Jugendschutz
und
Filtertechnologien im Internet

Eine Untersuchung der Secorvo Security Consulting GmbH
im Auftrag des
Projektträgers Multimedia des BMWi

Zielsetzung der Untersuchung

Ziel der vorliegenden Studie ist eine aktuelle Bestandsaufnahme der heute verfügbaren technischen Lösungen zur Umsetzung von Maßnahmen des Jugendschutzes beim Zugriff auf das Internet, deren Untersuchung und Bewertung hinsichtlich ihrer Eignung zur Umsetzung von Anforderungen des Jugendschutzes sowie die Entwicklung von Visionen und Anforderungen an ein geeignetes System zur technischen Unterstützung des Jugendschutzes. Als Randbedingungen sind dabei die technische und organisatorische Machbarkeit, der rechtliche Rahmen und die psychologisch-soziale Durchsetzbarkeit zu berücksichtigen.

BMWi Bundesministerium für Wirtschaft und Technologie

Bonn, Dezember 1999

Jugendschutz
und
Filtertechnologien im Internet

Eine Untersuchung der Secorvo Security Consulting GmbH
im Auftrag des
Projektträgers Multimedia des BMWi

Zielsetzung der Untersuchung

Ziel der vorliegenden Studie ist eine aktuelle Bestandsaufnahme der heute verfügbaren technischen Lösungen zur Umsetzung von Maßnahmen des Jugendschutzes beim Zugriff auf das Internet, deren Untersuchung und Bewertung hinsichtlich ihrer Eignung zur Umsetzung von Anforderungen des Jugendschutzes sowie die Entwicklung von Visionen und Anforderungen an ein geeignetes System zur technischen Unterstützung des Jugendschutzes. Als Randbedingungen sind dabei die technische und organisatorische Machbarkeit, der rechtliche Rahmen und die psychologisch-soziale Durchsetzbarkeit zu berücksichtigen.

Bonn, Dezember 1999

Die inhaltlichen Arbeiten wurden
im August 1999 abgeschlossen.

Jugendschutz
und
Filtertechnologien im Internet

– Kurzzusammenfassung –

- Der freie Zugang zum Internet birgt die Möglichkeit, daß Jugendliche auf pornographische, gewaltverherrlichende und volksverhetzende Inhalte zugreifen können. Dies stellt den Jugendschutz vor neue Herausforderungen. Auf dem Weg in die Informationsgesellschaft unterliegen die gesellschaftlichen Werte und Normen einem Wandlungsprozeß. Auf Jugendliche gerichtete Orientierungshilfen müssen diesem Prozeß Rechnung tragen.
- Die Förderung von Medienkompetenz bei Jugendlichen hat herausragende Bedeutung. Medienkompetenz meint hier sowohl die technische Beherrschung der Medien als auch einen qualifizierten, eigenverantwortlichen Umgang mit den Inhalten. Die Vermittlung von Medienkompetenz liegt dabei im Spannungsfeld zwischen Jugendschutz und Informationsfreiheit.
- Das IuKDG weist den Diensteanbietern eine differenzierte Verantwortung für Inhalte zu. Das Jugendschutzgesetz hebt neben staatlichen Maßnahmen auf eine freiwillige Selbstkontrolle, den technischen Selbstschutz und auf die maßgebliche Rolle der Erziehungsberechtigten ab.
- Technische Lösungen zur Filterung der Inhalte bieten bisher keinen adäquaten Schutz, und können prinzipiell keinen absoluten Schutz bieten. Verfügbare Filterprogramme zeigen wenig Treffsicherheit und sind leicht zu manipulieren; ihre Bedienung ist mühsam. Die deutsche Sprachfunktionalität ist unzureichend. Kategoriensysteme zur Kennzeichnung von Inhalten sind bisher nicht weit genug verbreitet, um als Basis für eine flächendeckende qualifizierte Filterung zu dienen. Ein auf den deutschen oder europäischen Kulturraum zugeschnittenes Werte- und Kategoriensystem existiert nicht.
- Als Handlungsoptionen bieten sich der Aufbau von Medienkompetenz, die Nutzung von sozialen Kontrollmechanismen (Aufsicht, Kontrolle von aufgesuchten Web-Seiten, soziale Ächtung von Verstößen etc.) und die Weiterentwicklung der technischen Unterstützung sowie Kombinationen dieser Maßnahmen an.
- Ein mögliches System zur technischen Unterstützung des Jugendschutzes kann auf der Basis von freiwilliger Selbstkontrolle eine möglichst weit verbreitete Einstufung der Internetseiten durch die Anbieter vorsehen, auf deren Grundlage der Abrufer gezielt filtern kann. Zur Unterstützung des Systems ist eine Infrastruktur erforderlich, die ein oder mehrere Kategoriensysteme zur Verfügung stellt, die nötige Filter- und Markierungssoftware verteilt und über eine Schlüsselinfrastruktur die Integrität und Authentizität solcher Einordnungen sicherstellt.
- Jedes System zur Inhaltsfilterung kann bei falscher Konfiguration und fehlender Kontrolle zur Beschränkung der Informationsfreiheit mißbraucht werden. Daher ist es notwendig, dies bei der Konzeption zu beachten und organisatorische Maßnahmen zur Mißbrauchsverhinderung vorzusehen.

Inhaltsübersicht

Abkürzungen

a.a.O.	am angegebenen Ort
Abs.	Absatz
AöR	Anstalt des öffentlichen Rechts
ARD	Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland
Art.	Artikel
Bd	Band
BGB	Bürgerliches Gesetzbuch
BMBF	Bundesministerium für Bildung und Forschung
BPjS	Bundesprüfstelle für jugendgefährdende Schriften
Buchst.	Buchstabe
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts
CIS	CompuServe Information Service
CRL	Certificate Revocation List
de lege ferenda	"nach noch zu schaffenden Recht“
de lege lata	"nach geltendem Recht“
DLR	Deutsches Zentrum für Luft- und Raumfahrt e.V.
DSig	Digital Signature Initiative
Fn.	Fußnote
FSF	Freiwillige Selbstkontrolle Fernsehen
FSK	Freiwillige Selbstkontrolle der Filmwirtschaft
FSM	Freiwillige Selbstkontrolle Multimedia-Diensteanbieter
GG	Grundgesetz
GjS	Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte
Halbs.	Halbsatz
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ID	Identifier
i. d. R.	in der Regel
i.V.m	in Verbindung mit
iCRT	Intelligent Content Recognition Technology
IP	Internet Protocol
ISP	Internetserviceprovider
IuK	Information und Kommunikation
IuKDG	Informations- und Kommunikationsdienste-Gesetz

JÖSchG	Gesetz zum Schutze der Jugend in der Öffentlichkeit
JZ	Juristische Zeitung
m. w. N.	mit weiteren Nachweisen
MDStV	Mediendienste-Staatsvertrag
n. v.	nicht verfügbar
Nrn.	Nummern
OCSP	Online Certificate Status Protocol
P3P	Platform for Privacy Preferences
PC	Personal Computer
PICS	Platform for Internet Content Selection
RDF	Resource Description Framework
RFC	Request for Comments
Rn.	Randnummer
RSACi	Recreational Software Advisory Council on the Internet
RStV	Rundfunk-Staatsvertrag
SSL	Secure Sockets Layer Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
URL	Uniform Resource Locator
USK	Unterhaltungssoftware Selbstkontrolle
vgl.	vergleiche
W3C	WorldWideWebConsortium
WWW	Word Wide Web
ZDF	Zweites Deutsches Fernsehen

0 Zusammenfassung wichtiger Ergebnisse

Ziel der vorliegenden Studie ist es, die heute verfügbaren technischen Lösungen zur Umsetzung von Maßnahmen des Jugendschutzes beim Zugriff auf das Internet

- in einer aktuellen Bestandsaufnahme zusammenzufassen,
- einer Untersuchung und Bewertung hinsichtlich ihrer Eignung zur Umsetzung von Anforderungen des Jugendschutzes zu unterziehen und
- Visionen und Anforderungen an ein geeignetes System zur technischen Unterstützung des Jugendschutzes zu entwickeln.

Als Randbedingungen waren dabei die technische und organisatorische Machbarkeit, der rechtliche Rahmen und die psychologisch-soziologische Durchsetzbarkeit zu berücksichtigen.

0.1 Neue Herausforderungen für den Jugendschutz

Alle in der Geschichte der Kommunikation vor der Verbreitung des Internet eingesetzten Verfahren zur Publikation von Informationen waren entweder auf einen sehr kleinen Teilnehmerkreis beschränkt oder benötigten die Kooperation mehrerer Individuen zur Produktion und Verbreitung der Inhalte. Es gab eine Publikationskette, in der viele Menschen (Autor, Lektor, Editor, Layouter, Setzer, Drucker, Lieferanten, Verkäufer, Leser) zusammenarbeiten mußten, um den Inhalt zum Empfänger zu bringen. Die damit verbundenen Kosten und die große Zahl der beteiligten Personen wirkten selektiv (damit auch kontrollierend und möglicherweise qualitativ aufwertend) auf die veröffentlichten Inhalte.

Das Internet ist eine Verkürzung dieser Kette: Es kommt zur direkten Kommunikation zwischen Autor und möglicherweise Millionen von Rezipienten, die dieselbe vereinheitlichte Kommunikationsinfrastruktur nutzen. Diese Infrastruktur stellt lediglich allgemeine Kommunikationsdienste zur Verfügung und hat weder Einfluß auf noch Kenntnis von den übertragenen Informationsinhalten. Im einzelnen heißt das:

- Die Inhalte können von jedem Nutzer, also auch von Kindern und Jugendlichen, jederzeit abgerufen werden, keinerlei definierte Abläufe ("Fernsehprogramm“) oder transportbedingte Verzögerungszeiten schränken diese Freiheit ein.
- Es gibt keine menschlichen Kontrollinstanzen zwischen Anbieter und Empfänger bzw. Abrufer (wie z.B. Videotheken, Fernsehsender oder Kinobetreiber im Falle des Mediums "Film“).
- Die Wahrscheinlichkeit eines zufälligen Abrufes von (unerwünschten) Informationen ist weitaus größer als bei herkömmlichen Medien.
- Für Anbieter und Abrufer gelten häufig verschiedene Regulative; eine Durchsetzung von rechtlichen Vorschriften ist also schwierig.

Welche Menge von potentiell jugendgefährdenden Inhalten aufgrund dieser vereinfachten Informationsübertragung im Umlauf ist, läßt sich in exakten Zahlen wegen der großen Menge von Internetangeboten und der ständigen Veränderungen nicht angeben; es läßt sich aber an Beispielen leicht zeigen, daß die absolute Anzahl groß ist und sowohl absichtliche Zugriffe möglich sind als auch zufällige Funde vorkommen.

So ist zum Beispiel ein Zugang zu jugendgefährdendem – speziell pornographischem – Material leicht möglich, wenn explizit danach gesucht wird. Suchvorgänge nach einfachen Schlagwörtern – "Sex“, "Porno“, "Gewalt“ – liefern eine große Anzahl von einschlägigen Treffern. Außerdem bieten spezielle Newsgroups entsprechende Bilder und Texte an. Auch

gibt es inzwischen spezielle Ratgeber für erotische Seiten, von denen eine Verzweigung auf jugendgefährdende Seiten einfach möglich ist.

Neben dem absichtlichen Aufsuchen solcher Angebote besteht eine hohe Wahrscheinlichkeit von Zufallstreffern: Auf häufig aufgerufenen Seiten – Telefonverzeichnisse, Suchmaschinen – findet sich Werbung für Erotikanbieter. In eigentlich "harmlosen“ Newsgroups werden entsprechende Nachrichten veröffentlicht, die Hinweise z.B. auf Erotikanbieter enthalten und den Browser z.T. direkt zum Öffnen der jeweiligen Einstiegsseite veranlassen. Und schließlich können auch Suchvorgänge nach harmlosen Schlüsselwörtern zu Verweisen auf jugendgefährdende Angebote führen, wenn in diesen Seiten absichtlich irreführende Schlagwortangaben vorgenommen wurden.

Zugangsbeschränkungen, wie sie für jugendgefährdende Angebote z.B. in Deutschland vorgeschrieben sind, können die Gefahr nicht bannen. Zum einen sind im Ausland bei weitem nicht alle entsprechenden Angebote zugangsbeschränkt. Zum anderen finden sich auch auf den Einstiegsseiten bereits für Kinder ungeeignete Bilder; die Zugangsbeschränkung läßt sich außerdem meist durch Eingabe einer Kreditkartennummer entsperren.

Bereits vor Beginn der Studie war zu vermuten, daß das Problem nicht allein durch technische Maßnahmen in den Griff zu bekommen ist. Alle bisher eingesetzten Filtersysteme und -versuche haben im günstigsten Fall den zufälligen Abruf einer Information verhindern können. In keinem dokumentierten Fall ist es bisher gelungen, eine Information oder gar eine Klasse von Informationen im Internet für einen bestimmten Abrufer nicht verfügbar zu machen. Oftmals ist es kaum gelungen, den Abruf signifikant zu erschweren. In bisher allen dokumentierten Fällen von Sperrungsversuchen war die Sperrung außerdem zu wenig paßgenau.

Zusammenfassend kann man also feststellen, daß im Internet eine nicht zu vernachlässigende Jugendgefährdung besteht, der aufgrund der neuen Struktur der Informations- und Inhaltsübertragung mit den bisherigen Konzepten des Jugendschutzes kaum zufriedenstellend zu begegnen ist. Dies hat einerseits Auswirkungen auf die Vorschläge für geeignete technische Ansätze zum Jugendschutz im Internet; hier werden grundsätzlich auch andere technische Mechanismen als im klassischen Jugendschutz zur Anwendung kommen müssen. Andererseits wird sich aufgrund der Tatsache, daß perfekter technischer Schutz generell nicht erreichbar ist, die Zielrichtung der Jugendschutzmaßnahmen noch mehr als bisher in Richtung des Aufbaus von Medienkompetenz bei jugendlichen und erwachsenen Nutzern der neuen Medien verschieben müssen.[1]

0.2 Juristische Aspekte

Neben den strafrechtlichen Vorschriften des Strafgesetzbuchs, die ein bestimmtes Verhalten generell nicht erlauben und damit (auch) dem Jugendschutz dienen, verfolgt vor allem das Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte (GjS) Ziele des Jugendschutzes. Das Gesetz sieht vor, daß Schriften, die geeignet sind, Kinder oder Jugendliche sittlich zu gefährden, in eine Liste aufzunehmen sind. Als ausdrückliche Beispiele werden genannt: unsittliche, verrohend wirkende, zu Gewalttätigkeit, Verbrechen oder Rassenhaß anreizende sowie den Krieg verherrlichende Schriften. Das Gesetz zielt dabei in erster Linie auf solche Schriften und Medieninhalte ab, die die im Strafgesetzbuch dargestellten Straftatbestände noch nicht erfüllen.

Die durch das IuKDG in das GjS eingefügte Vorschrift zielt darauf ab, durch dezentrale Beauftragte, die vor Ort die Interessen des Jugendschutzes wahrnehmen, eine dem

[1] Zu einem entsprechenden Schluß kommt z.B. auch der Schlußbericht der Enquete-Kommission "Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft“, Bundestagsdrucksache 13/11004.

Jugendschutz förderliche Infrastruktur zu schaffen. Der Diensteanbieter kann seiner Verpflichtung auch dadurch nachkommen, daß er eine Organisation der freiwilligen Selbstkontrolle zur Wahrnehmung der Aufgaben des Jugendschutzbeauftragten verpflichtet.

Mit dem Informations- und Kommunikationsdienste-Gesetz (IuKDG) wurden 1997 auch neue Jugendschutzregelungen eingeführt. Der Ansatz dabei war, daß sich die Indizierung gemäß dem geänderten GjS jetzt auch auf Inhalte von Webseiten beziehen kann.

Zusätzlich wurde ein neuer Absatz in das GjS aufgenommen, wonach eine indizierte Schrift nicht "durch elektronische Informations- und Kommunikationsdienste verbreitet, bereitgehalten oder sonst zugänglich gemacht werden“ darf (vgl. Art. 6 Nr. 3 Buchst. a) IuKDG).

Das Verbot der Verbreitung indizierter Schriften durch elektronische Informations- und Kommunikationsdienste greift dann nicht, "wenn durch technische Vorkehrungen Vorsorge getroffen ist, daß das Angebot oder die Verbreitung im Inland auf volljährigen Nutzer beschränkt werden kann.“ Die Vorschrift soll eine übermäßige Einengung der Informationsmöglichkeiten für Erwachsene aus Informations- und Kommunikationsdiensten vermeiden.

0.3 Soziologische Aspekte

In Kapitel 3 werden die Problematik des Jugendschutzes im Internet und der Einsatz von Filtersystemen aus soziologischer Sicht beleuchtet:

Die zunehmende Nutzung des Internet führt zu großen Veränderungen in allen gesellschaftlichen Bereichen. Diese lösen Ängste und Unsicherheiten aus, die insbesondere beim Umgang der Jugendlichen mit den neuen Medien in Erscheinung treten. In dem Zusammenhang wird in Frage gestellt, ob das vom Internet für Jugendliche ausgehende Gefährdungspotential realistisch oder nicht vielmehr überhöht eingeschätzt wird. Zweifellos erleichtert das Internet als neuer Verteilungsweg in vielen Fällen den Zugang zu Probleminhalten, wohingegen hinsichtlich dieser Inhalte überwiegend keine spezifische neue Qualität gesehen wird.

Jedenfalls sehen sich Eltern, Lehrer und staatliche Institutionen in der Pflicht, Jugendliche vor aus ihrer Sicht problematischen Inhalten des Internet zu schützen. Die Bewertung der Inhalte unterliegt dabei den Werterefenzen der Erwachsenen, die häufig aus der eigenen Kinder- und Jugendzeit stammen oder deren Geltung permanent durch die Massenmedien suggeriert wird. Dabei liegt ein latent gültiger und nur schwer präzise faßbarer Normen- und Wertekatalog der Gesellschaft zugrunde.

Der Schutz der Jugend gestaltet sich angesichts der modernen Medien deutlich komplizierter als früher. Der Umgang mit dem Internet übersteigt die kommunikativen Strukturen von Familien und Organisationen, weltweite Interaktionen per Netz werden möglich, der Anteil der möglichen "sozialen Kontrolle“ verringert sich.

Der Übergang zu mehr Autonomie und von "Fremd- zur Selbstkontrolle“ sollte heute möglichst frühzeitig bei den Jugendlichen erfolgen. Dabei müssen den Jugendlichen klare, moderne Erwartungsstrukturen angeboten werden, an denen sie sich reiben und mit denen sie sich auseinandersetzen können – auch und insbesondere im Umgang mit den neuen Medien. Filtersysteme für das Internet, in denen sich die normativen Gehalte der Gesellschaft spiegeln, können dabei Unterstützung leisten. Der Einsatz von (wenn auch in ihrer Schutzfunktion unzulänglichen) Inhaltsfiltern gibt darüber hinaus den verantwortlichen Erwachsenen das Gefühl, das gegenwärtig Machbare zu tun und den gültigen Wertekatalog zu sichern.

Bei der Entwicklung effizienter Filtersysteme und der zugrunde liegenden Bewertungssysteme sind auch die möglichen Gefahren zu beachten. Eine Explikation des latent vorhandenen Normen- und Wertekatalogs birgt soziologische Risiken wie eine

Steigerung des Konfliktlevels bis hin zum Verlust der bindenden Funktion. Auch können Filtersysteme mißbräuchlich eingesetzt werden und die Autonomie des Bürgers sowie sein Recht auf Informationsfreiheit beschneiden.

0.4 Technische Grundlagen

Um Jugendschutz im Internet technisch nach Möglichkeit wirkungsvoll zu unterstützen, ist eine Sortierung der Inhalte nach ihrem jugendgefährdenden Potential erforderlich. Die Durchführung einer solchen Sortierung (Filterung) wiederum erfordert, daß die Inhalte

- in Kategorien eingeordnet,
- gekennzeichnet und
- ausgewählt

werden. Abb. 0-1 beschreibt den schematischen Verlauf eines solchen Vorgangs.

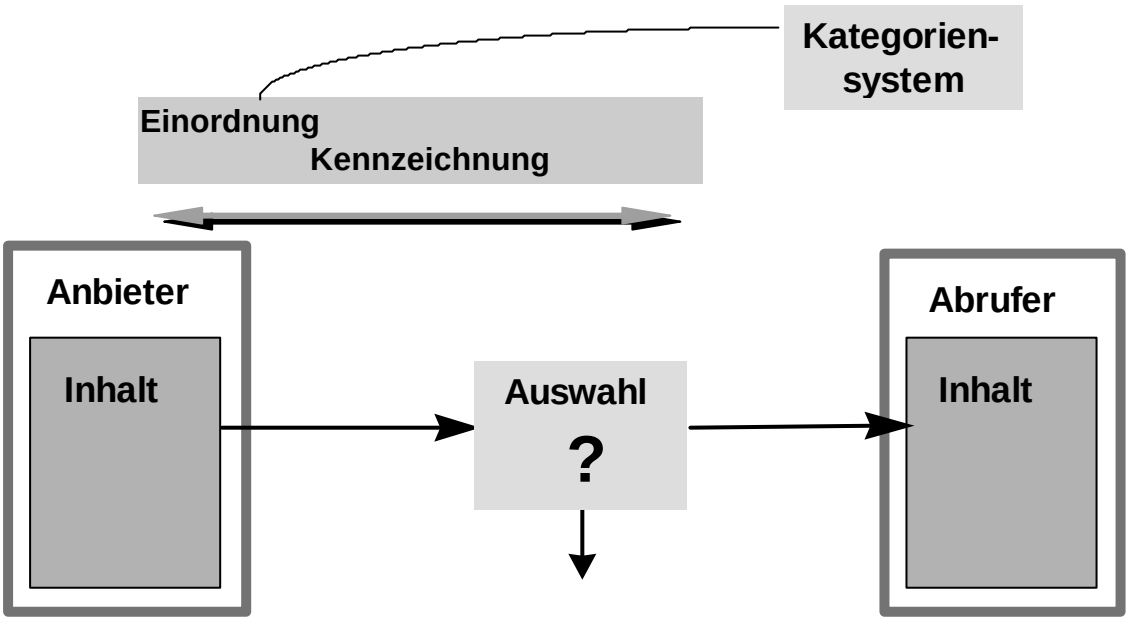


Abb. 0-1: Schematischer Ablauf von Filterung im Internet

Der Begriff der *Einordnung* beschreibt den Vorgang der inhaltlichen Zuordnung einer Internetseite in ein oder mehrere vorhandene Kategoriensysteme. Basis der Einordnung ist das zugrunde gelegte *Kategoriensystem*, da es wesentlichen Einfluß auf die Art der Einordnung hat: Es gibt den formalen Rahmen für die Einordnung vor, indem es eine begrenzte Anzahl verschiedener Kategorien zur Verfügung stellt und somit die Einordnung erleichtert. Zugleich legt es durch die Definition der Kategorien die Möglichkeiten der inhaltlichen Differenzierung fest. Art und Anzahl der Kategorien können sehr verschieden sein, z.B. nur "nicht jugendgefährdend“ und "jugendgefährdend“ unterscheiden, eine inhaltliche Feineinordnung vornehmen – "Bilder von Tieren“, "pädagogische Texte“, "deutschsprachig“ – oder auch formaler Art sein ("enthält keine Grafiken“, "enthält Java“, "nur Text“). Damit das System einfach angewendet werden kann, ist eine gute Abbildung der moralisch-ethischen und inhaltlichen Vorstellungen von Anbieter und Abrufer auch im internationalen Kontext erforderlich. Darüber hinaus ist Wert zu legen auf eine gute Verständlichkeit und eine leichte technische Anwendbarkeit.

Es gibt bereits verschiedene Kategoriensysteme; sie wurden allerdings alle für den amerikanischen Markt entworfen und entsprechen daher auch den dortigen Vorstellungen von

Jugendschutz. Außerdem liegen sie nur in englischer Sprache vor. Dies macht den Bedarf für ein europäisches System deutlich, das mehrere Sprachen integriert und dessen Abstufungen für internationale Verwendung geeignet sind. Um eine hohe Akzeptanz und eine daraus resultierende weite Verbreitung eines solchen Systems zu erreichen, sollten bereits in der Konzeptionsphase verschiedene gesellschaftliche Gruppen an der Definition der Kategorien beteiligt werden. Denkbar sind dabei auch mehrere, sich ergänzende und technisch miteinander kompatible Systeme.

Kategoriensysteme – auch Ratingsysteme genannt – dienen der inhaltlichen Einordnung der Internetseiten. Damit sie technisch verwendbar sind, ist eine technische Basis, eine Art "Übertragungsprotokoll“ erforderlich. Existierende öffentliche Kategoriensysteme basieren meist auf dem Standard von PICS (Platform for Internet Content Selection). PICS ist selbst kein Kategoriensystem, sondern ermöglicht eine formal-technische Definition solcher Kategorien und deren technische Verwendung bei der Erstellung von Internetseiten. Es enthält außerdem Zusatzfunktionen z.B. bezüglich der "Übersetzung“ verschiedener Systeme ineinander und zur Signatur von Kennzeichnungen. Da PICS bereits weit verbreitet ist, sollten neue Systeme ebenfalls auf dieser Basis aufbauen. Für das im weiteren dargestellte System ist allerdings eine Erweiterung des jetzigen Standards erforderlich.

Die *Einordnung* selbst kann auf Basis eines Kategoriensystems von verschiedenen Instanzen – Autor, dritte Instanz, Internet Community, Abrufer – durchgeführt werden, wobei die Entscheidung für eine Instanz unterschiedliche Auswirkungen auf Aufwand, Einheitlichkeit, Transparenz und Korrektheit hat.

- Der Aufwand wäre am niedrigsten, wenn der Autor die Einordnung selber durchführt; allerdings ist hier auch die Einheitlichkeit nur durch zusätzlichen Kontrollaufwand zu gewährleisten.
- Das Gegenteil liegt bei der Einordnung durch den Abrufer vor: Hier wäre der Aufwand zum Bearbeiten eines ausreichend großen Teils des Internets unübersehbar hoch, die resultierende Einordnung entspräche allerdings den Anforderungen des Abrufers vollständig.
- Zusätzlich zu berücksichtigen ist die Gefahr von absichtlichen Falscheinordnungen, die besonders bei der Erfassung durch dritte, von Anbieter und Abrufer verschiedene Personen besteht. Hier kann eine vom Abrufer unbemerkte Manipulation durch "Ausblenden“ bestimmter "unliebsamer“ Seiten erfolgen. Andererseits kann ein Einordnungsservice (*Third-Party-Rating*) einer vertrauenswürdigen Organisation eine sehr einheitliche Einstufung bieten. Hier kommt es also sehr auf die Auswahl der Instanz an, auf die ein Abrufer vertraut.

Die angeführten Gründe sprechen für eine Einordnung durch den Autor oder Abrufer. Da mit Blick auf die Fülle der Angebote der Aufwand bei Einordnung durch den Abrufer in der Praxis jedoch nicht zu leisten ist, kann in einem weit verbreiteten System nur die Einordnung durch den Autor sinnvoll durchgeführt werden. Ergänzungen durch Third-Party-Rating sind u.U. denkbar, sollten aber aufgrund der geschilderten Problematik nur zusätzliche Möglichkeit sein.

Nach der Einordnung erfolgt die *Kennzeichnung* der Seite. Das heißt, die Einordnung wird technisch zugänglich gemacht (z.B. mit dem bereits beschriebenen Verfahren nach dem PICS-Standard), indem z.B. ein Vermerk auf der Seite angebracht oder ein Eintrag in einer Kennzeichnungssammlung vorgenommen wird. Die technische Realisierung ist für statische Seiten relativ einfach; um dynamische und sehr heterogene Seiten und Server zu kennzeichnen, ist erhöhter Aufwand erforderlich.

Wünschenswert ist hier eine automatische Generierung der Eintragung in eine Kennzeichensammlung oder des Vermerks aus sprachlicher oder textueller Eingabe des Einordnenden. Existierende Systeme lösen dies z.B. durch WWW-Formulare. Beim Entwurf

des Systems sind die konkreten Anforderungen der Nutzer zu beachten, wie sie in dieser Studie ermittelt wurden.

Der letzte Schritt ist dann die eigentliche *Auswahl*: Auf Basis der durch eine Kennzeichnung verfügbaren Einordnung wird entschieden, ob eine bestimmte Seite auf dem Endsystem angezeigt wird oder nicht. Meist wird diese Entscheidung automatisiert gefällt und basiert auf einer Vorauswahl des Benutzers (z.B. Eltern, Lehrer) aus dem Kategoriensystem.

Charakterisierend für den Auswahlprozeß ist der Ort von Konfiguration und Ausführung:

- Der Auswahlprozeß kann auf dem Rechner ablaufen, an dem die Internetnutzung erfolgt (z.B. auf einem privaten PC). In diesem Falle wird das Filtersystem dort konfiguriert, also z.B. von den Eltern. Die Eltern können so ihre eigenen Vorstellungen von geeigneten und ungeeigneten Inhalten in den Auswahleinstellungen für ihre Kinder berücksichtigen. Ein auf dem eigenen PC ablaufender Prozeß ist allerdings oft einfacher durch die zu schützenden Kinder zu umgehen als ein entfernt ablaufender.
- Als Alternative kann der Auswahlprozeß auch auf einem zentralen Rechner (Server) z.B. beim Internetserviceprovider (ISP, Anbieter von Internet-Zugang) durchgeführt werden. Je nach System gilt dann eine Filtereinstellung für alle mit dem Server verbundenen Internetzugänge – geeignet z.B. für Computerräume in Schulen, aber äußerst ungeeignet für jede Art von individuellem Zugang – oder die Einstellungen können lokal gewählt und an den Server übertragen werden.

Dieser Ansatz ist in beiden Fällen als problematisch bezüglich Datenschutz und ungewollter Filterung einzuschätzen, da der Endbenutzer keinen direkten Einfluß auf die Filterung hat und zu ihrer individuellen Konfiguration detaillierte Angaben über seine persönlichen Wertvorstellungen machen muß. Die Gefahr von Manipulation ist geringer, da der jugendliche Endnutzer keinen Zugriff auf den Server hat

- Findet die Kommunikation zwischen Server und Internet-Software (Browser) verschlüsselt statt, wie es zum Beispiel bei allen Formen von eCommerce-Anwendungen der Fall ist, liegt die Information über den Inhalt der abgerufenen Seiten nur auf dem Rechner des Anbieters und des Abrufers vor. Dementsprechend kann die Auswahl in solchen Fällen nur auf dem lokalen Rechner stattfinden. Eine Filterung am Proxy ist in diesem Szenario ausgeschlossen.

Damit läßt sich zusammenfassend feststellen, daß ein Filter, der lokal eingesetzt und konfiguriert wird, besser geeignet ist, einen individuellen Jugendschutz unter Gewährleistung von Datenschutz und dem Recht auf freie Information (z.B. für volljährige Benutzer desselben Zugangs) technisch zu unterstützen. Prozesse auf Servern oder Proxies sind nur für Schulen, u.ä. sinnvoll.

In allen oben genannten Fällen ist für eine korrekte Auswahl außerdem zu garantieren, daß die Übertragung der Kennzeichnung korrekt verläuft, daß also

- der anbietende Rechner nicht manipuliert wurde, von dem der Vermerk abgerufen wird,
- der Vermerk auf dem Weg nicht verändert wurde,
- auch lokal kein Prozeß abläuft, der technische Veränderungen vornehmen kann.

Hierzu sind Mechanismen zur Sicherung von Authentizität und Integrität erforderlich, die allerdings von keiner heute verfügbaren Lösung angeboten werden.

Festzustellen ist außerdem, daß kein System absolute Sicherheit bieten kann. Außerdem können gerade relativ sichere Systeme nicht nur zum erwünschten Jugendschutz, sondern auch zur Manipulation und Beschränkung der Informationsfreiheit verwendet werden. Der Unterschied zwischen berechtigter Kontrolle und manipulativer Zensur reduziert sich also auf eine Frage von Konfiguration und Kontrolle. Daher sind Kontrollmaßnahmen und die

Schaffung von Medienkompetenz als Ergänzung zu einem technischen System unbedingt erforderlich.

0.5 Technische Tests

Durch technische Tests sollte im Rahmen der Studie ermittelt werden, ob es bereits Lösungen oder Produkte gibt, die eine zufriedenstellende technische Unterstützung des Jugendschutzes im Internet bieten. Zusätzlich sollten Anforderungen für geeignete Lösungen entwickelt werden. Dazu wurde aus den etwa fünfzig am Markt verfügbaren Produkten eine Vorauswahl getroffen, die sich an der Größe des Funktionsumfangs und den Anpassungsmöglichkeiten der Programme an die Nutzerbedürfnisse orientierte. Mit einigen dieser Produkte wurden Kurztests durchgeführt.

Als Resultat wurden drei Produkte – WebChaperone, CyberPatrol und das Gesamtkonzept von CompuServe – für detaillierte, intensive Tests ausgewählt.

Es wurden allgemeine Bedienungseigenschaften getestet, d.h. Installation, Konfiguration und die Dokumentation bzw. Hilfefunktion. Außerdem wurde die Filterfunktionalität untersucht (Positivlisten, Negativlisten, PICS, automatische Verfahren), die Filtereffektivität an einigen Beispielen überprüft und der Aufwand zur Umgehung der Sperrmechanismen ermittelt.

Im Ergebnis konnte keines der Produkte zufriedenstellen. Die vollständige Sperrung z.B. des Internetzugangs oder des News-Abrufes war zwar erfolgreich; auch nach PICS-Labeln konnte zuverlässig gefiltert werden. Die Filterung von sexuell-pornographischen Seiten war jedoch nur befriedigend, bei rassistischen und gewaltverherrlichenden Inhalten sogar völlig unzureichend. Dabei wurden englischsprachige Seiten korrekter als deutschsprachige behandelt; die deutsche Sprachfunktionalität ist nicht vorhanden oder völlig unzureichend. Z.T. sind die Programme außerdem sehr leicht zu umgehen oder zu deaktivieren. Sicherungsmechanismen für Integrität und Authentizität der Einordnungen waren nicht vorhanden.

0.6 Ergebnisse der Praxiserprobung

Im Rahmen einer Praxiserprobung wurde untersucht, welche Anforderungen Anwender an ein technisches System zur Unterstützung des Jugendschutzes im Internet stellen. Ziel dabei war, die Anforderungen der Nutzer an den Funktionsumfang solcher Systeme, aber auch an die Art und den Umfang der wünschenswerten Anpassungen an eigene Bedürfnisse zu ermitteln.

Die im Rahmen der Studie durchgeführten Umfragen zur Notwendigkeit von speziellen Jugendschutzmaßnahmen für das Internet ergaben, daß Lehrer, Eltern und Schüler die Gefährdung durch das neue Medium Internet eher gering einschätzten, während Experten und professionelle Anbieter eines öffentlichen Internetzugangs eher Anlaß zur Besorgnis sahen. Wenn Eltern den Zugang ihrer Kinder zum heimischen PC mit Internetanschluß so ähnlich regeln wie den Fernsehzugang oder wenn Organisationen in ihren Räumlichkeiten das Internetsurfen wie Zeitschriftenlesen behandeln (und kontrollieren), dann greifen dort soziale Kontrollmechanismen. Das für unangemessen angesehene Verhalten wird durch die im Falle des Fehlverhaltens folgenden Sanktionen verhindert. Schüler, die wissen, daß ihr Websurfen (zumindest im nachhinein) kontrolliert wird, erleben diese Kontrolle als bedeutsam und berücksichtigen sie in ihrem Surfverhalten. Es wird daher z.T. die Meinung vertreten, daß das reine Androhen von Sanktionierungs- oder Kontrollmaßnahmen ausreicht, um die ausreichenden Jugendschutz zu gewährleisten.

Die durchgeführten Praxistest ergaben weitere Anforderungen an eine technische Lösung:

- Eine Integration der Filtertechnologie in Anwendungsprogramme (Browser etc.) wäre hilfreich.

- Einfache Bedienbarkeit ist die Voraussetzung für die Akzeptanz bei den Nutzern.
- Die Technik sollte flexibel und individuell konfigurierbar sein, um eine gute Umsetzung der eigenen Vorstellungen von Jugendschutz zu ermöglichen.

Diese Ergebnisse wurden im Rahmen eines Praxistests vertieft und erweitert. Es wurden mit zwölf Probanden im Alter zwischen 16 und 57 Jahre mit den in Abschnitt 0.3 genannten ausgewählten Programmen getestet. Dabei wurden die Probanden gebeten, Ablauf, Installation, Konfiguration, allgemeine Nutzung und Deinstallation zu beurteilen. Ein Fragebogen zur Bedienbarkeit und Akzeptanz und ergänzende Interviews schlossen die Erprobung ab.

Aus diesen Befragungen ergaben sich neben den generellen technischen Mängeln, wie sie auch in den technischen Test ermittelt wurden, einige weitere erforderliche Verbesserungen:

- Durchgängige Verwendung der deutschen Sprache.
- Verbesserungen der Bedienungssteuerung.
- Intuitive Bedienungselemente.
- Bessere Übereinstimmung zwischen Programm- und Aufgabenstruktur.
- Ausbau des Manipulationsschutzes.
- Oberflächen- und Funktionalitätsintegration in Betriebssystem und Anwendungen.

Für Weiter- bzw. Neuentwicklungen ist daher zu empfehlen, die Technik von vornherein nutzerorientiert zu gestalten, um die aufgetretenen Probleme in der Bedienung zu vermeiden und eine reale Tauglichkeit und damit breite Akzeptanz des Systems zu fördern.

Sowohl die technischen als auch die praktischen Tests zeigten, daß keines der derzeit erhältlichen Filterprodukte in seinem aktuellen Stand in der Lage ist, eine zufriedenstellende Unterstützung des Jugendschutzes zu gewährleisten. Die größten Mängel sind fehlende Mehrsprachigkeit und mangelnde Transparenz der Filterkriterien. Alle derzeit existierenden Systeme sind nur einsprachig (Englisch) und beruhen in ihrer Abstufung auf dem kulturellen Hintergrund von Nordamerika. Um ein für Deutschland und Europa verwendbares System zu schaffen, ist also zumindest eine Übertragung in die jeweiligen Landessprachen erforderlich, die allerdings nicht nur eine Übersetzung durchführen darf, sondern auch Rücksicht auf die jeweiligen Kulturvorstellungen nehmen muß. Um dem grenzübergreifenden Charakter des Internet Rechnung zu tragen, ist langfristig ein mehrsprachiges und auch multikulturelles System anzustreben.

0.7 Lösungsvorschlag

Aufgrund der technischen und praktischen Tests hat sich ergeben, daß bisher keine geeigneten technischen Systeme zur Unterstützung des Jugendschutzes im Internet existieren; es gibt allenfalls viele Ansätze, die aber bisher in keinem Komplettsystem zusammengefaßt wurden.

Prinzipiell ist ein perfekter technischer Jugendschutz im Internet nicht zu erreichen – zu viele potentielle Fehlerquellen und Umgehungsmöglichkeiten bieten immer wieder die Gefahr für Fehler oder Manipulation. Jedes System kann also nur die Gefährdung verringern, nie aber völlig ausschalten. Hinzu kommt, daß der Einsatz solcher Systeme immer mit zusätzlichem Aufwand verbunden ist und außerdem das Risiko unerwünschter Effekte gesellschaftlicher und wirtschaftlicher Art in sich trägt.

Daraus könnte man nun ableiten, daß die generelle Idee des Jugendschutzes durch Vermeidung des Kontaktes von Jugendlichen mit jugendgefährdendem Material zu überdenken wäre. Geht man jedoch davon aus, daß die Technik prinzipiell nur unzureichend schützen kann, könnte man jedes technische Verfahren ablehnen und auf pädagogisch-

erzieherischen Schutz setzen: durch Medienkompetenz und intensive Betreuung der sich mit dem Internet auseinandersetzenden Jugendlichen.

Eine Betrachtung der technischen Möglichkeiten zeigt jedoch, daß durchaus Systeme vorstellbar sind, die zur Verbesserung des Jugendschutzes beitragen können – keinesfalls als Ersatz der pädagogischen Maßnahmen, aber als deren Hilfsmittel und sinnvolle Ergänzung.

Die geschilderten technischen Möglichkeiten erlauben eine Filterung auf vielerlei Art. Entscheidend für jedes System sind immer die Instanzen, bei denen Einordnung, Kennzeichnung und Auswahl des Filterprozesses bzw. deren Konfiguration angesiedelt sind (s.o.). Durch diese werden Einflußmöglichkeiten, Verantwortungsbereiche und auch die erforderliche oder mögliche Weitergabe von persönlichen Daten definiert. Außerdem ergeben sich daraus die notwendigen und möglichen Ansatzpunkte für Manipulationsschutz und Integritätssicherung.

Zusammengefaßt kann bezüglich der technischen Möglichkeiten folgendes festgestellt werden.

- Als Grundlage für ein Filtersystem ist ein geeignetes, allgemein akzeptiertes Kategoriensystem erforderlich. Als technische Basis bietet sich PICS an; allerdings sind hier noch einige Erweiterungen notwendig.
- Die Einordnung erfolgt sinnvollerweise beim Anbieter; eine Unterstützung (allerdings nicht im Sinne einer Alternative) durch Dritte ist denkbar.
- Die Kennzeichnung kann auf den Internetseiten selbst oder in separaten Listen erfolgen; in beiden Fällen ist durch Authentifizierung für eine gesicherte Übertragung bis zum Abrufer zu sorgen.
- Die Auswahl soll vom Endbenutzer (Erziehungsberechtigte, Lehrer) zu konfigurieren sein und aus Gründen des Datenschutzes und der Kontrolle über die Filterung auch lokal ablaufen. Dabei ist für ausreichende Manipulationssicherheit zu sorgen.

Begleitend ist das System zu kontrollieren und Mißbrauch zu sanktionieren.

Außerdem sollten Maßnahmen zur Entwicklung von Medienkompetenz den Einsatz des technischen Systems flankieren, sowohl um die Unvollständigkeit des technischen Schutzes zu kompensieren als auch um besonders bei Jugendlichen den kompetenten und kritischen Umgang mit dem Medium Internet zu fördern.

Es konnten in den verschiedenen Tests weiterhin Kriterien entwickelt werden, die eine einfache Nutzbarkeit und damit eine schnelle Verbreitung fördern.

Aus diesen Ergebnissen wurde ein Grobkonzept für ein System zur technischen Unterstützung des Jugendschutzes im Internet einschließlich flankierender Maßnahmen entwickelt. Abb. 0-2 zeigt die Grundzüge des technischen Ablaufs.

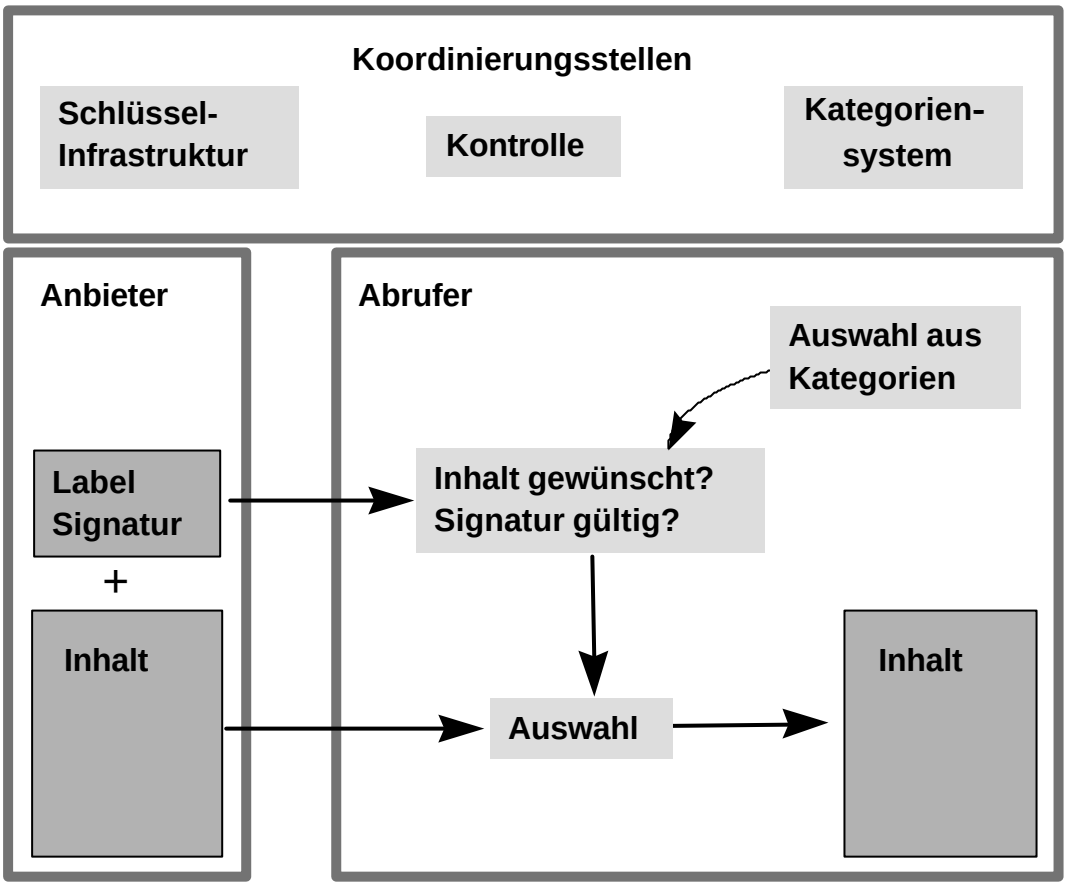


Abb. 0-2: Ablauf der vorgeschlagenen Lösung zur technischen Unterstützung des Jugendschutzes im Internet

Damit Anbieter und Abrufer die bereits beschriebenen Funktionen ausführen können, werden Koordinierungsstellen eingeführt, die neben der Aufklärung und Werbung für Jugendschutz und für die Verwendung des Systems die nötige Infrastruktur zur Verfügung stellen und weiterentwickeln und das Funktionieren des Systems beaufsichtigen.

Wichtiger Punkt ist hier eine Schlüsselinfrastruktur, die das digitale Signieren von Kennzeichnungen und die Verifikation dieser digitalen Signaturen beim Abrufer ermöglicht. Die Sicherheitsanforderungen an eine solche Schlüsselinfrastruktur sind niedriger als die anderer solcher Systeme; insofern kann sie mit geringerem Aufwand betrieben werden. Um das System durchzusetzen, müssen falsche Einstufungen sanktioniert werden. Als letzte Sanktionierungsmaßnahme im Rahmen eines mehrstufigen Sanktionierungskonzeptes wird der Entzug der Signierbefugnis vorgeschlagen; hierfür ist die Infrastruktur unter der Kontrolle einer oder mehrerer Koordinierungsstellen anzusiedeln.

Im Rahmen des Lösungsvorschlags wurden die verschiedenen Aspekte eines solchen Systems näher spezifiziert und konzipiert.

Zur Realisierung eines solchen technischen Systems sind folgende Schritte erforderlich:

- Entwicklung der nötigen Werkzeuge für Anbieter und Abrufer bzw. Anpassung existierender Lösungen.
- Erweiterung der PICS-Spezifikation, nach Möglichkeit Einbringung in die Standardisierung.
- Aufbau eines Kategoriensystem unter Berücksichtigung der einfachen Anwendung durch die Nutzer und einer intensiven Einbindung der potentiellen Anwender in die inhaltliche Konzeption.

- Aufsetzen einer Schlüsselinfrastruktur mit geeigneten Konzepten zur Schlüsselverteilung.
- Förderung der schnellen Verbreitung des Systems.
- Entwicklung und Durchführung eines flankierendes Medienkompetenzkonzeptes.

Die Feinkonzeption der einzelnen Bausteine kann auf dem in dieser Studie entwickelten Rahmen und der dargestellten Grobkonzeption aufbauen und damit Gegenstand weiterer Arbeiten sein. Sie sollte in enger Abstimmung mit allen Beteiligten (z.B. Content-Providern, Online-Service-Providern und Nutzern) erfolgen.

Parallel zur technischen Weiterentwicklung müßte detailliert untersucht werden, welche Kosten, rechtlichen Fragen und möglicherweise unerwünschten Auswirkungen mit der Einführung eines solchen Systems verbunden wären. Da in Australien bereits weitgehende gesetzliche Regelungen mit Jugendschutzintention verabschiedet wurden, wird empfohlen, die dortige Entwicklung zu beobachten und die dort gemachten Erfahrungen für die weiteren europäischen Planungen zu berücksichtigen.

1 Ausgangslage und Problemaufriß

Mit der Verabschiedung des Teledienstegesetzes (TDG) als Artikel 1 des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) hat der Deutsche Bundestag 1997 eine gesetzliche Regelung der Verantwortlichkeit von Diensteanbietern für Inhalte verabschiedet. Das IuKDG wird gemäß einer Entschließung des Deutschen Bundestages innerhalb von zwei Jahren evaluiert. Diese Evaluation soll zeigen, ob sich aus den Erfahrungen Anpassungsbedarf hinsichtlich des bestehenden Rechtsrahmens ergibt.

Eine Fragestellung in diesem Zusammenhang ist die der Leistungsfähigkeit von Technologien zur Umsetzung von Anforderungen des Jugendschutzes im Internet. Alle Personen, die in der Verantwortung für Kinder und Jugendliche stehen und einen Internetzugang bereitstellen, also z.B. Eltern oder Lehrer, sollten in der Lage sein, Jugendliche vor jugendgefährdenden Inhalten des Internet zu schützen. Dabei können technische Maßnahmen unterstützend wirken.

Ziel der zu erstellenden Studie ist es, die heute verfügbaren Techniken zur Umsetzung von Maßnahmen des Jugendschutzes beim Zugriff auf das Internet

- in einer aktuellen Bestandsaufnahme zusammenzufassen,
- einer Untersuchung und Bewertung hinsichtlich ihrer Eignung zur Umsetzung von Anforderungen des Jugendschutzes zu unterziehen und ggf.
- Visionen und Anforderungen an ein geeignetes System zur technischen Unterstützung des Jugendschutzes zu entwickeln.

Als Randbedingungen sind dabei die technische und organisatorische Machbarkeit, die rechtliche Zulässigkeit – auch im Spannungsfeld zwischen Jugendschutz und dem Recht auf freie Meinungsäußerung und freie Information – und die psychologisch-soziologische Durchsetzbarkeit zu untersuchen.

In den folgenden Abschnitten wird aus verschiedenen Blickwinkeln beleuchtet, wie groß die Gefährdung von Jugendlichen durch das Internet real ist und inwieweit daraus konkreter Handlungsbedarf im Sinne des Jugendschutzrechts folgt.

Nach einer Betrachtung der Kommunikationsform "Internet“ beginnen wir mit einer Erläuterung der Unterschiede zum Gefährdungspotential bei Druckerzeugnissen und Filmen und der daraus folgende Notwendigkeit anderer, neuer Maßnahmen zum Jugendschutz. In einer rechtlichen Abgrenzung zeigen wir kurz auf, welche Rechtsgebiete betroffen sind. Dann betrachten wir den Problemkomplex aus psychologischer, sozialer und technischer Sicht und nennen einige Initiativen und Organisationen, die sich mit dem Thema befassen. Den Abschluß macht die Definition von wichtigen Begriffen und Rollen, die wir im weiteren Verlauf der Studie untersuchen werden.

1.1 Veränderung der Kommunikation durch das Internet

Alle bisher in der Geschichte der Kommunikation eingesetzten Verfahren waren entweder auf einen sehr kleinen Teilnehmerkreis beschränkt und sehr flüchtig oder machten die Kooperation mehrerer Individuen zur Produktion und Verbreitung der Inhalte notwendig. Es gab eine Publishing-Pipeline, in der viele Menschen (Autor, Lektor, Editor, Layouter, Setzer, Drucker, Lieferanten, Verkäufer, Leser) zusammenarbeiten mußten, um den Inhalt zum Empfänger zu bringen. Die damit verbundenen Kosten und die große Zahl der beteiligten Personen wirkten selektiv (damit auch kontrollierend und teilweise qualitativ aufwertend) auf die veröffentlichten Inhalte.

Im Laufe der Geschichte ist der Trend zur Verkürzung der Publishing-Pipeline und zur Verbilligung der Stückkosten pro veröffentlichtes Exemplar klar erkennbar. Damit wurden auch Inhalte publizierbar, die es zuvor nicht "wert“ waren, veröffentlicht zu werden.

Das Internet ist die ultimative Verkürzung dieser Pipeline, denn im Extremfall (z.B. im Chat- oder News-Dienst) kommt es zur direkten Kommunikation zwischen Autor und Rezipient, die eine existierende Infrastruktur nutzen. Diese Infrastruktur erbringt keine Dienste mehr, die für diese eine spezielle Kommunikation nötig sind, sondern stellt lediglich allgemeine Kommunikationsdienste zur Verfügung. Damit sinken die Stückkosten für die Reproduktion eines Inhaltes nahezu auf Null, und jede Form der Selektion durch dritte Beteiligte entfällt. Entsprechend ist es möglich, beliebige Inhalte massenhaft zu kommunizieren.

Neu im Ansatz des Internet ist auch, daß es sich bei der im Internet auftretenden Kommunikation (mit Ausnahme von Usenet-News) nicht um ein Massenmedium im engeren Sinne handelt. Massenmedien zeichnen sich dadurch aus, daß einer großen Menge von Rezipienten derselbe Inhalt parallel zugänglich gemacht wird. Das ist genau nicht der Fall: Jeder Abruf einer Webseite ist beispielsweise eine individuelle Verbindung, vergleichbar einem Telefongespräch. Webserver können Webseiten spezifisch für Abrufer erzeugen, was immer häufiger geschieht: Sie orientieren sich dabei beispielsweise an Kriterien wie der eingesetzten Browsersoftware und deren Fähigkeiten, der eingestellten Landessprache, der Tageszeit und dem Datum, der IP-Nummer des Abrufers oder der in einem Cookie[2] übermittelten Benutzeridentität.

Die Einführung einer Instanz, die eine inhaltliche Einordnung von Dokumenten bereitstellt und die den Zugriff auf Dokumente für bestimmte Teilnehmer sperrt, läuft dabei dem technischen Entwicklungstrend entgegen, der Kommunikation immer unmittelbarer, d.h. mehr und mehr Mittler bei einer Kommunikation überflüssig macht. Zudem verwischen sich die technischen Grenzen zwischen privater und öffentlicher Kommunikation immer weiter (z.B. "private“ Homepage, Netzkameras). Entsprechend stellt die Schaffung eines solchen künstlichen, technisch nicht notwendigen Mittlers einen recht weitgehenden Eingriff in die Kommunikationsstruktur des Internet dar, der sich nicht fugenlos in das übrige Umfeld einpassen lassen kann. Die technischen Schwierigkeiten werden besonders deutlich, wenn man versucht, diese Mittlerinstanz auf dynamisch generierte Inhalte (z.B. mehrsprachige Seiten, Suchmaschinen, Katalogsysteme, Gästebücher oder Chatseiten) oder zugangsgeschützte Inhalte anzuwenden.

1.2 Abgrenzung zu anderen Medien

Ein bisher bei Film- und Printmedien nicht gekanntes Ausmaß an Verbreitung durch das Internet ist der entscheidende Unterschied, der neue Maßnahmen und Überlegungen zum Jugendschutz erfordert.

Die Gefährdung Jugendlicher durch Inhalte im Internet läßt sich – im Gegensatz zu anderen Medien wie Presse und Fernsehen – aufgrund der dezentralen und grenzüberschreitenden Struktur des Mediums "Internet“ durch Verbote kaum reduzieren:

- Die Inhalte können von jedem Nutzer, also auch von Kindern und Jugendlichen, jederzeit abgerufen werden.
- Es gibt keinerlei Programme oder zeitliche Abläufe; Zugriffe auf problematisches Material können jederzeit und auch zufällig erfolgen.
- Es gibt keine Instanzen zwischen Anbieter und Konsument, die kontrollierend wirken könnten (wie z.B. Videotheken, Fernsehsender oder Kinobetreiber im Falle des Mediums "Film“).
- Es ist kein physikalischer Auftritt von natürlichen Menschen erforderlich oder üblich, sondern alle Identitäten sind virtuell und bieten damit (für Anbieter und Konsument) die Möglichkeit, andere Rollen und Identitäten anzunehmen oder vorzuspiegeln.

[2] Vermerk eines Webservers auf dem Rechner des Abrufers

- Die Verbreitung erfolgt so schnell, daß Maßnahmen zur Blockierung nicht greifen. Außerdem ist die Infrastruktur technisch, nicht human und daher ohne Schwierigkeiten zum Unterlaufen von Blockaden verwendbar.
- Neben dem absichtlichen, vorsätzlichen Zugriff zu jugendgefährdenden Medien kommt eine zufällige Komponente hinzu; problematische Internetseiten können völlig unbeabsichtigt als Suchergebnis oder auf einen "Mouseclick“ hin erscheinen.
- Der Anbieter befindet sich häufig nicht im Land des Konsumenten; insofern gelten auch die lokalen gesetzlichen Regelungen nicht oder sind zumindest nicht durchzusetzen.
- Dynamische Inhalte entziehen sich einer statischen Einstufung.

Da aus diesen Gründen die Quellen des jugendgefährdenden Materials nicht allgemein zu kontrollieren sind, müssen technische Maßnahmen zum Schutz Jugendlicher am Endpunkt der Verteilung, also am einzelnen Rechner bzw. dessen Internetprovider ansetzen. Eine Unterstützung durch soziale Kontrollen – Lehrer, Eltern, Öffentlichkeit – ist unabhängig von der Form des technischen Systems immer erforderlich.

1.3 Bisherige relevante Untersuchungen

Mit dem Thema illegaler oder unerwünschter Inhalte im Internet haben sich bereits mehrere Studien beschäftigt:

- Europäische Kommission: Illegale und schädigende Inhalte im Internet, KOM(96)0487, 1996,[3] mit einem Zwischenbericht "Initiativen in den EU-Migliedstaaten“, Version 7, 4. Juni 1997,[4] sowie Entschließung des Rates zu illegalen und schädigenden Inhalten im Internet, 1997 (Bundesratsdrucksache 393/97, 16.05.97).[5]
- Diese erste große Untersuchung zu dem Thema "Illegale und schädigende Inhalte im Internet“ unterscheidet zwischen diesen beiden Kategorien. Konzeptuell wird der Einsatz von Filtersoftware als ein technischer Baustein für eine Lösung gesehen, aber auch darauf hingewiesen, daß die Fragen von Klassifizierung und Kodierung gerade in bezug auf internationale Kompatibilität noch nicht geklärt sind. Zusätzlich werden Maßnahmen angeregt, um Hersteller dazu zu veranlassen, Filtersoftware zu verbessern und sie Netzteilnehmern automatisch bereitzustellen.[6]
- A. A. Pitman, Scientific and Technological Options Assessment (STOA): Feasibility of censoring and jamming pornography and racism in informatics, Draft Final Report, PE 166 658, Luxemburg, Mai 1997[7]:
- Der STOA-Report befaßt sich mit der technischen Möglichkeit, pornographische und rassistische Inhalte aus dem Internet herauszufiltern. Er kommt zu dem Ergebnis, daß eine rein automatisierte Filterung nicht zum Erfolg führen kann und stellt mehrere Szenarien für den Einsatz von Filtersystemen vor.
- Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in den audiovisuellen und Informationsdiensten, Dok. KOM(96)483 endg. vom 16.10.1996.[8]

---

3 http://www2.echo.lu/legal/de/internet/communic.html

4 http://www2.echo.lu/legal/de/internet/wp2de.html

5 http://www2.echo.lu/legal/de/internet/resolde.html

6 Allerdings befinden sich die meisten Hersteller von Filtersystemen außerhalb der EU.

7 Teile zitiert in http://www.inet-one.com/cypherpunks/dir.97.08.28-97.09.03/msg00149.html.

8 http://www.echo.lu/legal/de/internet/gpde-toc.htm

- In diesem Grünbuch werden viele Aspekte im Zusammenhang mit der Bekämpfung der Verbreitung von menschenverachtenden und jugendgefährdenden Inhalten über verschiedene Medien wie Fernsehen und Internet untersucht. Das Grünbuch war Grundlage für einen breit angelegten Konsultationsprozeß[9], der u.a. zur Einrichtung des "Aktionsplans zur Förderung der sicheren Nutzung des Internet“ führte. Auf dem Grünbuch basiert auch die Empfehlung 98/560/G des Rates vom 24. September 1998 zur Steigerung der Wettbewerbsfähigkeit des europäischen Industriezweigs der audiovisuellen Dienste und Informationsdienste durch die Förderung nationaler Rahmenbedingungen für die Verwirklichung eines vergleichbaren Niveaus in bezug auf den Jugendschutz und den Schutz der Menschenwürde, EG-Abl L 270/48 vom 7.10.98.
- "Mißbrauch Internationaler Datennetze“, Bericht der Expertengruppe an die G8-Minister und Regierungsberater für Wissenschaft und Technologie (Carnegie-Gruppe), Rom, 17.10.97.[10]
- Eine Expertengruppe aus Juristen und Informatikern aus den G8-Staaten hat in diesem Bericht die Untersuchungsergebnisse über die gegenwärtige Situation bei der Nutzung des Internet und vergleichbarer Datennetze mit dem Schwerpunkt auf ihren potentiellen Mißbrauch zusammengefaßt. In vier Bereichen werden Gegenmaßnahmen vorgeschlagen:
  - Sensibilisierung und Aufklärung,
  - Einsatz technischer Mittel,
  - Rolle der Informations- und Kommunikationswirtschaft sowie
  - rechtliche Maßnahmen.
- Es wird auf weiteren Forschungsbedarf hingewiesen.
- Dritter Zwischenbericht der Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft: Zum Thema Kinder- und Jugendschutz im Multimediazeitalter, Bundestagsdrucksache 13/11001, 4. Mai 1998:
- Der Bericht befaßt sich mit Jugendschutz ganz allgemein und geht dabei auf die historische Entwicklung der verschiedene Medien und die Praxis in verschiedenen Nationen ein. Technische Schutzmöglichkeiten werden kurz angesprochen. Im Bereich des digitalen Fernsehens werden Ergebnisse einer Untersuchung mit Befragung und Praxistest vorgestellt. Abschließend werden Empfehlungen für medienpädagogische Maßnahmen gegeben.
- Lorrie Faith Cranor, Paul Resnick, Danielle Gallo: "Technology Inventory: A Catalog of Tools that Support Parents' Ability to Choose Online Content Appropriate for their Children“, Dezember 1997, überarbeitet September 1998.[11]
- In dem Dokument wird ein Überblick über die existierende Software gegeben, die Eltern dabei unterstützt, geeignete, kind- und jugendgerechte Inhalte von Online-Diensten und Internet auszuwählen. Die Autoren konzentrieren sich rein auf den technischen Ansatz; generelle Aussagen zum Problem "Jugendschutz im Internet“ werden nicht gegeben. Die Tests der Softwareprodukte ergeben, daß es zur Zeit kein perfekt funktionierendes System gibt.

9 http://www.echo.lu/legal/de/internet/gpconsult.html.

10 http://www.iid.de/iukdg/carnegie_d.html

11 http://www.research.att.com/projects/tech4kids/:

Die technischen Lösungsansätze für Filterung weisen einige Strukturen auf, die verwandt mit anderen Projekten sind. Sobald sich eine Filterung an Metainformationen orientiert, gehören dazu insbesondere verschiedene Projekte des World Wide Web Consortium (W3C) in Betracht, das an Standardisierungen für das WWW arbeitet:

- *Platform for Internet Content Selection* (PICS)[12]: Aufgrund von Metainformationen in bezug auf eine Webseite können Filterungen vorgenommen werden. PICS wird in Abschnitt 4.4 ausführlich vorgestellt.
- *Resource Description* Framework (RDF)[13]: RDF soll eine Infrastruktur zur Verfügung stellen, die den Austausch von Metainformationen über verschiedene Web-basierte Dienste ermöglicht. Die Entwicklung ist noch nicht abgeschlossen.
- *Digital Signature Initiative* (DSig)[14]: Das Projekt DSig soll es dem Abrufer ermöglichen, durch digitale Signaturen die Authentizität von Webinhalten oder zugehörigen Metainformationen zu erkennen.
- *Platform for Privacy Preferences* (P3P)[15]: P3P erlaubt anhand der Metainformationen beim Abrufer und beim Anbieter eine automatisierte Aushandlung darüber, welche personenbezogenen Daten der Nutzer dem Anbieter von Webseiten zur Verfügung zu stellen bereit ist. Die Spezifikation liegt in der Version 1.1 vor; es gibt zur Zeit noch keine allgemein verfügbaren Implementierungen.
- Eine Aushandlungskomponente, in diesem Fall zu den Sicherheitsbedürfnissen verschiedener an der Kommunikation Beteiligter, gehört ebenfalls zu den Basisfunktionen des Forschungs- und *Entwicklungsprojektes Sicherheit und Schutz in offenen Datennetzen* (SSONET)[16], das bis zum 31.08.99 an der TU Dresden durchgeführt wird. In dem Projekt wird eine Sicherheitsarchitektur entworfen und prototypisch implementiert.

1.4 Rechtliche Abgrenzung

Die Ansatzpunkte für die vorliegenden Studie liegen im bereits genannten IuKDG. Zur Klärung der Rechtspositionen müssen eine Anzahl anderer rechtlicher Bereiche berücksichtigt werden.

Wir werden daher den Jugendschutz in seiner bisherigen Form darstellen und zeigen, wo er durch das IuKDG ergänzt bzw. verändert wurde.

Dazu werden wir auf strafrechtliche Verbote eingehen, spezielle Regelungen für einzelne Medien nennen und in die Systematik der jugendschutzrechtlichen Vorschriften einführen. Schließlich kann dann gezeigt werden, wie die Regelungen für die neuen Medien in dieses Gerüst passen.

Aus diesen Gesetzen lassen sich Pflichten und Rechte für die beteiligten Rechtssubjekte ableiten.

Diese Aspekte werden im Kapitel "Rechtliche Rahmenbedingungen für Jugendschutz im Internet“ im Detail betrachtet und mögliche Regelungsoptionen zur Anpassung bzw. Erweiterung auf den Jugendschutz in neuen Medien diskutiert.

---

12 http://w3c.org/PICS/.

13 http://w3c.org/RDF/.

14 http://w3c.org/DSig/.

15 http://www.w3c.org/P3P/.

16 http://mephisto.inf.tu-dresden.de/RESEARCH/ssonet/ssonet.html.

In diesem Rahmen kann dann ein technisches System entwickelt werden, das den Jugendschutz gemäß den rechtlichen und auch weiteren gesellschaftlichen und sozialen Anforderungen realisiert.

1.5 Psychologische Aspekte

Die Eingrenzung der jugendgefährdenden Inhalte kann nach psychologischen Kriterien vorgenommen werden. Vorerst sollen die beiden relevanten Bereiche "Sexualität“ bzw. "Pornographie“ und "Gewalt“ bzw. "Gewaltverherrlichung“ und "rassistische Hetze“ unterschieden werden. Subsumiert man für unsere Zwecke "rassistische Hetze“ unter "Gewalt“, so bleiben zwei Hauptbereiche. Diese beiden Bereiche "Sex“ und "Gewalt“ können für Kinder und Jugendliche je nach Ausprägung des Inhaltes als absolut jugendgefährdend eingeschätzt werden. Davon ausgehend läßt sich der Sachverhalt folgendermaßen skizzieren:

Allen Szenarien gemeinsam ist das prinzipiell hohe Gefährdungspotential, das jedoch in den einzelnen Szenarien als unterschiedlich bedrohlich zu bewerten ist.[17]

Bei Themen aus dem sexuellen Bereich besteht die Besonderheit darin, daß je nach Alter eine ganz normale und durchaus entwicklungsförderliche, starke Neugiermotivation besteht. Diese läßt Jugendliche explizit nach auf Sexualität bezogenen Inhalten suchen. Die Problematik liegt dann darin, daß die Darstellung von "unnormalen“, erniedrigenden bzw. pathologischen Sachverhalten und Handlungen in Wort, besonders aber in Bild und Video die Rezipienten überrascht. Kinder und Jugendliche verfügen nicht über die passenden Abwehrmechanismen, um solche Inhalte verarbeiten zu können. Deshalb werden sexuell-erotische Inhalte, ganz besonders jedoch anstößige Darstellungen durch das Jugendschutzgesetz Kindern und Jugendlichen vorenthalten. Diese Schutzfunktion fehlt beim unkontrollierten Internetzugang und kann deshalb zu schweren "Verletzungen“ führen.

