Thomas Günter/Friedemann Schindler

Technische Möglichkeiten des Jugendschutzes im Internet

1 Einführung

Das Internet stellt den Jugendschutz vor besondere Herausforderungen und erfordert neben neuen gesetzlichen Regelungen auch die Entwicklung geeigneter technischer Schutzmaßnahmen. Internet-Angebote unterliegen keiner Vorabkontrolle wie Trägermedien, deren Alterseignung vor ihrer Veröffentlichung durch Selbstkontrollen geprüft und bei denen der Jugendschutz über Verkaufsbeschränkungen realisiert wird. Internet-Angebote sind zulassungsfrei, selbst Privatleute können ihre Angebote im Internet mit geringem finanziellen und organisatorischen Aufwand betreiben oder über Austauschplattformen zur Verfügung stellen. Anders als im Bereich des Rundfunks brauchen Anbieter keine Lizenz, deren Gewährung auch an die Einhaltung gesetzlicher Jugendschutzbestimmungen geknüpft ist. Im Unterschied zu den traditionellen Medien ist das Internet auch ein grenzüberschreitendes Medium, in dem nur ein kleiner Teil des weltweit verfügbaren Angebots Jugendschutzregelungen unterliegt, die bezüglich des Schutzniveaus mit den deutschen vergleichbar sind. Angesichts der Besonderheiten des Internets mit seiner grenzüberschreitenden Vielfalt und hohen Dynamik spielen technische Schutzmaßnahmen zur Gewährleistung des Jugendschutzes eine größere Rolle als in den traditionellen Medien. Viele Dienste des Internets wären ohne entsprechende technische Hilfen inzwischen praktisch nicht mehr nutzbar (z.B. E-Mail, Suchdienste).

Milliarden an Web-Seiten, die sich regelmäßig ändern, und Internet-Dienste, in denen Nutzer die Inhalte selbst generieren, stellen für technische Schutzmaßnahmen eine besondere Herausforderung dar. Technische Lösungen können den Jugendschutz im Internet nicht vollständig garantieren und pädagogische Begleitung bzw. die Medienerziehung von Kindern und Jugendlichen nicht ersetzen. Mit technischer Hilfe sind Gefährdungs- und Beeinträchtigungspotentiale aber reduzierbar: Bekannte unzulässige Angebote können blockiert, altersdifferenzierte Zugänge gewährt und problematische Kommunikationsakte leichter identifiziert werden.

Der Jugendmedienschutz-Staatsvertrag (JMStV), der am 01.04.2003 in Kraft getreten ist, sieht ein abgestuftes System von Anbieterpflichten vor, die geforderten Schutzmaßnahmen orientieren sich an der Jugendschutzrelevanz der präsentierten Inhalte (Schließung oder Sperrung). Das Zugänglichmachen absolut unzulässiger Angebote (z.B. Gewaltpornografie, Rassismus) ist generell untersagt. Bei jugendgefährdenden Inhalten (z.B. einfache Pornografie, indizierte Angebote) sind deutsche Anbieter zur Sicherstellung verpflichtet, dass Minderjährige nicht zugreifen können (Einrichtung einer Geschlossenen Benutzergruppe nur für Erwachsene). Anbieter von Websites, die Kinder und Jugendliche in ihrer Entwicklung beeinträchtigen können (z.B. Erotik-Sektionen großer Portale, Download von Demoversionen für Spiele ohne Jugendfreigabe), müssen Sorge dafür tragen, dass Minderjährige üblicherweise nicht auf diese Inhalte zugreifen können (Vorschaltung eines technischen Schutzes, Programmierung für ein anerkanntes Jugendschutzprogramm).

jugendschutz.net beschäftigt sich seit seiner Gründung im Jahre 1997 intensiv mit technischen Schutzlösungen und bewertet ihre Leistungsfähigkeit im praktischen Einsatz. Bereits 1997 hat jugendschutz.net Anforderungen für Geschlossene Benutzergruppen formuliert, um den Konsum von Pornografie auf Erwachsene zu beschränken. Bei deutschen Porno-Angeboten sind verlässliche Altersprüfungen inzwischen gebräuchlich. Die Anforderungen an Verifizie-

rungssysteme sind seit In-Kraft-Treten des JMStV auch gesetzlich fixiert und von der Kommission für Jugendmedienschutz (KJM) im Detail spezifiziert. Seit 1999 hat jugendschutz.net in verschiedenen Projekten die Wirksamkeit von Jugendschutzfiltern für das Internet recherchiert. Auch an der europäischen Diskussion (z.B. über die Beiratstätigkeit im Rahmen von Filterprojekten der EU-Kommission) und der Weiterentwicklung technischer Schutzlösungen (z.B. Filtersysteme für interaktive und mobile Dienste) beteiligt sich jugendschutz.net. Seit 2006 betreibt jugendschutz.net im Auftrag der KJM ein Prüflabor, in dem die Verlässlichkeit von Altersverifikationssystemen und die Wirksamkeit von Jugendschutzfiltern getestet werden.

2 Sperrung absolut unzulässiger Angebote

Darstellungen harter Pornografie (z.B. Kinder- und Gewaltpornografie), rassistische Hetze (z.B. volksverhetzende Inhalte) oder Darstellungen, die die Menschenwürde verletzen und Gewalt verherrlichen (z.B. Snuff- und Enthauptungsvideos[1]), dürfen nach dem JMStV auch über das Internet grundsätzlich nicht verbreitet und zugänglich gemacht werden. Dieses Verbot ist bei deutschen Angeboten vergleichsweise einfach durchzusetzen, weil die Anbieter der Inhalte (Content-Provider) und die Betreiber des Webservers, über den die Inhalte ins Netz gestellt werden (Host-Provider), einfach zu identifizieren und verantwortlich zu machen sind. Falls Content- oder Host-Provider der Aufforderung zur Einhaltung des Jugendschutzes durch jugendschutz.net nicht nachkommen, kann die zuständige Landesmedienanstalt nach Feststellung eines Verstoßes durch die KJM die Löschung oder Sperrung des Angebots verfügen.

