Kölner Arbeitspapiere zur Bibliotheks- und Informationswissenschaft
Band 8

Jugendschutz und Internet in Öffentlichen Bibliotheken

Susanne Klötzer

Juli 1998

Fachhochschule Köln
Fachbereich Bibliotheks- und Informationswesen

Klötzer, Susanne:

Jugendschutz und Internet in Öffentlichen Bibliotheken /

von Susanne Klötzer. -

Köln : Fachhochschule Köln, Fachbereich Bibliotheks- und

Informationswesen, 1998. -

(Kölner Arbeitspapiere zur Bibliotheks- und Informationswissenschaft; 8)

ISSN (Print) 1434-1107

ISSN (elektronische Version) 1434-1115

*Die **Kölner Arbeitspapiere zur Bibliotheks- und Informationswissenschaft** berichten über aktuelle Forschungsergebnisse des Fachbereichs Bibliotheks- und Informationswesen der Fachhochschule Köln. Veröffentlicht werden sowohl Arbeiten der Dozent/inn/en, als auch herausragende Arbeiten der Studierenden. Die Kontrolle der wissenschaftlichen Qualität der Veröffentlichungen liegt bei der Schriftleitung. Jeder Band erscheint parallel in Printversion und in elektronischer Version (über unsere Homepage: http://www.fbi.fh-koeln.de/papers/index/titel/htm).*

Fachhochschule Köln Fachbereich Bibliotheks- und Informationswesen Claudiusstr.1 D-50678 Köln

Tel.: 0221/8275-3376 Fax: 0221/3318583

Schriftleitung: Christine Bieletzki, Sabine Schäfer, Prof. Dr. Wolfgang G. Stock

Inhaltsverzeichnis

Zusammenfassung

Im Rahmen einer Diplomarbeit zum Thema "Jugendschutz und Internet in Öffentlichen Bibliotheken" werden die für den Jugendmedienschutz relevanten Gesetze vorgestellt. Neben dem Strafgesetzbuch und dem Gesetz über die Verbreitung jugendgefährdenten Schriften wird insbesondere auf die Jugendschutzregelungen des neu eingeführten Informations- und Kommunikationsdienste-Gesetzes des Bundes und des Mediendienste-Staatsvertrags der Bundesländer eingegangen. Es wird untersucht, welche Konsequenzen bestehende und durch das IuKDG neu hinzukommende Jugendschutzregelungen auf den Internet-Zugang einer öffentlichen Bibliothek haben. Abschließend werden Möglichkeiten genannt, die sich Öffentliche Bibliotheken mit Internet-Angebot bieten, um den jugendschutzrechtlichen Anforderungen gerecht werden zu können. In diesem Rahmen werden Arbeitsweisen und Charakteristika von Filtersoftware vorgestellt, die eine technische Regulierungsmöglichkeit des Internet-Zugangs bieten.

1 Einleitung

Für Bibliotheken und ihre Kunden ist das Internet aufgrund des großen weltweiten Informationsangebotes von Interesse. Es bietet seinem Besucher eine Vielfalt an Informationen für Bildung, Beruf und Freizeit.
Im folgenden geht es nicht um die positiven Aspekte des Internets, sondern um den Teil, der illegale und schädigende Inhalte enthält. Als Randerscheinung existiert im Internet ein Markt für Pornographie und für gewaltverherrlichendes und rechtsextremistisches Gedankengut. Diese Inhalte, die laut einer Schätzung der Bundesregierung ca. 1 % ausmachen, bringen das Internet immer wieder in die Diskussion.
Die illegalen und schädigenden Inhalte des Internets stellen die Bibliothek vor ein Problem, wenn sie das Internet Kindern und Jugendlichen zugänglich macht. Die Bibliothek hatte bislang die Möglichkeit, durch ihre fachkundige Auswahl zu verhindern, daß jugendgefährdende Materialien in die Bibliothek gelangen, beziehungsweise sie konnte durch Magazinaufstellung den freien Zugang zu solchen Materialien verhindern. Mit dem Internet-Zugang bietet sie jedem Kunden theoretisch den Zugang zu pornographischem, gewaltverherrlichendem oder rechtsextremistischem Material. Dies darf jedoch nicht dazu führen, daß sie Kindern und Jugendlichen den Zugang zum Internet untersagt. Gerade sie sind eine wichtige Zielgruppe von Bibliotheken, die die Möglichkeit haben muß, den Umgang mit dem Internet zu lernen.
Diese Problematik motivierte zu der vorliegenden Arbeit.

Zunächst wird in Kapitel 2 kurz auf die Entstehung und die technischen Grundlagen des Internets eingegangen. Des weiteren werden die Möglichkeiten der Kommunikation im Internet vorgestellt. Es werden die illegalen und schädigenden Inhalte und die Möglichkeiten zur Verbreitung in den Kommunikationsdiensten aufgezeigt. Ferner wird dargestellt, warum die bestehenden deutschen Gesetze nicht so einfach im Internet umzusetzen sind.

Kapitel 3 behandelt die für den Jugendmedienschutz relevanten Gesetze. Neben dem Strafgesetzbuch und dem Gesetz über die Verbreitung jugendgefährdender Schriften wird insbesondere auf die Jugendschutzregelungen des neu eingeführten Informations- und Kommunikationsdienste-Gesetzes des Bundes und des Mediendienste-Staatsvertrages der Bundesländer eingegangen.

Die für Anwendung und Kontrolle des Jugendschutzes im Internet zuständigen gesetzlich geforderten Organisationen werden in Kapitel 4 vorgestellt.

Kapitel 5 enthält die jugendschutzrechtlichen Anforderungen für den Internet-Zugang in Öffentlichen Bibliotheken. Neben den Benutzungsbeschränkungen, die bereits aufgrund bestehender gesetzlicher Jugendschutzregelungen einschränkende Wirkung auf die Ausleihe haben, wird untersucht, welche Konsequenzen sich aus den Jugendschutzregelungen im Informations- und Kommunikationsdienste-Gesetz ergeben.

Abschließend werden Möglichkeiten genannt, die sich Öffentlichen Bibliotheken mit Internet-Angebot bieten, um den jugendschutzrechtlichen Anforderungen gerecht werden zu können.

Eine Möglichkeit der technischen Regulierung des Internet-Zugangs ist die in Kapitel 6 behandelte Filtersoftware. Hier werden die Arbeitsweisen und Charakteristika sowie die Vor- und Nachteile vorgestellt.

Kapitel 7 stellt die Ergebnisse einer Umfrage im Rahmen der Diplomarbeit vor, in der Öffentliche Bibliotheken nach der Gestaltung ihres Internet-Zugangs für Kinder und Jugendliche befragt wurden.

2 Internet

2.1 Technik und Geschichte

Im Kalten Krieg wurde von der US-Regierung der Auftrag vergeben, ein Kommunikationsnetz zu entwickeln, daß selbst nach einem Atomkrieg noch eine sichere und effektive Kommunikation ermöglichen sollte. Die Lösung sah ein Netz ohne Zentrale, ohne Hierarchie und ohne direkte Verbindung zwischen Sender und Empfänger vor. So bestand die Möglichkeit, daß bei Ausfall eines einzelnen Computersystems die verbliebenen Netzabschnitte alternative Datenverbindungen aufbauen konnten. Aus dieser Grundidee heraus, die 1969 mit dem ARPANET ihren Anfang nahm, entstand das Internet (vgl. Klau 1995, 31).
Die ursprüngliche Absicht der US-Regierung, ein „unzerstörbares“ Kommunikationsnetz zu initiieren, ist für die heutigen mangelhaften Kontrollmöglichkeiten ausschlaggebend (vgl. Sieber 1996c, 429 ff).
Die Kommunikation der Rechner untereinander wird durch die freiwillige Akzeptanz des Netzwerkprotokolls TCP/IP ermöglicht. Das „Transmission Control Protocol“ (TCP) teilt die Daten in einzelne Pakete auf. Das „Internet Protocol“ (IP) versendet die Pakete zu ihrem Zielort. Dabei können die einzelnen Pakete unterschiedliche Wege durch das Netz nehmen. Am Ziel angekommen werden die einzelnen Pakete wieder zu einer Nachricht zusammengesetzt (vgl. Klau 1995, 33). Eine weitere Aufgabe des Netzwerkprotokolls TCP/IP ist es, dafür zu sorgen, daß wenn ein Netzknoten gesperrt ist, die Datenpakete auf einem anderen Weg zu ihrem Ziel kommen (vgl. Sieber1996c, 429 ff). Daß diese Versandart schwer zu kontrollieren ist, zeigt sich beispielsweise dadurch, daß ein pornographisches Bild in 50 Datenpakete zerlegt werden und über 16 Netzwerkknoten durch 7 Länder laufen kann. Der Betreiber eines Netzwerkknotens merkt zwar, daß einzelne Pakete über seinen Rechner laufen, den Inhalt kann er ohne die übrigen Pakete jedoch nicht entschlüsseln (vgl. Lahrmann 1997, 13). Da es keinen zusammenhängenden Datenstrom gibt, können Kontroll- und Schutzmechanismen nur beim Sender oder Empfänger eingesetzt werden (vgl. Klau 1995, 31).

Die anarchischen Strukturen und die Unkontrollierbarkeit des Datenflusses bereiten dem geltenden Rechtssystem Probleme. Um eine Straftat ahnden zu können, benötigt das deutsche Recht den Zugriff auf den Verursacher, der sich auf deutschem Territorium aufhalten muß.

2.2 Teilnehmer

Hinter dem Internet steht keine Firma oder Organisation, die das Netzwerk leitet. Statt dessen ist es eine Ansammlung tausender, individueller Netzwerke und Organisationen, die einzeln betrieben und finanziert werden. Die Summe dieser Netzwerke und Organisationen bildet das Internet (vgl. Gralla 1997, 5). Jeder Betreiber eines Servers sowie die Inhaber der Leitungen tragen zum Funktionieren des Netzes bei. Durch Hyperlinks können Verknüpfungen zu anderen Angeboten hergestellt werden, so daß ein Inhalte-Anbieter zum „kleinen Betreiber" werden kann. Die Grenzen zwischen Anbieter und Nutzer im Internet sind fließend. Jeder mit Zugang zum Internet kann Homepages erstellen und somit zum Anbieter werden (vgl. Engel 1996, 221). Um das Internet nutzen zu können, wird nur ein PC mit entsprechender, leicht erhältlicher Software, ein Modem und eine Telefonleitung benötigt. Auf diese Weise ist es jedem möglich, jederzeit seine Meinung im Internet zu verkünden.

Das Internet besitzt bis heute keine Zentrale, die in irgendeiner Form den Zugang oder die publizierten Seiten kontrolliert. Statt dessen wurde das Internet zu einem Lern- und Experimentierfeld für die soziale Selbstorganisation. Die Internet-Gemeinde hat einen Verhaltenskodex entwickelt, die sogenannte Netiquette. Unhöflichkeiten, Beschimpfungen und ähnliches werden zuerst mit einer Ermahnung von den übrigen Teilnehmern geahndet. Sollte das nicht ausreichen, kann der Netzzugang des „Störenfrieds" mit hunderten und tausenden E-Mails für einige Tage verstopft werden (vgl. Lahrmann 1997, 13).
Diese Selbstregulierung reicht jedoch nicht aus. Mit der steigenden Popularität des Internets hat auch die „Unterwelt" die Pfade des Netzwerks für sich entdeckt. Eine Vielfalt von Rechtsverstößen sind die Folge. Es werden unter anderem Straftaten im Bereich des Urhebergesetzes begangen, Software wird illegal vertrieben, Pornographie und nationalsozialistisches Gedankengut wird verbreitet und Kindesmißbrauch vorgeführt (vgl. Collardin 1995, 618).

2.3 Kommunikationsmöglichkeiten im Internet

Das Internet ist im Gegensatz zum Rundfunk- und Fernsehwesen überwiegend benutzerinduziert, da ein beträchtlicher Teil der Inhalte von Benutzern selbst und nicht von etablierten Verlegern publiziert wird (vgl. Illegal 1996, 6). Da niemandem das Internet gehört, ist auch keiner da, der den Zugang zum Internet beschränken kann oder die produzierten Inhalte kontrolliert oder bewertet. Jedem Teilnehmer ist es möglich, anonym auf Inhalte zuzugreifen und anonym seine Meinung zu äußern. Die Anonymität und die fehlende Kontrolle führt in einigen Fällen zu Enthemmungen.
Das Internet ermöglicht sowohl einen nationalen als auch einen internationalen Datenaustausch, in dem Daten mit strafbaren Inhalten übertragen werden können (vgl.

Sieber 1996c, 431). Im folgenden werden die populärsten Dienste und die jeweiligen Möglichkeiten des Mißbrauchs vorgestellt.

2.3.1 World-Wide-Web (WWW)

Spätestens mit Einrichten des World-Wide-Webs (WWW) Anfang der neunziger Jahre ist das Internet zu einem Massenmedium geworden.
Das WWW ist eine Sammlung von mehreren Millionen Web-Seiten. Jeder, der über einen Anschluß an das Internet mit entsprechender Software und Zugang zu Speicherplatz auf einem Host-Rechner verfügt, kann Web-Seiten im Internet publizieren (vgl. Illegal 1996, 6). Die multimedialen Fähigkeiten (Text, Bild, Ton) des WWW sind für einen Mißbrauch, beispielsweise im pornographischen Bereich, leider gut geeignet (vgl. Sieber 1996c, 433).

Eine Kontrolle im WWW ist aufgrund der Vielzahl der Web-Seiten kaum möglich. Zudem befinden sich die angebotenen Seiten in der Regel nicht auf den Computern des Zugangsvermittlers. Dieser hat nur die Möglichkeit, den gesamten Zugang zu einem WWW-Server mit rechtswidrigen Inhalten zu sperren. Damit ist nicht nur der Zugang zu den rechtswidrigen Inhalten, sondern das gesamte auf diesem Server vorhandene Material gesperrt (vgl. Sieber 1996c, 433).

2.3.2 E-Mail und Mailing-Listen

Bei E-Mail handelt es sich um elektronische Post. Sie ist eine der meist genutzten Dienste des Internets. Innerhalb kürzester Zeit können Nachrichten mit angehängten Grafiken, Video- und Klangdateien übermittelt werden (vgl. Gralla 1997, 45). Durch die Möglichkeit, Dateien anhängen zu können, eignet E-Mail sich zum Verbreiten von strafbaren Inhalten. Zudem ist es sehr leicht möglich, die Absenderadresse einer E-Mail zu verfälschen oder zu anonymisieren (vgl. Sieber 1996c, 431 f).
Des weiteren kann man mittels E-Mail an Diskussionsgruppen im Internet teilnehmen, die als Mailing-Listen bezeichnet werden. E-Mails werden an eine bestimmte Adresse gesandt und von dort aus an alle Gruppenmitglieder verteilt. Diese Listen werden genutzt, um sich untereinander über alle erdenklichen Themen auszutauschen. Zu unterscheiden sind moderierte und unmoderierte Listen. Bei unmoderierten Listen werden alle E-Mails automatisch weitergeleitet. Die E-Mails einer moderierten Liste werden von einem Moderator auf ihren Inhalt überprüft und erst dann an die Liste weitergeleitet. Ziel ist es, mehrfache, falsche oder zweifelhafte E-Mails von der Liste fernzuhalten (vgl. Klau 1995, 282 f).

Eine Überwachung von E-Mails ist schon wegen des „Briefgeheimnisses“ rechtlich problematisch. Mittels eines Textfilters könnten die Inhalte der E-Mails theoretisch zwar auf anstößige Begriffe hin überprüft werden, dies würde jedoch in der Praxis an den großen Mengen von versandten E-Mails scheitern. Textfilter können anstößige Begriffe erkennen, aber nicht den Kontext, in dem sie benutzt werden. Somit würden viele Beiträge mit nicht strafbaren und harmlosen Inhalten eliminiert (z.B. „Ich bin gegen Nazis.“). Diese Methoden würden auch nicht greifen, wenn die Texte von E-

Mails verschlüsselt sind. Zudem können angehängte Bild- und andere Binärdateien damit nicht überprüft werden (vgl. Sieber 1996c, 431 f).

2.3.3 Newsgroups

Newsgroups sind Diskussionsgruppen des Usenets. Das Usenet ist ein weltweites elektronisches Diskussionsforum, das einen Nachrichtenaustausch innerhalb des gesamten Internets ermöglicht. Newsgroups behandeln alle erdenklichen Themen, bei denen es etwas mitzuteilen oder zu diskutieren gibt. Spezielle News-Server halten die Newsgroups zum Abruf bereit, wobei die Auswahl der Newsgroups je nach News-Server unterschiedlich ist. Neben Texten können auch Bilder und Multimedia-Dateien in Newsgroups veröffentlicht werden. Aufgrund des hohen Speicherbedarfs der Newsgroups werden diese Nachrichten nach einigen Tagen - spätestens nach einigen Wochen - wieder gelöscht. Analog zu den Mailing-Listen gibt es moderierte und unmoderierte Newsgroups (vgl. Gralla 1997, 55).
Die Verbreitung einer Nachricht erfolgt sehr einfach. Sie wird zuerst auf dem News-Server des lokalen Netzes abgelegt und kann sofort innerhalb dieses Netzes gelesen werden. Die Nachrichten werden im Gegensatz zu Mailing-Listen nicht an die einzelnen Teilnehmer versandt. In bestimmten Zeitabständen treten unterschiedliche News-Server miteinander in Kontakt und die Nachrichten werden zum nächsten News-Server weitergeleitet. So geht es weiter und eine Nachricht kann innerhalb von drei Tagen die ganze Welt erreichen (vgl. Klau 1995, 333).

Da eine Newsgroup immer auf dem News-Server eines Providers gespeichert ist, besteht bei illegalen und schädigenden Inhalten die Möglichkeit, daß der Provider Newsgroups sperrt oder löscht. In so einem Fall können die Teilnehmer problemlos auf einen anderen News-Server zugreifen, der diese Newsgroup ebenfalls anbietet. Der Provider müßte den Zugang auf alle News-Server dieser Welt sperren, um so den Zugang zu dieser Newsgroup zu verhindern. Statt die gesamte Newsgroup zu sperren, kann der Provider auch einen Textfilter einsetzen, bei dem sich aber die gleichen Probleme wie bei der E-Mail ergeben (vgl. Sieber 1996c, 432).

