3. Abschnitt: Möglichkeiten kooperativer Kontrolle

Wird der Staat schwächer, muß er sich starke Partner suchen, um seine Ziele bestmöglich zu erreichen. Die vorangegangene Untersuchung hat gezeigt, daß sich allein im Wege gesetzlicher Inhaltskontrolle und deren hoheitlicher Durchsetzung nur ein geringer Teil der Kommunikation rechtswidriger digitaler Inhalte verhindern läßt. Genauso ist aber deutlich geworden, daß die Akteure neuer digitaler Kommunikationsformen durch technologische Veränderungen in die Lage versetzt werden, selbst Inhaltskontrollaufgaben wahrzunehmen. Sie kommen daher als Partner des Staates bei seinem Bestreben in Betracht, auch jenseits des Anwendungs- und Durchsetzungsbereiches bestehenden Inhaltskontrollrechts die Kommunikation rechtswidriger Inhalte zu minimieren.[910]

Für eine derartige Einbindung der Akteure digitaler Kommunikation in eine kooperative Inhaltskontrolle sind mehrere Konstellationen denkbar, bei denen sich unter Zuhilfenahme der technologischen Möglichkeiten digitaler Kommunikationsformen interessengerechtes Verhalten Privater und staatliche Rahmensetzung so ergänzen können, daß die Verbreitung rechtswidriger Inhalte auch in Fällen unterbleibt, wo eine gesetzliche Inhaltsbindung allein wirkungslos geblieben wäre (1. Kapitel). Wie diese kooperativen Kontrollformen und insbesondere die staatlichen Beiträge dazu rechtlich zu bewerten sind, ist bisher noch wenig geklärt (2. Kapitel).

1. Kapitel: Einbindung erstarkter Akteure digitaler Kommunikation zur Erreichung von Gemeinwohlzielen und Konzentration des Staates auf Vorfeldaufgaben der Inhaltskontrolle (kooperative Kontrolle)

Die durch die Digitalisierung entstehenden und sich verändernden Kommunikationsformen von rechtswidrigen Inhalten frei zu halten, liegt nicht ausschließlich im Interesse

910 Kooperationen zwischen Staaten sollen aus dem Rahmen dieser Untersuchung ausgeklammert bleiben. Sie werden im Folgenden nicht behandelt. In der Tat spricht viel dafür, daß auch internationale Vereinbarungen die Grenzen staatlicher Inhaltskontrolle nicht entscheidend beeinflussen können. Probleme, die sich aus der direkten Zuspielung digitaler Inhalte aus dem Ausland ergeben, vgl. *3. Kapitel:*, S. 147, können nur durch rechtsvereinheitlichende oder vollstreckungserleichternde Abkommen erreicht werden, die wegen des dazu nötigen Souveränitätsverzichts der Einzelstaaten auf multilateraler Ebene nur schwer zustandezubringen sind. Sie müßte zudem die "Rechtsoasen im Internet", vgl. *Hoeren, Thomas*, MMR 1998, 297 beseitigen, also weltweit wirken. Daher wird sich diese Kooperation auf weltweit konsensfähige Fragen wie Computerkriminalität, vgl. *Sieber*, CR 1995, 100 und evtl. die Ahndung von Kinderpornographie zu beschränken haben. Jedenfalls blieben auch dann Schwierigkeiten der Rechtsanwendung und –durchsetzung bestehen.
Ebenso ausgeklammert bleiben rein selbstregulative Institutionen, wie etwa virtuelle Schiedsgerichte, die sich derzeit im Internet bilden, vgl. *Arseneault, Michel*, Les justiciers du Web, Le Monde, Télévision, Radio, Multimédia v. 28./29.6.98, S. 34.