Sperrung unzulässiger Angebote durch Host-Provider

Wesentlich schwieriger stellt sich die Situation bei ausländischen Angeboten dar. Hier gibt es nur im Bereich der Kinderpornografie weltweite Verbotsregelungen, die zwar im Detail Abweichungen aufweisen, in den meisten Fällen aber zu einer Strafverfolgung der Anbieter und zur Schließung von Angeboten führen. Bei anderen Inhalten, die nach deutschem Recht absolut unzulässig sind, kontaktiert jugendschutz.net zuständige Stellen im Sitzland des Anbieters[2] oder versucht über den Host-Provider eine Schließung der Angebote zu erreichen. Insbesondere im Bereich unzulässiger rechtsextremer Propaganda ist die Kontaktaufnahme mit den Host- und Service-Providern häufig erfolgreich, weil viele die Nutzung ihrer Dienste zur Verbreitung von so genannter Hate Speech in ihren Geschäftsbedingungen untersagen. Inzwischen gelingt es so jugendschutz.net in 75 % der Fälle, rechtsextremen Angeboten auch im Ausland die Plattform zu entziehen.[3]

Einstellung von Service-Leistungen für illegale Angebote

Wenn Anbieter versuchen, mit absolut unzulässigen Inhalten Geld zu verdienen (z.B. mit dem Verkauf sexualisierter Darstellungen posierender Kinder), spricht jugendschutz.net die Betreiber von Abrechnungsdiensten an (z.B. Visa, Mastercard). Sie stellen ihren Service in der Regel

---

1 Snuff-Videos zeigen reale Tötungshandlungen zum Zweck der Unterhaltung der Zuschauer.

2 jugendschutz.net ist neben der Freiwilligen Selbstkontrolle Multimedia (FSM) und des Verbandes der deutschen Internetwirtschaft (eco) Gründungsmitglied des europäischen Verbundes von Beschwerdestellen (INHOPE), dem inzwischen 25 Hotlines in 23 Ländern angeschlossen sind. Daneben ist jugendschutz.net auch Mitglied des Internationalen Netzwerks gegen Cyber Hate (INACH), dem seit der Gründung im Jahre 2003 bereits 13 anti-rassistische Initiativen beigetreten sind.

3 Siehe hierzu den Bericht 2005 des entimon-Projektes „Rechtsextremismus im Internet – die Plattform entziehen und eine medienkompetente Auseinandersetzung fördern“ bei jugendschutz.net, abrufbar unter http://www.jugendschutz.net/pdf/Projektbericht2005.pdf.

sofort ein, da die Unterstützung des Handels mit unzulässigen Inhalten ihrer Unternehmensphilosophie widerspricht. So kann den Anbietern absolut unzulässiger Inhalte zumindest die finanzielle Basis entzogen werden, die in vielen Fällen die Hauptmotivation für das Betreiben solcher Angebote darstellt.[4]

Löschung unzulässiger Adressen aus dem Index von Suchmaschinen

Insbesondere bei so genannten Tasteless-Sites, die die Menschenwürde verletzende und unzulässige Gewaltdarstellungen präsentieren[5], sind über ausländische Host-Provider derzeit keine Erfolge zu erzielen. Gerade diese Angebote weisen aber eine besondere Jugendschutzrelevanz auf, da sie von Kindern und Jugendlichen vielfach als virtuelle Mutproben genutzt werden. In diesen Fällen besteht nur die Möglichkeit, die Nutzung zu blockieren oder zumindest die Auffindbarkeit zu erschweren. So haben sich die Betreiber großer deutscher Suchmaschinen beispielsweise selbst verpflichtet, entsprechende Fundstellen aus ihren Suchindexen zu löschen.[6] Bei dieser technischen Schutzlösung kommt die Liste der Bundesprüfstelle für jugendgefährdende Medien (BPjM) zum Einsatz, die den Suchmaschinen die Adressen der indizierten Telemedien zur Verfügung stellt. Seit der Implementierung des so genannten BPjM-Moduls sind z.B. die 76.000 Fundstellen, die derzeit im amerikanischen Google-Index zur bekanntesten Tasteless-Site verzeichnet sind, im deutschen Google-Index nicht mehr zu finden.

Sperrmaßnahmen von Zugangs-Providern und Backbone-Betreibern

Eine wirkliche Verhinderung des Zugriffs auf absolut unzulässige Angebote im Ausland ist nur Zugangsanbietern und Backbone-Betreibern (so genannte Access-Provider) möglich[7]. Sie können den Zugriff auf einschlägige Adressen wirksam blockieren. Notwendig sind entsprechende technische Schutzmaßnahmen vor allem bei so genannten Type-In-Angeboten, die nicht über Suchmaschinen gefunden werden. Adressen bekannter Tasteless-Angebote werden z.B. auf Schulhöfen getauscht und direkt in den Browser eingegeben. Im Mediendienste-Staatsvertrag (MDStV) wird eine generelle Verantwortlichkeit der Access-Provider richtigerweise verneint, da sie keine Kenntnis von unzulässigen Angeboten haben, die über ihren Zugang genutzt oder in ihrem Netz verteilt werden. Gleichwohl fordert der MDStV auch von Access-Providern Schutzmaßnahmen, sofern sie ihnen technisch möglich und zumutbar sind. Die technischen Möglichkeiten sowie die Frage der Zumutbarkeit lässt die KJM derzeit prüfen. Die KJM ist auch für den Erlass von Sperrverfügungen gegen Access-Provider zuständig.[8]