2.3.4 Internet Relay Chat (IRC)

Der Internet Relay Chat bietet den „direktesten“ Kommunikationsweg im Internet. Er ermöglicht das Chatten („Plaudern“) nahezu in Echtzeit. Mitteilungen werden über die Tastatur an die anderen Teilnehmer fast augenblicklich übertragen. Auf diese Weise können sich mehrere Menschen auf der Welt miteinander „unterhalten“. Der IRC ermöglichte zum Beispiel 1993 während des Putschversuches in Rußland oder bei dem Erdbeben in Los Angeles Kontakt zu Augenzeugen (vgl. Gralla 1997, 61).
Für jedes Thema gibt es einen Kanal, in dem sich der Besucher einwählen kann. Er legitimiert sich mit einem Codenamen und kann dann alle Nachrichten der anderen Teilnehmer lesen und mit-chatten. Es besteht auch die Möglichkeit, sich mit einem Teilnehmer ins „Separé“ zurückzuziehen. Hier kann er mit ihm unbeobachtet von den anderen Teilnehmern chatten (vgl. Gralla 1997, 61). Diese Separés werden auch von Pornohändlern für Verhandlungen mit ihren Kunden mißbraucht. Mit bis zu

300 pädophilen Nutzern pro Minute soll der IRC ein Umschlagplatz für den Vertrieb von Kinderpornographie sein (vgl. Lahrmann 1997, 16).

Da der IRC Kommunikation in Echtzeit ist und die Daten nirgendwo gespeichert werden, ist eine Kontrolle kaum möglich. Bei dem Service-Provider AOL befinden sich hierzu beispielsweise Lotsen „under-cover" in den Chatrooms, die die Unterhaltungen „beobachten" und notfalls eingreifen.

2.4 Inhalte

Das Internet bietet Kindern und Jugendlichen eine Vielzahl von positiven Informations- und Unterhaltungsangeboten für Schule und Freizeit.
Was anstößige Inhalte anbelangt, bringt das Internet nichts Neues. Die Kommission der Europäischen Gemeinschaften bezweifelt, daß in den neuen Diensten mehr strittige Inhalte enthalten sind, als in den traditionellen Medien. Sie räumt aber ein, daß in den neuen Diensten diese Inhalte deutlich sichtbarer, leichter zugänglich und schwerer zu kontrollieren sind (vgl. Grünbuch 1996, 13). Laut Schätzungen der Bundesregierung von 1996 beträgt der Teil der schädigenden und illegalen Inhalte weniger als 1% (vgl. Chancen 1996, 68).
Während das Internet auf der einen Seite eine Plattform für den demokratischen Informationsaustausch ist, wird es beispielsweise auf der anderen Seite von Pornographen, Pädophilen und Sekten genutzt, um ihre fragwürdigen Informationen zu verbreiten.
Für den Jugendschutz sind die Teile relevant, die Gefährdungspotentiale wie Rechtsextremismus, Gewaltverherrlichung und/oder Pornographie enthalten (vgl. Hilse 1997, 2). Durch die Verbreitung solcher Inhalte kommt das Internet immer wieder in die Diskussion.

Am 16.10.1996 veröffentlicht die EU-Kommission die Mitteilung über „Illegale und schädigende Inhalte" im Internet. Sie unterscheidet zwischen illegalen Inhalten, die als Straftat gelten (z.B. Kinderpornographie) und schädigenden Inhalten, die Erwachsenen erlaubt sind, aber auf Kinder eine schädigende Wirkung haben und ihnen nicht zugänglich gemacht werden sollen. Diese Differenzierung der Inhalte wird vorgenommen, weil sie unterschiedliche technische und rechtliche Regelungen verlangen (vgl. Illegal 1996, 10).

2.4.1 Illegale Inhalte

Die Verbreitung vieler Inhalte wird bereits durch verschiedene rechtliche Vorschriften eingeschränkt. Werden diese Vorschriften verletzt, hat das zur Folge, daß diese Inhalte illegal sind.
Darunter fallen die folgenden Bereiche:

- Schutz von Rechten des Einzelnen (Schutz der Privatsphäre und des guten Rufes),
- Verletzung des Urheberrechts,
- Verleumdungen und

– rechtswidrige vergleichende Werbung (vgl. Illegal 1996, 10).

Diese Rechte verteidigen die „verletzten“ Personen durch zivilrechtliche Klagen auf Schadensersatz oder einer gerichtlichen Verfügung. In einigen Fällen gibt es auch strafrechtliche oder verwaltungsrechtliche Rechtsmittel (vgl. Illegal 1996, 10).

Zu den illegalen Inhalten, die vom Staat verfolgt werden, gehören

– Kinderpornographie,
– Menschenhandel,
– rassistisches oder zum Rassenhaß anstiftendes Gedankengut,
– Terrorismus und
– sämtliche Formen des Betruges (vgl. Illegal 1996, 10).

Wenn Inhalte gegen das geltende Recht verstoßen, ist es Aufgabe des jeweiligen Staates, für die Einhaltung seiner Gesetze zu sorgen. Die technischen Grundlagen und die Internationalität des Internets verhindern jedoch die Durchführung einer wirksamen Kontrolle und erfordern eine grenzübergreifende Verfolgung von Straftaten (vgl. Illegal 1996, 11ff).

Wie schwierig das ist, zeigt das Beispiel Kinderpornographie. Während in einigen Mitgliedsstaaten der Europäischen Union Kinderpornographie laut Rechtsvorschrift verboten ist, bekommt sie in anderen Staaten nur den Status, „anstößiges Material“ zu sein (vgl. Illegal 1996, 11).

Um gegen illegale Inhalte einschreiten, beziehungsweise um sie verhindern zu können, empfiehlt die Kommission der Europäischen Gemeinschaften eine stärkere internationale Zusammenarbeit, z.B.

– die Schaffung von Selbstkontrolleinrichtungen der Internet-Zugangsanbieter und Diensteanbieter, die mittels eines gemeinsamen Verhaltenskodex illegale Inhalte verhindern; ebenso deren europaweite Zusammenarbeit,
– die Einsetzung einer „Cyberpolice“ im Rahmen von Europol,
– die verstärkte Zusammenarbeit von Justiz und Polizei,
– die Entwicklung von europaweiten rechtlichen Mindeststandards über gesetzwidrige Inhalte (vgl. Illegal 1996, 21).

2.4.2 Schädigende Inhalte

Schädigende Inhalte sind in ihrer Definition abhängig von dem kulturellen Umfeld und werden innerhalb der Grenzen eines Landes definiert. Werden die Wertvorstellungen oder die Gefühle eines Landes verletzt, besteht das Ziel, Regeln zum Schutz festzulegen. Dabei soll das Recht der freien Meinungsäußerung und der Informationsfreiheit nicht eingeschränkt werden (vgl. Illegal 1996, 11).

Zu den schädigenden Inhalten zählen aus deutscher Sicht Schriften, die nach Erfahrungen imstande sind, die gesunde sittliche Entwicklung von Menschen unter 18 Jahren zu beeinträchtigen. Dazu zählen Schriften, die unsittlich, verrohend wirkend, zu Gewalttätigkeit, Verbrechen oder Rassenhaß anreizen oder den Krieg verherrlichen (vgl. § 1 Abs. 1 GjS). Diese dürfen Erwachsenen, aber nicht Minderjährigen zugänglich gemacht werden.

Im Gegensatz zu den illegalen Inhalten kann der Staat zum Schutze Minderjähriger schädigende Inhalte nicht generell verbieten. Es ist ihm im Internet aber nicht möglich - verglichen mit anderen Medien wie Schriften, Rundfunk und Fernsehen - Regelungen zu treffen, die verhindern, daß Kinder und Jugendliche Zugang zu schädigenden Inhalte erhalten, diese jedoch Erwachsenen zugänglich bleiben. Aus diesem Grund liegt die Verantwortung bei dem Endverbraucher, der auf seinem heimischen PC Filtersoftware zum Schutz installieren kann (vgl. Illegal 1996, 19). Die Kommission der Europäischen Gemeinschaften sieht Filtersoftware nur als ein pragmatisches Instrument, mit dem die Verbreitung schädigender Inhalte an Minderjährige nicht rechtlich untersagt werden kann (vgl. Bericht 1997, 22).

2.5 Recht im Internet

Als globales virtuelles Netz ist das Internet nicht an territoriale Grenzen gebunden. Wäre es auf das Gebiet der Bundesrepublik Deutschland beschränkt, würden alle Teilnehmer einheitlich dem bundesdeutschen Recht unterliegen, welches „deutsche“ sozialethische Wertvorstellungen widerspiegelt. Die Bestimmungen des Gesetzes über die Verbreitung jugendgefährdender Schriften wären mit einem etwas größeren Aufwand genauso umsetzbar wie beispielsweise bei Rundfunk und Fernsehen.
Für die meisten illegalen und jugendgefährdenden Inhalte im Internet gibt es im deutschen Recht bereits einen Rechtsrahmen. Diese stehen somit nach deutschem Recht unter Strafe. Aus diesem Grunde kann man das Internet nicht als einen rechtsleeren oder rechtsfreien Raum bezeichnen, denn alle Beteiligten (Autoren, Inhalte-Anbieter, Host-Anbieter, Netzbetreiber, Zugangsanbieter und Endnutzer) unterliegen den Gesetzen des Landes, in dessen Gerichtsbarkeit sie sich befinden (vgl. Illegal 1996, 10). Ist die Identität und der Aufenthaltsort eines sich in Deutschland befindenden Anbieters bekannt, können die Staatsanwaltschaft und andere Aufsichtsbehörden bei Rechtsverstößen einschreiten. Es ist in diesem Fall unerheblich, ob sich die Inhalte auf einem deutschen oder ausländischen Server befinden (vgl. Engel 1996, 225).
Da sich das Internet nicht auf das Gebiet der Bundesrepublik Deutschland beschränkt, gestaltet sich die Verfolgung von Straftaten außerordentlich schwierig, wenn es sich um ausländische Anbieter/Teilnehmer handelt. Inhaltliche Standards sind auf der Welt nicht überall gleich und eine Inhaltskontrolle ist nur auf nationaler Ebene möglich. Dies bedingt das Hauptproblem der rechtlichen Situation. Es wird deutlich, daß von den Staaten gemeinsame Mindeststandards im Bezug auf das Recht entwickelt werden müssen (vgl. Illegal 1996, 12 ff).

Das Internet ist geprägt von einer massenhaften Individualkommunikation, wo jeder Teilnehmer Sender und Empfänger ist. Eine Kontrolle ist weder technisch noch organisatorisch möglich. Hinzu kommt die Zielsetzung der Internet-Gemeinde nach einer offenen Kommunikation frei von Kontrollen. Kontrollversuche werden als Störungen interpretiert, die sofort technisch umgangen werden können. Gegen Störungen gefeit zu sein, ist auch die ursprüngliche Entwicklungsvorgabe der US-Regierung für die Funktionsweise des Kommunikationsnetzes gewesen.

Da zahlreiche virtuelle Aktivitäten in der realen Welt Auswirkungen haben, bedarf es einer rechtlichen Regulierung. Gegen rechtliche Eingriffe wehrt sich ein Teil der Internet-Gemeinde. Statt dessen propagieren sie die Selbstregulierung, die sogenannte Netiquette. Sanktionen sind beispielsweise das „Zumüllen" einer Mailbox oder der Ausschluß aus einer Diskussionsgruppe. In vielen Bereichen greifen die Sanktionen der Netiquette jedoch nicht ausreichend, um Täter abzuschrecken. Es ist auch zu fragen, wer die Netiquette „macht", die Grenzen der Sanktionen festlegt und ihre Einhaltung überwacht. Somit obliegt es den Staaten, für eine Regulierung zu sorgen, um Straftaten zu verhindern bzw. begangene Delikte zu bestrafen und Minderheiten und bestehende Rechte des Einzelnen und der Allgemeinheit zu schützen. Die langjährige Abstinenz der Justiz kann auch nicht darüber wegtäuschen, daß das Recht und die begangenen Straftaten im Internet keinen anderen Stellenwert haben, als in der realen Welt (vgl. Sieber 1996a, 285 f).

3 Jugendmedienschutz

Der Jugendschutz besitzt in der Bundesrepublik Deutschland einen sehr hohen Stellenwert. Die im Grundgesetz verankerte Informations- und Meinungsfreiheit (§ 5 Abs. 1 GG) wird eingeschränkt durch „Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre" (§ 5 Abs. 2 GG). Geschützt werden Kinder und Jugendliche unter 18 Jahren (§ 1 Abs. 4 GjS).

Regelungen zum Jugendschutz sind verankert
- im Strafgesetzbuch,
- im Gesetz zum Schutze der Jugend in der Öffentlichkeit (JÖSchG),
- im Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte (GjS),
- im Mediendienste-Staatsvertrag und
- für Hörfunk und Fernsehen im Rundfunkstaatsvertrag bzw. in den Landesrundfunkgesetzen (vgl. Jugendmedienschutz 1995, 45).

3.1 Strafgesetzbuch (StGB)

Ausgangspunkt für den Jugendschutz sind die Tatbestände der §§ 131 und 184 des Strafgesetzbuches. Dieses Kernstrafrecht des Jugendschutzes kann gleichermaßen auf Anbieter im In- und Ausland angewandt werden, vorausgesetzt,
der strafrechtliche Erfolg tritt im Inland ein. Allerdings kann der Anbieter aus dem Ausland nicht so leicht zur Verantwortung gezogen werden (vgl. Scholz 1996, 8 f).

3.1.1 Gewaltdarstellungen, Aufstachelung zum Rassenhaß (§ 131 StGB)

§ 131 des Strafgesetzbuches wird 1973 aufgrund der zunehmenden Brutalisierung in den Medien und der Gefährlichkeit von exzessiven Gewaltdarstellungen eingeführt (vgl. Scholz 1992, 45).

Der Paragraph beinhaltet drei Tatbestandsalternativen (vgl. Jugendmedienschutz 1995, 45 ff):

- Schriften (i.S. von § 11 Abs. 3), die zum Rassenhaß aufstacheln.

Gemeint sind Schriften, die mittels rassenideologischer Hetze gegen Mitglieder einer im In- oder Ausland existierenden Rasse aufrufen.

- Schriften, die grausame oder sonst unmenschliche Gewalttätigkeiten gegen Menschen in einer Art schildern, die eine Verherrlichung oder Verharmlosung solcher Gewalttätigkeiten ausdrückt.

Darunter fallen Schriften, die menschenverachtende und rücksichtslose Tendenzen beinhalten, oder in denen „besondere Schmerzen oder Qualen körperlicher oder seelischer Art zugefügt werden und der Täter daneben aus gefühlloser und unbarmherziger Gesinnung handelt" (Scholz 1992, 95). Verherrlichung liegt vor, wenn die Gewalttätigkeit besonders heldenhaft dargestellt wird; Verharmlosung liegt vor, wenn die Handlung bagatellisiert wird (vgl. Jugendmedienschutz 1995, 46).

- Schriften, die grausame oder sonst unmenschliche Gewalttätigkeiten gegen Menschen in einer Art darstellen, so daß das Grausame oder Unmenschliche des Vorganges in einer die Menschenwürde verletzenden Weise erscheint.

Die Menschenwürde wird verletzt, wenn es sich um „exzessive Schilderungen von Gewalttätigkeiten“ (Scholz 1992, 95) handelt, die in allen Einzelheiten genüßlich geschildert werden.

Wer solche Tatbestände verbreitet, öffentlich ausstellt, anschlägt, vorführt oder sonst zugänglich macht, insbesondere Personen unter 18 Jahren, kann nach § 131 Abs. 1 Nr. 4 mit einer Geldstrafe oder einer Freiheitsstrafe bis zu einem Jahr bestraft werden.

3.1.2 Verbreitung pornographischer Schriften (§ 184 StGB)

In § 184 des Strafgesetzbuches werden zwei Arten von Pornographie unterschieden:

- die „einfachen“ (Jugendmedienschutz 1995, 47) pornographischen Schriften, die Erwachsenen zugänglich sind, aber Kindern und Jugendlichen unter 18 Jahren nicht zugänglich gemacht werden dürfen (§ 184 Abs. 1). Unter „einfacher“ Pornographie werden Schriften gefaßt, die ausschließlich oder überwiegend auf die Erregung eines sexuellen Reizes bei dem Betrachter abzielen.
- die „harte“ (Jugendmedienschutz 1995, 47) Pornographie, mit Darstellungen von „Gewalttätigkeiten, [...] sexuellen Mißbrauch von Kindern oder sexuelle[n] Handlungen von Menschen mit Tieren“ (§ 184 Abs. 3). Der Besitz, das Verbreiten und Zugänglichmachen dieser Pornographie ist generell untersagt und kann mit einer Freiheitsstrafe bis zu einem Jahr oder mit einer Geldstrafe bestraft werden.

3.2 Das Gesetz über die Verbreitung jugendgefährdender Schriften (GjS) in seiner bis zum 30.07.1997 gültigen Fassung

Neben den allgemeinen strafrechtlichen Bestimmungen wird der Schutz für Kinder und Jugendliche durch das Gesetz über die Verbreitung jugendgefährdender Schriften ergänzt. Das GjS findet Anwendung auf Schriften, Ton- und Bildträger, Ab-

bildungen und andere Darstellungen. Davon ausgenommen sind Kino- und Videofilme, wenn sie von der Obersten Landesbehörde für eine bestimmte Altersgruppe freigegeben sind, und Ausstrahlungen im Fernsehen (vgl. Jugendmedienschutz 1995, 56 ff).
„§ 1 Abs. 1 ist die zentrale Vorschrift des GjS und darüber hinaus gleichsam das Fundament des Jugendmedienschutzes in der Bundesrepublik Deutschland“ (Scholz 1992, 47). Er schreibt vor, daß „Schriften, die geeignet sind, Kinder oder Jugendliche sittlich zu gefährden“, in eine Liste aufzunehmen sind. Es handelt sich dabei um solche Schriften, die anerkannten und akzeptierten Erziehungszielen der Gesellschaft zuwiderlaufen (vgl. Jugendmedienschutz 1995, 56 ff), die laut Gesetz unsittlich, verrohend wirkend, zu Gewalttätigkeit, Verbrechen oder Rassenhaß anreizen oder den Krieg verherrlichen.
Ob ein Medium in diesem Sinne als jugendgefährdend einzustufen ist, wird mittels eines förmlichen Verwaltungsverfahrens von der Bundesprüfstelle für jugendgefährdende Schriften festgesetzt. Bei positiver Entscheidung erfolgt die Aufnahme in die Liste für jugendgefährdende Schriften. Gegen diese Entscheidung kann der Hersteller des Mediums Rechtsmittel einlegen. Mit der Aufnahme in die Liste unterliegt das Medium weitreichenden Einschränkungen, die in § 3 GjS geregelt werden (vgl. Jugendmedienschutz 1995, 56 ff).
In § 3 GjS wird das Verbreitungsverbot von Medien, die in die Liste aufgenommen worden sind (§ 1 GjS) oder als „schwer gefährdend“ (§ 6 GjS) gelten, geregelt. Solche Medien dürfen einem Kind oder Jugendlichen weder „angeboten, überlassen oder zugänglich gemacht werden“ (§ 3 Abs. 1 Nr. 1 GjS). Das heißt, sie dürfen nicht „an einem Ort, der Kindern oder Jugendlichen zugänglich ist oder von ihnen eingesehen werden kann, ausgestellt, angeschlagen, vorgeführt oder sonst zugänglich gemacht werden“ (§ 3 Abs. 1 Nr. 2 GjS). Diese Medien dürfen auch Erwachsenen nicht zugänglich gemacht werden, wenn Kinder oder Jugendliche Einblick haben. Es besteht die Ausnahme, daß jugendgefährdende Medien in Ladengeschäften für Erwachsene zugänglich gemacht werden können, wenn diese für Kinder und Jugendliche nicht zugänglich und nicht einsehbar sind (§ 3 Abs. 1 Nr. 3 GjS). Die Ladenräume müssen baulich und organisatorisch von den übrigen Geschäftsräumen getrennt sein. Das gilt für alle Formen der gewerblichen Gebrauchsüberlassung (vgl. Scholz 1992, 58).

