische Umfeld des Internet dar und nennt mögliche Strategien für Sofortmaßnahmen technischer und/oder rechtlicher Art zur Bekämpfung derartiger Inhalte im Internet.

1 DIE CHANCEN VON INTERNET

Internet bietet beträchtliche Möglichkeiten der globalen Nutzung für Informations-, Bildungs-, Unterhaltungs- und Geschäftszwecke. Zu verhältnismäßig niedrigen Kosten können große Informationsmengen in neuen Multimedia-Kommunikationsnetzen um den Globus geschickt werden. Vor allem Länder der Europäischen Union haben diese völlig neuen Chancen bereits ergriffen.

Im ***gesellschaftlichen Bereich*** kann Internet wesentliche Vorteile für die Bürger Europas bringen: In beispielloser Weise kann es ihnen zu Macht verhelfen und ihnen immer reichere Quellen digitaler Information erschließen. Internet wurde in mehreren Ländern zur Verbindung zwischen Behörden und Bürgern sinnvoll eingesetzt. Da der Zugang zur Informationsweitergabe auf lokaler und auch auf globaler Ebene problemloser vonstatten geht, können Einzelpersonen und Verbände über das Internet Informationen über ihre Tätigkeiten einem größeren Publikum kostengünstig zugänglich zu machen. ***Im kulturellen Bereich*** trägt Internet bereits wesentlich zur Schaffung und Verbreitung digitaler europäischer Multimedia-Inhalte bei, was der sprachlichen Vielfalt zugute kommt und den Stellenwert der Kulturen Europas in der Welt verbessert. Wie innovative Projekte zur Verbindung von ***Bibliotheken, Schulen und Hochschulen*** in Europa gezeigt haben, ist Internet außerdem der Schlüssel für eine neue ***Elektronikbildung***" und als solches der Eckpfeiler der neuen, weitreichenden Initiative der Europäischen Union: des Aktionsplans ***Lernen in der Informationsgesellschaft***".

Das Netz der Netze", das gegenwärtig den ***elektronischen Handel*** revolutioniert, wird in den kommenden Jahren wohl eine ***wesentliche Rolle für die Wirtschaft Europas*** spielen. Das steht in direktem Zusammenhang mit der Liberalisierung des europäischen Telekommunikationsmarktes, der zu niedrigeren Betriebskosten für Internet-Benutzer und Dienstanbieter führen sollte[1]. Wie der amerikanische Markt bereits zeigt, ***läßt Internet unmittelbar eine neue Internet-Wirtschaft entstehen,***[2] neuartige Unternehmen und neue Berufe tauchen auf (Internet-Infrastruktur und -Software, Internet-Zugangsanbieter, Vertrieb von Inhalten für private und geschäftliche Nutzung, Online-Einzelhandel und Finanzdienstleistungen). Über diese Internet- Kernwirtschaft" hinaus, bei denen Einnahmen direkt aus dem Internet entstehen, hat es ***indirekte Auswirkungen auf eine viel größere Internet-Einflußsphäre"***. Internet bewirkt so grundlegende Veränderungen bei mehreren Wirtschaftssektoren (Reisebranche, Versicherungen, Direktvertrieb, Electronic Publishing), läßt neue Märkte entstehen, senkt Kosten und verbessert den Dienst für die Kunden. Vor allem schafft es ***neue Möglichkeiten für europäische KMU***, die diesen neuen Zugang zu globalen Märkten über das World Wide Web nun intensiv nutzen. Entsprechend sind auch große Wirtschaftszweige wie der Direktvertrieb in Europa (der 1994 Einnahmen von insgesamt 37 Mrd. ECU darstellte[3]) und in erster Linie der traditionelle Katalogverkauf dabei, das Internet aktiv in ihre Marketing- und Lieferstrategien einzubeziehen, und sie planen die allmähliche Überführung eines wesentlichen Teils ihrer Tätigkeiten in das Internet.

Für ***Werbung und Marketing*** bietet Internet erwiesenermaßen etliche Vorteile. Da das Netz interaktiv ist und unmittelbare, leichte Kommunikation ermöglicht, können Werbetexte viel genauer als bisher auf die Zielgruppen zugeschnitten werden, und ein Feedback der bisherigen oder potentiellen Kunden ist möglich. Entsprechend bietet Internet bei der Nutzung für Transaktionen oder sogar für die Online-Lieferung von Inhalten beträchtliche Kosteneinsparungen.

---

1 Ein wesentlicher Faktor der Entwicklung des Internet-Markts in den USA waren die niedrigeren Telekommunikationskosten (niedrigere Kosten von Standleitungen für professionelle Benutzer, von Ortsgesprächen für private Nutzer).

2 Nach Schätzungen von Forrester Research wird die Internet- Kernwirtschaft" allein in den USA 1996 einen Wert von etwa 2,2 Mrd. $ darstellen. Im Jahr 2000 werden etwa 45,5 Mrd. $ direkt auf Internet-Tätigkeiten zurückzuführen sein [illegible] eine Steigerung um das Zwanzigfache in fünf Jahren. Ebenfalls nach Forrester Research werden die intensivsten Internet-Wirtschaftsbereiche sein: Internet-Infrastruktur (14,2 Mrd. $), Informationsinhalte für private Nutzer (2,8 Mrd. $ einschließlich Internet-Werbung und Ankauf von Rechten), Inhalte für kommerzielle Nutzung (6,9 Mrd. $ einschließlich jetzt über firmeneigene Netze bereitgestellte Wirtschaftsinformation), Online-Handel (21,9 Mrd. $ einschließlich 6,9 Mrd. $ aus neuen elektronischen Einzelhandelstätigkeiten und 15 Mrd. $ aus der Umstellung von traditionellen EDI-Systemen) und Finanzdienstleistungen (Verwaltung von Vermögenswerten und Sparguthaben in Höhe von etwa 46,2 Mrd. $ über das Internet).

3 Quelle: *Study on the Extent of Direct Marketing in the European Union*, Zwischenbericht von FEDIM für die Europäische Kommission

Die Allgemeinheit wird auf globalen Märkten in den ***elektronischen Handel*** einbezogen, und zugleich verändert Internet die Transaktionen zwischen Betrieben grundlegend, da die Unternehmen von firmeneigenen Netzen und geschlossenen Protokollen (wie dem herkömmlichen EDI) auf das Internet und firmeneigene Intranets" übergehen. In der globalen Internet-Wirtschaft ***verzeichnet dieser Bereich "Transaktionen zwischen Unternehmen" (Business to Business) gegenwärtig das größte Wachstum***. Er ist von grundlegender strategischer Bedeutung für die europäischen Unternehmen, die sich dem globalen Wettbewerb stellen.

Wie jeder andere Wirtschaftszweig kann das Internet für rechtmäßige Tätigkeiten benutzt oder von einigen Elementen der Gesellschaft mißbraucht werden. Beim Rahmen für Internet muß ***Wirtschaftsentwicklung*** vorgesehen sein, aber auch berechtigten ***sozialen und gesellschaftlichen Interessen*** Rechnung getragen werden. Bürger und Unternehmen müssen sicher sein können, daß man im Internet sicher und gefahrlos arbeiten, lernen und spielen kann.

In dieser Mitteilung geht es darum,

- ***zunächst kurz die verschiedenen Arten illegaler und schädigender Inhalte zu beschreiben,***
- ***sodann den technischen Handlungsrahmen zu prüfen, der bei illegalen und schädigenden Inhalten gegeben ist,***
- ***schließlich konkrete Maßnahmen vorzuschlagen, die schnell realisiert werden können.***

Abschnitt 2 enthält eine Beschreibung der einzelnen Internet-Anwendungen; in *Abschnitt 3* ist definiert, was unter illegalen und schädigenden Inhalten" zu verstehen ist; *Abschnitt 4* beschreibt, wie gegen illegale Inhalte vorgegangen werden kann; in *Abschnitt 5* geht es um die Behandlung schädigender Inhalte; in *Abschnitt 6* werden dann Vorschläge unterbreitet.

2 WIE ARBEITET INTERNET?

Internet ist das bekannteste Beispiel eines internationalen Rechnernetzes. Es ist nicht das erste und auch nicht das einzige derartige Netz, unterscheidet sich aber vor allem dadurch, daß niemand Eigentümer" des Netzes ist und daß in letzter Zeit normale" Bürger, Privatpersonen und Unternehmen, also nicht nur Wissenschaftler und Hochschulkreise, angefangen haben, es zu benutzen, so daß die Zahl der an Internet angeschlossenen Rechner sprunghaft angestiegen ist[4]. Im Gegensatz zu herkömmlichen Netzen wie Rundfunk- und Fernsehnetze

[4] Die Zunahme der Server, die Web-Inhalte anbieten, und der Zahl der angeschlossenen Benutzer ist verblüffend. Allein in Europa stieg die Zahl der Server von Januar 95 bis Januar 96 um 60 %. Siehe auch Statistik im IPSO-Newsletter, Ausgabe Juli

ist Internet im wesentlichen benutzerinduziert, da die Benutzer selbst und nicht etablierte Verleger einen beträchtlichen Teil der Inhalte erzeugen.