Im Zuge der Berichterstattung über Gewaltvideos auf den Handys von Jugendlichen und verstärkter Bemühungen gegen die Quellen dieser Darstellungen im Internet vorzugehen, ist es jugendschutz.net 2005 erstmals gelungen, einen Access-Provider (Backbone-Betreiber Level3) zu einer freiwilligen Sperrung zu veranlassen. In der Folge hatten deutsche AOL- und Arcor-Kunden, die über das Netz von Level3 geroutet werden, keinen Zugriff auf die bekannteste

---

4 Siehe dazu Frankfurter Rundschau: „Blutige Geschäfte – Deutsche Jugendschützer gehen gegen eine 'Snuff'-Seite auf einem US-amerikanischen Server vor“ vom 09.07.2005, abrufbar unter http://www.jugendschutz.net/news/200507/news_05-07-11_12-26-30_ap.html.

5 Tasteless-Sites sind Angebote, die „Geschmacklosigkeiten“ präsentieren. Die Bandbreite reicht von harmlosen Inhalten bis zu die Menschenwürde verletzenden Bildern von sterbenden oder schwer leidenden Menschen zum Zwecke der Belustigung der Nutzer.

6 Siehe dazu den Verhaltenssubkodex für Suchmaschinenanbieter, die sich in der FSM organisiert haben, unter http://www.fsm.de/de/Subkodex_Suchmaschinenanbieter.

7 Als Backbone bezeichnet man die Hauptstränge eines Netzwerks, die kleinere Teilnetze verbinden.

8 Siehe dazu das Interview mit dem Vorsitzenden der KJM, Prof. Wolf-Dieter Ring: Sperrverfügungen im Web als äußerstes Mittel denkbar, abrufbar unter http://www.heise.de/ct/hintergrund/meldung/43117.

Tasteless-Site.[9] Im Rahmen freiwilliger Selbstverpflichtungen der Zugangsanbieter werden in einigen europäischen Ländern bereits umfangreiche Blockaden vorgenommen.[10] So hat z.B. British Telecom eine technische Schutzlösung (Cleanfeed) entwickelt, um den Zugang auf unzulässige Inhalte zu blockieren, die nach englischem Recht als illegal zu bewerten sind. Die Sperrliste wird von der Internet Watch Foundation (IWF) erstellt.[11] Eine ähnliche technische Schutzlösung wird auch in Norwegen von der staatlichen Telekom eingesetzt. Hier stellt die Polizei die Sperrliste zur Verfügung.[12]

3 Geschlossene Benutzergruppe für jugendgefährdende Inhalte

Geschlossene Benutzergruppen für Erwachsene sind die wichtigste technische Maßnahme des Jugendschutzes. In den vergangenen Jahren sind in diesem Bereich nicht nur wesentliche gesetzliche Verbesserungen erzielt worden, auch das faktische Schutzniveau hat sich erhöht, weil pornografische Inhalte von deutschen Anbietern zunehmend nur noch für Erwachsene zugänglich sind. Mit In-Kraft-Treten des JMStV wurde für das Internet erstmalig die Möglichkeit gesetzlich geregelt, bestimmte unzulässige Inhalte unter Erlaubnisvorbehalt in Geschlossenen Benutzergruppen für Erwachsene zu präsentieren. Nach § 4 Absatz 2 Satz 2 JMStV ist ein Zugänglichmachen von (einfach) pornografischen, indizierten und sonstigen offensichtlich schwer jugendgefährdenden Inhalten im Internet nur dann zulässig, wenn der Anbieter sicherstellt, dass die Inhalte nur Erwachsenen zugänglich gemacht werden (Geschlossene Benutzergruppe). In der Praxis wird diesen Angeboten ein technischer Schutz (so genannte Altersverifikationssysteme) vorgeschaltet, der gewährleisten soll, dass Kinder und Jugendliche nicht zugreifen können. Jahrelang umstritten war, welche Anforderungen an Altersverifikationssysteme zu stellen sind. Nachdem die KJM als zuständige Medienaufsicht für das Internet die Anforderungen spezifiziert hat und diese durch zahlreiche Gerichtsentscheidungen bestätigt wurden, ist dieser Streit mittlerweile im Wesentlichen entschieden.

Anforderungen der KJM

Die KJM hat mit Beschluss vom 18.06.2003 die Anforderungen konkretisiert, die Systeme erfüllen müssen, um ein Sicherstellen im Sinne des § 4 Absatz 2 Satz 2 JMStV zu gewährleisten. Demnach ist der Zugangsschutz durch zwei Schritte zu gewährleisten:

- durch eine Volljährigkeitsprüfung, die über persönlichen Kontakt erfolgen muss (**Identifizierung**)
- durch **Authentifizierung** bei jedem Nutzungsvorgang, um das Risiko einer Weitergabe von Zugangsdaten an Minderjährige wirksam zu reduzieren.