§ 4 GjS regelt das Verbreitungsverbot außerhalb von Geschäftsräumen. Es umfaßt ein Verbreitungsverbot im Einzelhandel außerhalb von Geschäftsräumen (§ 4 Abs. 1 Nr. 1 GjS), in Kiosken (§ 4 Abs. 1 Nr. 2 GjS), im Versandhandel (§ 4 Abs. 1 Nr. 3 GjS) oder in gewerblichen Leihbüchereien oder Lesezirkeln (§ 4 Abs. 1 Nr. 4 GjS). An Personen, die Medien in dieser Form verteilen, dürfen Verleger und Zwischenhändler indizierte Medien nicht liefern (§ 4 Abs. 2 GjS). Weiter ist ihnen die Einfuhr indizierter Schriften untersagt (§ 4 Abs. 3 GjS). Ein bestehendes Indizierungsverfahren oder die Indizierung selbst darf nicht für die geschäftliche Publikumswerbung genutzt werden (§ 5 Abs. 1 GjS). Unter Strafe ist es untersagt, indizierte oder gemäß § 6 GjS schwer jugendgefährdende Schriften anzubieten, anzukündigen oder anzupreisen (§ 21 Abs. 1 Nr. 6 GjS) (vgl. Scholz 1992, 63). Von dieser Beschränkung ist

der Handel innerhalb der Medienbranche und an Orten ausgenommen, die für Kinder und Jugendliche weder zugänglich noch einsehbar sind (§ 5 Abs. 3 GjS). Ziel ist es, mit diesen Werbebeschränkungen jugendgefährdende Medien aus dem Wahrnehmungsbereich von Kindern und Jugendlichen zu verdrängen (vgl. Jugendmedienschutz 1995, 59).
Verstöße gegen die §§ 3 ff. GjS stehen gesetzlich unter Strafe. Sie werden sowohl bei Vorsatz als auch bei Fahrlässigkeit gemäß § 21 GjS verfolgt. Es kann eine Freiheitsstrafe bis zu einem Jahr oder eine Geldstrafe verhängt werden. Fahrlässig handelt jemand, der die Sorgfalt außer acht läßt (vgl. Scholz 1992, 85). Nach der Rechtsprechung ist dem Gesetz Genüge getan, wenn der BPjS-Report bezogen, regelmäßig ausgewertet und beachtet wird (vgl. Jugendmedienschutz 1995, 59). Schwer jugendgefährdende Medien können durch Strafgerichte beschlagnahmt und zum Zwecke der Vernichtung eingezogen werden.

3.3 Das Informations- und Kommunikationsdienste-Gesetz des Bundes und der Mediendienste-Staatsvertrag der Bundesländer

Seit dem 01.08.1997 regeln Bundesregierung und Bundesländer den Sachverhalt Multimedia mittels zweier neuer Gesetze. Ziel ist es, eine Rechtsgrundlage für die Diensteanbieter und Nutzer zu schaffen (vgl. Bundestags-Drucksache 13/7385, 1).

3.3.1 Die Entstehung

Das Internet kann zu minimalen Kosten von jedem genutzt werden. Es läßt sich im Gegensatz zum Rundfunk, der durch das Bundesverfassungsgericht zu einer positiven Regulierung seines Programms verpflichtet ist, durch staatliche Vorgaben kaum regulieren (vgl. Engel 1996, 223).
Mit der raschen Entwicklung des Internets zum allgemein zugänglichen Informations- und Kommunikationsmedium und zum Wirtschaftsfaktor kamen die ersten Forderungen nach einer rechtlichen Regulierung.
Bereits 1994 weist die Zentrale der Deutschen Telekom AG darauf hin, daß der Btx-Staatsvertrag angesichts neuer Entwicklungen im Anwendungsbereich und neuer Diensteanbieter auf dem Markt überholt sei. Der unabhängige Rat für Forschung, Technologie und Innovation fordert einheitliche wirtschaftliche Rahmenbedingungen bei Multimedia-Diensten. Außerdem sei eine Fortentwicklung im Datenschutz, der Datensicherheit, im Urheberschutz und im Jugendschutz erforderlich (Müller-Using/ Lücke 1997, 7 ff).
Unstrittig zwischen Bund und Bundesländer war die Wahrnehmung der Querschnittskompetenzen des Bundes für das Strafrecht, das Bürgerlichen Recht, den Datenschutz, den Jugendschutz und das Urheberrecht zur Regelung der entsprechenden Aspekte bei Multimedia-Diensten. In diesen Bereichen sollte das bestehende Gesetzeswerk erweitert werden (vgl. Müller-Using/ Lücke 1997, 7 ff).
Strittig war dagegen die Vorlage eines Gesetzes zur Regelung der Teledienste (TDG, Art 1 IuKDG). Hier wird im besonderen die Zulassung und die Inhaltsverantwortung der Diensteanbieter geregelt. An der Frage, ob der Bund oder die Bundesländer die Regelungskompetenz für die Teledienste haben, entstand der Streit. Da ein hoher Druck entstand, möglichst schnell zu einer gesetzlichen Regelung zu

kommen, setzten Bund und Bundesländer im Juli 1996 eine Verhandlungskommission ein, die den Streit schlichten sollte. Als Ergebnis wurde vereinbart, daß der „Bund neben der Querschnittskompetenz für bestimmte Anwendungen im Bereich der Multimedia-Dienste originär regelungsbefugt für das Teledienstegesetz ist, während die anderen Informations- und Kommunikationsdienste im Mediendienste-Staatsvertrag (der Bundesländer) erfaßt werden sollen“ (vgl. Müller-Using/ Lücke 1997, 7 ff).

3.3.2 Die Geltungsbereiche

Die am 01.08.1997 in Kraft getretenen Gesetze sind in Artikel 1 IuKDG (TDG) und Abschnitt 1 MDStV nahezu wortgleich. Sie unterscheiden sich im wesentlichen in ihren Geltungsbereichen. Kaum eine Kommentierung befaßt sich nicht mit der Abgrenzung der beiden Gesetzeswerke zueinander (vgl. hierzu Engel-Flechsig 1997, 231 ff; Bonin/Köster 1997, 821 ff ;Müller-Using/Lücke 1997, 7 ff).
Die Geltungsbereiche werden jeweils in § 2 TDG und MDStV geregelt. In diesen beiden Paragraphen wird ausgesagt, welcher Bereich in die Regelungskompetenz des Bundes und welcher Bereich in die Regelungskompetenzen der Bundesländer fällt.
Der Bund erhält die Zuständigkeit für „alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierten Daten wie Zeichen, Bilder oder Töne bestimmt sind [...]“ (§ 2 Abs. 1 TDG). Darunter fallen zum Beispiel Telebanking, Telespiele, Datenaustausch, Angebote von Waren und Dienstleistungen (§ 2 Abs. 2 TDG).
Der Mediendienste-Staatsvertrag regelt die an die Allgemeinheit gerichteten Informations- und Kommunikationsdienste (Mediendienste) in Text, Ton oder Bild (§ 2 MDStV). Dieser Bereich deckt die Massenkommunikation ab (vgl. Müller 1997, 28).

3.3.3 Das Informations- und Kommunikationsdienste-Gesetz (IuKDG)

Bei dem Informations- und Kommunikationsdienste-Gesetz handelt es sich um ein Artikelgesetz, in dem Erstregelungen mit Änderungen und Ergänzungen bereits bestehender Gesetze vereinigt werden. Weiter handelt es sich um ein Mantelgesetz, das unterschiedliche Rechtsmaterien um den Gegenstand Multimedia regelt (vgl. Engel-Flechsig 1997, 233).

Das Informations- und Kommunikationsdienste-Gesetz beinhaltet drei neue Gesetze:
- das Teledienstegesetz,
- das Teledienstedatenschutzgesetz und
- das Signaturgesetz.

In sechs weiteren Artikeln werden bestehende Bundesgesetze geändert:
- Änderung des Strafgesetzbuches,
- Änderung des Gesetzes über Ordnungswidrigkeiten,
- Änderung des Gesetzes über die Verbreitung jugendgefährdender Schriften,
- Änderung des Urheberrechtsgesetzes,

- Änderung des Preisangabengesetzes und
- Änderung der Preisangabenverordnung.

An dieser Stelle werden die für den Jugendschutz relevanten neu eingeführten und geänderten Gesetze kurz skizziert. Eine vertiefende Darstellung findet in den Kapiteln 3.3.5 und 3.3.6 statt.

Gesetz über die Nutzung von Telediensten (Artikel 1 IuKDG)
Hauptaufgabe des Gesetzes ist die Regelung der wirtschaftlichen Rahmenbedingungen für Informations- und Kommunikationsdienste. Dazu zählt die Zugangsfreiheit, die Regelung der Verantwortlichkeit von Diensteanbietern für eigene und fremde zur Nutzung bereitgehaltene Inhalte und die Anbieterkennzeichnung.

Änderung des Strafgesetzbuches (Artikel 4 IuKDG) und Änderung des Gesetzes über Ordnungswidrigkeiten (Artikel 5 IuKDG)
Vorgenommen wird die Klarstellung des Schriftenbegriffs im Strafgesetzbuch und im Gesetz über Ordnungswidrigkeiten. Der Schriftenbegriff wird ausgeweitet auf „elektronische, elektromagnetische, optische, chemische oder sonstige Datenspeicher". Erfaßt werden damit sowohl „Inhalte in Datenträgern (Magnetbänder, Festplatten, CD-ROMs u.a.) als auch in elektronischen Arbeitsspeichern, welche die Inhalte nur vorübergehend bereithalten" (Bundestags-Drucksache 13/7385, 36). Mit dieser Angleichung wird seitens des Gesetzgebers erreicht, daß mittels moderner Datentechnik verbreitete rechtswidrige Inhalte erfaßt werden (vgl. Bundestags-Drucksache 13/7385, 36).

Änderung des Gesetzes jugendgefährdender Schriften (Artikel 6 IuKDG)
Eingeführt werden auf die Informations- und Kommunikationsdienste bezogene spezifischen Jugendschutzregelungen.

3.3.4 Der Mediendienste-Staatsvertrag (MDStV)

Der Mediendienste-Staatsvertrag hat ebenso wie das Informations- und Kommunikationsdienste-Gesetz den Bereich der neuen Medien zum Regelungsgegenstand. Während das IuKDG schwerpunktmäßig die „Teledienste" regelt, d.h. sich auf die individuell und interaktiv angelegten Abrufdienste erstreckt, werden im MDStV Dienste mit massenkommunikativen Charakter geregelt (vgl. Gounalakis 1997, 2993).
Für diese an die Allgemeinheit gerichteten „Mediendienste" formuliert der MDStV - in Struktur, Aufbau und Wortlaut dem IuKDG in Art. 1 und 2 vergleichbar - den Anwendungsbereich und Regelungen für die Zugangsfreiheit und den Datenschutz. Darüber hinaus werden für die Werbung, den Jugendschutz, die Aufsichtsmaßnahmen und Ordnungswidrigkeitstatbestände eigene Regelungen getroffen (vgl. Engel-Flechsig 1997, 237 f).

3.3.5 Jugendschutzbestimmungen im IuKDG und MDStV

Die bisherigen Jugendschutzbestimmungen sind für die „alten" Medien auf nationaler Ebene als effektiv und praktikabel anzusehen. Altersfreigaben für Kino- und Vi-

deofilme werden, wenn auch nicht lückenlos, weitestgehend eingehalten und akzeptiert. Auch das Verbreitungsverbot für indizierte Medien kann hierbei überwiegend kontrolliert und umgesetzt werden. Eine zufriedenstellende Regelung gibt es für den Jugendschutz ebenso im Bereich der Computerspiele und im Fernsehen (vgl. Hilse 1997, 2 f). In den beiden neuen Gesetzen wird der Jugendschutz auf die neuen Medien erweitert. Mit § 5 TDG/MDStV (Verantwortlichkeitsregelung der Diensteanbieter), Artikel 6 IuKDG (Änderung des GjS) und § 8 MDStV (Jugendschutz) werden dazu wichtige Regelungen getroffen.

3.3.5.1 Verantwortlichkeitsregelungen im Teledienstegesetz (§ 5 TDG) und im MDStV (§ 5 MDStV)

Die Regelung zur Klarstellung der Verantwortlichkeit von Diensteanbietern für die Inhalte ihrer Angebote wird jeweils in § 5 TDG und MDStV festgelegt. Die Regelungen zu der zivilrechtlichen, strafrechtlichen und verwaltungsrechtlichen Verantwortlichkeit der Betreiber von elektronischen Informations- und Kommunikationsdiensten werden in weitgehender Übereinstimmung getroffen, unterscheiden sich aber in ihren Geltungsbereichen (vgl. Sieber 1997, 583).

Zunächst wird in § 3 Abs. 1 TDG der Begriff des Diensteanbieters präzisiert. Als Diensteanbieter im Sinne des Gesetzes gelten „natürliche oder juristische Person oder Personenvereinigungen, die eigene oder fremde Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln“. Diensteanbieter nehmen im wesentlichen drei Handlungsformen wahr, die aufgabenbezogen voneinander abgegrenzt werden (vgl. Bundestags-Drucksache 13/7385, 19).

§ 5 Abs. 1 TDG verfolgt den Grundsatz der Eigenverantwortung der Diensteanbieter für die von ihnen angebotenen eigenen Inhalte. Als eigene Inhalte sind auch die von Dritten hergestellten Inhalte zu sehen, die sich der Anbieter zu eigen macht. Der Urheber ist für rechtswidrige Inhalte nach der geltenden Straf- und Zivilrechtsordnung verantwortlich (vgl. Bundestags-Drucksache 13/7385, 20). Bibliotheken sind davon betroffen, wenn sie eigene Inhalte anbieten, z.B. eine Homepage.

§ 5 Abs. 2 greift die Verantwortlichkeit für fremde Inhalte auf. Angesprochen wird der Diensteanbieter, „der Inhalte in das Netz einstellt“ (vgl. Bundestags-Drucksache 13/7385, 20). Darunter sind die Diensteanbieter zu fassen, die als „technische Quelle“ oder „service provider“ fungieren, auf deren Server sich fremde Inhalte befinden und abgerufen werden können (vgl. Bonin/Köster 1997, 822).
Auch hier bleibt die Verantwortung in erster Linie beim Urheber. Diensteanbieter sind allerdings für rechtswidrige Inhalte verantwortlich, „wenn sie von diesen Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern“ (§ 5 Abs. 2 TDG). Die Verantwortlichkeit wird mit der Zumutbarkeitsklausel eingeschränkt. Einen unzumutbaren Aufwand stellt die Sperrung der Nutzung von ganzen Dienstbereichen oder die Einstellung des gesamten Teledienstes dar, wenn es sich nur um einzelne rechtswidrige Inhalte auf dem Server handelt (vgl. Bundestags-Drucksache 13/7385, 20).

Betroffen sind Öffentliche Bibliotheken, wenn sie auf einem eigenen Server Inhalte Dritter anbieten.

Die dritte Handlungsform wird in § 5 Abs. 3 TDG aufgeführt. Hierbei handelt es sich um den Zugangsvermittler, der nicht für rechtswidrige Inhalte Dritter verantwortlich zu machen ist. Als Zugangsvermittler wird bezeichnet, wer „fremde Inhalte ohne auf sie Einfluß nehmen zu können, zum abrufenden Nutzer durchleitet“ (Bundestags-Drucksache 13/7385, 20). Als Zugangsvermittler werden T-Online, AOL, Compuserve sowie die deutschen Universitäten bezeichnet (vgl. Bonin/Köster 1997, 822). Ob öffentliche Bibliotheken zu den Zugangsvermittlern und damit dem Gesetz nach überhaupt zu den Diensteanbietern gehören, ist abhängig von der Auslegung des Gesetzes und bedarf möglicherweise noch der Klärung.
Da ein Zugangsvermittler für rechtswidrige Inhalte Dritter nicht verantwortlich ist, ergeben sich für die Öffentlichen Bibliotheken keine Konsequenzen daraus, ob sie als Zugangsvermittler gelten oder nicht.

3.3.5.2 Jugendschutz im IuKDG (Artikel 6 IuKDG)

Artikel 6 des IuKDG regelt den Jugendschutz auf bundesrechtlicher Ebene.
Das Gesetz sieht ein inhaltlich aufeinander abgestuftes Konzept vor:

- Die Anpassung des Schriftenbegriffs parallel zum Strafgesetzbuch und zum Gesetz über Ordnungswidrigkeiten. Als Konsequenz daraus ist die Bundesprüfstelle für jugendgefährdende Schriften ermächtigt, jugendgefährdende Inhalte auf Datenträgern zu indizieren (Artikel 6 Nr. 2 IuKDG).
- Die Verpflichtung der Diensteanbieter zur Einführung technischer und sonstiger Vorkehrungen, um die Verbreitung von jugendgefährdenden Inhalten an Kinder und Jugendlichen unter 18 Jahren zu verhindern (Artikel 6 Nr. 3 IuKDG).
- Die Bestellung eines Jugendschutzbeauftragten für gewerbliche Informations- und Kommunikationsdienste (Artikel 6 Nr. 5 IuKDG) (vgl. Engel-Flechsig 1997, 237).