Eine Besonderheit von Internet ist, daß es ***gleichzeitig zum Publizieren und zum Kommunizieren eingesetzt*** werden kann. Im Gegensatz zu den herkömmlichen Medien kann der Benutzer beim Internet abwechselnd Nachrichten senden oder empfangen. Aus einem Empfänger kann jederzeit ein potentieller oder tatsächlicher Anbieter von Informationsinhalten werden. Darin ***unterscheidet sich Internet grundlegend vom herkömmlichen Rundfunk-/Fernsehwesen,*** aber ***auch von den herkömmlichen Telekommunikationsdiensten.*** Dieser ständige Wechsel vom Publizieren zu privater Kommunikation – also zwei Betriebsarten, für die traditionell sehr unterschiedliche rechtliche Regeln gelten – stellt eine der größten Herausforderungen der Internet-Regulierung dar.

Die vielen unterschiedlichen Arten der Verbreitung von Internet-Inhalten sind Ausdruck dieser strukturellen und entwicklungsbedingten Besonderheiten. Inwieweit illegale und schädigende Inhalte mit technischen Mitteln aufgespürt oder abgefangen werden können, ist von Anwendung zu Anwendung unterschiedlich.

Die meisten Einzelbenutzer haben nicht ständig einen direkten Zugang zum Internet, sondern gehen über einen Zugangsanbieter. Hierzu gehören

- ***Internet-Zugangsanbieter***, die speziell den Zugang zum Internet anbieten;

- ***Internet-Dienstanbieter***, die zusätzliche Leistungen erbringen wie die Speicherung von Inhalten (Hosting), die von ihnen selbst, von Benutzern oder aber von Dritten produziert werden (diejenigen, die Inhalte produzieren, sind hier als Inhaltsanbieter bezeichnet);

- ***Online-Dienstanbieter***, die Abonnenten firmeneigenes Material[5] auf ihre geschlossenen Systeme liefern und nun auch Internet-Zugang anbieten.

Der Begriff Internet-Dienstanbieter“ wird häufig im allgemeinen Sinn benutzt, ohne daß genau unterschieden wird zwischen dem *Dienst, der in der Bereitstellung des Zugangs zum Internet besteht*, und dem *Dienst als Inhaltshost*. Zugangsanbieter“ und Host-Dienstanbieter“ sind die Begriffe, die benutzt werden, um zwischen diesen beiden Gruppen zu unterscheiden. Ein- und dieselbe Firma kann natürlich beiden Gruppen gleichzeitig angehören.

---

http://www.ispo.cec.be/ispo/newsletter/ISPOJULY/ISPOJULY04.html (5 Millionen neue Server in den letzten 12 Monaten)

5 Derartiges "firmeneigenes Material" kann von dem Online-Dienstanbieter selbst oder aber für diesen im Rahmen eines Vertrags von Dritten (Unternehmen des Unterhaltungsbranche, Finanzdienst-Anbieter, Fluggesellschaft usw.) produziert werden. Wie herkömmliche Verleger übernimmt der Online-Dienstanbieter im allgemeinen die Verantwortung für den Inhalt dieses Materials.

Sowohl ***Zugangsanbieter***" als auch ***Host-Dienstanbieter***" stellen die Verbindung zum Internet her über eine Mietleitung, also eine Telekommunikationsverbindung, die von einem ***Netzbetreiber***" wie beispielsweise British Telecom bereitgestellt wird.

Das ***World Wide Web*** (WWW oder Web) ist der Bereich, in dem Seiten mit Text, Grafik und sogar Ton und Videoclips konsultiert werden können. Die Seiten sind über Hyperlinks" miteinander verbunden, die ein müheloses Sichten der Web-Inhalte ermöglichen. Solche Seiten kann jeder veröffentlichen, der Zugang hat zu Speicherplatz auf einem Host-Rechner mit Anschluß an Internet und der entsprechenden Software (Web-Server" oder Site"). Die Möglichkeit zum Verleger von Inhalten" zu werden wird häufig als billige Zusatzleistung von Internet-Zugangsanbietern eröffnet; auf diese Weise können Einzelpersonen Informationen genauso wie große Konzerne verbreiten. Die so veröffentlichten Seiten sind jedem Internet-Benutzer zugänglich, der sie anwählt; sie haben jeweils eine genaue Adresse, die zur direkten Abfrage oder zum Zugriff auf die Seite über Hyperlinks benutzt wird.

Die ***elektronische Post*** ermöglicht die Kommunikation zwischen Einzelpersonen. Eine Mitteilung kann über Adressenlisten auch problemlos an mehrere Empfänger geschickt werden. Im allgemeinen ist der Verfasser der Mitteilung über seine E-mail-Adresse zu ermitteln, es sind jedoch anonyme Weiterversandsysteme" entstanden, bei denen die Identität des Senders nicht an den Empfänger weitergegeben wird. An eine Internet-Adresse geschickte Mitteilungen werden in der Mailbox des Empfängers auf dem Mail-Server beim Zugangsanbieter gespeichert, bis der Empfänger sie liest.

In etwa 15 000 ***Newsgroups*** wird der Inhalt von Einzelpersonen gestellt, die Mitteilungen verschicken (das kann einfacher Text sein; sie können jedoch auch kodierte und somit übertragbare Grafiken umfassen). Diese Mitteilungen werden nicht an einem einzigen Ort gespeichert, sondern von einem Newsgroup-Server zum anderen kopiert. Wegen des enormen Speicherbedarfs sind diese Mitteilungen bei den Host-Dienstanbietern oft nur für eine beschränkte Zeit auf den Newsgroup-Servern verfügbar, und unter Umständen werden nicht alle Newsgroups angeboten. Das World Wide Web hat auch Sites, in denen Archive von Newsgroup-Material gespeichert und abgefragt werden können.

Außerdem bietet ***Internet Relay Chat*** (IRC) direkte Echtzeitkommunikation zwischen Internet-Teilnehmern; hier können persönliche Begegnungen und der Austausch von Material verabredet werden. IRC kann nun niedrig auflösende Videotechnik wie CUSeeMe unterstützen.

Auf all diesen Wegen können illegale und schädigende Inhalte weitergegeben werden. In den folgenden Abschnitten soll gezeigt werden, inwieweit sie kontrolliert werden können.

3 WAS SIND ILLEGALE UND SCHÄDIGENDE INHALTE?

Das Internet ist eine neue Verbreitungs- und Kommunikationsform. Wie viele andere Verbreitungsmöglichkeiten läßt sich das Internet nutzen als Instrument für illegale Tätigkeiten oder als Kanal für die Verbreitung schädigender oder illegaler Inhalte. Wie jede andere Kommunikationstechnik, z. B. Telefon oder GSM, kann dieses Netz von kriminellen Elementen eingesetzt werden, um ihre Aktivitäten leichter durchzuführen.

Für all diese Tätigkeiten gibt es bereits einen Rechtsrahmen. Deshalb existiert das Internet nicht in einem rechtsleeren Raum, denn alle Beteiligten (Autoren, Inhaltsanbieter, Host-Dienstanbieter, die die Inhalte speichern und zur Verfügung stellen, Netzbetreiber, Zugangsanbieter und Endbenutzer) unterliegen den bestehenden allgemeinen Gesetzen.

Bei illegalen und schädigenden Inhalten muß unbedingt zwischen diesen beiden Formen unterschieden werden, also illegalen einerseits und schädigenden andererseits. ***Diese Inhaltskategorien werfen völlig unterschiedliche Grundsatzfragen auf und verlangen sehr unterschiedliche rechtliche und technische Antworten.*** Eine Verquickung ***getrennter Fragen – z. B. der Zugriff von Kindern auf pornographisches Material für Erwachsene und der Zugriff von Erwachsenen auf Kinderpornographie*** – wäre gefährlich. Es wären eindeutig Prioritäten zu benennen und Ressourcen zu mobilisieren, um die wichtigsten Fragen anzugehen, wie beispielsweise die Eindämmung von Kinderpornographie oder die Nutzung des Internet als neue Technik für kriminelle Handlungen.

a. Illegale Inhalte

Die Nutzung und Verbreitung bestimmter Inhalte wird aus verschiedenen Gründen durch zahlreiche Vorschriften eingeschränkt. Ihre Verletzung bewirkt, daß die Inhalte illegal sind.

