4. Kapitel: Fehlende Durchsetzbarkeit staatlicher Regulierung der Kommunikation digitaler Inhalte

Soweit bestehende Regeln der Inhaltskontrolle auf die Kommunikation digitaler Inhalte übertragen werden können, oder soweit neue Inhaltskontrollvorschriften für diese Inhalte verfassungsgemäß geschaffen werden, müssen sie durchsetzbar sein, um ihren Zweck zu erreichen.

Durchsetzung bedeutet die Einleitung und Durchführung eines Verfahrens, im Rahmen dessen festgestellt wird, ob ein als möglicherweise rechtswidrig identifizierter Inhalt tatsächlich den Tatbestand einer Inhaltskontrollvorschrift erfüllt. Ist dies festgestellt, gehört zur Durchsetzung ebenfalls, die Rechtsfolgen der verletzten Vorschrift anzuwenden.

Die beschriebenen Unterschiede zwischen digitalen und herkömmlichen Medien machen nicht nur die Anwendbarkeit, sondern auch die Durchsetzung staatlicher Regeln der Inhaltskontrolle zunehmend schwieriger: Inhalte liegen nicht mehr regelmäßig in verkörperter Form (Zeitungen, Bücher, Videokassetten) vor, sondern werden unkörperlich verbreitet. Selbst bisher schon unkörperlich verbreitete Inhalte (Telefon-, Faxkommunikation) standen früher regelmäßig im Klartext für die rechtmäßige Inhaltskontrolle (durch Abhören) zur Verfügung, während sie heute ohne Schwierigkeiten versteckt und verschlüsselt kommuniziert werden können. Die Durchsetzung von Inhaltsbindungen kann sich nicht mehr wie früher auf wenige, regelmäßig bekannte und oft institutionalisierte Anbieter (Verlage, Rundfunkveranstalter) beschränken, sondern muß jedermann im Auge haben. Selbst herkömmliche Jedermannskommunikation (Telefon, Flugblätter, Kleinanzeigen) konnte leichter kontrolliert werden, weil sie regelmäßig auf das Inland beschränkt war; heute wird regelmäßig - ohne daß Kosten und Aufwand höher wären - aus und mit dem Ausland kommuniziert. Diese Faktoren erschweren die Identifikation von und den Zugriff auf rechtswidrige Kommunikation und auf ihre Akteure so erheblich, daß bereits von der „Ohnmacht des Staates“ in digitalen Medien gesprochen wurde[735].

I. Verfahrensgebundenheit der Durchsetzung von Inhaltskontrollvorschriften

Die Durchsetzung von Inhaltskontrollrecht ist im Rechtsstaat nur in Verfahren möglich, im Rahmen derer zum einen die Rechtswidrigkeit von Inhalten unter Anwendung der entsprechenden Vorschriften festgestellt wird und zum anderen Sanktionen hinsichtlich der Inhalte (Einziehung, Löschung, Sperrung) und der Verantwortlichen (Verurteilung zu Unterlassung, Schadenersatz, Strafe) angeordnet werden.

735 *Roßnagel*, ZRP 1997, 26; *Depenheuer*, AfP 1997, 669 (671).

Diese Verfahren unterscheiden sich zunächst danach, ob sie der repressiven Ahndung vermuteter Gesetzverstöße dienen oder der präventiven Gefahrenabwehr zuzuordnen sind. Gemäß Art. 5 Abs. 1 S. 3 GG ausgeschlossen sind Verfahren, die die Verbreitung von Inhalten überhaupt von einer vorherigen staatlichen Überprüfung und Genehmigung abhängig machen.[736]

1. Durchsetzung durch repressive Verfahren

Innerhalb der zur repressiven Inhaltskontrolle denkbaren Verfahren ist weiter nach der möglicherweise verletzten Inhaltskontrollvorschrift zu differenzieren:

Die Durchsetzung *strafrechtlicher* Inhaltsbindungen beginnt mit der Eröffnung eines strafrechtlichen Ermittlungsverfahrens. Dieses wird nach Kenntniserlangung vom Verdacht einer Straftat (einfacher Tatverdacht) von der Staatsanwaltschaft eröffnet, vgl. §§ 160 Abs.1, 152 Abs. 2 StPO[737]. Gleiches gilt für strafrechtliche Bestimmungen in anderen Gesetzen.

*Urheber*rechts- und *Wettbewerbs*regeln werden zunächst per Abmahnung durch die Betroffenen selbst und im Streitfall mit zivilgerichtlicher Hilfe durchgesetzt.

Verwaltungsrechtliche Inhaltsbindungen werden zunächst in Verwaltungsverfahren auf Antrag oder von Amts wegen durch die zuständige Behörde durchgesetzt. Ein *jugendschutzrechtliches* Indizierungsverfahren nach dem GjSM wird durch die in § 2 DVGjSM genannten Antragsberechtigten vor der Bundesprüfstelle für jugendgefährdende Schriften anhängig gemacht. Bei behaupteten Verstößen gegen *Datenschutzbestimmungen* kann sich jeder Betroffene an die Aufsichtsbehörden (§ 38 Abs. 1 BDSG) bzw. die Datenschutzbeauftragten (etwa § 21 Abs. 1 BDSG) wenden. Diese ergreifen weitere Maßnahmen, soweit ihnen die Anhaltspunkte für eine Verletzung zureichend erscheinen[738]. Verfahren bei Verstößen von Rundfunkveranstaltern gegen medienrechtliche Inhaltsbindungen des Rundfunkstaatsvertrages richten sich nach §§ 35ff. RStV. §

736 Zum verfassungsrechtlichen Zensurbegriff ausführlich Löffler – *Bullinger*,§ 1 Rn 127ff.

737 Die *Strafverfolgung* gehört nach fester Tradition auch dann zu den repressiven und nicht zu den präventiven Maßnahmen, wenn sie schon *vor* der Verbreitung eines Kommunikationsinhalts einsetzt, falls nach materiellem Strafrecht bereits die *Vorbereitung* oder der *Versuch* der Verbreitung strafbar ist (in diesem Sinne etwa BayVGH NJW 1983, 1339 (1340)). Der Versuch eines Verbrechens ist stets, der Versuch eines Vergehens dann strafbar, wenn das Gesetz es ausdrücklich vorsieht (§ 23 I StGB). Bei manchen schweren Straftaten wird bereits das Vorrätighalten von Druckwerken zwecks späterer Verbreitung unter Strafe gestellt, so für gewaltverherrlichende oder zum Rassenhaß aufstachelnde Schriften nach § 131 StGB. Um den Mißbrauch von Kindern für die Herstellung von Kinderpornographie wirksamer zu bekämpfen, ist sogar deren bloßer Besitz ohne nachweisbare Verbreitungsabsicht unter Strafe gestellt (§ 184 V StGB idF des 27. StrÄG v. 23. 7. 1993, BGBl. I S. 1346). Vgl. Löffler - *Bullinger*, § 1 LPG Rn. 151.

738 Vgl. zum Anwendungskonflikt zwischen § 38 und § 21ff. BDSG oben *bb. Datenschutzrechtlicher Vertraulichkeitsschutz*, S. 109.

18 MDStV regelt die verwaltungsbehördliche Aufsicht über die Einhaltung der speziellen Inhaltskontrollvorschriften für Mediendienste.

Zur Durchsetzungssicherung sind Zuwiderhandlungen gegen die fachbehördlichen Maßnahmen meist straf- oder bußgeldbedroht (vgl. etwa §§ 21 GjSM; 43, 44 BDSG; 49 RStV; 20 MDStV).

Zur Vermeidung weiterer Rechtsverstöße und wiederholter Rechtsverletzungen Betroffener können in diesen Verfahren repressiver Inhaltskontrolle teilweise auch vor endgültiger Feststellung der Rechtswidrigkeit des Inhalts vorläufige Maßnahmen zur Verhinderung weiterer Verbreitung erlassen werden.[739]

Ist die Rechtswidrigkeit des Inhalts endgültig festgestellt, sind drei Sanktionsmöglichkeiten denkbar. Der Inhalt kann entfernt[740], der Zugang zu ihm eingeschränkt werden[741] und – bei einmalig verbreiteten Inhalten die einzig mögliche Sanktion – die Verantwortlichen können zur straf-, ordnungs- oder zivilrechtlichen Haftung herangezogen werden.

2. Durchsetzung durch präventive Verfahren

Nicht immer muß die Einleitung repressiver Verfahren zur Inhaltskontrolle abgewartet werden. So kommt eine präventive Inhaltskontrolle durch möglicherweise Betroffene etwa in Gestalt vorbeugender Unterlassungsklagen im Wettbewerbs- oder Urheberrecht in Betracht[742].

Hauptsächlich findet der präventive Schutz der „öffentlichen Sicherheit und Ordnung" jedoch durch Polizei und Verwaltung unter Anwendung von speziellen Ermächtigungsnormen (etwa § 37 Abs. 1 S. 2 AuslG, Art. 31 BayPAG) oder der polizeilichen Generalklausel (etwa §§ 1, 3 PolGBW) statt. Weil alle gesetzlichen Inhaltskontrollvorschriften als Bestandteile der objektiven Rechtsordnung vom Schutzgut der öffentlichen Si-

739 Für Presseprodukte sind vor Verfahrenseröffnung erfolgende – präventiv-polizeiliche – Maßnahmen wegen des Grundsatzes der Polizeifestigkeit der Presse, dazu Löffler - *Bullinger*, § 1 LPG Rn. 193, nicht zulässig. In Betracht kommt nur die Beschlagnahme gem. §§ 111m, n StPO bzw. §§ 13 ff. LPG. Im Zivilverfahren kommt vorläufiger Rechtsschutz nach der ZPO in Betracht. Zu vorläufigen Maßnahmen im GjSM-Verfahren vgl. § 15 GjSM.

740 Dies wird z.B. durch Untersagung gem. § 18 Abs. 2 MDStV und / oder Einziehung gem. § 74 d StGB erreicht.

741 Vgl. §§ 3ff. GjSM, § 1 I Nr. 5 RStV, § 6 I Nr. 4 DWG, § 55 I Nr. 4 LMGbw, sowie die Verbreitungseinschränkungen in § 1 II, III, IV RStV, § 6 II, III, IV DWG, § 55 II, III, IV LMGbw, § 18 II MDStV.

742 Weder das Zensurverbot noch gesetzliche Vorschriften zum Schutz der Presse hindern nach allgemeiner Meinung die *Zivilgerichte* daran, vorbeugend zur *Unterlassung* etwa einer Presseäußerung zu verurteilen, wenn ein privater Betroffener dies beantragt (Maunz/Dürig/Herzog – *Herzog*, Art. 5 I, II Rn 300; von Münch / Kunig-*Wendt* Art. 5 Rn 66); doch ist zu prüfen, ob das Zivilgericht dabei die Meinungsfreiheit oder Pressefreiheit hinreichend berücksichtigt hat (BVerfGE 85, 1, 11ff. - *"Kritische Bayer-Aktionäre"*), vgl. *Bullinger* a.a.O. Rn. 139.

cherheit umfaßt sind, kommen gefahrenabwehrrechtliche Maßnahmen bereits dann in Betracht, wenn die Verletzung von Inhaltsbindungen erst droht. Dafür ist regelmäßig das Bestehen einer mindestens konkreten Gefahr oder einer Störung für das Schutzgut Voraussetzung. Nur zur Durchführung von Gefahrerforschungsmaßnahmen durch die Polizei reicht ein bloßer Gefahrenverdacht aus. Dabei ist zu beachten, daß für bereichsspezifische Gefahrenabwehrmaßnahmen bestehende Befugnisnormen der polizeilichen Generalklausel auch vorgehen, wenn sie im konkreten Fall nicht einschlägig sind und dann deren Anwendung ausschließen. Wegen des engen Grundrechtsbezugs der Kommunikationsinhaltskontrolle sind zudem präventiv-polizeiliche Standardbefugnisse entweder bereits gesetzlich eingeschränkt[743] oder jedenfalls im Rahmen der Rechtmäßigkeitsprüfung einer besonders strengen Verhältnismäßigkeitskontrolle zu unterwerfen.

Liegen die tatbestandlichen Voraussetzungen einer gefahrenabwehrrechtlichen Befugnisnorm vor, so kann die Polizei dem Störer (etwa §§ 6, 7 PolGBW) - und unter besonderen Voraussetzungen auch dem Nichtstörer (etwa § 9 PolGBW) - durch Verwaltungsakt verhältnismäßige Maßnahmen zur Gefahr- oder Störungsbeseitigung aufgeben.

II. Identifikation potentiell rechtswidriger Inhalte als Verfahrens- und Durchsetzungsvoraussetzung

Bevor bedenkliche Inhalte einem Verfahren zur Feststellung ihrer Rechtswidrigkeit zugeführt oder Gegenstand einer Polizeiverfügung werden können, bedarf es zunächst ihrer Identifizierung. In Betracht kommt - wie in herkömmlichen Medien - auch bei digitalen Kommunikationsinhalten eine Identifikation durch verschiedene Akteure. Insbesondere ist an eine Identifizierung bedenklicher Inhalte durch den Staat (1.), durch *provider* (2.) und durch die Nutzer selbst (3.) zu denken.

1. Identifikation durch den Staat

Unter Identifikationsmaßnahmen durch den Staat soll im Folgenden nur das *direkte* Tätigwerden staatlicher Organe beim Aufspüren bedenklicher Inhalte verstanden werden. *Indirekte* Maßnahmen, etwa die gesetzliche Verpflichtung von *providern* oder Nutzern zur Überprüfung von Inhalten, werden jeweils dort erörtert.

Eigene Maßnahmen staatlicher Stellen zur verdachtsunabhängigen Identifikation möglicherweise rechtswidriger digitaler Kommunikationsinhalte sind in verschiedenen Konstellationen denkbar, die in herkömmlichen Medien nicht oder nicht in vergleichbarem Ausmaß vorkamen.

743 So ist etwa die Beschlagnahme von Presseprodukten nach den LPGen nur unter Beachtung der für Beschlagnahmen im (repressiven) Ermittlungsverfahren bestehenden rechtsstaatlichen Sicherungen zulässig. Vgl. oben *(a) Polizeifestigkeit der elektronischen Presse*, S. 99.

Wie einzelne Telefonverbindungen, kann der Staat auch Datenleitungen abhören[744]. Durch Eingriffe in die Netzarchitektur und wirksame Kooperation zwischen Staaten bzw. Geheimdiensten kann auch ein Großteil des telekommunikativen Datenverkehrs nicht nur auf nationaler Ebene[745], sondern auch weltweit zentral abgehört werden. In jüngerer Zeit mehren sich die Hinweise, daß dies seit Ende des Zweiten Weltkrieges auch tatsächlich geschieht[746]. Wie effektiv ein derartiges System beim Abhören digitaler Kommunikationsinhalte tatsächlich sein kann, ist weithin unklar. Die bei diesem flächendeckenden Abhören gewonnenen Erkenntnisse können zur Einleitung von rechtsstaatlichen Inhaltskontrollverfahren zudem kaum benutzt werden, weil die Abhörpraxis regelmäßig verschleiert werden soll oder gesetzliche Grundlagen für sie fehlen.

Auf der Suche nach potentiell rechtswidrigen Inhalten kommt auch eine Sichtung der frei zugänglichen Informationsinhalte, etwa der im Internet zusammengeschlossenen *server*, in Betracht. Durch Einsatz von Software kann diese Fahndung automatisiert werden, wodurch ein gezieltes Suchen auch nach versteckten rechtswidrigen Inhalten möglich wird.

Werden derartige Ermittlungen offen geführt, sind also etwa staatliche Abrufe von *WWW*-, *FTP*- und *news*-Inhalten durch entsprechend identifizierbare Einträge in den Logfiles der besuchten *server* erkennbar oder präsentieren sich die Ermittler offen in *chatrooms* und *mailing lists*, so ist allerdings zu erwarten, daß Anbieter und Nutzer, die staatliche Kenntnisnahme von ihrer Kommunikation nicht wünschen, Gegenmaßnahmen ergreifen. Daher werden Ermittler zunehmend von den Möglichkeiten jedes Nutzers Gebrauch machen wollen, unter Pseudonym oder anonym kommunizieren, Inhalte abzurufen oder sich zuspielen zu lassen.