In Artikel 6 Nr. 1 des IuKDG wird die Bezeichnung des Gesetzes erweitert auf: „Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte“. Damit soll der Ausweitung des Schriftenbegriffs, die parallel zu der Ausweitung des Schriftenbegriffs im Strafrecht erfolgt (Artikel 4 IuKDG) (vgl. Engel-Flechsig/Maennel/Tettenborn 1997, 2990), auf Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen (§ 1 Abs. 3 GjS) und der damit einhergehenden Ausweitung des Geltungsbereichs Rechnung getragen werden (vgl. Bundestags-Drucksache 13/7385, 37).

Der Bund unterstellt damit die Inhalte der neuen Informations- und Kommunikationsdienste, „die für eine individuelle Nutzung [...] bestimmt sind“ (§ 2 Abs. 1 TDG), den Regelungen des Gesetzes über die Verbreitung jugendgefährdender Schriften und regelt sie nicht nach dem Vorbild des Rundfunkstaatsvertrags. Mit dieser Einordnung gewährleistet die Bundesregierung, daß in Folge der Indizierung von Schriften, die im Grundgesetz verankerte freie Meinungsäußerung und Informationsfreiheit (§ 5

Abs. 1 GG) nicht berührt wird, aber gleichzeitig der Schutz von Kindern und Jugendlichen (§ 5 Abs. 2 GG) bestehen bleibt. Indizierte Schriften unterliegen nur dem Abgabe-, Verbreitungs- und Werbeverbot an Kindern und Jugendlichen, bleiben für Erwachsene jedoch zugänglich (vgl. Engel-Flechsig/Maennel/Tettenborn 1997, 2990 ff).

Einen klarstellenden Charakter hat die Ergänzung des IuKDG in Artikel 6 Nr. 3a, in dem das bereits bestehende Verbreitungsverbot (§ 3 Abs. 1 GjS) in Form des Zugänglichmachens, Vorführens oder sonstigen Zugänglichmachens an einem Ort, der Kindern oder Jugendlichen zugänglich oder einsehbar ist, zusätzlich auf die Informations- und Kommunikationsdienste erstreckt wird (vgl. Bundestags-Drucksache 13/7385, 37 f).
„Anbieter indizierter Inhalte“ (Bundestags-Drucksache 13/7385, S, 38) werden verpflichtet, „durch technische Vorkehrungen Vorsorge“ (Bundestags-Drucksache 13/7385, S, 38) zu treffen, daß „das Angebot oder die Verbreitung im Inland auf volljährige Benutzer beschränkt werden kann" (§ 3 Abs. 2 Satz 2 GjS). Andernfalls bleibt das Verbreitungsverbot bestehen. Allerdings macht der Gesetzgeber eine Einschränkung, indem er sagt, „daß die technischen Vorkehrungen [...] in der Praxis zuverlässig umsetzbar sind und keine unzumutbaren Anforderungen an den Anbieter stellen“ (Bundestags-Drucksache 13/7385, S, 38) dürfen.

Um die Bundesprüfstelle zu entlasten und das Verfahren der Indizierung zu beschleuni-gen (vgl. Engel-Flechsig/Maennel/Tettenborn 1997, 2991), werden in § 18 GjS auch Schriften der Indizierung unterworfen, die „ganz oder im wesentlichen inhaltsgleich mit einer in die Liste aufgenommenen Schrift“ sind.
Hiermit soll „insbesondere verhindert [werden], daß in den Datennetzen Inhalte geringfügig verändert [werden] und durch die Möglichkeit der schnellen Veränderbarkeit aus dem Anwendungsbereich des Gesetzes herausfallen“ (Engel-Flechsig/Maennel/Tettenborn 1997, 2991).

„Ein Kernpunkt der vom Bund vorgeschlagenen Weiterentwicklung des Jugendschutzrechtes“ (Bundestags-Drucksache 13/7385, 38) ist der neue § 7a des GjS, in dem gewerbsmäßige elektronische Informations- und Kommunikationsdienste zur Bestellung eines Jugendschutzbeauftragten verpflichtet werden, wenn die Dienste allgemein angeboten werden und jugendgefährdende Inhalte enthalten können (Bundestags-Drucksache 13/7385, 38).
Der Jugendschutzbeauftragte hat den Auftrag, im Betrieb des Diensteanbieters flexibel und schnell auf das sich ändernde Informationsangebot zu reagieren. Er soll „als Ansprechpartner für die Nutzer und interner Berater der Diensteanbieter" (Bundestags-Drucksache 13/7385, 38) fungieren, wobei er „an der Angebotsplanung und bei der Gestaltung der allgemeinen Geschäftsbedingungen“ (Bundestags-Drucksache 13/7385, 38) zu beteiligen ist. Der Bund ermöglicht den Verzicht auf einen Jugendschutzbeauftragten, wenn der Diensteanbieter „eine Organisation der freiwilligen Selbstkontrolle zur Wahrnehmung der Aufgaben [...] verpflichtet“ (§ 7a GjS).

3.3.5.3 Jugendschutz im MDStV (§ 8 MDStV)

„Ein Kernstück des Staatsvertrags ist § 8, der Verbote für bestimmte Angebote und Bestimmungen zum Schutz der Jugend enthält. Den Ländern erschien es generell nicht ausreichend, den Jugendschutz auf die Anpassung des Gesetzes über die jugendgefährdenden Schriften (GjS) zu beschränken“ (Kuch 1997, 229 f).
Der Jugendschutz wird mittels eines abgestuften Regelungssystems für unzulässige Mediendienste und Jugendschutz durchgeführt (vgl. Müller 1997c, 29).
Die nach dem MDStV unzulässigen Angebote werden in § 8 Abs. 1 aufgeführt, dazu zählen Angebote,

- die nach § 130 StGB, § 131 StGB und nach § 184 StGB geregelt sind,
- die „den Krieg verherrlichen“,
- die „offensichtlich geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden“,
- die „Menschen, die sterben oder schweren körperlichen oder seelischen Leiden ausgesetzt sind oder waren“, darstellen.

Die Verbreitung dieser Angebote ist den Verteilerdiensten untersagt (§2 Abs. 2 Nr. 1 bis 3 MDStV), „es sei denn, der Anbieter trifft aufgrund der Sendezeit oder auf andere Weise Vorsorge“, daß jugendgefährdende Inhalte nicht Kindern oder Jugendlichen zugänglich gemacht werden können (§ 8 Abs. 2 MDStV). Ebenso ist den Abrufdiensten die Verbreitung verboten (§ 2 Abs. 2 Nr. 4 MDStV), es sei denn, daß „Vorkehrungen durch den Anbieter oder andere Anbieter bestehen, die dem Nutzer die Sperrung dieser Angebote ermöglichen“ (§ 8 Abs. 3 MDStV).
Diese abgestufte Regelung ermöglicht einen Ausgleich zwischen der Medienfreiheit der Erwachsenen und dem Interesse des Jugendschutzes, wie sie schon bei den Regulierungen des Fernsehens bestehen. Mit diesem rechtlichen Rahmen wird es Eltern und Pädagogen ermöglicht, ihre Verantwortung wahrzunehmen, indem sie den Zugang zu jugendgefährdenden Inhalten sperren (vgl. Müller 1997c, 30).

Analog zum IuKDG Artikel 6 Abs. 5 wird vom MDStV für gewerbsmäßige Mediendienste die Einstellung eines Jugendschutzbeauftragten gefordert.
In § 18 Abs. 1 MDStV wird die Überwachung des Jugendschutzes von einer „für den gesetzlichen Jugendschutz zuständigen Behörde“ gewährleistet. Bei Verstoß der Anbieter gegen die Bestimmungen des MDStV kann die Behörde die „Angebote untersagen und deren Sperrung anordnen“, aber nicht, „wenn die Maßnahmen außer Verhältnis zur Bedeutung des Angebots für den Anbieter und die Allgemeinheit“ stehen (§ 18 Abs. 2 MDStV). Eine vorsätzliche oder fahrlässige Ordnungswidrigkeit der Anbieter gegen die Jugendschutzbestimmungen (§ 20 Abs. 1 Nr. 2 MDStV), „kann mit einer Geldbuße bis zu fünfhunderttausend Deutsche Mark geahndet werden“ (§ 20 Abs. 2 MDStV).

3.3.6 Jugendschutzregelungen von IuKDG und MDStV im Vergleich

Mit der Schaffung des IuKDG und des MDStV verfolgten Bund und Bundesländer das Ziel, im Bereich der Online-Angebote für Rechtssicherheit zu sorgen. In der

Praxis kann die unterschiedliche Jugendschutzregelung für Individual- und Massenkommunikation zur Aushöhlung des Jugendschutzes führen (vgl. Müller 1997c, 30 ff).
Mittels Online-Diensten können Inhalte, die vorher in ihrer Verbreitung klaren Jugendschutzregelungen unterworfen waren, den ganzen Tag verfügbar sein. Dies trifft beispielsweise für Kino- und Videofilme zu, die nach dem Jugendschutz eine Alterskennzeichnung benötigen, um Kindern und Jugendlichen in der Öffentlichkeit zugänglich gemacht werden zu können (vgl. Müller 1997c, 30 ff). „Die überwiegende Anzahl der Text-, Ton- oder Bildangebote richten sich zwar an die Allgemeinheit, werden aber individuell abgerufen bzw. genutzt. Dies gilt beispielsweise für Filme, Spiele, Homepages, Teleshopping oder [...] Sexangebote. Die Anbieter jugendschutzrelevanter Produkte werden daher strengere Jugendschutzbestimmungen, wie der Mediendienste-Staatsvertrag sie vorsieht, eher zu vermeiden suchen und in die Nische der 'privaten' Kommunikation flüchten" (Müller 1997, 30).

Die Gewichtung des Jugendschutzes im MDStV und im geänderten GjS ist unterschiedlich.
Die Jugendschutzbestimmungen nach dem GjS haben einen repressiven Charakter. Eine Einhaltung der Bestimmungen durch eine Kontrollinstanz wird im Gegensatz zum MDStV (§ 18 Abs. 1 MDStV) nicht gewährleistet (vgl. Hönge 1997, 20 f). Weiter findet eine Indizierung nach dem GjS erst statt, wenn die Inhalte bereits verbreitet sind. Die Durchführbarkeit dieses Vorgehens bei den schnellebigen, rasch wechselnden, flüchtigen elektronischen Medien ist fraglich, zumal die Art der Verbreitungsbeschränkung nicht klar erkennbar ist (vgl. Kuch 1997, 229 f). Als problematisch ist auch anzusehen, daß der Zugang zu indizierten Seiten nach wie vor möglich ist (vgl. Müller 1997c, 27).
Der MDStV besitzt dagegen einen präventiven Charakter. Analog zu den Jugendschutzbestimmungen im Rundfunkstaatsvertrag werden die für den Jugendschutz erforderlichen unzulässigen Angebote verbindlich geregelt (vgl. Hönge 1997, 21).

Abschließend soll auf zwei Probleme aufmerksam gemacht werden, die sich durch den erweiterten Schriftenbegriff für die Bundesprüfstelle ergeben:
Der neugefaßte Schriftenbegriff im Strafgesetzbuch unterscheidet sich von dem im Gesetz über die Verbreitung jugendgefährdender Schriften. Im GjS unterliegt der Schriftenbegriff einer Einschränkung. Nicht erfaßt sind „Rundfunksendungen [...] sowie inhaltliche Angebote bei Verteilerdiensten und Abrufdiensten, soweit die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht" (§ 1 Abs. 3 GjS). Für die Bundesprüfstelle beginnt die Auseinandersetzung mit dem Merkmal der „publizistischen Relevanz". Während nach dem Strafgesetzbuch in allen Medien volksverhetzende Propaganda indiziert werden kann, ist für Internet-Angebote nach dem GjS zuerst zu überprüfen, ob die publizistische Relevanz im Vordergrund steht (vgl. Brockhorst-Reetz 1998, 4 f).

Es bestehen unterschiedliche Auffassungen, ob mit dem erweiterten Schriftenbegriff Internet-Angebote erfaßt werden. Die Rechtsprechung und die juristische Lehre

verlangt von dem Schriftenbegriff eine stoffliche Verkörperung von gewisser Dauer (vgl. Wassen 1998, 7).
Die eine Seite sieht mit dem Begriff „Datenspeicher“ die Inhalte der neuen Medien erfaßt (vgl. Brockhorst-Reetz 1998, 4). Internet-Angebote - besonders Grafiken - benötigen einen sehr großen Speicherplatz, wofür der Arbeitsspeicher eines Computers in der Regel nicht ausreicht. Sie befinden sich daher auf externen Datenspeichern (Festplatten, Streamerbänder, DAT sowie CD-ROMs), womit ein körperlicher Gegenstand vorhanden ist, um die Anforderung an den Schriftenbegriff zu erfüllen. Zusätzlich seien viele Daten auf den Datenspeichern der Service-Provider vorhanden, so daß ebenfalls eine stoffliche Verkörperung vorhanden sei (vgl. Beisel/Heinrich 1997, 360 ff).
Die Gegenargumentation sieht darin nur ein Hilfskonstrukt, denn ein großer Teil der Daten wird nur von Rechner zu Rechner übertragen, ohne daß die Daten auf dem Datenspeicher eines Service-Providers aufliegen. Internet-Angebote erscheinen nur flüchtig auf dem Bildschirm und nicht mit der geforderten stofflichen Verkörperung, wie sie durch Datenspeicher möglich sind. Weiter würde auch der Arbeitsspeicher nicht das Kriterium von stofflicher Verkörperung der Daten erfüllen, da beim Ausschalten alle Daten aus dem Arbeitsspeicher verschwinden und nach erneutem Start nicht mehr vorhanden sind (vgl. Wassen 1998, 7).

4 Anwendung und Kontrolle des Jugendschutzes im Internet

Die Anwendung und Kontrolle der gesetzlichen Bestimmungen werden durch unterschiedliche Einrichtungen und Gremien wahrgenommen. Diese werden nun vorgestellt.

4.1 Die Bundesprüfstelle für jugendgefährdende Schriften

Die Bundesprüfstelle für jugendgefährdende Schriften beginnt ihre Arbeit 1954 auf der Grundlage des am 14. Juli 1953 in Kraft getretenen Gesetzes über die Verbreitung jugendgefährdender Schriften (vgl. Schneider 1996, 177 ff). Im Rahmen des GjS obliegt es der BPSt, die Entscheidung zu treffen, ob ein Medium als jugendgefährdend einzustufen ist. Die Prüfung eines Mediums findet erst nach dem Erscheinen auf dem Markt statt. Die BPSt ist nur für die Indizierung zuständig, nicht aber für die Überwachung und Durchsetzung der Vertriebsbeschränkungen (vgl. Dittler 1997, 181 ff). Damit schließt der Gesetzgeber eine Zensur aus.
Ein Prüfungsverfahren wird nicht von der BPSt in Eigeninitiative angestoßen, sondern auf Antrag von den Obersten Jugendbehörden der Länder, den Jugendämtern, den Landesjugendämtern oder dem Bundesministerium für Jugend, Familie und Gesundheit. Der Antrag auf ein Prüfungsverfahren muß in schriftlicher Form mit Begründung, warum das Medium jugendgefährdend ist, erfolgen. In einem förmlichen Verfahren, in dem der Verleger und der Verfasser Stellung nehmen können, wird geprüft, ob eine Jugendgefährdung gemäß § 1 GjS vorliegt. Die in einem Verfahren gefallene Entscheidung kann nur auf dem Verwaltungsrechtsweg angefochten werden.

Die erste Indizierung von Internet-Seiten wird am 31.10.1997 im Bundesanzeiger Nr. 205 bekanntgegeben. Dabei handelt es sich um die Seiten des in Kanada lebenden Neonazis Ernst Zündel, die nach § 130 StGB (Volksverhetzung) indiziert werden. Dieser Indizierung folgen weitere mit pornographischen Inhalten.
Dem Gesetz nach unterliegen diese indizierten Seiten in der Bundesrepublik Deutschland einem Verbreitungsverbot. Daß das technisch unmöglich ist, zeigt das Beispiel der auf einem niederländischen Server befindlichen Internet-Seite der linksextremistischen Zeitschrift „Radikal". Mitte 1996 wurde die Bundesstaatsanwaltschaft auf den dort veröffentlichten „Kleinen Leitfaden zur Behinderung von Bahntransporten aller Art" aufmerksam. Die Bundesstaatsanwaltschaft verlangte von den deutschen Providern, den Zugang zu diesem Server zu sperren. Innerhalb kürzester Zeit wurde „Radikal" unter rund 50 verschiedenen Adressen auf mehrere Servern kopiert und war damit noch leichter zu finden als vorher. Während die Indizierung keine Wirkung auf das Verbreitungsverbot zeigte, weil die dafür notwendigen technischen Entwicklungen fehlen, führte sie zu einer ungeahnten Popularität der indizierten Seiten. In der Presse wurde die Indizierung bekanntgegeben und diskutiert. Es gab genügend Angaben zu den indizierten Seiten, so daß diese mittels einer Suchmaschine leicht auffindbar waren. Die Aufmerksamkeit, die diese Seiten durch den „Presserummel" um die Indizierung bekamen, stand im krassen Gegensatz zu dem Ziel, diese Seiten „aus dem Verkehr" zu ziehen (vgl. Dittler 1997, 181 ff).

Seit August 1997 hat die Bundesprüfstelle über 100 Indizierungsanträge von Internet-Angeboten bearbeitet, von denen zwei Drittel in die Liste der jugendgefährdenden Schriften aufgenommen worden sind. In der Praxis haben kaum Anbieter auf das elektronische Verbreitungsverbot reagiert (vgl. Brockhorst-Reetz1998, 5).

4.2 Die Freiwillige Selbstkontrolle der Multimedia-Diensteanbieter

Die „Freiwillige Selbstkontrolle der Multimedia-Diensteanbieter" (FSM) nimmt am 01.08.1997 mit dem in Kraft treten des IuKDG und des MDStV ihre Arbeit auf. Hintergrund der Gründung ist das geänderte Gesetz über die Verbreitung jugendgefährdender Schriften im IuKDG (Artikel 6 Nr. 5) und im § 8 Abs. 4 des MDStV. Beide fordern von gewerblichen Informations- und Kommunikationsdiensten einen Jugendschutzbeauftragten oder die Mitgliedschaft in einer Organisation der freiwilligen Selbstkontrolle. Mitglieder der FSM sind Verbände und Unternehmen der Multimediabranche.