des Staates, der dadurch seine Einrichtungen und abstrakte Allgemeinwerte schützt. An wirksamer Inhaltskontrolle sind vielmehr auch die Akteure selbst interessiert, deren Rechte und Rechtsgüter durch unerwünschte Inhalte oder durch die unerwünschte Verwendung von ihnen kommunizierter Inhalte bedroht werden. Dieses Interesse besteht grundsätzlich auch dann weiter, wenn die gesetzliche Bezeichnung unerwünschter Inhalte als „rechtswidrig" und die daran geknüpfte Sanktionsdrohung allein weniger als in herkömmlichen Medien geeignet ist, Anbieter von der Kommunikation dieser Inhalte abzuhalten. Dann müssen sich vielmehr wieder diejenigen Erwägungen und Rationalitäten bewähren, derentwegen gesetzliche Inhaltsbindungen geschaffen wurden. Der Staat kann dabei in verschiedenartigen Konstellationen dazu beitragen, eigenverantwortliches und interessengerechtes Verhalten der Akteure zu ermöglichen und zu fördern.[911]

I. Kooperation durch staatliche „Zertifizierung" freiwilliger Selbstkontrollverpflichtungen von Inhalteanbietern

Trotz der erheblichen technologischen Kontrollresistenz digitaler Kommunikationsformen spricht einiges dafür, daß zahlreiche *content, host* und *access provider* sich weitaus weniger „anarchisch" verhalten werden, als befürchtet werden könnte.[912] In einem offenen Wettbewerbsmarkt für digitale Inhalte bestehen für Anbieter verschiedene Anreize, ihr Angebot von rechtswidrigen Inhalten freizuhalten und das Vertrauen der Nutzer im Hinblick auf die Verwendung ihrer personenbezogenen Daten zu gewinnen. Der Staat könnte derartig interessengerechtes Verhalten von Anbietern dadurch fördern, daß er ihnen durch eine Zertifizierung ihrer Inhaltskontrollaktivitäten einen Wettbewerbsvorteil in einem umkämpften Meinungsmarkt verschafft.

1. Anreize zu freiwilliger Selbstverpflichtung

Wird die Bedeutung gesetzlicher Inhaltskontrollvorschriften als abstraktes Verhaltensregulativ zunehmend schwächer, treten für viele Anbieter digitaler Kommunikationsinhalte konkrete Eigeninteressen in den Vordergrund, die sie zunehmend dazu veranlassen werden, sich selbst öffentlich zur Einhaltung inhaltlicher Standards und zu einer die Interessen der Nutzer berücksichtigenden Verwendung personenbezogener Daten zu verpflichten.

911 *Grzeszick, Bernd,* AöR 123 (1998), 173 (184); *Depenheuer,* AfP 1997, 669 (671) spricht von der „Regelungskompetenz der Weltbürgergesellschaft".

912 Vgl. pointiert zur „Sicht des Pessimisten" *Engel,* AfP 1996, 220.

a. Qualitätswettbewerb zwischen Anbietern

Anbieter digitaler Inhalte befinden sich untereinander in einem ausgeprägten Qualitäts- und Glaubwürdigkeitswettbewerb[913], der noch zunehmen wird, wenn das explosionsartige Wachstum digitaler Dienste sich verlangsamt. Tauchen in den Angeboten eines Anbieters Inhalte auf, die von den Nutzern abgelehnt werden, läuft dieser unabhängig von eigenem Verschulden oder rechtlichen Wertungen Gefahr, an öffentlichem Ansehen zu verlieren. Gleiches ist für den Fall anzunehmen, daß gegenüber einem Anbieter ein auch nur leiser Verdacht aufkommt, er verwende ihm anvertraute personenbezogene Daten abredewidrig oder in anderer Weise zum Schaden seiner Nutzer. Wegen der Zugangsoffenheit des Marktes für digitale Kommunikationsformen[914] und seiner niedrigen Eintrittsbarrieren[915] sind zahlreiche Angebote ohne Schwierigkeiten substituierbar; folglich können derartige Ansehensverluste unmittelbar von Wettbewerbern ausgenutzt werden. Der Nutzer, der sich wegen des starken Wettbewerbs selten dauerhaft an bestimmt Anbieter binden muß, dessen Nachfrageposition also von hoher Elastizität ist, kann sofort den Anbieter wechseln, wenn ihm das Angebot – etwa wegen des Vorhandenseins rechtswidriger Inhalte oder des unzureichenden Privatheitsschutzes – nicht mehr zusagt.