Bei Gewaltdarstellungen ist die Sachlage ähnlich. Einen Unterschied kann man allerdings in der Neugiermotivation vermuten. Die Neugiermotivation nach sexuellen Inhalten ist entwicklungspsychologisch anders gelagert als die Neugiermotivation, anderen Leiden zuzufügen und/oder andere leiden zu sehen. Prinzipiell ist jedoch auch diese Neugiermotivation schon im Kinder- und Jugendlichenalter vorhanden, wenngleich die Ausprägung als schwächer einzuschätzen ist.

1.6 Soziale Aspekte

Um einen Einblick in das Problem der Jugendgefährdung zu bekommen, wie es die potentiellen Nutzer des Internet sehen, wurden vier Experten qualitativ interviewt. Es waren dies ein Professor für Informatik (Schwerpunkt Internet), ein Gymnasiallehrer (Fachbereich Computer), eine Publizistikexpertin (Betreuerin von öffentlichen Internetzugängen) sowie eine Sozialarbeiterin (Schwerpunkt Kinder- und Jugendarbeit).

Bezüglich der qualitativen Einschätzung des tatsächlichen Umfangs des Jugendgefährdung durch Inhalte des Internet lassen sich verschiedene Bereiche unterscheiden:

- Unkontrollierte Internetnutzung.
- Sozial kontrollierte Internetnutzung.
- Mischformen.

Bei unkontrolliertem Internetzugang liegt ein hohes Gefährdungspotential vor. Der Jugendschutz ist hier dramatisch in Frage gestellt. Die Abwesenheit von sozialer und

17 Steigernd für die Gefährdung in beiden Fällen wirkt die hohe Aufgeschlossenheit gegenüber neuen Inhalten sowie die hohe technische Expertise jugendlicher Computernutzer.

technischer Kontrolle ist als "worst case“ für den Jugendschutz anzusehen. Bei Abwesenheit von sozialen oder soziotechnischen Kontrollmechanismen müssen Filtertechnologien die Kinder und Jugendlichen vor gefährdenden Inhalten schützen. Während bei manchen Nutzern ein (möglicherweise ungerechtfertigtes) Vertrauen in die Technik besteht, äußern andere, geschulte Nutzer (eventuell übertriebenen) Pessimismus.

Eine Verbesserung der Situation läßt sich nach Meinung der Befragten durch soziale Kontrolle erreichen. Sind Erwachsene anwesend, während Kinder oder Jugendliche im Internet surfen, bestehen kaum Befürchtungen.[18] Viele Eltern vertrauen auch wohl oder übel ihren Kindern, schon nichts "falsch“ zu machen. Hier scheint aber ein gewisses Unbehagen zurückzubleiben.

Die höchsten Erfolgschancen sind offensichtlich soziotechnischen Kontrollmechanismen einzuräumen. So wird z.B. schon die Möglichkeit der Kontrolle der gesehenen Webseiten durch ein Logfile als hilfreich angesehen, in dem alle gewählten Webseiten protokolliert und somit eine zeitlich unabhängige Durchsicht ermöglicht wird. Die individuelle, nutzerorientierte Kombination von Filtertechnologien, sozialer Kontrolle und weiteren technischen unterstützenden Maßnahmen kann deshalb aus Sicht der befragten Nutzer am ehesten Jugendschutz im Internet gewährleisten. Die weiteren Untersuchungen innerhalb dieses Projektes werden dies im Einzelnen diskutieren. Insbesondere aus der Praxiserprobung ist weiterer Aufschluß über diese Aspekte zu erwarten.

1.7 Technische Aspekte

Die Sperrung von jugendgefährdenden Inhalten im Internet wirft eine Anzahl von technischen Problemen auf, die eine Reihe von Problemkomplexen im rechtlichen, gesellschaftlichen und wirtschaftlichen Bereich nach sich ziehen. Technisches Designziel muß sein, den Erziehungsberechtigten eine möglichst paßgenaue Sperrung von Dokumenten nach Kriterien zu erlauben, die von ihnen selbst konfiguriert und dem Entwicklungsstand der Kinder sowie persönlichen Erziehungszielen angepaßt werden kann. Dabei darf diese Sperrfunktion erwachsenen Internetteilnehmern den Zugriff auf das Internet nicht erschweren. Sie sollte außerdem möglichst so beschaffen sein, daß sie nur für den intendierten Einsatzzweck genutzt und nicht für verbotene Vorzensur mißbraucht werden kann.

Im Rahmen dieser Studie werden wir die verschiedenen existierenden Filtermechanismen auflisten und erläutern. Dabei werden wir uns an den verschiedenen Rollen im Internet orientieren. Wichtig ist dabei auch, auf mögliche Gefahren und Nebeneffekte der Anwendung der Technologien zu achten.

1.8 Subjektive Häufigkeit jugendgefährdender Inhalte

Generell kann eine Gefährdung von Jugendlichen nur dann auftreten, wenn sie entsprechende Inhalte tatsächlich zu sehen bekommen. Nun ist eine exakte zahlenmäßige Abschätzung der Anzahl von jugendgefährdenden Seiten im Internet aus zwei Gründen praktisch nicht durchführbar: Zum einen ändert sich das Angebot täglich, zum anderen wäre auch bei einem statischen Internet die Menge der Seiten kaum in sinnvoller Zeit zu zählen und zu klassifizieren.[19]

---

18 Inwieweit dieses Vertrauen gerechtfertigt ist, sei dahingestellt. Ein Befragter war sich zumindest bewußt, daß die bloße Anwesenheit eines Erwachsenen nicht ausreiche, da die Kinder/Jugendlichen auch unter Aufsicht an jugendgefährdende Inhalte gelangen könnten.

19 Immerhin gibt es verschiedene statistische Ansätze über das Internet (vgl. z.B. http://www.internet-shop.de/stati/indexstati.html); diese beziehen sich allerdings auf den Gesamtumfang und nicht auf die jugendgefährdenden Anteile. Auch die Bundesprüfstelle für jugendgefährdende Schriften (BPjS) hat einige Seiten und Server indiziert; sie arbeitet allerdings

Es kann allerdings anhand von vielen Beispielen gezeigt werden, daß der Kontakt mit potentiell jugendgefährdendem Material im Rahmen eines normalen Umgangs mit dem Internet leicht und zufällig möglich ist; ein unkontrollierter Umgang mit dem Medium "Internet“ birgt also ein nicht zu vernachlässigendes Gefährdungspotential für Kinder und Jugendliche.

Einen qualitativen Überblick über das Ausmaß der Informationsflut, die das Internet bietet und für die eine Kontrollmöglichkeit gefunden werden muß, zeigt die Momentaufnahme einer Suchmaschine[20]:

- AltaVista, www.altavista.de, 18. Januar 1999
  - Datenbankeinträge: über 140 Millionen Seiten
  - Einfache Suche nach "sex“: über 15 Millionen Seiten, davon viele mit erkennbarem erotisch-sexuellen Inhalt
  - Suche mit AltaVista Family Filters: über 14 Mio. Seiten, ausgefiltert werden nur Seiten mit explizitem Auftreten eines Begriffes aus der Sperrliste
  - Reduktion auf deutsche Angebote: etwa 2 Millionen Treffer.

Es ist anzunehmen, daß ein großer Teil dieser Seiten wegen der vielen möglichen Bedeutungen des englischen Wortes "sex“ keinerlei jugendgefährdendes Potential haben. Nimmt man aber nur an, daß zehn Prozent der so gefundenen Seiten für Kinder ungeeignet sind – eine Betrachtung der ersten hundert Treffer deutet auf einen deutlich höheren Anteil hin – so läßt sich immer noch eine so große Menge von potentiell jugendgefährdenden Seiten konstatieren, daß die Gefährdung keinesfalls als unerheblich eingestuft werden kann.

1.8.1 Auffinden durch "Zufallstreffer“

Das gezielte Auffinden potentiell jugendgefährdender Seiten ist einfach: Direktes Suchen mit einer der gängigen Suchmaschinen führt zu Tausenden von Treffern (s.o.), die zu einem nicht geringen Teil direkt zugänglich sind.

Auch ohne Absicht ist es jedoch möglich, Seiten mit erotisch-sexuellen oder auch pornographischen Inhalten angezeigt zu bekommen.

1.8.1.1 Werbung

Eine Möglichkeit dazu ist Werbung auf "harmlosen“ Seiten.

So hatte z.B. der Telefonverzeichnisanbieter *teleinfo* (http://www.teleinfo.de) einige Zeit Werbung für ein Angebot eingeblendet, das erotische Bilder beinhaltete (inzwischen ist sie durch andere Werbung ersetzt).

Von der Seite der BILD-Zeitung ist über deren eigene Seite "Cyber-sexy“ eine direkte Verzweigung auf einen amerikanischen Pornographie-Anbieter möglich, der zwar zugangsbeschränkt ist, aber auch in den zugänglichen Teilen potentiell jugendgefährdende Darstellungen enthält.[21]

---

nur auf Antrag und führt keine eigenen Suchen durch. Eigene Recherchen führen die Strafverfolgungsbehörden nur für nach § 184 StGB strafbare Inhalte, also z.B. Kinderpornographie durch. Diese stellen aber nur einen sehr kleinen Anteil des jugendgefährdenden Materials dar.

20 Dabei finden Suchmaschinen nicht einmal alle Seiten, z.B. nicht bei Zugangsbeschränkung, Eintrag nach Robot Exclusion Protocol o.ä.

21 Hier wäre es auch für Erwachsene komfortabel, diese Bilder ausfiltern zu können.

Auf einer Informationsseite über Telefontarife (http://www.teltarif.de) fand sich am 20.4.1999 die in der folgenden Abbildung dargestellte Werbung, die weiterführt auf ein Zeitschriftenangebot, das einen Internet-Erotik-Führer enthält (Abb. 1-1).

Auch wenn diese deutschen Angebote nicht als jugendgefährdend einzustufen sind, ermöglichen sie über die enthaltene Werbung einen indirekten Zugang zu anderen, problematischeren Angeboten.

Abb. 1-1: Werbung bei www.teltarif.de

1.8.1.2 Suchvorgänge

Suchvorgänge nach harmlosen Begriffen können Verweise auf pornographische Seiten liefern. Dies geschieht zum einen über zufällige Wortgleichheiten. Es werden aber häufig auch absichtlich durch den HTML-Befehl "keyword“ mehrdeutige oder auch unzutreffende und irreführende Schlüsselwörter hinzugefügt:

- "http://sex.erotikline.de“ hat als keyword "schwanger“;
- "http://www.peepshow-online.de“ hat als keywords "amateurphotos“, "jutta“, "kostenlos“.

1.8.1.3 News und Mail

In vielen News-Groups tauchen periodisch Werbenachrichten für Erotik oder Pornographie auf. Ein Beispiel aus der Gruppe *de.etc.finanz* ist der folgende Text:

Betreff: ABSOLUTELY TO SEE
Datum: Fri, 12 Mar 1999 16:38:48 GMT
Von: Ace@acme.com (Ace)
Firma: acme
Foren: de.etc.finanz.misc
100% ANONYMOUS, NO CREDIT CARD, NO SUBSCRIPTION, NO PASSWORD, NO CENSURING
100% ANONIMO, NO CARTA di CREDITO, NO SOTTOSCRIZIONI, NO PASSWORD, NO CENSURA
Italian
www.thirdsex.com

Die Beiträge enthalten z.T. sogar Verweise auf Internet-Seiten, die bei einigen Programmen selbsttätig den Internet-Browser starten und entsprechende Seiten aufrufen. Diese Funktion ist nur mit größerem Aufwand abzuschalten oder zu unterbrechen. Ähnliches gilt auch für E-Mail, insbesondere die verschiedenen Mailinglisten, da deren Adressen häufig öffentlich verbreitet werden. Dort taucht häufig "Spam“ (E-Mails unerwünschten Inhalt) mit entsprechenden Werbebotschaften auf.

1.8.2 Zugangsbeschränkungen

Eine Möglichkeit zur Reduktion des Zugriffs von Jugendlichen auf gefährdendes Material sind Zugangskontrollen für entsprechende Seiten. In vielen Ländern sind solche Kontrollen wegen existierender Altersbeschränkungen für Pornographie gesetzlich vorgeschrieben. Der Umfang des freigegebenen Materials und die Art der Zugangskontrolle wird jedoch sehr verschieden definiert. So reicht z.B. in den USA die Angabe einer gültigen Kreditkartennummer als "Age verification“ aus, hingegen ist in Deutschland ein Identitätsbeweis z.B. in Form der vollständigen Adresse und einer Ausweiskopie üblich.

Die Zugangskontrollen werden häufig nicht vom Anbieter der Pornographie selbst implementiert, sondern von Dienstleistern realisiert. Diese führen dann die Überprüfung der Identität und gegebenenfalls die Erhebung von Gebühren durch und veranlassen die Freischaltung – meist gleich für eine Reihe von Anbietern.

Deutsche Anbieter fordern bei der kostenpflichtigen Anmeldung meist eine Ausweiskopie; die daraufhin ausgestellte Benutzerkennung erlaubt den Zugriff auf viele Erotikseiten. Hier werden auf der Eingangsseite zwar die große Anzahl der Angebote erläutert, allerdings gibt es weder Bilder noch detaillierte Beschreibungen. Damit folgen diese Seiten der deutschen Gesetzgebung.

Ausländische Anbieter verfahren technisch gesehen nach demselben Prinzip. Allerdings reicht hier häufig schon eine Kreditkartennummer aus, um die Freischaltung bzw. die Ausstellung des für den Zugang benötigten Paßwortes zu veranlassen. Außerdem werben die Anbieter bereits auf ihren Eingangsseiten – also vor Aufruf der Zugangskontrolle – mit Bildern mit eindeutig pornographischem oder gewalttätigem Inhalt.[22]

In beiden Fällen dient die Zugangskontrolle weniger dem Jugendschutz als der Erhebung von Gebühren.

1.9 Überblick über Initiativen und Organisationen

Dieser Abschnitt gibt einen ersten Überblick über aus unserer Sicht wichtige Initiativen und Organisationen, die sich mit dem Thema Jugendschutz im Internet und seinen Aspekten

[22] Z. B. http://www.bizar.net

auseinandersetzen. Auch geben wir – soweit uns bekannt – den Stand der öffentlichen Diskussion zu manchen der besprochenen Initiativen und Organisationen wieder.

Fast alle Initiativen haben Webseiten im Internet. Daher lassen sich die meisten der Informationen an Ort und Stelle anhand der angegebenen Internetadresse nachlesen.

1.9.1 Initiativen der EU

Auf der Ebene der Europäischen Union beschäftigen sich mehrere Initiativen mit dem Thema "Jugendschutz im Internet“.

1.9.1.1 Best Use – "promoting best use, preventing misuse“

Um einen Schutz vor illegalen und schädigenden Inhalten im Internet zu schaffen, wird mit dem Projekt "Best Use“ der Europäischen Union[23] versucht, ein größeres Bewußtsein unter Eltern, Lehrern, der Öffentlichkeit und bei Herstellern für praktische Handlungsmöglichkeiten zu vermitteln. Diese Initiative berücksichtigt das Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in den audiovisuellen und Informationsdiensten, die Diskussion über illegale und schädigende Inhalte im Internet und begleitet den "Aktionsplan zur Förderung der sicheren Nutzung des Internet“. Auf der Webseite wird Informationsmaterial, insbesondere für Eltern und Lehrer, zur Verfügung gestellt. Neben der Einführung in das Thema mit rechtlichen und politischen Aspekten wird ein Überblick über Filtersoftware gegeben und auf Hotlines und andere Projekte verwiesen.

1.9.1.2 Aktionsplan zur Förderung der sicheren Nutzung des Internet / INCORE (Internet Content Rating for Europe)

Der Internet Action Plan[24] ("Aktionsplan zur Förderung der sicheren Nutzung des Internet“) ist ein mehrjähriges Programm der Europäischen Gemeinschaft und besteht aus vier Teilen. Neben dem Aufbau von Hotlines, Sensibilisierungs- und flankierenden Maßnahmen wird auch der Teil der Inhaltsfilterung bearbeitet. Für diesen Schwerpunkt wurde das Projekt INCORE (Internet Content Rating for Europe) ins Leben gerufen, in dem eine Machbarkeitsstudie für ein europäisches System mit (First-Party-)Rating von Inhalten erarbeitet und ein generisches Rating- und Filtersystem geschaffen werden soll, das für europäische Nutzer leicht einsetzbar ist. Der Bereich des WWW wird dabei von der Internet Watch Foundation (IWF)[25] bearbeitet. Ende 1999 soll die Machbarkeitsstudie abgeschlossen sein. Integriert werden sollen Testergebnisse von verschiedenen Systemen.

Um einen internationalen Standard zu entwickeln, haben sich Ende April 1999 die deutschen und britischen INCORE-Mitglieder in der ICRA (Internet Content Rating Alliance) mit Kollegen aus den USA, Australien, Kanada, Japan und Singapur zusammengeschlossen. Ergebnisse über ein mögliches Filterverfahren, das allen Kriterien von INCORE genügen soll, liegen noch nicht vor.

---

23 Vgl. http://www2.echo.lu/best_use/best_use.html.

24 Siehe http://www2.echo.lu/iap/.

25 Siehe http://www.internetwatch.org.uk/.

1.9.2 Australische Initiative

Australien hat im Mai 1999 ein sehr weitgehendes Gesetz zur Kontrolle von Internetinhalten beschlossen.[26] Am 01.01.2000 tritt die vorwiegend gegen pornographische Inhalte gerichtete Regulierung in Kraft, die der *Australian Broadcasting Authority* das Recht gibt, Internetprovider aufzufordern, binnen 24 Stunden Inhalte vom Netz zu nehmen oder den Zugang zu ihnen zu sperren, sofern sie sich auf einer ausländischen Website befinden. Dies soll pornographische Angebote, Anleitungen zum Bau von Bomben und andere illegale Inhalte betreffen. Angebote, die als "Nur für Erwachsene“ klassifiziert werden, dürfen nur Volljährigen zugänglich gemacht werden. Ziel des Gesetzes ist es, die australischen Bürger und vor allem die Kinder vor illegalen und anstößigen Inhalten schützen.

Gegen das Gesetz formiert sich eine breite Front von Interessengruppen aus der Wirtschaft, Aktivisten und Bürgerrechtlern.[27] Der Protest richtet sich gegen eine ganze Reihe von Aspekten des Gesetzes:

- Das Gesetz soll den Zugang zu schwer jugendgefährdenden Materialien[28] für alle Bürger verbieten und den Zugriff auf jugendgefährdende Materialien[29] auf Erwachsene beschränken.
- Die Kosten für die Implementierung des Gesetzes sollen die Zugangsanbieter tragen.
- Die Klassifizierung von Material soll unter anderem automatisch auf der Basis eines Schlüsselwortsystems erfolgen. Die Liste der gefilterten Schlüsselwörter ist noch nicht offengelegt, wurde aber durch differentielle Analyse von gefilterten und ungefilterten Seitenzugriffen teilweise ermittelt.[30]

Erste Untersuchungen von Experten prophezeien, daß das Gesetz untauglich sei, seinen intendierten Zweck zu erfüllen.[31]

1.9.3 Jugendschutz und Medienpädagogik

Die aufgelisteten Jugendschutzinitiativen sind aus den verschiedensten Quellen finanziert und organisiert. Ihnen gemeinsam ist es jedoch, den Jugendschutz als umfassende Aufgabe im Zusammenspiel von Technik, organisatorischen Randbedingungen und Medienpädagogik zu betrachten.

---

26 Gesetzestext verfügbar unter http://www.ozemail.com/~mbaker/amended.html, Zusammenfassung http://gomed.rodos.net/censor/bill-summary.html. Siehe auch Florian Rötzer: "Filtern für die Bürger“, 01.04.99, http://www.heise.de/tp/deutsch/inhalt/te/2705/1.html.

27 Electronic Frontiers Australia, http://www.efa.org.au/Campaigns/99.html.

28 "X and RC (refused classification) rated material.“

29 'R rated material.'

30 Eine vorläufige Liste dieser Schlüsselwörter ist unter http://www.anatomy.usyd.edu.au/danny/freedom/censorware/ifilter.html abrufbar.

31 http://www.securitysearch.net/search/papers/bsaprobs.htm, http://www.gtlaw.com.au/pubs/newdarkage.html.

1.9.3.1 jugendschutz.net[32]

Jugendschutz.net ist eine gemeinsame Stelle der Jugendministerien der Länder, die für die Beachtung des Jugendschutzes in neuen Informations- und Kommunikationsdiensten sorgen soll. Zielrichtung sind dabei die Mediendienste, also Angebote an die Allgemeinheit. Sie wirkt außerdem als Kontrollinstanz (vgl. Kapitel "Rechtliche Rahmenbedingungen für Jugendschutz im Internet“).

Die Initiative wurde 1997 in Konsequenz des Mediendienste-Staatsvertrags gegründet, um die Durchsetzung der dort enthaltenen Jugendschutzbestimmungen zu unterstützen. Sie widmet sich verschiedenen Bereichen.

So wurde z.B. ein Programm entwickelt, das nach potentiell jugendgefährdenden Inhalten sucht ("Crawler“). Damit wird – soweit möglich – eine Sichtung des Internetangebots vorgenommen, um bei Auffinden eines jugendgefährdenden Angebots entsprechende Maßnahmen einleiten zu können.

Diese Maßnahmen beginnen nach eigener Aussage jeweils mit einer Kontaktaufnahme mit dem Anbieter; sie gehen weiter mit der Kontrolle von vorgenommen Änderungen und enden – falls erforderlich – in einer Weitergabe der Informationen an zuständige Behörden.[33] Aus diesen Kontakten entstehen häufig auch Beratungsverhältnisse, in denen Jugendschutz.net die Anbieter bei der Einrichtung geeigneter Schutzmaßnahmen berät. jugendschutz.net ist jedoch nicht unumstritten.[34]

1.9.3.2 jugendmedienschutz.de[35]

Diese Initiative will eine Basis zu allen Aspekten des Jugendschutzes bieten. Sie ist innerhalb des Fördervereins für Jugend und Sozialarbeit e.V. angesiedelt. Hier wird eine große Palette an Informationsmöglichkeiten geboten, unter anderem eine aktuelle Broschüre "Gute Seiten, schlechte Seiten“ – Jugendmedienschutz und Internet[36].

---

32 jugendschutz.net
Fritz-Kohl-Str. 24, 55122 Mainz, E-Mail: buero@jugendschutz.net ,
Telefon: 06131/3285-20 oder -25, Fax: 06131/3285-22
http://www.jugendschutz.net/

33 Nach Angabe von Jugendschutz.net ist dieser Fall allerdings bisher nicht aufgetreten; die meisten Anbieter sind kooperativ. Allerdings besteht u.U. von Seiten des Anbieters kein Interesse, sich gerichtlich über die von ihren Inhalten ausgehende Jugendgefährdung auseinanderzusetzen, weil sie die Wirkung in der Öffentlichkeit fürchten.

34 Siehe Diskussionen in einschlägigen News-Groups und Mailinglisten.

35 Jugendmedienschutz.de im
Förderverein für Jugend und Sozialarbeit e.V., Rungestr. 20, 10179 Berlin,
Fax 030/279 01 26
http://www.jugendmedienschutz.de/ oder http://www.jugendschutz.org/

36 Gute Seiten – Schlechte Seiten – Jugendmedienschutz und Internet, herausgegeben vom Förderverein für Jugend und Sozialarbeit e.V., bestellbar über fjs, Rungestr. 20, 10179 Berlin.

1.9.3.3 Jugendschutz.de [37]

Hier handelt es sich um den losen Zusammenschluß mehrerer deutscher Fach- und Landesstellen zum Kinder- und Jugendschutz sowie der Bundesarbeitsgemeinschaft Kinder- und Jugendschutz. Einer der Schwerpunkte ist dabei die Medienpädagogik.

Gemeinsam wird ein Materialdienst angeboten, außerdem ein Veranstaltungskalender. Es gibt Arbeitsstellen in Baden-Württemberg, Bayern, Hamburg und Schleswig-Holstein. Jede dieser Stellen bietet wiederum ein eigenes Programm an Veranstaltungen, Informationen und Aktivitäten an.

1.9.3.4 Medienrat Internet[38]

Der Medienrat Internet ist ein Zusammenschluß von Privatpersonen, die nicht nur den Jugendschutz im Fokus haben, sondern ganz allgemein mit Aufklärung und technisch-organisatorischen Mitteln einen rechtssicheren Raum für den freien Fluß von Informationen im Internet anstreben. Entsprechend wird eine solche Diskussion durch Informations- und Diskussionsbeiträge z.B. auf ihrer Internetseite angestoßen.

1.9.3.5 Initiativen gegen Kindesmißbrauch und Kinderpornographie

Es gibt eine Reihe von Initiativen, die sich mit diesen Problemfeldern auseinandersetzen. Da es sich hier um strafbare (nicht nur jugendgefährdende) Inhalte handelt, sind z.T. auch staatliche Behörden daran beteiligt. Beispiele sind

- *Netz gegen Kinderpornographie*[39].
- *KidCareNet*[40].
- *Antiporno.de*[41].
- *Kommissariat 343, Polizeipräsidium München: Polizeistreife im Internet*[42].

1.9.4 Inhaltsanbieter

Bei den folgenden Initiativen geht es um die Wahrung der Interessen der Anbieter von Internetinhalten. Es wird also die Schnittmenge zwischen gesetzlich erlaubter Zugangskontrolle und möglichst weiter Verbreitung zur kommerziellen Nutzung gesucht.

1.9.4.1 Selbstkontrollorganisationen

Mehrere Bundesverbände der Inhaltsanbieter, zwei Online-Service-Provider und Unternehmen mit Multimediageschäftsfeldern haben am 09. Juli 1997 den eingetragenen Verein *Freiwillige Selbstkontrolle Multimedia-Diensteanbieter* e.V. (FSM)[43] gegründet.

---

37 Bundesarbeitsgemeinschaft Kinder- und Jugendschutz:
Haager Weg 44, 53127 Bonn
Tel. 0228/29 94 21, Fax 0228/28 27 73
http://www.jugendschutz.de/

38 http://www2.medienrat.de/medienrat/index.html

39 http://www.heise.de/ct/Netz_gegen_Kinderporno/

40 http://www.kidcarenet.de/index.htm

41 http://www.anti-kinderporno.de/

42 http://www.polizei.bayern.de/ppmuc/wir/k345.htm

Der Verein arbeitet auf Grundlage eines Schiedsgerichts, das eingehende Beschwerden bearbeitet und über deren Richtigkeit entschiedet. Die Mitglieder[44] haben sich verpflichtet, den Entscheidungen des Schiedsgerichtes Folge zu leisten.

Nicht direkt mit dem Internet, aber mit Randbereichen der neuen Medien beschäftigen sich

- die *Freiwillige Selbstkontrolle Fernsehen* (FSF)[45],
- die *Unterhaltungssoftware Selbstkontrolle* (USK)[46] und
- die *Freiwillige Selbstkontrolle der Filmwirtschaft* (FSK)[47].

1.9.4.2 Zugangskontrollsysteme

Auch im Interesse des Jugendschutzes und gleichzeitig im Interesse der Anbieter nicht jugendfreier Internetinhalte arbeiten die verschiedenen Zugangskontrollsysteme. Dabei stehen dort meist kommerzielle Interessen dahinter – sollen doch nicht nur jugendliche Surfer ferngehalten werden, sondern auch jene, die nicht für das Angebot bezahlen wollen.

Solche Systeme bieten zumindest in Deutschland einen soliden Zugangsschutz mit Identitätsüberprüfung; allerdings nur im strikten Sinne des Jugendschutzes. Inhaltsabstufungen werden dort nicht vorgenommen. Die angeführten Systeme sind in Deutschland angesiedelt; daher halten sie sich an die deutsche Gesetzeslage.

- *Jugendschutz.com*[48]:
  - Einführung in die Problematik.
  - Angebot von entsprechend geschützten Webservern.
- *X-ID*[49]*:*
  - Zugangskontrolle durch Vergabe einer Benutzerkennung
- *X-Check online*[50]*:*
  - Zugangskontrolle durch Vergabe einer Benutzerkennung

Natürlich gibt es solche Anbieter auch außerhalb Deutschland; ein in den USA besonders verbreiteter Service, der z.T. auch von deutschen Pornographie-Anbietern genutzt wird, ist *Adult Check*[51].

---

43 Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e. V. (FSM), z. Hd. Herrn Dr. Müller-Using, Deutsche Telekom AG, Postfach 2000, 53105 Bonn, Tel: 0228/1817330 http://www.fsm.de/

44 Bundesverband Deutscher Zeitungsverleger (BDZV), Bundesverband Informationsanbieter Online (BVIO), Deutsches Network Information Center e. G. (DeNIC), Deutscher Multimedia Verband (dmmv), Deutsche Telekom AG, Electronic Commerce Forum (eco), Gruner + Jahr Fernsehproduktions-GmbH, MSN LLC (MSN -The Microsoft Network, Online Pro Dienste GmbH & Co, Pro Sieben Media AG, Unterhaltungssoftware Selbstkontrolle (USK), Verband Deutscher Zeitschriftenverleger (VDZ), Verband Privater Rundfunk und Telekommunikation (VPRT)

45 http://www.fsf.de/

46 http://www.usk.de/, ebenfalls im Förderverein für Jugend und Sozialarbeit e.V. organisiert.

47 http://www.fsk.de/, Seite noch im Aufbau.

48 http://www.jugendschutz.com/

49 http://www.x-id.de/intern/besucher.htm

50 http://www.x-check.de/

1.9.5 Spezielle Angebote für Kinder

Eine andere Herangehensweise an die Schaffung von Randbedingungen für die sinnvolle Nutzung des Internet durch Kinder und Jugendliche sind spezifisch auf diese Zielgruppe abgestimmte und aufbereitete Inhalte. Ganze Listen finden sich z.B. bei Yahoo.[52] Im folgenden zeigen wir die Abbildungen einiger Eingangsseiten.

1.9.5.1 Das Kindernetz des Südwestrundfunks[53]

51 http://www.adult-check.com/

52 http://www.yahoo.de/Gesellschaft_und_Soziales/Kulturen_und_Gruppen/Kinder/Links_fuer_Kinder/

53 http://www.kindernetz.de/kik/index.html

1.9.5.2 Kidnet.de[54]

1.9.5.3 Kidsnet[55]

54 http://www.kidnet.de/

55 http://www.kidsweb.de/

1.9.5.4 Pixelkids[56]

1.9.6 Kurzübersicht

Es gibt eine sehr große Zahl von Informations- und Diskussionsangeboten zum Thema Jugendschutz und sicheres Internet für Kinder und allen Teilaspekten.

Die folgende Liste zeigt einen sortierten Ausschnitt.

1.9.6.1 Gesetze und Richtlinien

- Gesetze zum Jugendmedienschutz (Jugendschutz.org)
- Informations- und Kommunikationsdienste-Gesetz – IuKDG (Netlaw)
- Gesetzliche Bestimmungen zum Jugendmedienschutz (Universität Hamburg)

1.9.6.2 Rechtliche Aspekte

- Prof. Dr. Ulrich Sieber, Universität Würzburg: Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I) und (II)

1.9.6.3 Soziale Aspekte

- Medienpädagogik Uni Hamburg: Internetangebote für Kinder
- Internet und Soziale Arbeit – Kehr & Jansen
- Cyber-Rights: Censorship in law and practice

1.9.6.4 Technische Aspekte

Softwareüberblicke und -bewertungen

56 http://www.pixelkids.de/

- Technology Inventory (Cranor et al: AT&T Lab und Univ. of Michigan)
- SMART PARENTS: Softwareverzeichnis
- EPICReport – "Faulty Filters“
- Sicherheit, Datenschutz, Jugendschutz und Internetanbindung (Rittershofer)
- CyberPatrol 'Intolerance': Correctness or Bigotry?

Spezielle Suchmaschinen

- GO Network – Search with GOguardian (Infoseek)
- Lycos Search Guard
- Altavista Family Filter

Ratingssysteme

- PICS – Platform for Internet Content Selection
- RSACi – Recreational Software Advisory Council on the Internet
- SafeSurf
- evaluWEB
- ESRBI – Entertainment Software Rating Board Internet

1.9.6.5 Initiativen

Europäische Union

- Promoting best use, preventing misuse – Home page
- Action Plan on promoting safer use of the Internet
- INCORE – Internet Content Rating for Europe
- Internet content – EU Action
- Audiovisual Policy – Politique audiovisuelle – Politik im audiovisuellen Bereich

USA

- America Links Up!
- SMART PARENT-HOME
- Safety Tips for Kids on the Internet (FBI Educational Web Publication)
- Electronic Policy Network – Center for Media Education
- InternetTrend Watch for Libraries: February/March 1998:
- Alexander/Tate: Teaching Web Evaluation: Meeting the Challenge
- Censorware.org
- EPIC: ACLUv. Reno II – Challenge to Internet Censorship
- INTERNET FREE EXPRESSION ALLIANCE
- The National Fraud Information Center: Internet Fraud Watch
- Peacefire Censorware Pages

Deutschland

a) Öffentliche Hand

- Jugendschutz NRW: Internet
- Stellungnahme Berliner DSB zum Grünbuch der EU über Jugendschutz
- Jugendschutz-Richtlinien der Landesmedienanstalten

b) Jugendschutzinitiativen

- jugendschutz.net: Initiative der Jugendministerien der Länder
- Jugendmedienschutz
- Jugendschutz (Anwender) (Ausschnitt aus privat erstelltem Internet-Kurs)
- Medienrat Internet
- Kinder- und Jugendschutz (www.jugendschutz.de)

c) Initiativen gegen Kinderpornographie und Kindermißbrauch

- KidCareNet, gemeinsam gegen Kindesmißbrauch und Gewalt gegen Kinder
- Netz gegen Kinderporno (Heise Verlag)

d) Selbstkontrollinitiativen

- Freiwillige Selbstkontrolle Fernsehen
- USK – Unterhaltungssoftware Selbstkontrolle
- Freiwillige Selbstkontrolle Multimedia e.V.

e) Zugangskontrollen

- Jugendschutz.com
- x-Check
- X-ID
- Adult Check

f) Web-Sites für Kinder/Eltern

- Kidnet
- Das Kindernetz des Südwestrundfunks
- KIDSWEB
- Pixelkids

1.10 Rollen und Begriffe

Dieser Abschnitt definiert vorab einige wichtige Begriffe und Rollen, die wir im weiteren in dieser Studie immer wieder verwenden werden. Die Definitionen enthalten z.T. Vorgriffe auf die folgenden Kapitel, in denen alle technischen und organisatorischen Vorgänge im Detail diskutiert werden. Für die Begriffe werden wichtige Referenzkapitel und -abschnitte angegeben.

1.10.1 Begriffe

Um Jugendschutz im Internet technisch wirkungsvoll zu unterstützen, ist eine Sortierung der Inhalte nach ihrem jugendgefährdenden Potential erforderlich. Die Durchführung einer solchen Sortierung (Filterung) wiederum erfordert, daß die Inhalte

- in Kategorien eingeordnet,
- gekennzeichnet und
- ausgewählt

werden.

Dabei sind die Personen bzw. Instanzen, die die verschiedenen Vorgänge veranlassen oder durchführen, meist unterschiedlich.

Jeder dieser Vorgänge kann sich dabei auf ganze Server beziehen, auf Unterverzeichnisse oder einzelne Seiten, Dokumente oder Dateien. Jeder der drei Aspekte kann auf unterschiedliche Art und Weise und von verschiedenen Personen bzw. Instanzen mit jeweils spezifischen Vor- und Nachteilen durchgeführt werden.

Bevor die genannten Begriffe in den folgenden Kapiteln mit Inhalt gefüllt und diskutiert werden, soll zuerst formal geklärt werden, was mit diesen und anderen für den Fortgang wichtigen Begriffen gemeint ist.

1.10.1.1 *Kategoriensystem*

- Bedeutung:
  System von Kategorien, in die eine Internetseite eingeordnet wird.
- Häufig auch:
  Ratingsystem, im folgenden werden beide Begriffe synonym verwendet
- Referenz: Abschnitt 4.5.

1.10.1.2 *Einordnung*

- Bedeutung:
  Einordnung einer Internetseite in ein oder mehrere vorhandene Kategoriensysteme.
- Häufig auch:
  - *Einstufung* oder *Rating*, dieser Begriff wird im weiteren als Synonym zur Einordnung aufgefaßt.
  - *Bewertung*, dann aber wertneutral zu verstehen; dieser Begriff führt allerdings zu Mißverständnissen, er wird daher nicht weiter verwendet.
- Referenz: Abschnitt 4.3.1.

1.10.1.3 *Kennzeichnung*

- Bedeutung:
  Vermerk, der die Beschreibung einer Internetseite enthält. Der Begriff "Kennzeichnung“ allein macht keine Aussage darüber, wo dieser Vermerk zu finden ist.
- Häufig auch:
  Labeling
- Referenz: Abschnitt 4.3.2.

1.10.1.4 *Auswahl*

- Bedeutung:
  Entscheidung, ob eine bestimmte Internetseite anzuzeigen ist oder nicht; Auswahl erfolgt aufgrund der zur Beschreibung verwendeten Kategoriensysteme; technisch wird sie

durch Abfrage der Kennzeichnung realisiert. Die Auswahl beruht auf der Bewertung der Kategorien durch den Endnutzer. Auch die Wahl des Kategoriensystem ist bereits Teil der Auswahl.

- Häufig auch:
  Filterung, da die Auswahl der eigentliche Vorgang des Durchlasses oder Sperrens ist. Da mit Filterung aber auch der Gesamtkomplex bezeichnet wird, ist der Begriff eher ungeeignet und wird im weiteren nicht in dieser spezifischen Bedeutung verwendet.
- Referenz: Abschnitt 4.3.3.

1.10.2 Rollen

In bezug auf die Bereitstellung von Inhalten im Internet zum öffentlichen Abruf lassen sich verschiedene Rollen identifizieren. Die wichtigsten Rollen sind im folgenden für den Dienst WWW dargestellt. Bei anderen Diensten kann man ähnliche Rollen bestimmen. Die Rollenbestimmung ist notwendig, um die Beziehungen zwischen den handelnden Personen, ihre Verantwortlichkeiten, Interessen, Rechte und Pflichten analysieren zu können. Auch müssen die möglichen Auswirkungen der Inhaltsfilterung auf die unterschiedlichen Rollen untersucht werden. Die vorgestellten Rollen werden nicht notwendigerweise durch verschiedene Personen wahrgenommen, sondern können teilweise zusammenfallen.

1.10.2.1 Die Rollen im Anbieterbereich

Der *Content-Provider* (Inhaltsanbieter) ist derjenige, der die inhaltliche Verantwortung für das Dokument trägt, das zur Verfügung gestellt werden soll. In der Regel handelt es sich hierbei um den Verfasser.

Teilweise werden auch Inhalte mehrerer Verfasser zusammen zur Verfügung gestellt. Für solche Herausgeberschaften findet im Internet nicht unbedingt eine inhaltliche Kenntnisnahme oder Prüfung statt, sondern manchmal werden ähnlich dem News-Dienst Inhalte verschiedener Autoren auf einer Webseite zusammengefaßt. In einigen Fällen gibt es eine Redaktion oder Moderatoren.

Der *Presence-Provider* stellt den Rechner für die Inhalte des Content-Providers, die Anbindung ans Internet und den Abrufmechanismus zur Verfügung. Somit führt er das Web-Hosting durch.

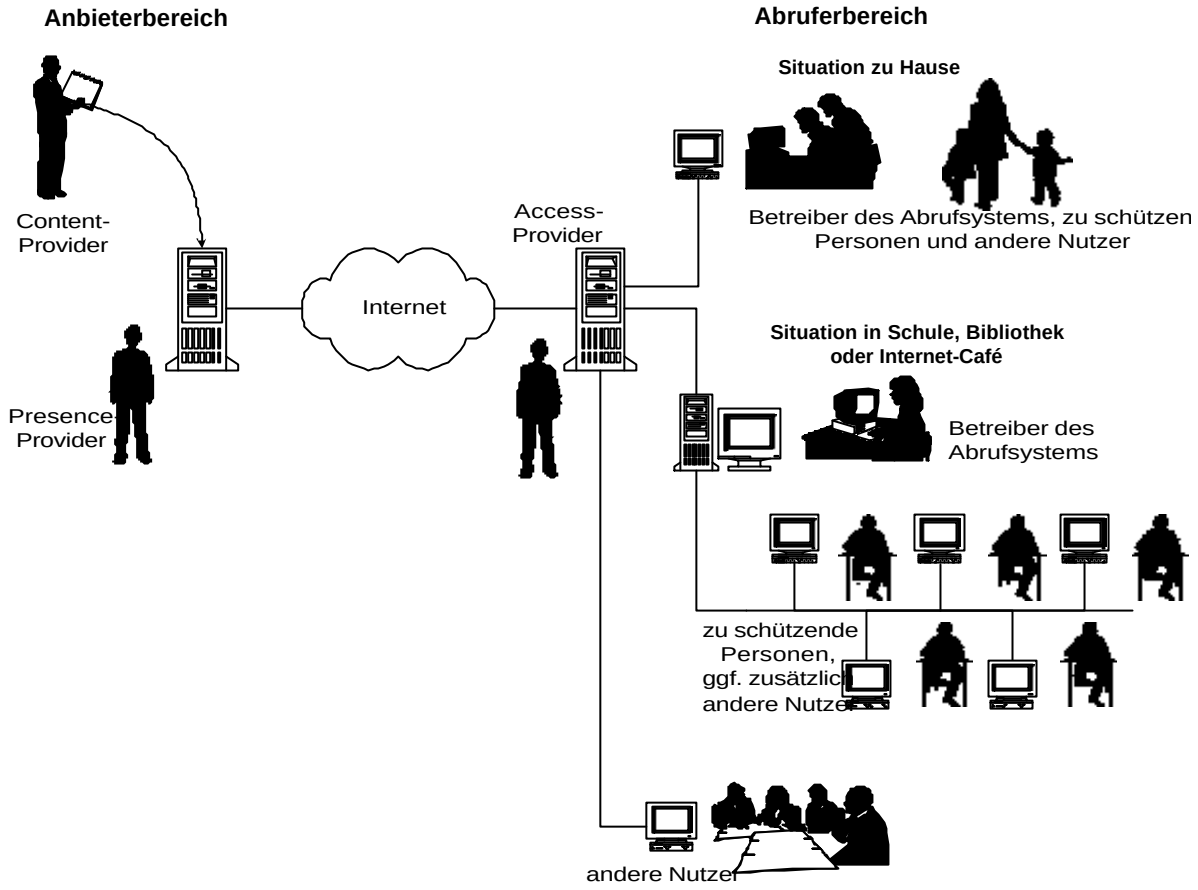


Abb. 1-2: Rollen im Internet

1.10.2.2 Die Rollen im Abruferbereich

Der *Access-Provider* stellt den Internetzugang für die Abrufer zur Verfügung und baut die Verbindung zu den angegebenen Webservern auf. Hierbei bedient er sich der Struktur des Internet, bei dem die Datenpakete über weitere Zwischenrechner geschickt werden. Die Abrufer sind in der Regel bei ihrem Access-Provider angemeldet und bezahlen ihn für seine Dienstleistung.

Beim Abrufer muß man die *zu schützenden Personen*, also Kinder und Jugendliche, von den *anderen Nutzern* auf demselben System unterscheiden. Die Hard- und Software für die Abrufer wird vom *Betreiber des Abrufsystems* zur Verfügung gestellt und administriert. Dabei handelt es sich zum einen um die erzieherischen Verantwortungsträger (zu Hause meist die Eltern; in der Schule die Lehrer), zum anderen um Betreiber von Internet-Cafés oder Internetzugängen in Bibliotheken, sofern diese nicht ebenfalls zu den oben genannten Access-Providern zu zählen sind. Das Abrufsystem besteht teilweise lediglich aus einem einzelnen Rechner, doch gerade im Bereich von Schulen oder Internet-Cafés gehören mehrere Computer, meist gebündelt hinter einem Proxy, zu dem Abrufsystem.

1.10.2.3 Die Rollen im Filterbereich

Sofern man davon ausgeht, daß für ein Filtern mit Verfahren zur Einordnung von Inhalten gearbeitet wird,[57] kommen weitere Rollen hinzu.

---

57 Die Notwendigkeit dazu ergibt sich aus der Untauglichkeit anderer Verfahren, wie sie in Abschnitt 4.2 dargestellt wird.

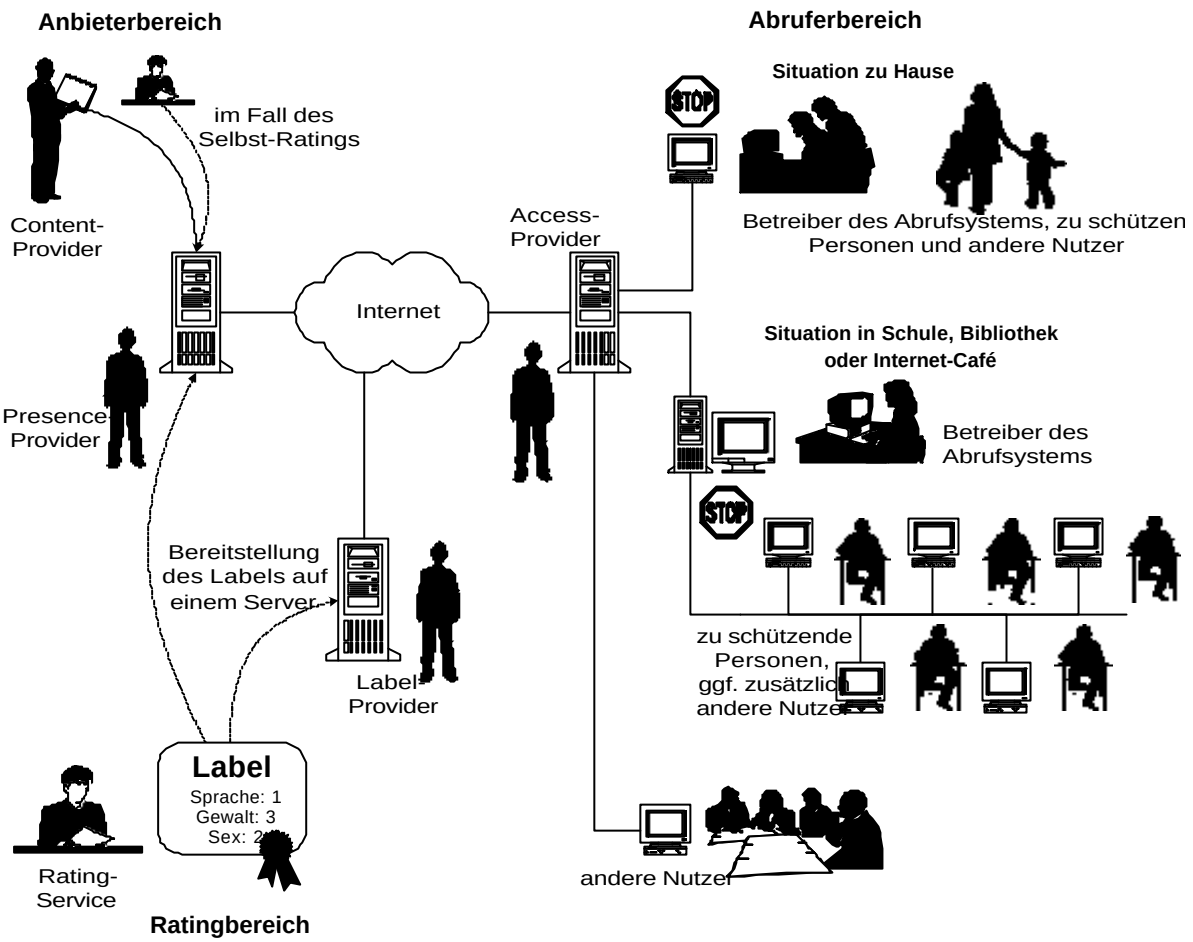


Abb. 1-3: Rollen im Internet bei Verwendung von Filterung

Rollen der Infrastruktur

Entwickler von Kategoriensystemen legen fest, welche Kategorien und Einordnungsregeln gelten können, und propagieren sie, damit sie beispielsweise in gängige Browser eingebaut werden und einen hohen Grad an Verbreitung erreichen.

Hersteller von Filtersystemen entwickeln und vertreiben Systeme, die sich für eine Filterung eignen. Dies sind zumeist Softwarelösungen, doch sind auch Kombinationen aus Hard- und Software denkbar.

Mit Hilfe von digitalen Signaturen könnte die Authentizität der Zuordnung von Labels zu Webseiten bestätigt werden. Dafür wären weiterhin *Zertifizierungsinstanzen* notwendig.

Rollen zur Realisierung des Ratings

Der *Rating-Service* weist den Inhalten Werte in bezug auf verschiedene Kategorien zu. Hierbei ist denkbar, daß die Autoren, dritte (unabhängige) Instanzen, die Internet-Community oder die Abrufer Einordnungen vornehmen.

Die Datensätze mit den Einordnungsinformationen (Labels) werden von *Label-Providern* zum Abruf zur Verfügung gestellt. Diese Informationen können in der Webseite des eigentlichen Inhalts integriert oder auf gesonderten Servern verteilt gespeichert sein. Im zweiten Fall muß für den Abruf einer Webseite zusätzlich eine Verbindung zum Label-Server aufgebaut und die Einordnungsinformation eingeholt werden.

Rollen zur Auswertung der Labels

Wer *Filterkriterien definiert*, legt fest, wonach gefiltert wird. Diese Filterkriterien werden in der Regel im Bereich der Abrufer definiert, beispielsweise durch die Erziehungsberechtigten. Doch dies könnte ebenso als Dienst von dritten Instanzen angeboten werden.

Beim *Betreiber des Filtersystems* kann es sich ebenfalls um einen Erziehungsberechtigten handeln, der die Software am Abrufsystem installiert und konfiguriert. Wiederum ist es jedoch möglich, daß das Betreiben eines Filters von einem Access-Provider wahrgenommen wird.

1.10.2.4 Sonstige Rollen

Im Gegensatz zu den Herstellern der Filtersysteme wurden *die Hersteller und Betreiber der sonstigen eingesetzten Hard- und Software* sowohl auf Anbieter- als auch auf Abruferseite sowie bei der Übertragung im Internet bislang nicht gesondert erwähnt, da sie in bezug auf diese Studie nur wenig spezielle Bedeutung haben.

Überall präsent ist die Rolle der *Angreifer*, denn in jedem der vorgestellten Bereiche können sie versuchen, das Verfahren zu stören.

2 Rechtliche Rahmenbedingungen für Jugendschutz im Internet

2.1 Einführung

Im folgenden soll der rechtliche Rahmen für den Jugendschutz, besonders unter dem Blickwinkel der Anwendung von Filtertechnologien im Internet dargestellt werden.

Folgende verschiedenen Rechtssubjekte sind vom Problemkreis Jugendschutz im Internet betroffen:

- die zu schützenden Kinder und Jugendlichen;
- die Eltern;
- staatliche Bildungsinstitutionen, vor allem Schulen;
- sonstige staatliche und nichtstaatliche Institutionen, die Rechner zur Verfügung stellen, mit denen auf das Internet zugegriffen werden kann (z. B. Internet-Cafés und öffentliche Bibliotheken);
- die Provider, wo erforderlich getrennt nach den Rollen Content-Provider, Presence-Provider (i. S. v. Betreiben von Web-Hosting) sowie Access-Provider;[58]
- Dritte, soweit ihre Rechte durch Filtermaßnahmen beeinträchtigt werden können.

2.2 Übersicht: Regelungen zum Jugendschutz in den neuen Medien

Im Bereich des Jugendmedienschutzes lassen sich im wesentlichen drei unterschiedliche Regelungsbereiche unterscheiden[59]:

- strafrechtliche Verbote;
- das Verfahren zur Indizierung von schädigenden Inhalten nach dem Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte;
- die Vorschriften zur Beschränkung der Verbreitung von Filmen, Videokassetten und anderen Bildträgern nach dem Gesetz zum Schutz der Jugend in der Öffentlichkeit;

2.2.1 Strafrechtliche Verbote

Zunächst gibt es allgemeine strafrechtliche Verbotsnormen, die sich an jedermann richten. Nicht alle derartigen strafrechtlichen Normen sollen ausschließlich dem Jugendschutz dienen. Rein jugendschutzrechtlich motiviert sind lediglich § 184 Abs. 1 Nrn. 1 bis 5 StGB[60]. Jugendschutz als ein zu schützendes Rechtsgut spielt auch eine Rolle bei § 86 (Verbreiten von Propagandamitteln verfassungswidriger Organisationen), § 86a (Verwenden von Kennzeichen verfassungswidriger Organisationen), § 130 Abs. 2 (Verbreiten

58 Zur technischen Definition dieser Rollen siehe Abschnitt 1.10.

59 Vgl. Bernhard Schraut, Jugendschutz und Medien, 1993, S. 27 ff.

60 Vgl. Lenckner, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 25. Aufl. 1997, § 184 Rn. 3.

volksverhetzender Schriften), § 131 (Verbreiten von Gewaltdarstellungen) und den übrigen Tatbeständen von § 184 StGB (Verbreitung pornographischer Schriften)[61].

Verboten ist zum einen die Verbreitung der in den einzelnen Vorschriften näher beschriebenen Informationen, also ihre Weitergabe mit dem Ziel, sie einem größeren Personenkreis zugänglich zu machen[62], oder das öffentliche Zugänglichmachen sowie schließlich bestimmte Vorbereitungshandlungen zu diesen beiden Varianten (vgl. § 86 Abs. 1, § 86a Abs. 1 Nr. 1, § 130 Abs. 2 Nr. 1 Buchst. a), b), d); § 131 Abs. 1 Nr. 1, 2, 4 sowie § 184 Abs. 3 StGB). Von dem mit Strafe versehenen Verbot nicht erfaßt ist hier die individuelle, nicht auf weitere Öffentlichkeit abzielende Weitergabe an eine andere Person. In einer zweiten Spielart ist das Zugänglichmachen der Informationen an eine Person unter 18 Jahren (§ 130 Abs. 2 Nr. 1 Buchst. c); § 131 Abs. 1 Nr. 3 sowie § 184 Abs. 1 Nr. 1 StGB) sowie bei einfacher Pornographie (deren Weitergabe an Erwachsenen nicht verboten ist) eine solche Präsentation etc. strafbar, bei der auch Jugendliche Kenntnis davon bekommen können (§ 184 Abs. 1 Nrn. 2 bis 5 StGB). In § 131 Abs. 2 und § 184 Abs. 2 ist auch die Verbreitung der bezeichneten Inhalte über den Rundfunk unter Strafe gestellt. § 184 Abs. 6 Satz 1 enthält eine Ausnahme für den Personensorgeberechtigten im Hinblick auf die Strafbarkeit nach Abs. 1 Nr. 1. Entsprechendes gilt für § 131 Abs. 1 Nr. 3 nach § 131 Abs. 4.

Außer aus den Vorschriften des StGB kann sich die Strafbarkeit auch aus Vorschriften des sog. Nebenstrafrechts ergeben. Dazu gehören z. B. die Strafvorschriften des Gesetzes über die Verbreitung jugendgefährdender Schriften und Medieninhalte und des Gesetzes zum Schutz der Jugend in der Öffentlichkeit.

2.2.2 Indizierungsverfahren nach dem GjS

Neben den strafrechtlichen Vorschriften, die ein bestimmtes Verhalten generell verbieten und damit (auch) dem Jugendschutz dienen, verfolgt vor allem das Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte (GjS) Ziele des Jugendschutzes. Das Gesetz sieht vor, daß Schriften, die geeignet sind, Kinder oder Jugendliche sittlich zu gefährden, in eine Liste aufzunehmen sind. In § 1 Abs. 1 Satz 2 GjS werden als ausdrückliche Beispiele genannt: unsittliche, verrohend wirkende, zu Gewalttätigkeit, Verbrechen oder Rassenhaß anreizende sowie den Krieg verherrlichende Schriften. Das Gesetz zielt dabei in erster Linie auf solche Schriften und Medieninhalte ab, die die oben dargestellten Straftatbestände noch nicht erfüllen.

Die Aufnahme in die Liste, die in einem detailliert geregelten Verfahren von der Bundesprüfstelle nach § 8 GjS ausgesprochen wird, zieht Verbreitungsverbote nach den §§ 3 und 4 sowie eine Beschränkung der Werbung gemäß § 5 GjS nach sich. Die Verbreitungsverbote der Nr. 1 bis 3 des § 3 GjS entsprechen den Formulierungen in § 184 Abs. 1 Nr. 1, 2 und 3a StGB (zu § 3 Abs. 1 Nr. 4 GjS sogleich unter IuKDG). Das Verbreitungsverbot außerhalb von Geschäftsräumen nach § 4 Nrn. 1 bis 4 GjS entspricht § 184 Abs. 1 Nr. 3 StGB. Es zielt darauf ab, jugendgefährdende Schriften nur noch in Geschäftsräumen, also in Ladengeschäften zu verbreiten.[63] Schließlich darf nach § 5 GjS einerseits nicht damit für eine Schrift geworben werden, daß ein Verfahren zu ihrer Aufnahme in die Liste anhängig gewesen sei oder ist, andererseits dürfen in die Liste aufgenommen Schriften nicht öffentlich beworben werden. Zuwiderhandlungen gegen die Vertriebs- und Werbeverbote werden nach § 21 GjS als Straftaten verfolgt. Die Tathandlungen entsprechen denen in § 184 StGB; hinzuweisen ist insbesondere auf die Strafbarkeit des

---

61 Vgl. Rainer Scholz, Jugendschutz, Textausgabe mit Erläuterungen, 3. Aufl. 1999, § 1 GjS, Anm. 1.

62 Vgl. Lenckner, oben Fn. 60, Rn. 57.

63 Vgl. Scholz, oben Fn. 61, § 4 GjS, Anm. 1.

Zugänglichmachens indizierter Schriften für Kinder und Jugendliche (§ 21 Abs. 1 Nr. 1 GjS). Im Unterschied zu den o. g. Vorschriften des StGB ist auch fahrlässige Tatbegehung möglich (vgl. § 21 Abs. 3 GjS).

Neben den in die Liste aufgenommenen Schriften unterliegen nach § 6 GjS auch sogenannte schwer gefährdende Schriften den dargestellten Vertriebs- und Werbebeschränkungen. Dies sind Schriften, die den Tatbestand der §§ 130 Abs. 2 ,131, oder 184 StGB erfüllen oder die offensichtlich geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden. Die Regelungstechnik des § 6 hat zur Folge, daß sich diejenigen, die einschlägige Schriften vertreiben wollen, nicht auf die Indizierung alleine verlassen können. Vielmehr müssen sie prüfen, ob die zum Vertrieb bestimmten Schriften und Medieninhalte nicht den Tatbestand der genannten Strafnormen oder des § 6 Nr. 3 GjS erfüllen.[64] Liegen bereits rechtskräftigen Urteile vor, die feststellen, daß eine Schrift pornographisch ist oder den in § 130 Abs. 2 oder § 131 des StGB bezeichneten Inhalt hat, so ergibt sich daraus zweifelsfrei, daß diese Schriften den Beschränkungen der §§ 3 bis 5 GjS unterliegt (vgl. § 18 Abs. 1 Satz 2 GjS). Schließlich greifen die Beschränkungen auch für Schriften, die ganz oder im wesentlichen inhaltsgleich mit einer indizierten Schrift sind, ohne daß diese in die Liste aufgenommen werden müßten (vgl. § 18 Abs. 1 Satz 1 GjS).

Die Bundesprüfstelle wird nur auf Antrag tätig. Zur Stellung des mit einer schriftlichen Begründung versehenen Antrags berechtigt sind die obersten Jugendbehörden der Länder (dies sind die zuständigen Landesministerien), die Landesjugendämter, die Jugendämter und das Bundesministerium für Familien, Senioren, Frauen und Jugend. Die Bundesprüfstelle entscheidet im gesetzlichen Regelfall in einer mündlichen, nicht öffentlichen Verhandlung mit einer Besetzung von zwölf Personen, wobei die einzelnen Beisitzer den im Regelungskontext einschlägigen Kreisen (§ 9 Abs. 2 und § 9a GjS) entstammen. Die Entscheidung ist ausnahmsweise im vereinfachten Verfahren ohne mündliche Verhandlung in einen Dreier-Gremium zulässig, wenn die Voraussetzungen des § 1 offenbar gegeben sind (§ 15a Abs. 1 GjS). Die Beteiligten des Verfahrens (Antragsteller, Verleger und Verfasser) sind von der beabsichtigten Indizierung zu benachrichtigten. Die Benachrichtigung muß ihnen im Regelfall mindestens zwei Wochen vor der mündlichen Verhandlung, bei Durchführung des vereinfachten Verfahrens mindestens eine Wochen vor der Entscheidung zugehen. Ein Dreier-Gremium ist auch für die vorläufige Anordnung zur Aufnahme einer Schrift in die Liste zuständig (§ 15 GjS). Allerdings ist die zeitliche Dauer einer vorläufigen Anordnung beschränkt auf höchstens zwei Monate; die vorläufige Anordnung darf nur ergehen, wenn die endgültige Anordnung offenbar zu erwarten ist und die Gefahr besteht, daß die Schrift kurzfristig in großem Umfang vertrieben wird. Als Beispiel für solche Fällen werden Produkte des Zeitschriftenhandels genannt.[65] Die Mitglieder der Bundesprüfstelle sind von Weisungen frei; ihre Beurteilungen sind gerichtlich nur eingeschränkt nachprüfbar.

Im Verfahren nach dem GjS kommt der Liste der indizierten Schriften eine erhebliche Bedeutung zu. Die Liste ist vom Vorsitzenden der Bundesprüfstelle zu führen. Eine Schrift ist unverzüglich nach der Entscheidung in die Liste aufzunehmen bzw. aus ihr zu streichen. Beides ist im Bundesanzeiger bekanntzumachen. Daneben hat der Vorsitzende der Bundesprüfstelle die Liste in einer übersichtlichen Zusammenstellung zu veröffentlichen und für Nachträge und eine Neuauflage zu sorgen. Dies geschieht durch Veröffentlichung im Börsenblatt des Deutschen Buchhandels, in der Fachzeitschrift "der neue Vertrieb“ und dem von der Bundesprüfstelle herausgegebenen "BPjS-Aktuell“. Die Liste ist für die Stellen, die Medien vertreiben, von erheblicher Bedeutung, da sie über die Strafbarkeit bestimmter Handlungen entscheidet.

---

64 Vgl. Scholz, oben Fn. 61, § 6 GjS, Anm. 1.

65 Scholz, oben Fn. 61, § 15 GjS, Anm. 1.

2.2.3 Das GjS und die neuen Medien

Mit dem Informations- und Kommunikationsdienste-Gesetz (IuKDG) wurden 1997 auch neue Jugendschutzregelungen eingeführt. Der Ansatz dabei war es, in das GjS eine Klarstellung aufzunehmen, daß sich die Indizierung auch auf Inhalte von Webseiten beziehen kann.[66]

Art. 4 Nr. 1 IuKDG aktualisiert zunächst den strafrechtlichen Schriftenbegriff in § 11 Abs. 3 StGB und weitet ihn ausdrücklich auf Datenspeicher aus. Damit ist sichergestellt, daß die oben aufgeführten Straftatbestände, die an den Schriftenbegriff anknüpfen, zweifelsfrei auch auf Informationen zur Anwendung kommen, die in digitalisierter Form über Rechnernetze verschickt oder abgerufen werden.[67] Eine entsprechende Klarstellung wurde auch in § 1 Abs. 3 GjS aufgenommen.[68] Die gesetzliche Klarstellung war deswegen geboten, weil der alte Schriftenbegriff des Strafgesetzbuches und des GjS von den Strafgerichten und den Verwaltungsgerichten unterschiedlich ausgelegt wurde.[69]

In § 3 Abs. 1 GjS wurde außerdem eine neue Nr. 4 aufgenommen, wonach eine indizierte Schrift nicht "durch elektronische Informations- und Kommunikationsdienste verbreitet, bereitgehalten oder sonst zugänglich gemacht werden“ darf (vgl. Art. 6 Nr. 3 Buchst. a) IuKDG). Die Vorschrift hat für sich genommen keinen über die Nummern 1 und 2 hinausgehenden Regelungsgehalt.[70] Sie ist aber erforderlich als Anknüpfungspunkt für die in § 3 Abs. 2 GjS durch Art. 6 Nr. 3 Buchst. b) IuKDG eingefügte Einschränkung des Verbreitungsverbotes. Das Verbot der Verbreitung indizierter Schriften durch elektronische Informations- und Kommunikationsdienste greift dann nicht, "wenn durch technische Vorkehrungen Vorsorge getroffen ist, daß das Angebot oder die Verbreitung im Inland auf volljährigen Nutzer beschränkt werden kann.“ Die Vorschrift soll eine übermäßige Einengung der Informationsmöglichkeiten für Erwachsene aus Informations- und Kommunikationsdiensten vermeiden.

Nach Art. 6 Nr. 5 IuKDG haben die gewerbsmäßigen Anbieter elektronischer Informations- und Kommunikationsdienste einen Jugendschutzbeauftragten zu bestellen, wenn sie allgemein angeboten werden und jugendgefährdende Inhalte enthalten können. Die neu als § 7a in das GjS eingefügte Vorschrift zielt darauf ab, durch dezentrale Beauftragte, die vor Ort die Interessen des Jugendschutzes wahrnehmen, eine dem Jugendschutz förderliche Infrastruktur zu schaffen. Der Diensteanbieter kommt seiner Verpflichtung auch dadurch nach, daß er einer Organisation der freiwilligen Selbstkontrolle zur Wahrnehmung der Aufgaben des Jugendschutzbeauftragten verpflichtet. Eine solche Organisation ist z. B. die *Freiwilligen Selbstkontrolle Multimedia* (FSM).

---

66 Mitte 1998 waren bereits 200 Online-Titel indiziert, vgl. Bettina Brockhorst, BPjS aktuell, 4/98, S. 8.

67 Vgl. Hans-Jörg Albrecht, in: BT-Drucks. 13/11001, S. 65.

68 Vgl. Art. 6 Nr. 2 IuKDG. Zur Abgrenzung gegenüber dem MDStV wurden aus dem Anwendungsbereich des GjS allerdings ausdrücklich Mediendienste im Sinne von § 2 MDStV ausgenommen.

69 Vgl. Scholz, oben Fn. 61, § 1 GjS, Anm. 9. Das OLG Stuttgart, NStZ 1992, S. 38, wandte in einer strafrechtlichen Entscheidung den Schriftenbegriff auch auf die Inhalte des Bildschirmtextes an. Die Verwaltungsgerichte verlangten dagegen eine dingliche Verkörperung der Information, z. B. OVG Münster, NJW 1993, S. 1494.

70 Vgl. Begründung des Gesetzentwurfs, BT-Drs. 13/7385, S. 37 f.; Scholz, oben Fn. 61, § 3 GjS, Anm. 6; jugendschutz.net, Erläuterung zum GjS, Nr. 5, http://jugendschutz.net/Pornographie_im_Internet1.html.

Die Regelung der Länder orientiert sich an den Regelungen aus dem Rundfunkbereich und versucht, den Jugendschutz in den Mediendiensten nach dem gleichen Schema sicherzustellen.