---

744 Gemeint ist hier nicht das heute als Ermittlungsmaßnahme zugelassene Abhören von Telefonen nach § 100a StPO, bzw. von Telekommunikaitonseinrichtungen nach der Fernmeldeüberwachungsverordnung (vgl. zum Entwurf einer Telekommunikationsüberwachungsverordnung oben *aa. Vertraulichkeitsschutz in Strafverfolgung und Strafrecht*, S. 107. Dies dient immer der Beweiserlangung hinsichtlich einer anderen Straftat (Katalogtat des § 100a StPO), nicht der verdachtsunabhängigen Identifikation bedenklicher Inhalte.

745 Etwa von Singapur und China wurde versucht, den gesamten leitungsgebundenen Internet-Verkehr mit dem Ausland durch ein zentrales Nadelöhr zu leiten, an dem der Staat nicht nur mithört, sondern auch filtert, vgl. *Wingfield, Nick, Macavinta, Courtney*, China´s National Intranet, http://www.news.com/News/Item/0, 4, 7025, 00.html v. 15.1.97 und *Human Rights Watch*, Silencing the Net: The threat to Freedom of Expression On-Line, http://www.epic.org/ free_speech/intl/hrw_report_5_96.html.

746 Vgl. die Berichterstattung zum sog. ECHELON-System. Ausgehend von einem Report des *Europaparlaments, Directorate General for Research (B), Scientific and Technological Options Assessment (STOA) Programme*, An Appraisal of Technologies of Political Control, PE 166 499 v. 6. Januar 1998, sind weitere Berichte zu Funktionsweise und Effizienz des ECHELON-Systems erschienen, vgl. etwa *McKay, Niall*, Eavesdropping on Europe, http:// www.wired.com/news/print_version/ politics/story/ 15295.html v. 30.9.98; *Moechel, Erich*, Bis Brother Preis geht an Echelon, http://www.telepolis.de/tp/ deutsch/inhalt/te/1613/1.html; *Poole, Patrick, S.*, Echelon:America´s Spy in the Sky, http://www.jya. com/echelon-usaj.htm.

Ebenso sind über die bloße Dienstenutzung hinausgehende Maßnahmen denkbar: Polizei und Staatsanwaltschaft können sich durch die Aufzeichnung von Kommunikationsdaten umfangreiche Kommunikationsprofile von Dienstenutzern verschaffen oder sogar durch gezielten Zugriff auf die Nutzungsprotokolle von *server*n *(Hacking)* feststellen, wer wann und wie lange bestimmte Inhalte abgerufen hat oder sich hat zuspielen lassen.

a. Rechtliche Schranken

Derartigen staatlichen Maßnahmen können rechtliche Schranken entgegenstehen, wenn sie die Schwelle zum Eingriff in Grundrechte von Inhalteanbietern oder Dienstenutzern überschreiten. Zur Bestimmung dieser Schwelle ist die Bedeutung betroffener Grundrechte für die typischen Vorgänge digitaler Kommunikation zu ermitteln.

aa. Grundrechtseingriffe durch staatliche Identifikationsmaßnahmen

Wie aus der überblicksartigen Zusammenstellung denkbarer staatlicher Aktivitäten ersichtlich, sind die Behörden zur Identifikation bedenklicher Inhalte in digitalen Medien nicht darauf beschränkt, fremde Telekommunikationsverbindungen abzuhören:

Angesichts der zunehmenden Überlagerung von individueller Kommunikationsart (*point-to-point*-Verbindungen) mit der Kommunikation überindividueller Inhalte[747] wachsen auch die Möglichkeiten des Staates, fremde Inhalte durch Zustandebringen eigener *point-to-point*-Verbindungen zu überprüfen. Während hier in herkömmlichen Medien selten die Frage eines Grundrechtseingriffs problematisiert wurde[748], stimmt Vergleichbares in digitalen Medien bedenklich. Die Frage, ob ein Eingriff in das Fernmeldegeheimnis vorliegen könnte, wenn der Staat etwa automatisch Tausende von Telefonnummern anwählt, um die angeschlossenen Anrufbeantworter auf rechtswidrige Ansagetexte zu prüfen, wurde bisher nicht relevant. Darum geht es jedoch heute, wenn die Eingriffsqualität maschinellen Suchens nach möglicherweise rechtswidrigen Inhalten auf „abrufbeantwortenden" *servern* im Internet[749] durch den Staat in Frage steht. Entsprechende Programme befinden sich bereits im Einsatz.[750]

In digitalen Medien existieren zudem Zwischenformen, die kaum noch sinnvoll Differenzierungen zulassen, nach denen ein rechtfertigungsbedürftiger Grundrechtseingriff

747 Vgl. oben *bb. Die Beliebigkeit von Öffentlichkeit als Strukturmerkmal der neuen Formen digitaler Kommunikation*, S. 60.

748 Bereits bei der Wahl eines ausschließlich öffentlichen Übertragungsweges (Rundfunk) wurde Verzicht etwa auf Vertraulichkeitsschutz vermutet, vgl. oben bei FN 155.

749 Vgl. oben S. 62.

750 So die PERKEO-Software. Perkeo wurde von einem Beamten des hessischen Landeskriminalamts entwickelt. Es generiert Prüfsummen für Dateien auf verdächtigen Datenträgern. Diese gleicht es mit den in einer Datenbank gespeicherten Prüfsummen bereits bekannter strafbarer Dateien (z.B. Bilder) ab. Das Programm ist bei verschiedenen Polizeidienststellen im Einsatz. Die Herstellerfirma gibt keine präzisen Informationen zur Funktionsweise des Programms, jedenfalls kann es einen Inhalt schon dann nicht wiedererkennen, wenn in ihm auch nur ein bit verändert ist, weil dann der abgeglichene „Hash-Wert" nicht mehr identisch ist, vgl. http://www.fitug.de/netpol/98/7.html.

dann zu bejahen ist, wenn der Staat Kenntnis von fremder Kommunikation nimmt (Abhören von Telefonverbindungen), nicht aber, wenn der Staat auf der Suche nach möglicherweise rechtswidrigen Inhalten eine eigene Kommunikationsverbindung zustande bringt (staatliches Anschauen von Rundfunkprogrammen, staatliche Zeitschriftenabonnements): Beim staatlichen „Mitlesen" von Kommunikation über *mailing lists* kommt zwar eine eigene Verbindung zwischen dem Inhalts(zwischen)versender (*mail exploder*) und der staatlichen Stelle zustande, die darüber telekommunikativ vermittelte Kommunikation findet jedoch inhaltlich zwischen den Autoren der Einzelbeiträge statt. An ihr ist der bloß mitlesende[751] Staat nicht aktiv beteiligt, wodurch solche Aktivität eher an das Abhören fremder Kommunikation erinnert.

Noch deutlicher wird dies in *chatrooms*. Hier entsteht ebenfalls eine eigene Kommunikationsverbindung zwischen dem *chat server* und der staatlichen Stelle. Liest der Staat aber nur die dort stattfindende (Echtzeit-)Kommunikation der *chatter* mit, sitzt er gleichsam stumm in der Ecke eines Versammlungsraumes und lauscht fremden Gesprächen.

Die beschriebenen Konstellationen folgen direkt aus der als Strukturmerkmal digitaler Medien herausgestellten Überlagerung von individueller und überindividueller Kommunikation[752]. Wie sich dort der Grad an „Individualität" der Kommunikation nicht mehr klar nach einzelnen technisch verschiedenen Dienstearten (Rundfunk, Telefon) bestimmt, sondern stufenlos je nach der gewählten Konfiguration beliebig konfigurierbarer Vermittlungseinrichtungen[753], bestimmt sich hier das Vorliegen eines Eingriffs nicht mehr klar nach Kommunikationstypen sondern entsprechend den durch den Anbieter getroffenen oder von ihm veranlaßten Zugangsbeschränkungen.

(1) Eingriffe in Art. 10 Abs. 1 GG (Fernmeldegeheimnis)

Adressiert ein Anbieter digitale Kommunikationsinhalte an einen oder mehrere bestimmte Empfänger, so kann er jedem an das Fernmeldegeheimnis gebundenen Nichtadressaten gegenüber grundrechtlichen Vertraulichkeitsschutz beanspruchen. Ein relevanter Verzicht auf Vertraulichkeitsschutz durch einen der Kommunikationspartner[754] liegt in diesem Fall nicht vor. Jede Kenntnisnahme des Staats von dieser Kommunikation ist so ein Eingriff in das Fernmeldegeheimnis, jede Kenntnisnahme eines an der Kommunikation nicht als Sender oder Empfänger beteiligten Anbieters von Telekommunikationsdienstleistungen ein Verstoß gegen § 85 TKG. Jede staatliche Abhörmaßnahme einer *point-to-point*-Verbindung zwischen Privaten ist daher unabhängig

751 Ein solches Verhalten wird in der „Netz"-Sprache „Lurking" (von engl. to lurk=sich verbergen) genannt.

752 Vgl oben *bb. Die Beliebigkeit von Öffentlichkeit als Strukturmerkmal der neuen Formen digitaler Kommunikation*, S. 60.

753 Vgl. dazu oben, S. 62.

754 Siehe zu dieser Möglichkeit oben *c. Vertraulichkeit von Kommunikation als Differenzierungskriterium des Inhaltskontrollrechts*, S. 43.

von der Art der kommunizierten Inhalte (persönliche *e-mail*, *WWW*-Abruf /-Zustellung, *video-on-demand*-Zuspielung) ein rechtfertigungsbedürftiger Eingriff in Art. 10 Abs. 1 GG.

Übermittelt ein Anbieter einen Inhalt an eine *mailing list* und überläßt dem dazugehörenden *mail exploder* die Einzelverschickung an die Listenmitglieder, so wählt er eine bestimmte Vermittlungskonfiguration: Er wünscht die Zustellung an und gleichzeitig die Zugangsbeschränkung auf einen an dem jeweiligen Listenzweck inhaltlich interessierten und deshalb auf diese Liste abonnierten Personenkreis (*Community*[755]). Nur soweit reicht folglich auch sein Verzicht auf Vertraulichkeitsschutz. Er rechnet - im Gegensatz zum Publizieren in freiverkäuflichen Zeitungen oder zum öffentlichen Anschlagen von Flugblättern - nicht damit, daß der Inhalt ohne einen dazwischentretenden „Vertraulichkeitsbruch" eines *Community*-Mitglieds direkt von dem nicht am Thema, sondern nur am Ausfindigmachen bedenklicher Inhalte interessierten Staat zur Kenntnis genommen wird.

Abonnieren Polizei oder Strafverfolgungsbehörden eine solche thematische *mailing list*, um potentiell rechtswidrige Inhalte zu identifizieren, liegt darin ein Bruch der geschützten *Community*-Vertraulichkeit und damit ein Eingriff in Art. 10 Abs. 1 GG. Dies gilt erst recht dann, wenn staatliche Stellen zum genannten Zweck anonym oder unter Pseudonym in *mailing lists* mitlesen.

Im Bezug auf *chatrooms* bieten sich die für *mailing lists* herausgearbeiteten Grundsätze dann an, wenn es sich um thematisch ausgerichtete Räume handelt. Dies ist allerdings selten der Fall. Wichtiger ist, daß die *chat*-Kommunikation noch deutlicher als die Beiträge in einer *mailing list* die Struktur eines Gesprächs unter den „Anwesenden" aufweist. Während das stille Mitlesen in *mailing lists* zu Informationszwecken (für inhaltlich Interessierte) durchaus üblich ist, dominiert beim *chatroom* das Interesse am Austausch kurzer Äußerungen in Echtzeit, wobei die Themen rasch wechseln und oft wenig Tiefe haben. Die *chat*-Kommunikation ist geprägt von der aktiven Beteiligung am „hier und jetzt" stattfindenden Gespräch. Das staatliche „*Lurking*"[756] in *chatrooms* auf der Suche nach rechtswidrigen Äußerungen hat daher stärker als das Mitlesen von *mailing lists* den Charakter des Abhörens fremder Kommunikation, obwohl auch hier technisch eine eigene Telekommunikationsverbindung zwischen der staatlichen Stelle und dem *chat server* besteht. Es ist daher ebenfalls als Eingriff in das Fernmeldegeheimis rechtfertigungsbedürftig.

Übermittelt ein Anbieter Inhalte an einen *WWW*-, Audio- oder Video-*server*, auf dem er selbst oder sein *provider* sie zum Abruf bereitstellt, so erfolgt deren Verbreitung nicht durch die positive Adressierung an bestimmte Empfänger oder *Community*-Mitglieder. Der Inhalt steht grundsätzlich - einem öffentlich angeschlagenen Flugblatt vergleichbar

755 Vgl. zu *Communities* in digitalen Medien auch *Dyson, Esther*, Release 2.0, S. 31 (47).

756 Vgl. FN 751.

- jedermann zum Abruf offen. Dennoch behält der Anbieter technisch die Möglichkeit, selbst oder durch seinen *host provider* diese Vermittlungseinrichtung (*server*) individuell zu konfigurieren. Er kann einzelne Abrufer anhand ihrer IP-Adresse[757] vom Zugriff ausschließen, etwa durch eine Paßwortabfrage nur bestimmte Abrufer zulassen oder den Abruf etwa durch Registrierungs- oder Bezahlungspflichten an Bedingungen knüpfen. Nutzt er keine dieser Möglichkeiten, verzichtet er, wie ein Anbieter einer frei erwerbbaren Zeitung oder einer frei empfangbaren Rundfunksendung vollständig auf Vertraulichkeitsschutz. Ein Eingriff in Art. 10 Abs. 1 GG kommt dann durch das bloße Abrufen dieser Inhalte von seiten staatlicher Stellen nicht in Betracht.

Nutzt der Anbieter allerdings seine Beschränkungsmöglichkeiten, verzichtet er folglich nur in entsprechendem Umfang auf Vertraulichkeitsschutz. Jedwede zweckwidrige Umgehung dieser Zugangsbeschränkungen durch den Staat führt demzufolge zu einem Eingriff in das Fernmeldegeheimnis. Darunter fallen etwa Maßnahmen wie die Benutzung von „neutralen" Rechnern oder Anonymisierdiensten durch BKA-Beamte für den Abruf von Inhalten, deren *server* so programmiert ist, daß er Abrufe von Maschinen im Subnetz „bka.de" nicht bedient; ebenso zu bewerten ist etwa auch eine falsche Berufsangabe eines Polizisten auf der Registrierungsseite eines *online*-Inhalts. Werden Inhaltsanbietern derart zugriffsbeschränkende Konfigurationen ihrer Vermittlungseinrichtungen durch Gesetz verboten, wäre darin ebenfalls ein Eingriff in Art. 10 Abs. 1 GG zu sehen. So müßte etwa § 18 Abs. 6 MDStV[758] das Fernmeldegeheimnis *verhältnismäßig* einschränken, wenn er nicht schon aufgrund des Verstoßes gegen Art. 19 Abs. 1, S. 2 GG (Zitiergebot) verfassungswidrig wäre[759].

Eine Mischform aus Versendung an eine *mailing list* und Bereithalten auf einem *server* ist das *posting* von Nachrichten im *news*-Dienst[760]. Seine Inhalte sind entweder über eine direkte Verbindung zum *news server* oder über das *WWW*[761] wie die Anschläge an öffentlichen Pinnwänden ohne Zugangsbeschränkungen abrufbar. Andererseits handelt es sich um thematisch geordnete Foren, die sowohl inhaltlich als auch historisch[762] den Charakter von *communities* haben[763]. Wer Nachrichten an *newsgroups* versendet, verzichtet dabei trotz fehlender direkter Möglichkeit der Zugangsbeschränkung für zweckwidrige Mitleser nicht vollständig auf jeden Vertraulichkeitsschutz. Liest der Staat zum

757 Zum Begriff vgl. oben S. 52.

758 Die Vorschrift lautet: „(6) Der Abruf von Angeboten im Rahmen der Aufsicht ist unentgeltlich. Anbieter haben dies sicherzustellen. Der Anbieter darf seine Angebote nicht gegen den Abruf durch die zuständige Aufsichtsbehörde sperren."