Die Volljährigkeitsprüfung über persönlichen Kontakt dient der sicheren Identifikation und Altersfeststellung von natürlichen Personen. Dabei ist unter „persönlichem Kontakt" verpflichtend ein Vergleich mit amtlichen Ausweisdaten und die Erfassung dieser Daten in einer Daten-

---

[9] Siehe dazu die Heise-Meldung: IP-Carrier Level3 sperrt Website auf Router-Ebene vom 25.08.2005, abrufbar unter http://www.heise.de/newsticker/meldung/63214.

[10] Siehe zur Diskussion über so genannte ISP-Sperrungen auf europäischer Ebene die Dokumentation der Veranstaltung der EU-Kommission: „Illegal Content: Blocking access to child sexual abuse images", abrufbar unter http://europa.eu.int/information_society/activities/sip/si_forum/forum_june_2006/agenda/index_en.htm.

[11] Siehe dazu die Heise-Meldung: British Telecom will Webseiten blockieren vom 06.06.2004, abrufbar unter http://www.heise.de/newsticker/meldung/47988.

[12] Siehe dazu die Heise-Meldung: Norwegische Polizei und Telenor entwickelten Kinderpornofilter vom 21.09.2004, abrufbar unter http://www.heise.de/newsticker/meldung/51318.

bank zu verstehen. Neben der Identifizierung durch geschultes Personal (z.B. in DHL-Filialen per PostIdent-Verfahren[13] oder am Point-of-Sales von Mobilfunk-Anbietern) kommen auch andere Varianten der Volljährigkeitsprüfung in Betracht, die eine ausreichende Verlässlichkeit bieten (z.B. Vergleich von Personendaten mit besonders qualifizierten Schufa-Daten, die nach dem Geldwäsche-Gesetz erhoben wurden, in Verbindung mit einer persönlichen Zustellung der Zugangsdaten).

Die Authentifizierung dient der Sicherstellung, dass nur identifizierte und altersgeprüfte Personen Zugang zur Geschlossenen Benutzergruppen erhalten, und soll die Weitergabe von Zugangsdaten an unautorisierte Dritte erschweren. Um die Vervielfältigung von Zugangsdaten zu verhindern, wird in der Regel eine Hardwarekomponente eingesetzt, die nur mit hohem Aufwand zu kopieren ist (z.B. Chip-, Geld- oder SIM-Karte, kopiergeschützte CDs/DVDs, Bauteile eines PCs mit eindeutiger ID-Adresse wie beispielsweise Netzwerkkarten). Um die Weitergabe von Zugangsdaten wirksam zu unterbinden, sind zusätzlich subjektive Risiken für den autorisierten Nutzer vorzusehen. Dies geschieht in der Regel dadurch, dass mit den Zugangsdaten für Geschlossene Benutzergruppen auch erhebliche finanzielle Risiken verknüpft werden (z.B. Bezahlfunktion für Produkte, die in der Geschlossenen Benutzergruppe oder angeschlossenen Partner-Shops angeboten werden).

Der JMStV enthält keine Regelung zur rechtsverbindlichen Zertifizierung von Schutzkonzepten für Geschlossene Benutzergruppen durch die KJM.[14] Allerdings ist die KJM im Rahmen ihrer allgemeinen Zuständigkeit zur Überprüfung der Einhaltung der Bestimmungen des JMStV nach §§ 14, 16 JMStV dazu übergegangen, Auskünfte zu Schutzsystemen nach § 4 Absatz 2 Satz 2 JMStV zu erteilen. Systeme werden gegebenenfalls positiv bewertet, wenn diese durch die Industrie zur Prüfung vorgelegt werden und den Anforderungen des JMStV entsprechen. Mittlerweile hat die KJM 14 Konzepte für komplette Systeme sowie für einzelne Module zur Sicherstellung einer Geschlossenen Benutzergruppe positiv bewertet.[15]

Anforderungen der Rechtsprechung

Die bisher ergangene Rechtssprechung zu Fragen einer geeigneten Altersverifikation stützt eine restriktive Auslegung des Merkmals des „Sicherstellens“ nach § 4 Absatz 2 Satz 2 JMStV im Sinne der KJM-Richtlinie.[16] Nach Auffassung des BVerwG ist eine zuverlässige Alterskontrolle anzunehmen, „wenn vor oder während des Vertragsschlusses ein persönlicher Kontakt mit dem späteren Kunden“ besteht und „zumindest eine weitere, im System angelegte effektive Vorkehrung“ getroffen wird, die die Weitergabe von Zugangsdaten wesentlich erschwert.[17] Der BGH hat in einer Strafrechtsentscheidung zu Videoverleihautomaten eine technische Alterskontrolle nur dann als ausreichend erachtet, wenn die technische Kennung nur an Erwachsene ausgegeben wird und zusätzlich weitere Zugangshindernisse im System integriert sind.[18]

---

[13] Im Post-Ident-Verfahren erfolgt eine zuverlässige Identifizierung eines Kunden im Rahmen eines persönlichen Kontakts durch Mitarbeiter der Post z.B. in einer Post-Filiale.

[14] Im Gegensatz dazu sieht der JMStV im Bereich der Jugendschutzprogramme in § 11 Absatz 2 JMStV eine Anerkennung durch die KJM ausdrücklich vor.

[15] Siehe hierzu die Zusammenstellung der Systeme mit positiver Auskunft auf der Website der KJM http://www.kjm-online.de/public/kjm/index.php?show_1=91,85,56.

[16] Eine Zusammenstellung zur Thematik findet sich bei *M. Döring/T. Günter*, Alterskontrollierte geschlossene Benutzergruppen im Internet gem. § 4 Absatz 2 Satz 2 JMStV, MMR 4/2004, S. 231 ff., abrufbar unter http://www.jugendschutz.net/materialien/mmr_avs.html.