Bei einigen Fragen geht es nicht um die Aufrechterhaltung der öffentlichen Ordnung, sondern eher um den Schutz von Rechten des Einzelnen (Schutz der Privatsphäre und des guten Rufs) sowie um die Bereitstellung eines Umfelds, in dem die Produktion von Inhalten gedeihen kann (geistiges Eigentum). Bei Inhalten, die beispielsweise eine Verletzung des Urheberrechts, eine Verleumdung, eine Verletzung der Privatsphäre oder rechtswidrige vergleichenden Werbung darstellen, wird in der Regel auf Initiative der Person vorgegangen, deren Rechte verletzt werden; dies geschieht in Form einer zivilrechtlichen Klage auf Schadensersatz oder einer gerichtlichen Verfügung, es gibt in einigen Fällen aber auch strafrechtliche oder verwaltungsrechtliche Rechtsmittel

(beim Datenschutz). Auch Host-Dienstanbieter können in Rechtsstreitigkeiten über derartige Inhalte verwickelt werden, wenn sie angeklagt werden, die Verbreitung von Material erleichtert zu haben.

Bestimmte Inhalte – das kommt noch hinzu – ***gelten*** nach den Rechtsvorschriften einiger Mitgliedstaaten ***als rechtswidrig***.

Dies ist beispielsweise der Fall bei Kinderpornographie, Menschenhandel, Verbreitung rassistischen Materials oder Anstiftung zum Rassenhaß, Terrorismus oder sämtlichen Formen des Betrugs (z. B. Kredtikartenbetrug).

Doch auch hier werden die Straftaten von Land zu Land unterschiedlich definiert. In der EU haben einige Mitgliedstaaten beispielsweise eigene Rechtsvorschriften für Kinderpornographie, während sie in anderen unter die allgemeinen Bestimmungen für anstößiges Material fallen.[6]

Wenn bestimmte Handlungen in einem Mitgliedstaat strafbar sind, in einem anderen aber nicht[7], ist es schwierig, sie grenzüberschreitend zu verfolgen.

b. Schädigende Inhalte.

Manche Arten von Material können die Wertvorstellungen und Gefühle anderer Personen verletzen, wenn sie beispielsweise jemanden wegen seiner politischen Ansichten, religiösen Überzeugungen, seiner Rassenzugehörigkeit u. ä. verletzen.

Was als schädigend betrachtet wird, hängt vom kulturellen Umfeld ab, das jeweils unterschiedlich ausgeprägt ist. Jedes Land entscheidet für sich, wo genau die Linie zu ziehen ist, was also zulässig ist und was nicht. Es ist deshalb unabdingbar, daß internationale Initiativen den unterschiedlichen moralischen Vorstellungen in den einzelnen Ländern Rechnung tragen und daß man versucht, Regeln zu finden, die gleichzeitig die Bürger vor anstößigem Material schützen und ihnen die Redefreiheit garantiert.

In diesem Kontext versteht es sich von selbst, daß die Grundrechte, insbesondere das Recht auf freie Meinungsäußerung, in keiner Weise eingeschränkt werden dürfen (Einschränkungen in den Mitgliedstaaten: siehe Grünbuch zum Jugendschutz und Schutz der Menschenwürde, Anhang III).

---

6 Vgl. Grünbuch zum Schutz von Minderjährigen und der Würde des Menschen in audiovisuellen und Informationsdiensten

7 beispielsweise die Veröffentlichung von *Mein Kampf*" von Adolf Hitler, denn in einigen Ländern, wie in Deutschland, ist die Leugnung des Holocaust verboten; dies ist in anderen Ländern nicht der Fall

4 ERMITTLUNG UND BEKÄMPFUNG ILLEGALER INHALTE IM INTERNET

Es ist Aufgabe der Mitgliedstaaten, für die Einhaltung der Gesetze zu sorgen, indem sie illegale Aktivitäten aufdecken und die Täter bestrafen. Aufgrund der Besonderheiten des Internet ist hier jedoch die Strafverfolgung komplizierter als bei klassischen" Delikten.

Während Gesetzesverletzungen in öffentlichen Internet-Anwendungen (World Wide Web) leicht aufzuspüren sind, ist dies bei privaten Anwendungen (E-Mail zum Beispiel) nicht leicht. Ebenso ist die Einhaltung der Gesetze einzelstaatlich verhältnismäßig leicht durchzusetzen; viel schwieriger ist es jedoch im internationalen Rahmen.

a. Technische Grenzen des Gesetzesvollzugs

Die technische Beschaffenheit von Internet ist Ursache dafür, daß bestimmte Kontrollen nicht greifen. Wegen der Art, in der Internet-Mitteilungen weitergeleitet werden können, ist eine Kontrolle de facto nur am Netzeingang und -ausgang möglich (also bei dem Server, über den der Benutzer Zugang erhält, oder bei dem Endgerät, über das die Informationen gelesen oder heruntergeladen werden, und bei dem Server, bei dem das Dokument veröffentlicht wird).

Selbst wenn ein veröffentlichtes Dokument infolge des Eingreifens der Behörden von einem Server entfernt wird, kann es leicht und schnell kopiert und an andere Server unter anderer rechtlicher Zuständigkeit weitergegeben werden, so daß es weiter verfügbar ist, sofern und solange diese Sites nicht auch gesperrt werden. ***Es ist*** mithin ***eine stärkere internationale Zusammenarbeit erforderlich, um sichere Häfen für Dokumente zu vermeiden, die gegen das Strafrecht verstoßen.***

b. Die Rolle der Internet-Zugangsanbieter und der Host-Dienstanbieter

Die Internet-Zugangsanbieter und die Host-Dienstanbieter ermöglichen den Benutzern Zugang zu Internet-Inhalten. Man darf jedoch nicht vergessen, daß die Hauptverantwortung für die Inhalte bei den Autoren und den Inhaltsanbietern liegt. Daher ist es unerläßlich, die genaue Verantwortungskette" zu ermitteln, damit für illegale Inhalte auch diejenigen zur Verantwortung gezogen werden, die sie verfasst haben.

i) Haftung der Internet-Zugangsanbieter und der Host-Dienstanbieter

Bei illegalen Inhalten (unterschiedlichster Art wie Kinderpornographie, Verstößen gegen das Urheberrecht, betrügerischen Warenangeboten, Verleumdungen usw.) ***kann die Haftung, die sich auch auf die Internet-Zugangsanbieter*** und die Host-Dienstanbieter ***erstrecken kann***, je nach den Umständen, ***unterschiedlich geregelt sein***: Durch das Strafrecht, durch das Zivilrecht (Schadenersatzklage wegen Verletzung des Urheberrechts oder Verleumdung oder Streitigkeiten aufgrund der Verträge mit Benutzern oder Netzbetreibern) oder durch das Verwaltungsrecht (die Regelung des Landes, in dem der Zugangsanbieter und der Host-Dienstanbieter tätig ist). Die ***Zugangsanbieter*** kontrollieren nicht direkt, welche Inhalte im Internet verfügbar sind oder welchen Teil davon ihre Kunden abfragen, aber dennoch wurde in einigen Fällen von behördlicher Seite gegen sie ermittelt. Grund hierfür: Illegale und schädigende Inhalte, auf die über die technischen Einrichtungen der Anbieter zugegriffen werden konnte. Unter Umständen muß das Gesetz geändert oder präzisiert werden, um den Zugangsanbietern und Host-Dienstanbietern, die in erster Linie eine Dienstleistung erbringen, dabei zu helfen, einen Weg zwischen dem Vorwurf der Zensur und der Gefahr der Haftbarmachung zu finden.

Bieten die ***Host-Dienstanbieter*** selbst Inhalte auf dem World Wide Web oder in Newsgroups an, so haften sie hierfür natürlich ebenso wie jeder andere Autor oder Inhaltsanbieter. In den Fällen, in denen die Inhalte von Dritten geliefert werden, muß die Haftung des Host-Dienstanbieters klar geregelt werden.

In mehreren Mitgliedstaaten[8] wurden Rechtsvorschriften verabschiedet oder vorgeschlagen, in denen die Haftung der Host-Dienstanbieter dahingehend definiert ist, daß sie nur haftbar sind für ein auf ihrem Server gespeichertes Dokument, wenn von ihnen billigerweise erwartet werden kann, daß sie das Dokument als *prima facie* illegal erkennen, oder wenn sie es unterlassen, mit angemessenen Maßnahmen dieses Material zu entfernen, wenn sie klar darauf hingewiesen worden sind.

Einige Bestimmungen gehen weiter und scheinen von den Zugangsanbietern zu verlangen, daß sie den Zugang zu anderen Sites, die illegales Material enthalten, beschränken.