759 Die Rechtsprechung des BVerfG schränkt die Geltung des Zitiergebots zwar stark ein, bei Art. 10 GG ist es jedoch zu beachten, vgl. die Aufstellung bei *Pieroth / Schlink*, Rn. 337.

760 Zur Funktionsweise des Newsdienstes vgl. oben bei FN 209.

761 Vgl. etwa Dienste wie http://www.dejanews.com, die die Inhalte von *newsgroups* als *WWW(HTML)*-Inhalte zum Abruf bereithalten.

762 Das zur Verbreitung von *News* geschaffene *Usenet* war ursprünglich von anderen Datennetzen klarer als heute getrennt.

763 Vgl. *Dyson*, a.a.O., S. 32.

Zwecke der Identifizierung potentiell rechtswidriger Inhalte in *newsgroups* mit, liegt auch darin ein Eingriff in Art. 10 Abs. 1 GG.

(2) Eingriff in Art. 5 Abs. 1 S. 1 bzw. Abs. 1 S. 2 1. Var. GG (Meinungs- bzw. Pressefreiheit[764])

Ebenso wie zur positiven Meinungsfreiheit gehört, daß die Meinung ihren Adressaten erreicht, gehört zur negativen Seite des Schutzbereichs, daß staatliche Regelung dem Äußernden nicht verbieten darf, Einzelne vom Empfang der Meinung auszuschließen.[765] Ergreift ein Anbieter digitaler Inhalte Maßnahmen, die bestimmte Nutzer von seiner Kommunikation ausschließen sollen, liegt in deren Umgehung durch den Staat ein Eingriff in die negative Meinungsfreiheit. Für telekommunikativ verbreitete Meinungen wird nach herrschender Ansicht allerdings Art. 10 Abs. 1 GG als spezielleres Grundrecht angesehen.[766]

Dennoch bleibt der Garantiegehalt der Meinungsfreiheit für staatliche Identifikationsmaßnahmen möglicherweise rechtswidriger Inhalte nicht ohne Bedeutung: Muß ein Inhalteanbieter fürchten, daß der Staat zum Zwecke der Gefahrenabwehr verdachtsunabhängig von ihm verbreitete oder zum Abruf bereitgestellte Inhalte selbst dann zur Kenntnis nimmt, wenn er dagegen die oben genannten Zugriffsbeschränkungen implementiert hat, so besteht die Gefahr, daß er auch vor rechtmäßigen Meinungsäußerungen zurückschreckt („*chilling effect*“)[767]. Aus diesem Grunde ist staatliches Tätigwerden, das Maßnahmen, die den Zugang staatlicher Stellen beschränken, verbietet[768] oder umgeht, ein Eingriff auch in Art. 5 Abs. 1 S. 1 GG.

(3) Eingriff in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (Recht auf informationelle Selbstbestimmung)

Das Grundrecht auf informationelle Selbstbestimmung gewährleistet die „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“[769]. Ein Eingriff in dieses Grundrecht ist „jeder persönlichen Lebenssachverhalten geltende Akt staatlicher Informations- und Datenerhebung und -verarbeitung“[770]. Persönlichen Lebenssachverhalten gilt auch diejenige Datenerhebung, die Kommunikationsinhalte mit ihren Nutzungsdaten verknüpft. Jede behördliche Erhe-

764 Wie oben, *f. Presserecht*, S. 93, gezeigt, werden vielerlei digitale Kommunikationsinhalte von der Pressefreiheit erfaßt. Teilweise werden jedoch die *Inhalte* von Presseerzeugnissen der Meinungsfreiheit unterstellt, vgl. FN 742.

765 *Pieroth / Schlink*, Rn. 614.

766 *Pieroth / Schlink*, a.a.O.

767 Vgl. *Simitis*, (FN 263), S. 311 mit Verweis auf die amerikanische Rechtsprechung zur Inhaltskontrolle im Internet, *ACLU v. Reno* 929 F.Supp. 824 (E.D. Penns. 1996), 26, 29, 39; *Reno v. ACLU*, a.a.O. (FN 364).

768 Vgl. § 18 Abs. 6 MDStV, dazu oben bei FN 758f.

769 BVerfG 65, 1 (43).

770 VGH Kassel, NVwZ 88, 642; *Meissner*, NVwZ 89, 1.

bung mit dem Ziel zu erfahren, wer was zu welchem Zeitpunkt an wen kommuniziert hat, ist damit ein Eingriff in das Recht auf informationelle Selbstbestimmung. Dies gilt unabhängig von der Zugangsoffenheit der Kommunikation, deren Inhalte und Umstände gespeichert werden. Staatliches Mitprotokollieren der Äußerungen und der Namen (Pseudonymen) ihrer Äußerer in *chatrooms*, staatliche Suche nach „Reizworten" mittels Suchmaschinen zur Ermittlung der Anbieter der gefundenen bedenklichen Inhalte, der staatliche Einsatz von Software, die selbständig die Inhalte von *server*n nach bestimmten Begriffen oder Datei-Prüfsummen[771] durchsucht sind demgemäß Eingriffe in den grundrechtlich geschützten Bereich, wenn - was meist der Fall sein wird - die gewonnenen Resultate persönliche Kommunikationsdaten (Namen von Autoren, Anbietern, Logfiles mit Angaben zu Zeit und Dauer der Kommunikation) enthalten und in irgendeiner Weise verarbeitet werden[772].

bb. Rechtfertigung von Grundrechtseingriffen bei staatlichen Identifizierungsmaßnahmen

Eingriffe in die genannten Grundrechte sind zu rechtfertigen, wenn sie durch Gesetz oder aufgrund Gesetzes erfolgen (Art. 10 Abs. 2 S. 1; Art. 5 Abs. 2 GG; BVerfGE 65, 1 (43ff.)).

Als gesetzliche Grundlagen für die beschriebenen Aktivitäten staatlicher Stellen zur Identifikation digitaler Kommunikationsinhalte kommen bestehende Vorschriften des Strafprozeßrechts nur soweit in Betracht als bereits ein Ermittlungsverfahren eingeleitet ist, in dessen Rahmen die entsprechenden Fahndungsmaßnahmen notwendig sind. Dies wird bei der derzeit von den Ländern und dem Bundeskriminalamt aufgenommenen präventiven Kontrollaktivität[773] regelmäßig nicht der Fall sein.

Diese muß auf gefahrenabwehrrechtliche Ermächtigungsgrundlagen gestützt werden. Alle Vorschriften, die hier anzuführen wären, werfen jedoch bei näherem Hinsehen Zweifel hinsichtlich ihrer Anwendbarkeit auf: Für Mediendienste normiert § 18 Abs. 1 MDStV die Aufgabe der zuständigen Länderbehörden, die Einhaltung des Staatsvertrages zu „überwachen". Eine Befugnis zu verdachtsunabhängigen Identifizierungsmaßnahmen ist darin nicht enthalten. Befugnisse verleiht erst § 18 Abs. 2 MDStV und nur für den Fall, daß der Verstoß bereits festgestellt ist. Die polizeigesetzlichen Vorschriften zur Datenerhebung (vgl. § 31 BayPAG) und zum Abhören von Telefonverbindungen wurden ersichtlich für Gefahrerforschungsmaßnahmen *im Einzelfall*, nicht jedoch für *flächendeckende* Identifikationsaktivitäten geschaffen, wie sie unvermeidlich mit einem maschinellen Durchsuchen von *server*-Inhalten in digitalen Medien verbunden wären.

771 Vgl. zur Funktionsweise des sog. PERKEO-Programms oben FN 750.

772 Zum datenschutzrechtlichen Verarbeitungsbegriff vgl. § 1 Abs. 5 BDSG und oben *bb. Datenschutzrechtlicher Vertraulichkeitsschutz*, S. 44.

773 Vgl. *Kahlweit, Cathrin*, Surfin' BKA, SZ, 17.12.1998, S. 19, *Deutsche Presseagentur*, BKA richtet Zentrale gegen Internet-Kriminalität ein, Dpa-Meldung v. 29.11.98, http://www. berlin-online.de/wissen/computermeldungen/.xtml/comp0318.html.

Die Anwendung der polizeirechtlichen Generalklausel (etwa §§ 1, 3 PolGBW) erscheint demgegenüber bereits wegen des Bestehens der genannten Spezialermächtigungen ausgeschlossen.[774]

Alle diese landesrechtlichen Grundlagen werfen zudem die Frage auf, ob nicht ein überwiegender Sachzusammenhang der genannten staatlichen Aktivitäten mit der Telekommunikation, die gem. Art. 73 Nr. 7 GG in ausschließlicher Bundeskompetenz steht, angenommen werden muß und damit - zumindest für einige Dienste[775] - auch hinsichtlich von Gefahrenabwehrbefugnissen eine bundesrechtliche Ermächtigungsgrundlage zu fordern ist[776]. Ein solche enthalten weder § 5 Abs. 4 TDG, der nur auf bestehende Ermächtigungen Bezug nimmt, noch etwa das BKA-Gesetz. Materiell- und kompetenzrechtlich ungesichert - und zumindest nach den vorliegenden Informationen in bedenklicher Nähe zu verbotener Mischverwaltung stehend - sind daher sowohl das derzeit praktizierte Modell, nach dem aufgrund eines Beschlusses der Innenministerkonferenz (Länder) eine „Zentralstelle gegen Internet-Kriminalität“ beim Bundeskriminalamt (Bund) die Aufgabe hat, „deliktsunabhängig“ im Internet zu surfen, um etwaige Straftaten aufzudecken[777], als auch die Organisation „jugendschutz.net“[778].

Noch zu schaffende Eingriffsermächtigungen für verdachtsunabhängige Identifikationsmaßnahmen stehen jedoch vor dem Problem, daß jede maschinelle Recherche nach bedenklichen digitalen Kommunikationsinhalten notwendig flächendeckend und ohne Beschränkung auf konkrete Verdachtsfälle geschieht.[779] Zudem müßte gesetzlich konkretisiert werden, was derartig „bedenkliche“ Inhalte ausmacht, wonach also zu suchen

774 Vgl. oben *2. Durchsetzung durch präventive Verfahren*, S. 164.

775 Diese Einschränkung müßte sich an der zwischen TDG und MDStV getroffenen Abgrenzung (§ 2 TDG / MDStV) orientieren, die allerdings ihrerseits in der Praxis schon wenig handhabbar ist.

776 A.A. der ehem. Staatssekretär im BMI, *Dr. K. Schelter*, vgl. *Schulzki-Haddouti, Christiane*, Nicht den Anschluß verlieren, http://www.heise.de/ct/98/18/084.html.

777 *Kahlweit*, a.a.O. Diese Stelle nimmt verschiedene der oben als Eingriffe beschriebenen Identifikationsmaßnahmen vor, unter anderem auch die Auswertung von *chatroom*-Kommunikation anhand von Logfiles, vgl. *Deutsche Presseagentur* (FN 773).

778 „Jugendschutz.net“, http://www.jugendschutz.net, ist eine Organisation der Bundesländer mit Sitz zunächst in Wiesbaden, jetzt in Mainz. Die rechtliche Qualität und gesetzliche Grundlage dieser „Stelle“ sind unklar. Praktisches Ergebnis ist die folgende Beschreibung von *Petra Müller*, Mitarbeiterin von „Jugendschutz.net“ in einem Vortrag vom 29.05.98 in Mainz „Jugendschutz.net - Konzeption, Arbeitsweise und öffentliche Resonanz“, über http://www.jugendschutz.net: „Aufgrund der beschriebenen rechtlichen Situation ist jugendschutz.net als Institution der Bundesländer primär für Mediendienste bzw. Allgemeinkommunikation zuständig. Hier könnte es, ..., eine Vielzahl von rechtlich strittigen Fällen geben. In der Praxis wirkt sich dies jedoch bisher nicht aus, da für unsere Arbeit eindeutig die Frage im Vordergrund steht, ob das betreffende Angebot Kinder und Jugendliche gefährden oder beinträchtigen könnte. Gegebenenfalls wird jugendschutz.net solche Angebote an alle zuständigen Behörden weiterleiten, an Strafverfolgungsbehörden ebenso wie an Behörden, die für die Verfolgung von Ordnungswidrigkeiten zuständig sind.“

779 Vgl. *Simitis*, (FN 263), S. 305ff.

wäre, um einen Verstoß gegen das allgemeine verfassungsrechtliche Bestimmtheitsgebot zu vermeiden.[780]

Eine entsprechende Ermächtigungsgrundlage zöge in noch stärkerem Maße als etwa die verdachtsunabhängige Personenkontrolle (§ 26 Abs. 1 Nr. 6 PolGBW) einen Freiheitsverlust *aller* Bürger nach sich, dessen Inkaufnahme erheblichem Rechtfertigungsdruck ausgesetzt wäre. Zwar kann - jedenfalls in Sonderfällen[781] - aus der objektivrechtlichen Dimension der Grundrechte eine staatliche Schutzpflicht entstehen, Grundrechtsgefährdungen durch Private mit hoheitlichen Mitteln abzustellen. Verletzt der Staat diese Handlungspflicht, verhält er sich verfassungswidrig. Kann aber der Staat eine verfassungsrechtliche Schutzpflicht wie regelmäßig nur unter Eingriff in Grundrechte der (potentiellen) Störer erfüllen[782], bedarf es einer Abwägung, die die Konsequenzen der Schutzpflichtverletzung mitbedenkt und nicht nur den Eingriff betrachtet. Aber selbst bei tatbestandlichem Vorliegen einer Grundrechtsrechtsgefährdung durch privates Handeln, hier etwa durch die Verbreitung illegaler digitaler Inhalte, steht das Entstehen *jeder* staatlichen Schutzpflicht unter dem Vorbehalt des Möglichen.[783] Zwar ist absolute Sicherheit nicht erreichbar und kann folglich nicht als Maßstab herangezogen werden. Stößt jedoch das hoheitliche Handeln zur Erfüllung der Schutzpflicht an „faktische Grenzen, an die (nicht unbeschränkt erweiterungsfähigen) Grenzen staatlicher Handlungskapazität und an die Grenzen der staatlichen Möglichkeiten, den Erfolg seiner Bemühungen zu garantieren“[784], kann der Schutzpflichtgedanke zur Rechtfertigung weitreichender Eingriffe gegenüber Bürgern, die ganz überwiegend gerade *keine* Störer sind, nicht herangezogen werden. Solche Grenzen könnten sich in ganz erheblichem Umfang aus den technologischen Besonderheiten digitaler Kommunikation ergeben:

b. Technologische Schranken

Am Beispiel des Internet verdeutlicht sich die mit herkömmlichen Medien unvergleichliche Kontrollresistenz offener, digitaler Medien. Vor allem die Menge und die Möglichkeit der Verschlüsselung von in digitalen Medien übertragenen Daten schaffen technologische Schranken bei der Identifikation illegaler und „schädigender“ Inhalte[785].

780 Dazu allgemein *Schneider, Hans,* Gesetzgebung, 2. Aufl., 1991, S. 35ff.; *Stern, Klaus,* Das Staatsrecht der Bundesrepublik Deutschland, Band 1, S. 828ff.

781 Vgl. die teils deutlich einzelfallhaften Entscheidungen des BVerfG, berichtet bei *Hesse, Konrad*, Die verfassungsrechtliche Kontrolle der Wahrnehmung grundrechtlicher Schutzpflichten des Gesetzgebers in FS-Mahrenholz, 1996, S. 541. Für eine allgemeine Anerkennung des Schutzpflichtgedankens grundlegend *Isensee, Josef,* Das Grundrecht als Abwehrrecht und staatliche Schutzpflicht, HdStR Bd. V, 1992, § 111.

782 *Isensee*, a.a.O. Rn. 168ff. nennt dies den „Schutzeingriff“.