2.2.4 Spezielle Regelungen für Filme, Videokassetten und andere Bildträger

Der dritte Regelungskomplex, in dem sich Vorschriften zum Jugendmedienschutz finden, ist das Gesetz zum Schutz der Jugend in der Öffentlichkeit (JÖSchG). Neben Vorschriften, die den Aufenthalt von Kindern und Jugendlichen an bestimmten Ort, die Ausgabe alkoholischer Getränke, öffentliche Tanzveranstaltungen etc. beschränken, finden sich im JÖSchG auch Regelungen zu Filmveranstaltungen, Videokassetten und vergleichbaren Bildträgern. Entsprechend seiner Zielrichtung, der Durchsetzung des Jugendschutzes, und im Hinblick auf das verfassungskräftige Verbot der Vorzensur beschränkt das JÖSchG die Zulässigkeit öffentlicher Filmveranstaltungen (§ 6) bzw. das öffentliche Zugänglichmachen bespielter Videokassetten und vergleichbarer Bildträger (§ 7) nicht generell. Wird sichergestellt, daß bei öffentlichen Filmveranstaltungen ausschließlich Erwachsene anwesend sind bzw. daß bespielte Videokassetten und vergleichbaren Bildträger ausschließlich Erwachsenen in der Öffentlichkeit zugänglich gemacht werden, so sieht das Gesetz keine Einschränkungen vor. Lediglich der Zugang von Kindern und Jugendlichen zu öffentlichen Filmveranstaltungen bzw. das öffentliche Anbieten bespielter Videokassetten etc. an dieselben ist rechtlich beschränkt. Kindern und Jugendlichen darf die Anwesenheit bei öffentlichen Vorführungen gestattet werden, wenn die Filme für die jeweilige Altersstufe freigegeben worden sind. Zur Verfügung stehen nach § 6 Abs. 3 Satz 1 JÖSchG fünf Freigabekennzeichnungen:

- freigegeben ohne Altersbeschränkung
- freigegeben ab sechs Jahren
- freigegeben ab zwölf Jahren
- freigegeben ab sechzehn Jahren
- nicht freigegeben unter achtzehn Jahren.

Kindern unter sechs Jahren ist die Anwesenheit grundsätzlich nur in Begleitung eines Erziehungsberechtigten gestattet.

Nach dem Wortlaut des Gesetzes obliegt die Einstufung von Filmen der obersten Landesbehörde, also dem zuständigen Landesministerium. Eine Entscheidung der Behörden wird faktisch durch ein Gutachten der freiwilligen Selbstkontrolle der Filmwirtschaft (FSK) ersetzt. Die FSK ist eine seit 1949 existierende Gründung der Spitzenorganisationen der Filmwirtschaft mit Sitz in Wiesbaden. Verfahren und Kriterien der Filmprüfung sind in den Grundsätzen der FSK niedergelegt. Neben Vertretern der Film- und Videowirtschaft wirken an der Filmbewertung Vertreter das Bundesministeriums des Innern, des Bundesministeriums für Familien, Senioren, Frauen und Jugend, der obersten Landesjugendbehörden, der Kultusministerien der Länder, der evangelischen und katholischen Kirche sowie der jüdischen Religionsgemeinschaft und des Bundesjugendringes mit. Die obersten Landesjugendbehörden bestellen dabei einen Ständigen Vertreter bei der FSK (vgl. § 3 FSK-Grundsätze). Die Prüfung wird auf Antrag eines Unternehmers, häufig des Filmverleihers, begonnen. Spielfilme werden dabei vom sogenannten Arbeitsausschuß in einer Besetzung mit sieben Mitgliedern geprüft. Gegen die Entscheidung ist Berufung möglich, es prüft dann der sogenannte Hauptausschuß in einer Besetzung mit neun Mitgliedern (vgl. im einzelnen § 5 Abs. 2 und 3 sowie §§ 9 ff. FSK-Grundsätze).

Die sehr offene Formulierung von § 6 Abs. 2 JÖSchG, wonach Filme dann für eine Altersgruppe nicht freigegeben werden dürfen, wenn sie geeignet sind, das körperliche, geistige oder seelische Wohl der Kinder und Jugendlichen zu beeinträchtigen, wird in §§ 2 und 18 der FSK-Grundsätze konkretisiert. Die obersten Landesjugendbehörden sind an das

Gutachten der FSK nicht gebunden; freilich werden sie ihre Entscheidung i. d. R. darauf stützen[71].

Der bei dem Bewertungsverfahren der FSK anwesende Ständige Vertreter der obersten Landesjugendbehörden hat nach § 6 Abs. 2 Satz 2 JÖSchG den Strafverfolgungsbehörden mitzuteilen, wenn in Betracht kommt, daß ein Film, der nicht unter 18 Jahren freigegeben ist, den Tatbestand des § 130 Abs. 2, des § 131 oder des § 184 StGB erfüllt. Allerdings hat das Bundesverfassungsgericht entschieden, daß dieses Mitteilungsverfahren nicht dazu führen darf, daß bereits vor Verbreitung eines Films strafrechtlich gegen denselben vorgegangen wird. Dies würde dem Verbot der Vorzensur widersprechen. [72]

Filme, die das Kennzeichnungsverfahren durchlaufen haben, fallen nicht mehr unter §§ 1 und 11 des GjS.

§ 7 JÖSchG enthält entsprechenden Vorschriften für das öffentliche Zugänglichmachen von bespielten Videokassetten und anderen vergleichbaren Bildträgern. Für die Kennzeichnung der Freigabe für die einzelnen Altersstufen gilt § 6 Abs. 2 und Abs. 3 Satz 1 sowie Abs. 6 JÖSchG. Die Alterseinstufung ist mit einem fälschungssicheren Zeichen vom Inhaber der Nutzungsrechte auf dem Bildträger in deutlich sichtbarer Form anzubringen. Nach § 7 Abs. 3 JÖSchG greifen bei der Einstufung "nicht freigegeben unter achtzehn Jahren“ Vertriebsbeschränkungen, die denen der §§ 3 und 4 GjS entsprechen. Im Gegensatz zur Filmbewertung führt die Bewertung von Videokassetten und vergleichbarer Bildträger nur dann zum Ausschluß der Anwendung des GjS, wenn der Bildträger wenigstens als "freigegeben ab sechzehn Jahren“ eingestuft ist. Bei der Einstufung "nicht freigegeben unter achtzehn Jahren“ ist also eine Indizierung nach dem GjS möglich.

Zuwiderhandlungen gegen die Vorschriften des JÖSchG sind nach § 12 Abs. 1 als Ordnungswidrigkeiten mit einem Bußgeld bis zu 30.000 DM bedroht (§ 12 Abs. 3 JÖSchG). Eine Strafbarkeit im Sinne des GjS kommt nur für Veranstalter oder Gewerbetreibende in Betracht, die entweder durch die Zuwiderhandlung ein Kind oder einen Jugendlichen in seiner körperlichen, geistigen oder sittlichen Entwicklung schwer gefährden oder die die Zuwiderhandlung aus Gewinnsucht begehen oder sie beharrlich wiederholen.

2.3 Schlußfolgerungen

Die Vorschriften zum Jugendschutz führen dazu, daß die Verantwortung für die Einhaltung jugendschützender Maßnahmen (und z. T. auch das Risiko der Strafbarkeit) neben den für die Inhalte Verantwortlichen auch diejenigen trifft, die das front-end kontrollieren. In erster Linie sind dies die Eltern, aber auch die Lehrer bei schulischem Internetzugang und andere Stellen. Diese haben zwar die prinzipielle Möglichkeit, einen Teil der gefährdenden Inhalte mit geeigneter Software zu unterdrücken. Problematisch ist jedoch, daß dies eine erhebliche Kompetenz im Umgang mit Computern erfordert, die nicht immer vorhanden sein wird. Wie die vorliegende Studie zeigt, nehmen auch viele Verantwortliche die jugendgefährdenden Potentiale des Internet nicht wahr oder unterdrücken das Bewußtsein der Gefährdung. Angesichts dessen kann davon ausgegangen werden, daß Minderjährige in nicht unerheblichem Umfang mit jugendgefährdenden Inhalten konfrontiert werden. Die folgenden Kapitel werden zeigen, daß eine technische Unterstützung des Jugendschutzes möglich ist.

71 Jedenfalls bis 1987 soll eine Kennzeichnung noch nie durch eine oberste Landesbehörde selbst vorgenommen worden sein, vgl. Peter Weides, NJW 1987, S. 224, S. 226 f.

72 BVerfGE 87, 209.

3 Soziologische Überlegungen

Die speziellen Charakteristika des Mediums "Internet" stellen den Jugendschutz vor neue Herausforderungen, die in diesem Kapitel aus soziologischer Sicht beleuchtet werden. Die Problematik ist so neu, daß bisher keine empirischen soziologische Untersuchungen vorliegen; daher werden im folgenden die zentralen Aussagen von einem theoretischen Rahmen abgeleitet.

3.1 Jugendschutz und Internet

Jugend wird immer dann zu einem Thema, wenn Jugendliche wahrnehmbar anders handeln, als ihre Eltern im Jugendalter gehandelt haben. Jugend entsteht als ein sozialer Tatbestand, sobald etwas als Jugend kommuniziert wird. Historische und soziologische Untersuchungen zeigen, daß andere Gesellschaften keine Jugend im Sinne einer recht lange währenden Übergangsphase zwischen Kindheit und Erwachsensein kennen.

Unter dem Etikett "Jugendschutz" versorgt sich eine moderne Gesellschaft mit leidlich konsistenten Erwartungstabilisierungen. Anders ist es kaum möglich, beispielsweise den Genuß von Alkohol als unproblematisches Alltagshandeln und zugleich als nicht wünschenswert auszuweisen. Anders ist es auch kaum möglich, einerseits Meinungsfreiheit und den freien Zugang zu beliebigen Mitteilungen zu schätzen und andererseits bestimmte Mitteilungen unter besonderen Bedingungen eben doch vom freien Zugang ausschließen zu wollen. Eindeutige Verbote mögen kurzfristig eine konsistente Sachlage erzeugen, erhöhen jedoch zugleich auf längere Sicht das Risiko, daß bei einem Übertritt von Verboten und der Feststellung, daß die Folgen des Übertritts doch nicht so schlimm wie befürchtet seien, die Normen und Werte nicht einmal mehr zumindest kontrafaktisch gelten. Erschwerend kommt hinzu, daß viele Verstöße keine unmittelbaren Konsequenzen nach sich ziehen oder wenn doch, daß diese dann eher abstrakte Formen annehmen. Es bedarf so gesehen folglich eines immer größeren Aufwands, um neuen Gesellschaftsmitgliedern die Funktion von Verboten zu erklären, die auch dann gelten, wenn niemand zusieht.

Der latent gültige Normen- und Wertekatalog, der nicht vollständig und hochauflösend über das positive Recht abgesichert wird[73], wird beispielsweise in Familien aktualisiert, wenn junge Eltern weitgehend unvorbereitet mit einem Mal eine All-Verantwortung für Kinder übernehmen müssen und ihnen in Konfliktsituationen oftmals nur diejenigen moralischen Muster zur Verfügung stehen, an die sie sich aus ihrer Kinder- und Jugendzeit erinnern. Die Geltung solcher Wertereferenzen wird zudem permanent durch Massenmedien aktiviert, wie etwa durch Nachrichten über kriminelle Ereignisse sowie durch Spielfilme, in denen psychische und soziale Abweichungen und Verfehlungen bearbeitet werden. Nicht nur Eltern, sondern auch Schulrektoren und Staatsanwälte können die aus ihrer Sicht problematischen oder gar kriminellen Inhalte des Internet, so wie sie ihnen zugetragen werden, deshalb nicht in der free-speech-Manier der Internet-Nutzeravantgarde unproblematisiert einfach hinnehmen oder gar feiern, weil sie neben den persönlich-moralischen auch den funktionalen Imperativen der Organisationen, in denen sie Positionen übernommen haben, folgen müssen. Für sie ist das Internet kein Terrain für spielerisch-experimentelle Technik-Adventures, sondern ernstzunehmender Teil ihres Alltags.

Dieser moralisch aufgeladene Wertekatalog wird nun allseits in Anschlag gebracht gegenüber den vermuteten Gefährdungen durch das Internet, solange keine verläßlichen Rechtsfiguren zur Verfügung stehen. Im Bezug zum Schutz von Kindern gegenüber problematischen Inhalten des Internet machen wir es uns in unseren soziologischen Überlegungen leicht:

---

73 ... und auch gar nicht abgesichert werden kann, weil Werte im Sinne eines universalen geheimen Quasi-Vertrags unterhalb der positiv formulierten Verträge "regeln", daß Verträge einzuhalten sind.

Kinder haben eindeutig der Aufsicht ihrer Eltern bzw. der Schule zu unterstehen. Es empfiehlt sich generell nicht, Kinder allein beliebig fernsehen, Märchenkassetten hören oder durch das Internet surfen zu lassen.[74] Wenn nicht einmal die als kindgerecht ausgewiesenen Medien garantiert traumatisierungsfrei ausgelegt sind – einmal ganz abgesehen davon, daß eine Sozialisierung ohne Traumatisierung vermutlich nicht denkbar ist -, dann kann dies vom gesellschaftlichen Universalmedium Internet erst recht nicht erwartet und gefordert werden.

Im Bezug zum Schutz von Jugendlichen ist die Situation dagegen komplizierter zu beurteilen, weil Jugendlichen kognitiv und emotional ein ungleich weitgehenderer Grad an Autonomie zukommt bzw. zuzugestehen ist und Jugendliche in ihren Autonomieübungen, gerade auch im Umgang mit technischen Medien, zu unterstützen sind. Es ist festzuhalten, daß beispielsweise Nacktbilder sowohl im Internet als auch am Zeitschriftenkiosk praktisch ohne besonderen Widerstand zugänglich sind – auch schon in einer Jugendzeitschrift wie der "Bravo". Die Hemmschwelle, einfach mal auf Verdacht "http://www.playboy.com" einzutippen oder in einer Suchmaschine nach "Porno", "XXX" oder "Sex" suchen zu lassen und dann die Treffer abzugrasen, ist als niedriger einzustufen, als in einem Supermarkt in einem der "Männermagazine" zu blättern.[75]

Als weitere besondere Komponente des leichten Zugangs wäre das eher zufällige Gewahrwerden jugendgefährdender Inhalte hervorzuheben. Der Zugang speziell zu Pornovideos ist, sofern das Angebot an Erotikfilmen insbesondere des Privatfernsehens nach Mitternacht Jugendlichen nicht hinreichend attraktiv erscheint, im Internet in Form von WebCam-Peepshows möglich, deren Bezahlung allerdings für Jugendliche erschwerend in der Regel über Kreditkarten geregelt ist. Zu berücksichtigen ist jedoch, daß der Zugang zu Porno- und insbesondere Gewaltvideos (man denke an Splatter-Videos oder japanische Mangas) auf konventionellem Wege für Jugendliche nicht schwierig ist.[76] Für eigentlich größer halten wir deshalb das Problem des Zugangs zu jugendgefährdenden Materialien spezifisch im Internet im Hinblick auf extremistische Schriften: Die gezielte Suche nach typischen Begriffen extremistischen Vokabulars kann hier schnell und leicht zu vollkommen haltlosen Hetzschriften führen. Allerdings wird auch dies wiederum etwas relativiert angesichts der Existenz stadtbekannter Buchläden mit einem spezialisierten Angebot zu politischen, philosophischen oder religiösen Publikationen, die die extremistische Ideologie von in der Regel gezielt knapp gehaltenen Hetzschriften erst vertiefen.

---

74 Uns fallen in den Kinderfilmen von Disney eine ganze Menge an Szenen auf, die bei Kindern zu traumatischen Erlebnissen führen können. Ebenso kann sich die frühe Lektüre von Märchen – man denke allein an "Hänsel und Gretel" oder "Rotkäppchen und der Wolf" problematisch auswirken.

75 Wenn man jugendpolitisch schon die dabei zutage tretenden Bilder als jugendgefährdend einstuft, dann empfiehlt es sich, in einer großangelegten Aufklärungsaktion in Publikumszeitschriften und Zeitungen darauf aufmerksam zu machen, daß die Betreiber solcher Websites die Aktionen ihrer Kunden in den Logdateien mitschneiden und diese Logdateien in der Regel selbstverständlich auch auswerten. Jugendliche (und sicher nicht nur die) sollten wissen, daß sie also nicht unbeobachtet sind, auch wenn sie vielleicht allein im Raum vor dem PC sitzen. Zumal nach einem Besuch einer solchen Website das Risiko groß ist, daß die nächsten Wochen und Monate über eine ganze Zahl an Sexbilder-Lockangeboten per E-Mail eintreffen und somit das Risiko besteht, daß die Eltern zumindest im Nachhinein von den Ausflügen mitbekommen.

76 An Videos für Erwachsene kann ein nicht hinreichend alt erscheinender Jugendlicher über den älteren Bruder des besten Freundes gelangen. Zutritt zu Kinofilmen für Erwachsene verschaffen sich Jugendliche in einem Großkino dadurch, indem sie für einen jugendfreien Film lösen, und nach dem Vorfilm des Erwachsenenfilms, wenn die Türwache fortgegangen ist, den Kinoraum wechseln.

Insofern läßt sich festhalten: Das Internet als neuer Verteilungsweg erleichtert zweifellos in vielen Fällen den Zugang zu Probleminhalten, während hinsichtlich der Inhalte keine spezifisch neue Qualität entsteht.

Analytisch gilt es zunächst zu beachten, daß das Gefährdungspotential des Internet nicht dem Medium selbst anzukreiden ist, weil das einer Verwechslung von Medium und Form gleichkäme. So wenig, wie es dem Medium Telefon (oder deren Betreiber) angelastet werden kann, wenn darüber ein Mord geplant wird, oder dem Medium Bahn (oder deren Betreiber), wenn sie massenhaft Steuerhinterzieher transportiert, kann es dem Internet (oder den Providern) angelastet werden, wenn sozial allgemein Unerwünschtes und Kriminelles sich im Medium des Internet ausformt. Nicht vom Internet gehen etwaige Gefährdungen aus, sondern von dessen Anwendungen. Wenn wir nachfolgend trotzdem von den Gefahren und Risiken des Internet sprechen, so ist dies nur als eine verkürzte Rede zu werten.

Der Grund, daß das Gefährdungspotential speziell des Internet über die Maßen und nachhaltig (nicht zu Unrecht!) hoch eingeschätzt wird, hat seinen Grund darin, daß dieses Medium ganz allgemein für mehr gesellschaftliche Unwägbarkeiten und womöglich für die Reaktivierung bereits stillgelegter Konflikte sorgt. Die diffusen Sorgen, die sich allesamt auf die Paradoxie des Zugleichs von Selbständigkeit und Nichtselbständigkeit beziehen, werden bekämpft durch Übertragungen auf bekannte Konfliktfelder, von denen Jugend, die obendrein mit den neuen Techniken oftmals auch noch umzugehen weiß, besonders geeignet ist, weil sie ohnehin in der Bearbeitung dieser Paradoxie steht. Soziologisch gesehen haben wir Zweifel, ob wirklich speziell die Jugendlichen gemeint sind oder ob sie nicht vielmehr nur in besonderer Weise dafür herhalten müssen, daß sich auf Basis der Internetnutzung sehr viel allgemeinere Veränderungen ankündigen, die ein jedes Gesellschaftsmitglied betreffen.

Diese allgemeinen gesellschaftlichen Entwicklungen lassen sich am Beispiel des Jugendschutzes an zwei Aspekten allerdings besonders klar veranschaulichen:

- Der Umgang mit dem Internet übersteigt die kommunikativen Strukturen von Familien und Organisationen, ist aber durch das Vorhandensein des PC gegeben. Andere Gefährdungen, die durch zum Teil rechtlich-autonomisierte Jugendliche sowie vor allem durch deren selbstbestimmtes Verfügen über Geld in Gang gesetzt wurden, sind mittlerweile akzeptiert. Anders gesagt: Daß Jugendliche mit Geld umzugehen wissen und sich darüber bewußt sind, daß schmerzende Verträge einzuhalten sind, davon darf man mittlerweile ausgehen. Inzwischen sind auch Regeln für den Radio- und Fernsehkonsum gefunden. Daß Jugendliche mit den Risiken des Internet grundsätzlich umzugehen wissen, muß sich erst noch erweisen. Das gleiche gilt für Erwachsene.
- Darüber hinaus werden die gebändigten Risiken für Jugendliche durch Nutzung des Internet womöglich reaktualisert, weil die gesellschaftlich vorhandenen Kommunikationsformen im Universalmedium Internet voll durchgreifen: Man kann im Internet mit wenig Mühen vom heimischen PC aus ebenso direkt Aktien kaufen wie eine unter Umständen riskante politische Kampagne etwa für oder gegen den Einsatz deutscher Soldaten in Jugoslawien starten oder an Diskussionen renommierter Wissenschaftler teilhaben, auch als Jugendlicher. Man kann natürlich ebenso umstandslos zum Opfer von Missionaren oder Kriminellen werden. Man ist mit dem Internet an allem Gesellschaftlichen sehr direkt dran. Es zeigt sich im Internet die volle kommunikative Wucht des gesellschaftlichen "Anything-goes".
- Es sind die großtechnischen Kommunikationssysteme wie das Internet, die die bislang noch nicht industrialisierten, man möchte fast sagen: die gemütlichen, von Raum und Zeit "entbetteten"[77] Bereiche der Gesellschaft industrialisieren.[78]

---

77 Vgl. Giddens, Anthony, 1996: Konsequenzen der Moderne, 1. Auflage, Frankfurt am Main: Suhrkamp.

- Die Veränderung der Kommunikationsmedien verändert die Formen der Interaktionen.[79] Der Standardumgang mit anderen Personen läuft nicht primär über die traditionelle Differenz bekannte/unbekannte Person in direkter Beobachtung von Interaktionen, sondern verlangt eine sehr viel höher ausdifferenzierte Auflösung der gegenseitigen Taxation und des daraus folgenden angemessenen Umgangs. Wir möchten diesen modernen Modus des standardisierten Umgangs, der sich historisch zunächst in den Städten ausbildete[80] und heute im Internet universalisiert ist, als "Vertrauen ohne Zutrauen" bezeichnen.[81] Diesen Modus des Umgangs zu erreichen, bei dem man vor einem Fremden nicht länger einfach wegläuft, sondern ihm erst einmal traut, ohne schon zutraulich zu sein, stellt historisch gesehen hohe Anforderungen an die (nicht nur) von Jugendlichen zu erbringenden Sozialisationsleistungen.[82]

Diese beiden Aspekte, nämlich daß das Internet sowohl als ein Medium für gesellschaftliche Kommunikationen, in denen Menschen einander medienvermittelt begegnen, als auch als eine aktive Maschinerie operiert, die als Eigensinn schöpfend wahrnehmbar wird[83], führen dazu, daß Computer und Internet als "Wunschmaschinen"[84] überhöht oder als "gefährliche Maschinen" diabolisiert werden. Das Internet fungiert in diesem zweifach ausgewiesenen Sinne als ein sehr wirkungsmächtiger Katalysator einer noch einmal zugespitzten Radikalisierung der Moderne. Deshalb wird allenthalben ein so enorm hoher Handlungsdruck verspürt, der nun insbesondere auch die Instrumentarien des Jugendschutzes herausfordert.

Die formelle Kontrollstrategie des Jugendschutzes besteht darin, die junge Generation vor schädigenden oder störenden Einflüssen zu bewahren oder zumindest abzuschirmen. Dieses Ziel ist ein genuin pädagogisches und leitet sich ab von einem spezifischen Jugendverständnis, wie es in der Bundesrepublik in den sechziger und Anfang der siebziger Jahre ausformuliert wurde und das im Grunde unverändert bis heute gilt.

Damals wurde bemerkt, daß die institutionellen Grundlagen des Jugendschutzes auf veralteten Vorstellungen bezüglich der Sozialisationsbedingungen von Jugendlichen aufbauen.[85] Nicht in Frage gestellt wurde, daß Jugend eine besondere Stellung gegenüber

---

78 Vgl. Rost, Martin, 1996: Zunft trifft auf High-Tech; in: Bulmahn, Edelgard/ Haaren, Kurt van/ Hensche, Detlef/ Kiper, Manuel/ Kubicek, Herbert/ Rilling, Rainer/ Schmiede, Rudi (Hrsg.), 1996: Informationsgesellschaft – Medien – Demokratie. Kritik – Positionen – Visionen, 1. Auflage, Marburg: BdWi-Verlag: 423-426 (http://www.netuse.de/~maro/mr_imd.html.)

79 Vgl. Rost, Martin, 1998: Die Technisierung der Kommunikation – Die Folgen für Organisation und Gesellschaft (http://www.netuse.de/~maro/mr_tdk.html).

80 Vgl. Simmel, Georg, 1984: Grundfragen der Soziologie: Individuum und Gesellschaft, 4. Auflage, Berlin; New York: de Gruyter (zum ersten Mal erschienen: 1917).

81 Als Fußgänger vertraut man z.B. darauf, daß ein Autofahrer bei Rot hält, ohne ihm dafür persönlich dankbar zu sein und stante pede Freundschaft zu schließen.

82 Nebenbei bemerkt ist dieser auf Kooperation angelegte Umgangsmodus das spieltheoretisch erzielbare Optimum (vgl. Axelrod, Robert, 1984: The Evolution of Cooperation, New York.). Man mag darin ein Indiz für den anhaltenden Prozeß der Zivilisation sehen.

83 Vgl. Esposito, Elena, 1993: Der Computer als Medium und Maschine; in: Zeitschrift für Soziologie, Jg. 22, H. 5: 338-354.; Rost, Martin, 1997: Anmerkungen zu einer Soziologie des Internet; in: Gräf, Lorenz/ Krajewski, Markus (Hrsg.), 1997: Soziologie des Internet. Handeln im elektronischen Web-Werk, Frankfurt am Main: Campus (http://www.netuse.de/~maro/mr_sdi.html).

84 Vgl. Turkle, Sherry 1986: Die Wunschmaschine – Der Computer als zweites Ich, Reinbek bei Hamburg: Rowohlt.

85 Vgl. Flitner, Andreas, 1965: Die gesellschaftliche Stellung von Jugendschutz und Jugendförderung, in: deutsche jugend, S. 209ff.

der Erwachsenenwelt einnimmt und somit auch besonders schutzbedürftig ist. Vielmehr wurde angemerkt, daß die Gefährdungen für die Jugend das Ergebnis von längerfristig laufenden Erziehungsdefiziten sind und nicht mehr aus zufälligen Ereignissen in der Lebensgeschichte bestehen.[86] Dies wurde nicht als Argument gegen den Jugendschutz eingewandt, sondern sollte darauf aufmerksam machen, daß Jugendschutz mit seiner punktuellen Wirksamkeit langfristige Entwicklungen nicht aufzuhalten in der Lage sei. Vielmehr sollten mit dem Jugendschutz die schlimmsten Mißstände unter Kontrolle gehalten werden und die Erwachsenen als Adressaten des Jugendschutzes verpflichtet werden. Dieser Kritik wurde im Kinder- und Jugendhilferecht (1991) insofern Rechnung getragen, als dort im Paragraphen 14 als originärer Jugendschutzauftrag formuliert wird, mit geeigneten Maßnahmen die Abwehrkräfte und die Eigenverantwortlichkeit von jungen Menschen zu stärken.

Die Debatte der sechziger und siebziger Jahre, die bis in die neunziger Jahre hinein reichte, wurde ganz im Horizont des Nationalstaates geführt. Diese Situation hat sich am Ende des zwanzigsten Jahrhunderts jedoch dahingehend geändert, daß Jugendschutz im Internet nunmehr im Kontext der Weltgesellschaft zu analysieren ist. Unsere Überlegungen laufen darauf hinaus, einen national sanktionierten Jugendschutz für das Internet zu formulieren, der die Anschlußfähigkeit an die Weltgesellschaft mit den Erfordernissen pädagogischer Strukturbildung, also den Sorgen der Eltern, Schuldirektoren, Jugendrichter bezüglich der dort transportierten kriminellen Inhalte Rechnung trägt, koppelt. Diese Sorgen sind weder einfach zu negieren noch einfach zu akzeptieren. Über diese Sorgen hinausgehend muß zusätzlich gesehen werden, daß unter dem Etikett des "Jugendschutzes" unbeabsichtigt womöglich Prozesse des Abbaus von Bürgerrechten – im Hinblick auf den Datenschutz, des Rechts auf Anonymität, der Privatsphäre und Meinungsfreiheit – in Gang gesetzt werden.

Als ein erstes Zwischenfazit läßt sich festhalten: Im Umgang mit dem Internet zeigen sich die gleichen Phänomene wie im Umgang mit den letztlich nicht rein national gestaltbaren globalen Finanzmärkten oder dem Bedarf nach global agierenden Organisationsstrukturen, die sich aufgefordert sehen, bei intranationalen Konflikten, in denen gegen Menschenrechte verstoßen wird, einzugreifen. Die Nationen sind in der Weltgesellschaft angekommen. Das Internet generiert Konflikte, die in einem weltgesellschaftlichen, übernationalen Rahmen zu bewältigen sind. Sie primär unter dem Aspekt des "Jugendschutzes" zu bearbeiten, mag mit guten Gründen zunächst besonders naheliegen, reicht aber nicht hin.

3.2 Jugend soziologisch

Jugend entsteht, wenn Personen als Jugendliche beobachtbar werden. Dies setzt erstens eine zeitliche Ausdehnung in Form einer Jugendphase mit als exklusiv ausgewiesenen Sachverhalten voraus. Zweitens ist damit die Vorstellung eines Übergangs von einem unmündigen Kind zum mündigen Erwachsenen verbunden, in dem Jugendliche begrenzt zurechnungsfähig sind.

Die drei wesentlichen weltgesellschaftlichen Differenzierungsmuster, die zugleich als spezifisch soziologische Leitunterscheidungen fungieren, lassen sich wie folgt darstellen: (a) *segmentäre Differenzierung*, die in einem besonderen Bezug zu Familien, Stämmen, Clans und ethnischen Zusammenhängen, generalisiert formuliert: zu einfachen Interaktionsformen, steht; (b) *geschichtet-hierarchische Differenzierung (Stratifikation)*, die in einem besonderen Zusammenhang zu organisatorischen Einheiten, etwa Nationalstaaten, Institutionen und Betrieben steht sowie (c) *funktionale Differenzierung*, die weltweit große Funktionssysteme jenseits der nationalstaatlichen Grenzen herausgebildet hat: Wirtschaft, Wissenschaft, Recht und Politik.

86 Vgl. Bundesregierung (Hrsg.), 1972: Dritter Jugendbericht, Bonn.

In hauptsächlich segmentär differenzierten Verhältnissen ist Jugend in diesem Sinne nicht auffindbar, weil diese Strukturierungsform zwar Altersunterschiede kennt, zugleich aber nicht die Möglichkeiten hat, Altersunterschiede im Modus von Stratifikation anzuordnen. In der Folge kennt diese Gesellschaftsformation nur Initiationsriten, die auf kurze Zeiträume bezogen den jugendlosen Übergang vom Kind zum Erwachsenen regeln. Noch in den unteren Lagen einer hauptsächlich geschichtet-hierarchisch differenzierten Gesellschaft ist diese jugendlose Form zu finden. Sie korrespondiert mit einer anspruchslosen Konzeption vom Erwachsenen. Umgekehrt gilt: Je anspruchsvoller das Rollenset des Erwachsenen, desto ausgedehnter die Jugendphase. Der unbedingt reziproke Charakter der durch segmentäre Differenzierung strukturierten Kommunikation ist mit einer Vorstellung von Jugend als einer besonderen Phase nicht vereinbar. Kinder werden harten Selektionen in Bezug auf das spätere Erwachsenensein unterworfen, dann einem Initiationsritus (also einer Probe) ausgesetzt und werden anschließend gesellschaftlich als voll zurechnungsfähig erklärt. Sie erreichen eine soziale Position und behalten diese bis an ihr Lebensende oder bis zu einem Totalausschluß (Bann, Verbannung). Eine Veränderung der sozialen Positionen im Zeitverlauf ist nicht vorgesehen – und damit auch keine Jugend. Solche jugendlosen Gesellschaften sind in der Gegenwart in segmentär differenzierten Subgesellschaften auffindbar: bei den Sinti und Roma sowie in Teilen der türkischen und griechischen Gesellschaft.

Jugend entsteht mit der Herausbildung geschichtet-hierarchischer oder stratifikatorischer Differenzierung. Mit der stratifikatorischen Differenzierung entstehen unterschiedliche Erwachsenenrollen, die zu bestimmten Erwartungssets kumulieren. Diese Erwartungssets wurden von der klassischen Jugendsoziologie in Analogie zu Klassenlagen[87] mit je unterschiedlichen Anforderungen und Ansprüchen verstanden. Diese unterschiedlichen Anforderungen und Ansprüche an Erwachsenenrollen induzieren dann in wiederum unterschiedlicher zeitlicher Ausdehnung eine Jugendphase als Übergang in diese differenten Rollensets (lange Adelsjugend, kürzere Bürgerjugend, kurze Arbeiterjugend). Das Problem der Generationen wird bis in die zwanziger Jahre des 20. Jahrhunderts analog zum Problem der sozialen Klassen angefaßt. Dabei wird viel Raum für unterschiedliche Jugendkonzepte im Rahmen stratifikatorischer Differenzierung offengelassen. So hat sich im deutschsprachigen Raum ein Jugendkonzept durchgesetzt, das mit dem Begriff der *Statuspassage*[88] bezeichnet wird. Dieses Konzept enthält die Vorstellung von Jugend als einer Passage von der Kindheit in eine sozial festgelegte Rolle des Erwachsenen. Es beinhaltet ein Verständnis von Jugend als einer Lebensphase, die eines besonderen Schutzes sowohl durch die Familie als auch durch staatliche Institutionen bedarf.

Im englischsprachigen Raum wird Jugend eher als eine eigenständige Lebensphase thematisiert. Im Übergang von der partikularistischen und eigensinnig wertoptimierenden Familie in die universalistische Welt der Erwachsenenrollen entsteht ein Strukturwiderspruch. Hier leisten Gleichaltrigengruppen (*peergroups*) die Herausbildung nicht-familiärer Dispositionen, die den Anschluß an die Erwachsenenwelt ermöglichen. In diesem Zusammenhang wird Jugend und Jugendkultur als weitgehend autonome Sphäre verstanden, in der Jugendliche sich wesentlich an Gleichaltrigen und nicht an Erwachsenen orientieren. Dies ging einher mit dem Entstehen der Popkultur in den USA und England. Dagegen haben sich im südeuropäischen Raum nur rudimentär Jugendvorstellungen entwickelt. Jugend findet dort noch vorwiegend im Horizont der Familie statt und ist erst abgeschlossen, wenn die Familie verlassen und ein eigener Haushalt gegründet wird, was bei Männern in der Regel dauern kann, bis sie fast dreißig Jahre alt geworden sind. Hier ist die starke Referenz der katholischen Kirche bis in das Jugendkonzept hinein zu veranschlagen.

---

87 Vgl. Mannheim, Karl, 1929: Das Problem der Generationen, in: Kölner Zeitschrift für Soziologie und Sozialpsychologie 1928/29.

88 Vgl. Schelsky, Helmut, 1957: Die skeptische Generation, Düsseldorf-Köln: Eugen Diedrichs.; Hurrelmann, Klaus, 1994: Lebensphase Jugend, Weinheim/ München: Juventa.

Ganz allgemein ist hervorzuheben, daß die Entwicklung von Jugendkonzepten ganz klar vom Selbstverständnis der Erwachsenenwelt abhängig ist. Damit Eltern Jugend thematisieren, muß das Verhaltensrepertoire hinreichend abgegrenzt und deutlich genug sein. Um einen Begriff von Jugend zu erzeugen, ist also zunächst ein hinlänglich scharf gestellter, stratifikatorisch differenzierter und anspruchsvoller Begriff von Erwachsenenrollen nötig und dann eine Einsicht in die je unterschiedlich ausgeprägten Strukturierungsmächte.

In der primär funktional-differenzierten Gesellschaft, worunter wir insbesondere die heutigen westlichen Nationalstaaten befaßt wissen wollen, wird dieses Übergewicht stratifikatorischer Differenzierung relativiert, also nicht einfach "abgeschafft", sondern um eine weitere, spezialisierte Erwartungsstruktur ergänzt. Dies hat unmittelbare Folgen für die Konzeption von Jugend. Wenn nämlich die gesellschaftliche Reproduktion nicht mehr über die organisierten Rollensets der Erwachsenen (also über Klassenlagen) gewährleistet wird, wird auch das Übergangsfeld, in dem sich ein Jugendkonzept erster Hand gebildet hatte, abgeschwächt und abgeblaßt. In der primär stratifikatorisch differenzierten Gesellschaft sind die Erwartungen an Jugendliche von den Rollensets der Erwachsenen abhängig und in der Folge reproduziert sich die Gesellschaft über diese Sets. Es war ungewöhnlich, wenn der Sohn eine Bauern oder Fischers nicht seinerseits Bauer oder Fischer wurde. Anders ist die Situation hingegen in der primär funktional-differenzierten Gesellschaft. Die Erwartungen an Jugendliche werden nicht nur von elterlichen Wünschen, die ihrerseits gesellschaftlich vermittelt sind, sondern darüber hinaus sehr direkt von den Imperativen der Funktionssysteme gesetzt.

Zugleich verstärkt sich in der primär funktional-differenzierten Gesellschaft die Debatte über Jugend, in der das Feld Jugend mit überkomplexen Ansprüchen aufgeladen wird. Werden die Rollensets der Erwachsenen unscharf, weil sich nicht mehr durch klar erkennbare Klassenlagen abgegrenzt sind, kann Jugend insofern leicht zuviel an möglichen Übergängen zugemutet werden. Dies bedeutet, daß Jugend zur eigentlichen lebenszeitlichen Belastungszone wird, in der alles mögliche zur Disposition steht. Jugend wird darüber hinaus zu einer Art Projektionsfläche für die persönliche wie auch die gesellschaftliche Zukunft, auf die eine Gesellschaft sämtliche Sorgen und Befürchtungen ebenso projiziert wie Hoffnungen und Träume einer besseren Welt. Jugend wird so einer extrem hohen Kontingenz ausgesetzt. Das Ergebnis: Diese hohe Kontingenz läßt Forderungen eines besonderen Schutzes für Jugendliche um so dringlicher erscheinen und verkürzt gleichzeitig die Reichweite einzelner Schutzmaßnahmen, wie sie in traditionell segmentären (Familien) oder stratifizierten (Organisationen) Kontexten entwickelt werden.[89]

Unter dem Regime der Funktionssysteme ist eine Übergangs- und Probezeit noch dringlicher erforderlich als in älteren Systemen. Doch ist funktional keine solche Übergangsphase vorgesehen und die alten Ansprüche sind gleichzeitig noch immer vorhanden. Auf funktionale Differenzierung kann also nicht länger in dem Modus stratifizierter Gesellschaften vorbereitet werden. Und zugleich braucht eine modern funktional-differenzierte Gesellschaft mehr Vorbereitungen, weil sie in vieler Hinsicht sehr viel anspruchsvoller ist als eine weniger komplex differenzierte Gesellschaft.

Jugend wird nicht nur zum Gegenstand von Rechtsprechung und Marketingstrategien, sondern auch von Wissenschaft. Und dies von dem Moment an, an dem das Alltagsfeld Jugend aufgrund der benannten Umstellung in den Differenzierungsformen aus Sicht der Eltern hinlänglich unscharf wird.

Wird Jugend in stratifizierten Kontexten unter dem Aspekt von Widerstand und Anpassung, also in der Form Rebellion, thematisiert, so steht heute eher die Differenz von Perturbation und Adaption im Vordergrund, die wir übergreifend als *Individualisierung* bezeichnen wollen. Mit Bezug auf Jugend soll dieser Begriff mehr und anderes als die "bloße" Rebellion gegen herangetragene, widersprüchliche Rollensets bezeichnen und auch die Aneignung von

89 Vgl. Herrmann, Thomas, 1995: Jugend im Stadtteil, Kiel.

funktional separierten Kompetenzen umfassen, gegen die sinnvoll eine Rebellion nicht einmal möglich ist. Das Umgehen von Content-Filtern ist in diesem Sinne kein Akt der Rebellion, auch wenn Eltern und Lehrer dies so thematisieren mögen, sondern vielmehr eine Kompetenzübung im selbstbestimmten Umgang mit dem modernen Kommunikationsmedium Internet.[90] Eltern, Rektoren und Vertreter staatlicher Institutionen müssen dabei berücksichtigen, daß Jugendliche die, von ihren Vormündern unter Umständen als problematisch ausgewiesenen, Inhalte ihren Interessen gemäß aktiv aufsuchen und in der Regel keine bloß passiven Opfer des Mediums Internet (bzw. deren Nutzern) sind. Jugendliche bilden, auch mit Hilfe des Internet, ihre eigene Kultur aus. Eine angemessene Jugendschutzpolitik hat diesem Umstand Rechnung zu tragen.

Jugendschutzpolitik hat in Deutschland eine lange Tradition. Bereits 1832 wird in Preußen die Kinder- und Jugendarbeit reguliert. Aber erst Anfang der achtziger Jahre dieses Jahrhunderts wird der Jugendmedienschutz zum Thema der Jugendpolitik. Im normativen Zentrum des Jugendschutzes steht von je her die Idee, Gefährdungen junger Menschen in der modernen Gesellschaft entgegenzuarbeiten, wo der Einflußbereich der Familie nicht hinreicht. Jugendschutz ist von seinem Selbstverständnis her Erziehungsfunktion und operiert so in der asymmetrischen Differenz von Selektion und Motivation. Die selektive Seite des Jugendschutzes besteht dabei traditionell in Verboten, die sich auf den Aufenthalt an jugendgefährdenden Orten, alkoholische Getränke, öffentliche Tanzveranstaltungen, Filmveranstaltungen, Bildträger, Spielstätten beziehen. Diese Verbote sind umfangreich im Gesetz zum Schutze der Jugend in der Öffentlichkeit geregelt und versuchen, wie bereits betont, den latenten Wertekanon der bundesrepublikanischen Gesellschaft geltend zu machen. Wie zweischneidig die Form des Verbots unterdessen ist, um Adaption zu erzeugen, kann im Medienbereich besonders gut beobachtet werden: Verbote generieren überhaupt erst den Impuls für die Beschäftigung mit einer Sache. Politisch formuliert: die hohe Tabuisierung des Hakenkreuzes (= Adaptionszwang) macht das Hakenkreuz für Jugendliche interessant, um Erwachsene, und zwar nicht nur die eigenen Eltern und Lehrer, sondern sozusagen die Gesellschaft überhaupt – was auch immer unter Gesellschaft verstanden werden mag, gekonnt zu schockieren (Perturbationswirkung). Es sind die Erwachsenen, die solche Aktionen dann eindeutig als politisch intendierte interpretieren. Wer sich erinnern mag... in den sechziger Jahren waren rote Fahne und roter Stern am höchsten tabuisiert.[91]

Der gegenwärtige Jugendschutz greift zwar über die klassische Form des bloßen Verbots in seiner praktischen Anwendung hinaus, indem die motivationale Seite in Form der Unterstützung von Lern- und Entwicklungsangeboten für Jugendliche stark gemacht wird, wie sie vor allem im Kinder- und Jugendhilferecht formuliert werden. Doch trotzdem gilt: Vom Gehalt des Jugendschutzes her betrachtet ist in Bezug auf Erziehung die Interaktion der wesentliche Aspekt. Ein auf diese Weise auf Interaktionskompetenzen zugerichteter Blick des Jugendschutzes bekommt das Medium Internet deshalb nicht angemessen in den Blick und reagiert deshalb im Zweifel unangemessen restriktiv.

Jugendliche müssen heute mit einer komplexen Anforderungsstruktur fertig werden. Die Sphäre der Arbeit ist traditionell codiert und konkret mit Erwachsenen besetzt. Ja, es ist überhaupt die Sphäre der Arbeit, an der der Status des Erwachsenseins festgemacht wird. Die latente, auf Dauer gestellte Überforderung von Jugend führt unseres Erachtens dazu, daß

---

90 Insgeheim sind Eltern und Schulrektoren vielmehr stolz auf diese Kompetenzen ihrer Schutzbefohlenen, zumal diese ihre eigenen Kompetenzen oftmals bei weitem überschreiten.

91 Dies ist selbstverständlich kein Spiel. Vielmehr nehmen Jugendliche in diesen Zusammenhängen wesentliche Muster aus dem Umfeld des Tabubereichs auf. So adaptiert die neurechte Hakenkreuzgemeinde den körperzentrierten Vitalismus und das völkische Pathos der Nationalsozialisten und die 68er übernahmen hypostasierte Arbeitsvorstellungen und ein Arbeiterklassenpathos.

sie beginnt, ein eigenes Referenzsystem auszubilden. Jugend weicht in den kulturellen Rahmen der Gesellschaft aus und beginnt diesen auszudifferenzieren. Als Indiz dafür werten wir das Entstehen der Popkultur in den sechziger Jahren insbesondere in den USA und England, deren Fortsetzung wir in der weltweit sich ausbreitenden Kultur der Cracker und Hacker sehen.[92]

Eine moderne Jugend ist insofern nicht länger nur als eine Übergangsphase zwischen Kindheit und Erwachsensein, sondern als Phase zur Entwicklung eigenständiger Lebensziele und neuer Lebensformen zu verstehen. Jugendliche formieren nicht nur eigene Interessen beispielsweise im Umgang mit dem Internet, sondern sie üben zugleich auch eine veränderte Wertstruktur ein. Es entsteht dadurch ein kultureller Rahmen, der womöglich die einstige Jugendkultur in eine junge Kultur transformiert.[93] Und es wird denkbar, daß sich die Kulturalisierung – wie einst das traditionelle Arbeitsparadigma – auf alle Gebiete des Lebens ausdehnt.[94]

Ob diese Entwicklung bereits in Deutschland vollgültig gegriffen hat, kann noch nicht als gesichert gelten. Festzuhalten ist, daß es in Deutschland eine ganze Reihe an etablierten, speziellen Jugendinstitutionen allein im Bereich der Ausbildung gibt, die auf die traditionelle (Arbeits-) Werte und Normen verpflichten und dieser Entwicklung recht wirksam entgegenstehen (Beispiele: Jugendaufbauwerk, Berufsbildungswerk, Jugendverbände (der Arbeiterwohlfahrt, der Diakonie, des paritätischen Wohlfahrtsverbands...)). Trotzdem: Jugend wird aus der Sicht der Alten gefährlich, weil mehr als nur die traditionell erwartbare Rebellion zu fürchten ist, die sich nach einiger Zeit wieder verflüchtigt. Womöglich ist der Faden zwischen den Generationen auf eine gewisse Art gerissen.[95]

Die älteren Generationen sind heute aufgefordert, den Jugendlichen klare, moderne Erwartungsstrukturen anzubieten. Wenn eine Gesellschaft sich im Medium der Jugend über den geheimen Wertekatalog verständigt, dann bedeutet das jedoch zugleich im Gegenteil, daß sich die Gesellschaft im Medium der Jugend über ihren normativen Rahmen auch verunsichern läßt. In neueren Ansätzen wird darauf hingewiesen, daß Jugendliche in diesem Sinne als "Seismographen" der politischen Entwicklung fungieren.[96] Die Verpflichtung auf einen zentral bestehenden Wertekatalog ist unmöglich und kann zugleich trotz aller Widersprüchlichkeit nicht einfach preisgegeben werden.[97]

Es zeigt sich, daß die Problemstellungen und Antworten des klassischen Jugendschutzes – nicht nur in Bezug auf den Einsatz von Content-Filtern – kaum auf Jugend in der modernen Gesellschaft zu übertragen sind. Wir wollen darauf aufmerksam machen, daß die Reichweite solcher Vorschriften wie die zum "Gesetz zum Schutz der Jugend in der Öffentlichkeit" und

---

92 Vgl. Eckert, Roland/ Vogelsang, Waldemar/ Wetzstein, Thomas A./ Winter, Rainer, 1991: Auf digitalen Pfaden. Die Kulturen von Hackern, Programmierern, Crackern und Spielern: Opladen.

93 Schulze, Gerhard, 1992: Die Erlebnisgesellschaft: Kultursoziologie der Gegenwart, Frankfurt am Main: Campus.: 368ff

94 Für diesen wichtigen Hinweis bedanken wir uns bei Torsten Böhm, für kritische Kommentare zum Text danken wir Michael Schack.

95 Man erinnere sich an den Sommer 1998, als in einer ganzen Reihe an Talkshows Zwanzigjährige die Ungerechtigkeiten des Systems des Generationenvertrags beklagten und diesen aufgekündigt sehen wollten.

96 Vgl. Hurrelmann, Klaus, 1992: Statusverunsicherungen und Statusängste im Jugendalter. Jugendliche reagieren heute wie empfindliche politische Seismographen – eine neue Herausforderung für die Jugendarbeit, in: Kind, Jugend, Gesellschaft H4, S.104ff.

97 In dieser Situation, das sei nur als Nebenbemerkung eingeschoben, darf gesellschaftspolitisch vom Versprechen der Erwachsenen, daß Jugend erwachsen wird, wenn sie nur die traditionelle Vollerwerbsreife erreicht, keine attraktiv-motivierende Wirkung auf Jugendliche erwartet werden.

daran angelagerte Verfahren so gering wie noch nie zuvor einzuschätzen ist, was allerdings nicht schon als Begründung für deren Fallenlassen hinreicht. Ganz im Gegenteil: Es ist unerläßlich, Jugendlichen klare Erwartungsstrukturen zu bieten, damit sie sich daran reiben und damit auseinandersetzen können. Es geht darum, die faktisch vorhandenen, normativen Gehalte der Gesellschaft zu verdeutlichen und dies im klaren Bewußtsein davon, daß diese Gehalte aber nur noch zu einem geringen Anteil in direkter Interaktion, also mittels direkter sozialer Kontrolle, stabilisierbar sind.

Die funktional-differenzierte Gesellschaft ist mit anderen Worten geradezu darauf angewiesen, daß die Umstellung von "Fremd- auf Selbstkontrolle"[98] bereits frühzeitig in der Jugendphase vollzogen wird. Es kommt also unseres Erachtens nicht darauf an, mit Bezug zum Internet den Zugang zu bestimmten Inhalten entweder zu verbieten oder vollkommen unproblematisiert freizugeben, sondern moderne Erwartungsstrukturen so auszulegen, daß sie erstens ihre normativen Gehalte selbst miterklären und zweitens weitere Strukturbildung ermöglichen. Spezifischer läßt sich dieser Punkt nicht formulieren. Die traditionellen Lösungen des reinen Verbots oder Nichtverbots haben jedenfalls je ähnliche Wirkungen: Sie werden Jugendlichen nicht gerecht, indem sie Jugend überfordern. So erhöht ein hoch gehängtes Verbot die Wahrscheinlichkeit, daß ein externes kriminelles Netz generiert wird, welches gegen den Wertekonsens der Republik operiert; mit entsprechenden Aufstiegschancen für Jugendliche, die Adaption findet dann halt in einer Negativkarriere statt.[99] Ein völliges Freilassen der Frage nach dem Jugendschutz im Internet bedeutet den völligen Verzicht auf die Formulierung von normativen Gehalten und überfordert Jugendliche dadurch, daß sie ihnen gerade diese normativen Gehalte vorenthält und sie also mit einer komplexen Selektionsproblematik allein läßt.

3.3 Filter-Strategien

Wie in einer modernen Gesellschaft infrastrukturelle Risiken gehandhabt werden, läßt sich an verschiedenen Technikbeispielen zeigen. Obwohl man weiß, daß die Post pornographisches oder extremistisches Material versendet, werden Briefe nur in ausgewiesenen Sicherheitsbereichen (wie z.B. Gefängnissen) gefiltert. Obwohl man weiß, daß das organisierte Verbrechen auch motorisiert daherkommt, werden trotzdem keine Filterstellen an Bundesautobahnen installiert, das Absperren von Straßen und Ringfahndungen, nachdem das Verbrechen geschah, muß unter besonderen Umständen reichen. Wichtig an diesen Beispielen ist, daß sie zeigen, daß in keinem Fall Strategien von perfekt undurchlässiger Abschottung, sondern je differenzierte Operationalisierungen auf Risikobasis gefahren werden.

Unter einem "Content-Filter" verstehen wir ein Ensemble, das aus einem Katalog an Referenzwerten und einer operativen Einheit besteht. Der Einsatz solcher Filter ist nie nur eine technische Frage, sondern immer, ganz gleich wie die technische Realisation aussieht, auch eine politische.

In unübersichtlichen Situationen, bei denen noch kaum Erfahrungen mit dem Internet vorliegen, gehört die rigide Referenz allein auf das eigene System – sei es die Familie, sei es die Schule oder die Verwaltung – zu den zunächst naheliegenden Strategien der Komplexitätsreduktion derjenigen, die für andere Verantwortung zu übernehmen haben. Auf

98 Vgl. Elias, Norbert, 1976: Über den Prozeß der Zivilisation – Soziogenetische und psychogenetische Untersuchungen. Erster Band: Wandlungen des Verhaltens in den weltlichen Oberschichten des Abendlandes. Zweiter Band: Wandlungen der Gesellschaft. Entwurf zu einer Theorie der Zivilisation, 1. Auflage, Frankfurt am Main: Suhrkamp.

99 Man denke hier beispielsweise an gut organisierte Tauschringe für geknackte Software auf dem Schulhof mit mächtigen Schülern, die aufgrund ihrer Tätigkeiten über ungleich mehr Geld verfügen als ihre Mitschüler.

Gefährdungen wird in segmentären Kontexten durch Abschottung, stratifikatorisch durch Bekämpfung und Verbote, modern funktional durch operationalisierte Transformationen von unspezifischen Gefahren in kalkulierbare Risiken reagiert.[100] Mit anderen Worten: Es liegt nahe, risikoavers erst einmal gar kein Internet auf dem Privat-PC oder in der Schule zuzulassen.

Solche fundamentalistischen und begrenzt wirkungsvollen Abwehrstrategien konnten bis etwa 1995 oder 1996 (als Selektionsstrategie sozusagen auf der Hardwareebene) gefahren werden, ohne daß daraus ein besonderer Legitimationsdruck für die Entscheider entstand. Das änderte sich recht zügig in dem Maße, in dem die Gesellschaft in aller Breite über die Chancen dieses Mediums reflektierte und ganz konkret Tagesschau und Heute-Journal ihre WWW-Adressen einblendeten. Sowohl Eltern als auch Schulrektoren wurden des Risikos gewahr, das entsteht, wenn sie ihre Schutzbefohlenen von modernen Technikentwicklungen fernhalten – zumal sie diejenigen waren (und zu einem guten Teil immer noch sind), die ihre mangelnden Computer- und Internetkenntnisse zu fadenscheinigen Kritiksimulationen veredelten. Ein Internetanschluß mußte her, womit das Problem, unerwünschte Inhalte außen vor zu halten, verschoben wurde: von der Hardwareebene des Internetanschlusses, der mittlerweile hergestellt ist, um eine Ebene hinauf in die Protokollebene.[101] Während bei Eltern zunächst noch eher das Kostenargument im Vordergrund stehen dürfte, warum sie den Jugendlichen keinen freien/ unbeaufsichtigten Internetzugang zugestehen, sehen sich die Lehrern/ Schulrektoren veranlaßt, den Zugang in der Regel nur unter Einsatz von Filtern zulassen zu können.

Verschiedene Filter-Strategien haben unterschiedliche soziale Folgen[102]:

- Zum einen lassen sich Positiv- und Negativlisten selber erstellen bzw. einkaufen, auf deren Basis bestimmte Inhalte des Internet untersucht werden und gegebenenfalls gesperrt werden. Statt so direkt auf die Inhalte zu zielen, kann ein Scanner auf der Protokollebene anhand von ähnlichen Listen bestimmte Server-Adressen erkennen und den Zugang unterbinden. Oder es kann ein Zwangsproxy, also ein bestimmter Weg ins Internet, vorgeschrieben sein. In beiden Fällen stellt sich die Frage, welche Instanz die Verfügungsgewalt über die Listen innehat: In welcher Hand liegt die Entscheidung darüber, welche Inhalte außen vor bleiben sollen und wie dies technisch zu regeln sei, zumal solche Listen praktisch niemals vollständig sein können? Traditionell sehen sich hier Familie und Staat herausgefordert, wir sehen hier zudem eine Nische für das Entstehen neuer Dienstleistungen.
- Auf der Kabelebene ließen sich Filterwirkungen darüber erzielen, daß nur bestimmte Provider für Jugendliche zur Einwahl ins Internet freigegeben sind oder empfohlen werden. Auch das ist ein Politikum: Entweder haben diese Provider sich ein Image als besonders solide und familienfreundlich agierend zugelegt. Oder eine vertrauenswürdige Institution hat ihnen ein entsprechendes Gütesiegel verliehen.
- Gewünschte Filterwirkungen werden sicher auch dann entstehen, sobald funktionierende Identifikationssysteme (etwa über Kartenleser am PC oder über biometrische Verfahren (Analyse der Retina, des Daumens, des Gesichts usw.) realisiert sind. Durch Identifikationssysteme ließen sich die Benutzer vor dem Zutritt zu bestimmten Diskussionsforen oder auch Webinhalten identifizieren. Allerdings steigern verläßlich funktionierende Identifikationsverfahren zugleich die Gefahr für Jugendliche dadurch, daß sie erst dann wirklich eindeutig zu erkennen sind. Diese Gefahr ist unseres Erachtens

100 Vgl. Luhmann, Niklas, 1991: Soziologie des Risikos; Berlin, New York: de Gruyter.

101 Zum 3-Schicht-Netzmodell: Rost, Martin/ Schack, Michael (Hrsg.), 1995: Der Internet-Praktiker – Referenz und Programme; Hannover: Verlag Heinz Heise. : 40ff.

102 Für Details der technischen Elemente vgl. Kapitel "Filtermechanismen".

denn auch die größte, die von der Nutzung des Internet durch Kinder und Jugendliche ausgehen kann. Der moderne "böse Onkel" ist nicht länger daran zu erkennen, daß er noch mehr Bonbons verspricht. Für einen Jugendlichen sind solche Erwachsene attraktiv, die vorgeben, ihn anders als seine Eltern zu verstehen, ihn in seinen Sorgen oder auch nur in seinen politischen, philosophischen oder erotischen Ansichten Ernst zu nehmen.

- Neben dem unmittelbaren Einsatz von Content-Filtern ist zu erwägen, mit ihrem Einsatz zu drohen. Solche zeitlich begrenzt eingesetzten Filter operieren in der Differenz Selbstbegrenzung/ Drohung. Interessant an zeitlich begrenzt eingesetzten Filtern ist eine wichtige Verschiebung in der Kausalattribution der Sperrung von Zugängen: Nicht die sperrende Instanz (Eltern, Lehrer, Staat) erscheint dann länger als ursächlich, sondern der Anbieter von Inhalten. Als soziologisch abgesichert darf hierbei gelten, daß die Drohung (in diesem Falle: mit Filtern) stärker beeindruckt als letztlich die Ausführung, weil die Drohung schädigende Ereignisse filtern kann, ohne schon die negativen Folgen einer Ausführung mit zu zeitigen. Es geht also darum, ein überzeugendes Filter-Instrumentarium bereitzuhalten und zugleich auf den Dauereinsatz zu verzichten.
- Neben dieser klassischen Methode der Drohung und Kontrolle durch eine dritte Instanz halten wir *selbstverpflichtende Verfahren* – unter Einbeziehung zeitlicher Begrenzungen und der Protokollierung von Aktionen – konzeptionell für am sinnvollsten. Selbstverpflichtende Verfahren entsprechen im Hinblick auf Risikoakzeptanz bei gleichzeitigem Rechtszugriff am ehesten modernen Erfordernissen. Hiernach wird jeder, der Inhalte ins Netz stellen möchte, darauf verpflichtet, die eigenen Inhalte angemessen zu bewerten bzw. zu verschlagworten.

Faktisch entsteht derzeit ein Gemengelage aus verschiedenen Filtern. EDV-Beauftragte der Schulen und der Bibliotheken sehen sich gehalten, auf den PCs ihres Einflußbereichs Internetfilter- oder Bewertungsprogramme zu installieren. Mit etwas Verspätung werden die Eltern folgen.

Als besonders wichtig schätzen wir den Einfluß der Webseiten von Jugendzeitschriften wie die Bravo und Mädchen sowie die von Popbands ein. Diese sind einer erhöhten Aufmerksamkeit ausgesetzt und können bei Verfehlungen zusätzlich anhand ökonomischer Sanktionen reguliert werden.

3.4 Jugendschutz und Bürgerschutz

Im diesem Abschnitt wollen wir die – durch eine Kontrollmöglichkeit durch Dritte – entstehenden Risiken für den Bürgerschutz problematisieren. Das Internet ist deshalb kommunikativ besonders leistungsfähig, weil es ein quasi raumloses, rein interessengesteuertes Zusammentreffen von Personen erlaubt. Genau durch diese Leistungsfähigkeit erhöht sich aber auch das Risiko, daß "falsche" Personen aneinandergeraten und zwecks Vermeidung dieses Risikos z.B. von staatlicher Seite private, bidirektionale Kommunikationen überwacht werden. Abstrakt gewendet: Risiken für den Nutzer gehen vom Internet aus, wenn ein Zuviel oder ein Zuwenig an Anonymität vorliegt. Ein Zuviel an Anonymität kann bedeuten, daß sich kriminelle Vergehen nicht auf Täter, denen man körperlich habhaft werden kann, zurechnen lassen. Ein Zuwenig an Anonymität kann bedeuten, daß genaue Daten über Menschen, die automatisch anfallen, zum Mißbrauch einladen.[103] Man kann an dem staatlichen Umgang mit dieser Gratwanderung zwischen zu viel und zu wenig Anonymität bemessen, inwieweit es sich um einen bürgerlichen Rechtsstaat handelt. Man kann an dem familiären Umgang mit dieser Gratwanderung

[103] Die Mißbrauchspalette reicht hier vom Betreiber einer Website, der anhand der Auswertung von Logdateien sein Produkte per E-Mail bei potentiellen Kunden bewirbt, bis hin zu totalitären Regimen, die systematisch die Bevölkerung bespitzeln und drangsalieren.

bemessen, inwieweit Eltern ihre Jugendlichen tatsächlich als autonome Persönlichkeiten begreifen.

Gerade in ihren funktional-differenzierten Bereichen ist eine moderne Gesellschaft auf ein hohes Maß an gesicherter Anonymität angewiesen: So beim Bezahlen (Geld außerhalb des Internet funktioniert ohne Verwaltungsoverhead perfekt gedächtnisfrei, es hinterläßt keine Spuren), bei einer geheimen Stimmabgabe im Rahmen einer Wahl, bei der Beurteilung der Publikationswürdigkeit eingereichter wissenschaftlicher Aufsätze. Ebenso ist sie darauf angewiesen, daß Bilanzen, Strategien oder auch nur Selbstoffenbarungen ohne Einblick durch Dritte mitgeteilt werden können. Diese auf Inhalte zielenden Daten gilt es zweifelsfrei zu schützen. Im Internet (oder auf einem PC mit Content-Filter) gilt es darüber hinaus, auch die Verkehrsdaten zu schützen. Verkehrsdaten bereiten den Datenschützern deshalb besonders viel Kopfzerbrechen, weil sie technisch an irgendeinem Punkt unvermeidlich anfallen und unter der Fragestellung zusammengeführt werden können: Wer kommuniziert in welcher Form und Intensität mit wem?[104] Weil es auf der Basis des Universalmediums Internet eines großen zusätzlichen Aufwands bedarf, um überhaupt nur die etablierten Formen an Anonymität und Privatheit zu wahren (durch Remailer, Mixe und Verschlüsselungsprogramme, um die Stichworte zu nennen), ist das Risiko unseres Erachtens besonders groß, daß unter dem Etikett "Jugendschutz" nun diese Gratwanderung zwischen einem Zuviel oder einem Zuwenig an Anonymität, unter dem Eindruck eines dringlichst zu gewährleistenden Jugendschutzes, durch die Installation von Content-Filtern aufgegeben und im Ergebnis dann ein Zuwenig an Anonymität in Kauf genommen wird. Was im Familiären noch hinnehmbar sein mag, nämlich daß Eltern anhand von Aktionsprotokollen Aufschluß erhalten darüber, was ihre Kinder mit dem PC anstellen, ist aus der Sicht eines Staatsbürgers (durchaus in der Inkarnation eines Schülers, Bibliothek-Benutzers aber auch eines Arbeitnehmers) nicht bedingungslos zu akzeptieren.[105] Diese Gefahren sind beim Entwurf von Fitlermechanismen und zugehörigen Infrastrukturen zu beachten.

Die soziologischen Folgen der Installation von Content-Filtern sind nicht klar absehbar, sie steigern aber vermutlich zunächst einmal den gesellschaftlichen Konfliktlevel.[106] Denn dadurch, daß sich die Rollenverständnisse immer weniger traditionell ergeben, sondern explizit gemacht werden müssen, weil sie einem Prozeß der zunehmenden Verrechtlichung unterliegen[107], führt auch die Installation von Content-Filtern zur Explikation des mehr oder weniger im Dunkel bleibenden gesellschaftlichen Wertekatalogs.

Man kann einerseits den Standpunkt vertreten, daß dadurch der Normen- und Wertekatalog dem positiven Recht zugänglich gemacht würde. Das ist zu begrüßen, weil rechtsstaatliche

---

104 Vgl. Gisor, Marc, 1996: Von Anarchie bis Orwell – Die Subgesellschaft Internet; in: Rost, Martin (Hrsg.), 1996: Die Netzrevolution – Auf dem Weg in die Weltgesellschaft, Frankfurt am Main: Eichborn-Verlag.

105 Vgl. Schulzki-Haddouti, Christiane, 1999: Abhören und Filtern gegen Kinderpornographie; in: Telepolis, http://www.heise.de/tp/deutsch/inhalt/te/2722/1.html. Daß diese Tendenz zur Inkaufnahme des Abbaus von Anonymität und geschützter Privatkommunikationen real besteht, zeigt sich besonders deutlich an den weltweit geführten nationalen Debatten darüber, ob eine starke, allein privat-zugängliche Verschlüsselung insbesondere von E-Mails (z.B. per PGP ohne key escrow) im Sinne einer normativen Kraft des Faktischen zugelassen bleibt oder nicht.

106 Erste deutliche Indizien dafür lassen sich im Zusammenhang mit der Überwachung von Arbeitnehmern ausmachen (vgl. Schmitz, Ulrich, 1996: Liebesgrüße vom Chef – Automatisierte Emailkontrolle über MIMEsweeper; in: iX 96/ 11: 80-85.).

107 Als Beispiele der zunehmenden Verrechtlichung möchten wir nur die große Zahl an aufwendig formulierten Dokumenten anführen, die heutzutage auszufüllen sind, bevor sich Ärzte auf Operationen, Verlage auf Autoren, Ehewillige auf eine Heirat oder Arbeitnehmer auf Arbeitgeber einlassen mögen.

Verfahren greifen. Es läßt sich andererseits der Standpunkt vertreten, daß eine Gesellschaft ohne latent bleibende Strukturen einen zu hohen Verwaltungsoverhead mitschleppt.[108] Die faktisch gültigen, latenten Wertereferenzen müssen, im Unterschied zum explizierten Recht, deshalb latent bleiben, um auch unter kontrafaktischen, widersprüchlichen, modernen gesellschaftlichen Verhältnissen noch zu binden. Werden solche Wertereferenzen anhand von Content-Filtern expliziert, vereinfacht und konsistent gemacht, so besteht das Risiko, daß diese die bindende Funktion verlieren. Ob sich für diesen möglichen Werteverlust zwangsweise Ersatz bildet, oder ob ein solcher Ersatz womöglich gar nicht (mehr) nötig ist, weil der Verwaltungsoverhead der positiven Rechtsprechung auch maschinell unterstützt bewältigt werden kann, ist vermutlich für niemanden klar absehbar. Es ist insofern damit zu rechnen, daß man sich erstens mit den Content-Filtern zunächst einmal all die Konflikte einhandelt, die man durch deren Verwendung eigentlich bändigen wollte. Und das kann zum zweiten heißen, daß diese Filter zwar unter dem Etikett "Jugendschutz" firmieren, aber umstandslos auch auf andere diskursive Bereiche übertragen werden, in denen sie kontrafunktional wären und unter Umständen zu einer Fundamentalisierung von Diskursen, etwa im Bereich der Politik oder der Wissenschaft, und zur Beeinträchtigung von Bürgerrechten führten.