Ziel der FSM ist es, den Jugendschutz in Online-Diensten soweit als irgend möglich zu gewährleisten und die Angebote von strafrechtlich verbotenen Inhalten freizuhalten (Rath-Glawatz/Müller-Using 1997, 53). Bewertungsmaßstab sind die im Verhaltenskodex der FSM niedergelegten Grundsätze zum Jugendschutz, journalistisch redaktionell gestalteten Inhalten sowie Anbieterkennzeichnung. Im Gegensatz zur Bundesprüfstelle für jugendgefährdende Schriften wird die FSM präventiv tätig, da die Mitglieder im Vorfeld versuchen, den Grundsätzen des Verhaltenskodex zu entsprechen (vgl. Rath-Glawatz/Müller-Using 1997, 53 ff).

Im Verhaltenskodex verpflichten sich die Mitglieder im Rahmen ihrer gesetzlichen Verantwortung, daß gesetzlich strafbare oder unzulässige Inhalte von ihnen nicht angeboten werden. Weiter verpflichten sich die Diensteanbieter, daß gesetzlich strafbare oder schädigende Inhalte nicht Kindern und Jugendlichen angeboten oder zur Nutzung vermittelt werden. Hierbei handelt es sich um die Inhalte, die Erwachsenen zugänglich bleiben dürfen. Hinzu kommen Inhalte, die das „körperliche, geistige oder seelische Wohl von Kindern oder Jugendlichen beeinträchtigen“ (vgl. Verhaltenskodex 1997, Ziffer 2 f).

Im Gegensatz zur Bundesprüfstelle für jugendgefährdende Schriften kann jeder bei der FSM Beschwerde über unzulässige oder jugendgefährdende Inhalte einlegen.
Danach erfolgt ein zweistufiges Verfahren. Zunächst findet eine Vorprüfung statt. Gehört die Beschwerde in den Zuständigkeitsbereich der FSM und ist sie begründet, wird sie dem betroffenen Mitglied zur Stellungnahme zugesandt. Nach der Stellungnahme wird vom Vorsitzenden der Beschwerdestelle alleine oder von einem Entscheidungsgremium über den Fall entschieden (vgl. Beschwerdeordnung 1997).
Abhängig von der Schwere des Verstoßes können folgende Sanktionen ausgesprochen werden: Hinweis mit Abhilfeaufforderung, Mißbilligung oder Rüge (Verhaltenskodex 1997, Ziffer 6a).
Während die ersten beiden Formen der Sanktionen unveröffentlicht bleiben, wird die Rüge im Tenor von der FSM publiziert und muß einen Monat lang im Dienst des Anbieters aufgeführt werden (vgl. Verhaltenskodex 1997, Ziffer 6b). Der Ausschluß aus der FSM erfolgt, wenn ein Mitglied trotz wiederholter Aufforderung einen Verstoß nicht beseitigt, beziehungsweise wenn es wiederholt die Sanktionen nicht befolgt (vgl. Verhaltenskodex 1997, Ziffer 6c). Ein Ausschluß aus der FSM sei insofern wirksam, da der Anbieter in der Öffentlichkeit „gebrandmarkt“ wird und die Akzeptanz für sein Angebot zurückgehen würde (vgl. Rath-Glawatz/Müller-Using 1997, 54). Dieser Einschätzung der Situation ist aus der Praxis der FSF (Freiwillige Selbstkontrolle Fernsehen) und dem Presserat entgegenzuhalten, daß die Sanktionen ohne Bußgeld nicht so gut greifen, da bei allen ethischen Erwägungen oft die ökonomischen Kriterien ausschlaggebend sind (vgl. FSM 1997, 17).

Der Verhaltenskodex der FSM stellt keine rechtliche Haftungsgrundlage dar. Nur Mitglieder sind verpflichtet, ihn einzuhalten. Bei berechtigten Beschwerden gegen Nichtmitglieder kann die FSM diese nur bitten, Abhilfe zu schaffen. Sanktionen können in diesem Fall nicht erfolgen. Noch schwieriger ist die Situation bei ausländischen Anbietern, denn diese unterliegen „nicht einmal“ dem deutschen Recht. In diesen Fällen kann die FSM die Beschwerden nur an andere europäische und internationale Selbstkontrolleinrichtungen weiterleiten. Aus diesen Gründen ist es der FSM nicht möglich, einen lückenlosen Jugendschutz im Internet zu gewährleisten (vgl. Rath-Glawatz/Müller-Using 1997, 54).

5 Jugendschutzrechtliche Anforderungen für den Internet-Zugang in Öffentlichen Bibliotheken

Die Bibliothek muß bei der Bereithaltung und Ausleihe von Medien einige Benutzungsbeschränkungen berücksichtigen. Diese ergeben sich, wie zuvor geschildert, aus der Einschränkung der Informationsfreiheit in § 5 Abs. 2 GG in Form von Vorschriften der allgemeinen Gesetze, des Jugendschutzes und der persönlichen Ehre. Werke, die diese Bereiche berühren, dürfen von der Bibliothek nicht verbreitet werden.

5.1 Benutzungsbeschränkungen

Zum einen unterliegt die Bibliothek den Benutzungsbeschränkungen aus strafrechtlichen Gründen. Zu berücksichtigen sind dabei schwerpunktmäßig die Tatbestände, die im Strafgesetzbuch als strafbare Verbreitung von Schriften genannt sind. Dabei handelt es sich um Schriften, die unter den Schriftenbegriff § 11 Abs. 3 StGB fallen und sich gegen die freiheitliche demokratische Grundordnung richten, die Taten befürworten, die den öffentlichen Frieden stören, Gewalttaten verherrlichen, ehrverletzende Tatsachen behaupten oder einen pornographischen Inhalt haben. Diese Schriften dürfen nicht verbreitet, ausgeliehen oder vorgeführt werden und sich nicht im Freihandbestand der Bibliothek befinden. Nur in begründeten Einzelfällen bei nachgewiesenem wissenschaftlichen Interesse und der schriftlichen Versicherung, daß diese Schriften niemanden sonst zugänglich gemacht werden, dürfen sie an einen Erwachsenen ausgeliehen werden (vgl. Kirchner 1981, 149 ff).

Zum anderen ergeben sich Benutzungseinschränkung aus den Bestimmungen zum Schutze der Jugend, die im Gesetz über die Verbreitung jugendgefährdender Schriften verankert sind. Mit dem GjS werden Kinder und Jugendliche unter 18 Jahren vor „unsittliche[n], verrohend wirkende[n], zu Gewalttätigkeiten, Verbrechen oder Rassenhaß anreizende[n] sowie den Krieg verherrlichende[n] Schriften“ (§ 1 GjS) geschützt. Voraussetzung für ein Verbreitungsverbot ist die Indizierung einer Schrift durch die Bundesprüfstelle für jugendgefährdende Schriften. Weiter unterliegen dem Verbreitungsverbot Schriften, die gemäß § 6 GjS eine „offensichtliche Jugendgefährdung“ beinhalten, so daß eine gesonderte Feststellung unterbleiben kann. Um zu verhindern, daß Kinder und Jugendliche unter 18 Jahren diese Schriften einsehen können, dürfen sich diese nicht im Freihandbestand der Bibliothek befinden. Sie dürfen im Katalog verzeichnet werden, es ist aber zu empfehlen, daß ein Hinweis auf die Benutzungsbeschränkung gegeben wird (vgl. Kirchner 1981, 149 ff).

5.2 Konsequenzen aus dem IuKDG

Einige Strafgesetze, die die Informationsfreiheit einschränken, setzen voraus, daß Informationen mit strafbarem Inhalt durch Schriften verbreitet werden. Um die Anwendbarkeit auf Teledienste und Mediendienste zu gewährleisten, wurde der bisherige Schriftenbegriff durch das IuKDG um den Begriff „Datenspeicher“ erweitert. Zu den bisher berücksichtigten Schriften, Ton- und Bildträger, Abbildungen und Darstellungen kommen damit „elektronische, elektromagnetische, optische, chemische

oder sonstige Datenspeicher“ (Bundestags-Drucksache 13/7385, 36) hinzu. Diese Erweiterung des Schriftenbegriffs erfaßt „sowohl Inhalte in Datenträgern (Magnetbänder, Festplatten, CD-ROMs u.a.) als auch in elektronischen Arbeitsspeichern“ (Bundestags-Drucksache 13/7385, 36). Der Straftatbestand der Verbreitung ist bereits mit der „Anzeige auf dem Bildschirm“ (Bundestags-Drucksache 13/7385, 36) erfüllt. Da bereits die Möglichkeit der Einsichtnahme in oder „auf“ jugendgefährdende Inhalte durch Kinder und Jugendliche unter 18 Jahren nicht statthaft ist, obliegt es der Bibliothek, Vorsorge zu treffen, daß keine jugendgefährdenden Inhalte aufgerufen werden können (vgl. Kirchner 1981, 156).

Das erweiterte Gesetz über die Verbreitung jugendgefährdender Schriften eröffnet dem „Anbieter indizierter Seiten“ (Bundestags-Drucksache 13/7385, 38), die Möglichkeit der Aufhebung des Verbreitungsverbotes. Dazu muß der Anbieter durch technische Vorkehrungen Vorsorge treffen, daß das Angebot auf volljährige Nutzer beschränkt bleibt (§ 3 Abs. 2 GjS).
Bezüglich der Rolle von Öffentlichen Bibliotheken kam es hierbei zu der Interpretation, daß sie „zukünftig allerdings gemäß den Vorgaben des GjS [...] geeignete Zugangssoftware installieren“ (Müller 1997a, 14) müssen.
Da in der Begründung zum IuKDG explizit der Anbieter indizierter Seiten genannt wird, entfällt diese Verpflichtung für Bibliotheken, da sie nicht Anbieter indizierter Seiten sind.
Die Bibliothek unterliegt eindeutig dem Verbreitungsverbot von jugendgefährdenden Schriften gemäß § 3 Abs. 1 Nr. 1-3 GjS. Wie die Kontrolle zu garantieren ist, ist nicht Gegenstand des Gesetzes.

Das IuKDG schreibt dem Diensteanbieter für die von ihm zur Nutzung bereitgehalten fremden Inhalte unter Berücksichtigung der Zumutbarkeit vor, daß technische Vorkehrungen vorzunehmen sind, wenn er Kenntnis über deren rechtswidrigen Inhalt besitzt (§ 5 Abs. 2 TDG).

Für fremde Inhalte, die der Diensteanbieter nicht zur Nutzung bereithält, sondern zu denen er lediglich einen Zugang vermittelt, ist er nicht verantwortlich (§ 5 Abs. 3 TDG). Hierzu werden ihm keine Vorschriften in Form von technischen Vorkehrungen auferlegt.
Da eine Öffentliche Bibliothek nur in Ausnahmefällen bei Betrieb eines eigenen Servers fremde Inhalte zur Nutzung bereithalten kann, wird sie als Diensteanbieter allenfalls durch § 5 Abs. 3 TDG berührt. Dies würde bedeuten, daß sie nicht zu der Gruppe der Diensteanbieter gehört, die zu technischen Vorkehrungen verpflichtet werden.

Neu dem Gesetz über die Verbreitung jugendgefährdender Schriften hinzugekommen ist der § 7a GjS, der für gewerbsmäßige elektronische Informations- und Kommunikationsdienste einen Jugendschutzbeauftragten vorschreibt.
In Frage zu stellen ist die Schlußfolgerung, nach der Bibliotheken „zukünftig allerdings gemäß den Vorgaben des GjS einen Jugendschutzbeauftragten benennen“

(Müller 1997a, 14) müssen. Der gleiche Verfasser kam in zwei anderen Aufsätzen allerdings auch zu einem anderen Schluß (vgl. Müller/Berger 1997, 1783 und Müller 1997b, 49 ff): „Nach bisherigem Verständnis betätigen sich die von öffentlichen Unterhaltsträgern finanzierten Bibliotheken nicht gewerbsmäßig. Deshalb kann vorläufig davon ausgegangen werden, daß öffentlich zugängliche Bibliotheken mit Internet-Arbeitsplätzen keinen (!) Jugendschutzbeauftragten bestellen müssen“ (Müller/Berger 1997, 1783).
Da Bibliotheken nicht als gewerbsmäßiger elektronischer Informations- und Kommunikationsdienst anzusehen sind, müssen sie keinen Jugendschutzbeauftragten benennen.

Da gemäß dem GjS § 21 Abs. 3 bereits die bloße fahrlässige Verbreitung von jugendgefährdenden Schriften strafbar ist, ist zur Vermeidung eines Fahrlässigkeitsvorwurfs eine Sorgfaltspflicht einzuhalten (vgl. Sieber 1997a, 288). Der Bibliothek genügte bislang die Kenntnis der Liste der jugendgefährdenden Schriften, die sie gezielt am Katalog zu überprüfen hat (vgl. Kirchner 1993, 62). Es wird zukünftig von den Gerichten noch zu klären sein, ob bei der Bereitstellung von öffentlich zugänglichen Internet-Plätzen die alleinige Kenntnis der Liste der jugendgefährdenden Schriften genügt oder ob weitere Aktivitäten erforderlich sind, um die Sorgfaltspflicht zu erfüllen.

Festzuhalten ist zum einen, daß eine Öffentliche Bibliothek keinen Jugendschutzbeauftragten bestellen muß. Zum anderen schreibt ihr der Gesetzgeber nicht vor, daß sie Filtersoftware installieren muß.

5.3 Empfehlungen

Da die schädigenden und illegalen Inhalte das Internet immer wieder in die Diskussion bringen, ist es für die Bibliotheken wichtig, daß sie das Thema im voraus regeln. Sie müssen dieses Thema aktiv angehen und zeigen, daß sie sich der Gefahren und der Problematik bewußt sind und Lösungen anbieten. Sie müssen im Vorfeld aufklären und reagieren, bevor sie mit Anschuldigungen und Kritik seitens der Politik, der Presse oder der Kunden konfrontiert werden.

Die zuvor vorgestellten Gesetzestexte regeln nicht, wie eine Bibliothek den Internet-Zugang gestalten kann, um den Anforderungen des Jugendschutzes zu entsprechen. Dazu werden im folgenden Möglichkeiten aufgezeigt, die sich der Bibliothek bieten.

Zunächst ist ratsam, daß die Benutzungsordnung Regelungen zur Internet-Nutzung enthält. Neben den üblichen Nutzungsmodalitäten (Dauer der Nutzung, mögliche Kosten, Reservierung, ...) ist klarzustellen, daß der Aufruf von jugendgefährdenden und illegalen Inhalten untersagt ist und auch „zufällig“ aufgerufene Seiten sofort verlassen werden müssen. Ebenso sollte sie die Reaktion auf einen Verstoß enthalten, beispielsweise den zeitweiligen oder vollständigen Ausschluß von der Internet-Nutzung (vgl. N0ßke 1997).

Zusätzlich sollte die Internet-Nutzung für Kinder und Jugendliche unter 18 Jahren geregelt werden. Im Rahmen der in Kapitel 7 dargestellten Umfrage fand sich ein Praxisbeispiel, in dem der Internet-Zugang für Kinder und Jugendliche in einem abgestuften System geregelt wird: Kinder unter 14 Jahren dürfen nur in Begleitung eines Erziehungsberechtigten und ab 14 Jahren nur mit Filtersoftware den Internet-Zugang nutzen. Ab 18 Jahren kann die Filtersoftware deaktiviert werden.
Bei Minderjährigen ist zu empfehlen, daß eine Einverständniserklärung der Erziehungsberechtigten vorliegt. Diese sollten genau über die möglichen „Gefahren" der Internet-Nutzung aufgeklärt werden. Dies kann mittels einer Informationsbroschüre erfolgen.

Neben der formalen Gestaltung in der Benutzungsordnung bietet sich die Möglichkeit der „sozialen Kontrolle", indem der Internet-Zugang nicht „versteckt", sondern zentral aufgestellt wird, so daß er von dem Personal und den Kunden eingesehen werden kann. Internet-Cafés verstärken diese „soziale Kontrolle", indem sie einen zweiten Bildschirm unter der Decke anbringen, so daß er deutlich einzusehen ist. Bei dieser Form ist zu beachten, daß dies bei einigen Themen zu einer Hemmschwelle bei den Kunden führen kann, wenn diese sich zu einem Thema wie beispielsweise AIDS oder Homosexualität informieren möchten.

Um Kindern und Jugendlichen einen sicheren Schutz zu bieten, kann die Bibliothek in Erwägung ziehen, dieser Gruppe nur unter Aufsicht den Internet-Zugang zu gewähren. Als Aufsichtspersonen kommen Erziehungsberechtigte, das Bibliothekspersonal oder geeignete andere Erwachsene in Frage.

Denkbar ist auch ein speziell für Kinder und Jugendliche gestaltetes Internet-Angebot, das nur Zugriff auf ausgewählte Inhalte ermöglicht. Spezielle Angebote für diese Gruppe gibt es bereits im Internet (Fun-Online, Computermaus). Technisch kann die Bibliothek dies mit separaten Zugängen umsetzen, die mit Filtersoftware ausgestattet sind und lediglich einen sorgsam selektierten Zugriff gewähren.

Die zuvor genannte Filtersoftware ist eine technische Möglichkeit zur Regulierung des Zugriffs auf Inhalte des Internets. Filtersoftware ist in amerikanischen Bibliotheken eine sehr umstrittene Methode der Regulierung. Während das Thema „Filtern oder nicht" viel Raum in der Diskussion des amerikanischen bibliothekarischen Alltags einnimmt, gibt es von deutschen Bibliotheken oder ihren Interessenvertretungen nahezu keine Untersuchungen oder Statements zum Einsatz von Filtersoftware.

6 Zugriffskontrolle durch Filtersoftware

Mit der Diskussion um schädigende und illegale Inhalte im Internet entstand die Forderung nach einer Regulierung des Internet-Zugangs für Minderjährige. Zu diesem Zweck entwickeln amerikanische Softwarefirmen seit 1995 Filtersysteme, mit denen es Eltern möglich ist, den Netzzugang an ihrem PC für ihre Kinder zu filtern und zu kontrollieren (vgl. Illegal 1996, 21). Filtersoftware ist eine Anwendung, die den Zugriff

auf bestimmte Informationen oder Dienste des Internets nach vorgegebenen Kriterien reguliert (vgl. Kossel 1996, 121). Die Hersteller versprechen, daß bei Einsatz von Filtersoftware nur noch jugendfreies Material den heimischen PC erreicht (vgl. Schmidt 1997, 224). Filtersoftware schränkt den freien Zugang der Kinder ins Netz deutlich ein, bietet aber entgegen den Aussagen der Hersteller keinen ausreichenden Schutz, so daß die Eltern nicht von ihrer Aufsichtspflicht entbunden werden (vgl. Kossel 1996, 121).