783 Vgl. *Isensee,* a.a.O., Rn. 144.

784 Vgl. *Isensee,* a.a.O.

785 Die Europäischen Gemeinschaft möchte bei der Inhaltskontrolle zwischen illegalen und „schädigenden“ Inhalten unterscheiden. Erstere sollen mit konventionellen Mitteln der staatlichen In-

aa. Technische Probleme der Identifizierung bedenklicher Inhalte in Echtzeit bei großen Mengen paketvermittelter Daten

Jeder - dem herkömmlichen Abhören vergleichbare - Zugriff auf Inhalte während des Verbreitungsvorgangs (Kabel, drahtlos) steht hinsichtlich paketverbreiter Inhalte vor dem Problem, daß die einzelnen einen Gesamtinhalt bildenden Pakete weder notwendig hintereinander noch notwendig auf demselben Übertragungsweg angetroffen werden. Notwendig wäre daher eine vollständige Kontrolle *aller* nationalen *Backbone*-Verbindungen, auf denen gleichzeitig verschiedenste Datenarten von Börsentransaktionen über Videokonferenzen zwischen Managern und Politikern, Kreditkartenautorisierungen bis zu Patientendaten transportiert werden.

Die Menge rechtswidriger Inhalte im Internet ist derzeit relativ gering.[786] Zu ihrer Identifikation wäre jedoch eine *komplette* Durchsuchung aller Inhalte im Netz nötig[787], die zudem wegen des nicht-statischen Charakters vieler Inhalte[788] in regelmäßigen Abständen wiederholt oder gar rund um die Uhr betrieben werden müßte. Eine manuelle Sichtung aller Inhalte ist angesichts der im Internet verbreiteten Datenmenge nicht möglich.[789] Auch maschinellen Verfahren stehen aus technischen Gründen Hindernisse entgegen:

Zunächst stellt sich die Frage, wonach eine solche maschinelle Kontrolle die Inhalte durchsuchen soll, um ihre inhaltliche Bedenklichkeit einwandfrei feststellen zu können. Eine Volltextsuche nach Schlüsselwörtern kommt dabei nur als vager Ausgangspunkt in Betracht, denn sie führt weder zu sicheren noch zu vollständigen Ergebnissen. Einerseits können fremdsprachige Inhalte nur ungenügend erkannt werden. Andererseits ist nicht sicher, daß durch Wörter wie z.B. *Brust* oder selbst *child pornography* tatsächlich nur rechtswidrige Inhalte erfaßt werden. Bei der Verwendung gängiger Filterprogramme

haltskontrolle geahndet werden, wobei Durchsetzungsprobleme durch verstärkte internationale Kooperation behoben werden sollen. Letzteren soll ohne staatliche Regulierung durch die Förderung von Selbstkontrollmaßnahmen begegnet werden. Vgl. *Europäische Kommission*, Illegale und schädigende Inhalte im Internet, KOM(96)487endg., *dies.*, Action Plan Promoting the Safe Use of the Internet; *Bangemann, Martin*, A New World Order for Global Telecommunications, http://www.ispo.cec.be/ infosoc/promo/speech/geneva.html. Technologisch hat diese Unterscheidung allerdings keine Basis. Sie beruht lediglich auf der – zweifelhaften – Annahme, daß hinsichtlich illegaler Inhalte eine einfachere und breitere Einigung unter den Nationalstaaten möglich ist.

786 Vgl. *Sieber*, CR 1997, 581 (587).

787 *Simitis*, (FN 263), S. 305f. spricht davon, wie leicht gerade in digitalen Medien Protektion in Oppression „umschlagen" kann.

788 Vgl. auch oben FN 519ff.

789 Der *News*dienst umfaßt derzeit ca. 35.000 Gruppen und mehrere Millionen Einzelnachrichten. Die Zahl der *WWW*-Seiten beträgt ca. 350 Millionen. Allein bei einem deutschen Internet-Service-*provider* werden durchschnittlich *News* einer Gesamtgröße von über 72 Gigabyte vorgehalten, vgl. *Sieber*, CR 1997, 653, IV mwN. Das insgesamt im Internet täglich bewegte Datenvolumen liegt im Terabytebereich, was der mehrfachen Datenmenge einer mittleren deutschen Universitätsbibliothek entspricht.

wird regelmäßig eine enorme Zahl unbedenklicher Inhalte mitausgefiltert.[790] Ebensowenig existiert ein Signaturverfahren, das internationale Inhalte zuverlässig mit einer bestimmten Kennzeichnung versieht, aus der für das Kontrollsystem eindeutig ersichtlich wäre, daß es sich um einen in Deutschland rechtswidrigen Inhalt handelt.[791] Zudem kann der beim Nutzer ankommende digitale Inhalt aus verschiedenen Datenbanken individuell generiert werden. Selbst einzelne Bits könnten theoretisch einzeln aus unterschiedlichen Quellen kommuniziert werden. Eine Kontrolle der transportierten Inhalte könnte in diesem Fall nur Teilstücke identifizieren, die für sich genommen unbedenklich sind und erst in ihrer endgültigen Zusammensetzung zu einem rechtswidrigen Inhalt werden.

Ferner stellt sich die Frage, wo nach den einschlägigen Schlüsselwörtern gesucht wird. Da eine staatliche Gesamtkontrolle von telekommunikativ paketverbreiteten digitalen Inhalten notwendig während des Verbreitungsvorganges der Daten zu geschehen hätte, wäre in jedem Fall eine Echtzeitkontrolle vorbeifließender Datenpakete nötig. Diese bestehen aus dem sogenannten *header*, der allgemeine Steuerinformationen zu dem jeweiligen Paket enthält und einem *Inhaltsteil*, der ein Bruchstück des Gesamtinhalts darstellt. Um diesen Inhaltsteil textmäßig nach Stichwörtern durchsuchen zu können, müssen die darin enthaltenen Informationen vom Format der Transportebene (Netzebene 2[792]) auf das Format der jeweils benutzten Anwendung (Netzebene 7) konvertiert werden. Die Implementierung eines dazu nötigen *Application Gateway*[793] führt bereits bei wesentlich kleineren Durchsatzraten, etwa bei *Firewalls* besonders sicherheitsbedürftiger Unternehmensnetze, zu erheblichen *performance*-Verlusten[794] und hätte auf nationaler Ebene den Infarkt aller öffentlichen Datennetze zur Folge.

Überlegungen, in derartige Technologie zu investieren müssen im Auge behalten, daß selbst eine perfekte Echtzeitdurchsuchung aller digitalen Kommunikationsinhalte durch die Benutzung überall kostenlos erhältlicher Verschlüsselungssoftware[795] umgangen werden kann.

---

790 Vgl. *The Censorware Project*, Blacklisted by Cyber Patrol, Über http://www.gilc.org; *Möller, Eric,* Das Betreten dieser Seite ist nicht gestattet, Kölner Stadt-Anzeiger v. 30./31.5.98, Wochenendbeilage, S. 7; *ACLU,* Fahrenheit 451.2: Is Cyberspace Burning? How Rating and Blokking Proposals Torch Free Speech on the Internet, http://www.aclu.org/issues/cyber/ burning.html .

791 Zum PICS-System vgl. unten *c. Verpflichtung der provider zur Verwendung eines Rating-Systems*, S. 181.

792 Die Ziffer der Netzebene nimmt Bezug auf das ISO/OSI-Schichtenmodell, das die verschiedenen Arbeitsschritte einer Netzkommunikation als aufeinander aufbauende Schichten darstellt. Vgl. eine ausführliche Erläuterung der einzelnen Schichten bei *Sieber,* CR 1997, 581 ff. Teil 1, III, 1 c).

793 Vgl. *Sieber,* CR 1997, 653, dort bei FN 164ff.

794 Vgl. *Sieber,* a.a.O.

795 Vgl. etwa die *PGP*-Software, oben FN 184.

bb. Technische Unmöglichkeit der Identifizierung bei verschlüsselten Inhalten

Verschlüsselte Inhalte sind erst gar nicht als möglicherweise rechtswidrig erkennbar. Einige Staaten haben daher Einschränkungen oder Verbote von Kryptographie eingeführt.[796] Nachdem in jüngerer Zeit auch in Deutschland Rufe nach Kryptografiekontrolle laut geworden waren[797], hat die Bundesregierung zuletzt einen eindeutig ablehnenden Standpunkt zu jeder Kryptographieregelung eingenommen.[798] Rechtliche Einschränkungen von freier Verschlüsselung, etwa durch Hinterlegungssysteme für private Schlüssel, sind nicht nur rechtsstaatlich bedenklich, sondern vor allem ein Sicherheitsrisiko[799]. Im Unterschied zur schon heute praktizierten und verfassungsrechtlich gedeckten Korrespondenzüberwachung gäbe eine Schlüsselhinterlegung dem Staat die Möglichkeit, nicht nur bestimmte Dokumente bestimmter Personen mitzulesen, sondern alle Nutzer zu überwachen.[800] Sichere nationale oder gar internationale Systeme für die Hinterlegung oder Rekonstruktion von privaten Schlüsseln, um den Zugriff von Behörden und Strafverfolgung auf verschlüsselte Daten oder Kommunikationsvorgänge zu ermöglichen, sind heute nicht realisierbar. Verfügbare Lösungen reduzieren die Sicherheit verschlüsselter Kommunikation auf ein für hochsensible Daten nicht erträgliches Maß und verteuern sie erheblich.[801] Derart in ihrer Sicherheit verminderte Verschlüsselung eignete sich nicht mehr zur Abwicklung globaler Finanztransaktionen und böte dem stark zunehmenden „*Electronic Commerce*“[802] nicht den notwendigen Schutz vor

796 In Frankreich und Rußland bestehen Nutzungsverbote für Kryptographietechniken ohne staatliche Erlaubnis, vgl. Loi No. 90-1170 du 30 Décembre 1990, http://www.dmi.ens.fr /dmi/equipes_dmi/grecc/loi.htm; Edict of the President of the Russian Federation about ... Sales and Use of Cryptographic Instruments ..., http://www.eff.org/pub/Privacy/Foreign_and_local/ Russia/russian_ crypto_ban_english.edict. In Frankreich wurden die Restriktionen – beginnend mit einer Gesetzesänderung 1996 – jedoch immer weiter gelockert, vgl. unten FN 1002. In den USA ist die Ausfuhr von Verschlüsselungssoftware eingeschränkt, vgl. zur Verfassungsmäßigkeit des mehrfach modifizierten und jüngst gelockerten Exportkontrollregimes US D.C. D.o.Col., *Karn v. US Dept. Of State*, 925 F.Supp.1 (1996). Ferner *Clausing, Jeri*, Encryption Debate Heats Up in Washington, CyberTimes v. 9.6.98; *Schulzki-Haddouti, Christiane*, Verschlüsselungstechniken sicherheitspolitisch umstritten, http://www.handelsblatt.de/cgi-bin/hbi.exe?SH=&iPV=0&FN=hb&SFN=news_ct_artcompu ter&iID =42158 Handelsblatt v. 26.10.98.

797 *Schulzki-Haddouti, Christiane*, Verschlüsselungstechniken sicherheitspolitisch umstritten, Handelsblatt v. 26.10.98, unter http://www.handelsblatt.de/cgi-bin/hbi.exe?SH=&iPV=0&FN=hb&SFN=news_ct_artcomputer&iID=42158. Zur heftig diskutierten Frage, ob frei erhältliche Verschlüsselungssoftware unter die Beschränkungen des getroffenen Wassenaar-Abkommens über Konventionelle Waffen, Dual-Use-Güter und -technologie (http://www.wassenaar.org) fällt, vgl. http://www.heise.de/tp/deutsch/inhalt/te/ 1708/1.html und die Diskussion unter dem Stichwort „Wassenaar“ in der Netlaw-*mailing list*, http://www.listserv.gmd.de/archives/NETLAW-L.html.

798 Vgl. unten *b. Sicherung der freien Benutzung von Verschlüsselung*, S. 221.

799 Vgl. ausführlich *Abelson, Hal*, et al., The Risks Of "Key Recovery," "Key Escrow," And "Trusted Third-Party" Encryption, 1998, http://www.cdt.org/crypto/risks98/. Aus deutscher Sicht *Rollecke, Lutz*, Hinterlegte Schlüssel bergen Risiken, Das Parlament Nr. 40 v. 25.9.98.

800 *Simitis*, (FN 263), S. 307.

801 Vgl. *Abelson*, (FN 799); *Rollecke*, a.a.O.

802 Rund 419 Mio. DM, so schätzt die US-Marktforschungsfirma *Forrester Research*, werden 1998 in Deutschland online erwirtschaftet. Bis 2001 soll der Umsatz auf fast 29 Milliarden Mark wachsen, SPIEGEL 31/98 v. 27.7.98, S. 72.

online-Kriminalität. Bilanziert man die Auswirkungen ungehinderter sicherer Verschlüsselung, verhindert sie mehr Kriminalität als sie hervorruft[803].

Ferner bleiben Nutzungseinschränkungen von Schlüsseln wirkungslos, weil einerseits Verschlüsselung auch ohne Benutzung von Schlüsseln erreicht werden kann[804] und andererseits durch die Kombination von Verschlüsselung und Steganographie[805] verschlüsselte Inhalte so verborgen werden können, daß nicht erkennbar wird, ob Verschlüsselung überhaupt stattgefunden hat.[806]

Außerdem verbieten sich Verschlüsselungsverbote, wo Authentizität gefördert werden soll: Ein Verbot von Verschlüsselung oder ein anfälliges Hinterlegungssystem für private Schlüssel bedeutet einen Sicherheitsverlust für digitale Signaturen und die Authentisierung von Dokumenten[807], weil zu diesen Vorgängen oft die gleichen Schlüssel wie zur Verschlüsselung benutzt werden. Die Glaubwürdigkeit der digitalen Signatur rührt jedoch gerade daher, daß *niemand* außer dem Signierenden den Schlüssel besitzt.[808]

Insgesamt ermöglicht das Internet verschlüsselte Kommunikation, die von keinem Dritten, auch nicht vom Staat, zu dechiffrieren ist[809]. So verschlüsselte Kommunikation erlaubt keinerlei Inhaltskontrolle durch andere Personen als diejenige, die den Empfängerrechner kontrolliert[810], weil übermittelte Inhalte schon gar nicht als möglicherweise rechtswidrig identifiziert werden können.

---

803 Vgl. *Abelson*, et al., (FN 799). Der amerikanische Rechtshistoriker und Computerrechtler *Eben Moglen*, der selbst mehrere Jahre Programmierer bei *IBM* war, ist deshalb der Auffassung, daß sich die Regierungen entscheiden müßten zwischen einem sicheren Weltfinanzverkehr und obligatorischen Kryptographiekontrollen. So *Moglen* im Kurs „Computers, Privacy and the Constitution" im Frühjahrssemester 1998 an der Columbia Law School.

804 Der US-Mathematiker *Ronald L. Rivest* hat ein Verfahren vorgeschlagen, das vollständig "sichere" Netzkommunikation ohne den Einsatz von Verschlüsselungstechnologie ermöglicht, von Kryptographie-Beschränkungen also nicht erfaßt wird, vgl. Chaffing and Winnowing, http://theory.lcs. mit.edu/~rivest/chaffing.txt.

805 Steganografie ist ein Verfahren, bei dem in digitalen Inhalten zusätzliche, nicht erkennbare Informationen versteckt werden.

806 *Huhn / Pfitzmann*, DuD 1996, 23ff.; *Roßnagel*, ZRP 1997, 26 (27f), der außerdem zurecht darauf hinweist, daß Verschlüsselungssoftware immer irgendwo erhältlich sein wird.

807 Vgl. das am 1. August 1997 im Rahmen des IuKDG (FN 10) in Kraft getretene SigG und die aufgrund dessen § 16 am 1. November 1997 in Kraft getretene Signaturverordnung, BGBl. I S. 1870, 1872.

808 *Abelson* et al., (FN 799).

809 Vgl. auch *Simitis*, (FN 263), 305f., der eine eigene Dialektik technischer Schutzmechanismen sieht. Vollendete Verschlüsselung schließe staatlichen Zugriff auch dort aus, wo er früher in Kauf genommen werden mußte. Er plädiert dafür, den „exzeptionellen Zugang" aufrechtzuerhalten, will den Staat aber nicht mit einem „Hauptschlüssel" ausstatten. Wie dies funktionieren soll, sagt er nicht. Fest steht jedenfalls, daß ohne staatlichen Zugriff auf private Schlüssel eine Entschlüsselung verdächtiger Kommunikation *ohne* Notifikation des Empfängers (durch Zwang, seinen privaten Schlüssel herauszugeben) nicht möglich ist. Gerade darauf kommt es Ermittlungsbehörden aber an, vgl. die Vorschriften zur Telefonüberwachung in §§ 100a f. StPO und das G 10 (dazu FN 153).