Der beschriebene Qualitätswettbewerb ist nicht auf kommerzielle Anbieter beschränkt. Auch nichtkommerzielle Angebote, die etwa wegen ihrer politischen oder journalistischen Inhalte hohe Nutzerzahlen anstreben, sind sensibel für Ansehensverluste. Anderes mag für Angebote gelten, die einen festen Nutzerstamm gerade dadurch gewinnen, daß sie extreme – gegebenenfalls auch rechtswidrige – Positionen vertreten. Gerade deren Nutzer werden aber ebenfalls ablehnend reagieren, wenn ihre persönlichen Daten nicht vertraulich behandelt werden.

b. Werbeabhängigkeit kommerzieller Anbieter

Angebote, die sich durch Werbung finanzieren, sind in besonderem Maße auf hohe Nutzerzahlen und auf das präzise Erreichen anvisierter Zielgruppen angewiesen. Weder diese Anbieter noch deren Werbekunden haben ein Interesse daran, daß von ihren Angeboten Inhalte kommuniziert werden, die eine breite Öffentlichkeit nicht wünscht. Dazu zählen insbesondere rechtswidrige Inhalte. Je mehr Nutzer sich über die Mißbrauchsmöglichkeiten im Klaren sind, die durch die Ansammlung persönlicher Daten gerade in den Händen kommerzieller Anbieter entstehen, desto intensiver werden auch

913 *Depenheuer*, AfP 1997, 669 (674).

914 Vgl. oben *cc. Die Vernetzung von Computern als Basis einer grenzüberschreitenden Transportplattform für digitale Inhalte*, S. 51.

915 Vgl. oben *d. Niedrige Eintrittsbarrieren*, S. 136.

Werbekunden darauf dringen, daß die Angebote, die sie mitfinanzieren, dem Sicherheitsbedürfnis der Nutzer entsprechen.

Von werbeabhängigen kommerziellen Anbietern ist daher in besonderem Maße zu erwarten, daß sie bereit sind, sich inhaltlichen Selbstverpflichtungen zu unterwerfen, die sie Nutzern und Werbekunden gegenüber als Wettbewerbsvorteil vermarkten können.

c. Erweiterte Sanktionsmöglichkeiten gesellschaftlicher Kontrolle

Mit Hilfe der neuen digitalen Kommunikationsformen, ist es jedermann möglich, binnen kurzer Zeit eine für jeden Inhaltsanbieter relevante Öffentlichkeit zu erreichen. Beschwerden selbst einzelner Nutzer, die substantiiert auf Versäumnisse beim Datenschutz, auf garantiewidriges Verhalten oder auf umstrittene Inhalte eines Anbieters aufmerksam machen, können allein durch ihre Öffentlichkeitswirkung erheblich größeren Druck auf Anbieter aufbauen, diese Praktiken abzustellen, als in herkömmlichen Medien.

Die Nutzung der technischen Möglichkeiten etwa des Internets zur Publikmachung und Bekämpfung nicht akzeptabler Praktiken einzelner Anbieter hat darüber hinaus eine Tradition. Wurden in den Anfängen des *Usenet*[916] Anbieter öffentlich bloßgestellt, die sich beharrlich weigerten, die *Netiquette*-Regeln[917] einzuhalten, sind heute häufig Anbieter von Werbemails von „Sanktionen" der Nutzer betroffen.

Anbieter müssen daher befürchten, daß sie bei zweifelhaftem Verhalten nicht lediglich einzelne Kunden verlieren, sondern daß bereits durch jeden Einzelfall eine „Lawine losgetreten" werden kann, die – je nach Zuschnitt des Angebotes – problemlos internationale Ausmaße erreichen kann. Daraus ergibt sich insbesondere für große Anbieter, bei denen hinsichtlich der Verwendung personenbezogener Daten ein erhebliches Mißbrauchspotential zu vermuten ist, ein Anreiz, sich selbst zur Einhaltung von Datenschutzstandards nachprüfbar zu verpflichten.[918]

2. Kooperationsbeitrag des Staates als vertrauenswürdiger Zertifikator von Selbstverpflichtungen im Meinungsmarkt

Kooperative Inhaltskontrolle entsteht, wenn der Staat Strukturen schafft, die die privaten Anreize in ein System zur Kontrolle von digitalen Kommunikationsinhalten einbinden. Er kann etwa anbieten, Inhaltskontrollmechanismen privater *content*, *host* oder

916 So wurden die *e-mail*-Adressen der Absender unverlangter Werbe-*e-mail* nicht selten mit automatisierter Antwortpost so überschwemmt, daß sie unbrauchbar wurden.