Neben den Filtermechanismen der jeweiligen Programme nutzen einige Produkte Klassifikationen von Rating-Systemen. Hierbei bewerten Organisationen oder Personen eine Web-Seite und klassifizieren sie, indem sie sie mit einem Label versehen. Einige Filterprogramme können diese Label nutzen, um den Zugang zu diesen Seiten zu regulieren.

Mit dem Einsatz von Filtersoftware und der Nutzung von Rating-Systemen wird die Verantwortung auf den Endverbraucher verlagert, der selber entscheiden muß, welche Inhalte auf dem heimischen Bildschirm erscheinen sollen (vgl. Illegal 1996, 21).
Erwägt eine Bibliothek den Einsatz von Filtersoftware, muß sie sich darüber klar sein, daß diese für Eltern zum Schutz ihrer Kinder entwickelt wurde und nicht für die spezifischen Anforderungen einer Bibliothek, deren Hauptaufgabe die Informationsvermittlung ist. Hinzu kommt, daß derzeit nur amerikanische Filtersoftware mit amerikanischen Wertvorstellungen erhältlich ist.
Der Einsatz von Filtersoftware - von Kritikern auch als „Zensur-Filter“ oder „Censorware“ bezeichnet - bringt den Vorwurf der Zensur mit sich. Einige amerikanische Bibliotheken werden bereits wegen des Einsatzes von Filtersoftware mit der Begründung verklagt, daß dies das Recht auf freie Meinungsäußerung der Erwachsenen behindere. Des weiteren würde sie nicht nur den Zugriff auf Seiten mit eindeutig sexuellen Inhalten, sondern auch den Zugriff auf legitime Angebote verhindern (vgl. Koehn 1998, 146). Bibliotheken sollten sich davon jedoch nicht verunsichern lassen. Zu den Hauptaufgaben des Bibliothekars zählt es, täglich zu selektieren, welche Materialien aus dem gesamten Medienangebot die Bibliothek anbietet. Im Rahmen der Literaturauswahl wird der Bibliothek bislang keine Zensur vorgeworfen und es wird vermutlich von den Kunden als selbstverständlich angesehen, daß keine jugendgefährdenden Inhalte in der Bibliothek vorhanden sind. Die Bibliothek sollte bei dem Vorwurf der Zensur darauf aufmerksam machen, daß sie einen informations- und bildungspolitischen Auftrag hat. Wenn sie bislang keine Playboyhefte angeboten hat, warum sollte es beim Online-Angebot anders sein?

6.1 The Internet Filter Assessment Project (TIFAP)

The Internet Filter Assessment Project - kurz als TIFAP bezeichnet - ist ein Zusammenschluß von 40 amerikanischen Bibliotheken, die von April bis September 1997 Filtersoftware getestet haben. Das Projekt entstand aus den Fragen und Problemen heraus, die durch den Einsatz von Filtersoftware in amerikanischen Bibliotheken entstanden. Geleitet wurde das Projekt von Karen G. Schneider, die die Ergebnisse

von TIFAP in dem Buch „A practical guide to internet filters“ zusammengefaßt hat. Die Kommunikation der Tester verlief überwiegend per E-Mail oder über das WWW. Ziel war es, Testberichte zu erstellen, in denen die spezifischen bibliothekarischen Erfordernisse berücksichtigt werden. Man wollte herausfinden, unter welcher Konfiguration eine Filtersoftware die besten Rechercheergebnisse liefert und trotzdem einen akzeptablen Schutz bietet. Grundlage waren Fragen, die teilweise direkt aus dem bibliothekarischen Informationsdienst entnommen wurden, andere wurden speziell für das Projekt entwickelt. Zusätzlich wurde eine Liste mit URLs getestet, die zu beanstandendes Material enthielten.

6.2 Arbeitsweisen und Merkmale von Filtersoftware

Die Filtersoftware untersucht die empfangenen Datenpakete anhand vorgegebener Stoppwörter, aufgeführten zu sperrenden URLs in Negativlisten oder nach Labels. Filtersoftware kann noch keine Bilder erkennen, so daß jugendgefährdendes Bildmaterial übertragen werden kann, wenn es nicht von einem eindeutig als jugendgefährdend zu identifizierenden Text begleitet wird (vgl. Illegal 1996, 25).

Filter- und Schutzsysteme lassen sich an drei Schnittstellen einsetzen (vgl. Grünbuch 1996, 58 f):

- Bei dem Anbieter von Inhalten:

Er kann auf einer Deckseite vor jugendgefährdenden Inhalten warnen und eine Alterskontrolle (schriftliche Beantragung oder Zahlung mit Kreditkarte) durchführen.

- Bei dem Provider:

Von dem Provider kann kein System zur systematischen Kontrolle der Inhalte verlangt werden. Er sollte aber veranlaßt werden können, den Zugang zu ihm bekannten jugendgefährdenden Inhalten zu sperren oder auf Erwachsene einzuschränken.

- Bei dem Nutzer:

Er kann Filtersoftware einsetzen.

Im folgenden wird nur auf die Filtersoftware eingegangen, die vom Nutzer am PC installiert wird. Sie bietet verschiedene Möglichkeiten, um den Zugang zu regulieren.

6.2.1 Stoppwortlisten

(vgl. Schneider 1997, 3 ff)

Die ersten Prototypen der Filtersoftware arbeiteten ausschließlich mit vordefinierten Stoppwortlisten. Die Stoppwörter zielen überwiegend auf das Thema Sexualität und entstammen der Umgangssprache, der vulgären Sprache und der Fachsprache. Ein Nachteil dieser Technik liegt darin, daß nicht berücksichtigt wird, daß ein Wort mehrere Bedeutungen haben kann und der Filter nicht immer den Kontext erkennt, in dem ein zu „beanstandendes“ Wort steht. Dies führt dazu, daß auch medizinische Informationen, Gedichte und Kinderreime mit gesperrt werden können. Diese Filter führen zu einer erheblichen Einschränkung in der Informationssuche. TIFAP hat in seiner Untersuchung festgestellt, daß ein Drittel der vorher festgelegten Suchfragen

mit eingeschalteter Stoppwort-Funktion nicht zu beantworten waren. Die Trefferquote erhöhte sich mit ausgeschalteter Stoppwort-Funktion auf bis zu 90 %. TIFAP empfiehlt daher den Bibliotheken, nicht mit der Stoppwort-Funktion zu arbeiten.
Trotz der Nachteile werden Stoppwortlisten weiter von den Herstellern angeboten, da die im folgenden behandelten Positiv- und Negativlisten im Erstellen kosten- und zeitaufwendiger sind.

6.2.2 Negativ- und Positivlisten

(vgl. Schneider 1997, 6 ff)
Wird die Stoppwort-Funktion nicht genutzt, sind sehr umfassende Negativ- oder Positivlisten erforderlich, um das Aufrufen von anstößigem Material zu verhindern. Zunächst werden Web-Seiten von Personen überprüft und klassifiziert. Diese Seiten werden entweder in Negativ- oder in Positivlisten eingetragen.

Negativlisten, oft auch Schwarze Listen genannt, beinhalten die Internet-Adressen der Web-Seiten, zu denen der Zugriff unterbunden werden soll. In der Regel werden die zu filternden Seiten in Kategorien unterteilt, so daß der Anwender wählen kann, welches Material er nicht aufrufen möchte. Einige Kategorien sperren dabei auch Web-Seiten mit Materialien, die tägliche Kundenfragen in der Bibliothek beantworten (z.B. AIDS, Abtreibung, ...). Bei diesen Web-Seiten handelt es sich um Materialien, die es in Bibliotheken als Printmedium ohnehin gibt. Es muß Klarheit bestehen, welches Material sich in welcher Kategorie befindet. Abhängig vom Filter kann der Begriff „Homosexualität“ beispielsweise in den Kategorien „Sexuality/Lifestyles“, „Lifestyle“, „Adult“ oder in mehreren Kategorien gleichzeitig eingeordnet sein.

Neben den Negativlisten gibt es Positivlisten. Diese beinhalten Internet-Adressen, die als unbedenklich bewertet werden. Einige Filterprogramme können wahlweise den Zugang zu allen anderen Web-Seiten unterbinden. Dieses Verfahren ist sehr einschränkend für den Internet-Zugang und derzeit gibt es kein kommerzielles Filterprogramm, das ausschließlich mit einer Positivliste arbeitet.

Bei Anwendungen von Negativ- und Positivlisten ist es wichtig zu wissen, welche Philosophie hinter dem Produkt steht. Die Kriterien, nach denen Web-Seiten gesperrt oder als unbedenklich eingestuft werden, sollten für den Nutzer ersichtlich sein.
In der Regel gewähren die Hersteller aus geschäftspolitischen Gründen keine Einsicht in die Negativlisten. Der Nutzer hat keine Möglichkeit festzustellen, wie umfangreich die Liste ist, ob die Einordnung der Web-Seiten in die einzelnen Kategorien inhaltlich konstant und nachvollziehbar ist oder ob vielleicht mehr gesperrt wird als gewünscht. Es ist wichtig, daß umfangreiche benutzereigene Positiv- und Negativlisten genutzt werden können, in denen der Anwender selber Web-Seiten sperrt oder freigibt und damit die Einstellungen der Positiv- und Negativlisten des Herstellers überschreiben kann.

Einige Filterprogramme sperren nur auf der Ebene der Top-Level-Domains (http://www.foodbirds.com). Sie erlauben damit keinen weiteren Zugang zu Unterverzeichnissen (http://www.foodbirds.com/birds/happy.com), die gegebenenfalls kein jugendgefährdendes Material enthalten.

Um Informationen zu versenden, benutzt das Internet-Protokoll Adressen, die aus 4 Zahlengruppen bestehen (http://148.129.129.31). Da diese Zahlengruppen schwer zu merken sind, wurde das Domain-Namen-System entwickelt. Anstelle der numerischen IP-Adresse tritt eine aus verständlichen Buchstaben und Wörtern bestehende Internet-Adresse (http://www.census.gov). Es ist wichtig, daß der Filter beide Adressen sperrt. Jeder, der ein wenig mit den technischen Grundlagen vertraut ist, weiß, daß er auch mit der erstgenannten numerischen Adresse den Host anwählen kann, wo das anstößige Material zu finden ist.

6.2.3 Weitere Aspekte

(vgl. Schneider 1997, 9 ff)

Abhängig von dem Produkt bietet Filtersoftware dem Nutzer noch verschiedene zusätzliche Funktionen, mit denen der Zugang reguliert werden kann:

- Regulierung verschiedener Dienste

Eine Option besteht darin, die Nutzung verschiedener Dienste zu sperren. Eine Bibliothek kann zum Beispiel den Zugang zum Internet Relay Chat einschränken oder das Versenden von E-Mails unterbinden.

- Zeitliche Regulierung

Eine weitere Möglichkeit bietet sich durch die zeitliche Regulierung. Dem Nutzer der Filtersoftware ist es möglich, den Internet-Zugang zu bestimmten Zeiten zu sperren.

- Unterschiedliche Benutzerprofile

Bei Bedarf können für verschiedene Benutzer unterschiedliche Zugangsmöglichkeiten definiert werden. Eltern können Kindern unterschiedlicher Altersgruppen individuelle „Internet-Freiheiten“ zugestehen. Die Bibliotheken können dies nutzen, um unterschiedliche Benutzerprofile für die verschiedenen Benutzergruppen zu definieren (beispielsweise um für Kinder unter 12 Jahren den Internet Relay Chat zu sperren).

Die verschiedenen Optionen können oftmals miteinander kombiniert werden, um beispielsweise zu Stoßzeiten das Chatten zu unterbinden.

Bibliotheken stellen weitere Anforderungen an Filtersoftware. Sie benötigen ein abgestuftes System der Verantwortlichkeiten, um zu verhindern, daß jeder Mitarbeiter in die Systemverwaltung eingreifen und beispielsweise die Negativlisten verändern kann. Es muß jedoch gewährleistet sein, daß jeder Informationsbibliothekar kurzfristig eine Sperre aufheben kann.

Von Bedeutung für eine Bibliothek ist auch, daß der Kunde klare Informationen bekommt, warum ihm der Zugriff auf eine Seite untersagt wird. Teilweise erscheint keinerlei Auskunft und die Übertragung bricht ab. In anderen Fällen werden nur unklare Meldungen gegeben, wie „Cyber Patrol Code 2“ oder „Blocked by

Surfwatch“. Manche Programme bieten die Möglichkeit, diese Meldungen zu bearbeiten.

6.3 Platform for Internet Content Selection (PICS)

PICS ist ein System, das Web-Seiten mit neutralen Labeln versieht. Mehrere Filterprodukte und der Microsoft Internet Explorer können den PICS Standard nutzen. Diese neutralen Label können vom Autor ins Dokument eingebaut werden. Zum anderen können auch unabhängige Organisationen oder Bewertungsbüros beliebige Seiten klassifizieren, ein Label zuordnen und in einer Liste die klassifizierten Seiten mit den zugeordneten Labeln aufführen. Bei Aufruf einer URL kann dann das Label entweder direkt dem Dokument oder aus der Liste des Bewertungsbüros entnommen werden. Je nach Filterkonfiguration werden Seiten gesperrt, deren Label auf schädigende Inhalte hinweisen oder aber im Extremfall werden alle Seiten gesperrt, die nicht über ein Label „freigegeben“ sind. Im letzen Fall führt das dazu, daß alle Seiten ohne Label gesperrt werden (vgl. PICS, Stand: 10.04.1998).

PICS verfolgt mit diesem Ansatz das Ziel, einer Zensur im Internet vorzubeugen. Man plädiert für die Selbstkontrolle und favorisiert standardisierte Bewertungssysteme ähnlich wie bei Video- und Computerspielen. PICS sieht vor, daß jeder freiwillig seine Seiten mit einem Label versieht, das den Inhalt der Seite kennzeichnet. PICS bietet lediglich den technischen Standard - die Entwicklung von Bewertungssystemen und die Bewertung wird von anderen Stellen vorgenommen. Der einzelne Nutzer muß sich ein Bewertungssystem aussuchen, das seinen moralischen Vorstellungen entspricht, um sich oder seine Kinder somit vor Gewalt, Pornographie und Neonazismus schützen.
Es gibt derzeit zwei bekannte Bewertungssysteme, Recreational Software Advisory Council (RSAC) und Safesurf, die auf Basis von PICS arbeiten (vgl. Post 1996, 66 ff).
RSAC wurde 1995 für die Bewertung von Video- und Computerspielen gegründet und hat ein Bewertungskonzept für Internetinhalte entwickelt (RSACi). RSAC arbeitet mit Unterstützung von Firmen wie Disney, Compuserve und Microsoft (vgl. Gröndahl 1997, 62). Safesurf ist eine Elterninitiative aus den USA.
Beide Bewertungssysteme wurden vom Microsoft Internet Explorer übernommen, jedoch noch nicht vom Netscape Navigator (vgl. Post 1996, 66 ff). Ebenso wie bei der Filtersoftware ist es wichtig zu wissen, welche moralischen, ethischen und politischen Ziele die kennzeichnende Stelle verfolgt.

Dem Ziel, alle Angebote des Internets mit Labeln zu versehen, steht die Größe und Dynamik des Internets entgegen. Kein Bewertungsbüro kann ausreichend Personal zur Verfügung stellen, um das Internet mit Labeln zu versehen (vgl. Kossel 1996, 121). 1996 gab es ungefähr 30 Millionen Web-Seiten, von denen RSAC und
Safesurf weniger als 200.000 gelabelt hatten. Das sind weniger als 0,7 % des Internets (vgl. Venditto 1996, 50). Für deutschsprachige Angebote sind beide Systeme derzeit noch unbrauchbar, da bislang kaum deutsche Web-Seiten gelabelt sind (vgl. Gröndahl 1997, 62).

PICS erhält starke Unterstützung seitens der US-Regierung (vgl. Gröndahl 1997, 62) und auch von der Europäischen Gemeinschaft, die PICS als die umfassendste und innovativste Lösung zur Regulierung des Zugangs zu anstößigen Inhalten ansieht (vgl. Illegal 1996, 22).

Befürworter sehen mit der Nutzung von PICS die Möglichkeit verwirklicht, durch den Einsatz unterschiedlicher Bewertungssysteme die verschiedenen moralischen, politischen und religiösen Auffassungen berücksichtigen zu können (vgl. Gröndahl 1997, 62). Einen weiteren Vorteil sehen die Betreiber von PICS darin, daß das Internet mittels der vergebenen Label „klassifiziert“ werden kann. PICS stellt den freiwilligen Labelern in Aussicht, daß demnächst auch Anwendungen entwickelt werden könnten, die Label nicht filtern, sondern Label suchen (vgl. PICS, Stand: 10.04.1998). Aber auch hier ist es fraglich, ob angesichts der Vielzahl von Web-Seiten vollständig und sinnvoll klassifiziert werden kann.
Kritiker sehen bereits durch die Existenz von PICS einen sanften Zwang, sich dem Bewertungssystem anzuschließen. Sie behaupten, Angebote ohne Label könnten über Bewertungsbüros nicht mehr angesprochen werden und würden so aufhören, zu existieren (vgl. Gröndahl 1997, 62). Zudem geht von den Anbietern der Bewertungssysteme die Gefahr einer zu großen Marktmacht aus. Sie könnten irgendwann die Forderung stellen, ihre Bewertungsdienste den Anbietern von Web-Seiten in Rechnung zu stellen (vgl. Kossel 1996, 121).

6.4 Betrachtung von zwei Filterprogrammen

Nach Vorstellung von Arbeitsweisen und Merkmalen von Filterprogrammen werden zwei Produkte vorgestellt. Mit Cyber Patrol wird ein Vertreter betrachtet, der überwiegend empfohlen wird. Das zweite Produkt, Cybersitter, erhielt unterschiedliche Kritiken und eignet sich trotz einiger guter Testberichte aufgrund seiner sehr restriktiven Filtermethoden nicht für den Einsatz in Bibliotheken.

6.4.1 Cyber Patrol

Cyber Patrol wird in vielen Testberichten favorisiert. In einer Umfrage (siehe Kapitel 7: Umfrageergebnisse) zeigte sich, daß Cyber Patrol die am häufigsten eingesetzte Filtersoftware in den befragten Bibliotheken ist. Auch TIFAP empfiehlt Cyber Patrol für den Einsatz in Bibliotheken.

Cyber Patrol bietet vielfältige Möglichkeiten, den Zugang zum Internet zu regulieren. Die komplexe Installation und die aufwendige Konfiguration, die für einen durchschnittlichen Nutzer nur schwer zu handhaben ist, wurden bemängelt.
Um eine auf die individuellen Bedürfnisse zugeschnittene Filterfunktion zu erreichen, muß man sich sehr intensiv mit der Konfiguration auseinandersetzen.