810 Verschlüsselte Inhalte können von keinem Wortfilter erkannt werden, mit falschen PICS-Labeln in Klartext versehene, im übrigen aber verschlüsselte Inhalte können von keinem *Rating*-System

2. Identifikation durch *provider* und Betreiber von Telekommunikationsanlagen

Nicht nur der Staat, sondern auch *provider* können zur Identifikation bedenklicher Inhalte in digitalen Medien tätig werden. Da von solchen Aktivitäten der *provider* regelmäßig auch Inhalte erfaßt würden, derentwegen staatliche Verfahren zur Feststellung ihrer Rechtswidrigkeit in Betracht kommen[811], ist der Staat an einer Zusammenarbeit mit den *providern* bei der Identifikation bedenklicher Inhalte interessiert[812]. Zu unterscheiden ist, ob *provider* durch Gesetz zu einem bestimmten Maß an Zusammenarbeit verpflichtet werden, oder ob kooperative Kontrollverfahren ohne gesetzliche Bindungen angestrebt werden.

Provider oder Betreiber von Telekommunikationsanlagen könnten durch Gesetz gezwungen werden, bedenkliche Inhalte zu identifizieren. Für eine derartige Regelung bieten sich verschiedene Varianten an. So könnten etwa *host provider* gesetzlich verpflichtet werden, staatlichen Stellen zur Suche nach bedenklichen Inhalten Zugang zu den auf ihren Rechnern gespeicherten Daten einzuräumen. *access provider* könnten gezwungen werden, ihre Knotenrechner für verdachtsunabhängige Kontrollen durch staatliche Stellen zu öffnen. Bei dieser Variante zeigen sich wegen der unmittelbaren Staatlichkeit der Kontrollmaßnahmen die oben[813] genannten rechtlichen und technischen Durchsetzungshindernisse.

Provider und Anlagenbetreiber können aber auch zur selbständigen Kontrolle aller Inhalte in ihrem Bereich verpflichtet werden mit der Auflage, bedenkliche Inhalte auszufiltern oder zur Einleitung weiterer Maßnahmen an staatliche Stellen weiterzuleiten. Schließlich können diese Akteure verpflichtet werden, ihren Kunden Software zur Verfügung zu stellen, mithilfe derer diese selbst Inhalte ausfiltern können.

a. Verpflichtung der *provider* und Anlagenbetreiber zur proaktiven Kontrolle

Eine Verpflichtung der *provider* und Anlagenbetreibern zur proaktiven Kontrolle von Inhalten, die über ihre Infrastruktur verbreitet oder zum Abruf bereitgehalten werden, bedeutete für die unter den Anwendungsbereich des Telekommunikationsgesetzes fallenden Akteure eine Einschränkung ihrer Verpflichtung zur Wahrung des Fernmeldegeheimnisses (§ 85 TKG[814]) zumindest hinsichtlich derjenigen Inhalte, die Vertraulichkeitsschutz beanspruchen können.[815] Vertraulichkeitsschutz in der Kommunikation zwi-

als „*misrated*“ entlarvt und ausgefiltert werden vgl. dazu für die *newsgroups Sieber*, CR 1997, 653, IV. 2. b); *von Bonin*, Content on Demand.

811 Dazu oben *I. Verfahrensgebundenheit der Durchsetzung von Inhaltskontrollvorschriften*, S. 162.

812 Vgl. die entsprechenden Aussagen des Direktors des *Bundeskriminalamts (BKA), Leo Schuster*, auf einer Tagung mit Internetprovidern, zu der das BKA am 14./15.12.98 eingeladen hatte bei *Schulzki-Haddouti, Christiane*, Internet-Hilfssheriffs, C't 01 / 1999, S. 16.

813 Dazu oben *1. Identifikation durch den Staat*, S. 165.

814 Vgl. zu dessen Anwendungsbereich FN 520.

815 Vgl. oben *(1) Eingriffe in Art. 10 Abs. 1 GG (Fernmeldegeheimnis)*, S. 168.

schen Privaten würde dadurch weiter reduziert.[816] Zudem läge in einer solchen Verpflichtung zur proaktiven Kontrolle eine Umkehrung der in § 5 Abs. 2, 3 TDG / MDStV getroffenen gesetzgeberischen Entscheidung, die rechtliche Verantwortlichkeit der *provider* zu begrenzen. Wären *provider* zur verdachtsunabhängigen Suche nach bedenklichen Inhalten verpflichtet, verlöre die in § 5 Abs. 2, 3 TDG / MDStV geforderte positive Kenntnis[817] ihre verantwortungsbegrenzende Funktion. Eine Verpflichtung zur proaktiven Kontrolle ist danach im geltenden Recht nicht nur nicht angelegt, sondern stünde im Widerspruch zu erst jüngst geschaffenen Regeln. Technisch stehen einer solchen Kontrollverpflichtungen die bereits oben ausführlich behandelten Hindernisse (v.a. große Datenmengen und Verschlüsselungsmöglichkeit[818]) entgegen.

Danach wäre es allenfalls einem *host provider* technisch möglich, die auf seinem Rechner dauerhaft gespeicherten[819], unverschlüsselten Inhalte zu kontrollieren, an deren Kenntnisnahme er nicht durch § 85 TKG gehindert ist.

b. Verpflichtung der *provider* zur Meldung bedenklicher Inhalte an den Staat

Die Einführung einer gesetzlichen Meldepflicht für bestimmte digitale Kommunikationsinhalte wäre ein Novum des deutschen Rechts. Bisher bestehen gesetzliche Pflichten von Privaten, dem Staat Meldung über ein bedenkliches Verhalten oder einen bedenklichen Zustand Dritter zu machen (Denunziationspflicht) nur unter sehr engen Voraussetzungen[820] bzw. dann, wenn Zustand oder Verhalten des Dritten eine über das Maß an persönlicher Vorwerfbarkeit hinausgehende Bedrohung für die Allgemeinheit darstellt.[821] Es handelt sich dabei grundsätzlich um Fälle akuter Bedrohung der Gesamtbevölkerung oder des Staatswesens, mit denen das Aufkommen bedenklicher Inhalte in internationalen Datennetzen kaum vergleichbar ist.

Eine solche Regelung dürfte zwangsläufig nicht nur diejenigen *provider* erfassen, die als bloße *host* oder *access provider* die Speicherung oder Weiterleitung von Inhalten übernehmen, die erstmalig von Dritten in digitalen Telekommunikationsmedien verbreitet wurden. Dies würde lediglich dazu führen, daß mißtrauische Anbieter sich nicht

816 Zu den bereits bestehenden Defiziten im Vertraulichkeitsschutz privater Kommunikation oben *g. Privatheit der Kommunikation*, S. 105.

817 Vgl. dazu oben S. 119. Auch *Sieber,* MMR 1998, 429ff. mit Verweis auf *Engel-Flechsig/ Maennel/ Tettenborn*, Neue gesetzliche Rahmenbedingungen für MultiMedia, Die Regelungen des IuKDG und des MDStV, 1998, S. 17f.; *Spindler*, NJW 1997, 3193, 3196.

818 Vgl. oben *b. Technologische Schranken*, S. 174.

819 Bei den nicht-statischen Inhalten der Dienste *News*, *chat*, Internettelefonie und (zumindest abgehende) *e-mail* ist bei größeren Datenvolumina eine zuverlässige Kontrolle nicht möglich, vgl. oben FN 519.

820 Vgl. den auf Katalogtaten und den Vortatzeitraum begrenzten und durch zahlreiche Ausschlüsse ergänzten Tatbestand der Nichtanzeige geplanter Straftaten (§§ 138, 139 StGB).

821 Vgl. etwa die ärzliche Meldepflicht bei ansteckenden Krankheiten nach §§ 5ff. BSeuchG.

mehr der Dienstleistungen von *provider*n bedienen, sondern eigene, direkt ans Internet angeschlossene Rechner zur Publikation verwenden.[822]

Werden aber auch *content provider* erfaßt, die auf eigener Infrastruktur Inhalte erstmals publizieren[823], wären diese zur Selbstmeldung auch selbst verfaßter Inhalte gezwungen, sofern diese bedenklich sind. Sofern aufgrund einer solchen Meldung dem Anbieter Strafverfolgung drohen könnte, ist ihre Anordnung mit dem Grundsatz des Selbstbezichtigungsverbots nicht in Einklang zu bringen und läßt realistisch kaum Akzeptanz erwarten.

Wiederum müßte eine solche Bestimmung definieren, welchen Kriterien Inhalte zu genügen haben, um als „bedenklich" meldepflichtig zu sein, wollte sie dem Verdikt der verfassungswidrigen Unbestimmtheit entgehen.[824]

c. Verpflichtung der *provider* zur Verwendung eines *Rating*-Systems

Eine technologische Möglichkeit, digitale Inhalte anhand bestimmter Kriterien zu filtern, bietet ein sogenanntes „*Rating*-System". Die Voraussetzung dafür hat die vom „*World Wide Web*-Konsortium" entwickelte „*Platform for Internet Content Selection (PICS)*"[825] geschaffen. Diese inhaltsneutrale Technologie erlaubt es, digitalen Inhalten, die auf der „Programmiersprache" des *WWW*, der *Hypertext Markup Language (HTML)* beruhen, bei der Inhaltsdarstellung nicht sichtbare Zusatzinformationen (*Metatags*) beizufügen, die von geeigneter Software leicht erkannt werden können. Diese Software erlaubt es weiterhin, anhand einzelner oder einer Kombination verschiedener *Metatags* die Darstellung oder Weiterleitung des Inhalts zu blockieren. Diese *Metatags* können auch Inhaltskategorisierungen enthalten.[826]

---

822 Der damit verbundene Kostenaufwand ist bereits gering und wird noch geringer werden, vgl. *Köhntopp, Kristian*, Paradigmenwechsel... in: Goltzsch, Patrick u.a., Netpol 11, FITUG, Netpol 11 v. 8.11.98.

823 § 5 Abs. 1 TDG stellt mißverständlich auf „eigene" Inhalte ab, die auch die „zu eigen gemachten" (Gesetzesbegründung TDG der Bundesregierung, BT-Drs. 13 / 7385, S. 19) umfassen sollen. *Altenhain, Karsten*, Die gebilligte Verbreitung mißbilligter Inhalte - Auslegung und Kritik des § 5 Teledienstegesetz, AfP 1998, 457 (459f.), will als eigene Inhalte auch solche ansehen, die der Anbieter „in sein Angebot übernommen hat". Wegen der schwierigen Abgrenzung, wann Inhalte „zu eigen gemacht" sind, sollte iSv § 5 Abs. 1 TDG als *content provider* von digitalen Inhalten jeder Anbieter im Sinne von § 3 TDG gelten, der im Bezug auf den fraglichen Inhalt und mit positiver Kenntnis davon die erste Verbreitungshandlung vornimmt.

824 Vgl. FN 780.

825 Vgl. zum Ganzen http://www.w3.org/PICS; *Staiman, Ari*, 20 Fordham Int´l L. J. 866 (1997). Eine graphische Darstellung der Funktionsweise von PICS findet sich unter http://www.sciam.com/0397issue/0397resnickbox1.html.

826 Dabei wird entweder ein Kategoriename („Gewalt", „Sex", „Extremismus") mit einem Wert kombiniert oder eine geeignete oder ungeeignete Alters- oder Personengruppe („ geeignet von 4-8 Jahren", „nicht unter 16", „nichts für Schreckhafte") spezifiziert. Vgl. dazu *Weitzner, Daniel J.*, Internet Family Empowerment White Paper, http://www.cdt.org/speech/empower.html.

Ein *PICS*-basiertes *Rating*-System ist technisch und inhaltlich offen. Es erlaubt einerseits eine Vielzahl (konkurrierender[827]) Bewertungssysteme, sowie die Bewertung (*Rating*) von *WWW*-Inhalten durch den *content provider* selbst oder einen Dritten. *PICS*-Filter können an verschiedenen Punkten des Verbreitungsvorganges telekommunikativer Inhalte eingesetzt werden, etwa bei Suchdiensten, bei *access* oder *host provider*n oder beim Nutzer selbst.

Staatlicher Zwang von *providern* zur Benutzung derartiger *Rating*-Systeme begegnet allerdings erheblichen Bedenken[828]:

Allein die Verpflichtung, nur Inhalte zu beherbergen (*host provider*) oder zum abrufenden Nutzer durchzuleiten (*access provider*), die mit der Bewertung im Rahmen eines eigenen[829] oder fremden[830] *Rating*-Systems ausgestattet sind, führt noch nicht zu einer Inhaltskontrolle. Es müßten zusätzlich inhaltliche Vorgaben gemacht werden, nach denen entsprechend bewertete Inhalte ausgefiltert würden. Diese sind allerdings kaum den Wertungen materieller (nationaler) Inhaltsbindungen durch Straf-, Wettbewerbs-, Urheber- oder Jugendschutzrecht anzupassen. Jede Bewertung eines Inhalts etwa als „strafrechtswidrig“ durch den Inhaltsanbieter, den *provider* oder einen Dritten nähme ein rechtsstaatliches Verfahren vorweg, das ja erst zu dieser Bewertung führen soll.

Jede Bewertung im Rahmen eines solchen Systems ist zudem zwangsläufig subjektiv. Im Falle von Selbst-*Rating* ist eher eine Unterbewertung, im Falle von Fremd-*Rating* etwa durch konservative Organisationen eher eine Überbewertung von bedenklichen Inhalten zu erwarten[831]. Entsprechend ungenau sind auch die Ergebnisse.[832]

Das System erfaßt derzeit nur Inhalte, die auf *HTML* basieren. Dies ist in erster Linie das *World Wide Web*. Selbst wenn aber auch Inhalte anderer Dienste durch ihre Konvertierung in *HTML* erfaßt werden können[833], könnten die *provider* unter dem Gesichtspunkt der Wahrung des Fernmeldegeheimnisses, sowie aus technischen Gründen nicht verpflichtet werden, jede *e-mail* oder jeden *newsgroup*-Beitrag, der ihre *server* benutzt oder durchquert, selbst zu bewerten. Sie müßten vielmehr unbewertete Inhalte gänzlich

827 Vgl. *Dyson, Esther*, Release 2.0, 1997, 170ff.

828 Bisher hat daher auch nur Singapur eine entsprechende Verpflichtung normiert, vgl. *Reuters*, Singapore orders ISP Nannyware, über http://www.wired.com v. 16.3.98.

829 Durch die PICS-Technologie kann jedermann ein eigenes *Rating*-System aufbauen.

830 Es existiert bereits eine Vielzahl von kommerziellen Bewertungssystemen, die mit PICS-Labeln arbeiten, vgl. *Faith Cranor, Laurie / Resnick, Paul/ Gallo, Danielle*, Technology Inventory – A Catalogue of Tools that Support Parents‘ Ability to Choose Online Content Appropriate for Their Children, http://www.research.att.com/projects/tech4kids/t4k.html.

831 Vgl. dazu *von Bonin*, Content Control on the Internet.

832 Vgl. *ACLU*, Fahrenheit 451.2: Is Cyberspace Burning? How Rating and Blocking Proposals Torch Free Speech on the Internet, http://www.aclu.org/issues/cyber/burning.html; *Spectacle.org*, Why I do not rate my site, http://www.spectacle.org/cda/rate.html#report.

833 Viele *e-mail*-Programme unterstützen etwa zur Erweiterung der Darstellungsmöglichkeiten die sog. HTML-Mail, ein Mailformat in HTML; *newsgroups* sind etwa über http://www.dejanews.com ebenfalls im HTML-Format abrufbar.

ausfiltern. Ein damit verbundener faktischer Zwang zur Selbstbewertung durch den *content provider* wäre ein erheblicher Eingriff in die (negative) Meinungsäußerungs- bzw. Pressefreiheit, da dieser dazu gezwungen würde, Meinungen zu äußern, die er sonst für sich behalten hätte[834]. Das gleiche Problem stellte sich auch für unbewertete *WWW*-Inhalte, die die überwiegende Mehrzahl darstellen. Noch 1997 konnte die mit weitem Abstand führende *Rating*-Agentur Bewertungen nur für ein gutes Tausendstel aller *WWW*-Inhalte anbieten[835].