Die ***Netzbetreiber*** ihrerseits haften in der Regel nicht straf- oder zivilrechtlich für die in ihren Netzen transportierten Inhalte; es kann von

[8] Österreich, Deutschland, Frankreich, Vereinigtes Königreich (Defamation Bill).

ihnen nach bestimmten Rechtsvorschriften oder Lizenzverträgen jedoch verlangt werden, daß sie gegenüber ihren Kunden (Zugangsanbietern) Schritte unternehmen, wenn diese Einrichtungen zur Weitergabe illegalen Materials benutzen.

Bei der Frage des Haftungsumfangs für Inhalte wie illegale vergleichende Werbung und Verletzungen des Urheberrechts muß auch die eingehende Untersuchung der Kommission über die Auswirkungen der nationalen Bestimmungen auf den Binnenmarkt, insbesondere in den Bereichen kommerzielle Kommunikationen und Urheberrecht, berücksichtigt werden[9].

ii) Selbstkontrolle auf nationaler, europäischer und internationaler Ebene

In mehreren Mitgliedstaaten haben die Internet-Zugangsanbieter und Host-Dienstanbieter bereits eine gewisse Selbstkontrolle eingeführt. Im Vereinigten Königreich wurde ***auf Initiative der Wirtschaft*** ein Verhaltenskodex eingeführt. Ein unabhängiges Gremium, die Safety Net Foundation" wurde eingesetzt; dieses neutrale Gremium bietet einen Bewertungsdienst für Newsgroups und eine Hotline, über die die Allgemeinheit Material melden kann, das sie für illegal hält. Ähnliches ist in Deutschland und den Niederlanden erfolgt.[10]

Die Kommission begrüßt diese allgemeine Tendenz zur Selbstkontrolle und hat die Schaffung eines europäischen Netzes der Verbände von Internet-Zugangsanbietern gefördert. Diese Zusammenarbeit könnte auf eine breitere internationale Ebene ausgedehnt werden. Da die Probleme in der Branche überall gleich gelagert sind, wäre es sinnvoll, wenn die für die Selbstkontrolle zuständigen Einrichtungen ihr Vorgehen vor allem in technischen Fragen koordinieren. Gleichzeitig können in dem stark dezentralisierten Internet-Umfeld die ***Benutzer einen sehr wichtigen Beitrag*** zur Selbstkontrolle der Branche leisten.

iii) Entfernung von Dateien aus den Servern

Wenn sich ein Host-Dienstanbieter darüber klar wird, daß auf seinem Server gespeicherte Inhalte allem Anschein nach illegal sind, muß er gezielte Schritte zur Entfernung dieses Materials unternehmen. Eine entsprechende Information kann von dem im Land des Anbieters eingesetzten Gremium zur Selbstkontrolle oder von einer entsprechenden

---

9 Vorschlag für eine Richtlinie über kommerzielle Kommunikationen, Entwurf einer Mitteilung über Folgemaßnahmen zum Grünbuch Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft.

10 Auch in Frankreich wurde in dem Bericht "*Rapport de la Mission Interministérielle sur l'Internet*" ein Verhaltenskodex vorgeschlagen. Text verfügbar: http:/www.telecom.gouvfr/english/sommaire.htm

Stelle in einem anderen Land kommen. Da Inhalt problemlos kopiert und an andere Server weitergegeben werden kann, müssen auch andere Dienstanbieter nicht nur in dem entsprechenden Land, sondern weltweit auf gleiche Weise vorgehen. Für diesen Prozeß wäre ein internationales Netz von Selbstkontrollgremien äußerst förderlich, allerdings würde der Aufbau eines derartigen Netzes zeitraubend sein.

iv) Zugangssperrung bei den Zugangsanbietern

Kann das illegale Material nicht aus dem Host-Server entfernt werden, beispielsweise weil sich der Server in einem Land befindet, in dem keine Kooperationsbereitschaft besteht, oder weil das Material in dem betreffenden Land nicht illegal ist, könnte die Sperrung des Zugangs beim Zugangsanbieter eine Alternative sein.

Bisher ist jedoch noch unklar, inwieweit es technisch möglich ist, den Zugang zu Material zu sperren, wenn es als illegal erkannt wird. Diese Frage muß unbedingt beantwortet werden, denn davon hängt der Haftungsumfang des Zugangsanbieters ab. Trotz mangelnder Klarheit bezüglich der technischen Machbarkeit wurde diese Vorgehensweise in einigen Ländern gewählt, da es sich bei den Zugangsanbietern um eine relativ kleine, gut zu identifizierende Gruppe handelt.

Einige Drittländer haben sehr weitgehende Vorschriften erlassen, die jeden direkten Zugang zum Internet über die Zugangsanbieter verhindern. Zugang ist nur über Zwischenserver möglich, ähnlich wie in Großorganisationen, wo das aus Sicherheitsgründen geschieht, ***und unerwünschtes Material wird von einer zentralen Stelle indiziert***; damit soll viel mehr kontrolliert werden als die Verbreitung des illegalen Materials, das Gegenstand dieser Mitteilung ist. ***Eine derart restriktive Regelung ist für Europa undenkbar, denn sie stünde im Widerspruch zur politischen Tradition und würde die persönliche Freiheit des Bürgers deutlich einschränken.*** Wegen der Komplexität und Offenheit der europäischen Kommunikationsinfrastruktur wäre eine solche Lösung wahrscheinlich auch nicht praktikabel.

Die deutschen Behörden sind vor kurzem auf eine andere Lösung gekommen: Sie fordern von den Zugangsanbietern, daß sie illegale Inhalte fallweise für ihre Teilnehmer sperren.

Im Fall CompuServe erachtete die Staatsanwaltschaft bestimmte über Newsgroups verbreitete Inhalte für illegal und forderte CompuServe[11] auf, den Zugang zu diesen Newsgroups zu sperren. Da die Software von CompuServe ursprünglich keine Unterscheidung zwischen deutschen

[11] Ein großer internationaler Anbieter von kommerziellen Online-Diensten mit Sitz in den USA, der Internet-Zugang anbietet und viele Abonnenten in Deutschland hat.

Teilnehmern und anderen ermöglichte, sperrte CompuServe bestimmte Newsgroups für alle Teilnehmer.

Daraufhin erhob sich weltweiter Protest, weil Deutschland seine Moralvorstellungen damit anderen aufzwang. Später machte CompuServe die inkriminierten Newsgroups für alle Teilnehmer außer Deutschland wieder zugänglich. Gegen andere in Deutschland ansässige Zugangsanbieter wurden die Behörden anscheinend nicht tätig. Soweit die Provider die betreffenden Newsgroups im Angebot hatten, hatten ihre Teilnehmer weiterhin Zugang zu den beanstandeten Inhalten.

In einem Fall aus jüngster Zeit drohte eine deutsche Staatsanwaltschaft den deutschen Internet-Zugangsanbietern Strafverfolgung an, falls sie den Zugang zu einem Magazin, das von einem Server in den Niederlanden verbreitet wurde und mutmaßlich den Terrorismus propagierte, nicht blockierten. Die Zugangsanbieter kamen dieser Aufforderung unter Protest nach. Damit wurden allerdings alle von dem niederländischen Server verbreiteten Inhalte, auch harmlose, für deutsche Teilnehmer gesperrt, während das beanstandete Dokument für Internet-Nutzer außerhalb Deutschlands zugänglich blieb. Nach diesen Vorfällen trafen die Zugangsanbieter sofort Vorkehrungen zur Umgehung von Sperrungsauflagen[12]. Es ist nicht klar, ob das Material in den Niederlanden als ungesetzlich gilt, auf alle Fälle sind die niederländischen Behörden nicht eingeschritten. Der niederländische Host-Dienstanbieter machte geltend, daß die Maßnahmen der deutschen Behörden eine Behinderung des freien Dienstleistungsverkehrs innerhalb der EU darstellten.

Eine Aufwärtssperrung von Sites kann deshalb einige beträchtliche Nachteile haben. Insbesondere würden kriminelle Benutzer dadurch nicht daran gehindert, zwischen verschiedenen Internet-Funktionen hin und her zu schalten, z. B. von einer Web-Seite zu einer Usenet-Newsgroup oder zur normalen E-Mail-Funktion.