917 Zu den *Netiquette* genannten Verhaltensregeln für die *online*-Kommunikation vgl. *Hambridge, S.*, Netiquette Guidelines.

918 Vgl. die Unternehmen, die sich von der US-amerikanischen Agentur „TrustE" zertifizieren lassen, http://www.truste.org.

access provider, die erwarten lassen, daß ihre Ergebnisse den inhaltlichen Wertungen und den datenschutzrechtlichen Anforderungen der jeweiligen Gesetzeslage entsprechen oder sogar noch darüber hinaus gehen[919], zu zertifizieren. Der Anbieter könnte dann damit werben, daß er sich zu einem der Gesetzeslage entsprechenden Inhalts- und Qualitätsstandard verpflichtet hat und sein Angebot mit diesem übereinstimmt.

Je höher die Anforderungen dieses Zertifikats insbesondere an die zur wirksamen und regelmäßigen Kontrolle seiner Einhaltung einzugehenden Selbstverpflichtungen sind, desto größer ist der zu erwartende Vertrauensgewinn und damit der Wettbewerbsvorteil für den zertifizierten Anbieter.[920] Anders als etwa in den USA spielt der Staat in Deutschland traditionell eine stärkere Rolle bei der Festlegung von Datenschutzregeln und Inhaltsbindungen. Er kann in Gestalt der gesetzlichen Vorschriften ein umfangreiches und allgemein anerkanntes Normprogramm als Grundlage von Selbstverpflichtungen anbieten. Er ist daher – zumindest für eine Übergangszeit – eher als private Institutionen in der Lage, ein Zertifikat auszustellen, das ausreichendes Vertrauen vermitteln kann, um Wettbewerbsvorteile für Anbieter entstehen zu lassen. Dies schließt ebensowenig wie bei bereits bestehenden Zertifizierungssystemen[921] aus, daß der Staat die unmittelbare Zertifizierung Privaten überläßt, die ihrerseits staatlich zertifiziert sind, solange damit nicht – etwa wegen Befürchtungen fehlender Unabhängigkeit der Zertifikatoren[922] – ein Vertrauensverlust des Zertifikats verbunden ist. Unklar bleibt, ob das in § 17 MDStV angesprochene Datenschutz-Audit diese Wirkungen erreichen kann. Bisher fehlen dazu noch ausgestaltende Regelungen, die eine abschließende Beurteilung ermöglichen könnten.[923]

Nötig ist eine erste rechtliche Bewertung eines solch umfangreichen Zertifizierungssystems, die Parallelen und Unterschiede zu bestehenden Instrumenten kooperativer Verwaltung aufdeckt und auftretende Grundrechtsfragen untersucht.[924]

---

919 Vgl. die Selbstverpflichtung der Freiwilligen Selbstkontrolle Multimedia *(FSM e.V.)*, oben FN 22.

920 Bloße Absichtserklärungen, wie sie etwa vom *Bundeskriminalamt* den deutschen „Internet Service Providern“ und „Online-Diensten“ vorgeschlagen wurden, vgl. den Text über https://www.iks-jena.de/mitarb/lutz/anon/isp.html, Nr. 5, erreichen diesen Zweck nicht.

921 Vgl. etwa das im Gesetz zur digitalen Signatur (Signaturgesetz – SigG, Art. 3 IuKDG) geregelte Zertifizierungsverfahren.

922 So ist die *Deutsche Telekom AG* Zertifikatsstelle nach dem SigG. Für eine Zertifizierung von inhaltlichen Selbstkontrollverpflichtungen wäre sie aber nicht geeignet, weil sie selbst als *provider* auftritt.