Daher ist beim Entwurf eines Jugendschutzkonzeptes für das Internet auf diese Gefahren besonderer Augenmerk zu legen.

Eine moderne Gesellschaft nutzt die Differenz von Moral, Ethik (im Sinne einer Moral verschiedener Moralen) und positivem Recht und stellt somit nicht alles in das Licht allein rechtstheoretischer Überlegungen und Regelungen. Wenn nun gesellschaftliche Konflikte auftreten, für die noch keine theoretisch überzeugende – oder für niedrige Rechtsinstanzen praktikable – Rechtsform gefunden wurde, wie derzeit in Bezug zu vielen Anwendungen des Internet, besteht das Risiko, daß diese Differenz deshalb zu Ungunsten des Rechts und zu Gunsten der Moral eingeebnet wird. Bloße Moral als Beurteilungsinstanz kann im Falle des gesellschaftlichen Universalmediums Internet nicht angemessen sein. Statt daß das hochreflektierte Rechtssystem greifen kann, bietet dann in vermeintlich dringlich zu lösenden Konfliktsituationen die veröffentlichte, nicht an Rechtsfiguren orientierte Meinung der Massenkommunikationsmedien Entscheidungsformen an. Und wieder: Es droht damit die Tendenz zu einer Art Fundamentalisierung des öffentlichen Diskurses, die gerade unter dem Etikett "Jugendschutz" und der Simulation persönlicher Betroffenheit von Eltern besonders schnell erfolgen kann.

3.5 Schlußfolgerungen

Es ist zu konstatieren, daß ein Bedarf nach auf Content zielenden Filtern besteht und diese auch eingesetzt werden. Dabei spielt es nicht unbedingt eine maßgebliche Rolle, wenn Technikexperten versichern, daß diese Filter leicht zu umgehen oder unter Umständen sogar wirkungslos seien.[109] Aufgrund der vielfachen zu konstatierenden technischen Unzulänglichkeiten ließe sich der Einsatz von Content-Filtern als bloß "symbolische Jugendpolitik" bezeichnen. Gleichwohl ist eine solche Politik nicht deshalb schon unwirksam, sondern ganz im Gegenteil einer modernen, pluralen Gesellschaft angemessen, weil sie dadurch immer auch noch das Andere zuläßt, ohne trotzdem an Bestimmtheit zu verlieren.

Wünschenswert wäre die Entwicklung von Filtermechanismen, die zugleich die Bürgerrechte schützen als auch einen effektiven Jugendschutz ermöglichen. Ein nicht reflektiertes

---

108 Im Jugendstrafrecht räumt man aus diesem Grunde den Richtern mit der Möglichkeit des Erstellens einer immer problematisierbaren Sozialprognose relativ viel Bemessungsspielraum ein. Denn es gilt, eine kriminelle Karriere zu verhindern, obwohl diese allein formal betrachtet als bereits eingeschlagen erscheinen mag.

109 Vgl. dazu das Kapitel "Realitätsnahe Praxiserprobung".

Experimentieren mit Filtersystemen, das unter dem Etikett "Jugendschutz" als besonders dringlich erscheint, ist jedenfalls riskant, wenn die so entstehende Filterinfrastruktur nicht nur auf den Jugendschutz, sondern auf die gesamtgesellschaftlichen Kommunikationen anwendbar ist. Man muß dabei gar nicht unterstellen, daß hierdurch der Abbau von Bürgerrechten intendiert ist. Wir könnten jedenfalls keine Instanz ausweisen, der wir ein solches Interesse unterstellten oder der wir eine Chance gäben, eine solche Strategie erfolgreich durchzuhalten.

Vielmehr ist hier mit den sich immer einstellenden nicht intendierten Folgen intentionalen Handelns zu rechnen... mit dem Zoll entstand der Schmuggel. Darüber hinaus ist im Zuge der Installation des Internet in die Gesellschaft allgemein mit sehr viel dramatischeren sozialen Folgen zu rechnen als nur einem unschützbaren Zugang zu beliebigen Mitteilungen für Jugendliche. Auf die Gesellschaft bezogen sind die Folgen unabsehbar, wenn der flexible gesellschaftliche Werte- und Normenhintergrund durch die Anwendung von Content-Filtern expliziert wird. Spezifisch auf den Jugendschutz bezogen ist es fraglich, ob unter womöglich als notgedrungen wahrgenommener Inkaufnahme des Abbaus von Bürgerrechten durch schnell zusammengestrickte Content-Filter-Konzepte eine Jugend geschützt werden kann, die es in der anvisierten Form nicht einmal mehr gibt.

Letztlich geht es unseres Erachtens in der soziologischen Beurteilung der Effizienz konkreter Filter also nicht darum, wie sicher diese tatsächlich Probleminhalte aussperren. Entscheidend ist vielmehr, daß Eltern, Lehrer und staatliche Institutionen sich unter starken Druck gesetzt sehen zu handeln und faktisch die angebotenen Filter einsetzen, um das gegenwärtig Machbare zu tun. Soziologisch gesehen versichern sie sich dadurch des geheimen-selbstverständlichen Wertekatalogs der deutschen Gesellschaft. Insofern erfüllen selbst technisch unzulänglich funktionierende Filter sowohl eine psychische als auch gesellschaftliche Funktion.

4 Technik

4.1 Kurzfassung

In diesem Kapitel werden die technischen Prinzipien und Grundlagen der Filtertechnologie im Internet dargestellt. Wir beginnen mit einem Überblick über mögliche Verfahren und identifizieren die dienstspezifische[110] Filtertechnik als einzige technisch sinnvolle Möglichkeit.

Daher wird die Filtertechnik für den Dienst WorldWideWeb im Detail dargestellt und die verschiedenen Optionen zu ihrer Realisierung diskutiert. Dazu werden die bereits in Kapitel 1 eingeführten Begriffe *Einordnung*, *Kennzeichnung* und *Auswahl* mit technischem Hintergrund gefüllt.

Es wird außerdem eine wesentliche Basis für Kennzeichnungssysteme vorgestellt: PICS[111]. Hierbei handelt es sich um eine technische Plattform, die die Definition und Verwendung von Labeln ermöglicht. Es zeigt sich im weiteren Verlauf, daß das bisher dort standardisierte Konzept eine gute Basis für das im Rahmen der Studie vorgeschlagene System ist; Erweiterungen sind allerdings noch nötig, insbesondere wenn es um die Einordnung dynamischer und gemischter Inhalte geht.

Basierend auf dem PICS-Standard gibt es verschiedene Kategorien- und Einordnungssysteme. Ihre Untersuchung ergibt, daß diese Systeme für den englischsprachigen Raum relativ gut geeignet sind. Allerdings liegt kein einziges System in deutscher Sprache vor. Ein weiteres Defizit besteht in der mangelnden Übertragbarkeit der existierenden Systeme ineinander und in ihrer unzureichenden Verbreitung.

Generell gilt für Filtertechnologien, daß sie keine absolute Sicherheit bieten können. Außerdem haben sie eine Reihe von unerwünschten Seiteneffekten, die wir im letzten Abschnitt dieses Kapitels diskutieren.

4.2 Technische Möglichkeiten der Inhaltskontrolle

Einen systematischen Überblick über die technischen Eingriffsmöglichkeiten im Internet gibt das Gutachten "Sperrungen im Internet: Fragen und Antworten – eine systematische Aufarbeitung der 'Zensurdiskussion' “[112], das 1997 für das BMBF erstellt wurde. Von besonderer Bedeutung ist dabei, zwischen den vollkommen unterschiedlichen Zielen der Durchsetzung der Unerreichbarkeit gesetzwidriger Inhalte und der Durchsetzung von Jugendschutz zu unterscheiden.

Wie auch die vorliegende Studie, konzentriert sich das Gutachten von 1997 hauptsächlich auf den Dienst WWW, da dies der einzige Dienst ist, der das Anbringen von Rating-Labels rechtfertigt. Andere Dienste (News, Chat/Internet Relay Chat) mit jugendschutzrelevanten Inhalten sind in der Regel zu flüchtig und zu wenig strukturiert, um dies zu ermöglichen. Insbesondere Chat hat alle Merkmale einer Unterhaltung und ist daher automatisiert kaum kontrollierbar (freie Form, hohe Geschwindigkeit). Ebenfalls ist es wenig hilfreich für das zu erreichende Ziel, daß Kommunikation im Netz heutzutage meistens nicht authentisiert erfolgt

110 Die Internet-Anwendungen E-Mail, News, Chat, WWW etc. werden als Dienste bezeichnet.

111 Platform for Internet Content Selection, eine Technologie, um Kennzeichnungen auf Webseiten anzubringen

112 In gekürzter Fassung erschienen: Kristian Köhntopp, Marit Köhntopp, Martin Seeger: "Sperrungen im Internet – Eine systematische Aufarbeitung der 'Zensurdiskussion' “, DuD 11/97, Seiten 626-631, http://www.koehntopp.de/kris/artikel/blocking

und daher die Integrität der Daten und damit auch die Integrität der Labels nicht sichergestellt werden kann. Durch kryptographische Sicherung mittels einer digitalen Signatur der Labels kann man immerhin sicherstellen, daß ein Label einer ausstellenden Stelle zugerechnet werden kann und daß das Label sich auf eine bestimmte Version einer Seite bezieht (d.h. die Seite ist automatisch nicht mehr gelabelt, wenn sich ihr Inhalt verändert). Zu beachten ist jedoch, daß, solange Kommunikation im Netz nicht oder nur sehr schwach authentisiert erfolgt, es nicht möglich ist, Mitteilungen ohne oder mit falscher Identität sicher auszuschließen. Man kann durch die Authentifizierung der Labels nur verhindern, daß solche Angebote ein Label haben.

Das Sperrungsgutachten diskutierte die Vor- und Nachteile eines Eingriffes auf den unterschiedlichen Schichten des Netz-Protokollstacks: Eingriffe auf der physikalischen Schicht[113], auf der Netz- oder Transportschicht[114] und auf den Anwendungsschichten[115].

Eingriffe sind nur auf den Anwendungsschichten sinnvoll, weil nur dort eine spezifischere Adressierbarkeit der einzelnen Mitteilungen möglich ist: Sperrungen auf niederen Ebenen würden immer zu viele andere Dienste und Mitteilungen betreffen, so daß die Sperrung unverhältnismäßig wäre. Zudem wäre sie leicht zu umgehen, solange der gesperrte Dienst überhaupt noch Kommunikationsmöglichkeiten zur Verfügung hat: Es ist ein Designfeature des Internet, Teilausfälle auf den niederen Schichten des Protokollstacks vor dem Nutzer verbergen zu können. Dabei spielt es keine Rolle, auf welche Ursachen diese Ausfälle zurückzuführen sind.

Vollsperrungen auf den niederen Ebenen sind auch nicht durchhaltbar, da derartige Vollsperrungen wegen der Vielzahl der Betroffenen (rechtmäßig oder nicht) ein solches Aufsehen erregen, daß sie sehr schnell umgangen oder unterlaufen werden.

Aufgrund der Struktur des Internet lassen sich solche Umgehungen der Sperrung grundsätzlich nicht ausschließen, insbesondere dann, wenn Teilnehmer "auf der anderen Seite der Sperrung“ aktiv daran mitarbeiten, die nicht erreichbaren Inhalte wieder zur Verfügung zu stellen. Die Sperrung muß von der weitaus überwiegenden Zahl der Teilnehmer als sinnvoll anerkannt und hingenommen werden, um wirksam zu bleiben. Das ist nur möglich, wenn sie spezifisch genug ist, um keine anderen als die gewünschten Inhalte auszublenden.

Die Datenmenge, um deren Kontrolle es hier geht, ist extrem groß und hat einen sehr hohen Grundumsatz, d.h. große Teile des Datenbestandes werden häufig aktualisiert. Es ist nicht erkennbar, daß eine zentrale Stelle, gleich welcher Größe, eine Einordnung z.B. aller Webseiten nach Jugendgefährdung vornehmen könnte. Nur ein verteilter Ansatz hat eine Chance zu funktionieren.

Automatische Einordnungsverfahren funktionieren nicht zufriedenstellend, da ihnen derzeit nur textuelle Inhalte zugänglich sind. Selbst wenn man sich auf Textanalyse beschränken würde, gelingt in der Regel nur die Erkennung von Inhalten mit direktem sexuellen Bezug automatisch aufgrund des spezifischen Vokabulars, das in solchen Texten meist verwendet wird. Es wird also nicht wirklich auf nicht jugendfreie Inhalte, sondern auf das Vorkommen von obszönen Worten abgesucht, was überwiegend ein anderer Sachverhalt ist. Demzufolge werden die viel gefährlicheren gewaltverherrlichenden oder volksverhetzenden Inhalte oftmals nicht automatisch erkannt, da hier das spezifische Vokabular, das mit den einschlägigen Inhalten einhergeht, nicht so ausgeprägt ist. Natürlich ist eine automatische Erkennung nach solchen Schlüsselwörtern auch in hohem Maße spezifisch für die jeweils verwendete Sprache. In der einschlägigen Literatur finden wir eine ganze Reihe von Berichten über

113 Störsender, Kabelunterbrechung

114 IP-Adressen nicht mehr vermitteln, Ports sperren

115 URLs, E-Mail-Adressen, Message-IDs

Probleme, die bei Online-Diensten wegen der Filterung nach Schlüsselwörtern aufgetaucht sind.[116]

Besonders problematisch sind automatische Einordnungsverfahren, weil sie zumeist ausschließlich nur zwischen "Ja“ und "Nein“ entscheiden können und weil sie vollkommen außerstande sind, über die Güte ihrer Entscheidung zu reflektieren. Dementsprechend fehlt auch die Möglichkeit, zweifelhafte Entscheidungen einem menschlichen Helfer zur genaueren Durchsicht vorzulegen. Die Schaffung einer Maschine, die solche Einordnungen automatisch treffen kann, ist äquivalent mit dem Problem der Konstruktion einer Maschine mit Moral.

Aus den vorhergehenden Betrachtungen ergibt sich, daß nur dienstspezifische Maßnahmen eine hinreichend hohe Selektivität haben, um einzelne Mitteilungen ausschließen zu können. Es muß also auf der Ebene eine Dienstes – im folgenden wird hauptsächlich WWW betrachtet – gefiltert werden.

4.3 Filtermechanismen

In diesem Kapitel werden wir die technische Umsetzung der bereits im Einführungskapitel diskutierten Begriffe *Einordnung*, *Kennzeichnung* und *Auswahl* vornehmen.

Im betrachteten Kontext erfolgt die Einordnung und die Auswahl unter der Zielsetzung "Jugendschutz“ und unterscheidet sich damit z.B. von dem in der Diskussion um die Verbreitung von kriminellen Inhalten einzunehmenden Standpunkt. Insbesondere ist hier die Beschränkung pädagogisch gewollt und somit in Hinblick auf einen Zensurverdacht bei funktionierender Filterung für Kinder unproblematisch.[117] Allerdings ist bei der konkreten Auswahl und Einordnung von Inhalten die Gefahr einer ungewollten Anpassung an fremde Bewertungsmaßstäbe zu beachten.

Insgesamt ist die Einordnung der Inhalte aufgrund der mangelnden Automatisierbarkeit der schwierigste Teil der Sortierung. Hier liegen aufgrund der Komplexität der Inhalte (Bilder, Audio-Sequenzen, semantische Zusammenhänge, ...) bisher keine vollständig befriedigenden Lösungen vor. Kennzeichnung und Auswahl von Inhalten lassen sich hingegen nach erfolgter Beschreibung technisch gut durchführen.

4.3.1 Einordnung

Inhalte im Internet – und auch in anderen Medien – können zunächst sehr einfach in "jugendgefährdend“ und "nicht jugendgefährdend“ unterschieden werden, wobei die zugrunde liegenden Maßstäbe z.B. den gesetzlichen Grundlagen entnommen werden können. Im Sinne einer sinnvollen Nutzung durch Jugendliche ist jedoch eine feinere Unterteilung hilfreich, z.B. nach Eignung für verschiedene Altersklassen (wie z.B. die Kategorien für die freiwillige Selbstkontrolle von Spielfilmen), aber auch nach der Art des Inhalts (Unterhaltung, Naturwissenschaft, Suchmaschinen, für Kinder geeignete Inhalte usw.). Eine solche Einordnung erlaubt eine spezifische Einstellung der verwendeten Filtersoftware nach den inhaltlichen, pädagogischen und sozialen Anforderungen.

In beiden Fällen stellt sich jedoch das Problem, den jeweiligen Inhalt den Kategorien zuzuweisen. Da dort Text, Bilder, Audio-Sequenzen etc. zusammenspielen, ist eine solche

---

116 Bericht von Clive Feather in comp.risks 18.07 vom 17.04.1996, daß AOL bei der Registrierung den Namen der britischen Kleinstadt "Scunthorpe“ ausblendet, so daß sich Bewohner mit dem Ortsnamen "Sconthorpe“ anmeldeten, http://catless.ncl.ac.uk/Risks/18.07.html#subj3; Sperrung von Material der Dichterin Anne Sexton, weil in ihrem Nachnamen die Zeichenkette "sex“ enthalten ist, http://www.liii.com/~just4fun/news/article1.htm.

117 Probleme in dieser Richtung treten dann auf, wenn Filterungen auch für Erwachsene erzwungen werden.

Einordnung nur sehr selten automatisiert möglich. Daher ist eine Einzelbetrachtung und Einordnung durch einen Menschen notwendig. Dies ist insbesondere auch dann von Bedeutung, wenn erst das Gesamtbild oder die Zusammenstellung der medialen Komponenten den Kontext schafft, der eine korrekte inhaltliche Einordnung ermöglicht. Alle derzeit verfügbaren Kategoriensysteme ordnen mediale Einzelkomponenten ohne Berücksichtigung ihres Kontextes ein.

Um eine Einheitlichkeit der durchgeführten Einstufungen zu gewährleisten, ist weiterhin eine detaillierte und eindeutige Festlegung der angelegten Maßstäbe erforderlich. Dies ist um so wichtiger, je mehr Personen an der Einordnung beteiligt sind.

Im Grundsatz besteht ein solches Kategoriensystem aus einer Liste von Inhaltsgruppen und einer mehr oder weniger detaillierten Beschreibung, was zu jeder dieser Gruppen gehört. Ein großer Teil der Schemata beschränkt sich auf eine Eingruppierung der Eignung für Kinder und Jugendliche in verschiedene Kategorien wie "Sexualität“, "Gewalt“, "Drogen“. Nur wenige existierende Kategoriensysteme sehen zusätzliche Inhaltsbeschreibungen vor wie "Politik“, "Einkaufen“ o.ä.

Diese Systeme können öffentlich zugänglich sein, z.B. wenn die Einordnung einer Seite vom Autor selbst vorgenommen wird.[118] Kommerzielle Hersteller werden ihre Schemata eher nicht veröffentlichen; insbesondere die Einordnungen einzelner Seiten werden in diesen Fällen nicht preisgegeben, da in ihrer Erstellung ein wesentlicher Teil der Leistung liegt. Oft unterbleibt eine Veröffentlichung des Kategoriensystems auch aus der (nicht unberechtigten) Befürchtung, Anbieter jugendgefährdender Seiten könnten das Wissen um die Kategorisierungskriterien zur Umgehung der technischen Filterlösungen mißbrauchen. Um als Endbenutzer eine geeignete Auswahl treffen zu können, ist allerdings eine Transparenz der Einstufung unabdingbar. Auch Fehleinstufungen können nur identifiziert werden, wenn Kontrollen möglich sind.[119]

Für die konkrete Durchführung der Einordnung in technischer Hinsicht ist zu unterscheiden, wo und durch wen diese Einordnung vorgenommen wird. Daraus ergeben sich unterschiedliche Konsequenzen für Aufwand, Verwaltung, Verwendbarkeit und Aktualisierung des Verfahrens.

4.3.1.1 Autor/Autorin

Die einfachste, dem Umgang mit Videos, Spielen etc. nachempfundene Variante ist eine Eigeneinordnung durch den Autor oder die Autorin einer WWW-Seite oder Dokuments. Der zusätzliche Aufwand bei der Erstellung von statischen Seiten ist relativ gering.

Voraussetzung für ein gutes Funktionieren einer Selbsteinordnung sind die Redlichkeit und Sorgfalt der Verfassenden und eine weite Verbreitung eines einheitlichen Kategoriensystems. Hat sich ein solches System (oder auch mehrere) und seine Verwendung einmal durchgesetzt, könnten eine Einstufung der neuen Seiten im Interesse der Verfasser sein, damit sie auch Jugendlichen hinter Filtersystemen zugänglich sind. Sofern nicht eingeordnete Inhalte generell automatisch ausgefiltert würden, könnte ein eigentlich freiwilliges System zu einem faktischen Zwang werden, wie dies z.B. in der Filmindustrie der Fall ist.

Die Gefahr bei diesem Ansatz ist, daß gerade bei potentiell jugendgefährdenden Inhalten Autorinnen und Autoren die eigenen Inhalte harmloser einschätzen werden als z.B. Eltern. Eine Kontrolle der Einordnungen ist also erforderlich – durch die Öffentlichkeit oder auch durch eine dafür zu schaffende Kontrollinstanz. Außerdem wird es immer Seiten ohne eine

---

118 Dies sind z.B. SafeSurf, RSACi, ESRB, evaluWeb. Näheres zu diesen Systemen, u.a. eine Liste ihrer Kategorien findet sich im Abschnitt "Ratingsysteme“.

119 Im Rahmen der Programmtests werden diese Aspekte für einige Produkte ausführlich untersucht.

solche Einordnung geben – und sei es nur durch technische Fehler bei der Übertragung. Es muß also immer zusätzlich eine Verfahrensvorschrift für solche Fälle geben.

4.3.1.2 Unabhängige Instanz

Eine einheitlichere Vorgehensweise ist die Durchführung der Einstufung durch eine dritte – von der die Seite verfassenden und lesenden Person verschiedene – Instanz. Der Aufwand ist bei der großen Anzahl von Internetseiten[120] beträchtlich. Daher verfolgen die Anbieter solcher Einstufungen meist spezifische Interessen. Diese können politisch sein (z.B. Elterninitiativen, politische Verbände, Initiativen für bestimmte politische Ziele etc.) – daraus resultierende Einstufungen sind oft frei verfügbar[121] – oder auch kommerziell (dann meist nicht frei verfügbar): Die Einstufung ist in diesem Fall als Dienstleistung gegen eine Gebühr erhältlich.[122] Die Einordnung könnte auch gesetzlich vorgeschrieben sein und müßte dann von den Seitenanbietern bezahlt werden; allerdings gibt es so etwas bisher nicht.

In der Einordnung schlagen sich die unterschiedlichen Interessen der Einordnenden nieder. Dies ist bei der Auswahl eines Filtersystems zu beachten, da sonst eine ungewollte und im Falle von nicht offengelegten Filterregeln auch unerkannte Einschränkung des Angebotes in Kauf genommen wird.[123] Gerade hier ist also die Einsicht in die Einordnungskriterien eine wesentliche Voraussetzung für deren Nutzbarkeit.[124]

4.3.1.3 Internet Community

Eine weitere, dem Charakter des Internet besonders entsprechende Variante ist eine Einstufung durch alle Netzteilnehmenden. Generell könnte dann jeder und jede einen Vorschlag zur Einordnung einer Seite an eine verwaltende Instanz schicken. Je nach Charakter des Systems würden die Einordnungen dort überprüft oder direkt in eine Liste eingefügt, die dann – eventuell unter Verwendung bestimmter Software – abrufbar gehalten werden könnte.

---

120 Allein die Suchmaschine von AltaVista (www.altavista.de) hat nach eigenen Angaben über 140 Millionen Einträge in ihrer Datenbank; die Gesamtzahl der Seiten liegt weitaus höher.

121 So gibt die Organisation "Hatewatch“ auf ihrem Server www.hatewatch.org viele Seiten an, die rassistische Äußerungen enthalten. Bei entsprechendem Interesse könnte man sie in die Sperrliste übernehmen. Auf der anderen Seite bietet der Südwestdeutsche Rundfunk auf www.kindernetz.de eine Sammlung speziell für Kinder geeigneter Seiten; solche Listen sind auch häufig in kommerziellen Produkten enthalten.

122 Meist sind solche Listen kommerziell erhältlichen Programmen beigefügt und ihre Bezahlung damit in der Lizenzgebühr enthalten; ihre Aktualisierungen sind meist gegen kleinere Gebühren (unter 50 DM pro Jahr) erhältlich.

123 Auf www.peacefire.org finden sich viele Fälle, in denen nach Kriterien des Jugendschutzes unproblematische Server in den Sperrlisten kommerzieller Programme auftauchten. Dies waren z.B. Seiten, die einzelne Programme kritisierten, Seiten von amerikanischen Frauenverbänden, aber auch die Seite des Vatikans, die durch die Bezeichnung www.eros.co.il in die Sperrliste von XSTOP geriet.

124 Eine gute Hilfe zur Überprüfung der Sperrlisten kommerzieller Produkte (die diese Listen meist nicht im Klartext mitliefern), ist der produkt- und herstellerunabhängige Censorware Search Engine (http://cgi.pathfinder.com/netly/spoofcentral/censored/index.html). Einige Herstellern erlauben ähnliche Überprüfungen auf ihren Websites, z.B. http://www.cyberpatrol.com/cybernot/ für CyberPatrol.

Häufig bieten Hersteller solche Möglichkeiten und erweitern damit ihre eigenen Listen nach dem Bedarf der Nutzer. Z.T. bieten die Hersteller sogar finanzielle Anreize, um von möglichst vielen Personen Resonanz zu erhalten.[125]

Die verwaltende Instanz muß allerdings dafür sorgen, daß die Einordnungen ein gewisses Grundmaß an Einheitlichkeit aufweisen. Es wird dabei mit großer Wahrscheinlichkeit zu Mehrfacheinordnungen mit unterschiedlichen Resultaten kommen. Daher muß es ein Konzept geben, wie mit solchen Widersprüchen umzugehen ist. Außerdem sollte es nicht möglich sein, durch mehrfache Einstufung einer Seite als "pornographisch“ diese für das Internet praktisch zu sperren, wenn sie z.B. politische Aussagen enthält.

Dies könnte z.B. dadurch abgefangen werden, daß ein Anbieter, der in dieser Weise (oder auch durch eine unabhängige Instanz wie im vorhergehenden Abschnitt beschrieben) durch Dritte klassifiziert wird, über die Tatsache des Einstufungsvorgangs informiert wird und dann die Möglichkeit hat, gegen eine eventuelle Falscheinordnung vorzugehen. Dies könnte auch die Schadensersatzproblematik[126] entschärfen.

Mit dieser Methode kann eine sehr große Zahl von Seiten ohne hohen (zentralen) Aufwand eingestuft werden.

4.3.1.4 Individuell

Das aus Benutzungssicht zuverlässigste Vorgehen ist eine Einstufung am Endrechner selber. So könnte z.B. ein Lehrer oder eine Lehrerin eine genaue Liste aller für eine bestimmte Klasse verfügbaren Seiten definieren; und nur diese sind dann zugänglich.

Der Konfigurationsaufwand dafür ist allerdings sehr groß, da jede Seite (oder wenigstens jeder Server oder jede Domäne) explizit eingegeben werden muß. Der im Vergleich zum Angebot im Internet geringe Umfang solcher Listen schränkt die Möglichkeiten des Internet drastisch ein. Daher ist eine solche Möglichkeit in vielen Produkten häufig nur als Ergänzung zu einem der anderen Verfahren integriert und wird kaum als Einzellösung angeboten.

125 Z.B. World Opinion Rating Community von NetShepherd.

126 Eine falsche Bewertung kann für einen Anbieter unter Umständen enorme Umsatzausfälle nach sich ziehen.

4.3.1.5 Zusammenfassende Übersicht

Einordnung durch	**Aufwand**	**Aufwand Verteilung**	**Einheitlichkeit**	**Offenlegung der Kriterien**	**Überprüfbarkeit**	**Korrektheit**
Autor	gering bis mittel (je nach Art der Webseiten)	gering bis mittel, wenn auf Seite vermerkt	schwierig hängt vom Selbstkontrollmechanismus ab	ja (sonst Vorgang unmöglich)	hoch (Kontrolle notwendig)	weniger hoch, da Inhalte als zu harmlos eingeschätzt
Unabh. Instanz	hoch	hoch, da in Liste zu sammeln	hoch	nicht immer	gering	hoch Maßstäbe möglicherweise unbekannt
Internet Community	gering	hoch	gering	ja	hoch	weniger hoch
Individuell	sehr hoch	keiner	sehr hoch	entfällt	entfällt	hoch

4.3.2 Kennzeichnung

Eine Einordnung ist nur dann für eine technische Unterstützung des Jugendschutzes verwertbar, wenn sie für das lokale Endsystem verfügbar ist. Dazu wird sie

- entweder direkt auf einer Webseite vermerkt und kann beim Abruf ausgewertet werden oder
- in getrennten Listen gesammelt, die dann für den abrufenden Computer verfügbar sein müssen, so daß dieser einen Abgleich durchführen kann.

4.3.2.1 Seitenmarkierung

In einer WWW-Seite enthaltene Kennzeichnungen können nur von den verfassenden Personen praktikabel durchgeführt werden, da sie im Quelltext der Seite enthalten sein müssen. Sie eignen sich daher nur für die Selbsteinstufung. Aktualisierungen sind ebenfalls nur vom Autor durchzuführen, wenn er oder sie den Inhalt der Seite ändert; für den filternden lokalen Rechner besteht also kein Aktualisierungsbedarf.

Um eine allgemeine Verwertbarkeit dieser Angaben zu gewährleisten, sind formale Regeln für die Integration und die Übertragung erforderlich (z.B. PICS[127]). Diese müssen eine Markierung jeder Seite ermöglichen, auch wenn sie nur aus einem Bild oder einer Audio-Sequenz[128] besteht und keine expliziten HTML[129]-Befehle enthält.

---

127 Platform for Internet Content Selection, http://w3c.org/PICS/, eine Initiative des WorldWideWebConsortiums (W3C), die Regeln zur Angabe und Übertragung von Bewertungen im Internet spezifiziert. Auf diese Spezifikation basieren die verbreitetsten Labeling-Systeme SafeSurf und RSACi (vgl. Abschnitt 4.5)

128 Eine Lösung, die sich nur für Musikdateien eignet, ist der neue MPEG7-Standard (Kompressionsverfahren), der im Rahmen einer MPEG-Datei die Angabe von inhaltlichen Stichwörtern oder Beschreibungen ermöglicht. Allerdings ist dies nicht so standardisiert, daß es bisher systematisch verwendbar wäre.

Ist ein solches System weit verbreitet, steigt die Motivation, Kennzeichnungen in eigene Webseiten einzufügen, da diese einerseits eine Blockade wegen fehlender Kategorisierung verhindern und andererseits die Anzahl der erwünschten Zugriffe steigern können.[130]

4.3.2.2 Sammlung in Listen

Ratings können statt auf der WWW-Seite selbst auch separat gesammelt und verwaltet werden. Dies geschieht im allgemeinen dann, wenn die Einordnung von Dritten (also Institutionen oder der Öffentlichkeit) durchgeführt werden.

Für die Verwaltungsinstanzen solcher Listen gelten ähnliche Anmerkungen wie die oben für die Einstufungsinstanzen gemachten: Es stehen meist politische oder kommerzielle Interessen dahinter, die bei der Auswahl einer Filterlösung beachtet werden sollten.

Für die konkrete Filterung muß eine solche Liste für den Endrechner verfügbar sein: entweder als lokal gespeicherte Kopie – die dann immer wieder durch aktuelle Versionen ersetzt werden muß – oder online auf einem aktiv arbeitenden Server, der vor dem Laden einer Seite jeweils über deren Zulässigkeit befragt wird (dann entfällt die Übertragung der neuen Versionen, der Server muß allerdings dauernd und schnell verfügbar sein.[131]).

In beiden Fällen ist die Aktualität einer solchen Liste der kritische Parameter für die Wirksamkeit und Korrektheit einer darauf aufbauenden Filterung: Im Internet entstehen ständig neue Seiten und werden bestehende verändert, so daß die Einstufung entsprechend schnell aktualisiert werden muß.

4.3.3 Auswahl

Die eigentliche Aufgabe eines Werkzeugs zur technischen Unterstützung des Jugendschutzes im Internet ist die Auswahl geeigneter bzw. die Sperrung ungeeigneter Seiten. Die Durchführung dieser Auswahl erfolgt entweder direkt auf dem Rechner des Abrufers oder auf den vorgeschalteten Netzkomponenten (Server eines Internetproviders, Proxy[132]).

Dies kann aufgrund eines oder mehrerer der genannten Kategorienschemata oder durch automatisierte Filterung geschehen; am effektivsten sind Kombinationen.

Wichtig ist in allen Fällen eine Authentifizierung der Einordnung, z.B. durch digitale Signaturen. Ansonsten könnte man mit einfachen "Filter-Filtern“ die Kennzeichnungen ausfiltern oder durch harmlose ersetzen.[133]

---

129 HTML: Sprache zur Programmierung von Internetseiten

130 Einige Systeme sehen neben der Angabe der Eignung für Kinder auch eine Inhaltsbeschreibung vor, die die Resultate von Suchvorgängen verbessern soll. Auch haben viele Anbieter von kostenpflichtigen Angeboten für Erwachsene kaum Interesse an jugendlichen Besuchern, da sie Kosten für die Internetnutzung verursachen, aber nicht zu den zahlenden Kunden gehören.

131 Außerdem fallen auf diesem Server viele aussagekräftige Benutzerprofile an, da ja vor dem Download jeder Seite, jedes Bildes und jedes anderen Files gefragt wird, wie das denn gekennzeichnet ist. Der Verkauf dieser Benutzerprofile würde möglicherweise den Betrieb des Ratingdienstes sogar finanzieren können; allerdings wäre bei Durchsetzung eines solchen Systems eine freie Bestimmung über die Weitergabe (oder eben die Nichtweitergabe) der persönlichen Daten bei Wunsch nach Filterung nicht mehr möglich.

132 Rechner, der als Vermittler beim Abruf von Internetseiten dient.

133 WebWasher und andere Programme, zum Beispiel der Internet Junkbuster, können von Benutzern eingesetzt werden, um Werbebilder, JavaScript, Java, Active-X, Popup-Fenster und andere Teile von Webseiten gezielt auszufiltern bzw. durch leere Bilder und harmlose Platzhalter zu ersetzen.

4.3.3.1 Inhaltseinordnung

Geschieht die Auswahl nach Inhaltseinordnung, so ist es für den Administrator des Systems möglich, in Abhängigkeit vom Kategoriensystem genaue Richtlinien für die Auswahl vorzugeben. So kann definiert werden, welche Inhalte angezeigt werden (z.B. jede Seite mit dem Label "für Kinder unter 10“ oder "Grundschule“) und welche Seiten verborgen bleiben (z.B. wenn nur "Naturwissenschaft“ zulässig sein und damit Seiten "nur für Erwachsene“ oder auch "Spiele“ gesperrt bleiben). Entsprechend spricht man von Positivauswahl – die anzuzeigenden Seiten werden charakterisiert – oder Negativauswahl, wenn die zu sperrenden Seiten benannt werden. Dabei ist eine Positivauswahl immer restriktiver, da damit alle Seiten ohne die geforderte Eigenschaft ausgeschlossen werden; hingegen erlaubt eine Negativauswahl weiterhin einen Zugriff auf fast alle Internetangebote, sofern sie nicht die ausgewählte Einordnung besitzen.

Eine Inhaltskennzeichnung in Reinform sperrt alle nicht eingestuften Seiten oder Server. Damit wird ein großer Teil des Internet von vornherein ausgeschlossen, solange sich nicht weltweit Kategoriensysteme verbreitet haben. Als alleiniger Mechanismus eignet sich eine Filterung nach Inhaltskennzeichnung also erst dann, wenn ein Großteil der Angebote eingeordnet ist.

4.3.3.2 Automatisierte Filterung

Um auch nicht gekennzeichnete Seiten oder Server beurteilen zu können, werden automatische Filtersysteme eingesetzt. Sie blockieren Seiten, auf denen bestimmte Schlüsselwörter oder Sätze enthalten sind oder zeigen zumindest diese Ausschnitte nicht an. Einige Systeme setzen auch kontextsensitive Verfahren ein.

Obwohl dieser Ansatz allein nicht zuverlässig filtern kann,[134] ist er u.U. als Ergänzung zu den oben genannten Filterungen nach Einordnungen hilfreich und kann gerade bei Negativlisten die Zuverlässigkeit erhöhen. Seine Leistungsfähigkeit hängt wesentlich von der "Intelligenz“ der Filterung ab.[135]

4.3.3.3 Filtermeldungen

Die Meldungen des Filtersystems beim Zugriff auf unerwünschte Inhalte können sehr unterschiedlich sein. Im einfachsten Fall werden z.B. bestimmte Wörter geschwärzt oder ausgeblendet (so z.B. NetNanny). Bei einigen Produkten funktioniert der Zugriff auf bestimmte Server einfach nicht (ähnlich wie bei einem Serverausfall, also ohne eine Meldung über erfolgte Filterung, so z.B. CyberSitter). Es sind auch Meldungen über den unerlaubten Zugriff möglich (z.B. CyberPatrol). Einige Produkte ergänzen eine solche Meldung durch Hinweise auf (für Kinder) geeignete Seiten und bereiten die Meldung auch optisch ansprechend auf (z.B. WebChaperone).

Durch triviale Änderung kann man diese Programme auch einsetzen, um Ratinginformationen auszufiltern oder durch harmlose Ratings zu ersetzen.

134 Ein gängiges Beispiel für eine unbeabsichtigte Sperrung ist das Internetangebot der University of Sussex auf www.sussex.ac.uk, das durch die Filterung nach dem Wort Sex u.U. gesperrt wird. Andererseits werden Bilder oder Audio-Sequenzen mit harmlosen Namen, aber rassistischem Inhalt durch Schlüsselwortfilterung nicht gesperrt.

135 Viele Filterprogramme bieten eine "kontextsensitive“ Filterung nach Schlüsselwörtern an (z.B. WebChaperone, NetNanny). Im einfachsten Fall sind dafür statt einzelner Wörter Sätze oder Ausdrücke enthalten, nach denen gefiltert wird. Aufwendigere Verfahren untersuchen, welche Wörter in der Nähe von problematischen Begriffen auftauchen, und fällen daraus ihre Filterentscheidung. Gängiges Testbeispiel ist dafür eine Suche nach "Safer Sex“. Auch nach einer Filterung sollten Angebote zur Verhütung oder zur Aids-Aufklärung weiter zu sehen sein.

Zusätzlich können der gesamte Filterprozeß oder auch nur die Regelverletzungen protokolliert werden. Manche Werkzeuge bieten außerdem noch spezielle Suchfunktionen oder Listen von für Kinder geeigneten Seiten an, auch direkt in der Meldung über eine gesperrte Seite. Solche Ergänzungsfunktionen sind nicht direkt für den Jugendschutz relevant; sie erfüllen eher pädagogische Funktionen, können aber die Akzeptanz des Systems steigern.

Generell leistet das Verhalten des Filterprogramms während der Internetnutzung einen wesentlichen Beitrag zur Akzeptanz bei den benutzenden Kindern und Jugendlichen. Es sollte die Filterung verständlich erläutern und die Benutzung des Internet weiterhin ermöglichen.[136] Dieser Aspekt wird bei der Auswertung der praktischen Tests näher erläutert.

4.3.4 Zusammenfassung

Es zeigt sich, daß es für das Zusammenspiel von Einordnung, Kennzeichnung und Auswahl von Internetinhalten zur technischen Unterstützung des Jugendschutzes viele verschiedene Ansätze gibt. Keiner der Einordnungsansätze und auch keiner der verschiedenen Filtermechanismen kann jedoch allein Jugendschutz gewährleisten. Daher sind zur optimalen technischen Unterstützung immer Kombinationen mehrerer Ansätze empfehlenswert, die sich gut an den individuellen Bedarf anpassen lassen. Entsprechend wird dies ein Auswahlkriterium für die zu testenden Produkte im weiteren Verlauf dieser Studie sein.

Wie in den einzelnen Abschnitten ebenfalls angerissen wurde, ist das Problem allerdings nicht allein durch technische Hilfsmittel zu lösen. Es müssen zusätzlich die organisatorischen und gesellschaftlichen Rahmenbedingungen geschaffen werden, die für eine möglichst weite Verbreitung der Einordnungen sorgen. Wie diese aussehen könnten, werden wir an anderer Stelle diskutieren.

4.4 Kennzeichnungssystem: PICS

4.4.1 Aufbau und Dienste

"Platform for Internet Content Selection“ (PICS)[137] ist eine Initiative des World Wide Web Consortiums (W3C), um Metadaten von Dokumenten zu verwalten. Dazu spezifiziert PICS ein abstraktes Verfahren zur Definition beliebiger Kategoriensysteme (Rating Systems), nach denen Inhalte eingeordnet werden können. Hat man sich auf dieser Basis ein oder mehrere konkrete Kategoriensysteme definiert, kann man Dokumente innerhalb dieser Systeme einordnen ("raten“, "bewerten“) und diese Einordnungen mit dem Dokument oder durch unabhängige Stellen verteilen lassen.

Wird die Einordnung eines Dokumentes durch den Autor selbst vorgenommen und zusammen mit dem Dokument verteilt, handelt es sich um ein First-Party-Rating. Dieses Verfahren erlaubt die Anwendung von PICS auf ausnahmslos alle Inhalte, einschließlich elektronischer Post. Alternativ kann die Einordnung eines Dokumentes durch Dritte (einer vom Autor unabhängigen Stelle) erfolgen, selbst gegen den Willen und ohne Kooperation des Autors. Bei diesem Third-Party-Rating ist es notwendig, das Bezugsdokument benennen zu

136 So lieferte z.B. NetNanny beim Aufruf der Werbeseite eines Anbieters von Pornographie etwa zwanzig Meldungen, daß einige Wörter nicht gezeigt werden. Jede dieser Fehlermeldungen erforderte eine Bestätigung mit Mausklick oder Tastendruck. Die gefilterte Seite war zwar nicht mehr zu lesen, die Bilder aber immer noch zu sehen. Andere Produkte, z.B. CyberPatrol oder WebChaperone, lieferten statt dessen eine Meldung über Filterung und zeigten die Seite gar nicht an.

137 Vgl. http://w3c.org/PICS/ mit Informationen zur Spezifikation, zum Funktionsumfang und zur Leistungsfähigkeit.

können. Daher ist in diesem Fall nur die Einordnung von Dokumenten möglich, die eine URL (Uniform Resource Locator, eindeutiger symbolischer Name eines WWW-Dokuments) haben.[138]

Es ist wichtig zu verstehen, daß PICS kein einzelnes, konkretes Kategoriensystem darstellt, sondern nur ein Verfahren vorgibt, mit dem man beliebige Kategoriensysteme maschinenlesbar formulieren kann. Programme, die PICS unterstützen, können die Beschreibung eines Kategoriensystems einlesen und danach Einordnungen von Dokumenten in dieses Kategoriensystem, sogenannte "PICS-Label“, auswerten. Beispiele für solche Kategoriensysteme, die sich nach PICS erfassen lassen, sind die FSK-Einordnung (eindimensional: Altersangabe) oder die RSACi-Einordnung[139] für Webseiten (vierdimensional: "Sex“, "Gewalt“, "Nacktheit“ und "Sprache“). Es werden in der Literatur jedoch auch PICS-Kategoriensysteme vorgeschlagen, die nicht auf den Bereich Jugendschutz zielen. Darunter ist ein Vorschlag, der sich auf den Einsatz von PICS im Bereich Urheberrecht und Rechtemanagement bezieht[140], das mit PICS verwandte Projekt P3P ("Platform for Privacy Preferences“)[141] des W3C sowie der Ansatz von Joel Reidenberg, PICS zur Signalisierung von Privacy-Optionen einzusetzen[142].

Mit einem Kategoriensystem werden die Dimensionen definiert, entlang derer später die Einordnung der Seiten erfolgt. Für jede dieser Dimensionen ist getrennt festlegbar, welcher Art die Skala ist (numerisch, numerisch-kontinuierlich, diskrete Werte ohne Ordnung). Einzelnen Werten oder Wertebereichen können Symbole zugeordnet werden. Für jede Dimension kann bestimmt werden, ob eine Einordnung Pflicht oder optional ist. Generell ist es möglich, in der Definition des Kategoriensystems Hinweise darauf unterzubringen, wie ein Browser oder ein anderes Werkzeug die Kategorien auf seiner Benutzeroberfläche darstellen soll.

4.4.2 PICS-Label

Die konkrete Einordnung eines Dokumentes in ein PICS-konform definiertes Kategoriensystem heißt PICS-Label. Ein PICS-Label ist ein einfacher Textblock, der alle zum Label gehörenden Informationen enthält: die Versionsnummer des verwendeten PICS-Standards, einen Verweis auf die URL, in der das verwendete Kategoriensystem definiert ist, sowie eine Einordnung einer URL oder einer Gruppe von URLs in dieses Kategoriensystem.

Wie PICS-Label aussehen können, zeigen folgende Beispiele, die aus dem HTML-Code der Webseiten des W3C und des Playboy extrahiert wurden:

- www.w3.org,
  `PICS-Label für RSACi und SafeSurf mit einer Null-Einstufung für`

---

138 Damit ist eine Einordnung keineswegs auf WWW-Dokumente beschränkt, sondern es ist ebenso möglich, News-Artikel anhand von Newsgroups oder anhand ihrer Message-ID oder auch beispielsweise FTP-oder Gopher-Dateien per URL zu identifizieren. Auf E-Mail-Nachrichten – sofern sie nicht inhaltlich über einen anderen Dienst verfügbar gemacht werden – kann sich eine URL nicht beziehen, sondern lediglich auf einen Adressaten (z.B. "mailto:name@domain.de“). Hierzu wäre eine PICS-Einordnung vermutlich nicht sinnvoll. Zur Definition von URL siehe RFC 1738, ftp://ftp.uni-paderborn.de/doc/rfc/rfc-1700-1799/rfc1738.gz.

139 Anbieter eines Kategoriensystems, vgl. Kapitel 4.5

140 Vgl. http://w3c.org/IPR/.

141 Vgl. http://w3c.org/P3P/.

142 Joel R. Reidenberg: Information Policy Rules through Law and Technology, 19th International Conference Privacy Data Protection Commissioners, Brüssel, 17.-19. September 1997, http://www.privacy.fgov.be/conference/pt4_2.html.

```
alle angegebenen Dimensionen:
<meta http-equiv="PICS-Label“ content='(PICS-1.1
"http://www.rsac.org/ratingsv01.html“ l gen true comment "RSACi
North America Server“ by "philipd@w3.org“ for
"http://www.w3.org“ on "1996.04.16T08:15-0500“ r (n 0 s 0 v 0 l
0))'>
<meta http-equiv="PICS-Label“ content='(PICS-1.1
"http://www.classify.org/safesurf/“ l gen true for
"http://www.w3.org“ by "philipd@w3.org“ r (SS~~000 1 SS~~100
1))'>
```

- www.playboy.com,
  PICS-Label für RSACi und Safesurf; bei RSACi mit der Einstufung "Nacktheit = 4, Sex = 3, Gewalt = 0, Sprache = 4“:

```
<meta http-equiv="PICS-Label“ content='(PICS-1.1
"http://www.rsac.org/ratingsv01.html“ l gen true comment "RSACi
North America Server“ for "http://www.playboy.com“ on
"1996.05.04T06:51-0800“ r (n 4 s 3 v 0 l 4))'>
<meta http-equiv="PICS-Label“ content='(pics-1.1
"http://www.classify.org/safesurf/“ l gen t for
"http://www.playboy.com/“ r (ss~~000 6 ss~~100 1))'>
```

Ein PICS-Label kann sich auf ein einzelnes Dokument oder auf einen ganzen Teilbaum einer Website beziehen. Genauere Einordnungen überschreiben dabei allgemeinere Einordnungen. Teil des PICS-Labels kann auch ein Vermerk über den Zeitpunkt der Einordnung, eine Geltungsdauer der Einordnung sowie eine Prüfsumme des eingeordneten Dokumentes sein (nur bei Einordnung spezifischer Dokumente). Optional kann das Label außerdem einen Vermerk enthalten, der angibt, wer (welche Person) die Einordnung vorgenommen hat und für wen (welche Organisation) die Einordnung vorgenommen wurde. Schließlich beinhaltet das PICS-Label die konkreten Werte, die über das Label dem Dokument oder den Dokumenten zugeordnet werden.

PICS-Label können auf verschiedenen Wegen verteilt werden: Sie können in dem Dokument, das sie einordnen, direkt enthalten sein oder von dem Webserver für dieses Dokument zusammen mit dem Dokument ausgeliefert werden. Das PICS-Label ist dann entweder im Kopf der Webseite direkt enthalten, oder es wird als Bestandteil des HTTP[143]-Dialoges bei der Anforderung der Webseite zusammen mit der eigentlichen Seite vom Servers übergeben. Der Standard sieht auch vor, PICS-Label als Bestandteile von Usenet-News-Nachrichten oder Internet-Mail im Kopf der jeweiligen Nachrichten zu verteilen. Ebenso ist es möglich, Labels für Dokumente von einer dritten Partei zu beziehen, wenn die betreffenden Dokumente durch eine URL eindeutig identifizierbar sind. Diese dritte Partei wird im PICS-System als *Label Bureau* (Verteilstelle für Labels, im folgenden auch Label-Provider) bezeichnet.

Um die Integrität der Label zu bewahren und die Einordnungen zurechenbar zu machen, sieht der Standard zwei Optionen vor: Als Bestandteil des Labels kann eine MD5-Prüfsumme mit dem Label zusammen übermittelt werden. Die Einordnung des Labels bezieht sich auf das Dokument mit der angegebenen MD5-Prüfsumme. Verändert sich also der Inhalt eines Dokumentes nach dessen Einordnung auch nur um ein einziges Bit, wird es eine andere MD5-Prüfsumme haben, so daß technisch die abgesicherte Zuordnung des PICS-Labels zu dem Dokument nicht mehr besteht. Das veränderte Dokument muß dann wie ein nicht eingeordnetes Dokument behandelt werden. Die zweite Option unterbindet das Fälschen oder Austauschen von PICS-Labels, indem die Einordnung selbst durch den Rating-Service (s.u.) digital signiert wird. Dadurch ist sichergestellt, daß die Einordnung eines Dokumentes

143 Protokoll zur Übertragung von Internetseiten

einem bestimmten Rating-Service zugerechnet werden kann. Einem Angreifer wird es so erschwert, Labels von bekannten und vertrauenswürdigen Rating-Services zu fälschen.

Der PICS-Standard selbst legt ausdrücklich nicht fest, wie die Schlüssel zur Prüfung der digitalen Signatur verteilt oder verwaltet werden. Er definiert lediglich, wie eine Signatur technisch auszusehen hat und auf welche Komponenten des PICS-Labels sie sich bezieht, d.h. welche Semantik das Vorhandensein einer gültigen Signatur an einem PICS-Label hat. Insbesondere ist zur Zeit nur vorgesehen, mediale Einzelkomponenten ohne Berücksichtigung ihres Kontextes mit PICS-Labeln zu versehen, die auch nur jeweils einzeln digital signiert sein könnten.

4.4.3 PICS-Rules

PICS-Rules sind ein Satz Regeln, mit denen ein entfernter Filter (Remote Filtering Agent; nicht auf dem lokalen System installiert) durch einen Dienstnehmer programmiert werden kann. Mittels PICS-Rules kann zum Beispiel beschrieben werden, welche Inhalte ein Online-Dienst einem Haushalt zur Verfügung stellen soll und welche Inhalte gemäß ihrer PICS-Label ausgefiltert werden sollen. PICS-Rules bieten aber auch die technische Möglichkeit, daß Provider beispielsweise staatliche Vorgaben umsetzen, welche Inhalte in ihren Proxy-Servern gemäß ihrer PICS-Labels blockiert werden müssen. Denkbar und im PICS-Rules-Standard explizit erwähnt ist weiterhin die Möglichkeit, daß die Filterkonfiguration für einen Nutzer zusammen mit seiner Suchanfrage an Suchmaschinen kommuniziert wird, so daß ausschließlich Verweise auf Seiten gefunden werden, die der Filterkonfiguration des Nutzer gerecht werden.

PICS-Rules legen fest, welche unterschiedlichen Kategoriensysteme für ein Nutzerprofil zutreffend sein sollen, welche Verteilstellen nach Einordnungen für diese Kategoriensysteme befragt werden sollen und welche Einstufungen in jedem dieser Kategoriensysteme notwendig sind, damit die Seite für dieses Nutzerprofil als akzeptabel bewertet wird. PICS-Rules liefert damit eine Lösung, mit der mehrere unterschiedliche Kategoriensysteme zu einem einheitlichen, vordefinierten Nutzerprofil zusammengefaßt werden können, und einen Mechanismus, ein solches Nutzerprofil zwischen beliebigen PICS-Rules kompatiblen Anwendungen auszutauschen.

Damit wird es auch möglich, fertige Profile für interessierte Nutzer zur Verfügung zu stellen, ohne daß diese sich mit den Details der Konfiguration befassen oder sich im einzelnen dafür interessieren müssen, welche Dokumente damit unter welchen Bedingungen gesperrt werden oder was die einzelnen Einordnungschemata bedeuten.

Aus den *Frequently Asked Questions* zu PICS[144]:

"Q: Setting the filtering rules is too much of a bother for me. Can't I just find someone I trust and install their rules?

A: Not yet, but we hope that vendors will implement this feature soon. This was one of the primary motivations for defining the PICS Rules interchange format for filtering rules, so that you'd be able to easily import and install filtering rules created by someone else that you trust.“

4.4.4 Rating-Services und Label-Provider

Ein Dienstleister, der ein Kategoriensystem definiert hat oder ein bestehendes Kategoriensystem unterstützt, kann Kennzeichnungen (Label) gemäß diesem Kategoriensystem erzeugen. So ein Dienstleister heißt in der Nomenklatur von PICS ein

144 Vgl. http://w3c.org/PICS/#FAQ.

"Rating-Service“ (Einordnungs- oder Auswertedienst). Diese Labels werden dann entweder mit dem Dokument selbst (in der Regel bei Einordnung durch den Anbieter, First-Party-Rating) oder durch Dritte zur Verfügung gestellt und verteilt. Diese Aufgabe wird durch sogenannte Label-Provider (Verteilstellen) vorgenommen. Der PICS-Standard geht davon davon aus, daß die meisten Rating-Services auch Label-Provider sein werden, setzt dies aber nicht konstruktionsbedingt voraus.

4.5 Kategoriensysteme

Generell beruht jede Filterung im Internet auf gewissen Kriterien, deren Erfüllung systematisch erkennbar ist und die damit eine Einordnung zulassen. Dies können die graphische Gestaltung einer Seite sein (so z.B. von Werbefiltern durchgeführt), Prüfsummen bestimmter Bilder (Kinderpornographie-Suchprogramm PERKEO) oder Schlüsselwortsuchen.

Soll jedoch dem Benutzer eine differenzierte Auswahl durch seine Filtersoftware ermöglicht werden, ist ein Kategoriensystem oder Ratingsystem zur Inhaltseinordnung der Seiten erforderlich. Allen solchen Systemen ist gemeinsam, daß sie ein Schema anbieten, in das Inhalte eingeordnet und aus dem die Eignung für Altersgruppen oder bestimmte Anwendungsgebiete ersehen werden können. Dabei kann die Einordnung direkt in eine Systematik von Altersgruppen[145] erfolgen oder in inhaltliche Kategorien[146], aus denen sich die Eignung für bestimmte Altersgruppen von jedem Benutzer bzw. Administrator individuell ableiten läßt.

Diese Systematik kann sehr einfach sein – also nur wenige Unterscheidungsmerkmale anbieten[147] – oder auch komplex mit vielen Kategorieebenen[148]. Die einfachen Systeme haben den Vorteil einer sehr schnell durchführbaren Einordnung und einer einfachen Filterung; komplexe Systeme bieten hingegen durch den größeren Konfigurations- und Filteraufwand eine bessere Anpassung an den individuellen Bedarf.

Kategoriensysteme gibt es als produktunabhängige Angebote verschiedener, meist nicht kommerzieller Institutionen, die den Standard zur Einordnung und z.T. auch einige Hilfswerkzeuge zur Durchführung der Einordnung zur Verfügung stellen, oder auch in Filterprodukte integriert, dann meist weniger transparent und eher proprietär.

Bereits im vorigen Kapitel wurde festgestellt, daß die Transparenz der Einordnungsmaßstäbe eine Grundvoraussetzung zu einer sinnvoller Nutzung und Kontrolle der Inhaltsfilterung ist. Diese Anforderung erfüllen alle von speziellen Filterprogrammen unabhängigen Systeme – die meist auf dem PICS-Standard basieren – nahezu vollständig. Im Gegensatz dazu sind die Maßstäbe der Einordnungslisten in kommerziell erhältlichen Produkten eher undurchsichtig.[149] Daher wird bei der folgenden Evaluation der Kategoriensysteme auf die proprietären Ansätze nicht eingegangen. Sie unterscheiden sich von den öffentlichen Systemen allerdings nur in der Realisierung, nicht aber in ihrer Einordnungssystematik.

---

145 Z.B. "Age Range“ von SafeSurf oder "Rating Categories“ von ESRB.

146 Z.B. "Content Descriptor“ von ESRB.

147 evaluWeb unterscheidet in "General Viewing“, "Parental Assistance“, "Mature Content“.

148 SafeSurf formuliert für zehn verschiedene Kategorien jeweils 9 Abstufungen.

149 Prinzipbedingt ist die Transparenz bei einem produktunabhängigen System eher zu gewährleisten, weil hier die Bewertung durch von der Organisation unabhängige Personen erfolgt, die sie nur bei Kenntnis der Maßstäbe qualifiziert durchführen können. Produktabhängige Bewertungsschemata sind eher nicht öffentlich, da in den Bewertungen ein wesentlicher Teil der – käuflich zu erwerbenden – Leistung liegt. Immerhin unterstützen die meisten dieser Systeme den PICS-Standard, erlauben also die Integration der Systeme.

4.5.1 Produktunabhängige Kategoriensysteme

Die am weitesten verbreiteten produktunabhängigen Kategoriensysteme beruhen alle auf dem PICS-System. Sie verwenden auf dieser Basis jeweils eigene formale Beschreibungssprachen, um einordnende HTML-Einträge zu erzeugen, deren Interpretation durch geeignete Programme möglich ist. Dabei können mehrere solche Einträge in einer Webseite enthalten sein, die Seite kann also gleichzeitig mehrere Einordnungen tragen.[150] [151]

Alle Systeme sind nur einsprachig (Englisch) und beruhen in ihrer Abstufung auf dem kulturellen Hintergrund von Nordamerika.

Um ein für Deutschland und Europa verwendbares System zu schaffen, ist also zumindest eine Übertragung in die jeweiligen Landessprachen erforderlich, die allerdings nicht nur eine Übersetzung durchführen darf, sondern auch Rücksicht auf die jeweiligen Kulturvorstellungen nehmen muß. Um dem grenzübergreifenden Charakter des Internet Rechnung zu tragen, ist langfristig ein mehrsprachiges und auch multikulturelles System anzustreben.

	Webseite	**Hintergrund**	**Software-plattform**	**Offenlegung der Kriterien**
ESRB	www.esrb.org/	Entertainment Software Rating Board, auch für PC-Spiele Auswertung frei, Einordnung eigener Seiten gegen Gebühr	PICS-fähiger Browser	ja
evaluWeb	calvin.ptloma.edu /~spectre/evaluweb/	nicht kommerziell	PICS-fähiger Browser	ja nur drei Einstufungen
RSACi	www.rsac.org/	Recreational Software Advisory Council (Internet) nicht kommerziell, finanziert durch Sponsoren	CyberPatrol Microsoft Internet Explorer	ja eher knapp
SafeSurf	www.safesurf.com/	Zusammenschluß von Eltern	PICS-fähiger Browser	ja; sehr ausführlich

Abb. 4-1: Übersicht Ratingsysteme

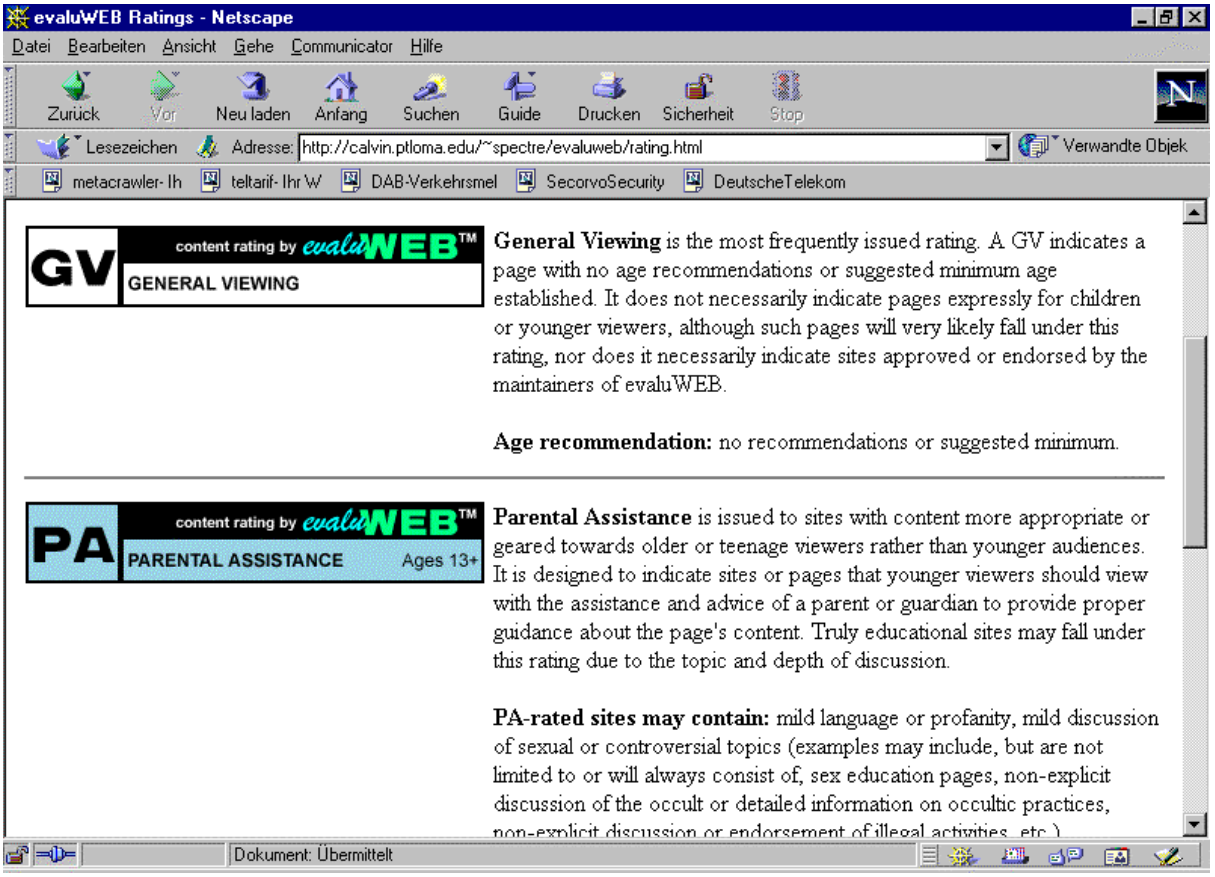
4.5.1.1 evaluWeb

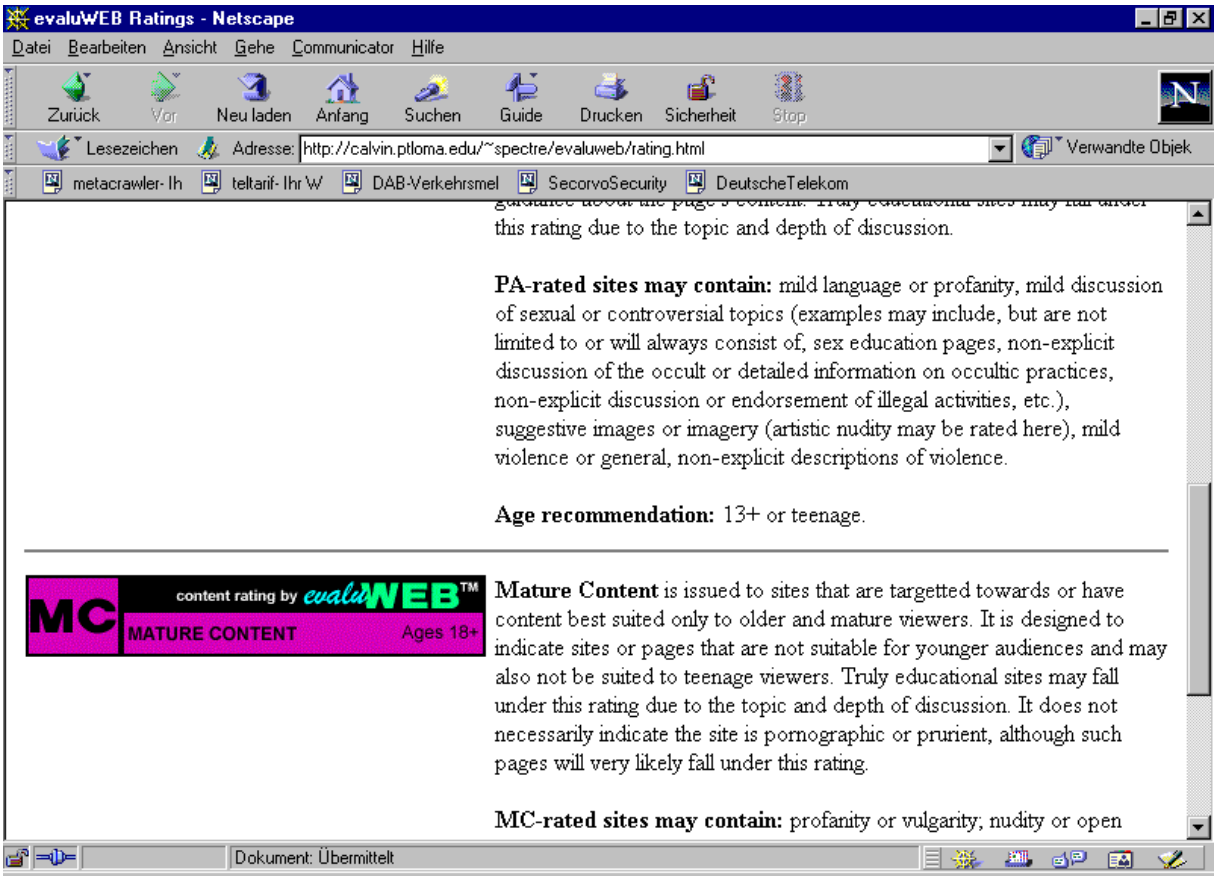
evaluWeb bietet drei Kategorien, die gleichzeitig Alterseignung und Inhalt kennzeichnen[152]:

150 Z.B. enthält http://www.playboy.com Bewertungen nach RSACi und SurfWatch.

151 Bisher gibt es keinerlei Plausibilitätsprüfungen über die Übereinstimmung der verschiedenen Bewertungseinträge. PICS-Rules erlaubt eine beliebige Kombination von PICS-konformen Kategoriensystemen, die nicht notwendigerweise inhaltlich sinnvoll sein muß.