Notwendig ist folglich, wie sich zeigt, eine ***Zusammenarbeit zwischen den Behörden und Internet-Zugangsanbietern, damit Eingriffe ihr Ziel erreichen, ohne dabei über das Notwendige hinauszugehen.***

c. Anonyme Internet-Benutzung

Normalerweise ist die Identität der Internet-Benutzer ersichtlich, entweder ist der Name des Autors oder seine Internetadresse (URL) auf einer World Wide Web-Homepage angegeben, oder es ist eine E-Mail-Adresse für elektronische Post oder eine Newsgroup-Mitteilung aufgeführt. Das entspricht dem demokratischen Grundsatz, wonach jedermann das Recht auf freie Meinungsäußerung hat, jedoch für seine Handlungen die Verantwortung übernehmen muß.[13] Diese grundsätzliche

---

12 Bei der letzten Zählung war das Dokument in 43 WWW-Sites und 2 Newsgroups eingespielt, und es ist auch bei einem E-Mail-Listenserver verfügbar.

13 In dem Vorschlag für eine Richtlinie zu Vertragsabschlüssen im Fernabsatz wird verlangt, daß die Identität des Lieferers, der die Waren und Dienstleistungen im Fernabsatz anbietet, erkennbar sein muß.

Möglichkeit zur legalen Zurückverfolgung sollte deshalb Eingang in nationale oder europäische Verhaltenskodizes für das Remailing finden.

Einige Strafverfolgungsbehörden haben sich besorgt über Techniken geäußert, die eine anonyme Benutzung des Internet ermöglichen. Dies könnte die Versendung illegalen Materials erleichtern, weil es die Identifizierung der Täter erschwert oder sogar unmöglich macht.

Dieses Problem betrifft nicht das World Wide Web, wo die Host-Dienstanbieter wissen, oder zumindest in Erfahrung bringen können, von wem die Inhalte stammen. Es ist den Benutzern indessen möglich, elektronische Post bzw. Mitteilungen an eine Usenet-Newsgroup zu senden, ohne daß der Empfänger Namen oder die E-Mail-Adresse des Absenders erfährt, weil eine zwischengeschaltete Stelle (die Person, die die Mitteilung anonym weitergeleitet hat) diese Information gelöscht hat.

Ein Benutzer kann stichhaltige Gründe dafür haben, daß er anonym bleiben möchte[14] (darunter Angst vor Repressalien wegen der geäußerten Absichten oder mangelndes Vertrauen in die Art, wie seine personenbezogenen Daten vom Empfänger benutzt werden).[15]

Die berechtigte Notwendigkeit von Anonymität sollte jedoch mit den Prinzipien der legalen Rückverfolgbarkeit abgestimmt werden. Die vor kurzem im Vereinigten Königreich vorgelegten Safety-Net-Vorschläge[16] befassen sich mit diesem Zwiespalt. Man ist der Auffassung, daß wirklich anonyme Erfassung eine Gefahr darstellt, nicht jedoch die Verwendung zurückverfolgbarer Pseudonyme. Es wird vorgeschlagen, bekannte Schlupflöcher zu schließen, die Rückverfolgbarkeit von Nachrichten zu verbessern und anonyme Remailer dazu zu verpflichten, Informationen über die Identität der Benutzer festzuhalten. Für diese Informationen gälten die Datenschutzgesetze, sie würden der Polizei unter Einhaltung angemessener datenschutzrechtlicher Bestimmungen zugänglich gemacht.

---

14 Darüber hinaus enthält die Europäische Menschenrechtskonvention einschlägige Bestimmungen, in denen das Recht auf Privatsphäre und Geheimhaltung sowie das Briefgeheimnis bekräftigt werden. Dieselben Grundsätze sind in den Verfassungen und den Verfassungstraditionen aller Mitgliedstaaten festgeschrieben. Vorbehaltlich einiger Ausnahmeregelungen, die in einer demokratischen Gesellschaft notwendig sind, werden sie im Post- und Telekommunikationssektor respektiert.
In ihrer Entscheidung gegen den amerikanischen Communications Decency Act machten die Richter deutlich, daß sie die Anonymität im Internet für schützenswert halten. Sie ist nach ihrer Ansicht notwendig für Internet-Nutzer, die auf sensible Information zugreifen wollen, wie sie auf den Web-Sites Critical Path AIDS Project, Queer Resources Directory (Zielgruppe jugendliche Homosexuelle) und Stop Prisoner Rape (SPR) gespeichert sind.

15 Siehe Abschnitte 29 und 30 des Britischen Vorschlags R3 Safety-Net" http://www.ispa.org.uk

16 R3: Rating, Reporting, Responsibility For Child Pornography and Illegal Material on the Internet", September 1996

Die Frage der legalen Rückverfolgbarkeit erfordert noch einige Arbeit an technischen Fragen und an der weltweiten Zusammenarbeit, damit die entsprechenden Maßnahmen greifen können.

d. Zusammenarbeit von Justiz und Polizei in der EU und weltweit

Wie oben dargestellt, sind die Straftaten von Land zu Land unterschiedlich definiert. Angesichts der Internationalität des Internet ist es möglich, daß sowohl der Autor, als auch der Inhaltsanbieter und der Host-Dienstanbieter dem Zugriff der nationalen Strafverfolgungsbehörden entzogen sind, obwohl die jeweiligen Inhalte nach der Gesetzgebung des betreffenden Landes verboten sind und unter Strafandrohung stehen. Das Strafrecht greift nur innerhalb der Staatsgrenzen. Daher wäre es wichtig, daß die Mitgliedstaaten gemeinsame Mindeststandards für ihr Strafrecht festlegen, um Schlupflöcher für Kriminelle zu stopfen.

Darüber hinaus sollte die Zusammenarbeit von Justiz und Polizei zwischen den EU-Ländern verstärkt werden, und man sollte eine engere Zusammenarbeit mit unseren wichtigsten Partnerländern außerhalb der Union in Betracht ziehen, z. B. auf der Grundlage von Konventionen oder neuen internationalen Rechtsinstrumenten.

In diesem Zusammenhang wäre es sinnvoll, die Zusammenarbeit auch auf die Prävention von Straftaten auszudehnen, zu deren Begehung man sich des Internet bedient.

Ferner wäre es denkbar, daß Techniker, Strafverfolgungs- und Strafrechtsexperten zusammen prüfen, wie gemeinsame Strafrechtsstandards am besten zu verwirklichen sind. Eine engere Zusammenarbeit zwischen Wirtschaft und Strafverfolgungsbehörden auf EU-Ebene sollte ebenfalls unterstützt werden.

Auf ihrem Treffen in Dublin haben die Justiz- und Innenminister vereinbart, im Rahmen von Europol die polizeiliche Zusammenarbeit bei der Bekämpfung von Sexualdelikten gegen Kinder und Menschenhandel (Kinder und Frauen) zu intensivieren und sich um gemeinsame Mindeststandards für die Gesetze gegen den sexuellen Mißbrauch von Minderjährigen zu bemühen. Das sollte als ein erster ermutigender Schritt in diese Richtung angesehen werden.

Desgleichen sollte die Erklärung des Weltkongresses gegen den sexuellen Mißbrauch von Kindern, der vor kurzem in Stockholm stattfand, die Grundlage für gemeinsame Maßnahmen bilden.

Hauptwaffe hierbei sind praktische Vorkehrungen zur Begrenzung des Zugangs Anfälliger zu derartigen Inhalten.

a. Der Grundsatz der freien Meinungsäußerung

Die von allen Mitgliedstaaten unterzeichnete Europäische Menschenrechtskonvention und Teile der allgemeinen Grundsätze im Gemeinschaftsrecht enthalten einschlägige Bestimmungen, in denen das Recht auf freie Meinungsäußerung garantiert wird. Es handelt sich nicht um absolute Rechte, sondern es bestehen wesentliche Auflagen, so daß zum Beispiel die Lizenzvergabe für Rundfunk, Fernsehen oder Film möglich ist. Derselbe Grundsatz hat Eingang in die Verfassungen oder die Verfassungstradition aller Mitgliedstaaten gefunden.

Die Trennlinie zwischen dem, was als Redefreiheit geschützt ist, und dem, was beschränkt werden kann, ist unter Umständen nicht leicht zu ziehen.