923 Vgl. *Trute*, VVDStRL 57 (1998), 218 (262). Zu den Anforderungen an ein wirksames Datenschutz-Audit vgl. *Arbeitskreis Datenschutz-Audit Multimedia*, Prinzipien, http://www.siline.com/gdd/mmprinzp .html.

924 Vgl. unten *I. Verfassungsrechtliche Bewertung der Zertifizierung von Selbstverpflichtungen*, S. 229.

I. Kooperation durch staatliche Unterstützung privaten Selbstschutzes

Die Technologie der digitalen Kommunikationsformen erhöht nicht einseitig die kommunikativen Möglichkeiten nur eines Kommunikationspartners. Genauso wie es Akteuren technologisch erleichtert wird, staatlichen Regelungen zu entgehen oder auszuweichen, werden spiegelbildlich ihre Kommunikationspartner in die Lage versetzt, sich vor unerwünschten Kommunikationsinhalten und -praktiken zu schützen. Empfänger können sich etwa durch die Verwendung von Filtersoftware gegen den Erhalt unerwünschter Inhalte schützen; Anbieter können durch die Verwendung von Verschlüsselungs- oder Anonymisierungstechnologie die unerwünschte Kenntnisnahme ihrer Kommunikation durch Dritte verhindern.

Nutzen diese Akteure derartige Möglichkeiten, hindern sie auch die Verbreitung heute als rechtswidrig eingestufter Inhalte und erreichen dadurch bereits Ziele der Inhaltskontrolle, die herkömmlich von staatlicher Regulierung verfolgt werden. Noch nicht immer haben sich jedoch Lösungen durchgesetzt, die dem Nutzer den Schutz anbieten, der technisch möglich wäre. Unterstützt und fördert der Staat diese Lösungen, leistet er einen Beitrag zu kooperativer Inhaltskontrolle.

1. Schutzmöglichkeiten des Kommunikationsempfängers gegen unerwünschte digitale Inhalte

Bei der Analyse der technischen Schutzmöglichkeiten des Empfängers ist zu differenzieren zwischen digitalen Inhalten, die ein Empfänger im Wege des Abrufes aus einer Datenbank bzw. von einem *server* selbst elektronisch anfordert und denjenigen, die er per adressierter Verschickung oder über einen *Push*-Kanal zugestellt bekommt.

a. Abgerufene Inhalte

Sofern der Empfänger abgerufene digitale Inhalte (etwa *WWW/FTP*-Dokumente oder *newsgroup*-Inhalte) über einen *access provider* erhält, der ihm den Zugang zu den entsprechenden *servern* verschafft, kann er sich bereits durch die Auswahl dieses *providers* gegen unerwünschte Inhalte schützen. Er kann einen *provider* wählen, der seinen Kunden nur solche Inhalte durchleitet, die er bereits nach eigenen Regeln[925] oder in Erfüllung einer dem Staat gegenüber eingegangenen Selbstverpflichtung[926] gefiltert hat. Je mehr die private Inhaltskontrolle in offenen digitalen Datennetzen an Bedeutung gewinnt, desto ausgeprägter wird der Wettbewerb sein, in dem der Kunde zwischen ver-

925 Vgl. *ots*, PSINet hält das Internet sauber, http://www.newsaktuell.de/4d.acgi$getstory?53704. Ähnliche Dienste werden in USA von zahlreichen Anbietern angeboten, vgl. http://www. websense.com; http://www.n2h2.com/bess-noframes.htm.

926 Vgl. oben *I. Kooperation durch staatliche „Zertifizierung" freiwilliger Selbstkontrollverpflichtungen von Inhalteanbietern*, S. 202.

schiedenen Filterpolitiken konkurrierender *access provider* wählen kann. Gegebenenfalls kann er auch individuelle Präferenzen mit dem *provider* vertraglich aushandeln oder es gleich dem *provider* überlassen, ihm ein Angebot von Inhalten zusammenzustellen, das ihn interessiert[927].