152 Für nähere Beschreibungen der Kategorien vgl. http://www.esrb.org/esrbi/about.html.


evaluWEB Ratings - Netscape
Datei Bearbeiten Ansicht Gehe Communicator Hilfe
Zurück Vor Neu laden Anfang Suchen Guide Drucken Sicherheit Stop
Lesezeichen Adresse: http://calvin.ptloma.edu/~spectre/evaluweb/rating.html
Verwandte Objek
metacrawler- Ih teltarif- Ihr W DAB-Verkehrsmel SecorvoSecurity DeutscheTelekom
GV
content rating by evaluWEB™
GENERAL VIEWING
General Viewing is the most frequently issued rating. A GV indicates a page with no age recommendations or suggested minimum age established. It does not necessarily indicate pages expressly for children or younger viewers, although such pages will very likely fall under this rating, nor does it necessarily indicate sites approved or endorsed by the maintainers of evaluWEB.
Age recommendation: no recommendations or suggested minimum.
PA
content rating by evaluWEB™
PARENTAL ASSISTANCE Ages 13+
Parental Assistance is issued to sites with content more appropriate or geared towards older or teenage viewers rather than younger audiences. It is designed to indicate sites or pages that younger viewers should view with the assistance and advice of a parent or guardian to provide proper guidance about the page's content. Truly educational sites may fall under this rating due to the topic and depth of discussion.
PA-rated sites may contain: mild language or profanity, mild discussion of sexual or controversial topics (examples may include, but are not limited to or will always consist of, sex education pages, non-explicit discussion of the occult or detailed information on occultic practices,
Dokument: Übermittelt


evaluWEB Ratings - Netscape
Datei Bearbeiten Ansicht Gehe Communicator Hilfe
Zurück Vor Neu laden Anfang Suchen Guide Drucken Sicherheit Stop
Lesezeichen Adresse: http://calvin.ptloma.edu/~spectre/evaluweb/rating.html
Verwandte Objek
metacrawler- Ih teltarif- Ihr W DAB-Verkehrsmel SecorvoSecurity DeutscheTelekom
this rating due to the topic and depth of discussion.
PA-rated sites may contain: mild language or profanity, mild discussion of sexual or controversial topics (examples may include, but are not limited to or will always consist of, sex education pages, non-explicit discussion of the occult or detailed information on occultic practices, non-explicit discussion or endorsement of illegal activities, etc.), suggestive images or imagery (artistic nudity may be rated here), mild violence or general, non-explicit descriptions of violence.
Age recommendation: 13+ or teenage.
MC
content rating by evaluWEB™
MATURE CONTENT Ages 18+
Mature Content is issued to sites that are targetted towards or have content best suited only to older and mature viewers. It is designed to indicate sites or pages that are not suitable for younger audiences and may also not be suited to teenage viewers. Truly educational sites may fall under this rating due to the topic and depth of discussion. It does not necessarily indicate the site is pornographic or prurient, although such pages will very likely fall under this rating.
MC-rated sites may contain: profanity or vulgarity; nudity or open
Dokument: Übermittelt

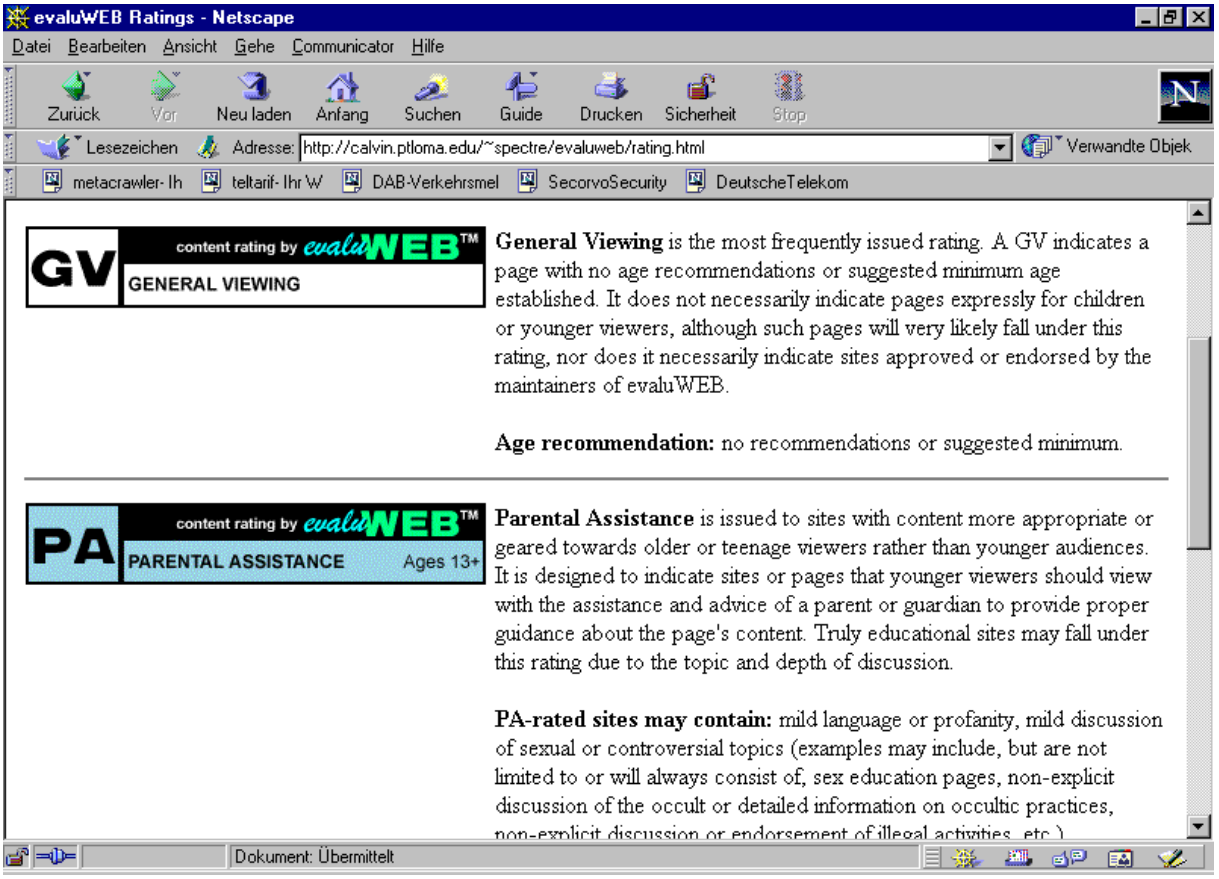


Abb. 4-2: Label von evaluWEb

Nach eigenen Angaben wurden bisher (Stand 2/99) über sieben Millionen Seiten eingeordnet.

Die Abfrage der Einordnungen erfolgt über einen eigenen PICS-Server und kann damit in jeden PICS-fähigen Browser integriert werden. Auf dem Webserver werden die Integration und eine Anleitung für verschiedene Versionen des Microsoft Internet Explorer angeboten.

Es gibt genaue, öffentlich zugängliche Richtlinien für die Einordnung; die Durchführung erfolgt durch einen automatisierten Prozeß ("Robot“[153]). Nach Angaben des Anbieters liegen etwa 85% der automatisch erzeugten Einordnungen im Rahmen der Richtlinien.[154] Allerdings ist der Algorithmus nach Angaben des Anbieters nur für englischsprachige Seiten geeignet, daher sind die Ergebnisse für deutsche Seiten vermutlich häufiger fehlerhaft.

Es lassen sich auf der Webseite[155] neben der interaktiven Durchführung einer solchen automatisierten Einordnung außerdem manuell Korrekturen und Eingaben von Einordnungen für Seiten in anderen Sprachen als Englisch durchführen.[156]

---

153 Genaue Angaben zur Funktionsweise des Robots sind auf http://calvin.ptloma.edu/~spectre/evaluweb/whitepaper.html zu finden.

154 Das bedeutet also z.B., daß von 10.000 bewerteten Seiten 1.500 in der falschen Kategorie landen. Werden dabei hauptsächlich harmlose Seiten gesperrt, ist dies sicher eine beträchtliche Einschränkung der Informationsfreiheit. Sind es hingegen im wesentlichen pornographische Seiten, die so den Weg zu den Kindern finden, kann man kaum von zuverlässiger Filterung sprechen. Um diese Zahl also genauer bewerten zu können, wäre eine Kenntnis der Fehlertypen erforderlich, die allerdings vom Anbieter nicht dokumentiert werden.

155 http://calvin.ptloma.edu/~spectre/evaluweb/

156 Nach der Durchführung fragt der Webserver, ob eine Darstellung des Logos auf der Seite gewünscht wird; im Bedarfsfall wird der HTML-Code zur Verfügung gestellt.

Tests zeigen, daß die automatisierte Einordnung für politisch extreme Seiten überhaupt nicht, für gewalttätige und erotisch-pornographische Angebote relativ gut funktioniert. Bei letzeren erfolgt auch bei deutschen Seiten häufig eine korrekte Einordnung; vollständig zuverlässig ist das System hier allerdings nicht.

Offensichtlich liegt hier ein einfacher, relativ sicherer Einordnungsmechanismus vor.[157] Das Vorgehen bei der Einordnung ist zwar nicht transparent; wegen der Einfachheit der Einordnungen ist eine Überprüfung und ggf. Korrektur aber leicht möglich. Für eine Verwendung in anderen Ländern als der USA muß allerdings eine Erweiterung auf andere Sprachen erfolgen.

Andererseits erlaubt dieses sehr einfachen Schema keine gute Anpassung an individuelle Vorstellungen und ist damit für eine Inhaltskontrolle nach feineren Kriterien als nur "jugendgefährdend“ und "nicht jugendgefährdend“ nicht geeignet. Es stellt sich die Frage, inwieweit der zugrunde liegende automatische Einordnungsvorgang auf eine größere Anzahl von Kategorien erweitert werden könnte.

4.5.1.2 RSACi

RSACi schlägt vier Kategorien vor, in denen es jeweils fünf Abstufungen gibt. Die Organisation bietet damit einen Kompromiß zwischen detaillierter Abstufung und überschaubarer Anzahl von Kategorien.[158]

Die Einordnung erfolgt mit Hilfe eines Fragebogens, der auf dem Webserver der Organisation zur Verfügung stellt. Während dieses Vorgangs wird jeder eingestufte Webserver oder -seite gleichzeitig registriert und Name und Adresse der anmeldenden Person gespeichert. Die resultierende Einordnung wird dann in Form eines dem Nutzer zur Verfügung gestellten HTML-Eintrags in die Seite integriert, das über einen PICS-fähigen Browser abgefragt werden kann.[159]

---

157 Nach eigenen Angaben liegen etwa 85% der automatisch erzeugten Einordnungen im Rahmen der eigenen Kriterien.

158 Über die Anzahl der bewerteten Seiten gibt der Webserver keine Auskunft.

159 Die Kategorien sind in Netscape und MS IE standardmäßig integriert.

	Violence Rating Descriptor	Nudity Rating Descriptor	Sex Rating Descriptor	Language Rating Descriptor
Level 4	Rape or wanton, gratitious violence	Frontal nudity (provocative display)	Explicit sexual acts or sex crimes	Crude, vulgar language; extreme hate speech
Level 3	Aggressive violence; death to humans	Frontal nudity	Non-explicit sexual acts	Strong language or hate speech
Level 2	Destruction of realistic objects	Partial nudity	Clothed sexual touching	Moderate expletives or profanity
Level 1	Injury to human being	Revealing attire	Passionate kissing	Mild expletives
Level 0	None of the above or sports related	None of the above	None of the above or innocent kissing, romance	None of the above

Abb. 4-3: Einordnungsschema von RSACi

4.5.1.3 ESRB

ESRB unterscheidet zwischen "Rating Categories“, die Alterseignung angeben, und "Content Descriptors“, die den Inhalt beschreiben. Es gibt folgende Einstufungen[160]:

RATING CATEGORIES

- Early Childhood
- Everyone
- Teen
- Mature
- Adults Only

CONTENT DESCRIPTORS

- Comic Mischief
- Mild Violence
- Violence
- Graphic Violence
- Nudity
  - Technical Nudity
  - Artistic Nudity
  - Nudity
- Suggestive Themes
- Mature Sexual Themes
- Strong Sexual Content
- Mild Language
- Strong Language
- Hate Speech
- Strong Hate Speech

Zusätzlich kann eine Seite mit der Information versehen werden, ob sie persönliche Daten abfragt, Kreditkartennummern verlangt u.ä. Bei entsprechender Einstellung des Browsers bzw. Filterprogramms werden auch diese Seiten nicht angezeigt.

Die Einordnung erfolgt durch unabhängige "Raters“, die gemeldete Seiten untersuchen. Dabei entstehen für den Herausgeber der Seiten Kosten in Form von (Lizenz-)Gebühren[161]. Sie wird direkt auf der jeweiligen Webseite vermerkt und kann abgefragt werden.

Für den Microsoft Internet Explorer gibt es ein importierbares Datenfile, das die Verwendung des ESRB-Ratings erlaubt.

160 Detaillierte Beschreibungen finden sich auf http://www.esrb.org/esrbi/about.html

161 100$ pro Site, geringere Gebühren bei Veränderungen und Aktualisierungen.

4.5.1.4 SafeSurf

SafeSurf hat von allen vorgestellten Systemen das Kategoriensystem mit den meisten Rubriken. Es bietet wie ESRB zum einen die Möglichkeit, die Altersgruppe für eine Seite direkt anzugeben, zum anderen Rubriken zur Beschreibung des Inhalts.

Für die "Age Range“ gibt es folgende Möglichkeiten:

1) All Ages

2) Older Children

3) Teens

4) Older Teens

5) Adult Supervision Recommended

6) Adults

7) Limited to Adults

8) Adults Only

9) Explicitly for Adults

Die inhaltlichen Kennzeichnung, aus der dann ein persönliches Filterprofil zusammengestellt werden kann, erfolgt über jeweils neun verschiedene Kategorien zu verschiedenen inhaltlichen Bereichen: [162]

Kategorien	**Themen**
1) Subtle Innuendo (Andeutung)	Profanity
2) Explicit Innuendo (Andeutung)	Heterosexual Themes
3) Technical Reference	Homosexual Themes
4) Non-Graphic-Artistic	Nudity
5) Graphic-Artistic	Violence
6) Graphic	Sex, Violence, and Profanity
7) Detailed Graphic	Other Adult Themes
8) Explicit Vulgarity	Glorifying Drug Use
9) Explicit and Crude	Intolerance
	Gambling

Dabei werden die Rubriken für einzelne Themen noch weiter präzisiert. Mit diesem System ist eine sehr genaue Beschreibung des Inhaltes einer Webseite möglich; entsprechend präzise kann auch die Filterung sein – Korrektheit in Einordnung und Konfiguration vorausgesetzt.

Die Durchführung der Einordnung erfolgt über ein Formular im Internet, in dem die verschiedenen Kategorien ausgewählt werden. Daraus wird automatisch die entsprechende

[162] Detailliertere Erläuterungen zur Bedeutung der Kategorie für den jeweiligen Themenbereich und zur technischen Spezifikation der Seitenmarkierung finden sich auf http://www.safesurf.com/ssplan.htm.

HTML-Zeile generiert und zum Kopieren zur Verfügung gestellt.[163] Eine ausführlichere Einordnung wird außerdem per E-Mail verschickt.

4.5.2 Zusammenfassung und Anforderungsentwicklung

Die vorgestellten Ratingsysteme decken die Bandbreite möglicher Systematiken gut ab.

Alle bieten eine einfache Möglichkeit, eine inhaltliche Einordnung in den entsprechenden maschinenlesbaren Code umzusetzen. Zum Teil ist dafür eine Registrierung erforderlich. Die dabei nötige Angabe von Namen und Adresse des Antragstellers kann eine Hemmschwelle sein. Daher ist die von SafeSurf verwendete Methode einer Bitte um Registrierung nach dem Einfügen der Einordnung im Sinne einer weiten Verbreitung hilfreicher, allerdings auf Kosten eines sinkenden Verhältnisses von registrierten zu eingeordneten, aber nicht registrierten Seiten.

Eine Unterteilung der Rubriken in direkte Alterseignung und Inhaltsbeschreibung ist sinnvoll, da von Benutzerseite damit einerseits eine einfache Einstellung über das Alter (geringer Konfigurationsaufwand, aber Abhängigkeit von der Einordnung der Autoren) möglich ist; andererseits steht auch eine Variante zur Verfügung, die eine individuelle Definition der zu sperrenden oder durchzulassenden Inhalte erlaubt. Um diesen Komfort in der Praxis zu realisieren, müssen allerdings für jede Webseite Einstufungen in beide Kategorien vorgenommen werden.

evaluWeb zeigt, daß es möglich ist, den Einordnungsvorgang automatisiert zu unterstützen. Allerdings ist das Verfahren nicht zuverlässig genug, um alleinige Basis eines Einordnungskonzeptes zu sein. Es wäre denkbar, es als Kontrollmechanismus für erfolgte Einordnungen zu verwenden. Außerdem könnte das Produkt in den lokalen Browser integriert werden, um die aufwendige und vom Standpunkt des Datenschutzes unerwünschte Verwendung von Servern zu vermeiden.

Auch als "Aushilfe“ für nicht eingeordnete Seiten könnte ein solches System prinzipiell Hilfestellung leisten; aufgrund zu geringer Zuverlässigkeit des Verfahrens und einem Mangel anderer Vorgehensweisen ist allerdings einer Sperrung nicht eingeordneter Seiten aus Sicherheitsgründen der Vorzug zu geben. Die Zahl der eingeordneten Seiten läßt sich z.B. durch eine Kombination mehrerer Systeme in einem Filtersystem deutlich erhöhen. Bei den vorgestellten PICS-basierten Systemen ist dies ohne weiteres möglich und wird zum Beispiel im *Microsoft Internet Explorer* bereits durch Importdateien realisiert. Eine solche Kombinierbarkeit erhöht auch die Bandbreite der Einordnungsmaßstäbe, unter den der Benutzer auswählen kann.

Alle vorliegenden Systeme sind für den amerikanischen Sprach- und Kulturraum entwickelt worden. Keines ist in der Lage, Seiten und/oder Kategorien in mehreren Sprachen zu verarbeiten. Hier sind Definitionen von mehrsprachigen Systemen erforderlich, die auch auf die kulturellen Unterschiede Rücksicht nehmen.

Außerdem weist auch keines der Systeme einzeln oder in Kombination mit anderen bisher eine genügend weite Verbreitung auf, auch nicht bei Betrachtung der Netzwelt in den USA. Hier sind Maßnahmen zur Bewußtseinsbildung sicher hilfreich; denkbar wären aber auch organisatorisch-rechtliche Rahmenbedingungen, die die Durchsetzung eines oder mehrere Einordnungssysteme fördern. Dabei sind allerdings mögliche Gefahren zu beachten: Ein einmal durchgesetztes Filtersystem kann durch langsame Änderungen an Transparenz und

---

163 Beispiel für einen Server, der in keiner der genannten Rubriken problematisch und für alle Altersstufen geeignet ist:
<META http-equiv="PICS-Label“ content='(PICS-1.1 "http://www.classify.org/safesurf/“ l r (SS~~000 1))'>

Neutralität verlieren und damit zur vom Endbenutzer unbemerkten massiven Beeinflussung der Filterung führen.

In diesem Abschnitt wurden nur Ratingsysteme betrachtet, die nicht nur in Verbindung mit einem Filterprodukt verwendet werden können. Daher ließe sich die Liste durch eine größere Anzahl von produktspezifischen Systemen ergänzen, die z.T. nicht nur Kategoriensysteme formulieren, sondern auch Listen von Webseiten vorhalten und Werkzeuge zur automatisierten Einordnung anbieten.

Für einige der Punkte ist es nicht wesentlich, ob das System – wie die hier beschriebenen – unabhängig von einem Produkt existiert oder in eines integriert ist. Ist allerdings ihre Verwendung an den Erwerb genau eines Produktes gekoppelt, wird dies meist auf Kosten von Transparenz und Beeinflußbarkeit gehen. Werden also integrierte Systeme verwendet, ist immer eine Unterstützung durch mehrere Filterprogramme anzustreben. Noch besser wäre die Möglichkeit der wahlweisen Importierbarkeit von Kategoriensystemen.

Zusammenfassend sind folgende Anforderungen an ein Ratingsystem zu stellen:

- Große Verbreitung;
- Mehrsprachigkeit;
- Einfachheit der Einordnung (automatisierte Erzeugung des Codes);
- Kombinierbarkeit mehrere Systeme.

4.6 Technische Verfahren und ihre Grenzen

Für die technischen Verfahren muß nicht nur die Funktionsweise untersucht werden, sondern man muß sich ebenso mit möglicherweise entstehenden Seiteneffekten, mit Umgehungsmöglichkeiten und mit Kosten beschäftigen.

4.6.1 Nicht intendierte Effekte

Um Jugendschutz durch technische Mechanismen im Internet mit möglichst wenig Auswirkungen auf andere Bereiche zu unterstützen, sähe die perfekte Lösung so aus, daß paßgenau die jugendgefährdenden Inhalte ausschließlich für Kinder und Jugendliche herausgefiltert würden. Dies ist aus den in den vorigen Abschnitten geschilderten Gründen mit den heutigen technischen Verfahren nicht möglich. Tatsächlich sind alle Methoden zur Zeit zu unspezifisch, d.h. einerseits wird häufig zuviel gefiltert, so daß auch jugendfreie Inhalte von der Filterung betroffen sind, andererseits kann man nicht ausschließen, daß Kinder und Jugendliche an jugendgefährdende Informationen herankommen, sofern man nicht den offenen Charakter des für sie nutzbaren Internet abschafft. Deswegen lassen sich gerade im Bereich der Inhaltsfilterung unbeabsichtigte Auswirkungen nicht verhindern.

Im folgenden sind die potentiell Betroffenen nach den in Abschnitt 1.10.2 eingeführten Rollen und mögliche Effekte dargestellt, die durch ein Filtersystem an sich oder auch durch erfolgreiche Angriffe auf das technische System verursacht sein können. Die Rollen, die sich aus der Filtertechnik ergeben, aber beim Abrufer ansetzen, sind zur besseren Übersichtlichkeit in Abschnitt 1.10.2 aufgeführt.

4.6.1.1 Effekte im Anbieterbereich: Content-Provider

Hier liegt das Hauptproblem bei den Nebenbetroffenen, d.h. weniger bei dem Anbieter der jugendgefährdenden Inhalte, sondern vielmehr bei Inhaltsanbietern von jugendfreien Informationen, die beim Einsatz von Filtertechnik für bestimmte Nutzergruppen ungewollt herausgefiltert werden. Dies ist beispielsweise der Fall, wenn unspezifisch alle WWW-Seiten von einem Server gesperrt werden (Sperrung auf Ebene der IP-Adressen), weil von dort ein einziger inkriminierter Inhalt abrufbar ist.

Bei Filtermethoden über ein Rating kann dann zuviel herausgefiltert werden, wenn entweder die abrufbare Einordnung inhaltlich falsch ist oder wenn keine Einordnung vorgenommen wurde bzw. abrufbar ist und nur eingeordnete Inhalte durch den Filter gelassen werden. Filtert man Suchwörter heraus, kann es sein, daß die angezeigten Informationen nicht mit der Semantik des Seiteninhalts übereinstimmen, ggf. dort sogar das Gegenteil zum Ausdruck gebracht wird.[164]

Ein Problem besteht darin, daß der Content-Provider in der Regel nicht weiß, daß seine Inhalte herausgefiltert werden, und daher den Fehler nicht korrigieren lassen kann. Es ist unter Umständen auch nachträglich nicht transparent, also nicht revisionsfest, wodurch eine falsche Einordnung verursacht wurde: durch eine inhaltliche Fehleinordnung (von wem?), durch eine Verfälschung bei der Abspeicherung (z.B. durch ein trojanisches Pferd) oder durch eine Verfälschung beim Abruf. Eine Filterung kann sich auch finanziell auswirken, wenn dem Anbieter beispielsweise Werbeeinnahmen oder sogar Aufträge entgehen, weil die Seite nicht abrufbar ist. Ebenso kann eine Filterung rufschädigend sein. Hier bietet sich ein Angriffsziel für Versuche, den Abruf von Webseiten der Konkurrenz zu behindern.

Eine weitere unbeabsichtigte Auswirkung für Content-Provider besteht dann, wenn der Presence-Provider, der die Inhalte auf einem Server bereitstellt, aufgefordert wird, diese zu sperren oder zu löschen, da sie aus Sicht des Jugendschutzes problematisch sind. Es kann hierbei zu der Situation kommen, daß der Presence-Provider auf eine weitere inhaltliche Prüfung verzichtet und nicht mehr bereit ist, die Webseiten des Content-Providers bereitzuhalten, selbst wenn eine Jugendgefährdung gerichtlich nicht festzustellen wäre. [165]

Weitere Auswirkungen ergeben sich für die Anbieter von dynamischen Inhalten, die erst im Moment des Abrufs generiert werden. Da sich der Inhalt solcher Seiten (Katalogsysteme, Newsticker, Community-Pages) von Abruf zu Abruf ändern kann, versagt der Ansatz der Einordnung durch Dritte vollständig. Es ist lediglich denkbar, daß die Anbieter solche Inhalte selbst einordnen. Bei Angeboten, deren Inhalt durch viele Teilnehmer generiert wird[166], und bei Community-Projekten ist dies aus denselben Gründen nicht möglich, aus denen sich z.B. Usenet-News einer effektiven Filterung entziehen: Das generierte Nachrichtenaufkommen ist unter Umständen viel zu groß, um von den Content-Providern dieser Dienste überblickt und eingeordnet zu werden.[167]

Auch durch PICS ist eine Einordnung solcher dynamischer Seiten kaum möglich, da nach diesem Standard nur Inhalte mit einer URL adressiert werden können. Eine einzelne Seite einer Community-Website oder eines Nachrichtenserver enthält aber in der Regel eine Vielzahl von Beiträgen unterschiedlichen Inhaltes und unterschiedlicher Autoren, die jedoch nicht einzeln adressierbar sind.

Websites, die Inhalte dynamisch generieren, erzeugen pro Abrufer in der Regel eine "Session“, die von Seite zu Seite weitergegeben wird und die es dem Server ermöglicht, für diesen Abrufer die gewünschten Inhalte gemäß der getroffenen Voreinstellungen zu erzeugen. Diese Session wird von vielen Systemen in der URL der Seite codiert und ist

---

164 Dies ist beispielsweise der Fall beim Einsatz des Programms CYBERsitter, bei dem aus "The Catholic church is opposed to all homosexual marriages.“ durch Herausfiltern des "verbotenen“ Wortes "homosexual“ für den Nutzer "The Catholic church is opposed to all marriages.“ wird (Beispiel von Brian Milburn, zitiert in http://www.mit.edu:8001/activities/safe/labelling/0198f1.html).

165 Vgl. dazu die Strategie von Jugendschutz.net nach Aussagen von Betroffenen, siehe auch Presseerklärung "Jugendschutz erfordert rechtsstaatliche Verantwortung“ des Virtuellen Ortsvereins der SPD (VOV) vom 06.06.99, von Helmut Pohl in de.org.politik.spd, de.alt.jugendschutz und de.soc.zensur gepostet.

166 Diskussionsforen wie zum Beispiel http://slashdot.org.

167 Bei Dejanews (deja.com) ist dieses Angebot mit den Usenet-News identisch.

einmalig (eine Session wird niemals wiederverwendet). Solche Server haben einen quasi-unendlich großen, durch Labels zu klassifizierenden URL-Raum, dessen Inhalt im wesentlichen durch den Teilnehmer und die von ihm getroffenen Voreinstellungen bestimmt wird. Die Generierung von digital signierten Labels für solche Seiten kann erst im Moment des Abrufes erfolgen und stellt beträchtliche Zusatzanforderungen an die verwendete Hardware.[168]

PICS erlaubt die pauschale Einordnung ganzer Teilbäume unter ein gemeinsames Rating. Im Sinne einer differenzierten Betrachtung ist dies jedoch nur eine Notlösung. Insbesondere besteht die Gefahr, daß Anbieter aus Bequemlichkeit, Kostengründen oder rechtlicher Unsicherheit ihre gesamte Website durch ein pauschales, an der Wurzel ihrer Website angebrachtes Label kennzeichnen. Sofern hierfür ein maximal ausschließendes Label verwendet wird, läuft dies der Notwendigkeit zuwider, Jugendlichen möglichst alle unkritischen Inhalte durch entsprechende Einordnungen freizuschalten, damit das Internet für diese seinen Wert behält. Prinzipbedingt kann ein solches "Pauschal-Label“ nicht durch eine MD5-Prüfsumme o.ä. an einen bestimmten Inhalt gebunden werden.

Paßwortgeschützte Bereiche entziehen sich einer Einordnung durch Rating-Services nahezu vollständig. Wenn für den Nutzer der Abruf nicht eingeordneter Seiten gesperrt ist und der Nutzer auf die Labels eines Rating-Services angewiesen ist, bedeutet dies für ihn, daß er keinerlei paßwortgeschützte Bereiche aufrufen kann. Auch hier kann eine Einordnung daher sinnvollerweise allein vom Anbieter der Seite vorgenommen werden.

4.6.1.2 Effekte im Abruferbereich

Access-Provider, Betreiber des Abrufsystems

Sofern der Access-Provider sich am Filterverfahren beteiligt, hat er dafür zu sorgen, daß das Verfahren korrekt abläuft. Damit würde er einen Teil der Verantwortung an dem Filterverfahren übernehmen, so daß Forderungen der Nutzer und Content-Provider auf ihn zukommen könnten.

Da die Access-Provider und die Betreiber des Abrufsystems die Ansprechpartner für die Abrufer sind, haben sie bei Problemen der Nutzer Hilfestellung zu leisten. Dies betrifft beim Einsatz von Filtersystemen im Abruferbereich nicht nur die Browser und sonstige Internetsoftware, sondern auch zusätzliche Filtermechanismen, selbst wenn sie nicht in der Verantwortung des Access-Providers oder des Betreibers des Abrufsystems liegen. Dies ist insbesondere dann ein Problem, wenn die Filtersysteme nicht erkennen lassen, ob eine technische Störung vorliegt oder ob ein Inhalt ausgefiltert wurde.

Zu schützende Personen

Unerwünschte Effekte treten dann ein, wenn die Filterung nicht paßgenau ist, d.h. jugendgefährdende Inhalte durchgelassen werden, der Filtermechanismus leicht zu umgehen ist, zu viele Inhalte nicht zugänglich sind oder wegen einer Ausfilterung von Wörtern o.ä. verfälscht dargestellt werden. Problematisch sind Angebote, die es erfordern, daß personenbezogene Daten der Kinder und Jugendlichen weitergegeben werden, und es ermöglichen, Nutzungsprofile durch einen Anbieter im Filterverfahren (z.B. dem Hersteller oder filternden Access-Provider) zu erstellen.

Insbesondere ist für jugendliche Nutzer ab einem bestimmten Alter eine Nutzung des Internet mit einem Jugendschutzfilter nur dann sinnvoll, wenn ihnen die nicht jugendgefährdenden

---

168 Nach ersten, groben Schätzungen werden entweder zwei- bis dreimal mehr RAM-Speicher oder eine zwei- bis dreimal größere Festplattenbandbreite (MB/s) notwendig, um digital signierte Labels für solche dynamisch generierten Seiten zu erzeugen. Man kann also zunächst einmal davon ausgehen, daß sich die Hardwarekosten für den Betreiber derartiger Systeme niedrig geschätzt verdoppeln.

Inhalte in ihrer weit überwiegenden Mehrzahl noch zur Verfügung stehen, auch wenn der Filter aktiv ist. Für den zu schützenden Jugendlichen ergibt sich bei einem installierten Filter aber in der Regel die Situation, daß nicht eingeordnete Inhalte unzugänglich werden. Die Gefahr einer solchen untragbaren Einschränkung läßt sich also nur durch eine große Verbreitung der Einordnung bannen.

In "Fahrenheit 451.2 – Is Cyberspace Burning?“[169] wird diese Situation so geschildert:
"You are a native of Papua, New Guinea, and as an anthropologist you have published several papers about your native culture. You create a web site and post electronic versions of your papers, in order to share them with colleagues and other interested people around the world. You haven't heard about the move in America to rate Internet content. You don't know it, but since your site is unrated none of your colleagues in America will be able to access it.“

In der Realität wird der Ausschluß nicht gelabelter Inhalte vermutlich schon früher anfangen: Nur große Sites werden ihre Inhalte einordnen; kleine, privat erzeugte Homepages werden in der Regel keine Einordnungen bekommen, weil sich die Autoren dieser Seiten nicht dafür interessieren, daß speziell auch Jugendliche auf ihre Inhalte zugreifen können, oder weil sie nicht wissen, wie sie korrekt einordnen können. Es könnte auch sein, daß sie auf ein Label verzichten, weil sie Angst haben, für falsche Labels zur Rechenschaft gezogen zu werden. Für Jugendliche hinter einem Filter, der nicht eingeordnete Inhalte sperrt, werden daher vor allen Dingen Inhalte großer kommerzieller Anbieter zugänglich sein, aber die Vielfalt kleiner, privater Homepages und Initiativen, die den eigentlichen Reichtum des Internet ausmachen, wird ihnen unzugänglich sein.

Beobachtbar ist dieser Trend schon jetzt: Firmen wie Disney und Time Warner, aber auch der Playboy haben ihre Angebote mit Labels versehen, doch selbst die deutschen Webseiten "jugendschutz.net“, "jugendschutz.de“ oder "fsm.de“ sind ebensowenig gelabelt wie die Seiten der Bundesregierung, der Bundesministerien und sämtliche Homepages von Privatpersonen, die in einer Stichprobe untersucht wurden.[170]

Für die Nutzer auf dem Abrufsystem entspricht die Einführung eines Filtermechanismus der Einführung eines künstlichen Mittlers, von dessen Funktion und Zustimmung der Erhalt der gewünschten Daten abhängig ist. Dies hat natürlich auch Auswirkungen auf die Performance, Verfügbarkeit und den Datenschutz:

- Wird bei der Filterung nach PICS zum Beispiel *Third-Party-Rating* verwendet und bei jedem Seitenabruf zunächst ein externer Label-Provider nach dem Rating für das abgerufene Dokument befragt, fallen dort detaillierte Verbindungsdaten für jeden Nutzer dieses Label-Servers an. Es entsteht eine lückenlose Liste aller abgerufenen URLs mit Datum und ggf. sogar authentisiertem Nutzernamen.[171] Dies könnte unter Umständen erwünscht sein[172], ist aber grundsätzlich zustimmungspflichtig und aus Gründen des Datenschutzes kritisch.

---

169 Vgl. http://www.aclu.org/issues/cyber/burning.html.

170 Zur Durchsetzung eines wie auch immer gearteten Ratingsystems sind jedoch die Vorbilder solcher Organisationen unbedingt erforderlich.

171 Wenn der Dienst des Label-Providers entgeltlich zur Verfügung gestellt wird, ist für Abrechnungszwecke in der Regel eine Authentifizierung des Nutzers notwendig.

172 Die Label-Verteilstelle könnte sich durch die Erfassung und den Verkauf der anfallenden Benutzerprofile finanzieren: Die anfallenden Profile sind wegen ihres einmaligen Detailreichtums von sehr großen Wert für die unterschiedlichen Gruppen von "Bedarfsträgern“ in Wirtschaft und Verwaltung.

- Wird bei der Filterung nach PICS Third-Party-Rating verwendet und ist der für jeden Seitenabruf zu befragende Label-Server vorübergehend nicht erreichbar, sind dem Nutzer überhaupt keine Seiten zugänglich. Der Label-Server wird Bestandteil eines kritischen Pfades für den Internetzugang; das Internet ist jedoch von der Konstruktion her zunächst einmal darauf ausgelegt, solche kritischen Pfade zu vermeiden.
- Selbst wenn der Label-Server online und erreichbar ist, wird der Zugriff darauf zum begrenzenden Faktor für die Abrufgeschwindigkeit, weil er Bestandteil des kritischen Pfades ist: Bei optimaler Implementierung sind der Abruf der eigentlichen Seite und der Abruf des zu dieser Seite gehörenden Labels parallelisiert, so daß sich als untere Schranke für die Anzeigezeit eines abgerufenen Dokumentes das Maximum der Abrufzeit für das eigentliche Dokument und der Abrufzeit des Labels ergibt. Für die Ermittlung dieser Zeiten kommt es unter hoher Last auf der Seite des Label-Servers wahrscheinlich weniger auf die Größe der Labels im Vergleich zur Größe der Dokumente an, sondern auf die Umlaufgeschwindigkeiten (*Round Trip Times*) von Datenpaketen zwischen dem Seitenabrufer und dem Label-Server. Bei einer naiven Implementierung erfolgt der Abruf eines Dokumentes und der Abruf des Dokumentlabels sequentiell, und die benötigten Zeiten addieren sich. Fest steht, daß der Betrieb eines Endnutzer-PCs durch den Einbau von Filtermechanismen weder schneller noch zuverlässiger werden kann. Das zu übertragende Datenvolumen wird bei allen beteiligten Parteien erhöht.
- In einer naiven Betrachtung erscheint es zunächst sinnvoll, in einem Proxy-Cache (Speicher eines Internet-Servers) die Labels für Dokumente zusammen mit den Dokumenten zu speichern. Dadurch würde es dem Abrufer ermöglicht, offline aus dem Cache zu arbeiten, und die Cache-Sicht wäre auch auf den ersten Blick konsistent, da zu jedem Dokument im Cache auch ein Label existiert. Tatsächlich ist es jedoch so, daß zu Dokumenten im Cache kein Label existieren muß, da das Dokument ja im Auftrag eines Abrufers geholt worden sein könnte, der kein PICS nutzt. Für diejenigen Dokumente, für die im Cache Labels existieren, ist es so, daß diese Labels unter Umständen nicht ohne Validierung benutzt werden dürfen. Die Lebensdauer eines Labels ist nämlich in einigen Fällen kürzer als die Lebensdauer des Dokumentes, für das es vergeben wurde – das Label könnte falsch vergeben oder das Zertifikat des Rating-Services könnte zurückgezogen worden sein. In diesem Fall ist es notwendig, für ein gültiges Dokument im Cache ein neues, aktuelles Label zu holen.
- Beim Betrieb eines Cache hat man also die Wahl, entweder einen gewissen Anteil von falschen oder ungültigen Labels in Kauf zu nehmen oder auf den Offline-Betrieb ("Surfen aus dem Cache“) zu verzichten. Entscheidet man sich für die erste Lösung, werden Zertifikatsrückrufe und korrigierte Labels sehr viel langsamer propagiert (eine Dauer von Tagen statt Sekunden), und es existiert kein Zeitpunkt mehr, zu dem alle Netzknoten konsistent denselben Informationsstand haben. Die zweite Lösung, nur online zu arbeiten, ist für viele Nutzer und insbesondere Schulen zur Zeit nicht finanzierbar.[173]
- Sofern beim Abruf die digitale Signatur der Label und ihrer Zuordnung überprüft werden muß, wird das Surfen im Internet schon deswegen langsamer, weil die Daten vor ihrer Darstellung insgesamt geladen und überprüft werden müssen. Hier kann es zu längeren Ladezeiten kommen, ohne daß dem Nutzer überhaupt etwas angezeigt wird, weil erst die Prüfung nach dem Laden ergeben hat, daß der Inhalt ausgefiltert wird.

Andere Nutzer auf demselben Abrufsystem

Die Aktivierung eines Filtersystems kann Nutzer auf demselben System derart beeinflussen, daß er falsche oder unvollständige Informationen aus dem Internet erhält, weil Teile gefiltert werden. Einige Systeme wirken sich darüber hinaus sogar auf gespeicherte Text- oder Bilddokumente sowie auf Paßwörter aus und filtern beispielsweise Zeichenketten heraus.

173 Diese Problematik trifft allerdings jede Form des Einsatzes von Cache-Systemen.

Auch weitere Einschränkungen bei der Arbeit im System können durch die Filtersoftware verursacht werden, z.B. in bezug auf die sonstige Softwarekonfiguration oder Deaktivierungs- oder Deinstallationsmöglichkeit der Filtersoftware. Wie auch bei den zu schützenden Personen sollten keine Nutzungsprofile außerhalb des eigenen Bereichs anlegbar sein.

Dabei besteht immer die Gefahr, daß erwachsene Nutzer eines Systems, das auch von Kindern genutzt wird, den PICS-Filter aus Bequemlichkeit nicht deaktivieren oder nicht deaktivieren können, weil die Kindersicherung für sie zu kompliziert zu bedienen oder weil eine Deaktivierung der Kindersicherung nicht vorgesehen ist. Möglicherweise nehmen sie die aktivierte Kindersicherung noch nicht einmal wahr, weil unter Umständen gar nicht angezeigt wird, daß eine Filterfunktion aktiv ist.[174] Dies ist auf jeden Fall zu verhindern, da sonst die Wahrnehmung des Grundrechtes auf freien Informationszugang eingeschränkt sein kann.

4.6.1.3 Die Effekte im Filterbereich

Beim Filtern kommt es stark darauf an, daß korrekt und revisionsfest gearbeitet wird. Dies betrifft die meisten Rollen: Die Hersteller von Filtersystemen sollten daher korrekt und transparent arbeitende Systeme zur Verfügung stellen, die Zertifizierungsinstanzen und Label-Provider sollten korrekte Schlüsselzertifikate bzw. Labels zum unverzüglichen Abruf bereithalten und die Rating-Service-Dienstleister sollten die inhaltliche Einordnung korrekt vornehmen.

Im Falle von Unstimmigkeiten oder Fehlern wären hier Haftungsfragen zu klären.

Insbesondere müssen hier Forderungen von Content-Providern oder von Nutzern und Betreibern von Abrufsystemen berücksichtigt werden, wenn die Filterung aus irgendwelchen Gründen nicht paßgenau ist. Da bei der Untersuchung von Haftungsaspekten jedoch eine Vielzahl von Beziehungen zwischen den unterschiedlichen Rollen zu analysieren ist, wurde dies im Rahmen der vorliegenden Studie nicht untersucht.

Ein unerwünschter Effekt auf die Akteure, die zur Filterung beitragen, z.B. der Rating-Service, der Label-Provider oder Filtersystem-Hersteller besteht darin, daß Begehrlichkeiten geweckt werden, auch andere als jugendgefährdende Inhalte auszufiltern, beispielsweise indem bestimmte Einordnungen vorgenommen werden oder zusätzlich "schwarze Listen“ in das Filtersystem integriert werden. Die Motive dafür sind vielfältig: So kann es darum gehen,

174 Diese Funktionalität wurde von einigen Erziehungsberechtigten gewünscht, um die Jugendlichen nicht zu motivieren, gegen die Sperre vorzugehen (vgl. Abschnitt 5.4.1.5).

kritische Stimmen auszufiltern oder den Zugriff auf Informationen von Konkurrenten zu erschweren.[175]

4.6.2 Umgehungsmöglichkeiten

Der Erstaufwand für Umgehungs-Angriffe auf Filtersysteme kann zunächst hoch sein. Ist ein solches System jedoch erst einmal geknackt, kann der Prozeß der Entfernung automatisiert und in einer leicht verständlichen Anleitung beschrieben oder gar in Gestalt eines Programmes implementiert und allgemein zur Verfügung gestellt werden. Mit diesem Hilfsmittel können dann auch technisch unbedarfte Nutzer die lokalen Filterkomponenten schnell und ohne großen Aufwand entfernen oder die Auswahl deaktivieren.[176]

Die Umgehung lokal installierter Filterkomponenten wird durch eine Reihe von Faktoren stark erleichtert:

- Die Filtersoftware wird überwiegend auf Windows 95, Windows 98 oder Macintosh-Rechnern (MacOS < Version 10) ablaufen. Diese Systeme bieten keine lokale Sicherheit, d.h. sie unterscheiden keine Benutzerrechte an Dateien und bieten keinen Zugriffschutz.
- Die genannten Systemplattformen sind hoch modular und bieten Zugriff auf sämtliche Systembibliotheken. So ist es zum Beispiel mit Hilfe von Visual Basic for Applications, also Makros in Word- oder Excel-Dateien, möglich, sämtliche Betriebssystemfunktionen eines Windows-Rechners zu nutzen, also etwa Dateien zu löschen, zu kopieren, Festplatten zu formatieren oder Systemdateien zu manipulieren. Zusätzlicher Code kann in solche Systeme als Anhang von E-Mails (Attachements) oder in Form von mit einem Web-Browser herunterladbaren ActiveX-Applets eingebracht werden. Im Extremfall würde ein Jugendlicher einfach ein in Java oder ActiveX geschriebenes Programmstück in seinem Browser starten, das einen Browser ohne Jugendschutzfunktionen realisiert.
- Die Filtersoftware ist frei erhältlich und kann von einem Angreifer in einer durch ihn kontrollierten Umgebung beliebig oft installiert und analysiert werden. Dies ermöglicht dem Angreifer, seinen Angriff durch ausführliche Analyse des Programmes (Reverse Engineering) in aller Ruhe "offline“ vorzubereiten und erst dann am Produktionssystem tätig zu werden, wenn er den Schutzmechanismus und seine Schwächen gründlich studiert hat und sich die für den Angriff benötigten Spezialwerkzeuge und Kenntnisse verschafft hat.

---

175 Man überlege sich folgende Szenarien:
Ein Anbieter im Ausland bietet eine xyz-Hatepage an, auf der ein deutscher Staatsbürger nach dessen Einschätzung verleumdet wird. Da dieser die Seite nicht an ihrer Ursprungsquelle abschalten lassen kann, möchte er entsprechende Einträge in das existierende Filtersystem zum Jugendschutz durchsetzen, damit immerhin weniger Abrufer in Deutschland diese Seite ansehen können.
Ein Anbieter im Ausland bietet Material an, über dessen Urheberrecht Zweifel besteht. Der Urheber möchte durch einen Eintrag im Filtersystem für Jugendschutz erzwingen, daß weniger Abrufer in Deutschland diese Seiten ansehen können. (Konkret könnten dies z.B. Informationen und Materialien über Scientology oder andere Sekten sein.) Damit könnte auch hier das Filtersystem zur Klärung rechtlich nicht durchzusetzender Forderungen mißbraucht werden.
Ein ähnlicher Vorgang führte zur Schließung des bekannten Anonymous Remailers anon.penet.fi (siehe Pressemitteilung vom 30.08.96, http://www.penet.fi/press-english.html); Scott McClare: "Scientology vs. The Net – Copyright violations reveal secret scriptures“, http://imprint.uwaterloo.ca/issues/022197/3Features/feat02.html; Rigo Wenning: "Das Internet – ein rechtsfreier Raum?“, JurPC Web-Dok. 16/1997, Abs. 1-26, http://www.jura.uni-sb.de/jurpc/aufsatz/19970016.htm).

176 Vgl. http://www.peacefire.org/.

- Ziel einer Umgehung ist es, ein unmodifiziertes Originalsystem wiederherzustellen. Ein solcher Angriff ist also auch ohne Kenntnisse über die interne Konstruktion der Filtersoftware dadurch möglich, daß man die Installation der Filtersoftware protokollieren läßt[177], um dann die durch die Installation der Filtersoftware veränderten Originaldateien und Registry-Einträge wieder von der Betriebssystem-CD-ROM zu installieren. Filtersoftware kann sich gegen solche Spionageversuche zur Wehr setzen, indem sie sich an wenig zugänglichen oder schlecht dokumentierten Schnittstellen des Systems festsetzt. Der Hersteller der Filtersoftware riskiert damit jedoch, daß das Gesamtsystem instabil, unbequem oder schlecht zu warten wird. Seinen Bemühungen sind daher im Gegensatz zu den Bemühungen des Angreifers enge Grenzen gesetzt.
- Sofern lokal gefiltert wird, ist zu berücksichtigen, daß in vielen Fällen die ausgefilterten Daten auf der Festplatte zwischengespeichert werden. Das heißt, daß die Inhalte zunächst auf den Rechner geladen werden und erst dann der Auswahlprozeß darauf zugreift. Dies ist insbesondere dann gängig, wenn die Authentizität des Labels anhand der digitalen Signatur geprüft werden soll. Durch einen direkten Zugriff auf diese Daten läßt sich häufig der Filtermechanismus umgehen. Schutz bieten allenfalls Sicherheitsmechanismen (sofern vorhanden) des lokalen Betriebssystems und ein rückstandsfreies Löschen der zwischengespeicherten Inhalte auf der Festplatte.

Möchte man Filtersoftware installieren, die einem ernsthaften Angriff standhält, bietet sich die Installation von isolierten Webterminals an, die ausschließlich über einen filternden Proxy-Cache auf das Internet Zugriff haben.[178]

Im Ganzen gesehen erscheint es nicht schwieriger, eine lokale Filtersoftware zu deinstallieren, als den Kopierschutz eines Computerspieles zu knacken.[179]

Andere Angriffe auf Filtersysteme spielen sich außerhalb der Clientplattform ab:

- Wenn Labels nicht digital signiert werden und diese Signaturen beim Abrufer nicht kontrolliert werden, ist es sehr leicht möglich, einen Proxy-Server zu konstruieren, der zwischen dem Label-Server und dem Abrufer positioniert ist und die vom Label-Server gelieferten Labels entweder entfernt oder durch falsche Einordnungen nach Belieben des Angreifers austauscht. In der Funktionsweise ähnlich dem *Anonymizer*[180] würde ein solcher *De-Label-izer* Webseiten im Auftrag eines Abrufers holen und diese dann mit einem gefälschten, beliebig manipulierten PICS-Label weitersenden ("Filter-Filter“).
- Wenn für den Abrufer verschlüsselte Ende-zu-Ende-Verbindungen zugelassen sind, ist eine Filterung nur noch dann möglich, wenn der Filter auf dem System des Abrufers greift[181], da ein Zugriff auf die verschlüsselte Kommunikation von keiner Partei auf dem Weg mehr möglich ist. Eine Filtermöglichkeit durch einen Proxy-Server, der den Zugriffen der Jugendlichen entzogen ist, entfällt in diesem Szenario, denn es ist genau der Sinn solcher Verschlüsselungstechniken, Angriffe eines Man-in-the-middle unmöglich zu machen. Den Sinn von Privatsphäre schützenden Verschlüsselungstechniken zu

177 Eine Funktion, die jede leistungsfähige Virenschutzsoftware mitbringt.

178 Wobei auf dem Chaos Communication Congress 1997 des CCC demonstriert wurde, daß auch ein gesichertes Webterminal, das sich bei jedem Einschaltvorgang von einer gesicherten Kopie neu installiert, innerhalb einer Stunde geknackt und so modifiziert werden kann, daß die darin enthaltenen Zugangskontrollen nicht mehr funktionieren.

179 Eine Aufgabe, von der einer der Autoren weiß, daß 14jährige Jugendliche sie selbständig und zuverlässig ohne Anleitung lösen können.

180 http://www.anonymizer.com/

181 Dort befindet er sich an exponierter Stelle für mögliche Angriffe durch die Nutzer des Systems.

vermitteln und ihre Anwendung alltäglich zu machen, ist jedoch ein wichtiges Lernziel für die Internetnutzung durch Jugendliche.

- Wenn bekannt ist, wie und nach welchen Kriterien gefiltert wird, dann ist es vergleichsweise leicht, die so entstehenden Sperrungen gezielt zu umgehen oder anders unwirksam zu machen. Dies ist auch den Anbietern von Katalogen mit zu sperrenden URLs bekannt: Alle Programme mit einer statischen Liste zu sperrender Angebote verschlüsseln diese Liste und versuchen, ihre Filterkriterien durch andere Methoden geheim zu halten.[182] Eine solche nicht offengelegte Liste von Einordnungskriterien widerspricht jedoch der geforderten Revisionsfestigkeit sowie sämtlichen Ansprüchen eines Rechtsstaates an derartige Eingriffe.

Grundsätzlich kann man sagen, daß PICS-Filter auf Proxy-Servern, die dem Zugriff der Endnutzer entzogen sind, vom Endbenutzer wesentlich weniger leicht manipulierbar sind. Der Einsatz solcher Filter bedingt jedoch, daß diese Nutzer keinen direkten Zugriff auf das Internet haben, sondern aufgrund der Konfiguration ihrer Systeme gezwungen sind, den Proxy-Server zu verwenden. Dies ist bei Online-Diensten, die keinen direkten Internetzugang anbieten, sondern diesen nur als Zusatzdienst emulieren, automatisch der Fall (z.B. AOL). Bei regulären Internet-Providern ist dies immer dann der Fall, wenn die Kunden entweder nichtöffentliche IP-Adressen nach RFC 1597 erhalten (10.x.x.x, 172.16.x.x oder 192.168.x.x, so zum Beispiel bei Germany.Net oder Metronet) oder wenn der Provider direkte Verbindungen zu Servern über den normalerweise für Internet verwendeten Port 80 sperrt (einige regionale Netsurf-Anbieter) und so die Nutzung seines Proxy-Servers erzwingt. Auch solche entfernt eingesetzten Filter können jedoch von einem entschlossenen Nutzer unterlaufen werden, insbesondere wenn er dabei Hilfe von außen bekommt.

Dieses Szenario entspricht im wesentlichen der Situation, in der sich Dissidenten in China[183] befinden, deren Internetzugriff die chinesische Regierung zu zensieren versucht. Über entsprechend konfigurierte "Anti-Zensur-Dienste“[184], die zum Beispiel am MIT (Massachusetts Institute for Technology) und anderen amerikanischen Universitäten betrieben werden, haben diese Nutzer dennoch unzensierten Zugriff auf die meisten Netzressourcen, wenn sie es wünschen.

Würden solche filternden Proxy-Server bei Access-Providern eingesetzt, müßten diese den Mischbetrieb erlauben, d.h. sie dürften den Zugriff für Erwachsene nicht beschränken, während sie gemäß den PICS-Voreinstellungen des Kunden filtern würden, wenn sich ein Jugendlicher einwählt. Erster Angriffspunkt wäre hier also die Benutzerauthentisierung, d.h. der Angreifer würde versuchen, sich als ein legitimer Nutzer auszugeben, für den keine Filtereinschränkungen aktiv sind.

---

182 Erich Moechel, "Sauberes Internet für Deutschland“, 30.10.98, http://www.heise.de/tp/deutsch/inhalt/te/1619/1.html: "[Der Provider] PSINet will 'gesetzestreues Surf-Vergnügen' möglich machen, aber ohne Garantie. [...] 'Die Stichwortkataloge und die genauen Filtermethoden müssen natürlich streng geheim bleiben', sagt der Pressesprecher von PSINet Deutschland, dem Tochterunternehmen des weltgrößten Internet Providers. 'Sonst könnte jeder sie ja relativ leicht umgehen.' “

183 "Political Security: A Closed or an Open Internet – The Great Red Firewall of China“, http://www.usembassy-china.gov/english/sandt/Inetcawb.htm.

184 Brian Ristuccia, 31.07.98: "Anti-Filtering-Proxy-Proxy: "httpd-afpp is designed to defeat the site-blocking fuctionality of censorware and filtering-proxies. The user first visits a site running the Anti-Filtering-Proxy-Proxy. Assuming this site is not blocked by the local filtering-proxy or censorware, the user is then free to browse any other web sites free of filtering-proxy or censorware restrictions.“, http://www.freshmeat.net/appindex/1998/07/31/901899756.html.

4.6.3 Aufwandsabschätzung

4.6.3.1 Kosten im Anbieterbereich

Für die Anbieter entstehen in erster Linie dann Kosten, wenn sie sich entschließen, ihre Angebote einzuordnen und mit Labels zu versehen. Diese Kosten sind höher, falls sie in die Gefahr geraten, für falsche Einordnungen haftbar gemacht zu werden, weil sie dann für die Einordnung auf den Rat von Experten zurückgreifen müßten.

Extreme Kosten können für alle Anbieter von dynamischen Inhalten entstehen, die ihre Seiten erst im Moment des Abrufes aus einer Datenbank oder einer anderen Datenquelle generieren, wenn diese sich dafür entscheiden, ihre Seiten individuell einzuordnen statt ein statisches, allgemeines Label für ihre gesamte Website zu erzeugen. Die Erzeugung von individuellen Labels, insbesondere von signierten Labels, wird eine mehr oder weniger große Änderung in der von diesen Anbietern eingesetzten Anwendung notwendig machen. Falls die verwendete Software vom Content-Provider nicht selbst entwickelt worden ist und auch nicht im Quelltext vorliegt, kann es dem Anbieter selbst unmöglich sein, diese notwendigen Änderungen selbst durchzuführen. Er ist dann vom Support seines Softwareherstellers abhängig.

Sollen die erzeugten Labels digital signiert sein, sind die notwendigen Änderungen in der Software zwangsläufig tiefgreifend und haben auch starke Auswirkungen auf die Performance: Da das PICS-Label entweder im HTTP-Dialog oder im Kopfteil (Header) der erzeugten Seite stehen muß, sich aber mit seiner kryptographischen Prüfsumme auf Informationen bezieht, die weiter unten auf der Seite stehen, muß zunächst die Seite erzeugt und lokal gepuffert und anschließend das Label generiert und signiert werden, bevor die Seite ausgeliefert werden kann. Der Signierprozeß macht es also notwendig, daß auf der Serverseite entsprechend viel Speicher oder Festplattenbandbreite bereitgestellt wird, um die erzeugten Seiten vor der Auslieferung puffern zu können. Dies kann insbesondere auf vielbeschäftigten Servern enorme Speichermengen binden.[185] Effektiv würde sich der notwendige Hardwareaufwand durch die Erzeugung von individuellen Labels bei dynamischen Seiten etwa verdoppeln.

Anbieter mit dynamisch generierten Inhalten können durch dritte Rating-Services oft allenfalls pauschale Labels erhalten, da derartige Sites einen quasi-unendlichen URL-Raum mit einem hohen Grundumsatz bei den Inhalten haben. Dies betrifft alle Nachrichten-Services (z.B. CNN oder Heise Newsticker), die meisten Webshops mit Katalogsystemen (z.B. Amazon oder Beate Uhse) und alle Community-Websites (z.B. Slashdot oder jede Homepage mit einem Gästebuch) sowie weitere dynamisch gestaltete Angebote. Betroffen von dieser Einschränkung, nur pauschale Labels für die gesamte Sites anbieten zu können, sind im Prinzip auch mehrsprachige Angebote und alle Angebote mit automatischer Content-Negotation nach HTTP-Protokoll, weil die Sprachauswahl bzw. die Festlegung anderer Eigenschaften der Seite aufgrund von Voreinstellungen im Browser dynamisch erfolgen und

185 Anzahl der simultanen Verbindungen pro Sekunde mal durchschnittliche Seitengröße mal durchschnittliche Übertragungszeit pro Seite in Sekunden, z.B. für http://slashdot.org im Durchschnitt 100 s^{-1} * 200 KB * 25 s = 488 MB durchschnittliche Puffergröße. In Lastspitzen kann sich dies leicht verfünffachen.

sich nicht in der URL niederschlagen.[186] Es wird hier also dieselbe URL für unterschiedliche Seiteninhalte erzeugt; um eine digitalen Signatur eines Labels ungültig zu machen, reicht jedoch schon die Änderung eines einzigen Bits einer Seite. Gerade im vielsprachigen Europa stellt dies eine weitgehende Einschränkung dar.

4.6.3.2 Kosten im Abruferbereich

Wird Filtersoftware auf dem Rechner des zu schützenden Endnutzers installiert, treten zunächst einmal Kosten für die Beschaffung von PICS-kompatibler Software, deren Installation und Anpassung auf. Zusätzliche Kosten können durch den notwendigen Benutzersupport entstehen, wenn es durch Fehlfunktion, Falschkonfiguration, nicht ausreichend ausgebildete Benutzer oder Manipulation zu Problemen mit dieser Software kommt. Arbeiten Erwachsene und die zu schützenden Jugendlichen an demselben Rechner, sind diese Supportkosten höher, da die Filtersoftware je nach Nutzer ab- und wieder eingeschaltet werden muß und sich dadurch auch das Verhalten des Systems ändern kann.

Die Installation von Filtersoftware auf einem Rechner eines Endnutzers zieht zusätzlichen Aufwand bei der Sicherung dieses Rechners gegen Manipulation nach sich, wenn die Installation der Software nicht bloß ein symbolischer Akt bleiben soll. Dies gilt um so mehr, wenn die verwendete Rechnerplattform keine lokale Sicherheit bietet.

Wird Filtersoftware auf einem zentralen Proxy-Server installiert, der dem direkten Zugriff der Endnutzer entzogen ist, kann eine große Anzahl von Arbeitsplätzen zentral administriert und konfiguriert werden, wodurch es zu geringeren Mehrkosten kommen und die Manipulationssicherheit steigen kann. Soll der Proxy im Mischbetrieb für Nutzer mit und ohne Filterbedürfnis betrieben werden, entsteht Aufwand hauptsächlich im Bereich der Benutzerauthentifizierung.

4.6.3.3 Kosten im Filterbereich

Auf Rating-Services und Label-Provider entfallen für die Bereitstellung ihrer Dienste Kosten, die durch den erforderlichen Personaleinsatz, die benötigte Leitungskapazität, die benötigte Software und weitere Betriebsmittel entstehen. Dazu kommen weitere Kosten für die Deckung von Forderungen, die sich aus möglicherweise ergebenden Haftungsansprüchen gegen den Betreiber einer solchen Infrastruktur ergeben bzw. Kosten für die Versicherung gegen solche Ansprüche und die daraus resultierenden Folgekosten.

Eine weitere Quelle von Kosten werden die Kosten für den Betrieb der Public-Key-Infrastruktur[187] für die digitale Signatur der Labels sein. Insbesondere wenn man sich für die Kombination von First-Party-Rating und digitales Signieren der Labels entscheidet, ist eine extrem große Anzahl von Schlüsseln zu verwalten.[188]

---

186 Siehe die Dokumentation zum Apache-Modul mod_negotiation, http://www.apache.org/manual/mod_negotation.html und zum Apache-Modul mod_mime, http://www.apache.org/manual/mod_mime.html. Effektiv liefert der Webserver bei einem Request für eine Seite http://www.server.de/index.html hier je nach Sprachvoreinstellung am Browser unter dieser URL entweder den Inhalt von index.html.de oder index.html.en oder einer anderen Sprachvariante, je nach Voreinstellung auf Seiten des Anwenders. Obwohl es sich hier um statische Seiten handeln kann, sind diese Seiten aufgrund der URL alleine nicht unterscheidbar und daher bei einem rein URL-basierten Identifikationsschema wie PICS nicht verwendbar.

187 Public Keys oder "öffentliche Schlüssel“ sind eine Möglichkeit, Verschlüsselung im Datenaustausch zu realisieren.

188 Vgl. Kapitel 6.

4.6.3.4 Allgemeine Kosten

Die genauen Auswirkungen von Rating-Services und Labels auf die Anzahl der Verbindungen, die Menge der übertragenen Daten und die generellen IP-Kosten sind nur schwer abzuschätzen. Dies hat seine Ursache teilweise auch darin, daß seit Ende 1995 mit der Abschaltung des NFS-Net-Backbone keine globalen Verkehrsdaten über das Internet mehr erhoben werden können und insbesondere Verkehrsanalysen, die den Datenverkehr im Internet nach Protokollen unterscheiden, nicht mehr durchgeführt werden. (Mehr Informationen über Verkehrsanalyse im Internet finde sich in den Arbeiten von K. Claffy[189] und W. Braun sowie auf Russ Haynals ISP-Page[190].)

Ebenso ist die Anzahl und Güte der erfolgten Einordnungen von Seiten in ein Kategoriensystem vorab nicht abschätzbar. Diese Faktoren wären jedoch bestimmend für den Aufwand, der für Kontrolle und Validierung der Seiteneinstufungen zu treiben ist.

Die weitere Entwicklung des Marktes innerhalb der nächsten fünf Jahre wird ebenfalls kostenbestimmend sein. Sobald die Kosten für Standleitungen innerorts unterhalb der 70 DM/Monat-Schwelle ankommen und durch sinkende Rechnerkosten ununterbrochen laufende Rechner in Haushalten populär werden[191], wird sich die Struktur der Anbindung von Haushalten noch einmal drastisch ändern. Viele Haushalte, die heute bei tickender Uhr über Telefoneinwahl nur temporär an das Internet angebunden sind, werden dann über Standleitung und einen Microserver, der zugleich Webserver und Firewall[192] ist, dauernd mit dem Netz verbunden sein. Diese Haushalte haben dann die Option, zugleich ihre eigenen Content-Provider, Presence-Provider und Abrufer für die Angebote anderer zu sein. Die Rolle des Internet Service Providers wird in dem Fall die eines reinen Access-Providers und Support-Dienstleisters

189 Siehe http://www.nlanr.net/Papers/kc_menu.html.

190 Siehe http://navigators.com/isp.html.

191 "Internet Appliances“ wie zum Beispiel der Cobalt Cube, http://www.cobalt.com.

192 Rechner, der ein Netz vor ungewollten Zugriffen von außen schützt.

5 Programmtests

5.1 Kurzfassung

Das flgende Kapitel beginnt mit einem Überblick über vorhandene Programme zur Internetfilterung. Aus diesen werden einige Produkte ausgewählt und einem genaueren technischen Test bezüglich ihrer Funktionalität unterzogen. Mit Hilfe von Befragungen wurden Erwartungen von Nutzern ermittelt und durch praktische Tests konkretisiert.

Es gibt auf dem Markt eine große Anzahl von Programmen, die Internetfilterung im weitesten Sinne durchführen. Für den Jugendschutz sind im wesentlichen drei Gruppen relevant:

- Stand-Alone-Programme zur Installation auf lokalen Rechnern
- Angebote von Online-Diensten
- Spezielle Internetinhalte für Kinder

Für den Test wurden daraus zwei Stand-Alone-Produkte – CyberPatrol und WebChaperone – und ein Online-Dienst-Angebot (CompuServe) ausgewählt.

Sowohl die technischen als auch die praktischen Test zeigen, daß keines der Produkte in seinem aktuellen Stand in der Lage ist, eine zufriedenstellende Unterstützung des Jugendschutzes zu gewährleisten. Die größten Mängel sind

- fehlende Mehrsprachigkeit und
- mangelnde Transparenz der Filterkriterien,

außerdem eine Reihe von technischen Problemen bei der Verwendung.

Obwohl das Ergebnis der Untersuchungen nicht die Identifikation eines geeigneten Werkzeugs zur technischen Unterstützung des Jugendschutzes im Internet ist, kann aus den geschilderten Tests immerhin ein detailliertes und realisierbares Anforderungsprofil für ein solches Hilfsmittel abgeleitet werden. Das in Kapitel 6 skizzierte technische Szenario baut u.a. darauf auf.

5.2 Überblick über Programme zur Internetfilterung

Die klassifizierten Methoden zur Inhaltsfilterung im Internet werden in einer Vielzahl von Programmen auf verschiedene Arten realisiert.

Neben *Filterprogrammen*, die direkt eine oder mehrere der beschriebenen Filtertechnologien anwenden (häufig mit weiteren Möglichkeiten zur Unterstützung und Kontrolle der Internetkommunikation), gibt es noch eine Vielzahl andere Angebote zur Aufbereitung des Internet für Kinder. So bieten *Suchmaschinen* spezielle Seiten an, die die Suchergebnisse filtern. Außerdem gibt es spezielle *Web-Angebote für Kinder* und Browser, die so konfiguriert werden können, daß ein Verlassen dieses Bereiches technisch verhindert wird.

Die Programme werden entweder auf dem *lokalen* Rechner bzw. dem Proxy eines LANs (Local Area Network) oder auf dem *Server* eines größeren Netzes oder Internetserviceproviders (ISP) installiert und konfiguriert. Bei einigen Anbietern ist die Filterung bereits in das *ISP-Angebot* integriert. Die Produkte unterscheiden sich meist wenig in den Grundfunktionen; es gibt allerdings erhebliche Unterschiede in der Oberfläche, den Konfigurationsmöglichkeiten und den Sonderfunktionen.

5.2.1 Klassifizierung und Übersicht

Die in diesem Abschnitt definierten Klassen und Merkmale orientieren sich an den grundsätzlichen Anforderungen für eine wirkungsvolle technische Unterstützung des Jugendschutzes. Dabei beruhen die meisten Angaben auf Informationen von Herstellern und anderen Reviews. Die Einordnung kann also insbesondere im Hinblick auf die Funktionsmerkmale der einzelnen Produkte keine Vollständigkeit garantieren. Die Bewertung wurde im Hinblick auf eine möglichst breite Funktionalität vorgenommen. Sucht man nach Programmen mit einzelnen Funktionsaspekten, kann die Auswahl anders ausfallen.