In Frankreich annullierte der Verfassungsrat kürzlich die Bestimmungen des Telekommunikationsgesetzes, in denen festgelegt ist, unter welchen Bedingungen Zugangsanbieter (einschließlich Internet-Anbieter) von der strafrechtlichen Haftung für die Inhalte, zu denen sie Zugang anbieten, entbunden sind. Das Gesetz ermächtigte den Conseil Supérieur de Télématique, Empfehlungen dazu zu unterbreiten, welche Inhalte zulässig sind. Der Verfassungsrat vertrat die Ansicht, daß diese Bestimmungen sorgfältiger abgefaßt werden müßten, da es um Fragen der persönlichen Freiheit gehe.[17]

Ein allgemeines Ergebnis ist: ***Eine wie auch immer geartete Regelung zum Schutz Minderjähriger darf nicht in Form eines uneingeschränkten Verbots der Benutzung von Internet zur Weitergabe bestimmten Materials erfolgen, das in anderen Medien frei verfügbar ist.*** Ein weiteres Ergebnis ist: Bestehende Bestimmungen zur Regelung von Inhalten müssen daraufhin geprüft werden, ob sie im Analogieschluß angewandt werden können; zudem sollten nicht allein

---

17 Der Verfassungsrat hat beschlossen, die Artikel 43-2 und 43-3 des Gesetzes über die Regelung des Telekommunikationsbereichs zu streichen. Begründung: Das Gesetz weist dem Conseil supérieur de la télématique die Aufgabe zu, Empfehlungen auszuarbeiten, die geeignet sind, die Einhaltung eines Verhaltenskodex durch bestimmte Kommunikationsdienste sicherzustellen, und diese Empfehlungen dem Conseil Supérieur de l'Audiovisuel zur Verabschiedung zu unterbreiten. Dabei wird der Inhalt der Empfehlungen, zu denen Stellungnahmen mit möglichen strafrechtlichen Auswirkungen abgegeben werden können, allein durch die sehr allgemeinen Bestimmungen von Artikel 1 des Gesetzes vom 30. September 1986 eingeschränkt.

deshalb die restriktivsten Regeln gewählt werden, weil Internet eine so große Reichweite hat.

In den Vereinigten Staaten entschied ein Gerichtshof auf Distrikt-Ebene, daß die Hauptbestimmungen des Communications Decency Act, des Gesetzes zum Schutz Minderjähriger, nicht verfassungskonform seien, und bezog sich dabei auf das im ersten Zusatz zur amerikanischen Verfassung festgehaltene Grundrecht auf freie Meinungsäußerung.[18] Das Gesetz sei zu weit gefaßt; zwar sei es legitim, Minderjährige zu schützen, aber die Dienstanbieter könnten nicht feststellen, ob ein Benutzer minderjährig ist; die Folge davon sei, daß in der Praxis nicht jugendfreie Inhalte überhaupt nicht ohne die Gefahr strafrechtlicher Verfolgung veröffentlicht werden könnten, was im Widerspruch stehe zu dem in der Verfassung verankerten Recht auf freie Meinungsäußerung.

b. Der Rechtsrahmen des Binnenmarktes

Der Informationsverkehr in Netzen, die sich über mehrere Länder erstrecken, ist seiner Natur nach grenzüberschreitend und ***unterliegt damit den Rechtsvorschriften zum Binnenmarkt und dem Wettbewerbsrecht.*** Er ist insbesondere ***durch den Grundsatz des freien Dienstleistungsverkehrs geschützt.*** Einzelstaatliche Stellen können Maßnahmen treffen, die diese Grundfreiheit einschränken, z. B. zum Schutz Minderjähriger, müssen dabei aber den Grundsatz der Verhältnismäßigkeit beachten. Anders gesagt: Staatliche Eingriffe dürfen nicht über das hinausgehen, was zur Erreichung des angestrebten Ziels notwendig ist.

Dementsprechend hat die Kommission kürzlich einen Vorschlag für eine Richtlinie angenommen, die auf Gemeinschaftsebene ein Verfahren für die Information und Kooperation zwischen den Mitgliedstaaten und der Kommission auf dem Gebiet der neuen Vorschriften zu den Diensten der Informationsgesellschaft festlegt.[19] Es soll für gesetzgeberische Transparenz sorgen, der erneuten Zersplitterung des Binnenmarktes entgegenwirken, die Interessen der Allgemeinheit wirksamer schützen und helfen, dem auf diesem Gebiet entstehenden Regulierungsbedarf gezielter zu entsprechen. Die vorgeschlagene administrative Zusammenarbeit zwischen den Mitgliedstaaten und der Kommission wird es der Europäischen Union außerdem ermöglichen, sich zu diesen Fragen auf internationaler Ebene umfassender zu äußern.

c. Filtersoftware für den Hausgebrauch: Eltern schützen ihre Kinder

---

18 US District Court for Eastern Pennsylvania: ACLU v. Reno, 11.Juni 1996 http://aclu.org/

19 KOM(96) 392 endg. vom 30.8.1996

Glücklicherweise gibt es technische Mittel, die es künftig erlauben werden, die unterschiedlichen moralischen Vorstellungen nicht nur in den verschiedenen einzelstaatlichen Rechtssystemen, sondern auch im persönlichen Urteil der Benutzer zu berücksichtigen. Damit werden sich zwei Ziele zugleich verfolgen lassen: der freie Informationsfluß und die Achtung persönlicher Wünsche.

Unter dem Druck der Öffentlichkeit ***wurden in den letzten zwei Jahren Filtersysteme entwickelt, mit denen Eltern den Zugang ihrer Kinder zu bestimmten Internet-Inhalten kontrollieren können.*** Die Zensur findet nicht an der Quelle statt (*Verhinderung* der Veröffentlichung illegalen Materials), sondern beim Nutzer (Verhinderung des *Zugangs Minderjähriger* zu schädigendem Material). Das Filtermodell, das auf die ***Verantwortung der Eltern und nicht*** auf die ***Staatsmacht*** setzt, wird von Industrie und Bürgerinitiativen favorisiert, weil es nach ihrer Ansicht bestimmte Probleme des Internet am wirksamsten löst und sich an unterschiedliche Normen von Moral und Anstand anpaßt. Es ist ein pragmatisches, kein rechtliches Instrument gegen die Verbreitung schädigender Inhalte über das Internet, wenn auch die Bereitstellung von Filtersoftware gewisse rechtliche Konsequenzen haben kann (Zugangsanbieter, die Filtersoftware anbieten, können für die Verbreitung solcher Inhalte nicht belangt werden).

Filtersoftware ist nicht nur am Endpunkt des Übertragungswegs einsetzbar, sondern auch an verschiedenen Stellen davor, z. B. bei den Dienst- und Zugangsanbietern.

Filtersoftware arbeitet nach drei wesentlichen Verfahren: mit Negativlisten (alle darin verzeichneten Sites sind gesperrt), mit Positivlisten (nur die darin verzeichneten Sites sind zugänglich) und mit neutraler Kennzeichnung, bei der die Sites vom Benutzer nach eigenem Ermessen eingestuft werden.

Das ***Negativlisten***-Verfahren ist bei autonomen Filtersystemen der ersten Generation wie Cyber Patrol weit verbreitet. Das im August 1995 eingeführte System Cyber Patrol arbeitet mit Internet-Zugangsanbietern und kommerziellen Online-Diensten zusammen. Seine CyberNOT-Liste enthält rund 7 000 Sites, die in zwölf Kategorien eingestuft sind (Gewalt/Verletzung des religiösen Empfindens, Nacktdarstellungen, Darstellung sexueller Handlungen, vulgäre Darstellungen, Rassismus/Beleidigung ethnischer Gruppen, satanische/sonstige Kulte, Drogen, Extremismus, Glücksspiel, Fragwürdiges, Illegales, Alkohol/Tabak). Eltern können den Zugang zu einer beliebigen Zahl dieser Kategorien sperren, in dem sie in der Programmanager-Maske die entsprechenden Kästen anklicken.

Das ***Positivlisten***-Verfahren beruht auf dem umgekehrten Prinzip. Eine Positivlisten-Software sperrt alle Internet-Inhalte mit Ausnahme derer, die in einer Liste zulässiger Inhalte verzeichnet sind. Dieses Verfahren wirkt stark einschränkend und läuft der Logik des Internet zuwider. Es ist aber sehr sicher und kommt vor allem an Schulen zum Einsatz.

Das Verfahren der ***neutralen Kennzeichnung***: Seit kurzem gibt es die "Platform for Internet Content Selection" (PICS), ein neues System zur neutralen Kennzeichnung und Filterung von Internet-Inhalten, das als Industriestandard propagiert wird. Es unterscheidet sich wesentlich von der Filtersoftware der ersten Generation. Bei ihm sind die Funktionen "Einstufung der Sites" und "Filterung" getrennt. Das ermöglicht ein hohes Maß an Flexibilität und Sicherheit und macht PICS ohne Zweifel zur umfassendsten und innovativsten Lösung des Problems.