Ist der Nutzer mit seinem Computer, Fernseher oder anderem Gerät entweder direkt in ein Netzwerk eingebunden, so daß er keinen *access provider* hat oder möchte er diesem eine Inhaltsauswahl nicht überlassen, so kann er im Einzelfall Suchdienste benutzen, die als Suchergebnis nur Inhalte liefern, die nach bestimmten Kriterien gefiltert sind.

Jeder Abruf eines bestimmten digitalen Inhalts ist zudem mit einer ausdrücklichen Auswahlentscheidung des Nutzers verbunden. Er folgt durch Anklicken einem *hyperlink* im *WWW*, lädt sich die Titelzeilen einer bestimmten *newsgroup* von einem *news server* herunter oder veranlaßt im Auswahlmenü eines *video-on-demand*-Anbieters die Zuspielung eines bestimmten Spielfilms. Dabei weiß er nicht nur, daß er einen Kommunikationsvorgang veranlaßt, sondern meist auch – zumindest ungefähr – welche Art von Inhalt er abruft. Ungewollt wird er mit unerwünschten Inhalten in der Regeln nur aus Versehen[928] oder bei gezielter Täuschung durch Inhaltsanbieter[929] konfrontiert.

Um sich auch gegen derartige Fälle zu schützen, kann der Nutzer eigene Mittel einsetzen, um die seiner Kontrolle unterstehenden Geräte seinen persönlichen Inhaltspräferenzen entsprechend zu konfigurieren. Dabei steht ihm verschiedene Software zur Verfügung: Es werden etwa Programme angeboten, die Werbebanner auf *WWW*-Seiten erkennen und diese bei der Inhaltsdarstellung ausfiltern[930] oder abgerufene Bilder anhand des Anteils hautfarbener Bildpunkte als Nacktbilder vermuten und ausfiltern[931]. Wortfilterprogramme blockieren die Darstellung von abgerufenen Textinhalten, wenn in ihnen unerwünschte Wörter in bestimmter Häufigkeit vorkommen. Andere Programme verhindern die Darstellung von Inhalten, deren Adressen (*URL*) in ständig aktualisierten Negativlisten auftauchen, die der Programmanbieter nach eigenen Kriterien zusammenstellt. Regelmäßig kann der Nutzer selbst die Wort- und *URL*-Listen ergänzen oder nur einige der angebotenen Inhaltskategorien blockieren.[932]

---

927 *Eli Noam* bezeichnet diesen „persönlichen Kanal“ als „Me-Channel“, *Noam, Eli,* The Stages of Television: From Multi-Channel Television to Me-TV, über http://www.vii.org/papers.

928 Manchmal führt ein Tippfehler bei der Eingabe eines *URL* dazu, daß man auf einer *WWW*-Seite mit Sexangeboten landet.

929 Ein Inhalt oder *hyperlink* wird gezielt falsch bezeichnet, die Anforderung des gewünschten Inhaltes wird unterwegs umgeleitet und es wird ein unerwünschter Inhalt zugespielt oder die Inhalte der angeforderten Seiten wurden verändert. Dabei handelt es sich um Fälle des *Hacking.*

930 Etwa der kostenlose *Webwasher* von Siemens, vgl. http://www.siemens.de/servers/wwash/wwash_ de.htm.

931 Vgl. etwa den *browser* „icab“, http://www.icab.de.

932 Vgl. eine Zusammenstellung der gängigen Filterprogramme *Cyber Patrol, Net Nanny, Cyber Snoop, Cybersitter* und *Surfwatch* unter http://www.zdnet.com/products/grids/webfilter.html.