[17] BVerwG NJW 2002, 2966 mit Anm. *T. Hörnle*.

[18] BGH MMR 2003, 582 mit Anm. *M. Liesching*.

Konkret mit der Vorschrift des § 4 Absatz 2 Satz 2 JMStV haben sich in letzter Zeit vor allem Straf- und Zivilgerichte beschäftigt. Das Kammergericht Berlin verurteilte einen Angeklagten mit Urteil vom 26.04.2004 zur Zahlung einer Geldbuße wegen Zugänglichmachens von pornografischen Angeboten entgegen § 4 Abs. 2 Satz 1 Nr. 1, Satz 2 des JMStV. Das Kammergericht verlangte in seiner rechtskräftigen Revisionsentscheidung entsprechend den Urteilen von BVerwG und BGH eine wirksame Schutzbarriere und sah eine Volljährigkeitsprüfung mittels Personalausweisnummer als untaugliches Mittel an.[19] Auch das OLG Düsseldorf hat als Revisionsinstanz in einem Strafurteil ausgeführt, dass eine effektive Barriere bestehen muss.[20] Im Rahmen eines Wettbewerbsverfahrens zwischen Anbietern von Altersverifikationssystemen hat sich das OLG Düsseldorf als Berufungsinstanz der überwiegenden Ansicht in Rechtsprechung und Literatur ebenfalls angeschlossen.[21] Allerdings steht die Revisionsentscheidung des BGH in diesem Fall noch aus.

Geschlossene Benutzergruppen in der Praxis

Geschlossene Benutzergruppen finden sich im Internet bisher vor allem im Bereich einfach pornografischer Angebote. Frei zugängliche pornografische Inhalte sind in Deutschland zunehmend seltener zu finden. Es gibt aber immer noch viele Angebote, die pornografische oder jugendgefährdende Darstellungen in Geschlossenen Benutzergruppen präsentieren, die den Vorgaben des JMStV nicht entsprechen. Das Sicherheitsniveau von Altersüberprüfungen ist seit In-Kraft-Treten des JMStV jedoch deutlich gestiegen. Erfreulicherweise spielt die unzureichende und von der Mehrheit der Anbieter pornografischer Inhalte jahrelang praktizierte Altersfeststellung per Perso-Check[22] keine große Rolle mehr. Die meisten Altersverifikationssysteme bieten mittlerweile auch eine Variante an, bei der die Identität eines Nutzers mittels persönlichen Kontakts (z.B. per PostIdent-Verfahren) überprüft wird. Große Defizite sind weiterhin im Bereich der Authentifizierung festzustellen. Zumeist können pornografische Angebote nach Eingabe von Login&Passwort betreten werden und verfügen damit über keinen ausreichenden Weitergabeschutz für Zugangsdaten.

Geschlossene Benutzergruppen wären auch bei anderen Internet-Angeboten sinnvoll einzusetzen, die ausschließlich Erwachsenen zugänglich sein dürfen (z.B. Glückspiele, Spielbanken, Online-Lotterien), sowie im Online-Verkauf von Produkten, die nur an Erwachsene verkauft werden dürfen (z.B. branntweinhaltige Getränke, Spiele und Videos, die für Kinder und Jugendliche nicht freigegeben sind).[23]

Umgang mit jugendgefährdenden Angeboten im Ausland

Im Bereich der jugendgefährdenden Inhalte, die über das Ausland ins Internet gestellt werden, gibt es derzeit keine wirksame Handlungsmöglichkeit für Kontrolleinrichtungen wie jugendschutz.net bzw. für die Internet-Aufsicht. Aufgrund der Fülle der Angebote führt ein Vorgehen gegen einzelne Angebote zu keiner spürbaren Verbesserung des Jugendschutzes. jugendschutz.net leitet bekannt gewordene Fälle zwar an Partner-Meldestellen im Ausland weiter, in der Regel bleibt dies jedoch ohne Erfolg, weil viele Organisationen nur gegen absolut unzuläs-

---

19 KG Berlin, Urteil vom 26.4.2004, AZ (5) 1 Ss 436/03 (4/04).

20 OLG Düsseldorf, Urteil vom 17.02.2004, AZ III-5 Ss 143/03 – 50/03 I.

21 OLG Düsseldorf, Urteil vom 24.05.2005, AZ I-20 U 143/04.

22 Prüfung des Alters an Hand der Personalausweis-Kennziffer, die auch Angaben zum Geburtsdatum des Ausweisinhabers enthält.

23 Siehe hierzu auch die Rechtsauffassung und Praxishinweise der Obersten Landesjugendbehörden zum Versandhandel nach § 1 Abs. 4 Jugendschutzgesetz (JuSchG), abrufbar unter http://www.mbjs.brandenburg.de/media/lbm1.a.1222.de/versandhandel_0905.pdf.

sige Inhalte vorgehen. Hier bedarf es künftig vor allem einer intensiveren internationalen Diskussion über den Jugendschutz und der Festlegung länderübergreifender Schutzstandards. jugendschutz.net versucht, jugendgefährdenden Websites im Ausland zumindest die Plattform in Deutschland zu entziehen oder ihre Auffindbarkeit so weit wie möglich zu reduzieren. Wichtige Ansatzpunkte sind hier die Bewerbung und Verlinkung ausländischer Angebote auf deutschen Portalen oder ihre Listung in deutschen Suchmaschinen.