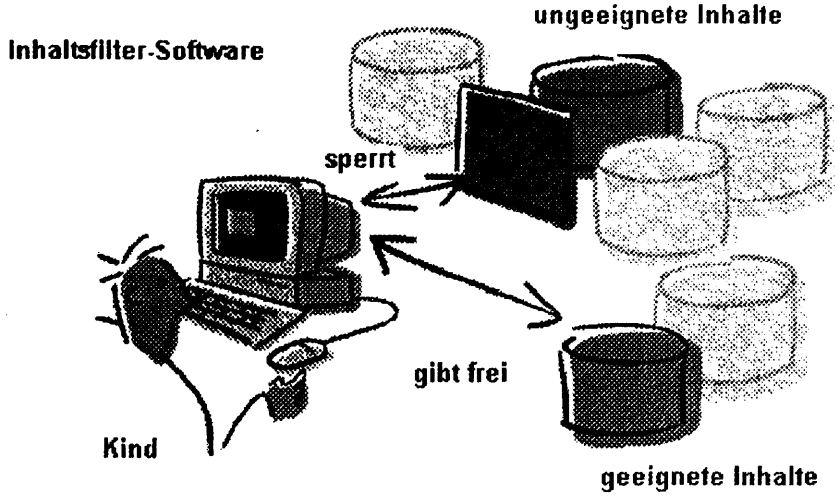

***Abbildung 1**: Filter-Software sperrt automatisch den Zugang zu bestimmten Dokumenten, jedoch nicht den Zugang zu anderen*[20].

d. PICS - ein weltweiter Industriestandard

PICS wurde im Mai dieses Jahres vom WorldWideWeb-Consortium (W3C)*[21] *offiziell vorgestellt. Es ist ein Versuch der Branche, einen weltweiten Standard einzuführen. PICS bietet Zugangskontrolle ohne Zensur" und wird von einer großen Zahl von Hardware- und Softwareherstellern, Zugangsanbietern, kommerziellen Online-Diensten, Verlagen und Inhaltsanbietern unterstützt. Es ist in die neueste Generation von Internet-Suchprogrammen wie Microsoft Explorer 3.0 und Netscape 3.0 integriert und wird auch von mehreren Filterprogrammen unterstützt.

Anders als die Filtersoftware der ersten Generation, die mit Stichwörtern und Ausschlußlisten arbeitet, arbeitet PICS nach dem ***Verfahren der neutralen Kennzeichnung und kann alle Sites filtern, die eine Internet-Adresse (URL) haben.*** (Web-Seiten, FTP, Usenet News). PICS versieht die einzelnen Sites mit wertneutralen Etiketten". Diese Etiketten können Information verschiedener Art tragen: Bewertungen (z. B. nach Sprache, Nacktdarstellungen, sexuellem Inhalt, Gewalt) oder mit Verweisen (auf Inhalte entsprechend ihrem Interesse für bestimmte Benutzerkreise). Ein Site ist nur zugänglich, wenn er 1. eine PICS-Kennzeichnung trägt und

---

20 Diese Netscape-Grafiken sind veröffentlicht auf den WWW-Consortium-Seiten zu PICS. Dieser Site bietet eine ausführliche technische Spezifikation zum PICS-Standard (http://www.w3.org/pub/www/PICS)

21 W3C ist ein Branchenkonsortium, das durch die Erarbeitung von Spezifikationen und von Mustersoftware die Entwicklung des Web und die Interoperabilität zwischen WWW-Produkten zu fördern sucht. W3C ist ein internationales Konsortium; es operiert unter dem gemeinsamen Dach des MIT Laboratory for Computer Science in den Vereinigten Staaten und des INRIA in Europa, die Unterstützung vor Ort leisten und Kernentwicklungen durchführen.Gegründet wurde W3C ursprünglich in Zusammenarbeit mit CERN, von wo das Web seinen Ausgang nahm, sowie mit Unterstützung der DARPA und der Europäischen Kommission.

sich 2. im Rahmen der von den Eltern am PC gesetzten Parametern bleibt. Bewertungen können auch von den Inhaltsanbietern selbst vorgenommen werden (etwa von Unterhaltungsanbietern, die familienorientierte Web-Sites betreiben) oder auch durch Dritte wie Religionsgemeinschaften und Elternvereinigungen. Jede Familie entscheidet selbst, welches Bewertungssystem sie wie verwendet und kann durch Setzen von Parametern bestimmen, was zugelassen und was gesperrt wird.

Die Bewertungssysteme können auf verschiedenen Wegen online oder offline (CD-ROMs) verbreitet und fortgeschrieben werden.

Eltern und Erzieher können den Zugang zu Sites beschränken, die 1. eine PICS-Kennzeichnung tragen und 2. den Parametern entsprechen, die sie auf dem PC gesetzt haben. Das Recreational Software Advisory Council (RSAC) bewertet Videospiele und Web-Inhalte nach den vier Kriterien Sprache, Nacktdarstellungen, sexueller Inhalt und Gewalt und mit den Graden 0 bis 4. Jede Familie kann zur Filterung des Angebots die Kriterien und Grade nach eigenem Ermessen verwenden.

Anders als der V-Chip für Fernsehgeräte, der hardwareseitig ganze Programme sperrt und anders als autonome Softwaresysteme, die alles sperren, was bestimmte vom Benutzer festgelegte Wörter enthält, können ***PICS-kompatible Systeme das Inhaltsangebot individuell nach den Vorstellungen der jeweiligen Familie oder Kultur filtern und sind dazu kostengünstig.*** Wenn auch das Internet ***neue Gefahren geschaffen hat, so bietet diese Filtertechnik doch Möglichkeiten***, die bei anderen Formen der Verbreitung von Inhalten nicht bestehen.

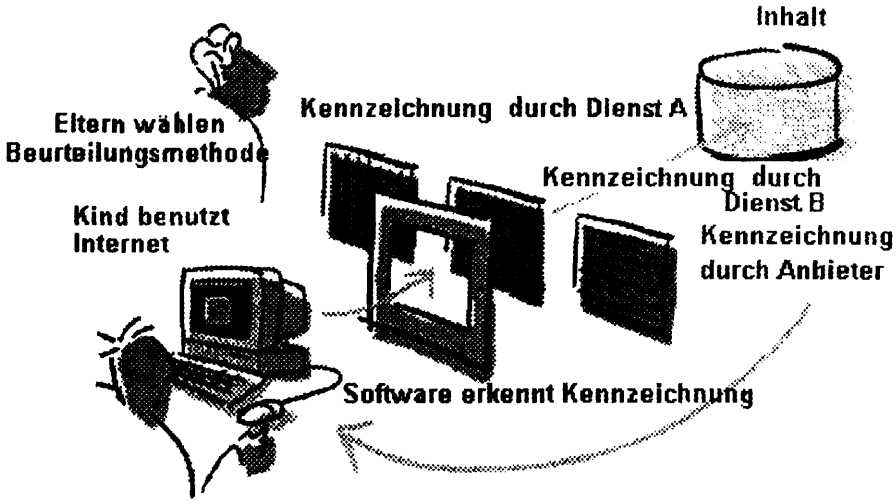

***Abbildung 2**: Die Sperrung von Inhalten durch Filtersoftware erfolgt anhand der Kennzeichnungen durch Anbieter und die Bewertungsstellen Dritter sowie anhand der Auswahlparameter, die die Eltern setzen.*

Die Arbeiten an Kennzeichnungs- und Beurteilungssystemen in der Rechnerumgebung versprechen auch interessante Möglichkeiten zu eröffnen in anderen digitalen Anwendungen, insbesondere auf dem Gebiet des digitalen Fernsehens,. Diese im Hinblick auf die überarbeitete Richtlinie über Fernsehen ohne Grenzen" wichtige Entwicklung wird im Grünbuch zum Jugendschutz und Schutz der Menschenwürde in den neuen audiovisuellen und Informationsdiensten behandelt.

e. Einsatzmöglichkeiten der Filtertechnik

Seit Erscheinen der ersten Prototypen, die mit Stichwörtern arbeiten und deshalb nicht zwischen Pornographie und Medizin unterscheiden können, ***hat sich die Filtersoftware wesentlich verbessert.*** Sie ermöglicht es Eltern jetzt, das Angebot nach bestimmten Wörtern oder Sites zu durchsuchen, kann allerdings noch keine unerwünschten Bilder erkennen, wenn sie nicht von eindeutigem Text begleitet werden, es sei denn, die Software wäre auf einen bestimmten Site hin konfiguriert worden. Bewertungsstellen können aber Sites nach ihrem visuellen Inhalt bewerten und sie damit der PICS-Filterung zugänglich machen.

Gegner des Filtermodells verweisen auf zwei wesentliche Gefahren: Unerwünschtes Material ist über ungeschützte Rechner nach wie vor zugänglich, und in den meisten Familien finden technisch versierte Kinder Mittel und Wege, um doch an unerwünschtes Material zu gelangen. Letzterem hat man bei der Entwicklung von PICS vorgebaut, seine Urheber versichern, es lasse sich nicht ausmanövrieren.