Hingegen könnte Echtzeit-Kommunikation etwa in *chatrooms*, in Live-*multicast*-Inhalten oder in der Internet-Telephonie derzeit überhaupt nicht in ein obligatorisches *Rating*-System integriert werden. Daß aber identische digitale Inhalte nur dann von einem gesetzlich auferlegten *Rating*-System erfaßt werden sollten, wenn sie in einem bestimmten Datenformat (*HTML*) vorliegen, sonst aber nicht, wäre als gesetzliches Differenzierungskriterium kaum sinnvoll. Der verpflichtete *provider* könnte die Kommunikation rechtswidriger Inhalte so nicht wirksam verhindern.

Ein obligatorisches *PICS*-Filtersystem auf der Ebene der *provider* würde zwangsläufig Inhalte blockieren, die ohne ein solches System frei zugänglich wären. Untersuchungen mit derzeit verfügbarer Software lassen keinen Zweifel daran, daß eine für eine gesetzliche Vorschrift hinreichend bestimmbare Beschränkung der Filterung auf rechtswidrige Inhalte nicht möglich ist.[836] Daher läge in einer Filterungs-Verpflichtung der *provider* auch ein Eingriff in die Informationsfreiheit der Nutzer, denen zwar aufgrund alternativer Einwahlmöglichkeiten (ausländischer *provider*, Satellit) und der Verschlüsselungstechnologie[837] der Zugang zu allgemein zugänglichen Inhaltsquellen nicht vollends abgeschnitten, aber dennoch erschwert wird. Angesichts der genannten Ungenauigkeit der Filterung wäre eine gesetzliche Verpflichtung der *provider* zur Benutzung eines *Rating*-Systems eine unverhältnismäßige Einschränkung der Informationsfreiheit.

Ein derartiges *Rating*-System auf Providerebene wäre mithin als Gegenstand gesetzlicher Vorgaben ungeeignet. Als auf Freiwilligkeit basierendes Angebot an die Nutzer im Rahmen einer bestimmten Geschäftspolitik oder politisch-weltanschaulichen Ausrichtung des Anbieters dagegen ist es ein wesentliches Element privaten Selbstschutzes vor

834 In den USA besteht eine ähnliche verfassungsrechtliche Lage. Nach *Riley v. National Federation of the Blind of North Carolina Inc*., 487 U.S. 781 (1988) unterliegen Regelungen, die Sprecher zu Angaben zwingen, die sie sonst nicht gemacht hätten, einer extrem strengen Prüfung unter dem Ersten Verfassungszusatz („exacting" First Amendment scrutiny).

835 *SurfWatch* führte 1997 etwa 350.000 bewertete *WWW*-Seiten, als bereits über 300 Millionen Seiten existierten. Vgl. *Dyson*, a.a.O.

836 Vgl. FN 832.

837 Verschlüsselte Inhalte entziehen sich letztlich einem *Rating*-System völlig, da auch Falschbewertungen nicht überprüft werden können. Würde ein PICS-System auf *provider*ebene alle verschlüsselten Inhalte (als pauschal falschbewertet) blockieren, liefe dies auf ein völliges Verschlüsselungsverbot hinaus.

rechtswidrigen Inhalten. *Access provider* und Suchdienste könnten auch damit werben, daß die von ihnen vermittelten Inhalte ein Bewertungssystem durchlaufen haben.[838]

3. Identifikation durch Nutzer

Am wahrscheinlichsten ist die Identifikation potentiell rechtswidriger digitaler Kommunikationsinhalte durch den Nutzer. Ihn gesetzlich zur Meldung bedenklicher Inhalte zu verpflichten, würfe neben den oben genannten rechtlichen Bedenken zur Denunziationspflicht auch offensichtliche Normakzeptanzprobleme auf: Entweder der Nutzer „stolpert" (trotz getroffener Sicherungsmaßnahmen) ungewollt über einen bedenklichen Inhalt. In diesem Fall wird er gegebenenfalls freiwillig von einer durch den Staat oder den *provider* eingerichteten „*Hotline*" Gebrauch machen, um den Inhalt zu melden. Sucht er interessiert nach bestimmten rechtswidrigen Inhalten oder unterstützt er zufällig gefundene, wird ihn auch eine Meldepflicht nicht dazu bringen, diese zu melden, zumal ihm ausreichend Möglichkeiten zur Verfügung stehen, sich gegen staatliche Ermittlungen zu wehren, die ihm etwa einen Verstoß gegen die Meldepflicht nachzuweisen versuchen. Ob eine entsprechende gesetzliche Verpflichtung, etwa durch ihre bloße Appellfunktion Nutzer dazu bewegt, bedenkliche Inhalte zu melden, die es ohne diese Verpflichtung nicht getan hätten, muß bezweifelt werden.

4. Ergebnis

Möglicherweise rechtswidrige Inhalte in digitalen Medien zu identifizieren, stößt in allen denkbaren regulatorischen Konstellationen auf erhebliche Probleme. Diese sind sowohl rechtlicher, als auch technischer Natur. Welche im Kontext der Kommunikation digitaler Inhalte, in dem das Recht schwerlich mit der technischen Entwicklung Schritt halten kann, bedeutsamer sind, sei dahingestellt. Jedenfalls scheint eine auch nur annähernd vollständige Identifikation rechtswidriger – und möglicherweise rechtswidriger – digitaler Kommunikationsinhalte aussichtslos.

III. Sanktionierung rechtswidriger Inhalte

Sofern die Identifizierung bedenklicher digitaler Inhalte trotz der dargestellten Schwierigkeiten gelungen ist und deren Rechtswidrigkeit im rechtsstaatlichen Verfahren endgültig festgestellt wurde, können verschiedene Maßnahmen durch Behörden oder Gerichte angeordnet werden, um die weitere Verbreitung dieser Inhalte zu verhindern. Auch diese Maßnahmen begegnen in digitalen Medien Durchsetzungsproblemen.

838 Dazu ausführlicher unten *3. Abschnitt: Möglichkeiten kooperativer Kontrolle*, S. 201.

1. Zugangssperrung zu rechtswidrigen Inhalten

Zu denken ist zunächst an die *Sperrung des Zugangs* zu einem rechtswidrigen Inhalt. Diese Maßnahme ist ihrer Natur nach auf Inhalte beschränkt, die an einem bestimmten Ort gespeichert sind, zu dem abrufende Nutzer Zugang haben. So kann etwa der Zugang eines *e-mail*-Nutzers zu seinem Postfach auf dem *server*-Rechner seines *mail providers* gesperrt werden oder - der häufigere Fall - der Zugang zu Text-, Ton- oder Bildinhalten auf frei zugänglichen *servern* im *WWW*.

a. Schwierigkeiten der Zugangssperrung durch verschiedene Akteure

Durchsetzungsprobleme im Hinblick auf Zugangssperren variieren mit den funktionellen Merkmalen des Akteurs, der die Sperre vornimmt.

aa. Host provider

Sofern die Inhalte, zu denen der Zugang gesperrt werden soll, auf *ausländischen servern* gespeichert sind, scheitern Aufforderungen des deutschen Staates an *server*-Betreiber oder die sie beherbergenden Staaten, den Zugang zu den betreffenden Inhalte zu sperren jedenfalls dann, wenn diese im Ursprungsland nicht rechtswidrig sind oder dort internationale Rechts- oder Vollstreckungshilfeabkommen keine Anwendung finden.[839]

Ein *inländischer provider* kann dagegen - sofern ihn nach dem einschlägigen Sachrecht eine Verantwortlichkeit trifft[840] - verpflichtet sein, den Zugang zu Inhalten zu sperren. Technisch ist ihm dies jedoch nur dann möglich, wenn sich die fraglichen Inhalte auf *server*n befinden, die er *selbst kontrollieren* kann.

Hinsichtlich aller Inhalte, die auf *fremden server*n gespeichert sind, ist der *host provider* schon deshalb machtlos, weil er zu diesen Rechnern regelmäßig keine Verbindung unterhält oder herstellt, die er gegebenenfalls sperren könnte. Er kann allenfalls auf seiner Infrastruktur gespeicherte Inhalte daraufhin untersuchen, ob sie *hyperlinks* zu anderswo „gehosteten" als rechtswidrig erkannten Inhalten enthalten und diese - unter Eingriff in die von seinen Kunden erstellten Inhalte - deaktivieren. Ob er dazu bereits gesetzlich verpflichtet ist, hängt davon ab, ob den *host provider* aus § 5 Abs. 2 TDG / MDStV eine Verantwortlichkeit für die auf seinen Rechnern gespeicherten Links trifft. Diese Frage ist umstritten.[841] Ungeachtet aller bereits strukturellen Zweifel an einer Haftung des *host*

839 Zu Datenoasen im Internet und ihrer Funktionsweise vgl. *Hoeren, Thomas,* MMR 1998, 297; *Goltzsch, Patrick,* Datenoasen I / II, FITUG, Netpol 11 v. 8.11.98.

840 Siehe oben *3. Übertragung geltender Grundsätze der Verantwortlichkeit auf die Akteure digitaler Kommunikation*, S. 112.

841 Vgl. *Ernst, Stefan,* NJW-CoR 1997, 224; *Flechsig, Norbert P. / Gabel, Detlev,* CR 1998, 351; *Vassilaki, Irini E.,* CR 1999, 85.

*provider*s[842], setzt § 5 Abs. 2 TDG / MDStV die positive Kenntnis[843] des *host provider*s von dem Link und seinem Zielinhalt voraus, die in der Regel fehlen wird. Ob er zur Überprüfung auf seinen Rechnern befindlicher Speicherinhalte auf *hyperlinks* zu bestimmten Inhalten und gegebenenfalls zu deren Deaktivierung aufgrund Gesetzes (etwa gefahrenabwehrrechtlich) verpflichtet werden kann, richtet sich nach § 5 Abs. 4 TDG / § 18 Abs. 2 S. 2 MDStV. Für Sperrungsanordnungen gegenüber dem *host provider* verlangt nur die Bundesvorschrift dessen positive Kenntnis vom Inhalt (Link). Wird der *host provider* zur vollständigen Durchsuchung seiner Rechner auf derartige *hyperlinks* verpflichtet, läge darin eine Maßnahmen gegen einen Nicht-Störer (der *host provider* ist weder Urheber noch Verbreiter des *hyperlinks*), die zudem in die Meinungsfreiheit aller Inhalteanbieter eingriffe, die auf dem *server* dieses *providers* Inhalte zum Abruf bereit halten.[844] Derartiges wäre wegen der strengen Verhältnismäßigkeitsanforderungen nur in extremen Ausnahmefällen denkbar.[845]

bb. Access provider

Access provider befinden sich an der Schnittstelle zwischen dem Nutzer und den *server*-Rechnern, von denen die Nutzer Inhalte abrufen. Sie scheinen daher in besonderem Maße in der Lage zu sein, deren Zugang zu als rechtswidrig identifizierten Inhalten zu sperren.[846]

Dabei sind zwei Möglichkeiten denkbar. Zum einen können *access provider* die für die Kunden *ankommenden* Datenpakete daraufhin überprüfen, ob sie Dateien enthalten, deren Inhalt als rechtswidrig identifiziert worden ist. Dieses kann anhand eines Abgleichs der Datenpakete mit einer sogenannten „Negativliste" erfolgen, in der die entsprechenden Dateinamen oder Internet-Adressen (*URL*s[847]) gespeichert sind. Zum anderen könnten *abgehende* Nutzerabrufe etwa nach *WWW*-Inhalten oder *newsgroups* anhand der „Negativliste" geprüft werden. Wird ein derart „indizierter" Inhalte abgerufen oder zugespielt, würde der *access provider* dessen Weiterleitung an den Nutzer blockieren. Dieser Gedanke fand seinen Niederschlag in dem von deutschen Providern konzi-

842 Siehe oben *3. Übertragung geltender Grundsätze der Verantwortlichkeit auf die Akteure digitaler Kommunikation*, S. 112.

843 Siehe oben *3. Übertragung geltender Grundsätze der Verantwortlichkeit auf die Akteure digitaler Kommunikation*, S. 112.

844 Zu derartigen mittelbaren Grundrechtseingriffen vgl. unten FN 1074.

845 Nicht anders kann es folglich beurteilt werden, wenn *provider* gesetzlich dazu verpflichtet würden, sich von ihren Kunden vertraglich entsprechende Durchsuchungsbefugnisse einräumen zu lassen.

846 Die dahingehenden Möglichkeiten gegenüber ansonsten von jeder Inhaltsverantwortlichkeit ausgeschlossenen *access provider*n gem. §§ 5 Abs. 4 TDG, 5 Abs. 3 S. 2 iVm 18 Abs. 3 MDStV drücken diese Einschätzung auch des Gesetzgebers aus.

847 *Uniform Ressource Locator*, gewissermaßen der Name des speziellen Inhalts im Netz.

pierten „*WebBlock*“-System, das allerdings überwiegend als technisch ungeeignet und rechtlich fragwürdig bezeichnet wurde.[848]

Solche Sperrungsversuche sind außerdem wegen der großen Menge der duplizierten („gespiegelten“) Inhalte nicht wirksam und zielgenau möglich. *Newsgroups* werden nach dem *store-and-forward*-Prinzip in regelmäßigen Abständen komplett auf alle *server* weiterverschoben, die die betreffende Gruppe abonniert haben. Somit wird gewährleistet, daß auf allen *server*n in kurzer Zeit die neuesten Nachrichten abrufbar sind. Jeder Nutzer hat aber nicht nur auf einen, sondern – wenn gewünscht – auf weltweit alle *news server* Zugriff. Inhalte von *WWW*-Seiten können mit jedem üblichen browser dupliziert und entweder lokal gespeichert oder – als sog. „*mirror site*“ – unter einer anderen Adresse wieder ins Internet gestellt werden. Dies geschieht häufig als Reaktion auf staatliche Sperrungen: Als zur Verhinderung der Zugangs zu der in Deutschland verbotenen Ausgabe 154 der Zeitschrift ”radikal” der niederländische *server* „xs4all“ gesperrt wurde, war die fragliche Zeitschrift zeitweise von 60 anderen Internet-Adressen[849] sowie über 25 Telefondirektleitungen in den Niederlanden und die *newsgroup* „de.org.politik.spd“, den ”virtuellen Ortsverein” der SPD, abrufbar. Deutsches Vorgehen gegen den kanadischen Neonazi *Ernst Zuendel* führte dazu, daß dessen Seiten auf zahlreichen US-Universitäts-*servers* gespiegelt wurden und sogar vom *server* des renommierten *Massachusetts Institute of Technology (MIT)* abrufbar waren, dessen Sperrung sich keine wichtige Forschungseinrichtung der Welt leisten kann.

b. Schwierigkeiten der Sperrung bestimmter Inhalte und Dienste

Unabhängig von dem für die Zugangssperrung in Anspruch genommenen Akteur müssen Sperrungsanordnungen so eng wie möglich auf den bestimmten als rechtswidrig erkannten Inhalt beschränkt werden. Eine zu weitreichende Sperrungsanordnung würde zwangsläufig auch die Erreichbarkeit rechtmäßiger Inhalte beeinträchtigen. Wenn etwa ein ganzer *server* anhand seiner IP-Adresse gesperrt wird, ist jede Kommunikation auch rechtmäßiger Inhalte mit ihm unterbrochen. So wurden bei der Sperrung der Adresse des niederländischen *server*s „xs4all“, von dem die in Deutschland verbotene Ausgabe Nr. 154 der Zeitschrift „Radikal“ abgerufen werden konnte, nicht nur die von der Generalbundesanwaltschaft beanstandeten Inhalte, sondern auch die *WWW*-Seiten von über

848 *Bruells, Peter,* Design- und Machbarkeitsstudie der Komponenten *NewsWatch* und *WebBlock*, http://www.medienrat.de/doku/studie/index.html; *Köhntopp, Marit, Köhntopp, Kristian,* Stellungnahme zur Design- und Machbarkeitsstudie der Komponenten *NewsWatch* und *WebBlock*, http://www.medienrat.de/doku.html, *Gramm, Tobias; Schneider, Michael,* Zur zivilrechtlichen Haftung eines Internet Service *providers* der einzelne Dienste oder das Gesamtangebot eines anderen *providers* sperrt, http://www.medienrat.de/doku.html . Von der Bundesanwaltschaft wird das System aber anscheinend für zumutbar gehalten, vgl. *Generalbundesanwalt beim BGH,* Einstellungsverfügung v. 13.2.98 im Verfahren 2 BJs 104/96-4, MMR 1998, 93.