4 Jugendschutzfilter bei beeinträchtigenden Angeboten

Neben der Blockade absolut unzulässiger und jugendgefährdender Angebote im Ausland besteht die Hauptaufgabe von Jugendschutzfiltern in der Gewährleistung eines altersdifferenzierten Zugangs zu entwicklungsbeeinträchtigenden Inhalten.

In Analogie zur Altersklassifizierung im Bereich der Trägermedien forderten zunächst die Jugendminister die Entwicklung von Jugendschutzfiltern, die ein nach Altersgruppen abgestuftes System von Surfräumen ermöglichen.[24] Diese Forderung hat auch im JMStV ihren Niederschlag gefunden. Dieser verpflichtet Anbieter in § 5 JMStV erstmals, bei entwicklungsbeeinträchtigenden Angeboten altersdifferenzierte Zugänge zu gewähren und Sorge dafür zu tragen, dass Kinder und Jugendliche Angebote „üblicherweise nicht wahrnehmen", die Minderjährige der jeweiligen Altersgruppe beeinträchtigen können. Neben einer entsprechenden Begrenzung der Sendezeit und der Vorschaltung von technischen Mitteln sieht der Gesetzgeber in § 11 JMStV ausdrücklich vor, dass Anbieter ihr Angebot für ein von der KJM anerkanntes Jugendschutzprogramm programmieren können.[25]

Vorgaben der KJM an Jugendschutzprogramme

Die KJM hat die Anforderungen für die Anerkennung von Jugendschutzprogrammen nach § 11 JMStV konkretisiert. Demnach reicht es nicht aus, wenn Jugendschutzprogramme die Fähigkeit besitzen, effizient zu filtern. Sie müssen auch faktisch eingesetzt werden, um ihre Schutzwirkung zu entfalten. Wichtige Prüfpunkte der KJM sind deshalb neben der Effizienz der Filterung auch die Akzeptanz von Jugendschutzprogrammen durch Eltern und Pädagogen (z.B. Kosten, Aufwand für Beschaffung, Installation, Konfiguration und Updates) sowie die gesellschaftliche Akzeptanz der Kriterien, die der Filterung zu Grunde liegen. In jedes Klassifizierungs-Schema fließen die moralischen und politischen Wertvorstellungen der Hersteller ein, dementsprechend gibt es gravierende Unterschiede zwischen den verwendeten Schemata.[26] Gerade Filtersysteme aus den USA basieren häufig auf Wertesystemen, die mit europäischen Vorstellungen nicht (vollständig) kompatibel sind. Beispielsweise blockieren sie häufig jede Diskussion über Sexualität,[27] während die Themenbereiche Gewalt und Rechtsextremismus wesentlich liberaler als in Deutschland gehandhabt werden.

---

[24] Bei der Klassifizierung und Filterung von Internetangeboten sollte „ein Empfehlungsraum für Vorschul- und Grundschulkinder, ein Schutzraum für ältere Kinder und junge Jugendliche und ein Surfraum für ältere Jugendliche (…) zugrunde gelegt werden." (siehe Beschluss der Jugendministerkonferenz vom Mai 2003: „Konzeption zur Entwicklung einer effektiven Kinderschutzsoftware").

[25] Gemäß § 11 Abs. 3 JMStV ist Jugendschutzprogrammen die Anerkennung zu erteilen, „wenn sie einen nach Altersstufen differenzierten Zugang ermöglichen oder vergleichbar geeignet sind."

[26] Die wenigsten Filterhersteller dokumentieren und begründen ihre Klassifizierungssysteme. In der Regel sind auch keine Aussagen zu finden, wie bei Klassifizierungsproblemen verfahren wird und welche Instanzen letztlich darüber entscheiden, welcher Kategorie ein Web-Angebot zugeordnet wird.

[27] Häufig blockiert werden z.B. auch spezielle Aufklärungsangebote für Jugendliche wie Sextra von ProFamilia oder Loveline der Bundeszentrale für gesundheitliche Aufklärung.

Grundkonzepte der Filterung von Web-Seiten

Filtersysteme sind technische Schutzmaßnahmen, die den Zugriff auf Informationen oder Dienste des Internets nach vorgegebenen Kriterien regulieren. Sie können auf dem Rechner des Nutzers, auf einem zentralen Internet-Rechner einer Institution (z.B. auf einem Proxy-Server einer Schule) oder auf den Rechnern eines Zugang-Providers (z.B. AOL) installiert sein und unterschiedliche Aktivitäten auslösen: vor problematischen Seiten warnen, den Weg durch das Netz im Detail aufzeichnen, inkriminierte Seiten blockieren oder sogar einen Rechner komplett ausschalten. Sie basieren auf wenigen Grundkonzepten:

- redaktionelle Klassifizierung. Positivlisten lassen nur kindgeeignete Angebote zu, die von einer Redaktion begutachtet und ausgewählt wurden. Umgekehrt blockieren Negativlisten alle Angebote, die bei händischer Sichtung als jugendschutzrelevant eingestuft wurden.

- automatische Klassifizierung. Hier entscheiden Algorithmen darüber, ob ein Angebot zugänglich ist oder nicht. Die einfachste Form ist das Keyword-Blocking, das alle Seiten sperrt, die bestimmte Forbidden Words enthalten. „Intelligentere" Filtersysteme werten verschiedene typische Merkmale einer Web-Seite aus (z.B. statistische Analyse des gesamten Textes einer Web-Seite), um sie automatisiert zu kategorisieren.

- Selbstklassifizierung der Anbieter. Jeder Anbieter versieht seine Web-Seiten mit einem virtuellen Kennzeichen, das die Inhalte klassifiziert. Eine Software auf dem Rechner des Nutzers liest das Label aus und entscheidet an Hand der Nutzereinstellungen, ob das Angebot angezeigt wird oder nicht.