Cyber Patrol unterstützt die Verwaltung von bis zu neun unterschiedlichen Benutzerprofilen. Der Zugang zum Administrationsmenü ist kennwortgeschützt. Die Sper-

rung eines als anstößig bewerteten Inhaltes kann kurzfristig aufgehoben werden. Dazu ist die Eingabe eines entsprechenden Kennwortes notwendig (vgl. Schneider 1997, 146 ff).

Neben einer zeitlichen Zugangsregelung bietet Cyber Patrol die Sperrung verschiedener Dienste. Die Filtersoftware arbeitet mit einer auszuschaltenden Stoppwortliste und einer Negativliste (CyberNot-Liste). Erstellt wird die Negativliste von einem aus amerikanischen Eltern und Lehrern bestehenden Team (vgl. Munro 1997, xyz). Die zu sperrenden Inhalte werden in zwölf Kategorien unterteilt (zum Beispiel: Violence/Profanity, Full Nudity, Sexual Acts/Text, Drugs/Drug Culture, Militante/Extremist, Sex Education). Der Nutzer kann wählen, welche Kategorien er filtern möchte. Neben der von Cyber Patrol erstellten Negativliste, besteht die Möglichkeit zur Erstellung einer lokalen CyberNot- und CyberYes-Liste (vgl. Schmidt 1997, 225 f). Hierbei können maximal 64 in der CyberNot-Liste geführte URLs freigegeben und bis zu 64 zusätzliche URLs gesperrt werden.

Eine weitere Schutzmöglichkeit bietet Cyber Patrol mit PICS und der Unterstützung der beiden Rating-Systeme Safesurf und RSAC an.
TIFAP testete Cyber Patrol mit unterschiedlichen Konfigurationen und kam zu dem Ergebnis, daß der Filter lediglich bei einer minimalen Konfiguration ohne Stoppwort-Funktion ein gutes Verhalten zeigte. Nicht zu beanstandende Seiten wurden dann in bis zu 10% der Fälle gesperrt. Pornographisches Material blieb in 10% der Fälle zugänglich. Einschränkend muß gesagt werden, daß TIFAP gemäß amerikanischen Moralvorstellungen vorrangig mit Blick auf sexuelle und pornographische Inhalte testete und weniger hinsichtlich Gewalt oder Nationalsozialismus (vgl. Schneider 1997, 146 ff). Cyber Patrol beanstandete auch mit allen aktivierten Filtern nicht die Seiten der Neonazis (vgl. Schmidt 1997, 226).
Dieser Fall zeigt, daß für die deutschen Bibliotheken ein deutlicher „Nachbesserungsbedarf“ besteht. Allerdings stehen nur 64 URLs zum Eintrag in die lokale CyberNot-Liste zur Verfügung, in der auch die von der Bundesprüfstelle für jugendgefährdende Schriften indizierten URLs aufgenommen werden müssen.

Zu bemängeln ist bei Cyber Patrol die Meldung, die bei Sperrung einer aufgerufenen Web-Seite erscheint. Der Nutzer bekommt nur eine wenig aussagekräftige Meldung (zum Beispiel „Cyber Patrol Code 2“), die nicht verändert werden kann.

6.4.2 Cybersitter

Mit Cybersitter wird eine Filtersoftware vorgestellt, die in verschiedenen Testberichten stark voneinander abweichende Beurteilungen erhielt. Trotz einiger guter Beurteilungen eignet sie sich nicht zum Einsatz in Bibliotheken.

In den Zeitschriften Internet World (vgl. Venditto 1996, 49-58) und dem PC-Magazin (vgl. Cyber Patrol 1997) wird Cybersitter als eine effektive Lösung bezeichnet, mit der Internetinhalte und Online-Aktivitäten gut zu kontrollieren sind. In der Zeitschrift c’t (vgl. Schmidt 1997, 224 ff) ist Cybersitter der einzige Filter, der nicht mit einfa-

chen Tricks zu umgehen ist, dessen restriktive Filtermethoden aber nicht wünschenswert sind.

Die Installation und Konfiguration von Cybersitter ist einfach und übersichtlich. Cybersitter bietet die Möglichkeit, verschiedene Dienste zu regulieren. Die gesamten Online-Aktivitäten können überwacht und protokolliert werden. Cybersitter ermöglicht dem Nutzer, die Negativliste durch weitere URLs zu ergänzen (vgl. Cybersitter 1998). Es ist aber nicht möglich, über eine Positivliste gesperrte Web-Seiten zugänglich zu machen.
Während Cyber Patrol sich während seiner Filteraktivität mit einem Icon dem Nutzer bemerkbar macht, läuft Cybersitter unsichtbar im Hintergrund mit und greift sogar in diverse Windows-Applikationen ein (vgl. Schneider 1997, 115).

Gefiltert wird mittels einer Negativliste und einer Stoppwortliste, die nicht auszuschalten ist. Cybersitter verspricht seinen Kunden auf der Homepage, daß Stoppwörter in ihrem Kontext betrachtet und auch Doppeldeutigkeiten erkannt werden (vgl. Cybersitter 1998). In verschiedenen Testberichten kam man zu gegensätzlichen Ergebnissen. Cybersitter sperrte nicht nur „breast“, sondern auch Kochrezepte zu „chicken breast“ (vgl. Schneider 1997, 114). Da Cybersitter nicht nur das Wort unterdrückt, sondern auch die Zeichenfolge, wird beispielsweise neben dem Wort „sex“ auch die englische Grafschaft „Sussex“ gesperrt (vgl. Schmidt 1997, 232). Auch Wörter wie „fascist“ und „fascim“ werden ausgefiltert, unabhängig davon, ob es um Nazipropaganda oder geschichtliche Aufklärung geht (vgl. Möller 1998, 15). Cybersitter sperrt zwar die Seiten des in Kanada lebenden Neonazis Ernst Zündel, ermöglicht aber den Zugriff auf Adolf-Hitler-Seiten (vgl. Schmidt 1997, 232).
Während Cybersitter beim Filtern von Wörter sehr „effektiv“ arbeitet, ist die Filterfunktion leicht zu umgehen, wenn man die gesperrte URL mit ihrer numerischen IP-Adresse ein-gibt (vgl. Schneider 1997, 114).

Cybersitter filtert nur auf Ebene der Top-Level-Domains und unterdrückt gegebenenfalls somit auch den Zugang zu den gesamten Unterverzeichnissen (vgl. Möller 1998, 15).

Es wurde festgestellt, daß Cybersitter mehr als nur anstößige Inhalte unterdrückt. Es werden unter anderem Informationen über Verhütung, Abtreibung und Minderheiten gesperrt. Dies mag daran liegen, daß hinter Cybersitter die konservative Organisation „Focus on the Family“ steht, die familienorientierte traditionelle Werte vertritt (vgl. Möller 1998, 15).
Bemerkenswert ist, daß auch Web-Seiten unterdrückt werden, die Cybersitter oder das Filtern im Internet kritisieren (vgl. Schneider 1997, 114). In einem deutschen Testbericht wird Cybersitter als ein Filterprogramm mit „Filterwahn“ beschrieben, das „ohne Rücksicht auf Stabilität und Informationsfreiheit alles kappt, was auch nur verdächtig aussieht“ (Schmidt 1997, 232).

6.5 Vor- und Nachteile des Einsatzes von Filtersoftware

Ein Vorteil der Filtersoftware ist, daß die unterschiedlichen Normen an Moral und Anstand eines Landes ebenso wie die individuellen Vorstellungen der Endverbraucher berücksichtigt werden können. Bei dem Zusammenfluß der unterschiedlichen Kulturen im Internet wird nie ein gemeinsamer gültiger Standard gefunden werden können, was ins Internet darf und was nicht (vgl. Illegal 1996, 21).

Der entscheidende Nachteil der Filtersoftware ist in der „Unerschöpflichkeit" des Internets zu sehen. Es ist unmöglich, das gesamte Internet nach fragwürdigen Inhalten abzusuchen. Die Ersteller der Negativlisten arbeiten in der Regel auch nur mit Suchmaschinen, die ihnen helfen, das Internet nach fragwürdigen Inhalten zu durchsuchen (vgl. Schneider 1997, 7). Dabei ist es leicht möglich, daß immer wieder Seiten durchschlüpfen und somit ist es kaum möglich, die jugendgefährdenden Inhalte lückenlos zu erfassen.

Für deutsche Anwender ist zu beachten, daß mit der Filtersoftware amerikanische Wertvorstellungen transportiert werden. Der Schwerpunkt der Regulierung liegt bei pornographischen Seiten, weniger bei Inhalten zu Themen wie Gewalt und Nationalsozialismus. Ebenso arbeiten die Stoppwortlisten hauptsächlich mit amerikanischen Wörtern, so daß deutsche Suchwörter durchkommen können. Es gibt noch keine deutschen Versionen (vgl. Schmidt 1997, 225).

Ebenso verhält es sich mit Rating-Systemen. Die beiden gängigen Rating-Systeme kommen aus Amerika und spiegeln somit die amerikanischen Wertvorstellungen wieder. Es gibt kaum deutsche gelabelte Seiten. Auch die Kommission der Europäischen Gemeinschaften macht auf diesen Mißstand aufmerksam. Da die amerikanischen Wertvorstellungen nicht vorbehaltlos übernommen werden können, ist es für die Anwendung des PICS-Standards erforderlich, in Europa eigene Rating-Systeme zu entwickeln (vgl. Illegal 1996, 26). Für eine deutsche Bibliothek ist der Einsatz von Rating-Systemen noch nicht zu empfehlen, da zum einen noch kein europäisches oder deutsches Rating-System vorliegt. Zum anderen waren 1996 von 30 Millionen Web-Seiten weniger als 200.000 gelabelt. In diesem Anteil von 0,7 % sind kaum deutschsprachige Seiten enthalten.

7 Umfrageergebnisse

Im Rahmen der Diplomarbeit wurde eine Umfrage vorgenommen (Anlage 9), in der 40 Bibliotheken einen Fragebogen per E-Mail erhielten. In einem zweiten Schritt wurde der Fragebogen in den Mailing-Listen Inetbib und Forumoeb veröffentlicht. Ziel war es festzustellen, wie Bibliotheken den Internet-Zugang für Kinder und Jugendliche gestalten.
27 Bibliotheken haben geantwortet. Darüber gab es Interesse an den Umfrageergebnissen.

Eine erste Einschränkung wird durch das Alter vorgegeben. 6 Bibliotheken gewähren ohne Altersbeschränkung einen Zugang. Am häufigsten ist Jugendlichen erst ab 14 Jahren ein Zugang zum Internet erlaubt.

16 Bibliotheken fordern für den Internet-Zugang bei Minderjährigen eine Einverständniserklärung der Erziehungsberechtigten. In einigen Fällen werden die Erziehungsberechtigten über die Gefahr des Aufrufs jugendgefährdender Inhalte informiert. Es wird ihnen auch mitgeteilt, daß Filtersoftware nur einen bedingten Schutz darstellt und immer wieder jugendgefährdende Inhalte durchschlüpfen können.
In einigen Bibliotheken dürfen Kinder und Jugendliche unter 18 Jahren nur unter Aufsicht des Personals surfen.

Alle Bibliotheken haben ihren Internet-Zugang zentral oder einsehbar für Personal oder Kunden aufgestellt und setzen dadurch auf die soziale Kontrolle.

11 Bibliotheken setzen bereits Filtersoftware ein, 7 davon als Reaktion auf das IuKDG. Eine Bibliothek erhöhte deshalb die Altersgrenze auf 18 Jahren.
Eine Bibliothek gab an, daß der einzige Grund für die Installation der Filtersoftware ist, daß sie vom Gesetz gefordert sei. Sie steht dem Einsatz der zur Zeit erhältlichen Filtersoftware generell negativ gegenüber, da es kein Produkt gibt, daß das leistet, was sie benötigt.

Überwiegend (in 9 von 11 Fällen) wird Cyber Patrol genutzt - meist aufgrund von Empfehlungen anderer Bibliotheken.

7 von 11 Bibliotheken beklagen Einschränkungen; eine Bibliothek konnte keine Erfahrung sammeln, da die Filtersoftware erst seit einer Woche installiert war.

Nur 2 von 11 Bibliotheken, die Filtersoftware einsetzen, hatten keine Probleme mit der Installation. Bei weiteren 2 Bibliotheken scheiterte der geplante Einsatz der Filtersoftware an technischen Problemen.

Es zeigte sich, daß trotz des Einsatzes von Filtersoftware immer wieder jugendgefährdendes Material aufgerufen werden konnte und die Filterfunktion leicht zu umgehen ist.

Bei Verstößen gegen die Auflagen der Bibliothek (Aufruf jugendgefährdender Inhalte) steht anfangs meistens nur eine mündliche Verwarnung, danach kommt es zu einem zeitweisen bis dauerhaften Ausschluß von der Internet-Nutzung. 7 Bibliotheken haben für diesen Fall keine Reaktionen vorgesehen oder machten dazu keine Angabe.

In der Regel findet eine Kombination aus sozialer Kontrolle, Einverständniserklärung der Eltern und Filtersoftware oder „begleitetes“ Surfen statt.

8 Schlußbetrachtung

Die durch das Informations- und Kommunikationsdienste-Gesetz (IuKDG) eingeführten rechtlichen Rahmenbedingungen zum Sachverhalt Multimedia regeln nicht explizit, wie Bibliotheken ihr Angebot der Internet-Nutzung zu gestalten haben, um den Jugendschutz zu gewährleisten.

Nach dem neuen Teledienstegesetz (TDG) ist die Bibliothek für den Inhalt ihrer eigenen Homepage verantwortlich (§ 5 Abs. 1 TDG). Des weiteren steht eine Öffentliche Bibliothek mit eigenem Server in der Verantwortung, wenn sie beispielsweise ihren Kunden erlaubt, auf diesem Homepages oder andere Angebote zu hinterlegen. Sie wäre verpflichtet, den Zugang zu rechtswidrigen Inhalten zu sperren, wenn sie davon Kenntnis erhielte und die Sperrung keinen unzumutbaren Aufwand darstellen würde (§ 5 Abs. 2 TDG).
Ob Bibliotheken Zugangsvermittler im Sinne von § 5 Abs. 3 TDG ist, ist noch zu klären. Für die Bibliotheken ergeben sich daraus aber keine weiteren Konsequenzen, da den Zugangsvermittler für fremde rechtswidrige Inhalte keine Verantwortung trifft.

Die durch das IuKDG erfolgten Änderungen des GjS „Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalten“ führt bei Öffentlichen Bibliotheken zu keinen Veränderungen. Durch die durchgeführte Erweiterung des Schriftenbegriffs um „Datenspeicher“ unterliegen nun auch jugendgefährdende Internet-Angebote einem Verbreitungsverbot.

Die Bibliothek ist nach wie vor gemäß § 3 Abs. 1 bis 3 GjS zum Jugendschutz verpflichtet. Die Interpretation des neu gefaßten GjS, daß Bibliotheken nun gemäß § 3 Abs. 4 GjS verpflichtet sind, technische Vorkehrungen zu treffen, trifft nicht zu. Ebenso besteht für Bibliotheken keine Verpflichtung, einen Jugendschutzbeauftragten gemäß § 7a GjS zu benennen.
Vor Einführung eines Internet-Angebotes müssen Bibliotheken sich Gedanken machen, wie sie bei diesem Medium den Anforderungen des Jugendschutzes gerecht werden können. Sie sollten dieses Thema aktiv und präventiv angehen, um nicht von einem Rechtfertigungsdruck überrascht zu werden, der im Rahmen der Diskussion um illegale und schädigende Inhalte des Internets entstehen kann. Dazu sollten in der Benutzungsordnung Regelungen zur Internet-Nutzung aufgenommen werden.
Eine Verpflichtungserklärung, keine rechtswidrigen Inhalte aufzurufen, ist sinnvoll. Minderjährige sollten nur mit einer schriftlichen Einverständniserklärung der Erziehungsberechtigten Zugang zum Internet erhalten.
Ein weiteres Instrument ist die soziale Kontrolle durch gut einsehbare Internet-Plätze.

Es wird deutlich, daß die Bibliothek auf das Verantwortungsbewußtsein jedes einzelnen Kunden angewiesen ist, um Kinder und Jugendliche vor schädigenden Einflüssen des Internets zu schützen.

Eine weitere Möglichkeit bietet der Einsatz von Filtersoftware, mit der der Zugriff auf das Internet reguliert werden kann. Bei der Auswahl von Filtersoftware und der Nut-

zung von Rating-Systemen ist zu beachten, daß der überwiegende Teil amerikanischen Ursprung ist und nicht in allen Punkten den hiesigen Wertvorstellungen entspricht. Solange es keine Alternativen zur Regulierung des Internets gibt und Bibliotheken die Beaufsichtigung von Kindern und Jugendlichen nicht gewährleisten können, sollten sie Filtersoftware ernsthaft in Erwägung ziehen. Bislang fehlt in deutschen Bibliotheken eine koordinierte Betrachtung dieser Möglichkeit. Derzeit ist jede Bibliothek weitestgehend auf sich selbst gestellt. Aktivitäten analog zum amerikanischen Projekt TIFAP sind sinnvoll und wünschenswert - die deutschen Bibliotheken sind aufgefordert, es ihren amerikanischen Kollegen gleich zu tun.

9 Anhang

Text des Fragebogens

Der Fragebogen wurde im Januar 1998 erstellt. Ausgehend vom derzeitigen Kenntnisstand wurde angenommen, daß die Installation von Filtersoftware zwingend vom IuKDG vorgeschrieben wird. Als Ergebnis dieser Diplomarbeit wurde jedoch festgestellt, daß sich der zwingende Einsatz von Filtersoftware aus dem IuKDG nicht ableiten läßt.

Fragebogen zum Thema „Internet und Jugendschutz in Oeffentlichen Bibliotheken" im Rahmen einer Diplomarbeit von Susanne Kloetzer an der FH Koeln, Fachbereich Bibliotheks- und Informationswesen.

Bei einigen Fragen sind mehrere Antwortmoeglichkeiten gegeben.
Bitte markieren Sie (z.B. mit vorangestelltem „X") zutreffende Aussagen.

In einigen Faellen wird auch zu Freitextantworten aufgefordert; hier stehen dann drei Punkte „...".