Beim Benutzer zu installierende Filtersoftware der beschriebenen Art dürfte praktisch ***überall billig erhältlich*** sein und es trotz all ihrer Beschränkungen ***den Eltern ermöglichen, ihre Kinder vor unerwünschten Inhalten zu schützen.***

f. Europäische Bewertungssysteme

Europäischen Internet-Nutzern müssen Bewertungssysteme zur Verfügung stehen, die ihren Bedürfnissen entsprechen. Sie dürfen nicht gezwungen sein, mit Systemen zu arbeiten, die für die USA entwickelt wurden, wo andere Ansichten darüber herrschen können, was Minderjährigen zugänglich gemacht werden darf. Deshalb ***ist die Entwicklung europäischer Bewertungssysteme zu fördern.*** Dabei soll kein für ganz Europa einheitliches System entstehen, weil das dem Subsidiaritätsprinzip zuwiderliefe und als Versuch gesehen werden könnte, Europa eine Einheitsmoral zu verordnen. ***Die europäischen Inhaltsanbieter und Bewertungsstellen sollen vielmehr nachdrücklich dazu angehalten werden, ihre eigenen Bewertungssysteme zu entwickeln.*** In jedem Fall wäre dafür Sorge zu tragen, daß bei derartigen Systemen - Bewertung, Listen, Selbstkontrolle - von offenen, auf europäischer oder internationaler Basis entwickelten und nicht herstellereigenen Standards ausgegangen wird.

Parallel dazu sollte die Entwicklung einer europäischen Software zur Filterung und Zurückverfolgung (damit man feststellen kann, woher die illegalen Inhalte kommen) im Rahmen der FuE-Programme der Gemeinschaft gefördert werden.

Um die Öffentlichkeit zur Aufdeckung und Meldung illegaler und schädigender Inhalte anzuhalten, sollen außerdem Meldesysteme ("Hotlines") eingerichtet werden. In den USA haben sich bereits Bürgerinitiativen gebildet, die an der Aktualisierung von Listen und an der Überprüfung von Bewertungen mitwirken.

g. Sensibilisierung der Öffentlichkeit

Das Problem illegaler und schädigender Inhalte im Internet ist weder mit strengem Gesetzesvollzug noch mit bloßem Vertrauen in die Technik wirksam zu lösen, seine Lösung erfordert die Sensibilisierung der Öffentlichkeit. ***Entsprechende Maßnahmen sollen bewirken, daß die Benutzer Nutzen und Gefahren des Internet erkennen.*** Insbesondere Eltern und Erzieher sollten lernen, mit Filtersoftware und Bewertungssystemen umzugehen.

6 MÖGLICHE STRATEGIEN/SCHLUSSFOLGERUNGEN

Die Kommission ist der Auffassung, daß die nachfolgend beschriebenen Maßnahmen zur Eindämmung des Flusses illegaler und schädigender Inhalte im Internet durchgeführt werden sollten. Mit ihnen wird das Ziel verfolgt, den Bürgern der Europäischen Union zu größerem Nutzen aus einem erweiterten Informationszugang über das Internet zu verhelfen. Grundlage für ihre Annahme sollte der EG-Vertrag (freier Dienstleistungsverkehr) sein oder die Zusammenarbeit im Innen- und Justizbereich.

Bei den Vorschlägen geht es um ***erste Sofortmaßnahmen.*** Damit soll keinesfalls anderen Vorschlägen vorgegriffen werden, die sich aus den Diskussionen über das Grünbuch zum Jugendschutz und Schutz der Menschenwürde in den neuen audiovisuellen und Informationsdiensten ergeben.

1. Illegale Inhalte

a. ***Kooperation zwischen Mitgliedstaaten***

Die Zusammenarbeit der Mitgliedstaaten ist unerläßlich, wenn man die Quellen, aus denen gesetzeswidriges Material kommt, bekämpfen und die Weitergabe von Kopien beschränken will.

Die Kooperation im Innen- und Justizbereich muß so ausgeweitet werden, daß sie auch umfaßt

- den ***Austausch von Informationen*** über die Anbieter gesetzeswidriger Inhalte und die Durchsetzung bestehender Rechtsvorschriften über gesetzeswidriges Material;

- die Veranlassung der Mitgliedstaaten,sich - wenn auch auf dem kleinsten gemeinsamen Nenner - auf eine ***europaweit einheitliche Definition*** gesetzeswidriger Inhalte zu einigen.

b. ***Haftung der Zugangsanbieter und Host-Dienstanbieter***

Es sollte festgestellt werden, ob in einem gemeinsamen europäischen Rahmen geklärt werden müßte, inwieweit die Zugangsanbieter und Host-Dienstanbieter für illegale Inhalte haftbar gemacht werden könnten.

c. ***Förderung von Selbstkontrolle***

Im Interesse einer verstärkten Selbstkontrolle wird die Kommission weiterhin die ***Zusammenarbeit zwischen Verbänden von Internet-Zugangsanbietern fördern.*** In den Mitgliedstaaten, in denen derartiges noch nicht angelaufen ist, wäre dieser Prozeß in Gang zu

setzen. Im Zusammenhang mit der Rolle der Zugangsanbieter und Host-Dienstanbieter bei der Beschränkung der Weitergabe illegalen Materials wird die Kommission die ***Erörterung und Erforschung der technischen Aspekte*** dieser Frage unterstützen.

2. Schädigende Inhalte

Maßnahme der Gemeinschaft zur Förderung der Benutzung von Filtersoftware und Bewertungssystemen

- In einer Empfehlung des Rates könnte die klare politische Botschaft formuliert werden, daß ***die Benutzung von Filtersoftware wie PICS*** und eines europäischen Bewertungsystems bzw. mehrerer solcher Systeme ***nahegelegt*** wird. Die Kommission hat bereits an die Branche appelliert, eine gemeinsame Plattform zu bilden, damit Filtersysteme gemeinschaftsweit eingesetzt werden können.

- Die europäischen ***Inhaltsproduzenten*** sollten ermutigt werden, bei diesem System zusammenzuarbeiten und einen eigenen ***Verhaltenskodex für im Internet veröffentlichte Inhalte*** mit systematischer Selbstbewertung des Inhalts aufzustellen.

- Eine Kommissionsinitiative zugunsten ***nationaler Sensibilisierungsmaßnahmen für Eltern und Lehrer*** ist vorgesehen.

3. Internationale Fragen

a. Eine internationale Konferenz

Auf dem Industrierat am 8. Oktober 1996 wurde das Angebot Deutschlands, eine internationale Konferenz auszurichten, angenommen. Vertreten sein werden die Strafverfolgungsbehörden, ferner Zugangsanbieter, Host-Dienstanbieter und Benutzer. Inhaltlich geht es in erster Linie um:

- die Realisierbarkeit von ***Sofortmaßnahmen einschließlich eines Rahmens für internationale Zusammenarbeit*** ausgehend von den bestehenden Rechtsvorschriften;

- die Erörterung der ***Möglichkeit einer internationalen Konvention über illegale und schädigende Inhalte.***

b. Ausdehnung des Dialogs

Da an diesem Dialog die größtmögliche Zahl von Ländern beteiligt sein muß, könnte er dann auf eine Organisation mit umfassenderer Mitgliedschaft ausgedehnt werden, z. B. die OECD, die Welthandelsorganisation, die Vereinten Nationen oder eine ihrer Sonderorganisationen.

4. Flankierende Maßnahmen

a. Mechanismus zur Förderung der Transparenz

Regulierungsfragen werden auf Gemeinschaftsebene systematisch und transparent erörtert, um dadurch zu kohärenten und effizienten Lösungen zu gelangen.

b. Informations-Web-Site

Auf dem World Wide Web wird (mit einem Kommissions-Server als Host) ein Site geschaffen, der Originalinhalte und Verbindungen zu entsprechenden Seiten in anderen Sites enthält. Dieser Web-Site wird Teil eines umfassenderen Satzes von Web-Seiten sein, die sich mit dem ganzen Bereich der Information und ähnlichen Fragen beschäftigen und im Rahmen des Aktionsplans "Lernen in der Informationsgesellschaft" geschaffen werden sollen.

Als Material kämen in Betracht: a) Informationen und Anleitungen für Eltern, Lehrer und Kinder; b) Software für Elternkontrolle; c) Informationen über Tätigkeiten staatlicher Stellen (EU-Institutionen, Mitgliedstaaten, Drittländer, internationale Organisationen und Nicht-Regierungsorganisationen).

ISSN 0254-1467

KOM(96) 487 endg.

DOKUMENTE

DE

15 16 06

Katalognummer : CB-CO-96-517-DE-C

ISBN 92-78-10299-7

Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften

L-2985 Luxemburg