Diese Grundkonzepte der Filterung werden inzwischen vielfach kombiniert, um die Wirksamkeit zu erhöhen, aber auch um altersdifferenzierte Zugänge zu schaffen.

Wirksamkeit von Jugendschutzfiltern noch unbefriedigend

Zur Wirksamkeit von Filtersystemen liegen keine belastbaren Vergleichszahlen vor. Es fehlen einheitliche Maßstäbe und standardisierte Testverfahren.[28] Die Filterhersteller verweisen jeweils auf Wirksamkeiten von 95–98 %, es bleibt aber in der Regel unklar, auf welcher Basis diese Zahlen erhoben wurden (z.B. ob nur jugendschutzrelevante Web-Seiten in den Test einbezogen wurden, aus welcher Kategorie von Web-Seiten das Testszenario bestand, wer und nach welchen Kriterien die Testung vorgenommen hat). In den meisten Tests wird eine Trefferquote von 80 % bereits als gutes Ergebnis gewertet, während Eltern und Pädagogen einen Filter wohl kaum als gut bezeichnen würden, der jede fünfte jugendschutzrelevante Seite passieren lässt. Hier gibt es mit der KJM erstmals eine Instanz in Deutschland, die beauftragt ist, Maßstäbe der Bewertung zu entwickeln und zu setzen.

Den letzten umfangreichen Test von Jugendschutzfiltern hat jugendschutz.net vor In-Kraft-Treten des JMStV im Auftrag der Obersten Landesjugendbehörden im Dezember 2002 durchgeführt. Exemplarisch getestet wurden zehn gebräuchliche Filtersysteme, die verschiedene Filtermechanismen repräsentierten. Der Test sollte Hinweise liefern, welche Effektivität beim Sperren jugendschutzrelevanter Webangebote zu erzielen ist (Blocking) und in welchem Umfang dabei auch erwünschte Inhalte blockiert werden (Overblocking). Das Testszenario bestand aus einer Liste mit

[28] Die EU-Kommission hat dazu beispielsweise eine Studie in Auftrag gegeben, die „eine objektive, vom Verkäufer oder Anbieter unabhängige Bewertung der derzeit auf dem Markt angebotenen Filtersoftware und -dienste durch Sachverständige" ergeben soll. (http://europa.eu.int/information_society/activities/sip/programme/workprogramme/index_en.htm).

2.250 Web-Adressen, die nach Jugendschutzrelevanz klassifiziert waren, verschiedene Bereiche repräsentierten (Sex/Pornografie, Gewalt, politischer Extremismus, Bildungsangebote für Kinder und Jugendliche) und mit unterschiedlichen Methoden (Suche in Suchmaschinen, hoch frequentierte Angebote, Empfehlungslisten) zusammengetragen wurden. Die Effizienz der getesteten Filtersysteme war sehr unterschiedlich. Die besseren Systeme zeigten im Bereich Sex/Pornografie zufrieden stellende Ergebnisse, in den Bereichen Rechtsextremismus und Gewalt versagten sämtliche getesteten Jugendschutzfilter. Die wirksamsten Systeme arbeiteten mit automatischen Klassifizierungsverfahren, die sich auch am Surfverhalten der Nutzer orientieren. Die präziseste Filterung gelang Systemen, die automatische Verfahren mit redaktioneller Pflege koppeln.

Die Effizienz verfügbarer Filtersysteme ist insgesamt noch unbefriedigend. Die Zukunft von Jugendschutzfiltern liegt in der Entwicklung von Klassifizierungsmechanismen, die Kontextinformationen stärker berücksichtigen, und in der intelligenten Kombination unterschiedlicher Filterkonzepte. Bessere Ergebnisse sind von Systemen zu erwarten, die automatische Klassifizierungen durch redaktionell erstellte Listen ergänzen und intelligent mit der Selbstklassifizierung der Anbieter verknüpfen. Hier sind insbesondere Inhalteanbieter und Betreiber von Filtersystemen gefordert, bei der Gestaltung ihrer Angebote und Dienste künftig altersdifferenzierte Zugangsmöglichkeiten vorzusehen und die diesbezüglichen Anforderungen des Jugendschutzes besser zu berücksichtigen.

Bisher keine Jugendschutzprogramme mit Anerkennung

Derzeit ist es nicht möglich, Empfehlungen für bestimmte Jugendschutzfilter auszusprechen, da noch kein System von der KJM anerkannt wurde oder seine altersdifferenzierte Wirksamkeit unter vergleichbaren Bedingungen nachgewiesen hat. Die KJM kann vor der Anerkennung von Jugendschutzprogrammen zeitlich befristete Modellversuche mit neuen Verfahren, Vorkehrungen oder technischen Möglichkeiten zur Gewährleistung des Jugendschutzes zulassen. Derzeit werden drei Systeme in Modellversuchen geprüft: ICRAdeutschland (Selbstklassifizierung der Anbieter), Jugendschutzprogramm.de (redaktionell erstellte Blockadeliste für die ICRA-Plattform) und System-I (Kombination von Positivliste für Kinder mit einer automatisch klassifizierten Blockadeliste für Jugendliche). Abhängig vom Ergebnis eines Modellversuchs kann das betreffende Jugendschutzprogramm eine Anerkennung durch die KJM erhalten. Die Modellversuche sind aber grundsätzlich ergebnisoffen. Sie stellen nicht zwingend eine Vorstufe oder gar Garantie für die Anerkennung eines Jugendschutzprogramms dar.