5.2.1.1 Kategorien

Die technischen Umsetzungen lassen sich in drei Typen unterteilen:

- Stand-Alone-*Filterprogramme* werden zusätzlich zu den Kommunikationsprogrammen installiert und konfiguriert; sie beobachten dann die transportierten Daten und beeinflussen die Abrufe gemäß ihrer Einstellung. Für die spätere Anwendung ist es außerdem wichtig, ob sie lokal oder auf einem Server installiert werden; daher wird dies zusätzlich vermerkt.
- Ein solches Programm kann alternativ in das Angebot des *Internet Service Providers* integriert sein; damit entfällt die lokale Haltung von Programm und Konfigurationsdateien. Zusätzlich erfolgt die Pflege der Filterkriterien und -listen an zentraler Stelle – mit weniger Aufwand bei der Verwendung, aber auch weniger Einfluß auf die Filterung und außerdem der Preisgabe des kompletten Abrufprofils des Kunden.
- Zusätzlich zu den Filterprogrammen gibt es *sonstige Angebote*, die die Benutzung des Internet für Kinder unterstützen. Sie enthalten meist keine Sperrfunktionen und sind daher nur als Ergänzung zu anderen Filtertechnologien zu sehen.

In den folgenden Tabellen sind zu jedem Produkt einige charakteristische Merkmale angegeben. Dabei wurden die implementierten Filterverfahren, die Konfigurationsmöglichkeiten und die Zielgruppe des Programms angegeben, soweit dies aus den vorliegenden Informationen zu ersehen war.

Daraus wird abgeleitet, ob und warum die einzelnen für eine möglichst effektive technische Unterstützung des Jugendschutzes geeignet sind.

Kriterien dafür sind:

- ein großer Funktionsumfang (mindestens Positiv- und Negativlisten und Schlüsselwörter, möglichst auch PICS und kontextsensitive Verfahren),
- offene Bewertungskriterien für die mitgelieferten Listen, möglichst Listen im Klartext oder Werkzeug zur Überprüfung,
- Anpassungsmöglichkeiten an den konkreten Bedarf (Sicherheit, Altersgruppe, Wertvorstellungen), möglichst auch die Einrichtung mehrerer Benutzer mit unterschiedlichen Anforderungen,
- einfache Verwendbarkeit (sowohl in der Konfiguration als auch im Gebrauch), soweit sie sich ohne detaillierte Tests feststellen läßt,
- die Verfügbarkeit in Deutschland.[193]

[193] Das Vorliegen einer deutschsprachigen Version der Software und deutscher Kategorien ist zwar für eine spätere Verwendung z.B. in Schulen unabdingbar. Hier wird diese Forderung jedoch nicht aufgestellt, da nur eines der Programme (CyberPatrol) über eine deutschsprachige Version verfügt, die aber nicht als Testversion verfügbar ist.

Die letzte Spalte dient zur Vorauswahl für den detaillierten Produkttest. Neben einer generellen Eignung für den technischen Jugendschutz nach den genannten Kriterien sind hier für eine Berücksichtigung außerdem die Verfügbarkeit des Programmes und der nötigen Hardware und eine Anwendbarkeit auf Deutschland Voraussetzung.

Bei der Vorauswahl wurde sichergestellt, daß alle grundlegenden Filtermechanismen und die wesentlichen Zusatzfunktionen berücksichtigt wurden; die Filterfunktionen der nicht einbezogenen Produkte finden sich in den ausgewählten vollständig wieder.

5.2.1.2 Filterprogramme

Die folgende Tabelle gibt einen Überblick über existierende eigenständige Filterprogramme, die entweder lokal oder auf einem Server arbeiten. Die Informationen beruhen auf den eigenen Angaben des jeweiligen Herstellers und Reviews von dritter Seite.[194] Mit einem Teil der Programme werden im weiteren Verlauf eigene Tests durchgeführt, siehe unten.

Produkt	**Webseite**	**Typ**	**Anmerkungen**	**Jugend-schutz möglich[195]**	**Weitere Tests**
Access Management Engine (AME)	www.bascom.com	Filterprogramm lokal	nur Positivliste	nein, zuwenig Funktionen	nein
Bess	www.n2h2.com	Filterprogramm Server oder Proxy	mittlerer Funktions-umfang, Kunden z.B. ISPs	ja	bedingt schwierig zu testen
ChoiceView	www.cleanscreen.net	Filterprogramm Proxy	eigene Listen, kontextsensitive Untersuchung, Schutzklassen und Listen einstellbar	bedingt, kein PICS	nein
Click and Browse Jr.	www.netwavelink.com	Filterprogramm lokal	nur Positivliste	nein, zuwenig Funktionen	nein
Cyber Patrol	www.learningco.com	Filterprogramm lokal	verschiedene Methoden, großer Konfigurationsspiel-raum, PICS, deutsche Version	ja	ja

194 Vgl. auch

- Lorrie Faith Cranor et al, Technology Inventory – A Catalog of Tools that Support Parents' Ability to Choose Online Content Approrpriate for their Children, http://www.research.att.com/projects/tech4kids/t4k.html,
- SmartParents – Protect your kid, http://www.smartparent.com/protect.htm,
- Jürgen Schmidt, Kindersicheres Netz, c't 15/97
- So schützen Sie Ihre Kinder, Tomorrow, 2/99

195 Im Sinne der Kriterien des vorhergehenden Abschnittes.

Produkt	Webseite	Typ	Anmerkungen	Jugend-schutz möglich[195]	Weitere Tests
Cyber Snoop	www.pearlsw.com	Filterprogramm lokal	ähnlich CYBERsitter	ja	ja
CYBERsitter	www.solidoak.com	Filterprogramm lokal	Negativliste, PICS, kontextsensitive Untersuchungen	ja	ja
DiskTracy	www.disktracy.com	Filterprogramm lokal	Suchen und Protokollieren, eingeschränkte Sperrfunktion	bedingt, zuwenig Funktionen	nein
EdView	www.edview.com	Filterprogramm lokal	Positivliste mit eigenen Angeboten, pädagogischer Hintergrund	bedingt, große Einschränkung des Internets	nein
Greenbox	www.greenbox.net	Filterprogramm Server	großer Funktionsumfang Hardware im Angebot enthalten	ja	nein, da nicht frei verfügbar
GuardiaNet	www.guardianet.net	Filterprogramm lokal	Positivliste, z.Z. automatisch erstellt, Listen konfigurierbar, PICS	ja, wenn Listen von guter Qualität	ja
IBM Web Traffic Express	www.ics.raleigh.ibm.com	Filterprogramm Server	PICS, nur Sperrung Zielgruppe: Firmen	nein, zuwenig Funktionen	nein
I-Gear	www.urlabs.com	Filterprogramm Server	sehr teuer, nur Sun-Solaris	nein, Speziallösung	nein, nicht verfügbar
Internet Filter	turnercom.com/if/	Filterprogramm lokal	einfache Funktionen	bedingt, zuwenig Funktionen	nein
KidDesk Internet Safe	www.edmark.com/prod/kdis	Filterprogramm lokal	nur Positivliste	nein, zuwenig Funktionen	nein
Kids CyberHighway	www.att.net	Filterprogramm lokal	CyberPatrol integriert, kinderfreundliche Oberfläche	ja	ja, alternativ zu CyberPatrol
Kids Protection Online	www.kpo.net	Filterprogramm lokal	Negativliste Integration in AOL möglich	nein, zuwenig Funktionen	nein

Produkt	Webseite	Typ	Anmerkungen	Jugend-schutz möglich[195]	Weitere Tests
Kidsafe Explorer	www.arlington.com.au	Filterprogramm lokal	nur Positivliste Sperrung anderer Programme auf lokalem Rechner	nein, zu große Einschränkung	nein
Mail Gear	www.urlabs.com	Filterprogramm lokal	nur Mail	nein, zuwenig Funktionen	nein
Microsoft Internet Explorer	www.microsoft.de	Filterprogramm lokal	RSACi integriert, weitere Filtersysteme durch *.rat Dateien importierbar	bedingt, da keine Listen, einfach zu umgehen	nein
Net Nanny	www.netnanny.com	Filterprogramm lokal oder Server	Positiv- und Negativlisten, Wortfilterung, kein PICS, Zusatzfunktionen zur Computerkontrolle	ja	ja
Net Rated	www.netrated.com	Filterprogramm lokal	Negativliste, Wortfilterung, Computerkontrolle,	bedingt, wenig Konfiguration	nein
Net Shepherd World Opinion Rating Service	www.netshepherd.com	Filterprogramm lokal (Liste auf dem Server)	Kombination aus kostenfreier Software und kostenpflichtigen Abruf von Informationen, PICS-fähiger Browser erforderlich.	bedingt, da wesentlich von Zusatzsoftware abhängig	nein
NetFilter	www.netfilter.com	Filterprogramm Server	feste Liste von Adult-Sites wird gesperrt, Server-Lösung, teuer	nein, zuwenig Funktionen	nein
Netscape Communicator 4.5	www.netscape.com	Filterprogramm lokal	RSACi und SafeSurf auf PICS-Standard keine Listen	bedingt, da keine Listen	nein
Perkeo	www.perkeo.net	Filterprogramm lokal	Sucht nach bekannten kriminellen Inhalten per Fingerprint von Dokumenten und Bildern; daher Zielgruppe Serverbetreiber, aber keine vollständiger Jugendschutz	nein, zuwenig Funktionen	nein

Produkt	Webseite	Typ	Anmerkungen	Jugend-schutz möglich[195]	Weitere Tests
PlanetView	www.planetview.com	Filterprogramm lokal (Liste auf Server)	Funktion auf dem Server, der jedesmal abgefragt werden muß, Negativlisten	bedingt, langsam, Funktionalität klein	nein
SaveOur System	sos.sterlingweb.com	Filterprogramm lokal	Viele Einstellmöglichkeiten Schutz vor Datenverlust integriert	ja	ja
SmartFilter	www.smartfilter.com	Filterprogramm Server	Server-Lösung	bedingt, da sehr teuer	nein
SurfMonkey	www.surfmonkey.com/quick_tour/qt_browser.htm	Filterprogramm lokal	Basiert auf SurfWatch kindgerechte Oberfläche, kein PICS, eigenes Angebot nur MS IE	ja, für jüngere Kinder	bedingt, da kein PICS
SurfWatch	www.surfwatch.com	Filterprogramm lokal, Server	Lösungen für Client und Servers, sehr flexibel, kein PICS	ja	ja
The Internet Filter	www.turnercom.com	Filterprogramm lokal	Sehr tief im System, nur Negativlisten, wenige Voreinstellungen	nein, zuwenig Funktionen	nein
TripleExposure	www.ips-corp.com/tripleex.htm	Filterprogramm lokal	nur Protokollierung	nein	nein
WatchGuard SchoolMate	www.watchguard.com/schoolmate.html	Filterprogramm Server	speziell für Schulen, Filterung geschieht durch Cyberpatrol	nein, Schwerpunkt liegt auf Netzadministration für Schulen	nein
WebChaperone with iCRT	www.webchaperone.com	Filterprogramm lokal	Negativ-, Positivlisten, PICS, Kontextbeurteilung	ja	ja
WebDoubler	www.maxum.com/WebDoubler/	Filterprogramm lokal	teuer, nur für Macintosh, wenig Funktionen	nein, zuwenig Funktionen	nein
WebSENSE	www.websense.com	Filterprogramm Server	eher für große Netze, kein PICS	nein, zuwenig Funktionen	nein

Produkt	Webseite	Typ	Anmerkungen	Jugend-schutz möglich[195]	Weitere Tests
WebSense	www.websense.com	Filterprogramm lokal, Server	noch nicht verfügbar	nein	nein
WinGuardian	www.webroot.com	Filterprogramm lokal	nur Protokollierung	nein, zuwenig Funktionen	nein
WinWhatWhere	www.winwhatwhere.com	Filterprogramm lokal	nur Protokollierung und Zeitmanagement	nein, zuwenig Funktionen	nein
Wizguard	Www.wizguard.com	Filterprogramm lokal	keine Listen, kontextsensitives Filtering, PICS	ja	ja
X-STOP	Www.xstop.com	Filterprogramm lokal	nur Pornographie, nur Negativliste	nein, zuwenig Funktionen	nein

5.2.1.3 Internetserviceprovider

Verschiedene Provider haben bereits eine Filterung in ihr Angebot integriert. Die Funktionen sind ähnlich wie bei den Stand-Alone-Produkten. Allerdings entfällt der Installationsaufwand; und auch eventuelle Probleme im Zusammenspiel zwischen Filtersoftware und Internetprogramm reduzieren sich. Andererseits ist die Konfiguration weniger transparent. Auch müssen bei der Konfiguration immer Daten an den ISP übergeben werden (z.B. das Vorhandensein minderjähriger Kinder oder Informationen über politische und/oder pädagogische Präferenzen), die sich in den Einstellungen der Filterung niederschlagen. Auch der Filtervorgang selber findet beim Provider statt und kann dort "mitgeschnitten“ werden.

Die folgende Tabelle gibt einen Überblick über die wichtigsten Internetprovider in Deutschland und deren technische Unterstützung des Jugendschutzes.[196]

Produkt	Webseite	Anmerkungen	Integrierter Jugendschutz vorhanden (ISP/Client)
America Online Parental Controls	www.aol.com	eigene Funktionalität, nutzerspezifische Sperrung bestimmter Funktionen (Email, WWW) möglich, CyberPatrol integriert	ja/möglich
Compuserve	www.compuserve.com	eigene Funktionalität, CyberPatrol wird "unterstützt“	ja/möglich

196 Selbstverständlich kann mit jedem ISP die ganze Palette der Filterprogramme genutzt werden. Hier werden jedoch die bereits in der ISP-Software bzw. im ISP-Angebot integrierten Möglichkeiten betrachtet.

Produkt	Webseite	Anmerkungen	Integrierter Jugendschutz vorhanden (ISP/Client)
T-Online	www.t-online.de	nach Auskunft des technischen Services kein eigenes Angebot; Verwendung von CyberPatrol möglich	nein/möglich
germany.net	www.germany.net	Auskunft des technischen Service: Schreibberechtigungen werden nur an Personen ab 16 vergeben, ohne Schreibberechtigung ist kein Zugriff auf Server außerhalb der Domain .de möglich, innerhalb von .de als jugendgefährdend eingestufte Server sind generell gesperrt. keine sonstige Filterung	nach Angabe /nein

In Amerika gibt es weitere Anbieter, die in ihren Internetservice Filterfunktionen integriert haben.[197] Sie sind zum Teil in ihrem Internetangebot zielgruppenspezifisch ausgerichtet, also z.B. für Familien oder Schulen. Der Umfang ihrer Technologie für die Filterung ist eher knapp.

5.2.1.4 Sonstige Angebote

Neben den Filterprogrammen, die entweder zusätzlich zur Internetzugangssoftware betrieben werden oder von den ISP direkt zur Verfügung gestellt werden, gibt es ergänzende Angebote, die die Nutzung des Internet durch Kinder und Jugendliche sinnvoll gestalten helfen. Dies sind z.B. spezifisch konfigurierbare Suchmaschinen und besondere Kinder-Sites. Sie sind z.T. mit einfachen Filterfunktionen ausgestattet, die ein Verlassen des entsprechenden Servers verhindern. Für einen umfassenden technischen Jugendschutz bieten sie nicht genug Funktionen.

Im folgenden finden sich einige Beispiele für solche Kombinationen von kinderspezifischem Angebot und elementaren Filterungen; eine umfassende Liste über Angebote für Kinder wird im Rahmen der Übersicht über Initiativen zum Jugendschutz zusammengestellt.

Produkt	Webseite	Typ	Anmerkungen	Jugendschutz möglich?
AltaVista Filtered Search Service	www.altavista.digital.com	Suchmaschine	nur Suchfunktion, keine Sperrfunktionen	nein, zuwenig Funktionen

197 Z.B. FamilyConnect (www.familyconnect.com), Integrity Online (www.integrityonline com/kids.htm), Mayberry USA Filtered Internet Access Accounts (www.mayberry.net), Scholastic Network (www.scholasticnetwork.com)

Produkt	Webseite	Typ	Anmerkungen	Jugendschutz möglich?
Bonus.com the SuperSite for Kids	www.bonus.com	Web-Angebot für Kinder Filterprogramm (eingeschränkt)	großes Eigenangebot, keine Kosten, drei Altersklassen, keine lokale Software, daher keine Konfiguration möglich, eigene Listen	bedingt, fehlende Konfiguration, Angebot müßte für D neu erstellt werden
Disney's Blast Online	www.disney.com	Web-Angebot Kinder Filterprogramm (eingeschränkt)	wenig Funktionen, sehr produktbezogen, Integration von SurfWatch möglich	nein, zuwenig Funktionen

5.2.2 Kurztests und Auswahl

5.2.2.1 Kurztest Filterprogramme

Die gemäß der Tabelle aus Abschnitt 5.2.1 für weitere Tests geeigneten Produkte aus der obigen Übersicht wurden einem Kurztest unterzogen, um die endgültige Auswahl von drei Produkten fundiert durchführen zu können.

Dieser Test bestand aus der Installation, einer AltaVista-Suche nach den Stichworten "sex“ und "safer sex“, dem Aufruf einiger der gefundenen Seiten und einer Deinstallation.[198]

Die Installation war bei allen Produkten problemlos, die Ersteinstellung unterschied sich allerdings in Komfort und Erläuterung sehr. Alle Produkte reagierten auf die gefundenen Seiten mit Filterung; allerdings waren die Meldungen sehr unterschiedlich. Ebenfalls alle Produkte waren in der Lage, Seiten mit Aufklärung über "Safer Sex“ nicht zu filtern; allerdings rutschen dann auch einige erotisch-pornographische Seiten mit durch den Filter. Die Deinstallation war nicht bei allen Produkten erfolgreich. Der hier durchgeführte Test diente nur dem prinzipiellen Überprüfen der Funktionalität; die Ergebnisse wurden daher nicht im Detail ausgewertet. Eingehende Untersuchungen zur Filterqualität folgen für die ausgewählten Produkte.

Generell sind sich alle Produkte in ihrem funktionalen Umfang sehr ähnlich; Unterschiede liegen meist in der Benutzungsoberfläche und in Art und Umfang der Konfiguration. Kriterien für die Auswahl für weitere Tests sind daher eine leichte Bedienung, eine hohes Akzeptanzpotential durch eine intuitiv bedienbare Oberfläche und klare Sperrmeldungen. Außerdem soll ein möglichst großes Spektrum an Konzepten und Zielgruppen abgedeckt werden[199].

198 Da alle Programme für die Kurztests nur in einer englischen Version vorlagen und damit auch die Schlüsselwortliste nur aus englischen Begriffen bestand, mußten hier zur Überprüfung der grundsätzlichen Funktionsfähigkeit englische Begriffe verwendet werden.

199 Schwierigkeiten mit der Lauffähigkeit wurden zwar angemerkt, bei der Auswahl aber nicht negativ berücksichtigt, um nicht zufällige Inkompatibilitäten mit dem Testsystem zum Kriterium zu machen. Für die ausführlichen Tests im weiteren Verlauf der Studie werden definierte Testsysteme verwendet, um auch die Lauffähigkeit im Detail zu untersuchen.

Produkt	Verfügbarkeit	Anmerkungen	Technische Tests
GuardiaNet	kostenloses Demo	gute Installation, braucht spezielles Update zu Win95, Deinstallation nur mit Code, der nur telefonisch erhältlich ist, blockiert Netscape	bedingt ja sehr wirksam gegen Löschen
CYBERsitter	kostenloses Demo	unsichtbar, Blockade ist von ausgefallenem Server nicht zu unterscheiden, geringe Flexibilität[200]	bedingt ja (funktional den anderen unterlegen, aber sehr weit verbreitet)
CyberPatrol	kostenloses Demo	gutes Setup, viele Einstellmöglichkeiten, knapper Funktionstest erfolgreich, deutsche Meldungen	ja
WebChaperone with iCRT	kostenloses Demo	Sofort verwendbar, Registrierung erforderlich, gute Meldungen (für Kinder)	ja
Kids CyberHighway	nicht verfügbar	keine Version verfügbar (auch nach Herstelleranfrage), Funktionen wie CyberPatrol	nein
Net Nanny	kostenloses Demo	einfach zu starten, zusätzliche Kontrolle über den gesamten Computer, Sperrmeldungen sehr verwirrend (Blinken, viele Fenster/Meldungen, sehr störend), geringe Filterwirkung	nein Fehlermeldungen nicht konstruktiv
SaveOurSystem	nicht verfügbar		nein
SurfWatch	kostenloses Demo	Paßwortschutz von Anfang an, selbständige Netzverbindung bei Installation (dauert lange), nach Neustart automatisch aktiv, keine Multiuser-Fähigkeit, sehr umfangreiche Listen	nein, kein PICS, Funktionalität kleiner als die anderer Programme
Cyber Snoop	kostenloses Demo	keine Vorkonfiguration, kein PICS, läuft instabil unter Win95, Deinstallation mühsam	nein, da kein PICS, Installation mühsam
WizGuard	kostenloses Demo	einfach zu starten, Sperrung erzeugt Meldung über Netzfehler, Konfigurationsmöglichkeiten sehr gering	nein, Konfigurationsmög- lichkeiten zu eingeschränkt

200 Vgl. auch: Jürgen Schmidt, Kindersicheres Netz, c't 15/97

5.2.2.2 Auswahl

Die vier in der Tabelle markierten Produkte eignen sich für einen detaillierten Test. Sie unterschieden sich im funktionalen Umfang kaum; mit ihnen wird also die Palette der vorhandenen Filtertechnologien gut abgedeckt:

- GuardiaNet
- CyberSitter
- WebChaperone with iCRT
- CyberPatrol

Um auch die Vor und Nachteile einer Filterung beim ISP zu untersuchen, sollte auch einer dieser Anbieter – also AOL oder CompuServe – in die Tests einbezogen werden.

Daher wird der Test mit einem ISP-Angebot und zwei der vier anderen Einzelprodukte durchgeführt. Aufgrund des Kurztests wird *CyberPatrol* und *WebChaperone* der Vorzug vor CyberSitter und GuardiaNet gegeben.

Beide ISP-Angebote basieren auf CyberPatrol, so daß ähnliche Ergebnisse zu erwarten sind. Aus technischen Gründen wird der Test mit CompuServe durchgeführt.

Bei den Tests ist darauf zu achten, daß neben der Funktion der einzelnen Programme auch die grundsätzlichen Wege der Filterung kritisch betrachtet werden. Ergebnis der technischen und praktischen Tests soll neben einer Aussage über das Programm auch die Konkretisierung einer Vision über die Gestaltung eines optimalen Filterprogrammes sein. Dies wird sich auch in den Testkonzepten niederschlagen.

5.3 Technische Tests der Filtersoftware

Zur systematischen Untersuchung einiger Produkte werden Fragestellungen und Anforderungen im Hinblick auf die in den vorangehenden Kapiteln zusammengestellten Anforderungen entwickelt und darauf basierend die Eigenschaften der zu testenden Produkte ermittelt und bewertet. Diese Bewertung bildet zusammen mit den Praxistests die Grundlage der im weiteren entwickelten Vision eines möglichst wirkungsvollen und zugleich realistischen Filterkonzeptes.

5.3.1 Technische Anforderungen

Um einen einfachen und effektiven Gebrauch der filtertechnischen Hilfsmittel auch für Nutzer zu ermöglichen, die mit den Details der Internetkommunikation nicht vertraut sind, bestehen hohe *allgemeine Anforderungen* an

- eine gute Dokumentation,
  die sich schnell erschließen läßt, ausführliche Suchfunktionen bietet und umfassende Hilfestellung bei Fragen von Installation, Konfiguration und Gebrauch leistet;
- die Einfachheit der Anwendung,
  d.h., einfache und gut geführte Installation, zuverlässige Deinstallation und eine Verwendung sämtlicher Kommunikationsdienste in der gewohnten Form, so sie nicht unter die gesperrten Kategorien fallen, außerdem direkt verwendbare Voreinstellungen und einfache Zugänglichkeit der Konfigurationsmenüs für die Administration;
- Zusatzfunktionen
  (z.B. Limitierung der Gesamtzeit des Internetzugangs, Zeitverwaltungen, Unterbindung der Weitergabe persönlicher Daten)
  Inwieweit diese erwünscht sind, hängt stark von den individuellen Anforderungen der

Nutzer ab; sie werden daher im Testbericht ebenfalls aufgelistet und in den Kontext des Jugendschutzes eingeordnet.

Bezüglich der implementierten *Filterfunktionalität* sollen die in bei der Untersuchung der Filtertechnologien formulierten Forderungen erfüllt werden, nämlich

- eine große Vielfalt der verfügbaren Funktionen,
  realisiert durch die Möglichkeit der Kombination mehrerer Verfahren. Mindestens Positiv- und Negativlisten für Seiten und Schlüsselwörter müssen zur Verfügung stehen. Außerdem soll möglichst auch PICS unterstützt werden und die Schlüsselwortfilterung soll kontextsensitive Elemente enthalten;
- eine umfassende Konfigurierbarkeit der Filterfunktionen,
  also detaillierte und trotzdem handhabbare Eingabemöglichkeiten für die persönlichen Präferenzen (sowohl zur expliziten Sperrung als auch zur expliziten Freigabe bestimmter Seiten oder Server), unterstützt durch sinnvolle und transparente Voreinstellungen, Mehrbenutzerfähigkeit;
- die Transparenz der Bewertungen,
  d.h. Veröffentlichung aller Kriterien und Überprüfbarkeit der Bewertungen für bestimmte Seiten, Server oder Wörter (in Form einer Klartextversion der Listen oder eines Werkzeugs zur Überprüfung), Offenlegung aller kontextabhängigen Filterverfahren.

Die vorhanden Filterfunktionen müssen auch *faktisch* eine effektive Filterung gewährleisten. Um dies zu testen, wird die Einhaltung der definierten Filterkriterien überprüft; dabei sollen keine (oder nach Maßgabe der Technik möglichst wenige) der Konfiguration nicht entsprechenden Sperrungen oder Freigaben erfolgen. Dieser Anforderung ist aufgrund der Komplexität besonders schwer zu genügen.

Als letzer Punkt ist eine hohe *Manipulationssicherheit* der vorgenommenen Einstellungen und der Filterwirkung unabdingbar, also eine verschlüsselte und versteckte Ablage der entsprechenden Dateien, die Unmöglichkeit der Umgehung bei Neustart des Rechners und gegebenenfalls eine zuverlässige Protokollierung der Netzkommunikation.

5.3.2 Testkriterien

Aus diesen allgemeinen technischen lassen sich detaillierte Fragestellungen ableiten. In der folgenden Darstellung werden sie differenziert in die Rubriken "Allgemeines“, "Filterfunktionen“, "Filtereffektivität“ und "Manipulationssicherheit“.

5.3.2.1 Allgemeines

Voraussetzungen

Zuallererst wird festgestellt, welche technischen Anforderungen die Software stellt, also

- welche Betriebssysteme unterstützt werden (Win95, Win98, WinNT oder weitere)
- welche Menge an Arbeitsspeicher und freiem Platz auf der Festplatte erforderlich sind,

außerdem eventuell spezielle Forderungen an

- den verwendeten Internet-Browser (Hersteller und Version) oder
- die Internetzugangssoftware.

Diese Informationen sind im allgemeinen der Programmdokumentation zu entnehmen; ihre Richtigkeit wird allerdings im Laufe des Tests soweit möglich überprüft.

Außerdem ist aufzuführen, wie das Programm erhältlich ist, welche Kosten entstehen – sowohl einmalig für die Programmlizenz als auch für Abonnements für Aktualisierungen – und auf welchem Wege evtl. nötige Aktualisierungen durchgeführt werden.

Dokumentation

Um das Programm effektiv verwenden zu können, ist eine ausführliche Dokumentation erforderlich. Beim Test ist festzuhalten, in welcher Form (z.B. online, verschiedene Dokumentenformate, z.B. pdf oder rtf) die Hilfe vorliegt. Das Hilfesystem sollte eine Suche über Stichworte ermöglichen; hilfreich sind auch Suchen im Kontext eines bestimmten Begriffes.

Generell sind die Übersichtlichkeit der Hilfe zu bewerten und einige beschreibende Stichworte zu Funktion, Umfang und Zweckmäßigkeit zu geben.

Einmalige Vorgänge

a) Installation

Um die Installation möglichst einfach zu gestalten, ist eine hohe Automatisierung wünschenswert.

Eventuelle Fehlermeldungen sollten gut verständlich sein und zumindest einen Hinweis auf die Behebung geben (z.B. die Installation einer zusätzlichen Systemkomponente mit Angabe der Bezugsquelle im Internet).

Nach der Installation sollte ein Protokoll der installierten Dateien vorliegen.

Da alle Filterprogramme in die Kommunikationsfunktionen des Systems eingreifen, ist eine Deinstallation nur mit Hilfe des entsprechenden Hilfsprogramms möglich; ein diesbezüglicher Hinweis darf daher im Rahmen der Installation nicht fehlen.

Nach der Installation sollte das Programm automatisch starten bzw. einen Neustart vorschlagen und nach diesem aktiv sein. Wünschenswert ist dabei ein Erscheinen des Konfigurationsbildschirms beim Erststart oder zumindest eine Information darüber, welche Einstellungen erforderlich oder sinnvoll sind.

b) Konfiguration

Die Erstkonfiguration soll möglichst schon bei der Installation, spätestens aber beim ersten Start automatisch erfolgen. Dabei sollen alle benötigten Informationen verständlich abgefragt werden.

Im einzelnen können dies z.B. sein:

- Informationen über vorliegende Hard- und Software (deren Erfassung sollte allerdings möglichst automatisch geschehen)
- Auswahl von Filterverfahren (welche gibt es?)
- Einrichtung verschiedener Benutzer mit verschiedenen Schutzklassen
- Anpassung von Positiv- und Negativlisten an die persönlichen Vorstellungen
- Aktivierung der Sonderfunktionen des Programms.

Der Programmtest soll feststellen, welche dieser Möglichkeiten vorhanden sind, welche Optionen es jeweils gibt und wie komfortabel die Konfiguration zu bedienen ist. Außerdem ist zu überprüfen, ob es eine Hilfefunktion oder eine Dokumentation gibt und wie gut diese ist.

c) Deinstallation

Die Deinstallation muß auf jeden Fall automatisch geschehen. Nach dem Vorgang dürfen keine Programmreste auf der Festplatte verbleiben.

Zu überprüfen ist daher, ob noch Einträge im Startmenü vorhanden sind und ob es noch einen Ordner oder Dateien mit den Programmnamen auf der Festplatte gibt. Außerdem darf bei Windows-Systemen auch die Registry[201] keine Programmeinträge mehr enthalten.

Sollte es eines Neustarts bedürfen, um die Funktionen des Programms endgültig zu deaktivieren, so sollte dieser – nach Anfrage – selbsttätig durchgeführt werden.

Wünschenswert ist außerdem eine Protokolldatei, die Auskunft über die gelöschten Dateien gibt; im besten Fall wird diese automatisch und nachprüfbar mit der entsprechenden Protokolldatei der Installation abgeglichen.

d) Gebrauch

Im Gegensatz zur Konfiguration, die hauptsächlich vom Administrator oder von den Eltern durchgeführt wird, wird das Programm dauerhaft eher von Kindern bzw. Jugendlichen verwendet. Optimale Funktion weist es auf, wenn außer gelegentlichen Sperrmeldungen keine erkennbare Beeinflussung des Rechners stattfindet. Außerdem sollten eventuell vorhandene Protokollfunktionen korrekt arbeiten. Desweiteren ist die Sicherheit des Programms gegenüber Manipulationen der Filtereinstellungen, der Protokolldateien und einer Deinstallation zu testen. Im einzelnen stellen sich folgende Fragen:

e) Genereller Eindruck

- Welchen Gesamteindruck hinterläßt das Programm?
- Ist sein Betrieb am Rechner zu erkennen (z.B. durch Einblendung in der Startzeile, Einblendung im Browser)?
- Treten Störungen bei normalem Internetbetrieb auf?[202]
- Gibt es weitere Anmerkungen?

f) Sperrmeldungen

- Wie sehen Sperrmeldungen aus?
- Gibt es verschiedene?
- Sind sie nachvollziehbar?
- Ist es möglich, den Grund der Sperrung zu ermitteln?

g) Protokolle

- Welche Möglichkeiten zur Protokollierung gibt es?
- Was wird protokolliert?
- Sind sie vollständig (Stichprobe)?
- Sind die Protokolle zugänglich/editierbar?

h) Aktualisierung

- Erfordert das Verfahren eine Aktualisierung?
- Wie wird sie durchgeführt?
- Wie häufig werden neue Daten angeboten?

---

201 Der Ort, an dem das Betriebssystem Konfigurationsinformationen ablegt.

202 Hiermit sind vor allem technische Probleme mit dem Netzwerk gemeint. Da diese allerdings nicht immer von funktionierenden, aber sehr langsamen Übertragungen zu unterscheiden sind, sollten auch keine zu großen Verzögerungen durch die Filterung hervorgerufen werden (oder diese zumindest für den Benutzer sichtbar und nicht mit Netzwerkproblemen verwechselbar sein).

- Was wird aktualisiert?
- Müssen dabei Daten des Endbenutzers an den Programmherstellers übertragen werden? Was geschieht in diesem Fall mit den Daten?
- Welche Kosten sind mit der Aktualisierung verbunden?

i) Stabilität und Fehlermeldungen

- Gab es in der Testphase Probleme mit der Stabilität des Rechners oder der Netzverbindung, die auf das Programm zurückzuführen sind?
- Gab es Fehlfunktionen?
- Wenn ja, waren sie gut erläutert? Behebbar?

5.3.2.2 Filterfunktionen

Die Funktionalität kann in den meisten Fällen der Dokumentation entnommen werden. Es werden hier die Filterverfahren, die Bewertungsmethoden und die Sonderfunktionen betrachtet.

Filterverfahren

In einem ersten Schritt wird geprüft, welche der existierenden Verfahren im Programm implementiert sind, also Positivlisten, Negativlisten, Ratingsysteme und automatisierte Verfahren wie Schlüsselwortsuchen, und welche Algorithmen im einzelnen verwendet werden.

Dabei sind folgende Aspekte von besonderem Interesse:

- Können in die Adresslisten zusätzliche Seiten/Server eingefügt werden?
- Sind die Inhalte der Listen überprüfbar (als Klartext oder mit speziellem Hilfsprogramm)?
- Sind die Listen ausreichend gegen die Verwendung als Quelle für jugendgefährdende Inhalte geschützt? [203]
- Ist das System PICS-kompatibel?
- Werden konkrete Ratingsysteme (SurfWatch, RSACi, andere) unterstützt?
- Welcher Art ist die Schlüsselwortfilterung?
- Ist die Schlüsselwortliste veränderbar?
- Wie oft finden Aktualisierungen statt?
- Welche Art von personenbezogenen Daten fallen bei der Nutzung des Programmes auf dem System und beim Bereitsteller der Filterlisten an?

Außerdem soll vermerkt werden, welche Protokolle kontrolliert werden (http, ftp, nntp, smtp) und ob Unterschiede zwischen der Funktionalität und Effektivität der Filterung bei verschiedenen Diensten bestehen.

Grundlagen der Inhaltsbewertung

Um die verwendeten Bewertungsverfahren möglichst genau kennenzulernen, sind folgende Punkte zu klären:

- Welche Art von Bewertung wurde vorgenommen (auch mehrere)?

---

203 Hier entsteht ein zu lösender Konflikt mit der vorhergehenden Anforderung, den das Programm befriedigend lösen soll.

- Wer hat bewertet?
- Liegen die Bewertungskriterien vor?
- Sind die Listen individuell zu ergänzen?
- Ist es möglich, gemäß den eigenen Anforderungen Wörter und/oder Seiten aus den Listen zu streichen?

Schutzklassen

Um eine Anpassung an den individuellen Filterbedarf zu ermöglichen, sollte das Programm entweder vordefinierte gut erläuterte Schutzklassen besitzen oder zumindest die Definition solcher Klassen ermöglichen.[204]

Außerdem sollte es die Einrichtung mehrerer, zu unterschiedlichen Schutzklassen gehörender Benutzer ermöglichen. Weiterhin wäre es sinnvoll, für jeden Benutzer separate Veränderungen der Filtereinstellungen zuzulassen.

Sonderfunktionen

Unter diesem Punkt ist eine Liste der vorhandenen Zusatzfunktionen aufzustellen. Dies könnten zum Beispiel sein

- ein Zeitmanagement für den Internetzugang,
- die Sperrung bestimmter oder aller Programme auf einem Rechner,
- ein Eingabeschutz für bestimmte Wörter und Zahlen, z.B. zur Verhinderung der Weitergabe persönlicher Daten,
- außerdem verschiedene Funktionen zum Protokollieren der Kommunikation.

5.3.2.3 Filtereffektivität

Die Effektivität der Filterung wird anhand einiger Beispiele exemplarisch überprüft.

Filterbeispiele

- Suche nach "sex“ (bei AltaVista)
  Überprüfung der Anzahl der Treffer im Vergleich zur ungefilterten Suche; Aufruf der ersten 10 Treffer und Test der Filterwirkung
  Wunsch: keine Anzeige von Seiten mit offensichtlich erotisch-sexuellem Inhalt; je nach Filtereinstellung auch keinerlei Anzeige von Informationen über Sexualität
- Suche nach "safer sex“ (bei AltaVista)
  Überprüfung der ersten 10 Treffer auf ihren Inhalt
  Wunsch: wie bei "sex“, allerdings Anzeige von informativen Seiten zur gesundheitlichen Aufklärung
- Überprüfung der Sperrung von Diensten
  Filetransfer, News, WWW, evtl. andere Sperrwirkungen.

Einzelseiten

Außerdem führten wir einen Einzeltest mit verschiedenen Seiten auf Filterwirkung und Filtergrund durch. Dafür haben wir verschiedene Seiten ausgewählt, die entweder immer

[204] Mit Schutzklasse bezeichnen wir hier die Zusammenfassung mehrerer Filtereinstellungen (z.B. "kein Sex“, "keine Gewalt“, "keine E-Mails mit Attachement“, "Spiele“, "kein Online-Shopping“) zu einer Gesamtkonfiguration (z.B. "Kinder unter 10 Jahren“); damit wird eine einfache Erstkonfiguration ermöglicht, die dann nach und nach an den exakten persönlichen Bedarf angepaßt werden kann.

gefiltert werden müssen, immer unproblematisch sind oder deren Zulässigkeit von der aktuellen Filtereinstellung abhängt.[205] Die Einordnung in zu sperrende und freizugebende Inhalte orientiert sich an den Kriterien des Jugendschutzes.[206]

Neben der generellen Filterung soll das Augenmerk auch auf den Filtergrund gelegt werden. Wenn die Seite explizit in der Sperrliste zu finden ist, sagt dies zwar etwas über die Vollständigkeit der Liste aus; die Reaktion des Programmes auf ähnliche Seiten, die nicht bekannt sind, ist jedoch unklar. Insofern sollten beim Test immer auch Seiten überprüft werden, die in keiner Liste explizit enthalten sind. Gegebenenfalls ist die vorgeschlagene Auflistung von Referenzseiten daher sinnvoll zu ergänzen.

Im einzelnen haben wir Seiten aus den folgenden Rubriken getestet

- Politik – Information und Extremismus
- In diese Kategorie fallen Seiten mit politischen und auch zeitgeschichtlichen Informationen, aber auch politisch extreme Aussagen. Für letzere haben wir bevorzugt solche Inhalte ausgewählt, die in Deutschland als jugendgefährdend indiziert oder sogar verboten sind.
- Gewalt
- Die auffindbaren Seiten enthalten gewaltverherrlichende Computerspiele oder Gewalt im Zusammenhang mit Sexualität.
- Sexualität
- Hier gibt es Seiten mit unterschiedlichem sexuellem Inhalt. Die deutschen Seiten sind nicht als jugendgefährdend klassifiziert, aber für kleine Kinder trotzdem ungeeignet. Z.T. enthalten sie Äußerungen eher komischen Charakters, die aber aufgrund des Themenbereiches für jüngere Kinder gesperrt bleiben sollten. Andere Seiten bieten sehr explizite und z.T. gewalttätige Bilder an und dürfen die Filterung in keinem Fall passieren.
- Gesundheitliche und sexuelle Aufklärung
- Die Sperrung dieser Seiten ist für kleine Kinder sinnvoll; gerade für Jugendliche bieten solche Seiten aber wertvolle Hilfen und sollten auf keinen Fall gesperrt werden. (Außerdem stellen solche Seiten natürlich den Filtermechanismus auf die Probe, da eine Unterscheidung von erotischen Seiten über Schlüsselwörter o.ä. nicht mehr problemlos möglich ist.)
- Allgemeine Information
- In dieser Rubrik wird das allgemeine Verhalten getestet; es werden Seiten mit Einkaufsangeboten aufgerufen, außerdem Kinoprogramme und Spezialangebote für Kinder.

Außerdem wird die Seite der Organisation "Peacefire“ getestet, die große Kritik an Filterprogrammen äußert und deshalb bei einigen Produkten auf der Sperrliste landete (ohne in die zu sperrende Kategorie zu gehören).

5.3.2.4 Manipulationssicherheit

Ein abschließend wichtiger Punkt, der eine Grundlage für das Vertrauen in ein Filterprogramm bildet, ist die Sicherheit gegen absichtliche Manipulation. Im einzelnen tauchen dabei folgende Fragen auf:

---

205 Die einzelnen Adressen finden sich im Anhang; sie und die verschiedenen Seiten liegen auch elektronisch vor.

206 Vgl. z.B. Informationsschrift BPjS: Info zum Jugendmedienschutz, Drei-W-Verlag, Essen

- Wird das Programm automatisch gestartet?
- Ist eine einfache Umgehung bzw. ein Ausschalten (z.B. durch Installation und Nutzung eines anderen Browsers oder durch Verwendung von Word BASIC o.Ä.) möglich?
- Sind die Filtereinstellungen ausreichend geschützt (Paßwort, Konfigurationsdateien)?
- Ist eine Deinstallation möglich?
- Ist das Programm einfach zu löschen?
- Gibt es sonstige einfache Möglichkeiten, den Filterprozeß zu unterbrechen oder zu manipulieren?

Es ist generell davon auszugehen, daß absolute Sicherheit für den störungsfreien Ablauf des lokalen Filterprozesses nicht gewährleistet werden kann. Ziel muß es also hier sein, es "so schwierig wie möglich“ zu machen, die Filterung zu unterlaufen.

5.3.3 Durchführung der Tests

Nicht für alle Produkte lassen sich alle oben gestellten Fragen beantworten; z.T. sind sie auch nicht relevant. Daher findet sich im folgenden jeweils eine Zusammenfassung der relevanten, produktspezifischen Erkenntnisse aus den technischen Tests.

Alle Tests wurden unter Windows 95 durchgeführt; als Internetbrowser wurde die deutsche Version von Netscape 4.5 verwendet.

Die Teststruktur wurde für den Test bei CompuServe wegen der systematisch anderen Struktur des Systems abgeändert.

5.3.3.1 WebChaperone

Allgemeines

WebChaperone liegt vor in Versionen für Windows 95 und Windows NT. Es ist ca. 3 MB Platz auf der Festplatte erforderlich. Das Programm setzt als Browser Netscape oder Microsoft Internet Explorer jeweils ab Version 3.0 voraus.

Die Lizenzgebühr beträgt ca. 50 USD. Aktualisierungen sind aufgrund der Verwendung automatisierter Bewertung nicht erforderlich, ebenso keine Online-Verbindungen. Es entstehen also neben der Lizenzgebühr keine weiteren Kosten.

Die Hilfe erfolgt über HTML-Files unter Verwendung des eingestellten Browsers. Die enthaltenen Informationen sind übersichtlich und konnten auf fast alle im Rahmen der Tests auftauchenden Fragestellungen Antwort geben.

Besonders der Installationsprozeß ermöglicht es, direkt und ohne weitere Einarbeitung die nötigen Einstellungen vorzunehmen und sofort die erforderlichen Benutzer zu definieren und Ihnen die geeigneten Filteroptionen zuzuordnen. Allerdings aktiviert sich die Filterfunktion nicht selbsttätig, sondern muß durch bestimmte Einstellungen in den Konfigurationen der Netzverbindung aktiviert werden.[207]

Das Programm ist jederzeit durch das entsprechende Symbol in der Funktionsleiste zu erkennen.

Die Sperrmeldungen sind graphisch und textuell aufbereitet. Sie enthalten einen Rückverweis auf die vorige Seite und eine Möglichkeit zum Verzweigen auf spezielle Seiten von

[207] Es konnte auch im Kontakt mit dem Hersteller nicht geklärt werden, warum dieser Effekt auftrat.

WebChaperone mit Links zu für Kinder geeigneten Angeboten.[208] Auch Netzfehler wie nicht antwortende Server oder nicht vorhandene Seiten werden in diesem Format angezeigt.

Es gibt keine deutsche Version.

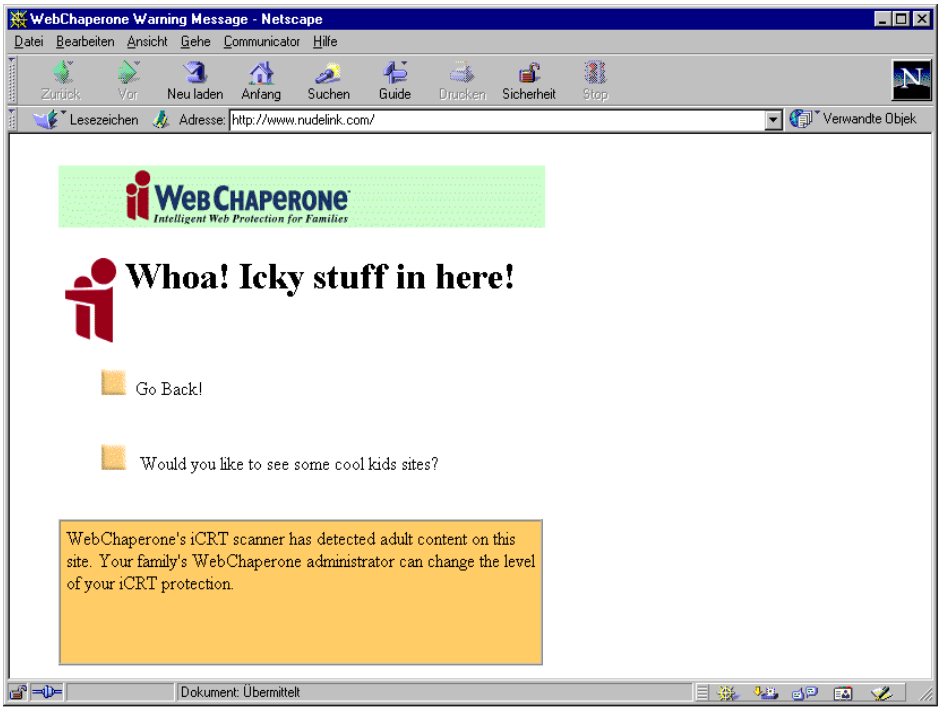


Abb. 5-1: Beispiel einer Sperrmeldung von WebChaperone

Filterfunktionen

Die Funktionalität von WebChaperone beruht auf einer patentierten Technologie iCRT[209], die eine automatisierte Bewertung der Seiten durchführt. Dabei werden kontextsensitive Verfahren eingesetzt. Zielrichtung ist die Ausfilterung von pornographischem und sexuell explizitem[210] Material; Erweiterungen auf weitere im Sinne des deutschen Jugendschutzes problematische Seiten (Rassismus, "Hate speech“ etc.), sind angekündigt, aber bisher nicht realisiert.

Neben diesem Verfahren wird PICS in Form von RSACi unterstützt. Außerdem kann eine Liste mit zusätzlich zu sperrenden Seiten angelegt werden (sie ist in Voreinstellung leer). Eine explizite Freigabe bestimmter Seiten ist nicht möglich.

Es ist die Definition mehrerer Benutzer möglich, die in eine von vier Alterskategorien[211] eingeordnet werden können. Jede dieser Abstufungen enthält ein voreingestelltes Schutzniveau – zusammen gesetzt aus einem Schutzlevel nach iCRT und einer PICS-Einstufung. Diese Level sind dann für jeden Benutzer separat zu verändern; die Listen

---

208 Diese Verzweigung führt allerdings dazu, daß bei jeder Sperrmeldung der Server von WebChaperone aufgerufen wird und damit quasi eine Nachricht über die Verwendung des Programms und ggf. die aufgerufene Seite verschickt wird.

209 Vgl. http://www.rulespace.com oder http://www.webchaperone.com/about.html

210 "sexually explicit“

211 Child, Pre-teen, Teenager, Adult. "Child“ garantiert eine strenge Filterung mit dem Seiteneffekt, daß möglicherweise auch unproblematische Seiten manchmal gesperrt werden. "Adult“ ist hingegen für Erwachsene gedacht, die aus Komfortgründen eine Sperrung von zufällig angewählten pornographischen Seiten wünschen.

können ebenfalls individuell konfiguriert werden. Nach einer einstellbaren Zeit der Inaktivität und bei Benutzerwechsel werden Speicher- und Festplattencache gelöscht.

Eine Überprüfbarkeit des Bewertungsergebnisses ist durch die Software selbst direkt möglich (nämlich durch Seitenaufruf und Überprüfung des Ergebnisses); eine Korrektur ist nur in restriktiver Richtung, nämlich durch Hinzufügung zur Sperrliste möglich; wie erwähnt sind explizite Freigaben nicht vorgesehen.

Filtereffektivität

Die Suche nach Wörtern wie "sex“ oder "safer sex“ bei einer Suchmaschine führt immer zu einer Sperrmeldung; eine solche Suche ist also nicht möglich. Damit wird zwar der Kontext unzureichend berücksichtigt, andererseits liefert auch eine Suche nach "safer sex“ so viele für Kinder ungeeignete Seiten, daß eine solche Einschränkung im Sinne der Sicherheit toleriert werden kann (die Vorschlagsliste sollte im besten Falle andere Zugangsmöglichkeiten zu entsprechenden Informationen enthalten, bisher ist sie lediglich auf das Alter des Kindes abgestimmt).

Die Sperrung anderer Dienste außerhalb des Browsers erfolgte nicht zufriedenstellend (News-Abfrage ist möglich).

Bei den Tests einzelner Seiten kristallisiert sich folgendes Bild heraus: Es werden mit großer Zuverlässigkeit englischsprachige erotisch-pornographische Seiten gefiltert. Sowohl deutsche Seiten mit gleichem Inhalt als auch alle Seiten mit politisch extremen Aussagen bleiben ungefiltert. Solche Seiten konnten nur richtig bewertet werden, wenn sie ein RSACi-Label enthielten.

Der Automat scheint also bei den Seiten, für die er entworfen wurde, gut zu funktionieren, allerdings ist das Hinzufügen zusätzlicher inhaltlicher Rubriken nicht möglich (es sei denn über PICS oder durch explizite Serverangabe). Die Resultate der Filterung sind nach diesen Regeln plausibel. In diesen Rahmen paßt auch, daß das Peacefire-Angebot nicht gesperrt wird; es entsteht allgemein kein Eindruck einer unerwünschten Zensur oder Einschränkung.

Die Filterergebnisse während des Tests änderten sich nicht durch eine Veränderung des Schutzlevels bei iCRT; die Filterung scheint also auf diese Anpassung recht unempfindlich zu reagieren. Für die PICS-Bewertung werden Einstufung und zu filternde Bewertungen exakt definiert, so daß die Reaktion hier eindeutig und korrekt ausgeführt werden kann.

Manipulationssicherheit

Der Programmstart beim Anschalten des Rechners erfolgt durch einen Eintrag in der Datei "win.ini“. Dieser Eintrag kann manuell gelöscht werden; allerdings wird er beim Neustart des Rechners automatisch wieder eingefügt. Gibt man der Datei aber zusätzlich das Attribut "read only“, kann diese Einfügung nicht erfolgen; damit wird der Start des Filterprogramms wirkungsvoll unterbunden.

Außerdem sind die einstellbaren Sperrlisten im Klartext auf der Festplatte abgelegt und problemlos editierbar (d.h. das Format ist sehr einfach und das Programm kann die Manipulation nicht erkennen).

Zusätzlich erfordert das Programm die Angabe eines Proxies in der Browsereinstellung. Hier kann der eigene Rechner[212] verwendet werden. Wird statt dessen aber "direkter Internetzugang“ gewählt, was im Rahmen der Browsereinstellung problemlos möglich ist, erfolgt keinerlei Filterung.[213]

---

212 mit IP-Nummer 127.0.0.1

213 Dieses Problem entfällt also nur dann, wenn der Internetzugang immer über einen Proxy erfolgt.

5.3.3.2 CyberPatrol

Allgemeines

CyberPatrol ist verfügbar für Windows 95, Windows 98 und Windows NT, außerdem für Macintosh. Als Ergänzung gibt es eine Version für eine Installation auf einem Proxy und Speziallösungen für die Proxy-Server von Novell und Microsoft. Für die Einzelplatzversion sind ca. 5MB Speicher auf der Festplatte erforderlich. Besondere Anforderungen an den Browser werden nicht spezifiziert.

Das Programm ist – sowohl in seiner englischen als auch in der neuen deutschen Variante – für ca. 50 DEM zu erwerben. Der genannte Anschaffungspreis beinhaltet eine dreimonatiges Recht zur Aktualisierung der enthaltenen Listen; eine Verlängerung kostet jeweils etwa 30 USD für 6 Monate. Es gibt Sonderkonditionen für Mehrfachlizenzen und Schulen (bisher nur für den amerikanischen Markt). Die Aktualisierung kann automatisch erfolgen oder manuell angestoßen werden; sie dauert je nach Umfang einige Sekunden bis Minuten. Da ein täglicher Aktualisierungsservice angeboten wird, können hierbei einige Online-Kosten entstehen.

Das Programm bietet eine übersichtliche Online-Hilfe-Funktion; zur Einrichtung von Benutzern sind die Erläuterungen allerdings etwas zu knapp.

Der Installationsprozeß ist einfach und das Programm ist nach einem – selbst initiierten – Neustart automatisch aktiv. Allerdings sind die Filtereinstellungen noch zusätzlich zu treffen; in Voreinstellung sind alle Dienste freigegeben. Auch die – im Prinzip mögliche – Einrichtung mehrere Benutzer ist recht umständlich und wird nicht vom Programm vorgeschlagen.

Der Gesamtauftritt hat als Motto die Kontrolle durch einen Sheriff und verwendet daher auch entsprechende graphische Elemente. Ob der dadurch entstehende "amerikanische Touch“ gefällt oder nicht, hängt sehr vom persönlichen Geschmack ab. Abgesehen davon ist der Gesamteindruck positiv: alle Bedienungselemente sind gut zugänglich und intuitiv zu verstehen.

Ob das Programm – durch ein Symbol in der Funktionsleiste – als aktiv zu erkennen ist oder nicht, läßt sich einstellen.

Wird eine zu sperrende Seite aufgerufen, erfolgt eine Meldung "Zugriffssperrung durch CyberPatrol!“ unter Angabe einer Ziffer, aus der der Grund der Sperrung abgleitet werden kann.[214]

Es liegt neben der Originalversion auch eine deutsche Variante vor; die Funktionalität – insbesondere die enthaltenen Listen – beziehen sich jedoch weitestgehend auf den amerikanischen Teil des Internets.

Als Zusatzfunktionen ist eine benutzerabhängige Internetzeitverwaltung integriert (mit Angabe eines generelle Zeitfensters, z.B. zwischen 15 Uhr und 18 Uhr und einer maximalen Zeitdauer, z.B. 10 Stunden pro Woche). Die effektiv "im Internet“ verbrachte Zeit kann im Nachhinein auch über längere Zeiträume überprüft werden.

Weiterhin wird die Sperrung bestimmter lokaler Programme (z.B. Spiele) angeboten. Es ist zudem eine Zusatzfunktion (ChatGuard) enthalten, die die Angabe von persönlichen Daten in Chat-Kanälen verhindern soll.

[214] 1: Sperrung aufgrund der IP-Adresse; 2: Sperrung aufgrund des Verzeichnisses; 3: Sperrung nach SafeSurf; 4: Sperrung nach RSACi; 5: Sperrung nach der IRC-Sperrliste; 8: Sperrung aufgrund der Domäne.

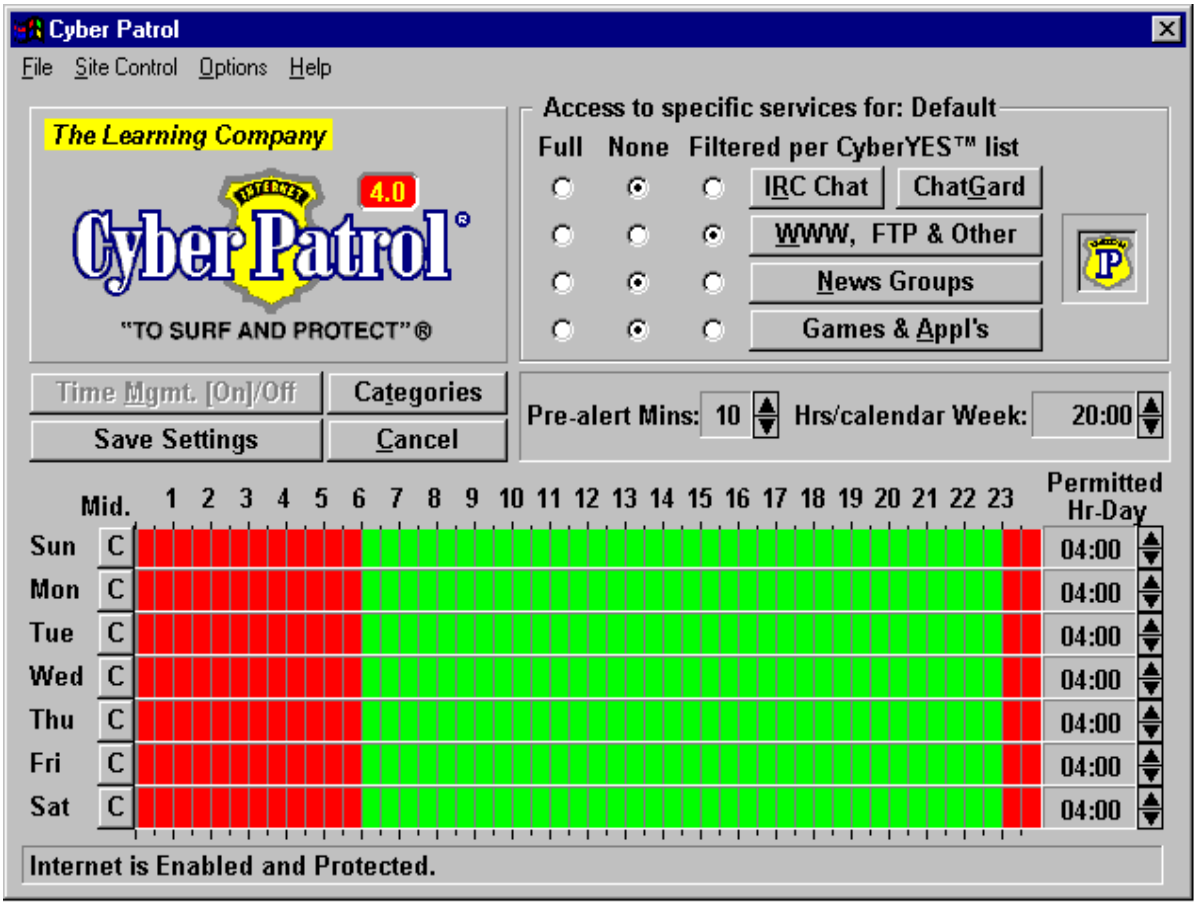


Abb. 5-2: Der Konfigurationsbildschirm von CyberPatrol

Filterfunktionen

Die Funktionsweise von CyberPatrol beruht auf mitgelieferten und täglich aktualisierbaren Listen, die verbotene (CyberNOT-List) und erlaubte (CyberYES-List) Seiten und Server enthalten. Die Listen sind verschlüsselt und daher nicht direkt kontrollierbar; allerdings bietet CyberPatrol auf einer Webseite ein Werkzeug zur Überprüfung der Einträge in der CyberNOT-List an .[215]

Die Bewertungsgrundlagen für die Listen sind veröffentlicht,[216] eine Nachfrage nach den Hintergründen einer einzelnen Bewertung gestaltet sich allerdings recht aufwendig. Immerhin wird über ein Instrument nachgedacht, strittige Bewertungen kontrolliert zu diskutieren.

Nach diesen Kriterien werden Seiten in die folgenden Kategorien eingeordnet, die separat blockiert oder freigegeben werden können:

- Violence/Profanity; Partial Nudity; Full Nudity; Sexual Acts; Gross Depictions; Intolerance; Satanic/Cult; Drugs/Drugs culture; Militant/Extremists; Sex Education; Questionable/Illegal & Gambling; Alcohol & Tobacco.

Es können keine Seiten aus diesen Listen entfernt werden.

Ebenso gibt es eine CyberYES-List[217] mit erlaubten Seiten in den Kategorien:

215 http://www.cyberpatrol.com/cyberNOT/default.htm

216 CyberNOT-List: http://www.cyberpatrol.com/cp_list.htm.

217 CyberYES-List: http://www.cyberpatrol.com/cp_listy.htm

- Games & Toys; Art, Books & Music; Movies & TV; Outdoors & Sports; Pets, Animals & Dinosaurs; Vacations & Travel; Puzzles & Hobbies; School Work; Volunteer & Help; Reference Materials; Schools on the Net; Parents & Teachers

Zusätzlich zu den Listen wird PICS in der Form von RSACi und SafeSurf unterstützt. Eine Integration weiterer PICS-Systeme ist nicht möglich (zumindest keine Erwähnung in der Dokumentation).

Außerdem können eigene Listen von erlaubten und verbotenen Seiten erstellt werden, die immer Vorrang vor den integrierten Listen haben. Damit ist also die individuelle Freigabe oder Sperrung von Seiten unabhängig von Änderungen durch Aktualisierungen u.ä. möglich.

Die Definition mehrere Benutzer ist möglich. Für jeden ist die gesamte Konfiguration individuell einzustellen und abzuspeichern. Der Zugangsschutz erfolgt über ein separates Paßwort. Die Installation ist allerdings etwas mühsam.

Filtereffektivität

Die Suche bei AltaVista ist generell möglich, es werden alle Ergebnisse angezeigt. Bei den Suchergebnissen des Stichwortes "sex“ sind nahezu alle gefundenen Seiten gesperrt. Die Suche nach "safer sex“ ist eher problematisch: Es werden zwar hauptsächlich Seiten mit nicht ganz so explizitem Inhalt gefunden, allerdings können sie – wahrscheinliche gerade deswegen – fast alle angezeigt werden. Es befinden sich z.B. Vertriebsseiten von erotischem Spielzeug darunter, die tatsächlich in der Sprache recht zurückhaltend sind, aber sicher trotzdem nicht dem entsprechen, was sich Eltern als für ihr Kind geeignet vorstellen.

Die Blockierung anderer Dienste war erfolgreich.

Bei der Überprüfung der Testseiten wurde eingestellt, daß die in der CyberNOT-List enthaltenden Seiten gesperrt werden sollen.[218] Damit konnte ein Großteil der englischsprachigen erotisch-pornographischen Seiten und ein Teil der deutschen Angebote gleichen Inhalts erfaßt werden. Außerdem unerreichbar waren die von der BPjS indizierten Angebote von E. Zuendel (Code 2). Ebenfalls unzugänglich, da in der CyberNOT-List enthalten, sind die Seiten von *Peacefire* (vgl. Initiativenübersicht).

Insgesamt ist die subjektive Plausibilität der Filterung deutlich niedriger als die bei der automatisierten Filterung von WebChaperone. Ähnliche Seiten können durchaus unterschiedliche Ergebnisse erzeugen, wenn eine in der Liste enthalten ist, die andere nicht.

Die PICS-Filterung erfolgt zuverlässig.

Unterschiedliche Schutzlevel haben kaum Einfluß.

Manipulationssicherheit

Deinstallation ist nur mit Paßwort möglich. Löschen dieses Programmes führt – wie bei allen anderen auch – zu deutlicher Verwirrung der Netzfunktionen; es ist aber durchaus möglich, dies bei entsprechenden Fertigkeiten manuell zu korrigieren.

Auch ist der automatische Start beim Hochfahren zu verhindern: Dieser automatische Start erfolgt durch einen Eintrag in der Datei win.ini. Diese ist manuell zu ändern und die entsprechende Zeile kann gelöscht werden. Dieser Vorgang allein verhindert die Filterung noch nicht; nach einem Neustart taucht der Befehl wieder auf und garantiert weiterhin den Schutz. Setzt man allerdings zusätzlich das Attribut "read only“ für eben diese Datei, entfällt der Start von CyberPatrol beim Rechnerstart und damit auch jede Filterung.

---

218 Bei der Verwendung der CyberYES-List von erlaubten Seiten ist die Sicherheit der Filterung sehr hoch. Allerdings sind in dieser Konstellation praktisch alle deutschen Seiten (egal welchen Inhalts) nicht erreichbar; damit wird das Programm in dieser Einstellung für den deutschen Raum praktisch unbrauchbar, wenn nicht eine große Anzahl von Seiten manuell hinzugefügt wird.

Deutsche Funktionalität

In deutscher Fassung liegt sowohl die Stand-Alone-Version vor als auch das auf CompuServe basierende Produkt.[219] Die deutsche Version unterscheidet sich im Aussehen nur durch eine z.T. wörtliche Übersetzung von der englischen.

Nach Angaben des Herstellers werden die CyberNOT- und die CyberYES-Liste nicht verändert (daher erfolgt die Aktualisierung auf dem gleichen Weg wie bei der englischen Variante); in ihr sind zwar auch deutsche Seiten enthalten, der Schwerpunkt liegt dort jedoch nicht. Der Hersteller teilte uns mit, daß die Liste von bei Internet Relay Chat (IRC) zu sperrenden Wörtern (die auch auf Webseiten angewendet werden kann) für den deutschen Sprachraum angepaßt wurde; dies gilt aber nicht für die Stand-Alone-Version, sondern nur für die in CompuServe integrierte Fassung.

Insofern ermöglicht das Programm durch seine deutsche Oberfläche zwar eine einfachere Bedienung; der Forderung nach an den deutschen Sprach- und Kulturraum angepaßten Filterkriterien kann es aber nicht genügen.

5.3.3.3 CompuServe

Allgemeines

CompuServe bietet integrierte Schutz- und Filterfunktionen unter dem Stichwort "Parental Controls“. Dabei wird in zwei Rubriken unterschieden:

Zum einen können die Internetdienste News (nntp), Filetransfer (ftp) und Telnet innerhalb des CompuServe Information Service (CIS) gesperrt oder beschränkt werden und Filterregelungen auf die CIS-Inhalte angewendet werden.

Zum anderen können auch Webinhalte (http) gefiltert werden; hierfür wird eine spezielle Version von CyberPatrol verwendet.

Die Filterfunktionen innerhalb von CompuServe können betriebssystemunabhängig, die Internetfilterfunktionen auf Windows-Betriebssystemen genutzt werden. Zusätzliche Kosten – neben der CompuServe-Gebühr und eventuellen Online-Kosten für Listen-Updates – entstehen nicht.

CIS-Filterung

Es ist eine vollständige Sperrung der genannten Dienste oder eine Einschränkung möglich. Die Einschränkung erfolgt nach den Regeln von CyberPatrol – angegeben ist eine relativ alte Version der Bewertungskriterien, die sich von der aktuellen, nur in Englisch vorliegenden allerdings kaum unterscheidet und gut übersetzt ist. Außer der Aktivierung bzw. Deaktivierung sind hier keine Einstellungen möglich; der ganze Konfigurationsprozeß wirkt etwas "angestaubt“, ist aber gut dokumentiert und einfach nachvollziehbar.

Es ist einstellbar, ob die Aktivierung nur für die aktuelle Sitzung oder für alle neuen Anmeldungen gelten soll; diese Angaben sind durch ein Paßwort geschützt.