849 Vgl. *Wenning*, Jur-PC Web Dokument 46/1998. Zu ähnlichen britischen Erfahrungen, vgl. *N.N.*, Nottinghams Sherriffs geben auf, http://www.intern.de/97/17/3.htm.

6.000 Anbietern gesperrt. Ebenso wurde der *e-mail*-Verkehr mit diesem *server* durch die Adreßsperrung gestört.[850] Ebenso verhält es sich, wenn anhand der Port-Nummer nur ein Dienst auf einem *server* gesperrt wird.[851]

Dies wäre - soweit zurechenbar vom Staat veranlaßt - jedoch ein nicht erforderlicher bzw. im engeren Sinne unverhältnismäßiger Eingriff in die Meinungsäußerungsfreiheit der Autoren derartig gesperrter rechtmäßiger Inhalte sowie in die Informationsfreiheit ihrer Nutzer.

Je genauer aber die Sperrung eingegrenzt wird, desto leichter kann sie umgangen werden. Wird lediglich ein bestimmter *WWW*-Inhalt anhand seiner *URL* gesperrt, so kann diese Adresse rasch verändert und der Inhalt damit selbst von dem gleichen *server* wieder unverändert abgerufen werden. Als der *server* "xs4all" auf Druck deutscher Ermittlungsbehörden vom Deutschen Forschungsnetz gesperrt wurde, wechselte er seine IP-Adresse halbstündlich und machte so die Sperrung weitgehend wirkungslos.[852] Wenn einzelne Seiten aus mehreren „Bausteinen" bestehen, die etwa als *„frames"* oder *„inline links"*[853] erst beim Aufbau der abgerufenen Seite aus verschiedenen Quellen bezogen und zusammengesetzt werden, und von diesen „Bausteinen" nur einer rechtswidrige Inhalte enthält, so müßte eine verhältnismäßige Sperrungsanordnung auf diesen einen „Baustein" bzw. seinen Dateinamen begrenzt werden, weil eine weitergehende Sperrung nicht erforderlich wäre. Einer solchen Anordnung jedoch kann, sogar ohne daß sich die Abrufadresse des Gesamtinhalts ändern müßte, durch bloße Änderung des Namens des rechtswidrigen „Bausteins" begegnet werden.

Die Unterbrechung etwa einer Kabelverbindung innerhalb des „Internet" ist in allen digitalen Medien, die paketadressierte Inhalte nach dem TCP/IP-Protokoll verbreiten, zur Zugangssperrung gänzlich ungeeignet. Das Transportprotokoll ist bestimmungsgemäß dazu programmiert, sich in diesem Fall alternative Verbindungswege zu suchen.[854] Selbst für den Fall, daß ein einzelner Nutzer jede Verbindung mit seinem *access provider* verlöre, kann er bereits heute über Telefondirektleitungen oder Satellit direkt auf alle Inhalte etwa im Internet zugreifen.[855]

---

850 Vgl. *Sieber,* CR 1997, 653ff. IV. 3. c).

851 Zum ganzen ausführlich *Sieber,* a.a.O..

852 *Sieber,* CR 1997, 653 ff.

853 Vgl. dazu *Berners-Lee, Tim,* Axioms of Web Architecture :2, http://www.w3.org/DesignIssues/LinkLaw.

854 Der vom US-Verteidigungsministerium konzipierte und finanzierte Vorgänger des Internet, das ARPA-Net sollte sicherstellen, daß auch bei Ausfall verschiedener Netzabschnitte selbständig alternative Datenverbindungen aufgebaut würden, und so auch im Falle eines Atomschlages die verschiedenen militärischen Einrichtungen der USA kommunikationsfähig blieben. Diese Grundstruktur ist bis heute erhalten geblieben. Vgl. *Sieber*, CR 1997, 581 (594).

855 Vgl. dazu im Einzelnen *Sieber,* CR 1997, 653, dort FN 182ff.

2. Löschung rechtswidriger Inhalte

Verschiedene der genannten Durchsetzungshindernisse können vermieden werden, wenn den verantwortlichen Akteuren - soweit sie dazu technisch in der Lage sind[856] - sofort die Löschung der als rechtswidrig identifizierten Inhalte aufgegeben wird.

Damit ist der Inhalt von dem betroffenen *server* nicht mehr abrufbar, ohne daß es umfangreicher Maßnahmen zur Zugangssperrung bedarf. Die Erreichbarkeit und die Verbreitungstiefe des Inhalts wird jedoch - auch nach bisherigen Erfahrungen mit staatlichen Durchsetzungsmaßnahmen - selbst durch eine Löschung insgesamt nicht entscheidend beeinträchtigt. Internetnutzer sind vielfach bestrebt, Sperrungs- wie Löschungsgebote, die als staatliche Zensur empfunden werden, unwirksam zu machen.[857] Durch die weltweiten Möglichkeiten schneller Kommunikation verbreiten sich Nachrichten von staatlichen Löschungsanordnungen so schnell, daß an der weiteren Erreichbarkeit der fraglichen Inhalte interessierte Nutzer diese schneller kopieren, spiegeln und anderweitig sichern können, als eine rechtsstaatliche Löschungsmaßnahme durchgeführt ist. Zudem war bei bisher bei derartigen Fällen immer ein hoher Aufmerksamkeitsgewinn der rechtswidrigen Inhalte zu verzeichnen, der zu massenhaften Abrufen dort geführt hat, wo gerade weitere Kenntnisnahme verhindert werden sollte - und wohl auch hätte verhindert werden können, wenn nicht zu staatlichen „Zensurmaßnahmen“ gegriffen worden wäre.

Sollen rechtswidrige Inhalte von *newsgroups* gelöscht werden, muß eine Löschungsanordnung nur an einen oder wenige *news server* wirkungslos bleiben, weil für den interessierten Nutzer weltweit alle *news server* gleich einfach erreichbar sind.

3. Ergebnis

Können trotz aller rechtlichen und technischen Schwierigkeiten digitale Kommunikationsinhalte in rechtsstaatlicher Weise als rechtswidrig identifiziert werden, ist es jedoch kaum möglich, deren weitere Verbreitung oder Erreichbarkeit effektiv durch Sperrungs- oder Löschungsgebote zu verhindern. Zur Löschung rechtswidriger Inhalte kann – unter Einschränkung durch die bei FN 849 genannten Maßnahmen Dritter – wirksam nur der *content provider* selbst verpflichtet werden. Dazu müßte er jedoch seinerseits identifiziert werden können.

856 Vgl. zu dieser Voraussetzung auch § 18 Abs. 2 MDStV. Nach dem oben Gesagten sind nur *host provider* in der Lage, Inhalte auf eigenen Servern zu löschen.

857 Vgl. oben FN 849ff.

IV. Identifizierung und Sanktionierung von Anbietern digitaler Kommunikationsinhalte

Nach den bestehenden Vorschriften zur Inhaltskontrolle[858] können verschiedene Inhaltsmittler für rechtswidrige Kommunikationsinhalte verantwortlich sein. Das Gesetz denkt dabei regelmäßig zunächst an die Verantwortlichkeit des sogenannten *content providers*, also des Anbieters, der im Bezug auf den Inhalt die erste Verbreitungshandlung vornimmt, etwa das Unternehmen, das die wettbewerbswidrige Anzeige schaltet oder die Partei, die rechtswidrige Dokumente an einen *WWW-server* schickt, von dem sie zum Abruf bereitgehalten werden. Auch §§ 5 Abs. 1 TDG / MDStV will den *content provider* erfassen[859], ist jedoch wegen seines Abstellens auf das irrelevante Merkmal des „eigenen" Inhalts unglücklich formuliert.[860]

Diese Verantwortlichkeit kann gegenüber den *content providern* nur durchgesetzt werden, wenn ihre Identifizierung gelingt. Diese wird jedoch durch die Möglichkeit anonymer oder pseudonymer Inhaltsangebote ebenso erschwert wie durch die Beliebigkeit von Authenzität in digitalen Medien.

1. Anonymität

a. Das Abgrenzungsproblem im geltenden Recht: Anonymitätsgarantie für Nutzer, Anonymitätsverbot für Anbieter

Nach der durch die „Multimediagesetze" des Bundes und der Länder geschaffenen Rechtslage ist ein *Anbieter* von Medien- oder Telediensten zwar gemäß § 6 Abs. 1 MDStV für alle, gemäß § 6 Abs. 1 TDG für seine geschäftsmäßigen Angebote zur Angabe seines Namens und seiner Anschrift verpflichtet. Dagegen ist die anonyme *Inanspruchnahme und Bezahlung* von Tele- und Mediendiensten in §§ 13 Abs. 1 MDStV, 4 Abs. 1 TDDSG ausdrücklich garantiert.

Fraglich ist, wo die Grenze zwischen *Inanspruchnahme* von Diensten durch *Nutzer* und *Angebot* zu ziehen ist. „Nutzer" sind nach § 3 Nr. 2 TDG / MDStV Personen, die Dienste „nachfragen".[861]

858 Vgl. oben *I. Systematik staatlicher Inhaltskontrolle*, S. 26.

859 Dies ergibt sich aus der Gesetzesbegründung zu § 5 Abs. 1 TDG, vgl. BT-Drs. 13/7385 S. 19, zu § 5 Abs. 1 MDStV, Gesetzbegründung S. 6, die klarer von der Verantwortlichkeit von Anbietern für die „von ihnen selbst angebotenen" Inhalte spricht.

860 Vgl. oben FN 823. Er wird dementsprechend auch im nicht-juristischen Schrifttum falsch verstanden, *Ferderrath, Hannes*, ZUM 1999, 177 meint, § 5 I TDG spreche von dem, der Inhalte „anfertigt".

861 Das Gesetz entfernt sich damit von dem ansonsten gebräuchlichen technischen Nutzungsverständnis, wonach Nutzer derjenige ist, dem der Datenstrom entgegenfließt, und definiert den Nutzer als Nachfrager von Diensten im wirtschaftlichen Sinn.

Damit wird unzweifelhaft demjenigen, der reine Nutzungshandlungen vornimmt, also etwa kinderpornographische Bilder von *WWW*-Seiten *abruft*, schon durch das Gesetz Anonymität zugebilligt. Durchsetzungshindernisse etwa bei der Strafverfolgung nach § 184 Abs. 5 StGB werden damit zugunsten des Privatheitsschutzes in Kauf genommen.

In gleicher Weise nehmen auch *Verfasser von e-mail- und news-Nachrichten* sowie Teilnehmer im *chatroom* eine vom *provider*[862] zur Verfügung gestellte hard- und softwaremäßige Infrastruktur in Anspruch. Ebenso verhält es sich bei Nutzern, die etwa von der durch ihre *access / host provider* angebotenen Möglichkeit Gebrauch machen, *private Homepages* zu erstellen, die dann im *WWW* abrufbar sind[863]. Derartige Dienste werden auch von reinen *host providern* im Internet angeboten und sind werbefinanziert, also für den Nutzer kostenlos[864].

Fraglich ist, ob diese Verfasser von *e-mail-*, *news-* und *chat*-Nachrichten und Autoren privater Homepages als *Nutzer* Anonymitätsschutz genießen oder nicht doch als *Anbieter* zu sehen sind. Für den Anbieterbegriff des § 3 TDG /MDStV ist erforderlich, daß *Dienste* „zur Nutzung bereitgehalten" werden. Unter dem Wort *Dienst* wird aber kaum die Darbietung – die *e-mail-* oder *news*-Nachricht, die Homepage – selbst verstanden werden können, sondern die technisch-organisatorische Gesamtheit, im Rahmen derer die Übermittlung stattfindet.[865] Einen solchen Dienst bietet aber der Autor einer *e-mail-*, *news-* oder *chat*-Nachricht genausowenig selbst an wie der Autor einer privaten Homepage, sondern allenfalls derjenige, auf dessen Speichermedium die Homepage sich befindet[866] oder der den *chat*, *mail* oder *news server* zur Verfügung stellt. Dies anders zu sehen und die genannten Akteure statt als Nutzer als Anbieter zu bezeichnen[867] wäre *contra legem* (Widerspruch zu § 3 Nr. 2 TDG /MDStV). Ihnen eine „Doppelrolle" als Nutzer *und* Anbieter zuzusprechen, führte zu unauflösbaren Widersprüchen bei der Frage der Anonymität.

862 Nicht nur Dienste wie „*Hotmail*", http://www.hotmail.com, die rein internet-basierte *e-mail*konten anbieten, sondern auch die Internet - *access provider* wie *AOL*, *CompuServe* und *T-Online*, die *e-mail* oder *chat* als proprietären Service anbieten, nehmen dabei Funktionen des providers war.

863 Diese Möglichkeit räumen etwa die bekannten deutschen Online-Dienste *AOL, CompuServe* und T-*Online* ein.

864 Derartiges wird etwa von Diensten wie www.geocities.com, www.blabla.com, kostenlos.freepages. de oder home.pages.de angeboten.

865 Dies ergibt sich etwa aus der Formulierung von § 2 Abs. 2 Nr. 3 TDG („Angebote *zur Nutzung* des Internet", Herv. v. Verf.) und § 2 Abs. 2 Nr. 4 MDStV („Abruf*dienste, bei denen ....darbietungen* ... übermittelt werden", Herv. v. Verf.).

866 Klargestellt wird dies auch in Art. 14 des Vorschlags für eine europäische E-Commerce-Richtlinie, Richtlinien der EG zum elektronischen Handel (Vorschlag KOM(1998)586 endg. (FN 14)), wo der *host provider* als jemand bezeichnet wird, der Informationen „im Auftrag des Nutzers des Dienstes" speichert.

867 So im Falle von Homepages die Gesetzesbegründung zum TDG, BT-Drs. 13/7385, S. 19.

Einzig gangbarer Weg nach geltender Rechtslage ist, Nutzer dieser Dienste aus dem Anbieterbegriff des § 3 TDG / MDStV - und damit auch aus dem Anwendungsbereich des § 6 TDG / MDStV - auszunehmen.[868]

b. Anonymität als technische Möglichkeit in digitalen Medien

Dieses Ergebnis ist auch systemkonform, wenn ein Blick auf die technischen Möglichkeiten geworfen wird, Inhalte anonym zu nutzen oder anzubieten.

Eindeutige Nutzungshandlungen wie etwa der Abruf von Inhalten von Severrechnern im *WWW* können auf verschiedene Arten so durchgeführt werden, daß sie nicht zur Identität des Nutzers zurückverfolgt werden können. Wer sich etwa über einen kommerziellen *access provider* mit dem Internet verbindet, erhält bei jeder „Sitzung" eine sog. dynamische IP-Adresse, deren Nutzer nur unter Abgleich mit den Verbindungsdaten des *providers* festgestellt werden kann. Auch auf diese Weise kann der Name des Nutzers nicht in Erfahrung gebracht werden, wenn dieser entsprechend seinem Recht aus §§ 4 Abs. TDDSG, 14 Abs. 1 MDStV anonym oder unter Pseudonym die Dienste des *access provider*s nutzt[869]. Der Benutzer an öffentlichen Internetterminals ist grundsätzlich nicht identifizierbar. Zusätzlich kann jeder Nutzer zur Verschleierung seiner IP-Adresse einen Anonymisier-Service benutzen[870]. *WWW*-Seiten, die etwa eine *online*-Registrierung verlangen können die gemachten Angaben mit Ausnahme der *e-mail*-Adresse, die aber ebenfalls innerhalb von fünf Minuten anonym eingerichtet werden kann, nicht überprüfen. Problematisch ist bisher noch die Wahrung von Anonymität bei der Nutzung von kommerziellen Angeboten, die bezahlt werden müssen. Die dort notwendige Angabe von Name und Kreditkartennummer oder Bankverbindung ermöglicht noch jederzeit die Identifizierung des Nutzers. Es existieren jedoch bereits zahlreiche Technologien, die anonymes Bezahlen digitaler Kommunikationsinhalte selbst (etwa Software oder *online*-Zeitungen) oder durch sie bestellter Waren und Dienstleistungen - wie bei der Benutzung von Bargeld - ermöglichen.[871]

---

868 Nach dieser Betrachtung wird augenfällig, wo das Problem der gesetzlichen Begriffsbestimmungen liegt: Ein *Inhalt*, auf den § 5 TDG / MDStV abstellt, ist nicht synonym mit einem *Dienst*, auf den § 3 TDG / MDStV abstellt. Da der denklogisch auch für die Anwendung von §§ 5, 6 TDG / MDStV vorrangig zu klärende Anbieterbegriff aber nur über das Bereithalten von *Diensten* definiert ist, fällt jeder Anbieter von Inhalten, der nicht zugleich auch *Dienste* anbietet, aus der Anbieterdefinition heraus. Dies ist für die Verantwortlichkeit unschädlich, da der auf diese Akteure anwendbare § 5 Abs. 1 TDG / MDStV ohnehin nur auf die allgemeine Rechtslage verweist, vgl. dazu oben S. 117f.