Vorschaltung einer technischen Schutzlösung als funktionierende Alternative

Da noch keine anerkannten Jugendschutzprogramme zur Verfügung stehen, sollten Anbieter von entwicklungsbeeinträchtigenden Darstellungen, die den Anforderungen des JMStV genügen wollen, einen technischen Schutz vorschalten. Die KJM hat bereits verschiedenen Vorschaltsystemen eine positive Auskunft erteilt. Kern dieser technischen Schutzlösungen ist in der Regel die Prüfung der Personalausweis-Kennziffer.

Als positives Beispiel kann die integrierte Schutzlösung von T-Online fungieren, die im Rahmen des neuen Triple-Play-Angebots für den Videos-On-Demand-Dienst entwickelt wurde. Inhalte nach § 4 Absatz 2 Satz 2 sowie alle Filme ohne Jugendfreigabe sind hier nur Erwachsenen in einer Geschlossenen Benutzergruppe zugänglich, während Filme, die Jugendliche beeinträchtigen können, vorgesperrt werden. Die Set-Top-Box, über die das Videoangebot abgerufen wird, liefert T-Online in einer kindersicheren Konfiguration aus, d.h. beeinträchtigende Inhalte sind erst nach Eingabe einer eigens dafür vorgesehenen Jugendschutz-PIN zugänglich.

5 Zusammenfassung und Ausblick

Während die Sperrung absolut unzulässiger deutscher Angebote unproblematisch durchzusetzen ist, scheitert sie bei ausländischen Angeboten häufig an unterschiedlichen rechtlichen Maßstäben. Hier sind technische Blockadelösungen weiter zu entwickeln und nach dem Vorbild der Betreiber von Suchmaschinen entsprechende Selbstverpflichtungen für Access-Provider zu etablieren, um Anbietern absolut unzulässiger Darstellungen wirksam ihre Plattform zu entziehen.

Im Bereich jugendgefährdender Inhalte hat der JMStV Geschlossene Benutzergruppen für Erwachsene als geeignete technische Schutzlösung etabliert. Die KJM hat die Anforderungen an Altersverifikationssysteme spezifiziert; diese Eckpunkte sind inzwischen auch durch Gerichtsurteile bestätigt. Das Schutzniveau bei deutschen jugendgefährdenden Angeboten hat sich bereits deutlich verbessert. Gegen jugendgefährdende Angebote, deren Zugangsschutz den Vorgaben des JMStV noch nicht entspricht, muss weiterhin entschieden vorgegangen werden. Jugendgefährdenden Angeboten aus dem Ausland kann in Deutschland die Plattform wirksam entzogen werden, ansonsten ist ihre Verfügbarkeit nur über Filtersysteme zu reduzieren.

Von Anbietern entwicklungsbeeinträchtigender Darstellungen fordert der JMStV die Einrichtung altersdifferenzierter Zugänge. Bisher hat noch kein dafür vorgesehenes Jugendschutzprogramm seine Wirksamkeit nachgewiesen, potentiell wirksame Filteransätze werden aber im Rahmen von Modellversuchen erprobt. Anbietern beeinträchtigender Darstellungen bleibt derzeit nur die Vorschaltung einer technischen Schutzlösung. Die KJM hat entsprechende Verfahren (z.B. Perso-Check) bereits auf ihre Tauglichkeit geprüft. Derzeit präsentieren selbst namhafte deutsche Portale noch beeinträchtigende Darstellungen ohne ausreichende Schutzvorkehrungen. Die Entwicklung altersdifferenzierter Vorschalt- und Filtersysteme und ihre wirksame Implementierung sind nötig, um im Internet ein vergleichbares Schutzniveau wie in den traditionellen Medien zu erreichen.

Während der Zugang zu Angeboten im World Wide Web relativ einfach zu reglementieren ist, stellen interaktive Dienste wie Chats neue Herausforderungen für die Entwicklung technischer Schutzlösungen dar. Minderjährige werden dort häufig Opfer sexueller Belästigungen und Übergriffe. Wegen der Flüchtigkeit der Chat-Kommunikation sind Chat-Räume nur beschränkt zu kontrollieren. Ihre Betreiber können durch strukturelle und technische Maßnahmen aber ein größeres Maß an Sicherheit gewährleisten. Inzwischen experimentieren einige Chat-Betreiber mit speziellen Filtersystemen, die problematische Kommunikationsakte zwischen Erwachsenen und Kinder identifizieren können. Diese technischen Schutzlösungen dienen nicht der automatisierten Blockade problematischer Inhalte, sondern sollen die Moderation von Chat-Diensten vereinfachen.

Die Diskussion um Gewaltvideos auf Handys verweist auf neue Notwendigkeiten für den Einsatz technischer Schutzmaßnahmen. Mit der Verfügbarkeit internetfähiger Handys und mobiler Spielgeräte wird die Mediennutzung weiter individualisiert und der elterlichen Kontrolle zunehmend entzogen. Angesichts der Tatsache, dass jugendliche Handy-Nutzer künftig ständig online sein werden, muss die Entwicklung wirksamer und nach Altersgruppen differenzierender Schutzmaßnahmen forciert werden. Anbieter sind verstärkt aufzufordern, technische Schutzmaßnahmen nicht nur optional anzubieten, sondern Internetzugänge künftig kindersicher vorzukonfigurieren.

Verf.: Günter, Thomas, Justiziar von jugendschutz.net, Wallstraße 11, 55122 Mainz

Schindler, Friedemann, Leiter von jugendschutz.net, Wallstraße 11, 55122 Mainz