Frage 1)
Seit wann bietet die Bibliothek einen Internet-Zugang fuer Nutzer an?
Antwort (Datum):

Frage 2)
Ab welchem Alter erhalten die Nutzer den Internet-Zugang?
Antwort (Alter):

Frage 3)
Wie hoch ist die Anzahl der Internetzugaenge/-Plaetze fuer Nutzer?
Antwort (Anzahl):

Frage 4)
Wo befinden sich die Nutzer-Zugaenge?
Antwortmoeglichkeiten:
-im Sichtfeld des Personals
-zentral an einer Stelle, oder
-verteilt in der Bibliothek
-abgetrennt/separat, nicht fuer Personal einsehbar, oder
-offen/einsehbar fuer das Personal

Frage 5)
Gibt es fuer den Internet-Zugang bei Kindern und Jugendlichen Besonderheiten?
Antwortmoeglichkeiten:
-diese Zugaenge werden vom Personal beaufsichtigt
-Einverstaendniserklaerung der Erziehungsberechtigten muss vorliegen
-die Zugaenge sind raeumlich getrennt von den anderen (z.B. in KiBue)
-die Zugaenge haben einen technisch anderen Zugang, und zwar: ...
-andere Besonderheiten, und zwar: ...

Frage 6)
Welche Reaktionen sind beim Abruf jugendgefaehrdender Inhalte durch Kinder und Jugendliche von der Bibliothek vorgesehen?
Antwortmoeglichkeiten:
-keine
-voruebergehender Ausschluss vom Internetzugang
-dauerhafter Auschluss vom Internetzugang
-sonstige Reaktionen, und zwar: ...

Am 1. August 1997 trat das Informations- und Kommunikationsdienstgesetz (IuKDG) in Kraft. Darin werden unter anderem technische Vorkehrungen zum Jugendschutz verlangt, wenn der Ort fuer Kinder oder Jugendliche zugaenglich ist oder von ihnen eingesehen werden kann, ausgestellt, angeschlagen, vorgefuehrt oder sonst zugaenglich gemacht wird.
Dies fuehrte auch verstaerkt zu einer Diskussion des Themas Jugendschutz und Internet in Bibliotheken.

Frage 7)
Hat das IuKDG bei Ihnen zu Aenderungen beim Internet-Zugang gefuehrt?
Antwortmoeglichkeiten:
-die Altersgrenze fuer die Benutzung wurde angehoben, und zwar auf:...
-es wurde Filtersoftware installiert
-es gab andere Veraenderungen, und zwar: ...

Frage 8)
Werden vom Nutzer abgefragte Adressen protokolliert und ueberprueft?
Antwort (ja/nein):

Frage 9)
Wird Filtersoftware eingesetzt?

Antwort (ja/nein):

Falls Sie Filtersoftware einsetzen, bitte Fragen 9.1 - 9.7 beantworten;
sonst bitte weiter mit Frage 10.

Frage 9.1)
Welche Filtersoftware setzen Sie ein?
Antwort (Produkt[e]):

Frage 9.2)
Welche Auswahlkriterien waren ausschlaggebend?
Antwort (Kriterien):

Frage 9.3)
Wodurch erhalten Sie bei Softwareproblemen Unterstuetzung/Hilfe?
Antwortmoeglichkeiten:
-aus dem Handbuch/den Unterlagen zur Software
-vom Hersteller
-aus Fachzeitschriften, und zwar (Titel): ...
-Online-/Internet, und zwar (Adresse/Website): ...
-anderweitige Unterstuetzung, und zwar: ...
-keine Unterstuetzung, reine Eigeniniative
-es gibt keine Probleme mit der Software

Frage 9.4)
Welche Konsequenzen ergaben sich aus dem Einsatz von Filtersoftware?
Antwortmoeglichkeiten:
-erhoehter Administrationsaufwand
-(negative) Kritik von Benutzern
-sonstige Auswirkungen, und zwar: ...

Frage 9.5)
Wurden durch den Einsatz der Filtersoftware Einschraenkungen bei
der Recherche bekannt?
-nein, keine Einschraenkungen bekannt geworden
-ja, Recherchen wurden eingeschraenkt, und zwar bei: ...

Frage 9.6)
Sind trotz Filtersoftware Abrufe jugendgefaehrdender Inhalte bekannt
geworden?
Antwort (ja/nein):

Frage 9.7)
Wie beurteilen Sie die eingesetzte Filtersoftware?
Antwortmoeglichkeiten:
-geringer Aufwand fuer Verwaltung und Bedienung
-vertretbarer Aufwand fuer Verwaltung und Bedienung
-zu hoher Aufwand fuer Verwaltung und Bedienung
-gute Filterfunktion/Zuverlaessigkeit
-akzeptable Filterfunktion/Zuverlaessigkeit
-mit Filterfunktion/Zuverlaessigkeit nicht zufrieden

Frage 10)
Sind Sie mit einer Veroeffentlichung der Ergebnisse einverstanden?
Antwort (ja/nein):

Weitere Anmerkungen: ...

Fuer Rueckfragen bitte noch:

- Anschrift
- Telefon
- Email
- Ansprechpartner

nennen. Herzlichen Dank!

Literaturverzeichnis

(Beisel/Heinrich 1997)
Beisel, Daniel; Heinrich, Bernd: Die Zulässigkeit der Indizierung von Internet-Angeboten und ihre strafrechtliche Bedeutung.
In: Computer und Recht, 13 (1997), Heft 6, S. 360-363.

(Bericht 1997)
Bericht über die Mitteilung der Kommission über illegale und schädigende Inhalte im Internet. - Luxemburg : Amt für Veröffentlichungen der Europäischen Gemeinschaften, 1997. - ISBN 92-78-19964-8. - 20. März 1997, PE DOK A4-0098/97
URL: http://www.europarl.eu.int/dg1/a4/de/a4-97/a4-0098.htm

(Beschwerdeordnung 1997)
Beschwerdeordnung des Vereins „Freiwillige Selbstkontrolle Multimedia-Diensteanbieter". - Köln, 09.07.1997.

(Bonin/Köster 1997)
Bonin, Andreas v. ; Köster, Oliver: Internet im Lichte neuer Gesetze.
In: Zeitschrift für Urheber- und Medienrecht, 41 (1997), Heft 11, S. 821-829.

(Brockhorst-Reetz 1998)
Brockhorst-Reetz, Bettina: Internet.
In: BPjS-Aktuell : Bundesprüfstelle für jugendgefährdende Schriften, Amtliches Mitteilungs-blatt, 1998, Heft 1, S. 3-6.

(Chancen 1996)
Chancen durch Multimedia / Hrsg: Presse- und Informationsamt der Bundesregierung. - Bonn : Presse- und Informationsamt der Bundesregierung, 1996.

(Collardin 1995)
Collardin, Marcus: Straftaten im Internet - Fragen zum internationalen Strafrecht.
In: Computer und Recht, 11 (1995), Heft 10, S. 618-622.

(Cyber Patrol 1997)
Cyber Patrol 3.1, Cybersitter 2.1 : Editors' Choice.
In: PC-Magazin, April 1997 (USA),
URL: http://www.zdnet.com/pcmag/features/utility/ufuec.html [Stand: 24.02.1998].

(Cybersitter 1998)
Cybersitter Product Information, [1998].
URL: http://www.solidaoak.com/cybersitter.html [Stand: 10.04.1998].

(Dittler 1997)

Dittler, Ullrich: Computerspiele und Jugendschutz. - Baden-Baden : Nomos Verlagsgesell-schaft, 1997. - ISBN 3-7890-4778-3.

(Engel 1996)
Engel, Christoph: Inhaltskontrolle im Internet.
In: Archiv für Presserecht, 27 (1996), Heft 3, S. 220-227.

(Engel-Flechsig 1997)
Engel-Flechsig, Stefan: Das Informations- und Kommunikationsdienstegesetz des Bundes und der Mediendienstestaatsvertrag der Bundesländer.
In: Zeitschrift zum Urheber- und Medienrecht, 41 (1997), Heft 4, S. 231-239.

(Engel-Flechsig/Maennel/Tettenborn 1997)
Engel-Flechsig, Stefan ; Maennel, Frithjof A. ; Tettenborn, Alexander: Das neue Informa-tions- und Kommunikationsdienstegesetz.
In: Neue juristische Wochenschrift, 1997, Heft 45, S. 2981-3000.

(FSM 1997)
Freiwillige Selbstkontrolle für Multimedia-Anbieter.
In: Funkkorrespondenz, 1997, Heft 35, S. 17.

(Bundestags-Drucksache 13/7385)
Gesetzentwurf der Bundesregierung : Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG). - Bundestags-Drucksache 13/7385
URL: http://dip.bundestag.de/cgi-bin/dipwww_nofr?a=druckform&b=894209768-16720&c=/usr7/goldop

(Gounalakis 1997)
Gounalakis, Georgios: Der Mediendienste-Staatsvertrag der Länder.
In: Neue juristische Wochenschrift, 1997, Heft 45, S. 2993-3000.

(Gralla 1997)
Gralla, Preston: So funktioniert das Internet. - 4. Aufl. - München : Markt und Technik, 1997. - ISBN 3-8272-5209-1.

(Gröndahl 1997)
Gröndahl, Boris: Alles unter Selbstkontrolle.
In: Die Zeit, vom 22. August 1997, S. 62.

(Grünbuch 1996)
Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in den audio-visuellen und den Informationsdiensten / Kommission der Europäischen Ge-

meinschaften. - Luxemburg : Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften, 1996. - ISBN 92-78-10178-8. - KOM (96) 483 endg.
URL: http://www.iid.de/informationen/gpde/

(Hilse 1997)
Hilse, Jürgen: Auf der Datenautobahn mit Vollgas in die Sackgasse?
In: Jugendschutz und Internet / hrsg. von der Bundesarbeitsgemeinschaft Kinder- und Jugendschutz e.V. - Bonn : Bundesarbeitsgemeinschaft Kinder- und Jugendschutz e.V., 1997, S. 1-10.

(Hönge 1997)
Hönge, Folker: Jugendschutz und Mediendienste.
In: Jugendschutz und Internet / hrsg. von der Bundesarbeitsgemeinschaft Kinder- und Jugendschutz e.V. - Bonn : Bundesarbeitsgemeinschaft Kinder- und Jugendschutz e.V., 1997, S. 20-23.

(Illegal 1996)
Illegale und schädigende Inhalte im Internet : Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschaft- und Sozialausschuss und den Ausschuss der Regionen / Kommission der Europäischen Gemeinschaften. - Luxemburg : Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften, 1996. - ISBN 92-78-10299-7. - KOM (96) 487 engd
URL: http://www2.echo.lu/legal/de/internet/content/communic.html

(Jugendmedienschutz 1995)
Jugendmedienschutz / Arbeitsgemeinschaft Kinder- und Jugendschutz Landesstelle Nord-rhein-Westfalen e.V. ... - 3. überarb. Aufl. - Essen : Drei-W-Verl., 1995. - ISBN 3-928168-15-0.

(Kirchner 1981)
Kirchner, Hildebert: Bibliotheks- und Dokumentationsrecht. - Wiesbaden : Reichert, 1981. - ISBN 3-88226-112-9.

(Kirchner 1993)
Kirchner, Hildebert: Grundriß des Bibliotheks- und Dokumentationsrechts. - 2. durchges. Aufl. - Frankfurt am Main : Klostermann, 1993. - ISBN 3-465-02602-0.

(Klau 1995)
Klau, Peter: Das Internet. - 1. Aufl. - Bonn [u.a] : IWT-Verl., 1995. - ISBN 3-8266-2600-1.
(Koehn 1998)
Koehn, Michael: Jugendgefährdend.
In: Buch und Bibliothek, 50 (1998), Heft 3, S. 146.

(Kossel 1996)

Kossel, Axel: Kindersicherung.
In: c't, 1996, Heft 9, S. 120-121.

(Kuch 1997)
Kuch, Hansjörg: Der Staatsvertrag über Mediendienste.
In: Zeitschrift für Urheber- und Medienrecht, 41 (1997), Heft 4, S. 225-230.

(Lahrmann 1997)
Lahrmann, Markus: Unter Verdacht: Internet.
In: Jugendschutz und Internet / hrsg. von der Bundesarbeitsgemeinschaft Kinder- und Jugendschutz e.V.. - Bonn : Bundesarbeitsgemeinschaft Kinder- und Jugendschutz e.V., 1997, S. 20-23.

(Möller 1998)
Möller, Erik: Die heilige Familie der Inquisition.
In: Die Tageszeitung, vom 12 März 1998, S. 15.

(Müller a 1997)
Müller, Harald: Die rechtlichen Aspekte des Internet für Bibliotheken.
In: Internet / hrsg. von der Redaktion Buch und Bibliothek. - Bad Honnef : Bock und Herchen, 1997, - (BUB special). - ISBN 3-88347-196-8, S. 11-14.

(Müller b 1997)
Müller, Harald: Was bedeutet Internet im rechtlichen Sinne für Öffentliche Bibliotheken.
In: Internet in öffentlichen Bibliotheken. - Berlin : Dt. Bibliotheksinst., 1997. - (Dbi-Materialien, 163). - ISBN 3-87068-963-3, S. 44-51.

(Müller/Berger 1997)
Müller, Harald ; Berger, Gabriele: Informations- und Kommunikationsdienste-Gesetz.
In: Bibliotheksdienst, 31 (1997), Heft 9, S. 1781-1786.

(Müller c 1997)
Müller, Petra: Mulitmedia ohne Grenzen?
In: Jugendschutz und Internet / hrsg. von der Bundesarbeitsgemeinschaft Kinder- und Jugendschutz e.V. - Bonn : Bundesarbeitsgemeinschaft Kinder- und Jugendschutz e.V., 1997, S. 24-32.

(Müller-Using/Lücke 1997)
Müller-Using, Detlev ; Lücke, Richard: Neues Recht für Multimedia-Dienste.
In: BPjS-Aktuell : Bundesprüfstelle für jugendgefährdende Schriften, Amtliches Mitteilungs-blatt, 1997, Heft 3, S. 7-17.

(Munro 1997)
Munro, Kathryn: Cyber Patrol.

In: PC-Magazin, April 1997 (USA),
URL: http://www.zdnet.com/pcmag/features/utility/filter/ufu1.html [Stand: 4.02.1998].

(Noßke 1997)
Noßke, Thomas: Einrichtung eines Internet-PC in öffentlichen Bibliotheken in Sachsen-Anhalt : Fragenkatalog zur Vorbereitung des Internet-Arbeitsplatzes ; Fragen zu Ihrer Benutzungsodnung
URL: http://www.fh-merseburg.de/~wwwbib/oebib/Katalog.html#F06 [Stand: August 1997]

(PICS 1998)
Platform for Internet Content Selection, [1998].
URL: http://www.w3.org/PICS/ [Stand: 10.04.1998].

(Post 1996)
Post, Hilde-Josephine: Sauberfiltern.
In: c't, 1996, Heft 8, S. 66-69.

(Rath-Glawatz/Müller-Using 1997)
Rath-Glawatz, Michael ; Müller-Using, Detlev: Freiwillige Selbstkontrolle Multimedia-Dienste-anbieter e.V. (FSM).
In: JugendMedienSchutz-Report, 1997, Heft 5, S. 53-55.

(Rath-Glawatz/Waldenberger 1997)
Rath-Glawatz, Michael ; Waldenberger, Arthur: Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V.
In: Computer und Recht, 13 (1997), Heft 12, S. 766-769.

(Schmidt 1997)
Schmidt, Jürgen: Kindersicheres Netz?
In: c't, 1997, Heft 15, S. 224-232.

(Schneider 1997)
Schneider, Karen: A practical guide to internet filters. - New York : Neal-Schuman, 1997. - ISBN 1-55570-332-4.

(Schneider 1996)
Schneider, Wilfried: Geschichte und Arbeitsweise der Bundesprüfstelle für jugendgefährdende Schriften.
In: Medien und Gewalt / Bundesministerium des Inneren. - Bonn : Bundesministerium des Inneren, 1996, S. 177-184.

(Scholz 1992)
Scholz, Rainer: Jugendschutz. - 2. Aufl. - München : Beck, 1992. - ISBN 3-406-35947-7.

(Scholz 1996)
Scholz, Rainer: Kein Jugendschutz im Internet?
In: AJS-Forum, 1996, Heft 3, S. 8-9.

(Sieber a 1996)
Sieber, Ulrich: Cyberlaw: Die Entwicklung im deutschen Recht.
In: Cheswick, William R.: Firewalls und Sicherheit im Internet. - Bonn [u.a.] : Addison-Wesley, 1996. - ISBN 3-89319-875-X, S. 285-324.

(Sieber b 1996)
Sieber, Ulrich: Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I).
In: Computer und Recht, 13 (1997), Heft 10, S. 581-598.
URL: http://www.jura.uni-wuerzburg.de/lst/sieber/; dann Publikationen

(Sieber c 1996)
Sieber, Ulrich: Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen (1).
In: Juristenzeitung, 51 (1996), Heft 9, S. 429-480.
URL: http://www.jura.uni-wuerzburg.de/lst/sieber/; dann Publikationen

(Venditto 1996)
Venditto, Gus: Safe Computing.
In: Internet World, 1996, September, S. 49-58.

(Verhaltenskodex 1997)
Verhaltenskodex des Vereins: „Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V.“ . - Köln, 09.07.1997.

(Wassen 1998)
Wassen, Hans-Josef: Verfolgung von Straftaten in Datennetzen.
In: BPjS-Aktuell : Bundesprüfstelle für jugendgefährdende Schriften, Amtliches Mitteilungsblatt, 1998, Heft 1, S. 6-14.

Abkürzungsverzeichnis

AfP	Archiv für Presserecht
AOL	American Online
BPSt	Bundesprüfstelle für jugendgefährdende Schriften
Btx	Bildschirmtext
ca.	circa
CR	Computer und Recht
d.h.	das heißt
E-Mail	Electronic-Mail

EU	Europäische Union
GjS	Gesetz über die Verbreitung jugendgefährdender Schriften, ab dem 01.08.1997 Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte
IP	Internet Protocol
IRC	Internet Relay Chat
i.S.	im Sinne
IuKDG	Informations- und Kommunikationsdienste-Gesetz
JMS-Report	Jugendmedienschutz-Report
JZ	Juristenzeitung
MDStV	Mediendienste-Staatsvertrag
NJW	Neue Juristische Wochenschrift
PICS	Platform for Internet Content Selection
RSAC	Recreational Software Advisory Council
s.	siehe
StGB	Strafgesetzbuch
TCP	Transmission Control Protocol
TDG	Teledienstegesetz
TIFAP	The Internet Filter Assessment Project
u.a.	und andere
URL	Uniform Resource Locator
u.s.w.	und so weiter
WWW	World Wide Web
z.B.	zum Beispiel
ZUM	Zeitschrift für Urheber- und Medienrecht