Zugangssperrung auf CIS-Inhalte für Erwachsene erfolgt zuverlässig; alle Angebote, die in diese Kategorie fallen sind unter dem Stichwort "go AOCL“ aufgelistet; dort werden auch entsprechende Hinweise auf den erforderlichen Jugendschutz gegeben. Die Meldungen erfolgen z.T. in Englisch[220]. Die wesentlichen Dinge sind jedoch verständlich in Deutsch dokumentiert.

---

219 Die Numerierung der Versionen ist für beide Produktlinien nicht konsistent.

220 Diese Sprachmischung findet sich auch in den sonstigen Angeboten von CompuServe.

Internet

Zur Internetfilterung kann online eine – speziell an CompuServe angepaßte – Version von CyberPatrol geladen werden. Sie beinhaltet ein einjähriges Recht zum Bezug der aktualisierten Listen und ist kostenlos. Direkt nach der Installation ist eine Online-Registrierung erforderlich.

Die Installationsanleitungen haben ebenfalls ein altmodisches Erscheinungsbild, führen aber klar und einfach durch den Prozeß.

Das Auftreten des Programms ist außer einer anders lautenden Versionsnummer und der Einblendung CompuServe im Titel identisch mit der Version 4.0 des Stand-Alone-Produktes CyberPatrol. Die verwendete Sprache ist durchgängig Deutsch.

Motivation

Der von CompuServe angebotenen Jugendschutz unterscheidet sich in der Funktionalität wenig von den Stand-Alone-Produkten. Durch die Integration in den Internetzugang ist jedoch ein einfacherer Zugriff auf den Jugendschutz betreffende Informationen und eine einfachere Installation möglich. Die Hemmschwelle vor der Verwendung von Filterprogrammen – im Normalfall aufgebaut durch Anschaffungskosten und Installationsaufwand – wird damit erheblich gesenkt.

Konkret erfolgen Hinweise an verschiedenen Stellen:

- während der Installation von CompuServe;
- bei Zugriff auf Inhalte für Erwachsene – sowohl bei direktem Aufruf als auch bei Zugang über entsprechende Listen;
- unter dem Stichwort "go Internet-Zugriffskontrolle“;
- durch verschiedene Suchfunktionen.

Der erzeugte Gesamteindruck stellt die Filterwerkzeuge als gute Hilfsmittel dar, um das Surfen durch Kinder "sicher“ zu machen; es wird aber gleichzeitig auf die Unzulänglichkeiten hingewiesen und auf die – auch bei Einsatz dieses Programmes weiterhin bestehende – Verantwortung der Eltern aufmerksam gemacht.

Alles in allem ist eine solche Integration aus Gründen der Motivation sehr sinnvoll. Es kann gezielt Information verteilt werden; und auch die technische Installation wird erheblich erleichtert. Andererseits fallen verschiedene Daten des Endbenutzers beim ISP an, die das Problem des Datenschutzes aufwerfen. Außerdem ist in einer solchen Verbindung noch stärker auf eine zu garantierende Unabhängigkeit und Transparenz des Bewertungsvorgangs zu achten.

Welches oder welche Verfahren letztlich integriert werden, spielt für diese Fragen keine Rolle. Selbstverständlich stellen sich die Funktionalitätsprobleme und -mängel hier wie bei den Stand-Alone-Produkten gleichermaßen dar. [221]

Es wäre denkbar, entsprechende Einstellungen von vornherein in die Gesamtkonfiguration eines jeden Internetzugang zu integrieren und damit einer weiten Verbreitung solcher Systeme Vorschub zu leisten.

---

221 Die Angebote von CIS bilden hier eine Ausnahme: Da alle Angebote von CompuServe selbst erzeugt werden, ist eine Kategorisierung und die darauf aufbauende Filterung problemlos und sicher möglich. Der Anteil des CIS-Angebots am Gesamtumfang der über den Internetzugang von CompuServe zu erhaltenden Informationen ist jedoch gering.

5.3.4 Zusammenfassung

Die Bedienbarkeit und die Hilfefunktionen sind bei allen drei Programmen gut. Die Konfigurationen sind ebenfalls zumeist gut durchzuführen. Die Benutzereinrichtung unterscheidet sich im Konzept: Einmal wird die Einrichtung während der Installation abgefragt – mit dem Vorteil einer intuitiven Vorgehensweise, aber dem Nachteil einer etwas längeren Installationsphase, im anderen Fall ist eine Voreinstellung enthalten und weitere Benutzer können später definiert werden. Die nachträgliche Einrichtung ist allerdings nicht intuitiv.

Die Filterung wird bei den getesteten Produkten entweder aufgrund einer automatisierten Bewertung oder aufgrund von Listen durchgeführt, jeweils unterstützt von individuellen Listen und PICS-Ratings. Dabei ist keines der Programme in der Lage, vollständig korrekt zu filtern.

Der automatisierte Bewertungsprozeß macht einen plausiblen Eindruck, läßt aber genauso wie die Listenbewertung Seiten unangebracht durch. Generell funktioniert die Filterung überhaupt nur im erotisch-pornographischen Bereich zufriedenstellend, alle anderen Inhalte werden nicht ausreichend abgedeckt. Auch die Mehrsprachigkeit der Filterungen ist unzureichend.

Nur in einem Teilaspekt erfolgt eine zuverlässige Filterung[222]: Sind die Seiten PICS-bewertet, können alle Programme eine zuverlässige Einordnung in das Filterprofil vornehmen. Außerdem besteht zumindest in einem Programm die Möglichkeit, nur explizit von der Administration freigegebene Seiten erreichbar zu machen. Letzeres bedeutet generell eine große Einschränkung; die (PICS-)Einordnung durch Anbieter mit gleichzeitiger Auswahl der Inhalte durch die Nutzer könnte bei genügender Verbreitung eines solchen oder ähnlichen Bewertungssystems ein gangbarer Weg sein.

Eine nach Alter abgestufte Filterung scheint eher schwierig zu realisieren zu sein; zumindest konnte sie bei den Tests nicht festgestellt werden.

Die Transparenz und insbesondere die Überprüfbarkeit der Bewertungen ist in allen getesteten Fällen nur unzureichend gelöst. Weder die nicht im Klartext vorliegenden Listen noch die nur grobe Beschreibung des automatisierten Verfahrens lassen ein Nachvollziehen des Bewertungsvorgangs im Detail zu. Korrekturen sind im Fall des automatischen Verfahrens gar nicht und im Falle der Listenverwaltung nur über einen langwierigen Vorgang möglich. Auch hier hat das PICS-Verfahren prinzipielle Vorteile, sofern eine geeignete Infrastruktur unterlegt ist.

Ein weiteres wesentliches Problem ist die mangelnde Sicherheit vor Manipulationen. Beide Stand-Alone-Programme können sehr einfach deaktiviert werden.[223] Selbst bei Verwendung einer sicheren Einbindung ist immer ein Löschen der Programmdateien möglich; dies führt jedoch im allgemeinen zu einem Zusammenbruch der Netzverbindung und damit nicht zum gewünschten Effekt. Einzig die interne CompuServe-Sicherung läßt sich nicht ohne Paßwort deaktivieren; sie deckt aber nur einen sehr kleinen Bereich ab.

Fazit daraus ist, daß unbedingt eine Integration in Browser oder Netzzugangssoftware derart anzustreben ist, daß keine separaten Filterkomponenten identifizierbar sind. Dies kann z.B. durch eine Filterkomponente im Browser geschehen (bisher bieten die meistverbreiteten Programme lediglich eine PICS-Unterstützung an)[224] oder in der Verwendung einer Filtersoftware auf dem verwendeten Internet-Server.

---

222 Auch die CyberYES-List bietet aus individueller Sicht keine absolute Sicherheit, da ihr Inhalt nicht der persönlichen Kontrolle unterliegt.

223 Prinzipiell ist ein besseres Verstecken im System möglich; CyberSnoop verwendet ein anderes Verfahren, daß im Rahmen des Tests nicht gebrochen werden konnte.

224 In diesem Falle sind allerdings Maßnahmen gegen die Installation eines anderen Browser ohne diese Funktionalität zu treffen.

Damit liefert keines der Programme einen ausreichenden Schutz. Für eine Weiterentwicklung müssen einerseits

- die Mehrsprachigkeit verbessert,
- die Kriterien besser veröffentlicht und
- die Manipulationssicherheit erhöht werden.

Andererseits ist eine zuverlässige Filterung mit den in den Produkten integrierten Verfahren nur provisorisch zu realisieren. So wäre die Schaffung einer verbreiteten Bewertungsinfrastruktur in der Art von PICS ein Weg zu einer umfassenderen Lösung. In diesem Falle könnte jede der getesteten Anwendungen verwendet werden, da sie alle das PICS-System unterstützen.

5.4 Realitätsnahe Praxiserprobung

Nach der technischen Evaluation der Produkte sollen sie auch in ihrer praktischen Nutzbarkeit untersucht werden. Das vorliegende Kapitel unterzieht einerseits vorhandene Filtertechnologie einer Bewertung nach den Kriterien "Akzeptanz“ und "Bedienbarkeit“ und analysiert andererseits das soziotechnische Umfeld, in dem Filtertechnologie eingesetzt wird oder eingesetzt werden könnte. Neben einer Bestandsaufnahme sollen mögliche Sachverhalte, die die Eignung von Filtertechnologie zur Umsetzung von Anforderungen des Jugendschutzes beeinflussen, untersucht und bewertet werden. Die technische Unterstützung des Jugendschutzes wird somit unter Nutzeraspekten und unter soziotechnischen Aspekten beleuchtet. Von dieser Analyse und den Tests werden Empfehlungen abgeleitet. Während dabei die qualitativen Interviews die Wahrnehmung von Jugendschutz und Filtertechnologie im Internet durch Nutzer in der Breite untersuchen, unterzieht der Nutzertest drei exemplarische Filterprogramme einer detaillierten Prüfung im konkreten Nutzungskontext.

5.4.1 Qualitative Interviews

Ziel der qualitativen Interviews war es, die subjektive Bewertung der Funktionalität und Tauglichkeit von Filtertechnologien zu erheben sowie deren Akzeptanz zu erfragen. Darüber hinaus wurden Einsatzszenarien für Filtertechnologie in ihren soziotechnischen Aspekten empirisch erhoben. Das Umfeld zu kennen, in dem Filtertechnologie eingesetzt wird, ermöglicht es, förderliche und hemmende Kontexteigenschaften (sowohl sozialer, technischer als auch psychologischer Art) zu identifizieren.

5.4.1.1 Methode

Als primäre Nutzer wurden zwei Lehrer, zwei Eltern und drei Schüler den qualitativen Interviews unterzogen. Darüber hinaus wurden ein Universitätsprofessor (Informatik, Schwerpunkt Internet) sowie eine Sozialpädagogin (Schwerpunkt Jugendarbeit) als Sachverständige befragt. Vier Angehörige einer Bank und einer Zeitung, die beide ein öffentlich zugängliches Internetangebot bereitstellen, nahmen ebenfalls an Interviews teil. Die Befragungen dauerten etwa eine Stunde. Dabei wurden die Teilnehmer i. d. R. einzeln vom Interviewer nach einem Interviewleitfaden befragt.

Beide Lehrer waren die zuständigen "Computerlehrer“ von Gymnasien. Die Eltern waren für minderjährige Kinder verantwortlich und hatten einen Internetanschluß zu Hause, der den Kindern zugänglich war. Die Schüler besuchten sämtlich Gymnasien. Es handelte sich um Jugendliche im Alter zwischen 16 und 17 Jahren.

Der Universitätsprofessor war durch seine Forschungstätigkeit auf dem Gebiet "Internet“ und durch seine profunde Kenntnis der Filtertechnologie als Fachmann ausgewiesen. Die Sozialpädagogin wurde als Expertin für Jugendschutz hinzugezogen.

Die vier Angehörige der Bank bzw. der Zeitung arbeiteten in ihrer Stellung als Angestellte vor Ort, als Führungskräfte (Abteilungsleiter) sowie als Geschäftsführer aus unterschiedlichen Perspektiven am Problem der Jugendgefährdung durch das Internet, genauer durch einen öffentlich zugänglichen WWW-Anschluß.

Nach der Beschreibung der empirisch vorgefundenen Installationen im soziotechnischen Kontext werden die Ergebnisse der Interviews in zwei Hauptthesen dargestellt und eine Sammlung von Anforderungen an Filtertechnologie dokumentiert.

5.4.1.2 Vorgefundene Installationen

Um ein Bild von den vor Ort angetroffenen Installationen zu geben, werden im folgenden drei Nutzungsszenarien kurz dargestellt.

Halböffentlicher Zugang

In den beiden untersuchten Schulen gab es einen für Schüler zugänglichen Internetanschluß in einem Computerlabor. Dieses Labor bestand jeweils aus acht bis neun PCs, die über einen Server an das Internet angeschlossen waren. Durch den Server wurde der Internetzugang auch gesteuert. Sämtliche WWW-Seiten, auf die die Schüler zugriffen, wurden in einem Logfile verzeichnet. Die zuständigen Computerlehrer machten stichprobenartige Kontrollen der abgerufenen Seiten. Dabei wurde sowohl nach eindeutigen Namen der URLs gesucht als auch Zufallsstichproben gezogen. Die Schüler wußten im Prinzip, daß so ihr Websurfen (zumindest im nachhinein) kontrolliert wurde. Sie wußten jedoch nicht im Detail, wie dies vonstatten ging. Diese Kontrollmöglichkeit wurde von den Schülern als bedeutsam erlebt und in ihrem Surfverhalten berücksichtigt. Die Computerlehrer andererseits waren sich bewußt, daß sie mit der manuellen Stichproben des Webzugriffs keine echte Kontrolle leisten können. So entzog sich z.B. das Chatten völlig ihrer Kontrolle, obwohl dieses von den Schülern rege in Anspruch genommen wurde. Meist waren die Schüler bei ihrer Nutzung des Internetangebots in den Computerlabors in Gruppen anwesend.

Öffentlicher Zugang

Der öffentliche Internetzugang in der Bank und in der Zeitungsfiliale bestand jeweils in einem Internetterminal. Während bei einer Lokation ein handelsübliches Inhaltsfilterprogramm (CyberPatrol) installiert war, fehlte bei der anderen Lokation jegliche technische Kontrolle. Diese hatte die Installation von Filtertechnologie jedoch in der Planung und die Realisierung stand bald bevor. Bei beiden Lokationen waren die Internetterminals in öffentlich zugänglichen und gut einsehbaren Räumlichkeiten mit zwar tageszeitlich schwankendem, aber meist hohem Publikumsverkehr. Auch waren meistens Angestellte vor Ort. Nutzer der Internetterminals mußten also damit rechnen, in ihrem Internetverhalten beobachtet zu werden. Die Angestellten hatten z.B. auf jugendliche Internetnutzer ein besonderes Auge, ohne jedoch lückenlose Kontrolle auch nur annähernd leisten zu können.

Bei der Bank handelte es sich um eine Lokation mit bewußt forciertem Automateneinsatz. Um diesen kundengerecht zu präsentieren, unterstützte eine speziell geschulte Servicemannschaft die Kunden im Umgang mit den Geräten und erledigt auch kleinere Bankgeschäfte "von Hand“. Durch eine helle und von außen gut einsehbare Architektur war hier ein Umfeld geschaffen worden, das – zunächst nur für die ansprechende Präsentation und angstfreie Bedienung der anderen Automaten gestaltet – auch für die soziale Kontrolle des Internetterminals optimal ist. Aber auch hier gibt es Stunden mit wenig Publikumsverkehr, in dem Kunden sich allein und ohne Servicepersonal vor dem Internetterminal befinden.

Privater Zugang

Der private Zugang zum Internet bestand aus einem PC zu Hause, der über Telefon an das Internet anzuschließen war. Bei den befragten Eltern war keine Filtertechnologie installiert. Der Zugang zum PC wurde ähnlich gehandhabt wie der Zugang zum Fernseher. Es gab dort

offensichtlich starke, sozial bedingte Unterschiede im Internetzugang. In Erzählungen auch von anderen Internetzugängen von zu Hause wurde von Regelungen wie "völlig frei“ und "gar kein Zugang erlaubt“ berichtet.

Obwohl über die Möglichkeit, die Kinder und Jugendlichen z.B. die Kosten der Internetnutzung tragen zu lassen, in dieser Befragung keine empirischen Informationen erhoben werden konnten, läßt sich aus psychologischer Sicht vermuten, daß dies ein sinnvolles Kontrollinstrument sein kann. Es käme dabei weniger auf eine effektive Kostendeckung an. Wichtiger wäre vielmehr die soziale Kontrolle an, die damit verbunden ist, daß sich Eltern und Kinder auf ein gemeinsames Vorgehen einigen und die Eltern durch die Abrechnung einen Überblick über das Internetsurfens behalten. Die Kinder können im Gegenzug die Erfahrung machen, daß sich die Eltern um die Internetnutzung kümmern. Denn als problematisch ist vor allem der unbeaufsichtigt-vernachlässigte Internetkonsum anzusehen.

5.4.1.3 Öffentlich versus privat: Unterschiedliche Bewertung der Gefährdung

Alle Befragten äußerten sich dahingehend, daß sie sich der Jugendschutzproblematik bewußt seien. Sie nahmen die prinzipiellen Gefahren wahr und beschrieben sie technisch korrekt. Dabei standen für die Nutzer die Gefahren durch jugendgefährdende Inhalte über das WWW im Vordergrund. Inhaltlich wurde meist nur die Pornographiethematik für relevant erachtet. Politisch-extremistische und gewaltbezogene Inhalte wurden als randständig bewertet. Auch das Funktionsprinzip von Filtertechnologie war den Befragten ausreichend bekannt.

Die folgende Beschreibung stellt eine Kompilation aus den Einzelaussagen dar. Sie kann als "Durchschnittsauffassung“ der Befragten interpretiert werden. Die Nutzer stellten sich das Internet als ein weltumspannendes Netz von Datenleitungen vor, an das viele Computer angeschlossen seien. Diese Netz sei irgendwie chaotisch und es gebe keine Kontrolle darüber. Weltweit könne eine unkontrollierbare Menge von Personen und Organisationen Informationen in dieses Netz "einspeisen“. Daß darunter auch jugendgefährdende Inhalte sein können, war den Befragen bewußt. Die Filtertechnologie wurde als ein Mechanismus zwischen der Computerleitung und dem eigenen Computer verstanden, der als "Türsteher“ zum eigenen Computer fungiert. Der Mehrzahl der Befragten war die Filterung nach sexuell anstößigen Wörtern bekannt. Wie der Filtermechanismus im Einzelnen funktioniert und welche verschiedenen Kriterien und zu filternden Eigenschaftsdimensionen es gibt, war nur wenigen Nutzern bekannt.

In bezug auf eine Bewertung der tatsächlichen Jugendgefährdung unterschieden sich zwei Gruppen. Während Lehrer, Eltern und Schüler die Gefährdung eher gering einschätzten, äußerten sich die Experten und professionellen Anbieter eines öffentlichen Internetzugangs besorgt. Es lassen sich zwei Nutzungsszenarien voneinander abgrenzen: Während der öffentliche Internetzugang als gefährlich wahrgenommen wurde, wurde der halböffentliche, d.h. der Internetzugang in der Schule, und der private Zugang als ausreichend sicher empfunden. Im Folgenden sollen diese beiden Szenarien einzeln charakterisiert werden

Der öffentliche Zugang

Die zum öffentlichen Zugang befragten Personen hatten entweder schon Filtertechnologie installiert oder waren kurz davor. Sie hatten die Entscheidung über die zu treffenden Maßnahmen nach sachlichen Gesichtspunkten organisiert und fachkundigen Personen übertragen. Die Tatsache, daß die Befragten die Jugendgefährdung (u.a. wegen möglicher rechtlicher oder öffentlichkeitswirksamer negativer Konsequenzen) professionell angehen, spricht für einen rationalen Umgang mit der Problematik. Es gab zwischen den Befragten jedoch große Unterschiede, was die subjektiv empfundene Tauglichkeit von Filtertechnologie angeht. Während eine Organisation das Jugendschutzproblem durch die Installation eines Filterprogrammes als erledigt ansah, hegte die andere Organisation Zweifel an der alleinigen Tauglichkeit. Diese versuchte deshalb, die Problematik durch soziale Kontrolle einerseits und anhaltende Aufmerksamkeit des Managements andererseits in den Griff zu bekommen.

Der halböffentliche und private Zugang

Die Lehrer, Eltern und Schüler, die sich auf ein halböffentliches Angebot in den Schulen oder ein privates Angebot zu Hause bezogen, bewerteten die tatsächliche Jugendgefährdung als gering. Sie stellten sich unter Jugendgefährdung meist sexuell-pornographische Inhalte vor, die jedoch über das jugendgefährdende Potential von Männermagazinen oder entsprechenden Filmen oder Berichten im unverschlüsselten Fernsehen nicht hinausgingen. Dieser Vergleich zu am Kiosk oder im Fernsehen dargebotenen Inhalten wurde als entlastend für die eigene Verantwortung seitens der Lehrer und Eltern oder die eigene Gefährdung seitens der Schüler angeführt. Auch wurde auf Kontrolle mit sozialen Mechanismen verwiesen, die im halböffentlichen oder privaten Raum üblich sind, vgl. Abschnitt 5.4.1.4.

Die Schüler hatte offensichtlich kein Bewußtsein über die Gefährdung. Sie nahmen an, daß sie zwar erotisches oder pornographisches Material finden konnten. Daß dieses Material ihnen möglicherweise schaden kann, war zumindest den befragten Schülern nicht bewußt. Ohne die Befragungsergebnisse überstrapazieren zu wollen, kann man davon ausgehen, daß dieses Bewußtsein bei Kindern und Jugendlichen zumindest unterentwickelt ist

Gesamtbewertung

Die beiden Experten sahen unabhängig vom Nutzungskontext ein großes Gefährdungspotential. Dieses müsse mit Nachdruck angegangen werden. Die Filtertechnologie wurde dabei vom Informatikprofessor sehr skeptisch bewertet. Die Sozialpädagogin betonte – ungeachtet der technischen Tauglichkeit von Filtertechnologie – eine Abhängigkeit der tatsächlichen Tauglichkeit von ihrer Einbettung in der sozialen Kontext.

Aus psychologischer Sicht fällt auf, daß diejenigen Personengruppen, die Filtertechnologie nicht eingesetzt hatten, das Gefährdungspotential als gering einschätzen, während die Anwender von Schutzprogrammen die Gefahr z.T. als enorm bezeichneten. Beide Einschätzungen sind – ganz unabhängig von der objektiven Gefährdung – psychologisch plausibel. Anwender von Filterprogrammen müssen ihre "Kosten“ damit rechtfertigen, daß damit eine reale Gefahr abgewendet wird. Verantwortliche, die auf den Einsatz von Kontrollsystemen verzichten, können dies nur dann tun, wenn sie behaupten, es sei keine Gefahr virulent. Vor diesem Hintergrund muß der Versuch einer objektiven Bewertung der Jugendgefährdung durch Inhalte des Internet vorsichtig unternommen werden. Die Befragung der Nutzer allein reicht dazu nicht aus. Es müssen auch rechtliche und soziale Bewertungsmethoden verwendet werden, die in anderen Arbeitspaketen der vorliegenden Studie zur Anwendung kommen.

5.4.1.4 Filtertechnologie: Technisches Hilfsmittel sozialer Kontrolle

Interessant ist aus technischer und rechtlicher Perspektive der Sachverhalt, daß sämtliche Befragten das Jugendschutzproblem nicht allein in ihren technischen oder rechtlichen Aspekten sahen, sondern von ihrem lebensweltlichen Standpunkt häufig soziale Gesichtspunkte thematisierten. Um der lebensweltlichen Auffassung der Betroffenen gerecht zu werden, sollte man Jugendschutz und Filtertechnologie im Internet als soziotechnische Problematik verstehen. Darin werden dann technische und soziale Aspekte nicht getrennt, sondern systemisch verknüpft formuliert. Auch rechtliche Aspekte etc. werden in dieses System eingeflochten.

Von dieser Annahme ausgehend ist auch eine durchgängige Beobachtung zu nennen: Jugendschutz wird nach Auffassung der Befragten nicht vor allem durch technische, sondern durch soziale Kontrolle zu erreichen versucht. Exemplarisch läßt sich die Aussage eines Lehrers nennen, der jegliche technische Filterung dem verfolgten pädagogischen Konzept untergeordnet wissen wollte. Auch die Schüler sahen prinzipiell keinen Unterschied zwischen dem Verhalten in der Klasse, auf dem Schulhof oder privat mit Freunden zum Verhalten in den Computerlabors. D.h. für sie greifen in allen Situationen vornehmlich die sozialen Kontrollmechanismen. Die technischen Kontrollmöglichkeiten ordnen sich auch für die

Schüler diesen sozialen Regeln unter. Wenn Eltern den Zugang ihrer Kinder zum heimischen PC mit Internetanschluß so regeln wie den Fernsehzugang oder wenn Organisationen in ihren Lokationen das Internetsurfen wie Zeitschriftenlesen behandeln (und kontrollieren), dann greifen auch dort soziale Kontrollmechanismen. Diese bestehen hauptsächlich darin, das für unangemessen angesehene Verhalten durch sozialen Druck zu sanktionieren. Wesentliche Bestimmgröße dieser so aufgefaßten Kontrolle sind die Normen, die Wahrnehmung durch andere Personen sowie die Möglichkeit zur Einflußnahme.

Normen

Die Normen für das, was als angemessen und unangemessen angesehen wird, können sich zwar von den objektiven Normen (d.h. z.B. die rechtlichen Rahmenbedingungen, aber auch Regelungen der freiwilligen Selbstkontrolle) zur Identifizierung jugendgefährdender Inhalte unterscheiden. Die Befragungen zeigten in der Praxis aber keine Unterscheidung zwischen dem, was als unangemessen und dem, was als jugendgefährdend empfunden wird. In Frage stehen vielmehr interindividuelle Unterschiede und solche zwischen Gruppen. Es besteht die Möglichkeit, daß sich Subgruppen mit deutlich abgesenkten Standards bilden. Innerhalb dieser Gruppen ist somit ein vom Gesetzgeber verlangter Schutz der Jugend nicht mehr unbedingt gewährleistet.[225]

Bei den befragten Personen ließen sich zwar im wesentlichen ähnliche Normen feststellen. Extrapoliert man jedoch die Differenzen, die sich schon innerhalb der befragten Stichprobe fanden, so sind die aus der Literatur berichteten Unterschiede durchaus plausibel. Versucht man, die unterschiedlichen Normen zu bewerten, so sind die Randbedingungen des verfassungsmäßig garantierten Rechtes der freien Meinungsäußerung und des Rechts auf Information zu beachten. Sie führten dazu, daß die Forderung nach "freiwilliger Selbstkontrolle“, daß also der Einsatz und die Konfiguration benutzerseitig zu kontrollieren sein müssen, aufgestellt wurden. Vor diesem Hintergrund scheiden Bemühungen zur Vereinheitlichung der Normen aus. Die Methode der sozialen Kontrolle erweist sich hier einer technischen Kontrolle nicht als unterlegen. Für die Filtertechnologie kann gefolgert werden, daß sie die Nutzer darin unterstützen soll, auch unterschiedliche, benutzerseitig auszuwählende Normen durchzusetzen.

Wahrnehmung durch andere Personen

Kritisch für die verhaltensleitende Funktion von Normen ist es, daß das in Frage stehende Verhalten bzw. die zu bewertenden Inhalte durch andere Personen wahrgenommen werden. Primär wichtig für das Funktionieren sozialer Kontrolle ist, von anderen Menschen gesehen zu werden. In bezug auf das Internet ist hier mit prinzipiellen Einschränkungen zu rechnen, da ein Bildschirm auf den Nutzer ausgerichtet ist und nicht auf andere Beobachter. Auch erzählten die Schüler, daß sich Inhalte auf einem Bildschirm (durch Fensterverkleinerung) schnell verstecken lassen. Die soziale Kontrolle kommt hier an Grenzen, so daß technische Mechanismen dies auffangen müssen.

Möglichkeit zur Einflußnahme

Oben wurde schon vom unterschiedlichen Umgang je nach dem Ausmaß an Öffentlichkeit berichtet. Paradoxerweise wurde ein öffentlicher Internetzugang von den Beteiligten in dieser Hinsicht als unbeobachteter empfunden als ein halböffentlicher oder privater. Dies hängt damit zusammen, daß im halböffentlichen und privaten Raum die Möglichkeiten zur Durchsetzung von Normen größer sind. Personen, die sich untereinander bekannt sind, können sich gegenseitig in ihrem Verhalten beeinflussen. Daraus läßt sich für öffentliche

225 Weitere Hinweise könnte man sich vom Umgang mit dem Medium Fernsehen erwarten, bei dem ja nach Bildung und Schicht z.T. deutliche Unterschiede zu beobachten sind. So hat sich zum Beispiel gezeigt, daß in sozial schwächeren Familien ein erhöhter Fernsehkonsum (auch von jugendgefährdenden Filmen) zu beobachten ist.

Internetzugänge eine geringere soziale Kontrolle ableiten, so daß dort ein höheres Maß an technischer Kontrolle mit Filtertechnologien nötig wäre.

Aus Nutzersicht ist also die soziale Kontrolle die primär anzuwendende Methode, um Jugendschutz zu erreichen. Technische Hilfen (wie Protokollierung, aber auch Filtertechnologien) werden als unterstützende Hilfen wahrgenommen und angenommen. Aus obigen Überlegungen läßt sich somit ein Bedarf, der über die soziale Kontrolle hinausgeht, ableiten. Nutzer brauchen funktionierende Filtertechnologie, um Jugendschutz umsetzen zu können.

Aus psychologischer Perspektive fällt ein weiteres Detail auf, daß sich nämlich die Urteile je nach Rolle und eigenem Verhalten unterscheiden. Die öffentlichen Anbieter sind es gewohnt, Sachfragen in professioneller Weise funktional und organisatorisch zu handhaben. Da sie Sicherungstechnik einsetzen, können sie es sich "leisten“, das Internet als Jugendgefährdung zu bewerten. Die Lehrer und Eltern dagegen werden üblicherweise nicht mit derartigen technisch-organisatorischen Anforderungen konfrontiert. Sie wenden deshalb die (sozialen) Mechanismen an, die sich zur Lösung vorangegangener Problemen als geeignet erwiesen haben.

Insofern könnte ein einfach zu installierendes, gut verständliches technisches Angebot die Position der Eltern verändern und ihren "Werkzeugkasten“ zur Kontrolle erweitern. Denkbar wäre z.B. die Integration in das Angebot eines Internetserviceproviders oder eine vorgeschriebene Selbstkontrolle, deren Auswertung standardmäßig in jedem Browser integriert ist.

5.4.1.5 Nutzeranforderungen an Filtertechnologie

Filtertechnologie wurde auf Anfrage von allen befragten potentiellen Nutzern als positiv bewertet. Auch die Schüler äußerten den Wunsch, zur Rechtfertigung der ihnen übertragenen Selbstverantwortung durch technische Kontrollmechanismen unterstützt zu werden. Nach den "Kosten“ gefragt, waren alle Befragten auch zu einem finanziellen Engagement bereit. Die in der Befragung geäußerten Meinungen lassen ein substantielles Nutzerbedürfnis und somit ein reelles Nachfragepotential vermuten.

Interessanterweise wurde auf die Frage nach möglichen Einbußen bei der Performance von den Lehrern und den Schülern jedoch keine Zugeständnisse gemacht. Im Zweifelsfall wurde es für wichtiger erachtet, auf "erlaubte“ Inhalte zugreifen zu können als den Zugang auf "verbotene“ Inhalte zu verhindern. Während also das unbeabsichtigte Sperren von "erlaubten“ Seiten ein K.O.-Kriterium für Filtertechnologie zu sein scheint, dürfen nach Ansicht der Lehrer und Schüler schon mal "verbotene“ Seiten den Filter passieren. Dies wird dann nachvollziehbar, wenn man bedenkt, daß die technischen Maßnahmen ja nur als Ergänzung der sozialen Kontrolle verstanden wurde.

Die Äußerung eines anderen Befragten, Filtertechnologie habe nur dann Sinn, wenn sie garantiert alle "verbotenen“ Seiten ausfiltert, steht damit im Widerspruch. Festhalten läßt sich, daß die potentiellen Nutzer z.T. unrealistisch hohe Ansprüche an Filtertechnologien haben. Eine mögliche Lösung wäre, Filterprogramme nur als Ergänzung zu sozialer Kontrolle einzusetzen. Somit verschiebt sich der Fokus von der Bereitstellung guter Filter hin zur deren optimierten Einbindung in den soziotechnischen Kontext.

Über die Tauglichkeit von existierenden Filterprogrammen gefragt, zeigte sich das ganze Spektrum von "Placebo“ bis hin zu "dann kann ich mich drauf verlassen.“ Die Bewertung gründete sich meist nur auf vagen Informationen. Der Kenntnisstand zu konkret existierender Filtertechnologie kann deshalb als eher gering geschätzt werden, auch wenn das Prinzip weitgehend verstanden wird. Hier muß im Sinne einer sinnvollen Umsetzung von Jugendschutz durch Filterung noch Aufklärungsarbeit geleistet werden.

Obige Ausführungen belegen, daß die Nutzerpopulation Filterprogramme als Hilfsmittel ansieht. Aus anderen Untersuchungen im Sicherheitsbereich lassen sich Parallelen ziehen.

Auch dort werden Sicherheitsprogramme lediglich als Hilfsmittel, als Werkzeug angesehen. Sie werden erst dann nachgefragt, wenn entweder die primären Funktionsbedürfnisse vollständig befriedigt sind oder ein Schaden bereits eingetreten ist. Dies hat zur Folge, daß Sicherheitsfunktionalität eher selten als eigenständiges Produkt vermarktet wird, sondern als Teil von größeren Programmpaketen. Sicherheitsfeatures werden auch selten als eigenständiger Vorteil, sondern eher als zum (gehobenen) Standard gehörend verkauft. Für einzelnstehende Filterprogramme lassen sich deshalb Probleme bei der Verbreitung erwarten. Die Einbindung in Provider-Softwarepakete (wie AOL oder T-Online), Web-Browser oder Schulsoftware-Pakete erscheint erfolgversprechender.

Da Sicherheitsfeatures, wie es Filtertechnologie ist, für den Nutzer nur einen Nebennutzen darstellen, werden sie seltener benutzt. Durch die geringe Nutzungsfrequenz stellen sich erhöhte Anforderungen an deren Bedienbarkeit. So muß die Oberfläche intuitiv und ohne Lernaufwand zu bedienen sein. Da sich die Bedienbarkeit als ein wesentliches Kriterium für die Nützlichkeit von Sicherheitsfunktionen erwiesen hat, ist darauf im Rahmen der Praxiserprobung besonderes Augenmerk zu richten (vgl. "Realitätsnahe Praxiserprobung“).

Nimmt man die Nutzeranforderungen ernst, daß Filter nur ein "Werkzeug“ in den Händen der Nutzer ist, so ergibt sich die Forderung, daß Filtertechnologie vom Nutzer flexibel einsetzbar und frei konfigurierbar sein muß. Die unterschiedlichen Normen und Verwendungszwecke und die damit verbundenen unterschiedlichen Nutzergruppen (Kinder, Jugendliche, Erwachsene) machen eine Einflußnahme auf den Filterprozeß durch eigene Positivlisten und Negativlisten etc. nötig. Auch das Format, in dem auf die Sperrung angeforderter Seiten hingewiesen wird, sollte konfigurierbar sein. So äußerte ein Lehrer den Wunsch, aus pädagogischen Gründen auf jegliche Rückmeldung, die zum Umgehen der Sperre einlädt, zu verzichten. Es ist aber auch der gegenteilige Fall denkbar, daß die Anzeige, eine "verbotene“ Seite angefordert zu haben, schon bestrafend wirkt und das entsprechende Verhalten in Zukunft unterlassen wird.

Ein offener Fragekomplex ist der Umgang von Filterprogrammen zur Sicherung unterschiedlichen Zugangsmethoden zum Internet wie WWW, Chatten, E-Mail etc. Die Befragten sahen hauptsächlich nur das WWW als potentiell jugendgefährdend an. Chatten und E-Mail wurden von der überwiegenden Mehrzahl gar nicht in Betracht gezogen.

5.4.2 Nutzertest

Dieser Abschnitt ist eine Fortführung des vorhergehenden Kapitels "Technische Tests der Filtersoftware“. Während bisher die technischen Aspekte der Tauglichkeit von Filtertechnologien untersucht wurden, steht hier die praktische Gebrauchstauglichkeit im Mittelpunkt. Zusammen mit den technischen Untersuchungen soll damit eine Vision eines möglichst wirkungsvollen und zugleich realistischen und von den Nutzern bedienbaren und akzeptierten Filterkonzeptes entwickelt werden.

5.4.2.1 Methode

Im Folgenden wird die Methode des Nutzertests beschrieben. Dabei wird nach der Definition der Fragestellung die Stichprobe der beteiligten Versuchspersonen beschrieben und die verwendete Soft- und Hardware angegeben. Im Anschluß wird der Ablauf der Untersuchung vorgestellt und das Untersuchungsdesign spezifiziert.

Fragestellung

Die Fragestellung der Gebrauchstauglichkeit wurde in die Aspekte "Usability“ (Gebrauchstauglichkeit im engeren Sinne) und "Likeability“ (Akzeptanz) unterteilt. Die Fragestellung der Usability untersuchte, wie gut, d.h. wie zügig, fehlerfrei bzw. fehlertolerant die Nutzer Filterprogramme anwenden können. Es wurden sowohl die aktuelle, objektive Bedienung beobachtet als auch subjektive Komponenten erhoben wie Kritikpunkte und

Verbesserungsvorschläge. Die Usability wurde sowohl einzeln für alle Schritte der Verwendung von Filterprogrammen – von der Installation über die Konfiguration und Nutzung bis zur Deinstallation – untersucht, als auch insgesamt gemessen. Die Likeability, also wie sehr die Nutzer den Umgang mit den Programmen mögen und deren Einsatz akzeptieren, wurde wiederum für die einzelnen Arbeitsschritte und für die gesamthafte Wahrnehmung erhoben. Darüber hinaus wurden zur weiteren Entwicklung einer Vision eines verbesserten Filterkonzeptes auch qualitative Fragen nach geeigneten Filterkategorien sowie nach als tauglich empfundenen Darstellungskonzepten gestellt.

Versuchspersonen

Es nahmen 12 Probanden an der Praxiserprobung teil.

Das Durchschnittsalter der Schülerpopulation lag bei 17 Jahren. Der jüngste Schüler war 16 Jahre, der älteste 18 Jahre alt. Die Erwachsenenstichprobe wies ein Durchschnittsalter von 40 Jahren auf. Der Altersbereich ging von 26 bis 57 Jahren.

Die Schülerpopulation bestand aus fünf Schülern und einer Schülerin. Die Erwachsenenpopulation bestand aus fünf Männern und einer Frau.

Die Erwachsenen waren in Berufen wie (großteils) Lehrer beschäftigt, aber auch Sozialpädagogen, Psychologen sowie in der Finanzbranche beschäftigt.

Die Stichprobe ist durchaus repräsentativ für die Population der Eltern und Schülern, die sich verstärkt mit dem Thema Internet beschäftigen. Sie ist jedoch durch den unterrepräsentativen Anteil von Frauen nicht geeignet, die fernere Zukunft, in der mehr Mädchen und Frauen mit Computern und Internet arbeiten werden, anzusehen. Trotzdem ist die Stichprobe gut geeignet, die gestellten Usability- und Likeabilityfragestellungen des Praxistests zu beantworten.

Verwendete Soft- und Hardware

Es wurden drei Filterprogramme[226] untersucht. Es waren dies:

- WebChaperone V 1.8,
- CyberPatrol V 4.0 sowie
- CyberPatrol für CompuServe, V 3.

Es standen zwei Hardwaresysteme zur Verfügung, ein Desktop-PC und ein Laptop. Beide verwendeten das Betriebssystem Windows 95 und waren über Modem mit dem Internet verbunden. (Es ergaben sich keine Unterschiede durch die verschiedenen Hardwaresysteme, so daß im folgenden darauf nicht mehr eingegangen wird.)

Ablauf

Nacheinander wurden die folgenden vier Arbeitsschritte durchgeführt:

- Installation,
- Konfiguration,
- Nutzung und
- Deinstallation.

Die Probanden waren angehalten, "laut zu denken“, also ihr Verhalten zu kommentieren und ihre Gedanken, Gefühle und Verhaltensintentionen zu äußern. Bei den Arbeitsschritten wurde

226 Eine detaillierte Beschreibung der Programme findet sich im Kapitel "Technische Tests“.

das Verhalten der Probanden und parallel deren Bemerkungen erhoben. Ein anschließender Fragebogen zu den Arbeitsschritten maß die Zufriedenheit mit den einzelnen Schritten und gab dazu Gelegenheit, Anmerkungen zu machen. Anschließend wurde ein produktübergreifender Fragebogen zur subjektiven Nützlichkeit von drei Features vorgelegt. Zwei weitere Fragen zu Filterkategorien und Darstellungsmöglichkeiten wurden in einem qualitativen Interview diskutiert. Die Erhebung von Personendaten bildete den Schluß.

Einleitung: Die kurze Einleitung informierte die Probanden über den Sinn der Studie und gab eine Orientierung über den Ablauf.

Installation: Die Probanden wurden gebeten, das Programm zu installieren. Die Installationspakete befanden sich in einem entsprechenden Verzeichnis auf der Festplatte.

Konfiguration: Die Probanden sollten das Produkt für einen Erwachsenen, für eine achtjährige Lea sowie für einen sechzehnjährigen Michael konfigurieren.

Nutzung: Die Probanden surften im Internet und wählten dabei teils vorgegebene, teils selbst gewählte Internetseiten an. Die Probanden sollten in den verschiedenen Rollen (Erwachsener, Lea, Michael) durchs Internet surfen und dabei die subjektive Tauglichkeit der Filters bewerten. Im Rahmen der Nutzung mußten ggf. die Filter ein- oder umgeschaltet werden. Wurden Seiten gefiltert, so stießen die Probanden auf die je produktspezifische Sperrmeldung. Im Rahmen der Nutzung wurden die Probanden auch explizit befragt, wie sie sich eine mögliche Manipulation der Filterung vorstellen würden.

Deinstallation: Die Probanden sollten das Produkt deinstallieren.

Beim **Fragebogen zum Produkt** bewerteten die Probanden das jeweilige Produkt auf einer fünfstufigen Skala bezüglich der folgenden Aspekte:

- Insgesamt,
- Installation,
- Konfiguration,
- Nutzung: Filterwirkung, Sperrmeldung, Anzeige des Produktes, Nutzung insgesamt,
- Deinstallation,
- Manipulation.

Zu jedem Aspekt konnten die Probanden eigene Anmerkungen notieren. Darüber hinaus wurden die Probanden aufgefordert, weiter zu notieren, was ihnen am besten bzw. am schlechtesten gefallen hat und was dem Produkt noch fehlt bzw. hinzugefügt werden sollte. Auch die nicht erfüllten Erwartungen der Nutzer wurde erhoben.

Feature-Fragebogen: Die Probanden gaben ihre Bewertung folgender Features ab:

- Beschränkung des WWW-Zugangs auf bestimmte Tageszeiten oder eine bestimmte Dauer pro Woche,
- Sperrung der Installation und/oder Nutzung anderer Programme,
- Sperrung der Eingabe von Kreditkartennummern, Adressen und Telefonnummern,

Interviewfrage zu Filterkategorien: Es wurde die Frage diskutiert, welche Filterkategorien für sinnvoll erachtet werden.

Interviewfrage zur Filterdarstellung: Die Probanden sollten im Gespräch darstellen, wie sich das Filterprogramm "darstellen“ solle, also welche Metaphern oder Persönlichkeitskonstrukte als sinnvoll und angenehm bewertet werden.

Untersuchungsdesign

Die Probanden bearbeiteten je nur ein Filterprogramm. Das Hauptinteresse der Auswertung bestand darin, die Stärken und Schwächen der einzelnen Produkte und die daraus resultierenden Empfehlungen darzustellen. Darüber hinaus wurde auch ein Vergleich zwischen den Produkte bezüglich Ihrer Gebrauchstauglichkeit gezogen. Die Antworten zu den produktübergreifenden Fragestellungen wurden über alle Probanden aggregiert.

5.4.2.2 Produktübergreifende Usability

Bei allen untersuchten Filterprogrammen traten erheblich technische Probleme bei der Installation und/oder Nutzung auf. Diese Probleme führen dazu, daß keines der existierenden Programme in ihrer jetzigen Form für durchschnittliche Nutzer empfohlen werden kann. Insofern ergibt sich hier derselbe Eindruck wie in der Untersuchung der rein technischen Aspekte. Die folgende Untersuchung sieht explizit von diesen Problemen ab und bewertet die Programme so, als ob sie keine technischen Mängel hätten.

Auch war die englische Sprache ein erhebliches Problem. Für die korrekte und akzeptierte Anwendung von Filterprogrammen ist für die Masse der deutschsprachigen Nutzer die durchgängige Verwendung der deutschen Sprache unabdingbar. Die Übersetzung des Programmes CyberPatrol für CompuServe ist deshalb nicht ausreichend, weil weiterhin die US-amerikanischen Konzepte verwendet werden. Im Verlauf des Praxistests wurde diese Schwäche durch sprachliche Hilfe durch den Versuchsleiter ausgeglichen und ist nicht Thema dieser Untersuchung.

Bei allen Programmen wurde der nötige Neustart des Computers nach der Installation als störend empfunden. Auch wurde davon ausgegangen, daß man bei der Deinstallation Probleme mit dem Registry-Eintrag bekommen würde. Eine "saubere“ Deinstallation war ein immer wiederholter Wunsch der Probanden.

Für alle Programme, die in der vorliegenden Untersuchung in der Version für Windows 95 getestet wurden, wurde immer wieder der Wunsch geäußert, die Betriebssysteme Windows 98 oder Windows NT verwenden zu können. Insbesondere der höhere Sicherheitsstandard und die Möglichkeit, die Konfiguration der Filter effizient für ganze Nutzergruppen durchführen zu können, standen dabei im Vordergrund.

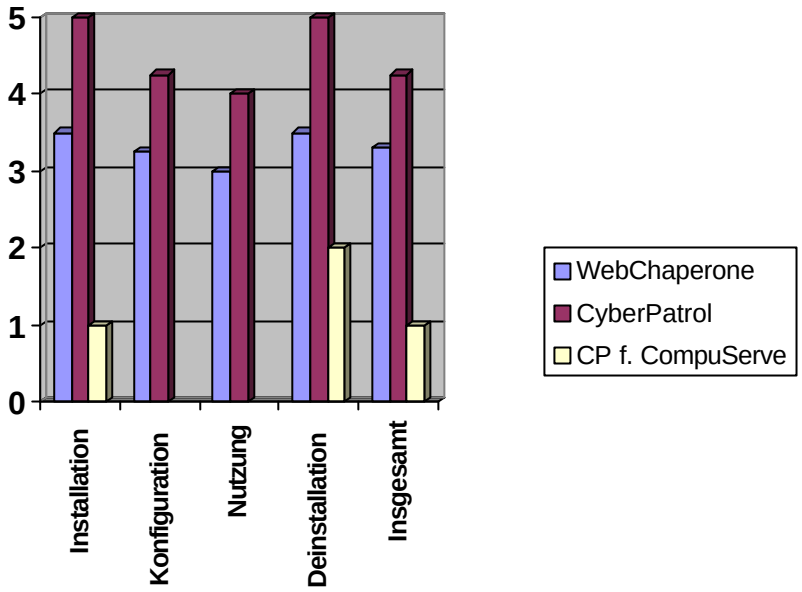


Abb. 5-3: Bewertung der Arbeitsschritte Installation, Konfiguration, Nutzung, Deinstallation sowie der Gesamtbewertung der Produkte WebChaperone, CyberPatrol und CyberPatrol für CompuServe auf einer fünfstufigen Skala von 1 = "sehr unzufrieden“ bis 5 = "sehr zufrieden“.

Zwischen privaten und schulischen Nutzern bestanden Unterschiede. Die Programme wurden aber für eine private Nutzung getestet. Für die Verwendung der Programme in der Schule ist hauptsächlich im technischen Bereich mit anderen Nutzungswünschen zu rechnen. Insbesondere kommt dort meist eine Client/Server-Architektur zum Einsatz, die die Programme vor ganz neue Herausforderungen stellt. Darüber hinaus besteht jedoch kein Anhaltspunkt, nach dem mit größeren Abweichungen von den im folgenden dargestellten Ergebnissen zu rechnen sei.

5.4.2.3 WebChaperone

Die folgenden drei Abschnitte stellen die Erkenntnisse zu den drei untersuchten Produkten dar. Abb. 5-3 präsentiert die Zusammenfassung der Bewertung der drei Produkte durch die Probanden. Erläuterungen befinden sich im weiteren Text.

Der erste Abschnitt zeigt die Ergebnisse des Praxistests des Filterproduktes WebChaperone.

Installation

Im Fragebogen wurde der Installationsprozeß im Mittel mit einer 3,5 auf der fünfstufigen Skala von 1 = "sehr unzufrieden“ bis 5 = "sehr zufrieden“ bewertet. Dies entspricht etwa einem "neutral“ bis "befriedigend“. Die Werte reichten von 2 bis 5.

Die Installation des Filterprogrammes bereitete den Testpersonen keine Schwierigkeiten. Sie wurde wie bei einem "normalen Durchschnittsprogramm“ und auch "angenehm“ erlebt und konnte ohne längeres Überlegen zielstrebig durchgeführt werden. Die Erläuterungstexte des Installationsprogrammes wurden i.d.R. nicht gelesen, sondern übersprungen.

Einmal wurde der Wunsch nach einer kurzen, klaren schriftlich vorliegenden Instruktion geäußert, die die einzelnen Schritte erklärt und v.a. auf das Icon rechts unten am Bildschirmrand hinweist, welches die erfolgreich abgeschlossene Installation bestätigt.

Konfiguration

Die Konfiguration wurde im Mittel mit 3,25 bewertet, also neutral mit einer leicht positiven Tendenz. Der Wertebereich umfaßte die Werte 3 bis 4. Die Konfiguration des Programmes wurde je nach Computererfahrung unterschiedlich beurteilt. Von computer- und interneterfahrenen Testpersonen wurde die Einrichtung verschiedener Nutzer meist als relativ leicht bewertet. Diesbezüglich wenig erfahrene Personen erlebten sie jedoch als umständlich (vgl. auch Abb. 5-4).

Es wurden einige kleinere Kritikpunkte genannt. Z. B. der Sachverhalt, daß man sowohl durch das Aktivieren des "Next“-Knopfes als auch durch Anklicken des Reiters zur nächsten Seite kommt, führte zu leichten Irritationen, die sich durch eine leichte Überarbeitung jedoch beheben ließe. Auch die klarschriftliche Paßworteingabe wurde kritisiert etc.

Konzeptionelle Schwierigkeiten hatten die Probanden mit der Unterscheidung in *Child*, *Pre-Teen* und *Teenager*. Diese wurde z. T. als nicht besonders übersichtlich sondern eher als unnötig beurteilt. Man müßte sich hier bei der Übertragung ins Deutsch besondere Mühe gehen, auch im europäischen Raum übliche Altersklassen zu berücksichtigen. Auch die Schutzklassen *Minimum*, *Medium* und *Maximum* sollten erläutert werden. Diese Hilfe sollte durch einen separaten Button oder über die Hilfe direkt erreichbar sein. Möglicherweise könnte man auch auf diese Unterteilung in Altersklassen (nicht aber auf Schutzklassen) verzichten.

Die Bedienung war nicht gegen Fehler gesichert. Z.B. bei der Aufgabe, das Programm für einen Erwachsenen, einen sechzehnjährigen Jugendlichen und für eine Achtjährige einzustellen, wurde einmal der Jugendliche fälschlicherweise im Register *Adult Set Up* angelegt. Anschließend gelang es nicht, die falsch angelegte Person wieder aus dem Register zu löschen. Die Testperson versuchte dies erfolglos mit dem *Leave*-Button.

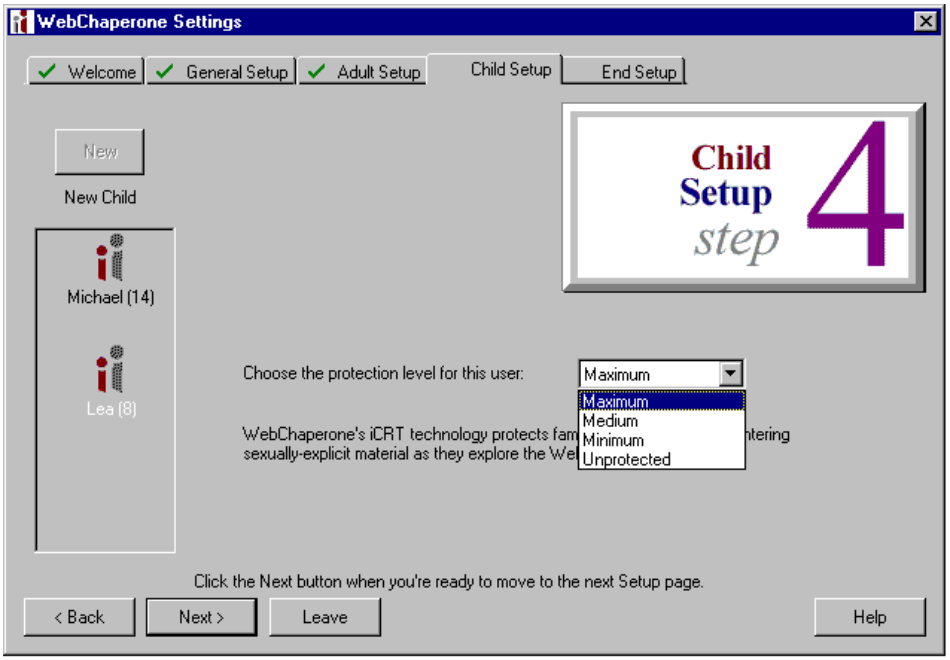


Abb. 5-4: Screenshot der Konfiguration von WebChaperone.

Ein weiterer Kritikpunkt stellte außerdem die Vielzahl von Paßwörtern dar, welche es sich zu merken gilt, wenn viele Benutzer eingerichtet werden.

Computererfahrene Probanden waren sich ziemlich sicher, daß das Programm beim Start einer Internetsitzung gemäß ihrer Einstellungen zuverlässig filtern werde. Die eher unerfahrenen Testpersonen hingegen war sich "nicht so sicher, ob alles o.k. ist“ und hätten das Programm "auf jeden Fall erst selbst geprüft“, bevor sie einem ihrer Kinder Zugang zum Netz gewährt hätten.

Der nötige Computer-Neustart wurde als ärgerlich empfunden.

Auch aus der Sicht des Softwareergonomen ist die Konfiguration zwar nicht in allen Details als vorbildlich zu bewerten. Der Prozeß von Installation und Konfiguration sowie die verwendeten Darstellungsprinzipien sind jedoch tauglich und angemessen.

Nutzung

Die Nutzung wurde im Mittel als 3, d.h. "neutral“ bewertet. Die Werte reichten von 1 bis 4.

Als negativ wurde allgemein beurteilt, daß man beim Internetsurfen nicht klar erkennen könne, ob das Filterprogramm aktiv sei oder nicht. Geschulte Probanden sahen darin aber kein Problem, da das Symbol in der linken unteren Bildschirmecke dies anzeige.

Folgende Verbesserungsvorschläge wurden genannt:

- Zu Beginn der Internetsitzung sollte ein eigenes Fenster erscheinen, das anzeigt, daß das Filterprogramm aktiv ist und das den Benutzer auffordert, sich einzuloggen.
- Es sollte direkt darauf hingewiesen werden, daß das Icon am rechten Bildschirmrand die Aktivität des Filterprogramms symbolisiert.
- Durch Doppelklick auf das Icon sollte ein komplettes Fenster mit Statusanzeige geöffnet werden .
- Es sollte am Bildschirm angezeigt sein, wer mit welcher Sicherheitsstufe gegenwärtig eingeloggt ist.
- Die Einstellung "Current User: Default“ (Aktueller Nutzer: Standard) wurde als "keine Filterung“ mißinterpretiert. Hier sollte ein aussagekräftigerer Name gefunden werden.

Die Darstellung einer Sperrmeldung des Produktes findet sich in Abb. 5-1 auf Seite 117.

Manipulation

Auf einer fünfstufigen Skala von 1 = "sicher möglich“ bis 5 = "unmöglich“ wurde die Manipulierbarkeit von WebChaperone mit im Mittel 2,7, also als wahrscheinlich möglich bewertet. Die Testpersonen gehen davon aus, daß das Filterprogramm manipulierbar ist und von einer computererfahrenen Person unwirksam gemacht werden kann. Die Probanden waren davon überzeugt, daß es keinen hundertprozentigen Schutz bieten könne.

Deinstallation

Die Deinstallation wurde im Mittel mit 3,5 als neutral bis befriedigend bewertet. Sie wurde jedoch z.T. als 1, z.T. als 5 bewertet. Die eine sehr schlechte Bewertung wurde nur aufgrund einer nicht vollständigen Deinstallation gegeben. Wird dieser technische Fehler behoben, so kann mit sehr positiven Bewertungen gerechnet werden.

Die Deinstallation des Programmes wurde in Abhängigkeit von den vorhandenen Computerkenntnissen sehr unterschiedlich beurteilt. Ein wenig erfahrener Proband konnte das Programm nur mit viel Unterstützung deinstallieren. Er hatte keine Idee, wo eine Deinstallation möglich ist. Verunsicherung erzeugte insbesondere auch die Aufforderung, das Paßwort einzugeben. Dem Probanden war unklar, welches der verschiedenen Paßwörter gefordert ist und er gab fälschlicherweise sein "Adult User-“ anstelle des Hauptpaßwortes an.

Die anderen Probanden dagegen beurteilten die Deinstallation als "sehr einfach, wenn man weiß, wo man Programme installiert bzw. deinstalliert“ . Positiv wurde beurteilt, daß neben der "klassischen“ Deinstallationsmethode (über Start – Einstellungen – Systemsteuerung – Software...) eine zweite, einfachere Möglichkeit besteht (Start – Programme – WebChaperone – Uninstall WebChaperone).

Gesamtbeurteilung des Filterprogrammes

Die Probanden sind mit WebChaperone ziemlich zufrieden. Der Mittelwert der Gesamtbewertung ist 3,3 mit Werten zwischen 3 und 4. WebChaperone ist ein eher zurückhaltend gestaltetes Filterprogramm. Es ist an vielen Stellen vorbildlich dem Aufgabenablauf der Filternutzer angepaßt. Es weist im Detail jedoch noch korrigierbare Schwächen auf.

Die Installation ist im Prinzip einwandfrei. Die Konfiguration schließt sich unmittelbar an die Installation an und kann i.d.R. leicht und in einem Zug durchgeführt werden. Der Aufruf der Programms und der Wechsel zwischen verschiedenen Nutzern solle etwas modifiziert werden, ist von Konzept her aber in Ordnung. Die Deinstallation ist ziemlich problemlos.

5.4.2.4 CyberPatrol

Im Folgenden werden die Ergebnisse des Praxistests der Filterprogrammes "CyberPatrol“ dargestellt

Installation

Alle Probanden bewerteten die Installation mit 5, waren also "sehr zufrieden“. Die Installation von CyberPatrol bereitete den Testpersonen keine Schwierigkeiten und konnte ohne längeres Überlegen zielstrebig durchgeführt werden. Der Installationsmodus sei ganz normal und nicht komplizierter als bei anderen Programmen. Die Erläuterungs- und Lizenztexte wurden nicht gelesen.

Lediglich der Übergang von der Installation zur Konfiguration nach dem Computer-Neustart wurde als problematisch bewertet. Zu Beginn sollte – so ein Proband – automatisch ein "Hilfefenster“ erscheinen, welches die Grundfunktionen kurz und prägnant erklärt.

Konfiguration

Die Konfiguration wurde nicht ganz so positiv bewertet. Der Mittelwert betrug 4,25, was einer Bewertung von "befriedigend“ mit positiver Tendenz entspricht. Der Wertebereich umfaßte die Werte 4 bis 5.

Das "Headquarter“ ist die zentrale Seite, auf der Konfigurationen durchgeführt werden, vgl. Abb. 5-5. Die Fülle des Funktionsumfanges beeindruckt die Probanden. Die Zeitsteuerung fiel am ehesten ins Auge und lenkte dadurch von den eigentlichen Filterfunktionen ab. Die Orientierung im Programm fiel den Probanden schwer. Es gab keinen vorgegebenen Aufgabenablauf zur Einrichtung verschiedener Nutzer. Dies führte zu z.T. erheblichen Problemen. Das "Headquarter“ unterschied nicht klar zwischen personenbezogenen Einstellungen (*Access to specific services*) und allgemeinen Einstellungen (*Time Mgmt. On/Off*; etc.). Die Nutzer hatten erhebliche Probleme, das Produkt überhaupt zu verstehen. Die Buttons auf dem Hauptbildschirm (=Headquarter) erweckten zwar den Eindruck, alles beeinflussen zu können. Diese Funktionsvielfalt wurde (insbesondere bei der Unterscheidung zwischen Chat, WWW, News und Programmnutzung sowie die Möglichkeit der Listenkonfiguration) als positiv empfunden. Gleichzeitig hatten die Probanden nicht den Eindruck, diese Vielfalt auch beherrschen zu können. Es blieben meist noch Unsicherheiten über die tatsächliche Einstellung und Wirkung.

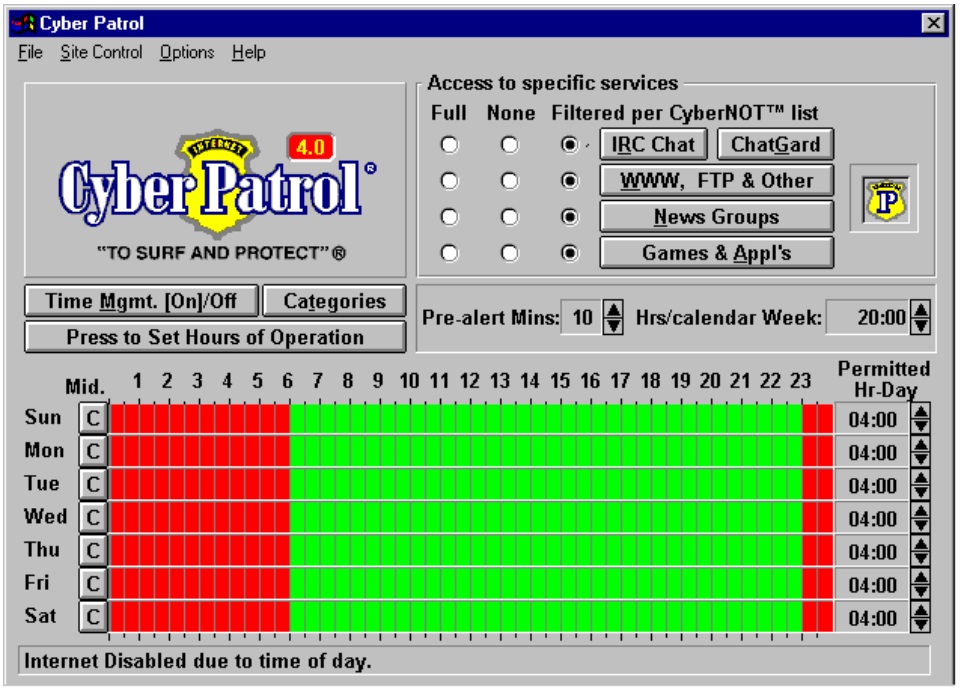


Abb. 5-5: "Headquarter"/Steuerpult zur Konfiguration von CyberPatrol.

Es gab eine Reihe von einzelnen Kritikpunkten:

- Die Zeit-Editierung ist umständlich.
- Bei Betätigung des "Save"-Buttons verschwindet dieser zugunsten eines Zeiteinstellungs-Buttons.
- Die Nutzereinrichtung über das file-Menu ist "versteckt" und umständlich.
- Das Deputy-Konzept (Definition eines Haupt- und eines Nebenadministrators) wurde nicht verstanden.
- Die Headquarter-Metapher wurde nicht nachvollzogen.
- Die Nutzer erwarteten die Möglichkeit, Profile einzugeben.
- Die klarschriftliche Paßworteingabe wurde kritisiert. Besser wäre eine doppelte, maskierte Paßworteingabe.
- Zwar wurde die Anlage der einzelnen Benutzer als einfach bewertet. Die jeweiligen Einstellungen festzulegen wurde jedoch als schwer und unübersichtlich beschrieben.
- Bei falscher Paßworteingabe wurde die 15-Sekunden-Sperre als verbleibende Zeit, in der eine erneute Paßworteingabe möglich war, interpretiert. Dies führte innerhalb der 15 Sekunden zu großer Eile, nachfolgend zu Ärger.
- Teils verwendet das Programm die Konzepte nicht korrekt. So finden sich Anzeigen wie "Lea als Lea", wenn der Nutzer als "Lea" eingeloggt ist. Überhaupt wurden z. B. Icons zur besseren Navigation zwischen den Nutzern vorgeschlagen. Der Benutzer sollte auch in der Titelleiste angezeigt werden.

Nutzung

Alle Probanden waren mit der Nutzung des Produktes "zufrieden" (4).

Als Verbesserungsvorschläge wurden eine deutlichere Rückmeldung gewünscht. Die Sperrmeldung gab keinen Hinweis auf evtl. geeignete Seiten oder an wen man sich ggf. wenden könne. Auch die angegebene Codenummer wurde als unverständlich und damit

störend empfunden. Die Umschaltung zwischen verschiedenen Nutzern wurde als unbefriedigend empfunden.

Manipulation

Die Manipulation wurde mit 3,25 als wahrscheinlich möglich bewertet. Es gab Einschätzungen mit 4 und mit 1. Die Testpersonen gehen davon aus, daß das Filterprogramm manipulierbar ist und von einer computererfahrenen Person unwirksam gemacht werden kann.

Deinstallation

Alle Probanden waren "sehr zufrieden“ mit der Deinstallation (Mittelwert = 5). Sie wurde von den Testpersonen als sehr einfach beurteilt und konnte zügig durchgeführt werden. Besonders komfortabel sei die Deinstallation, weil sie direkt im Programm unter "File“ aufgerufen und durchgeführt werden kann. Es sollte jedoch sehr deutlich auf den nötigen Computer-Neustart hingewiesen werden bzw. dieser automatisch vorgeschlagen werden. Die Nichtbeachtung dieses Neustarts führt bei erneutem Installationsversuch zu fatalen Problemen.

Gesamtbeurteilung des Filterprogrammes

Mit 4,25 sind die Probanden "zufrieden“ mit CyberPatrol. Es macht auch aus softwareergonomischer Sicht einen befriedigenden Gesamteindruck. Die Installation ist in Ordnung. Die relativ gute Bewertung der Konfiguration durch die Probanden ist jedoch nicht nachvollziehbar. Aus der Sicht des Softwareergonomen ist diese klar mit Mängeln behaftet. Positiv ist nur zu bewerten, daß viele Funktionen auch von den Nutzern wahrgenommen werden. Diese Funktionsvielfalt müßte in einen verbesserten Programm jedoch strukturierter dargeboten werden. Der umständliche Wechsel zwischen verschiedenen Nutzern ist unnötig und störend. Die Deinstallation ist bis auf den nötigen automatischen Hinweis auf den nötigen Computer-Neustart in Ordnung.