869 Unzutreffend ist insofern, wenn *Dr. K. Schelter*, ehem. Staatssekretär im BMI, die *access provider* und ihre Gratisangebote, bei denen Namensangaben der Nutzer nicht überprüft werden, für die anonyme Nutzung des Internet verantwortlich macht. Vgl. *Schulzki-Haddouti, Christiane*, Nicht den Anschluß verlieren, http://www.heise.de/ct/98/18/084.html.

870 Etwa http://www.anonymizer.com.

871 *Froomkin, Michael A.*, Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases, 15 U. Pittsburgh Journal of Law and Commerce 395 (1996) http://www.law.miami.edu/~froomkin/articles/oceanno.htm; *Chaum, David*, Achieving Electronic Privacy, Scientific American, August 1992, 96; http://ganges.cs.tcd.ie/mepeirce/Project/

Aber auch die oben diskutierten erweiterten Nutzungsmöglichkeiten wie etwa das Verschicken von *e-mail*, das Posten von *news*-Nachrichten oder die Teilnahme in einem *chatroom* sind technisch problemlos anonym möglich. Soweit dabei über das *WWW* auf diese Dienste zugegriffen wird, sind die oben genannten Anonymisierungsmöglichkeiten nutzbar. Für anonyme *e-mail* stehen im Netz zahlreiche „*anonymous remailer*" zur Verfügung, bei deren korrekter Benutzung eine Rückverfolgung einer *e-mail* zum Absender nicht möglich ist.[872] Wer anonym oder unter pseudonym eine private Homepage auf einem *server*-Rechner im *WWW* zum Abruf bereitstellen will, kann sich bei einem der genannten Dienste[873] unter falschem Namen unidentifizierbar registrieren.

Diese für das Internet geltenden technischen Merkmale sind nicht unbedingt auf andere Netze zu übertragen, in denen auch digitale Inhalte kommuniziert werden können. Sofern solche Netze etwa nicht das TCP/IP-Protokoll oder einen anderen offenen Standard benutzen, sondern ein von ihren Betreibern kontrolliertes proprietäres Kommunikationsprotokoll, können in solche Protokolle Rückverfolgungsmöglichkeiten eingebaut sein, die die anonyme Nutzung und das anonyme Angebot von digitalen Inhalten verhindern.

c. Weitreichende Folgen der Verhinderung von Anonymität

Die bereits von Interessengruppen und Europäischer Union erhobene Forderung, Anonymität im Internet weiter einzuschränken und dies technologisch durch die Entwicklung zuverlässiger Rückverfolgungstechniken zu sichern[874], ist praxisfern und auch rechtspolitisch zweifelhaft. Zunächst müßte eine solche Regelung eine klare Grenzziehung zwischen der unbestritten wünschenswerten Möglichkeit anonymer bzw. pseudonymer *Nutzung*[875] und dem verbotenen *Anbieten* erlauben. Dies ist - wie oben gezeigt - extrem schwierig. Solche Vorhaben machten eine strikte Kontrolle aller *access provider* weltweit, ein weltweites Verbot der „*anonymous remailer*" und „*anonymizer*", sowie

---

Chaum/sciam.html. Vgl. auch *Reuters*, Immer mehr Banken testen Zahlungen im Internet, SZ v. 7.8.98, S. 19; vgl. unten bei FN 987f.

872 *Froomkin*, (FN 871).

873 Vgl. oben FN 864.

874 Vgl. *Europäische Kommission*, Illegale und schädigende Inhalte im Internet, KOM (96) 487, 14f.; den gleichen Bedenken begegnet auch die Forderung von Oberstaatsanwalt *Klaus Finke*, Hannover, Online-Dienste zu verpflichten, die Datenspuren, die jeder Nutzer hinterläßt, langfristig zu speichern, http://www.spiegel.de/homepage/home/strafverfolgung_in.html. Diese Forderung wird mittlerweile auch offiziell vom Bundesinnenministerium unterstützt, vgl. *Schulzki-Haddouti, Christiane*, Nicht den Anschluß verlieren (Interview mit *Prof. Dr. Kurt Schelter*, Staatssekretär im Bundesinnenministerium), http://www.heise.de/ct/98/18/084.html.

875 Die Möglichkeit von Anonymität und Fälschung im Netz gibt dem Nutzer Verhandlungs- und Selbstbestimmungsmacht bezüglich der von Werbewirtschaft und „*Electronic Commerce*" benötigten Faktoren „Identität" und „Authentizität" (Vgl. *von Bonin*, Content on Demand.). Diese würde durch ein Verbot dieser Technologien zerstört, bevor sich selbstregulative Strukturen herausbilden könnten. Die Möglichkeit der Anonymität zu erhalten und zu fördern, liegt daher auch im Interesse eines Staates, der seinen Bürgern den wirksamen Selbstschutz in der elektronischen Kommunikation ermöglichen will (Vgl. Roßnagel, ZRP 1997, 26 (29f.).).

eine weltweite Identifikation an öffentlichen Internet-Terminals nötig.[876] Dem Staat würden erstmalig Überwachungsmittel in die Hand gegeben, die unmittelbar jeden Teilnehmer im Internet beträfen und technisch nicht auf mit rechtsstaatlichen Sicherungen versehene Ausnahmefälle begrenzt werden können.[877] Insgesamt würde durch ein Anonymitätsverbot ein zweifelhafter Zuwachs an Strafverfolgungsmöglichkeiten mit dem hohen Preis der Aufgabe wirksamer Privatheitsgarantien durch Anonymität bezahlt[878].

Um in Netzen mit offenen Standards ein Anonymitätsverbot durchzusetzen, müßten anonym oder unter pseudonym angebotene Inhalte ausgefiltert werden. Eine solche Filterung könnte allenfalls durch die Einführung einer obligatorischen digitalen Signatur[879] erreicht werden, deren Authentizität bei jedem Kommunikationsvorgang überprüft wird. Nicht signierte Inhalte[880] würden durch eine zentrale Filtereinrichtung gestoppt und ihre Verbreitung somit unterbunden. Eine entsprechende zentrale Filtereinrichtung wäre strukturell den gleichen Problemen ausgesetzt wie das „*WebBlock*"-System.[881] Darüber hinaus wäre ein solches System international nicht durchsetzbar und somit wirkungslos. Insbesondere die USA – nach wie vor der wichtigste Inhalteanbieter weltweit – könnten sich nicht anschließen, da dort das Angebot anonymer Inhalte verfassungsrechtlich geschützt ist.[882]

Ein Anonymitätsverbot in nicht zugangsoffenen Netzen mit proprietärem Standard – etwa einem unter privater Kontrolle „außerhalb" des Internet betriebenen interaktiven Kabelnetz – führt dazu, daß Betreiber große Ansammlungen personenbezogener Daten ihrer Nutzer anhäufen können. Diese haben zunehmend wirtschaftlichen Wert. Je nach der Bedeutung und Nutzungsintensität eines solchen Netzes können daher erhebliche Anreize der privaten Betreiber entstehen, staatliche Inhaltskontrollreglen über die Verwendung personenbezogener Daten nicht einzuhalten. In diesem Falle könnten die zu erwartenden Gefahren für die informationelle Selbstbestimmung der Nutzer eines sol-

876 Selbst das reichte noch nicht, weil praktisch sichere Anonymität auch z.B. durch rotierende *IP*-Adressen hergestellt werden kann. Soll Rückverfolgbarkeit tatsächlich verwirklicht werden, wären tiefe Eingriffe in Netzstruktur und –funktionalität nötig, die weltweit nicht durchzusetzen sein dürften.

877 Vgl. *Simitis*, (FN 263), S. 307. Vgl. auch oben *1. Identifikation durch den Staat*, S. 165.

878 Die Möglichkeit, anonym digitale Medien zu nutzen ist daher auch rechtspolitisch eine zentrale Forderung von Datenschützern, vgl. *DVD*, Datenschutzrechtliche Erwartungen an die rot-grüne Bundesregierung, http://www.aktiv.org/DVD; *Rannenberg, Kai*, Datenschutz als Innovationsmotor statt als Technikfeind in Bäumler, Helmut, Der neue Datenschutz, S. 190ff.

879 Vgl. Art. 3 IuKDG („Gesetz zur digitalen Signatur (Signaturgesetz - SigG)").

880 Es wäre möglich, bestimmte Dienste wie *e-mail* oder *News*-Nachrichten auch ohne Signatur durchzulassen, da die zu prüfenden Datenpaket-Header mit einer Dienstekennung ausgestattet sind.

881 Vgl. FN 848.

882 Vgl. FN 37.

chen Netzes nur durch eine staatliche Regelung gebannt werden, die die anonyme Nutzung ausdrücklich zuläßt[883].

2. Authentizität

Ein weiteres Durchsetzungshindernis für Sanktionen gegen Anbieter digitaler Kommunikationsinhalte ist die Beliebigkeit von Authentizität. Genausowenig wie aus dem Namen unter einer *news*-Nachricht geschlossen werden kann, daß die Nachricht von dem Namensträger versandt wurde, kann aus der Absenderadresse einer *e-mail* gefolgert werden, daß der Inhaber dieser Adresse tatsächlich Absender dieser *e-mail* ist. Authenzität herzustellen liegt vielmehr im Belieben des Senders, der zu diesem Zweck die Nachricht mit einer digitalen Signatur[884] versehen kann. Aus der Tatsache, daß ein bestimmter Inhalt etwa auf einer *WWW*-Seite erscheint, die zu der *domain* eines bekannten Anbieters gehört, kann ebensowenig geschlossen werden, daß der Inhalt von diesem Anbieter stammt. So erschien am 13. September 1998 auf der Hauptseite der *New York Times Online*[885] statt der neuesten Nachrichten ein Aufruf einer US-amerikanischen Hackergruppe[886]. Zahlreiche weitere Fälle ähnlicher Art wurden weniger öffentlich.[887]

Die dadurch offenkundige Möglichkeit derartiger Kompromittierungen von *server*n kann auch die Durchsetzung von Inhaltsbindungen gegenüber Anbietern rechtswidriger Inhalte erschweren: Wehrt sich ein Anbieter, dem die Publikation rechtswidriger Inhalte im *WWW* vorgeworfen wird, mit der Behauptung, sein Rechner sei Opfer einer „Hakking-Attacke“ geworden, ist ihm dieses kaum zu widerlegen, zumal die Protokolle der *server*-Zugriffe (*log files*) ausschließlich in seiner eigenen Verfügungsgewalt stehen. Im Gegensatz zu vergleichbaren Fällen in der physikalischen Welt (eine extremistische Organisation behauptet, Unbekannte hätten ihren Namen für ein volksverhetzendes Flugblatt verwendet) fehlen jede Spuren für polizeiliche Ermittlungsarbeit: Niemand wurde beim Verteilen beobachtet, es gibt kein Papier, das sich zurückverfolgen ließe, niemand wurde in einem Kopierladen gesehen oder hat eine Druckerei beauftragt.[888] Ein Zwang zur Authentizierung jedweden Inhalts durch eine obligatorische digitale Signatur

883 Eine den §§ 13 Abs. 1 MDStV, 4 Abs. 1 TDDSG entsprechende Regelung fehlt bisher etwa im TKG und der Telekommunikationsdiensteunternehmendatenschutzverordnung (TDSV) vom 12. Juli 1996 (BGBl. I S. 982).

884 Vgl. zum Verständnis *TeleTrust Deutschland e.V.*, Digitale Signatur - Wie unterschreibt ein Computer?, über http://www.TeleTrusT.de.

885 http://www.nytimes.com.

886 Vgl. QuickLinks v. 16.10.98, http://www.qlinks.net.

887 Im Oktober 1998 hatte die offizielle Menschenrechtsseite der chinesischen Regierung (http://www.humanrights-china.org) plötzlich die ungewollte Überschrift „Propaganda“, vgl. QuickLinks v. 29.10.98, http://www.qlinks.net; in ähnlicher Weise wurden die Inhalte einer Seite des griechischen Erziehungsministeriums verändert, vgl. http://actu.nomade.fr/ actu/articles/ 19981121170501-multimedia- 0106949.shtml.

888 Vgl. *Froomkin, Michael A.*, (FN 871), II. A.

ist aus den oben genannten[889] Gründen rechtspolitisch bedenklich und international - und damit überhaupt - nicht durchsetzbar.

3. Weitere Durchsetzungshindernisse

Weitere Hindernisse, rechtliche Sanktionen selbst als Anbieter der fraglichen Inhalte festgestellten und identifizierten Anbietern gegenüber durchzusetzen ergeben sich - wiederum - aus dem weltumspannenden Charakter digitaler Medien. Selbst ein in auf Deutschland bezogener und in deutscher Sprache abgefaßter rechtswidriger Inhalt kann - und wird zunehmend - von Personen angeboten werden, die nicht in Deutschland leben und der deutschen Personalhoheit nicht unterliegen. Unabhängig von der Frage, ob auf derartige Inhalte deutsches Inhaltskontrollrecht anwendbar ist und die Anbieter vor deutsche Gerichte gezogen werden können[890], sind die Möglichkeiten, Sanktionen dem ausländischen Anbieter gegenüber auch tatsächlich durchsetzen zu können, sehr begrenzt.

V. Ergebnis

Die Durchsetzung von Inhaltsbindungen mit hoheitlichen Mitteln ist nicht nur wegen des nationalen Geltungsbereiches des Inhaltskontrollrechts, sondern auch wegen der technischen Besonderheiten der Kommunikation digitaler Inhalte viel weniger erfolgversprechend als in herkömmlichen Medien. Die erst durch die digitalen Kommunikationsformen jedermann gewährten Möglichkeiten, global, verschlüsselt und - wenn gewünscht - anonym jedweden auch audiovisuellen Inhalt zu kommunizieren, stellen strukturelle Hindernisse für die hoheitliche Durchsetzung von Inhaltsbindungen dar. Zwar ist ein Verstoß etwa gegen Impressumspflichten auch im Pressebereich (anonyme Flugblätter) schwer zu sanktionieren, aber die Benutzung der neuen Formen digitaler Kommunikation erlaubt Kommunikationsvorgänge mit erheblicher Wirkung, bei denen keine physikalischen Spuren hinterlassen werden. Technologien, deren unreglementierte Verfügbarkeit einerseits die unverzichtbare Voraussetzung für sichere Datenkommunikation ist – etwa die Verschlüsselung –, errichten andererseits unüberwindliche Durchsetzungshindernisse für den Staat. Die einerseits zur wirksamen Verhinderung von Datenmißbrauch unabdingbare Möglichkeit anonymer Kommunikation verhindert andererseits genauso wirksam die Identifikation von Anbietern rechtswidriger Kommunikationsinhalte.

889 Vgl. oben *1. Anonymität*, S. 190.

890 Vgl. dazu oben *1. 3. Kapitel: Bedeutungsverlust nationaler Regulierung*, S. 147.