Im Vergleich zu WebChaperone schneidet CyberPatrol in der Wahrnehmung der Probanden bei allen Aspekten besser ab, vgl. Abbildung 1. Die Menge der Kritikpunkte, die Vielzahl der gemachten Fehler und die offensichtlichen Probleme der Nutzer mit CyberPatrol relativieren diese bessere Bewertung jedoch. Was die Gebrauchstauglichkeit und den Gesamteindruck angeht, ist deshalb aus Sicht des Softwareergonomen CyberPatrol unterlegen. Die offensichtliche Funktionsvielfalt ist jedoch besser als beim Mitbewerber WebChaperone. Dies könnte dazu geführt haben, daß CyberPatrol bei den Nutzern so "gut ankommt“. Als Ausgangsbasis für ein zu entwickelndes Filterprogramm ist das Konzept von WebChaperone vorzuziehen. Es sollte jedoch versuchen, die Vielfalt der verfügbaren Funktionen von CyberPatrol auch auf dem Bildschirm klar strukturiert sichtbar zu machen.

5.4.2.5 CyberPatrol für CompuServe

Das Produkt CyberPatrol für CompuServe (Version 3.0.4) ist (abgesehen von der Übersetzung ins Deutsche) weitgehend ähnlich mit der englischsprachigen Version von CyberPatrol, die unter oben behandelt wurde. Im folgenden werden deshalb nur die spezifischen Unterschiede thematisiert.

Installation

Die Probanden waren mit der Installation "sehr unzufrieden“ (1). Der farbige Installationsbildschirm und die sich immer gleich wiederholende Musik wurde als nervig und störend empfunden. Schon die erste Dialogbox "Willkommen!“ (vgl. Abb. 5-6) ist offensichtlich unlogisch: "Sind Sie mit der folgenden Erklärung einverstanden, klicken Sie auf [Weiter].“ heißt es dort. Wie können die Nutzer wissen, ob sie mit der folgenden Erklärung

einverstanden sein werden, sie konnten sie ja noch nicht lesen. Dieser an sich kleine Fehler ganz zu Beginn des Installationsprozesses führte zu Widerstand der Probanden.

Abb. 5-6: Screenshot "Willkommen!“ bei der Installation von CyberPatrol für CompuServe.

Für die Installationshinweise wurde fälschlicherweise ein Warnungssymbol verwendet (roter Kreis) statt eines Hinweissymbols (gelbes Dreieck). Die an sich wichtigen Installationshinweise wurden oft übersprungen, da sie für eine "langweilige“ Lizenzvereinbarung gehalten wurden. Die Dialogbox "Installation abgeschlossen!“ wird von anderen durch CyberPatrol geöffneten Fenstern überdeckt. Es wird unnötigerweise automatisch das Autostart-Fenster geöffnet. Der Aufforderung, den Readme-Text zu lesen, kamen die meisten Probanden zunächst nicht nach. Es besteht auch eine Inkongruenz zwischen der Aufforderung, die Readme-Datei zu lesen und den Neustart durchzuführen.

Wegen technischer Probleme konnten die Probanden die Installation nicht erfolgreich abschließen.

Konfiguration

Die Konfiguration wurde wegen der fehlgeschlagenen Installation mit der oben beschriebenen Version von "CyberPatrol“ geprüft. Die Ergebnisse sind dort dargestellt.

Nutzung

Für die Ergebnisse zur Nutzung gelten dieselben Feststellungen wie bei "CyberPatrol“. Abgesehen davon stellten es sich die Probanden bei der Version CyberPatrol für CompuServe als positiv, wenn auch nicht besonders wichtig vor, daß das Filterprogramm im Internetprovider integriert ist.

Manipulation

Die Manipulierbarkeit wurde interessanterweise mit 4 als eher unmöglich bewertet. Eventuell führten die vielen Probleme dazu, daß das Programm als "unzugänglich“ wahrgenommen wurde.

Deinstallation

Mit der Deinstallation waren die Probanden "zufrieden“ (2). Auch bei CyberPatrol für CompuServe gab es wie bei der anderen Version von CyberPatrol keine Probleme bei der Deinstallation. Die Möglichkeit, zwischen automatischer und benutzerdefinierter Deinstallation zu wählen, wurde nicht als sinnvoll bewertet.

Gesamtbeurteilung des Filterprogrammes

Die Gesamtbeurteilung von CyberPatrol für CompuServe wurde mit 1 = "sehr unzufrieden“ bewertet. Dies ist aber hauptsächlich auf die mangelhafte Installation zurückzuführen. Die Einbindung in den Provider wurde als positiv empfunden, wenn auch nicht als notwendig. Genauere Hinweise könnte man sich von Internetnutzern erwarten, die CompuServe regelmäßig nutzen.

5.4.2.6 Features und Konzepte

Im folgenden werden die Ergebnisse des Feature-Fragebogens dargestellt und die Erkenntnisse aus den Interviews zu den Fragen nach möglichen Filterkategorien sowie nach eventuellen Darstellungsformen vorgestellt.

Der produktübergreifende Fragebogen enthielt die folgenden drei Fragen. Sie konnten auf einer fünfstufigen Skala von 1 = "völlig sinnlos“ bis 5 = "sehr sinnvoll“ beantwortet werden.

Einstellung von Dauer und Tageszeit

"Es ist bei manchen Filterprogrammen möglich, die Dauer und Tageszeit, an der gesurft werden kann, einzustellen. Würden Sie diese Möglichkeit für sinnvoll halten?“ Die mittlere Bewertung war mit 4 "sinnvoll“. Es kamen Bewertungen von 2 (sinnlos) bis 5 (sehr sinnvoll) vor.

Benutzung / Installation anderer Programme

"Es ist bei manchen Filterprogrammen möglich, auch die Benutzung und / oder die Installation anderer Programme zu sperren. Würden Sie diese Möglichkeit für sinnvoll halten?“

Der Mittelwert betrug 4,6, was einer Bewertung als "sinnvoll“ bis "sehr sinnvoll“ entspricht. Die schlechteste Bewertung war eine 3 (neutral), sieben Probanden gaben die beste Note 5.

Eingabe von Kreditkartennummern, Adressen und Telefonnummern

"Es ist bei manchen Filterprogrammen möglich, die Eingabe von Kreditkartennummern, Adressen und Telefonnummern zu sperren. Würden Sie diese Möglichkeit für sinnvoll halten?“

Der Mittelwert von 4,8 zeigt, daß fast alle Probanden diese Möglichkeit als "sehr sinnvoll“ bewerteten. Es kamen nur noch zweimal die Bewertung 4 vor.

Filterkategorien

Das Interview zu den Filterkategorien richtete sich nach folgendem Interviewleitfaden:

- Nach welchen Eigenschaften sollten die Internetseiten Ihrer Ansicht nach gefiltert werden?
- Wie würden Sie die Seiten beschreiben, die durchkommen sollen (für Erwachsene, Jugendliche, Kinder)?
- Wie würden Sie die Seiten beschreiben, die gesperrt werden sollen (für Erwachsene, Jugendliche, Kinder)?
- Welche Kategorien der Filterung halten Sie demnach für sinnvoll?

In den Interviews zeigten sich erwartungsgemäß sehr unterschiedliche Meinungen zu möglichen Filterkategorien. Trotzdem läßt sich zum Fragekomplex der Filterkategorien ein Fazit ziehen. Denn ein Muster zeigen erstaunlich viele Probanden. Diese sprachen sich für die folgenden drei Filterkategorien aus.

- Sex/Pornographie
- Gewalt
- Ideologie / Politischer Extremismus

Interessant dabei ist besonders die bewußte Beschränkung auf eine überschaubare Anzahl an Kategorien. Auch die Inhalte der Kategorien waren meist ähnlich. Es zeichnete sich ein Konsens ab, daß die drei Kategorien möglicherweise auch mit einer übergreifenden,

allgemeinen Kategorie verknüpft werden könnte. Diese übergreifende Kategorie könnte dann "Alter (1 bis 18 Jahre)“ oder "Schutz (gering bis hoch)“ oder "Filterung (stark bis schwach)“ o. ä. heißen. Zur Veranschaulichung schien ein "Mischpultmodell“ geeignet. Dabei gab es drei einzelne Regler "Sex/Pornographie“, "Gewalt“ und "Ideologie“. Diese können von einem übergeordneten Regler "Filterstärke“ eingestellt werden, aber auch einzeln nachjustiert werden.

Einzelne Probanden sprachen sich auch für mehr Kategorien aus wie z. B. neben obigen drei Kategorien auch

- Drogen
- Waffendarstellung, -gebrauch und Anleitungen zum Selberbasteln
- Demütigung von Menschen
- Tierquälerei.

Es gab aber auch Probanden, die sich diesbezüglich ganz auf die Hersteller von Filterprogrammen verlassen würden.

Die Einstellungsfeinheit (bzw. Rasterung im Mischpultmodell) sollte nach Meinung der Probanden etwa bei 3, 4, 5 oder 7 Rasterstufen liegen. Natürlich sprachen sich auch manche Probanden für gröbere (2 Rasterstufen) oder feinere Stufen aus. Man kann davon ausgehen, daß 4 oder 5 Rasterstufen eine gute Ausgangsgröße wären.

Filterdarstellung

Das Interview, das geeignete Darstellungen der Filterprogramme erheben sollte, verwendete den folgenden Leitfaden:

- Welche Filtermechanismen werden als angenehm erlebt?
- Wie sollten diese dargestellt werden?
- Wie sollte sich das Produkt "verhalten“, damit Sie es als angenehm / unangenehm empfinden?
- Wenn Sie sich das Produkt als "Figur“ / "Gestalt“ vorstellen, um was für eine Person / Persönlichkeit handelt es sich dann?
- Was sind ihre primären Wesenszüge (autoritär? streng? gütig? lustig? komisch? drohend?)?
- Wie sollte sie nicht sein?
- Wie sollte sie dargestellt werden (Filtermeldung)?

Die Probanden äußerten eine unübersehbare Vielfalt an Vorschlägen und Vorlieben. Im Gegensatz zur Frage nach den Filterkategorien gab es keine eindeutige Übereinstimmung. Es ließen sich eher ein Negativbild von zwei möglichen Positivbildern abgrenzen.

Das Negativbild wurde als eine Art autoritärer Filter, eine strenge Vater- oder Polizistenfigur angesehen. Als schlimm wurde auch die Möglichkeit angesehen, daß die "verbotenen“ Seiten gespeichert und dann von den Eltern bemerkt würden.

Positiv könnte jedoch eine Art großer Bruder aufgefaßt werden. Dies macht WebChaperone schon ganz gut vor. Als wichtig wurde dabei genannt, daß das Filterprogramm immer partnerschaftlich bleibt und nicht von ober herunter, sondern auf eine Weise "von gleich zu gleich“ ist. Es könnte auch ein Freund o. ä. sein.

Eine andere Möglichkeit wäre ein Auftritt des Filters ohne jede Personifizierung. Eine Meldung wie z.B. "Diese Seite wurde durch das Programm XY gesperrt. Bitte wenden Sie sich an den

Administrator, wenn Sie nähere Informationen oder die Freigabe wünschen.“ Als wichtig wurde empfunden, daß klar hervorgeht, wer (bzw. welches Programm) die Sperrung verursacht hat bzw. an wen man sich wenden kann.

5.4.2.7 Fazit und Handlungsempfehlung

Sieht man von den rein technischen Problemen ab, so bieten die untersuchten Filterprogramme gute Ansätze für mögliche Weiterentwicklungen. Die Erfüllung folgender Forderungen sind jedoch für den deutschsprachigen Markt Voraussetzung:

- Die technischen Probleme müssen ausgemerzt werden.
- Es muß durchgängig die deutsche Sprache verwendet werden.

Die Installation mit üblichen Hilfsprogrammen zur Installation ist unproblematisch.

Die Konfiguration sollte in etwa wie bei dem Filterprogramm WebChaperone gelöst sein. Als gut zu bewerten ist die übergangslose Aufnahme der Konfiguration im Anschluß an die Installation. Es gibt im Detail jedoch deutlichen Verbesserungsbedarf in der Darstellung. Es sollte versucht werden, die Funktionsvielfalt so deutlich werden zu lassen, wie dies das Programm CyberPatrol erreicht, wenngleich auch eine klarere Struktur erkennbar sein sollte. Wie dies im Einzelnen auszusehen hat, ist noch offen. Für die Kategorienfilterung (nach Ratings und/oder nach Keywords) erscheint ein "Mischpult“-Modell zumindest möglich. Bei der Gestaltung zukünftiger Filterprogramme sollte mehr Gewicht auf die Passung zwischen Programm und Aufgabenstruktur gelegt werden.

Die Deinstallation ist weitgehend unproblematisch.

Der Manipulationsschutz sollte weiter ausgebaut werden, um technische Probleme durch Manipulationsversuche auszuschließen. Möglicherweise könnte die verstärkte Nutzung von Betriebssystemfunktionalität (z.B. von Windows NT) Abhilfe schaffen. Überhaupt sollte eine Oberflächen- und Funktionalitätsintegration mit dem Betriebssystem vorangetrieben werden, so daß die Programme übergangslos mit dem Betriebssystem funktionieren.

Für Weiter- bzw. Neuentwicklungen bietet es sich an, von Anfang an mit den zukünftigen Nutzern zusammenzuarbeiten um konzeptionelle Fehlentwicklungen wie bei den untersuchten Programmen auszuschließen. Schließlich muß auch die rein technische Fehlerfreiheit deutlich gesteigert werden.

6 Perspektiven des technischen Jugendschutzes im Internet

In der vorliegenden Studie wurden die zur technischen Unterstützung des Jugendschutzes im Internet zur Verfügung stehenden Technologien einer gründlichen Untersuchung unterzogen. Daraus konnte eine Vielzahl von detaillierten Anforderungen an eine geeignete Realisierung abgeleitet werden.

In diesem Kapitel werden wir nun aus diesen Einzelaspekten das Gesamtbild eines organisatorisch-technischen Systems zusammensetzen, das einen möglichen Lösungsansatz für die technische Unterstützung des Jugendschutzes im Internet zeigt.

Zuerst wird das Gesamtkonzept in seiner Struktur grob beschrieben; danach skizzieren wir die einzelnen Komponenten etwas detaillierter. In einem letzten Abschnitt weisen wir außerdem auf die Gefahren hin, die ein solches System bei Mißbrauch in sich birgt und denen daher besondere Beachtung geschenkt werden sollte.

Beginnen werden wir mit einem kurzen Resümee der wichtigsten Ziele und Anforderungen.

6.1 Ziele und Anforderungen

Mit einem Konzept zur systematischen technischen Unterstützung des Jugendschutzes im Internet sollen die folgenden Ziele verfolgt werden:

- Unterstützung von Erziehungsberechtigten beim Schutz Jugendlicher vor jugendgefährdenden Inhalten im Internet,
- Bereitstellung technischer Mechanismen zum Schutz jugendlicher "Surfer“ vor ungewollten, zufälligen aber auch neugierigen Zugriffen auf Internetseiten mit jugendgefährdendem Inhalt,
- dabei zugleich Erhaltung des Internet als eine auch Jugendlichen frei zugängliche Informationsquelle,
- Vermittlung einer umfassenden Medienkompetenz durch Sensibilisierung und Aufklärung der Internetnutzer,
- Schaffung von Rechtssicherheit für Anbieter und Abrufer, besonders aber für die Mittler der Informationsübertragung (Access- und Presence-Provider),

Bei dem zu konzipierenden Lösungskonzept und den Empfehlungen für das weitere Vorgehen sind die folgenden Anforderungen zu beachten:

- die rechtlichen Rahmenbedingungen des Jugendschutzes, aber auch der Datenschutz und das Recht auf Information,
- ein guter Schutz vor jugendgefährdenden Inhalten, aber auch die Verhinderung von Möglichkeiten der Willkür bei Einordnung und Filterung,
- die technische Machbarkeit, das heißt z.B. zumutbarer Aufwand für Anbieter und Abrufer, sowie eine gute "Usability“ für diese beiden Gruppen,
- ein Beibehalten der bisherigen Struktur des Internet als freies Informationsmedium, das ein wertvolles Instrument der Informationsgesellschaft ist.

6.2 Gesamtkonzept der Lösung

Grundidee des vorgeschlagenen Konzeptes ist, die formale Einstufung der Inhalte auf den Inhaltsanbieter und die Auswahlhoheit auf den Abrufer zu übertragen, beide mit geeigneten

Werkzeugen und einer zugrunde liegenden Infrastruktur zu unterstützen und den Ablauf in geregelte Bahnen zu lenken.[227]

Alle anderen Beteiligten – insbesondere die Informationsvermittler – könnten auf diese Weise weitgehend aus der Verantwortung entlassen werden. Dies ist wünschenswert, da sie technisch kaum in der Lage sind, eine trennscharfe Filterung mit zumutbarem Aufwand durchzuführen.

Dieses Konzept der Verteilung von Verantwortung läßt sich direkt in technischen Prozessen konkretisieren.

6.2.1 Ablauf

Der grundlegende Ablauf der entworfenen Jugendschutzfilterung ist danach folgender:

Es wird ein *Kategoriensystem* zur Einordnung zur Verfügung gestellt (z.B. durch Koordinierungsstellen), mit dem die Inhalte der Seite thematisch eingestuft werden können. Inwieweit das Kategoriensystem auch inhaltliche Kategorien zur Verfügung stellt oder nur eine Einstufung in "jugendgefährdend“ und "nicht jugendgefährdend“ zuläßt, muß im einzelnen diskutiert werden. Kriterium könnte dabei auch ein eventueller Mehrwert durch erweiterte Suchfunktionen bei vielen Kategorien sein. Denkbar sind außerdem mehrere solche Systeme, die technisch ineinander überführbar sind.

Die Einordnung soll der *Anbieter* durchführen und zur Authentifizierung auch digital signieren; entsprechende Werkzeuge müssen verfügbar sein.[228] Da der Anbieter nach geltendem Recht seinen Namen in jedem Falle angeben muß (Impressum), entsteht durch die Signatur kein Verlust einer vorher bestehenden Anonymität.

Ziel ist es, mit begleitenden Maßnahmen verschiedener Art eine so weite *Verbreitung* dieses Systems zu erzielen, daß eine *flächendeckende Filterung* auf dessen Basis möglich ist. Wünschenswert wäre außerdem eine internationale Akzeptanz des Systems.

Dann kann der *Abrufer* mit einem lokal konfigurierten System aufgrund der z.B. durch PICS-Kennzeichnung vermerkten Einordnungen auswählen, welche Seiten angezeigt werden und welche nicht.

Neben der Möglichkeit des Jugendschutzes bieten sich dem Abrufer damit auch andere Möglichkeiten der gezielten Auswahl und Suche nach bestimmten Inhalten. Wird das System explizit auch für solche Zwecke angelegt, könnte damit ggf. eine Steigerung der Akzeptanz erreicht werden.

Das System wird unterstützt von Koordinierungsstellen, die neben dem Kategoriensystem auch die technischen Werkzeuge zur Verfügung stellen und an den technischen Fortschritt anpassen. Sie müssen außerdem die Infrastruktur für die Signaturen vorhalten und als Sanktionsinstanz bei Mißbrauch des Systems – insbesondere bei falschen Einstufungen – eingreifen.

---

227 Nach der Rechtslage müssen Anbieter von jugendgefährdenden Inhalten den Zugriff für Kinder und Jugendliche technisch beschränken. Zumindest für einen Teil der jugendgefährdenden Inhalte wäre dies auch durch eine solche Kombination von formaler Einstufung und verfügbarer Auswahllogik denkbar.

228 Auf Basis der aktuellen Rechtslage kann eine solche Einordnung für Anbieter nicht jugendgefährdender Inhalte nicht verpflichtend sein. Ähnliches läßt sich auch aus verschiedenen Stellungnahmen von Bundesrat und Bundesregierung zur Einbringung des IuKDG in den Bundestag, Drucksache 13/7385 vom 09.04.1997, entnehmen.

6.2.2 Organisatorischer Rahmen

Der organisatorische Rahmen, den das technische System als Grundlage braucht, besteht aus

- einem Kategoriensystem[229], das auf der Basis einer möglichst allgemeinen, nicht nur auf Experten beschränkten Diskussion zu erarbeiten ist und technisch zur Verfügung stehen muß,
- einer Koordinierungsstelle oder einem Netzwerk solcher Stellen, die die Schlüsselverwaltung für ein System zur Sicherung von Integrität und Authentizität der Label übernehmen und fehlerhafte Einordnungen sanktionieren,
- einer rechtlichen Konkretisierung zur Schaffung von Rechtssicherheit für alle beteiligten Gruppen mit dem Ziel, daß die Verwendung des Systems als ausreichend im Sinne des Jugendschutzgesetzes klassifiziert wird,
- einer Motivations- und Durchsetzungsstrategie, die dafür sorgt, daß sich das System schnell verbreitet, möglichst auf freiwilliger Basis.

Außerdem sind Regeln für die Übergangsphase festzulegen.

6.2.3 Technisches System

Das technische System besteht aus

- der technischen Definition des genannten Kategoriensystems auf Basis von PICS mit nötigen Erweiterungen,
- einer einfachen Möglichkeit für den Anbieter, Einordnungen durchzuführen, diese in Seiten einzubauen und digital zu signieren,
- optionalen Rating- und Label-Providern sowie
- einer einfachen Möglichkeit für den Abrufer, zuverlässig aufgrund der Einordnungen der Anbieter auszuwählen (angepaßte Client-Komponente).

Das System sollte im Rahmen der technischen Möglichkeiten manipulationssicher sein.

6.2.4 Aufbau von Medienkompetenz

Die Unterbindung des Zugangs zu jugendgefährdenden Inhalten für minderjährige Nutzer sollte ergänzt werden durch Maßnahmen, die den Zugang zu jugendgeeignetem Material verbessern und erleichtern.

Als Ergänzung und komplementäres Angebot zur technischen Verhinderung des Zugriffs Jugendlicher auf jugendgefährdende Inhalte können z.B. unterstützend spezielle jugendgeeignete mediale Angebote gefördert und übersichtlich präsentiert werden ("Kinder-Netz“).

6.3 Organisatorischer Rahmen

6.3.1 Koordinierungsstellen

Den Ankerpunkt des organisatorischen Rahmens bildet eine Kontrollinstanz unter öffentlicher Kontrolle, die die Funktionen des Systems überwacht und steuert. Sie hat eine Funktion analog zur BPjS ("BPjW“ – Bundesprüfstelle für jugendgefährdende WWW-Seiten). Ob es

[229] oder auch mehreren Systemen, die dann technisch kompatibel sein müssen.

sich hierbei um eine einzige Institution oder ein Netzwerk von Koordinierungsstellen handelt, hängt von der detaillierten Konzeption des Systems ab; beide Varianten sind möglich.

Da sie auch die Sanktionen für Mißbrauch des Systems ausspricht, dient sie gleichzeitig als Puffer für Attacken auf eventuell ungerechtfertigte Einstufungen oder direkte Angriffe auf Anbieter. Die Möglichkeit der Druckausübung auf den Anbieter über dessen Presence-Provider kann somit entfallen, da ein gegen die Einstufung verstoßender Anbieter immer direkt an eine der Kontrollstellen gemeldet wird.

Diese Koordinierungsstellen haben fünf Hauptaufgaben:

- den Aufbau des Kategoriensystems,
- die Erstellung und Verteilung der Werkzeuge und Hilfsmittel,
- die Verwaltung der zum Signieren erforderlichen Schlüssel und Zertifikate,
- die Kontrolle von Einordnungen und Kennzeichnungen und die Sanktionierung bei Falscheinordnungen,
- die gesellschaftliche Motivation zur Verwendung des Systems (Aufklärung, Bewerbung).

6.3.1.1 Schlüsselverwaltung

Generell gilt, daß Schlüssel zum Signieren von Internetseiten und Einordnungen keinesfalls gleichzeitig auch für andere Zwecke verwendet werden dürfen, da andere Anwendungen höhere Sicherheitsniveaus und andere Verteilungskonzepte erfordern.

Die Generierung eines Signierschlüssels erfolgt sinnvollerweise nicht zentral, da dies unnötigen Aufwand zur Folge hätte. Er kann lokal, beim Endnutzer (in diesem Falle Anbieter) oder dessen Presence-Provider erfolgen. Die Zertifizierung des öffentlichen Schlüssels erfolgt durch eine autorisierte Zertifizierungsstelle und nur bei Vorliegen einer schriftliche Einwilligungserklärung zur Nutzung dieses Schlüssels durch den Schlüsselinhaber.

Es ist zu überlegen, inwieweit ein solches Zertifikat nur gegen Gebühr erhältlich sein sollte. Mit einer solchen Gebühr sinkt möglicherweise die Motivation zur Verwendung des Systems; anderseits lassen sich durch die Gebühr zusätzliche Sanktionierungsmaßnahmen erzeugen (s.u.). In jedem Falle sollte der Verwaltungsaufwand zur Gebührenhebung möglichst klein gehalten werden; so könnte der Betrag z.B. in der Gebühr für den Internetzugang enthalten sein.

Prinzipiell müssen die Koordinierungsstellen auch die Liste der zurückgerufenen, ungültigen Zertifikate pflegen und Nutzern zugänglich machen. Allerdings ist dies bei bestimmungsgemäßem Gebrauch der Schlüssel nur mit wenig Aufwand verbunden:

- Geht ein Schlüssel oder das Zugangspaßwort verloren, ist keine Sperrung, sondern lediglich das Ausstellen eines neuen Zertifikates erforderlich. Die mit dem alten Schlüssel signierten Seiten bleiben weiterhin gültig.
- Wurde ein Schlüssel kompromittiert, ist ein Rückruf erforderlich; dabei ist darüber nachzudenken, ob sich ein Zeitstempel so realisieren läßt, daß auch in diesem Falle Seiten, die vor der Kompromittierung signiert wurden, gültig bleiben.

Sowohl für den Gültigkeitszeitraum der Zertifikate als auch für die Häufigkeit und Art der Verteilung von Rückruflisten sind geeignete Abwägungen zwischen Sicherheit und Aufwand vorzunehmen und die Abläufe entsprechend zu definieren.

6.3.1.2 Kontroll-Policy

Es ist denkbar, daß die Koordinierungsstellen auch selber Einordnungen kontrollieren; aufgrund der Menge der Seiten werden sie aber wesentlich auf Meldungen der Internetnutzer angewiesen sein.

Das Vorgehen beim Auffinden einer möglicherweise fehlerhaft eingeordneten Seite ist dann z.B. so:

- **1. Stufe**:
  Es wird – möglicherweise über ein Formular an der zentralen Stelle – eine Nachricht vom Abrufer an den Anbieter generiert, daß eine falsche Einstufung vorliegt. Eine Kopie dieser Nachricht geht an eine der Koordinierungsstellen.[230]
  Reagiert der Anbieter mit einer Korrektur – weil ein technischer Fehler vorlag oder er die Fehleinstufung anerkennt – meldet er dies ebenfalls an die Koordinierungsstelle, "löscht" damit die erste Nachricht und der Vorgang ist beendet. Zur Unterstützung wäre ein automatisiertes Kontrollverfahren sinnvoll, daß die Veränderung der Einordnung überprüft.
- **2. Stufe**:
  Reagiert der Anbieter nicht, schreitet die Koordinierungsstelle selbst ein und fordert zu einer Änderung auf.
- **3. Stufe**:
  Erfolgt auch dabei keine Reaktion, wird das Signaturschlüsselzertifikat für ungültig erklärt und ist damit in der nächsten Rückrufliste enthalten. Die digitalen Signaturen unter den Seiten des Anbieters werden anschließend vom Filtersystem abgewiesen. In besonderen Fällen können außerdem rechtliche Maßnahmen gegen den Anbieter wegen Verstoßes gegen den Jugendschutz eingeleitet werden.

Generell sollte diese Policy so konkretisiert werden, daß die Rückruflisten klein bleiben. Es wäre also möglich, vor den Rückruf des Schlüssels noch einige Sanktionsstufen zu setzen (z.B. Strafgebühren).

6.3.1.3 Kategoriensystem und Software

Das Gesamtsystem hat nur dann Potential für eine weite Verbreitung, wenn es mit möglichst vielen Beteiligten abgestimmt ist. Daher sind sowohl die Online-Dienste wie T-Online, CompuServe, AOL als auch sonstige große Anbieter – dabei gerade auch die mit nicht immer für Kinder geeigneten Inhalten – in den Entwicklungsprozeß mit einzubeziehen. Ziel muß es sein, einerseits ein möglichst gut zur Beschreibung vieler – jugendschutzrelevanter, aber zumindest optional auch anderer – Inhaltsformen geeignetes Kategoriensystem zu entwickeln und andererseits bereits im Entwicklungsprozeß Klarheit über die Praxis der Einordnungen gerade bei schwierig zu beschreibenden Seiten – dynamische Inhalte, Nachrichten – abzustimmen. Dabei sind Ausnahmen für solche Seiten kritisch, da sie zum Unterlaufen des Systems genutzt werden können.

In diesem Prozeß können auch bereits Anforderungen an die Software erarbeitet werden. Die Koordinierungsstellen müssen dafür sorgen, daß die Software für alle Anbieter und Abrufer verfügbar ist. Denkbar wäre hier z.B. die Verteilung durch die Access-Provider. Sie haben außerdem für ausreichende Erläuterungen zur einfachen Verwendung zu sorgen und eine Betreuungsstelle für Probleme mit der Software einzurichten.

---

230 An dieser Stelle sollte man über eine Anonymisierung des kritisierenden Abrufers nachdenken, um die Diskussion möglichst immer über eine der Koordinierungsstellen zu führen.

6.3.2 Motivation

Neben der generell erforderlichen Öffentlichkeitsarbeit, die die Problematik des Jugendschutzes im Internet und die für die neuen Medien allgemein erforderliche Neukonzeption der Medienkompetenz ins Bewußtsein rückt, bietet das dargestellte Konzept verschiedene Effekte, die als Motivation und Durchsetzungswerkzeug verwendet werden können.

6.3.2.1 Gesellschaftliche Mechanismen

Als ersten Schritt könnten z.B. alle öffentlichen Verwaltungen mit gutem Beispiel vorangehen und ihre Seiten einstufen. Wenn möglich, sollten auch die privaten Organisationen, die an der Entwicklung des Kategoriensystems beteiligt waren, so vorgehen.[231]

Des weiteren empfiehlt es sich, eine erweiterte Medienkompetenz auch für nicht jugendliche Surfer zu fördern, die die allgemeine Nutzung des Internet verbessert. Ergänzende Maßnahmen erhöhen damit die Relevanz und so auch die Nutzung des Ratingsystems.[232]

Die durch ein solches System zu erwartende Popularisierung der digitalen Signatur – quasi als Übung, da das Sicherheitsniveau nicht so hoch ist wie bei anderen Anwendungen – kann möglicherweise auch andere Nutzungsmöglichkeiten der digitalen Signatur fördern.

6.3.2.2 Logos

Um das technische System ins Bewußtsein der Internetnutzer zu rücken und Anbietern die Werbung mit ihrer Beteiligung am System zu erlauben, kann es sinnvoll sein, Anbietern die Möglichkeit einzuräumen, ein entsprechendes Logo in ihre Seiten einzublenden. Das Logo soll lediglich einen Hinweis auf eine erfolgte Einordnung geben; es sollte kein "Gütesiegel“ für jugendfreie Seiten sein, sondern nur die Tatsache, daß eine Einordnung existiert, neutral dokumentieren. Zusätzliche Logos für bestimmte Einordnungen sind denkbar. Alle Logos sind markenrechtlich so zu schützen, daß eine mißbräuchliche Verwendung geahndet werden kann.

Um die Qualität einer Einordnung zu markieren, ist für kommerzielle Rating-Provider die Einblendung eines Logos "diese Seite wurde von xyz eingestuft“ als verpflichtend vorzusehen. So kann der Abrufer erkennen, auf wessen Einstufung seine Filterung beruht.

6.3.2.3 Motivation von Anbietern

Im Rahmen der aktuellen Jugendschutzdiskussionen taucht bei privaten und kommerziellen Anbietern immer wieder die Frage auf, wie sie sich im Rahmen des Jugendschutzrechts so verhalten können, daß sie keine Probleme befürchten müssen. Wird nun mit dem vorgeschlagenen Konzept eine "sichere“ Vorgehensweise definiert, werden viele Anbieter froh über eine solche Möglichkeit sein und sie nutzen. Ist dann die Technik so konzipiert, daß sie möglichst wenig Fehler machen können, ist eher mit einer schnellen Verbreitung zu rechnen.

Eine weitere Motivation für alle Anbieter ist die Möglichkeit, die Kennzeichnung zur gezielten Suche nach bestimmten Inhalten zu nutzen. Ihre gekennzeichneten Inhalte finden also eher den Weg zum gewünschten Publikum als Seiten ohne Label. Zur Umsetzung dieses

---

231 Dies ist wohl eine realistische Annahme. So haben sich einige Online-Dienste bereits dazu geäußert, daß sie ihre Inhalte nach existierenden Systemen bewerten wollen.

232 Viele Anbieter verwenden bereits heute sogenannte "Meta-Tags“ zur Angabe von Schlagworten zu ihren Internet-Seiten, die das Suchen von bestimmten Seiten erleichtern. Derselbe Zweck kann mit einem Ratingsystem erreicht werden.

Ansatzes ist die bereits genannte Integration der PICS-Label als Suchkriterien in die Suchmaschinen kommerzieller Anbieter sehr wichtig.[233]

Das letzte Argument gilt in besonderem Maße für kommerzielle Anbieter. Die gezielte Suche nach jugendgefährdenden, also z.B. pornographischen Angeboten, wäre genauso möglich. Entsprechend eingeordnete Seiten könnten möglicherweise – je nach Inhalt – sogar auf die bisher erforderliche Eingangsseite mit Warnungen verzichten und dort schon Werbung für ihre Angebote machen.

Die wünschenswerte Verbreitung des Kategoriensystems läßt sich außerdem dadurch unterstützen, daß die Zielgruppen erweitert werden: Es wäre neben einem *Kinder-Netz* ein *Auto-Netz*, eine *Computer-Netz* und auch ein *Erotik-Netz* möglich, alle auf Basis der Auswahl nach entsprechenden Kennzeichnungen. Damit würde neben dem Jugendschutz auch die allgemeine Verwendbarkeit des Internet gesteigert.

In diesem Kontext ist es außerdem erforderlich, daß Internet-Suchmaschinen eine Suchmöglichkeit nach den entsprechenden oder auch allen PICS-Labeln bieten – analog zu den jetzt bereits verfügbaren Keywords.

6.3.3 Rechtliche Perspektive

Im Kapitel 2 haben wir bereits ausführlich die Positionen der beteiligten Gruppen dargestellt. In diesem Abschnitt soll daher nur eine kurze Einordnung des hier entwickelten Konzeptes in den existierenden Rahmen erfolgen.

6.3.3.1 Verantwortlichkeit

Die gesamte Verantwortung für die Ausführung der systemrelevanten Vorgänge liegt im vorgeschlagenen System beim Anbieter und beim Abrufer. Der Anbieter soll eine Einordnung seiner Inhalte vornehmen,[234] der Abrufer wählt daraufhin qualifiziert aus.

Es liegt keine technische Funktion und damit auch keine Verantwortung bei Mittlern (Access-Provider, Presence-Provider) vor, außer möglicherweise die Wahrnehmung einiger Verteilungsdienste (Software, Zertifikat, Hotline).

Wer am Filterprozeß beteiligt ist, übernimmt damit auch für seinen Bereich die Verantwortung. Dies trifft insbesondere diejenigen, die die inhaltliche Einordnung übernehmen (Anbieter oder auch Third-Party-Rating-Dienste), aber auch andere Bereitsteller von Labels oder Filtertechnologie.

6.3.3.2 Recht auf Grundversorgung

Generell besteht durch den Aufbau einer Infrastruktur zum Filtern von Information die Gefahr einer mißbräuchlichen Verwendung. Ein solcher Mißbrauch wäre insbesondere die generelle Filterung des Internet für bestimmte, nicht jugendliche Benutzer.

Prinzipiell kann und darf es private Anbieter solcher vorgefilterten Inhalte geben *(Kinder-Netz*, *Auto-Netz*, *Bücher-Netz*, *Erotik-Netz*, *deutschsprachiges Netz* ...). Jedoch muß für jeden erwachsenen Nutzer an jedem Ort und jederzeit ein ungefilterter Zugang zum Internet

---

233 Dies wird zur Zeit mit der Begründung nicht unterstützt, daß damit auch eine invertierte Suche, z.B. nach explizit jugendgefährdendem Material, ermöglicht würde.

234 Auch eine fehlende Kennzeichnung kann in dem hier vorgeschlagenen System als Basis für eine Auswahlentscheidung benutzt werden, z.B. für eine Sperrung, die allerdings konfigurierbar zu halten ist.

bestehen und jeder Anbieter muß immer die Möglichkeit haben, Inhalte anzubieten – auch ohne Rating.

Daher ist ein solcher "freier“ Zugang im Rahmen der Grundversorgung von staatlicher Seite sicherzustellen.

6.3.3.3 Datenschutz

Wenn alle Anbieter die Einordnung lokal auf ihren Seiten vornehmen, fallen keine zusätzliche Nutzerdaten an.

Der Anbieter muß seine Identität auch nach geltender Rechtslage durch ein Impressum preisgeben (Anbieterkennzeichnung); die digitale Signatur ändert daran nichts.

Alle Filterprozesse des Abrufenden laufen auf seinem lokalen System ab; zusätzliche personenbezogene Daten fallen also nur hier an, weder beim Anbieter noch auf dem Übertragungsweg. Anforderungen des Datenschutzes in Schulnetzen u.ä. werden durch das System nicht berührt.

Wird die Einordnung hingegen von einem Server abgefragt, entstehen dabei genaue Profile mit Benutzerkennung und URL, für die die Einordnung abgefragt wurden. Da die Verwendung eines solchen Providers aber im Endausbau des Systems für keinen Abrufer oder Anbieter zwingend ist, liegt es in der freien Entscheidung eines Endbenutzers, Verträge jeder Art mit solchen Providern abzuschließen und der Verwendung persönlicher Daten zuzustimmen oder sie abzulehnen.

6.3.4 Aufwandsschätzung

Durch eine geeignete Wahl des Gültigkeitszeitraums von Schlüsselzertifikaten und weitgehend automatisierte Verfahren für die Zertifikatsausstellung und den Zertifikatsrückruf kann der Aufwand auch bei 10 Millionen Zertifikaten in Deutschland (und möglicherweise 200 Millionen Zertifikate in der EU) in einem realistischen Rahmen gehalten werden. Zusätzlich sollte auf der Seite des Abrufers im Filterprogramm die Möglichkeit bestehen, die Gültigkeitsdauer von Zertifikats-Rückruflisten (CRLs) zu konfigurieren, um den durch den Abruf von CRLs entstehenden Kommunikationsaufwand zu begrenzen. Auch der Einsatz von Teil-CRLs und *CRL Distribution Points* sollte im technischen Konzept erwogen werden.

6.4 Technik

Die folgende Abschnitte beschreiben die erforderlichen technischen Komponenten im Detail.

Dabei sollte berücksichtigt werden, daß das vorgeschlagene Technikkonzept weder den Anspruch hat noch die Möglichkeit besitzt, eine vollständig unumgehbare Filterung zu gewährleisten.

Mit dem definierten Konzept ist aber eine vertretbar zuverlässige Filterung nach Kriterien des Jugendschutzes (oder auch anderen) möglich, die im Rahmen der vom Jugendschutzrecht geforderten Zumutbarkeit ausreichend ist.

6.4.1 Kategoriensystem

Aus den technischen Untersuchungen hat sich ergeben, daß ein Kategoriensystem dann gut zur Einordnung und Auswahl von Seiten zu verwenden ist, wenn es sowohl grobe als auch feine Einstufungen zuläßt. Über ausführliche Befragung der potentiellen Nutzer – das sind in diesem Falle Anbieter *und* Abrufer von Internet-Informationen – sollte hier eine geeignetes System entworfen werden.

Vordringlich sind inhaltliche Einordnungen erforderlich; als Ergänzung – und nur vorsichtig zu verwenden, weil ein Teil der Auswahlkompetenz dabei vom Abrufer auf den Anbieter übergeht – sind subjektive Kategorien wie Alterseignung sinnvoll. Gerade für diesen Typ sind exakte Definitionen der Kategorien erforderlich. Außerdem ist das System so zu konzipieren, daß nur dann Einordnungen in subjektive Kategorien möglich sind, wenn diese Einstufung zusätzlich zu einer wertneutralen, beschreibenden Kategorieauswahl durchgeführt wird.

Bei der Formulierung des Systems ist darauf zu achten, daß wertneutrale Vokabeln auch für die Einstufung solcher Seiten gefunden werden, die unter Gesichtspunkten des Jugendschutzes als gefährdend einzustufen wären. Nur so ist die Akzeptanz auch bei derartigen Anbietern durchzusetzen.

Außerdem ist auch bei der Formulierung der Einordnungspolicy auf Klarheit und Neutralität größter Wert zu legen. Ziel muß es sein, die Einordnungen soweit zu neutralisieren, daß sich jeder Abrufer aus seinen eigenen Kultur- und Moralvorstellungen ein individuelles, befriedigendes Konzept von Jugendschutz zusammenstellen kann. Hier wäre zu prüfen, inwieweit sich moralische Vorstellungen durch wertneutrale Kriterien abbilden lassen oder ob besondere kulturelle oder moralisch wertende Kategorien erforderlich sind.

Technisch sind zusätzlich die folgenden Punkte zu standardisieren:

- Einbinden der Einordnung (sinnvollerweise auf Basis von PICS mit den notwendigen Erweiterungen),
- Auslesen der Kennzeichnung,
- Importkonzept in Browser,
- Auslesen von Ratings bei Rating-Providern.

Um existierende Strukturen zu nutzen, wäre eine automatisierte Übertragungsmöglichkeit anderer existierender Systeme (vgl. Kapitel 4.5) wünschenswert. Dazu müssen die Regeln definiert und im Browser implementiert sein.)

6.4.2 Anbieter

Für den Anbieter sind die Definition von Regeln zur Einordnung und Kennzeichnung und Werkzeuge zu deren Durchführung erforderlich.

Die Regeln zur Einordnung wurden bereits im Abschnitt über Kategoriensysteme diskutiert. Konkretisierungen zur Kennzeichnung und zu einigen denkbaren Funktionen der Werkzeuge finden sich im folgenden.

Wegen der Wichtigkeit werden wir die Maßnahmen zur Sicherung der Authentizität und Integrität in einem separaten Abschnitt diskutieren.

6.4.2.1 Kennzeichnungssystem

Das Kennzeichnungssystem muß eine technische Plattform zur Formulierung von Kategoriensystemen und zur (HTML-)Codierung der Seiteneinordnungen sein. Wichtig ist, daß es einen Standard für die Signatur von Einordnung und Seite gibt. Außerdem sollte das Zertifikat selbst in der Seite enthalten sein, um bei der Prüfung keine Zugriffe z.B. auf einen Directory Service zu erfordern.

Eine bereits existierende und gut verwendbare technische Plattform zur Formulierung und Übertragung von Kennzeichnungen bietet PICS. Hier ist eine Konkretisierung bezüglich der Signaturen erforderlich, die bereits im Gange ist. Außerdem sind Konzepte für verschiedene, z.B. dynamische Internetseiten weiterzuentwickeln.

Sollen außerdem Rating-Provider – vgl. nächster Abschnitt – zugelassen sein, ist zusätzlich die Standardisierung der Kennzeichnungsabfrage bei diesen Providern nötig.

Um die Kennzeichnung zu erleichtern, sollten Kennzeichnungen von Servern und Directories möglich sein. Hier müßte eine geeignete Möglichkeit gefunden werden, auch diese Inhalte zu signieren.

Es sollten zudem automatisierte Verfahren entwickelt werden, die auf Anbieterseite die Einordnung und das digitale Signieren dynamisch erzeugter Seiten ermöglichen.[235] Dabei darf der Aufwand für die dynamische Erstellung eines Labels nicht unzumutbar steigen. Der PICS-Standard ist dazu in seiner aktuellen Form nur bedingt geeignet, da die Anforderungen, die er an Form und Position des Labels stellt, bei einer dynamischen Erzeugung kaum einzuhalten sind.

6.4.2.2 Seitengenerierung

Statische Webseiten werden im allgemeinen mit HTML-Editoren erstellt. Um die Hemmschwelle für die Bewertung möglichst niedrig zu machen, sollte für Editoren eine automatische Funktion zur Einordnung und zum digitalen Signieren der Seite entwickelt werden.

Diese Funktion soll mit einfachen graphischen Mitteln ("Schieberegler“) eine Einordnung der erstellten Seite in das Kategoriensystem ermöglichen. Um ein unabsichtliches Vergessen zu vermeiden, ist eine Warnung bzw. ein Hinweis beim Abspeichern einer Seite ohne Label denkbar.[236] Eine Einbindung eines Logos zur Kennzeichnung der erfolgten Bewertung sollte möglich sein.

Technisch könnten diese Funktionen durch die Hersteller der Editoren, aber auch durch ein kostenfreies, z.B. von staatlicher Seite zur Verfügung gestelltes PlugIn, realisiert werden.

Auch für die Erstellung von dynamische Seiten muß eine Integration der definierten Verfahren (vgl. vorhergehender Abschnitt) erfolgen.

6.4.3 Abrufer

Der Abrufer braucht ein Filterwerkzeug, daß als Konfiguration eine Auswahl aus den Kategorien des Systems zuläßt und dann daraufhin entscheiden kann, welche Seiten angezeigt werden und welche nicht. Dabei sollte der Abrufer entscheiden können, ob nicht eingeordnete Inhalte grundsätzlich dargestellt oder grundsätzlich nicht dargestellt werden. Es sollte einstellbar sein, wie der Abrufer auf die Tatsache eine Filterung hingewiesen wird. Insbesondere darf eine Sperrmeldung nicht so aussehen wie eine Fehlermeldung. Denn dann ist weder die Aktivierung des Filters transparent für den Abrufer, der sich vielleicht gar nicht über die Filterung im klaren ist, noch ist ein sinnvoller Support durch Betreiber des Abrufsystems oder Access-Provider möglich.

Die Auswahl anhand von Kategorien sollte ergänzt werden können durch Positiv- oder auch Negativlisten (z.B. Freischaltung von Pressetickern, internationalen Seiten o.ä.) und andere in den entsprechenden Teilen dieser Studie dargestellten Filtermechanismen.

Der Abrufer muß außerdem die Möglichkeit haben, auch andere Dienste als WWW soweit möglich jugendgerecht zu behandeln.

---

235 So könnte z.B. in einem Warenhauskatalog die Einordnung von der Art der dargestellten Ware abhängen (Kinderspielzeug bekäme eine andere Einstufung als Kondome), von der Möglichkeit der Online-Bestellung und von der Preiskategorie.

236 Es muß allerdings weiterhin auch möglich sein, Seiten ohne Einstufung zu erstellen. Ob die Einstufungsfunktionalität überhaupt aktiv wird, könne z.B. in den Einstellungen des Editors konfigurierbar sein.

Schließlich muß alle Software hinreichend manipulationssicher sein; hier sind unterschiedliche Anforderungen je nach Einsatzort (Privathaushalt, Schule, Öffentlichkeit) zu erfüllen.

Die Grundlagen zur Authentifizierung werden in einem späteren Abschnitt erörtert.

6.4.3.1 Browser

Da der Webzugang im allgemeinen über einen Browser erfolgt, sollte die für den Jugendschutz erforderliche Funktionalität dort integriert werden. Es muß also ein PlugIn zur Verfügung stehen, das die Signaturprüfung durchführt und dann aufgrund der Kennzeichnung über die Darstellung der Inhalte entscheidet.[237]

Um die Benutzbarkeit zu erhöhen, ist es sinnvoll, graphische Elemente zur Signalisierung einer aktiven Filterung zu verwenden. Auf diesem Weg können auch die Einordnungen der aktuellen Seiten angezeigt werden, z.B. in Form zusätzlicher Logos in der Statuszeile (analog zur Kennzeichnung von verschlüsselten SSL-Verbindungen).

6.4.3.2 Manipulationssicherheit

Die heutzutage eingesetzten Rechner weisen häufig keine große Manipulationssicherheit auf. Dies bedingt, daß aufgesetzte Filterprogramme leicht zu deaktivieren oder zu umgehen sind. Eine absolute Sicherheit gibt es in diesem Bereich nicht. Jedoch kann ein Betreiber eines Abrufsystems z.B. in einer Schule recht viele zusätzliche Maßnahmen treffen, um die Sicherheit vor einer Manipulation durch die Nutzer zu erhöhen:

- Sperren der Diskettenlaufwerke, sofern sie nicht benötigt werden,
- Verwenden eines Betriebssystems, das Zugriffsberechtigungen und Authentifizierungsmechanismen wie Paßwörter unterstützt,
- Restriktive Vergabe von Zugriffsberechtigungen, so daß keine mitgebrachten oder zugesandten Programme ungesichert ausgeführt werden können (hierzu gehören auch Makros, die Makroviren enthalten können),
- Schutzsysteme vor Viren und trojanischen Pferden, auch für Mail-Attachments,
- Unterbinden einer ungesicherten Ausführung von aktiven Inhalten im WWW (ActiveX, Java, JavaScript).

Bei Filterung der Inhalte am Nutzer-PC kommt hinzu, daß die Daten erst vollständig auf den Rechner geladen werden müssen, damit vor der Auswahlentscheidung die digitale Signatur über Dokument und Einordnung geprüft werden kann. Hier wird es nicht möglich sein, die Daten immer vollständig im Arbeitsspeicher zu halten; zur Zeit (beispielsweise beim MS Internet Explorer) liegen die geladenen Daten in einem Cache-Bereich der Festplatte und sind dort über das Dateisystem zugreifbar gemäß den Sicherheitsrichtlinien des Betriebssystems[238].

Der technische Schutz muß durch organisatorische Maßnahmen ergänzt werden. Der Betreiber muß z.B. Sorgfalt beim Umgang mit Administrationspaßwörtern walten lassen. Auch sollte er sich über bekanntgewordene Sicherheitslücken informieren und Gegenmaßnahmen treffen. Gerade in kleinen Netzen an Schulen, in Bibliotheken oder Internet-Cafés bietet sich der Einsatz von Netz-PCs an, so daß bei jedem Neustart die Konfiguration der Rechner von einem Server, der geschützt in einem verschlossenen Raum steht, wiederhergestellt wird und keine lokalen Datenbestände angelegt werden können.

---

237 Letzeres wird von gängigen Browsern für bekannte Ratingsysteme bereits durchgeführt (vgl. Kapitel "Ratingsysteme“).

238 Bei Betriebssystemen ohne lokale Sicherheit also uneingeschränkt.

6.4.4 Sicherung von Integrität und Authentizität

Den organisatorischen Hintergrund für die Authentifizierung haben wir bereits beschrieben (vgl. 6.3.1.1).

In diesem Abschnitt sind daher nur noch einige Punkte aufgeführt, die für die lokale Durchführung der Signaturerzeugung und -verifikation erforderlich sind.

- Der technische Vorgang der Schlüsselgenerierung und -zertifizierung sollte möglichst automatisiert geschehen. Es ist zu prüfen, ob es sinnvoll ist, hier die Access-Provider in die technische Funktionalität einzubeziehen. Auf jeden Fall ist die vom Nutzer selbst zu bedienende Software so einfach zu gestalten, daß sie auch technisch nicht versierte Nutzer nicht ausschließt.
- Um eine aufwendige Zertifikatsverteilung und vor allem große lokale Zertifikatslisten zu vermeiden, sollten die Zertifikate in der signierten Seite enthalten sein. Nur die Schlüssel der Zertifizierungsstelle selber müssen vorher auf einem sicheren Kanal übertragen werden; dies könnte z.B. im Rahmen der Softwareverteilung geschehen.
- Zur Erhöhung der Performance sollte beim Abrufer über eine besondere Behandlung häufig gebrauchter Zertifikate und Schlüssel nachgedacht werden. Zum Beispiel könnten diese Schlüssel lokal gespeichert werden; eine wiederholte Übertragung könnte damit eventuell entfallen. Im Rahmen der Gültigkeitsprüfung könnte man kritische Schlüssel definieren, deren Gültigkeit besonders häufig überprüft wird, wogegen für andere vertrauenswürdige Schlüssel das Intervall zwischen den Überprüfungen länger gewählt wird.
- Statt einer Verzeichnisdienst-basierten CRL-Verteilung und -Prüfung könnte auch ein Protokoll zur Online-Prüfung von Zertifikaten eingesetzt werden (z.B. Online Certificate Status Protocol – OCSP). Dabei besteht allerdings die Möglichkeit, daß wiederum Benutzerprofile anfallen.
- Die Sicherheitsanforderungen an die Schlüssel und Zertifikate sind niedriger als bei anderen Infrastrukturen. Daher ist die Handhabung von Zertifikaten und Rückruflisten weniger kritisch; auch können z.B. die Lebensdauern von Rückruflisten länger gewählt werden. Insgesamt kann auch ein Schlüssel aus einer anderen Infrastruktur verwendet und im Rahmen der hier verwendeten Infrastruktur lediglich ein weiteres Mal zertifiziert, also beglaubigt werden. Damit ist ein Entzug der Singnierbefugnis für die Einordnung von Webseiten möglich, ohne die sonstigen Verwendungszwecke des Schlüssels und seiner weiteren Zertifikate einzuschränken.
  Inwieweit aufgrund der reduzierten Sicherheitsanforderungen eine Verwendung eines separaten Schlüssels sinnvoll ist – der weniger aufwendig gesichert werden muß – ist im Einzelfall zu überprüfen.

6.5 Medienkompetenz

Um eine nicht nur technisch, sondern auch inhaltlich effektive Nutzung des Internet zu unterstützen, bestehen verschiedene Möglichkeiten zum Aufbau von Medienkompetenz. Dabei soll sowohl für die zu schützenden Minderjährigen als auch für die den Schutz konfigurierenden Personen – also Eltern oder Lehrer – die technische Filterung durch ein komplementäres, positives Angebot relevanter Inhalte ergänzt werden.

6.5.1 Internetportal für Kinder und Jugendliche

Zum einen sind spezielle Internetportale für Kinder und Jugendliche denkbar. Solche Anbieter würden nur den Zugang zu jugendfreiem Material erlauben, würden aber darüber hinaus dieses jugendfreie Angebot speziell aufbereiten und möglicherweise auch durch eigene Angebote ergänzen.

Neben speziellen Inhalten wären hier Link-Sammlungen möglich; auch eine eigene Suchmaschine, die ausschließlich aus nicht jugendgefährdenden Inhalten auswählt, ist hier sinnvoll.

6.5.2 Hilfen für Erziehungsberechtigte

Eine Lehrseite für Erwachsene (Eltern, Lehrer) sowie eine Einführung in den Jugendschutz und die Funktionsweise des Internet sollten die Darstellung ergänzen

Weiterhin könnten schulische Stellen Konfigurationsbeispiele für Schulen und Home-PCs zur Verfügung stellen, die neben der Filtereinstellung auch Listen von besonders für Kinder und Jugendliche geeigneten Seiten enthalten und Hinweise auf Unterrichtsmaterial machen. Falls diese Seiten nicht gekennzeichnet sind (wovon bei internationalen Seiten auszugehen ist), könnten solche staatlichen Stellen auch ein Third-Party-Rating vornehmen und technisch zur Verfügung stellen.

6.6 Grenzen des Ansatzes

In verschiedenen Bereichen stößt der Ansatz an Grenzen. Zum Teil lassen diese sich durch weitere Entwicklungen beseitigen. Zum einem weiteren Teil sind sie jedoch systematisch bedingt und können daher nur abgeschwächt, aber nie ganz beseitigt werden.

6.6.1 Beschränkung auf WWW

Generell können alle Dienste im Internet zur Übertragung jugendgefährdender Inhalte genutzt werden. Eine technische Begrenzung ist aber nur für WWW sinnvoll, da Dienste wie News oder Chat quasi einer Unterhaltung zwischen zwei Personen entsprechen, die zu schnell und flüchtig ist, um sie effektiv kontrollieren zu können.
Für News wäre aus technischer Sicht die Verwendung digitaler Signaturen prinzipiell möglich. Allerdings ist der Übertragungsaufwand relativ gesehen ungleich größer als bei WWW-Diensten. Außerdem ist Anonymität beim Versenden häufiger vorhanden und auch gewünscht; daher eignen sich konventionelle digitale Signaturen dafür nicht.
In den News ist der größte Teil des potentiell jugendgefährdenden Materials schon am Namen der News-Group erkennbar; daher kann eine Sperrung dieser Gruppen oder eine explizite Freigabe bestimmter, zumindest thematisch unproblematischer Gruppen schon recht erfolgreich sein. Zusätzliche einfache Filter z.B. zur Unterbindung selbstöffnender Hyperlinks gewährleisten dann einen ausreichenden Schutz.
Zur Erleichterung für den Abrufer ist eine Liste von jugendgeeigneten News-Groups denkbar.

6.6.2 Umgehung, Fehler

Prinzipiell sind Filter auf lokalen Maschinen immer zu umgehen; alle Maßnahmen können nur den dafür erforderlichen Aufwand erhöhen.
Auch zufällige oder absichtliche Fehler beim Rating lassen sich nicht immer vermeiden, da der Kontrollmechanismus langsam ist. Vor dem Einschreiten einer Koordinierungsstelle wird die Seite oder der Server immer eine gewisse Zeit lang mit falscher Einstufung verfügbar sein.

6.6.3 Software

Geeignete Software ist bisher nicht verfügbar; es wird daher einige Zeit dauern, bis die Software entwickelt ist und für die Endbenutzer zur Verfügung steht.

6.6.4 Aufwand

Im Gegensatz zum ungefilterten Internet entsteht ein höherer Aufwand: Es ist eine zentrale Infrastruktur erforderlich, der Anbieter muß seine Seiten einstufen, der Abrufer muß zusätzliche Software verfügbar haben und während des Internetabrufs die Filterfunktionen zusätzlich ausführen.

Neben diesem technischen Aufwand sind außerdem organisatorische Anreize zur Anwendung des Systems zu schaffen.

6.7 Gefahren

Da ein Filterungskonzept gleich welcher Art – insbesondere dann, wenn es sich besonders gut gegen Mißbrauch schützen kann – immer auch Gefahren politisch-gesellschaftlicher Art birgt, sind solche Aspekte beim Entwurf und Betrieb des geschilderten Systems immer im Auge zu behalten.

6.7.1 Umgang mit nicht eingeordneten Seiten

Eine Auswahl durch Filterung funktioniert allerdings nur, wenn Aktionen für nicht eingeordnete Inhalte definiert sind. Wie man sich leicht überlegen kann, ist es zur Erzielung von Jugendschutz sinnvoll, nicht eingeordnete Seiten zu sperren. Damit ist "Jugendschutz“ sofort hergestellt: Alle möglicherweise gefährlichen Seiten sind entweder nicht eingeordnet oder nicht mit einem zulässigen Label versehen und daher auch nicht mehr erreichbar. Die Sicht des Teilnehmers hinter dem Filter auf das Netz präsentiert ein vollkommen jugendfreies Netz. Damit ist aber auch das Internet als solches nicht mehr insgesamt sichtbar, weil auch eine riesige Menge jugendfreier, aber nicht eingeordneter Seiten nicht mehr erreichbar ist.

Die vorgeschlagene Einordnung von Seiten durch Rating-Services hat in dieser Konfiguration nur den Zweck, die *nicht* jugendgefährdenden Seiten für die Jugendlichen wieder erreichbar zu machen, d.h. für Jugendliche hinter Filtersystemen überhaupt wieder ein Internet sichtbar zu machen. Konsequenterweise müssen also die Anbieter von jugendfreien Seiten besonders motiviert werden, ihre Seiten einzuordnen und diese Einordnung so jugendfrei wie rechtlich möglich zu machen, damit diese Seiten für Kinder und Jugendliche wieder zur Verfügung stehen. Mit der Einordnung von Inhalten ist allerdings auf jeden Fall ein Aufwand für ihren Anbieter verbunden. Derzeit ist unklar, mit welcher rechtlichen Legitimation den Anbietern von unkritischen Inhalten im Internet dieser Aufwand zugemutet werden könnte.

Generell muß der Umgang mit nicht eingeordneten Seiten lokal z.B. durch Lehrer und Eltern einstellbar sein. So wäre es denkbar, daß Eltern im Hinblick auf den Entwicklungsstand ihrer Kinder individuell entscheiden, wie mit nicht eingeordneten Seiten umgegangen werden soll. Ein achtjähriges Kind könnte z.B. nur Zugang zu eingeordneten Seiten erhalten, wogegen dem Zwölfjährigen zusätzlich bestimmte Bereiche (deutsche Seiten, bestimmte Sammlungen, die aller Voraussicht nach nicht jugendgefährdend sind) zugänglich sind und die Sechzehnjährige schon Zugang zu allen nicht eingeordneten Seiten erhält, die nicht auf einer Liste von besonders jugendgefährdenden Seiten zu finden sind.

6.7.2 Beschreibung von Inhalten

Eine andere Beschränkung von Rating- und Labelingsystemen ergibt sich aus der Tatsache, daß Inhalte beschrieben werden müssen: Solche Systeme stellen eine Metrik für Inhalte dar. Die Definition der Metrik selbst definiert eine Art Koordinatensystem, bei dem sich die Autoren von Inhalten zum Zwecke der Einordnung ihrer Inhalte nur *innerhalb* dieses Koordinatensystems bewegen können.

Einige Anbieter kontroverser Inhalte haben schon erklärt, daß sie keinesfalls innerhalb eines solchen Koordinatensystems Position beziehen möchten, weil ihnen die "Nachbarn“, also ähnlich eingeordneten Inhalte, unter Umständen nicht gefallen:

- Aus http://www.msen.com/~weinberg/rating.htm, "Rating the Internet“:
  'Jonathan Wallace, thus, in an article called "Why I Will Not Rate My Site“ asks how he is to rate "An Auschwitz Alphabet“, his powerful and deeply chilling work of reportage on the Holocaust. The work contains descriptions of violence done to camp inmates' sexual organs. A self-rating system, Wallace fears, would likely force him to choose between the unsatisfactory alternatives of labeling his work as suitable for all ages, on the one hand, or "lump[ing it] together with the Hot Nude Woman page“ on the other. It seems to me that at least some of the rating services problems' in assigning ratings to individual documents are inherent. It is the nature of the process that no ratings can classify documents in a perfectly satisfactory manner, and this theoretical inadequacy has important real-world consequences.'
- Aus http://www.dcia.com/cyberbur.html, "Fahrenheit 451.2: Is Cyberspace Burning?“:
  'Kiyoshi Kuromiya, founder and sole operator of Critical Path Aids Project, has a web site that includes safer sex information written in street language with explicit diagrams, in order to reach the widest possible audience. Kuromiya doesn't want to apply the rating "crude“ or "explicit“ to his speech, but if he doesn't, his site will be blocked as an unrated site. If he does rate, his speech will be lumped in with "pornography“ and blocked from view. Under either choice, Kuromiya has been effectively blocked from reaching a large portion of his intended audience - teenage Internet users - as well as adults. [...] Kuromiya could distribute the same material in print form on any street corner or in any bookstore without worrying about having to rate it. In fact, a number of Supreme Court cases have established that the First Amendment does not allow government to compel speakers to say something they don't want to say – and that includes pejorative ratings.'

Metriken haben umgekehrt starke Auswirkungen auf Inhalte und Form von Websites, die nicht unbedingt in der Intention derjenigen lagen, die die Metrik einmal definiert und etabliert haben. So gibt es zum Beispiel Anbieter von Werbebannerservern, die andere Inhaltsanbieter für das Anzeigen von Werbebannern bezahlen. Die Bezahlung ist um so höher, je öfter das Werbebanner aufgerufen wird (Metrik: Anzahl der Abrufe). Derartige Dienste sind bei Anbietern von Erotikseiten sehr beliebt, weil Erotikseiten sehr hohe Seitenabrufzahlen haben. Um die Anzahl der Seitenabrufe weiter zu steigern, setzen die Anbieter der Sexseiten JavaScript-Code ein, der für jedes vom Seitenabrufer geschlossene Fenster zwei neue Fenster öffnet. Auf diese Weise werden weitere Werbebanner geladen, die Anzahl der Seitenabrufe also gesteigert. Die ursprüngliche Intention der Metrik, nämlich die Anzahl der Personen zu zählen, die die Werbung tatsächlich gesehen haben, spielt hier keine Rolle mehr – es liegt eine dysfunktionale Metrik vor.

Es ist zu erwarten, daß die Anbieter von solchen Angeboten die ihnen auferlegte Metrik sehr genau analysieren und ihre Angebote derart optimieren werden, daß sie als möglichst jugendfrei eingestuft werden, um eine möglichst große Reichweite zu haben. Ähnliche Effekte sind aus der Filmindustrie bekannt, in denen Filme durch Erotik- und Actionszenen möglichst attraktiv gemacht werden sollen, ohne die Altersfreigabe "frei ab 12“ oder "frei ab 16“ zu überschreiten, um auf diese Weise den Kreis der potentiellen Kunden nicht schon im Vorfeld zu beschränken. Sähe ein Einordnungssystem also Ausnahmen (weniger strenge Maßstäbe) für Anbieter von Nachrichtenservices oder Communities vor, ist zu erwarten, daß sehr viele Anbieter von nicht jugendfreien Angeboten auf eine Darstellungsform wechseln, die sie in die Kategorie von Nachrichtenservices oder Communities fallen läßt. Auch wäre es wettbewerbsverzerrend, wenn Anbietern wie den "Top 100“ Ausnahmen beim Einordnen zugestanden würden.

6.7.3 Mißbrauch

Ein Beispiel für einen solchen Mißbrauch von Technologie durch ein totalitäres Regime ist der bereits genannte Versuch der chinesischen Regierung, für ihre Dissidenten den Zugang zum Internet zu sperren bzw. zu zensieren.

Das zugrunde liegende Problem ist, daß die auf diese Weise unter der Überschrift "Jugendschutz“ etablierte Filterstruktur in ihrem Zweck nicht konstruktionsbedingt festgelegt ist, sondern durch bloße Veränderung der Filterkriterien in ein totalitäres Instrument verwandelbar ist. Diese Wandlung ist unter Umständen so subtil, daß der genaue Zeitpunkt der Wandlung nicht festgestellt werden kann. Das Internet wird als Medium der politischen Diskussion unbrauchbar, wenn in diesem Medium, in dem über die Gesellschaft und ihre Regeln diskutiert wird, einige Diskussionsteilnehmer die existierenden Filtermechanismen möglicherweise nutzen können, um den Verlauf der Diskussion steuern. Daher ist es unbedingt notwendig, daß sich Erwachsene leicht und jederzeit beweisbar ungefilterten Zugang zum Netz verschaffen können.

Das z.B. in PICS vorgesehene System, das Label mit optionaler digitaler Signatur und PICS-Rules enthält, liefert alle Elemente, die notwendig sind, um eine (ggf. auch totalitäre) politische Kontrolle über das Internet auszuüben: Durch die Definition eines geeigneten Kategoriensystems würde der passende Bezugsrahmen geschaffen, um mißliebige Inhalte zu erfassen und zu bewerten. Label können auch ohne jegliche Kooperation mit dem Anbieter durch Dritte vergeben werden. Durch die digitale Signatur der Labels sind diese nicht fälschbar und auch nicht durch dynamische Generierung der Inhalte zu unterlaufen. PICS-Rules erlauben es schließlich, die Proxies und Filter der zugelassenen Provider und Nutzer zentral zu steuern. Dadurch, daß PICS-Rules auch die Kommunikation von Filterregeln an Suchmaschinen erlaubt, wird dem Nutzer seine Einschränkung unter Umständen nicht einmal bewußt, da auch die Suchmaschinen keine Treffer auf Seiten mehr liefern, die nach der PICS-Einstellung für diesen Anwender sowieso nicht erreichbar wären. "Any content-based regulation of the Internet, no matter how benign the purpose, could burn the global village to roast the pig.“[239]

Da ein solcher Mißbrauch nicht durch technische Maßnahmen unterbunden werden kann, sind die geschilderten organisatorischen Kontrollen notwendig und wichtig. Insbesondere muß auch die Garantie für Erwachsene auf ungefilterten Zugang zum Internet überprüft werden.

239 Judge Stewart Dalzell, ACLU -v- Reno, 11 June 1996, Nach dem Communications Decency Act-Urteil (http://www.aclu.org/court/renovacludec.html), zitiert unter http://rene.efa.org.au/liberty/label.html.