Viele Filterprogramme[933] unterstützen daneben auch die Blockierung unerwünschter Inhalte mit Hilfe des *PICS*-Standards[934]. Dieses System bietet besonders effektive Möglichkeiten der Filterung von Inhalten, die mit einem *PICS*-kompatiblen *Rating*, einer Zusatzinformation über Inhaltseigenschaften der abgerufenen Information, ausgestattet sind. *PICS* ist eine Technologie, die es ermöglicht, zum einen für einzelne digitale Inhalte „Etiketten" (*labels*) zu erzeugen und zu publizieren, und zum anderen Programme in die Lage zu versetzen, diese Etiketten zu erkennen. Sie erlaubt einem Anbieter oder einer dritten Person, einen digitalen Inhalt zu etikettieren und einem *PICS*-fähigen *browser*, diese Etiketten zu finden und zu interpretieren. Das Etikett kann dabei entweder mit dem Inhalt selbst verbunden sein oder sich in der Datenbank einer *Rating*-Agentur[935] befinden, die der Nutzer beim Abruf automatisch *online* kontaktiert. Jedermann kann eigene Angebote etikettieren und jedermann kann eine *Rating*-Agentur betreiben. Umgekehrt kann ein Nutzer nicht nur bestimmen, anhand welcher *Rating*-Kategorien, sondern auch unter Verwendung welcher *Rating*-Agentur er Inhalte blokkieren möchte. Der Nutzer kann die *Ratings* verschiedener Organisationen, deren Einschätzung er für einzelne Inhaltskategorien vertraut, kombinieren. Er kann seinen Computer etwa so konfigurieren, daß er alle Inhalte blockiert, die von der katholischen Kirche in der Kategorie „offener Sex" mit einem Wert über 5 eingestuft werden, mit Ausnahme der Inhalte, die von der Aids-Hilfe mit dem *Rating* „besonders informativ" versehen wurden. Hinsichtlich der Vielfalt verschiedener *Rating*-Agenturen, -Typen und -Kombinationen bestehen technisch keine Begrenzungen. Wie in anderen Märkten auch, werden sich weiter verbreitete *Rating*-Agenturen herausbilden, aber der *PICS*-Standard ermöglicht prinzipiell einen offenen, dezentralisierten Markt, in dem Inhaltsbeschreibungen verschiedenster Stimmen mit verschiedensten Nutzerpräferenzen in Übereinstimmung gebracht werden können.[936]

b. Adressiert zugestellte und im *Push*-Dienst kommunizierte Inhalte

Erreichen den Nutzer Inhalte per *e-mail* oder *e-mail*-Anhängsel, muß er diese in der Regel erst aus seinem Postfach bei seinem *mail provider* abrufen. Wie mit seinem *access provider* kann er auch mit dem *mail provider* vereinbaren, daß dieser eingehende Inhalte bereits filtert.[937]

---

933 Vgl. die umfangreiche Analyse und vergleichende Darstellung aller gängigen Filterprogramme von *Faith Cranor/ Resnick/ Gallo,* Technology Inventory – A Catalogue of Tools that Support Parents' Ability to Choose Online Content Appropriate for Their Children (FN 830).

934 Vgl. oben bei FN 257, 825.

935 *Rating*-Agenturen können ihre *PICS*-Etiketten manuell (durch Mitarbeiter), maschinell oder aufgrund von Vorschlägen Dritter erstellen, vgl. eine Übersicht über die verschiedenen Modelle unter http://www.w3.org/PICS/raters.htm.

936 Zum Ganzen, *Dyson, Esther*, Release 2.0, 1997, 170ff.; *von Bonin*, Content on Demand.

937 Viele *e-mail*-Dienste bieten etwa das Ausfiltern von unverlangter Werbemail (*Spam*) an, vgl. etwa *Global Message Exchange (GMX)*, unter http://www.gmx.de.

Um sich vor unverlangter Werbepost (*Spam*) zu schützen, hat jeder Nutzer die Möglichkeit, sich in sogenannte *„Robinson"*-Listen einzutragen[938], an deren Mitglieder kein *Spam* verschickt wird. Die überwiegende Anzahl der Werbemail-Versender respektiert diese Selbstkontrollmaßnahme des generellen *„opt-out"*. Zunehmend ermöglichen sie auch ein individuelles *„opt-out"*, durch das der Nutzer die weitere Zustellung von Werbung dieses Absenders verhindern kann[939]. Gängige *e-mail*-Programme erlauben dem Benutzer regelmäßig auch, eingehende Post im eigenen Rechner nach eigenen Kriterien zu filtern. Es läßt sich etwa einstellen, daß *e-mails* ohne Absender- oder *„Reply"*-Adresse[940], sowie Nachrichten einer bestimmten Größe, Absenderadresse oder *–domain* gelöscht werden, bevor der Nutzer von ihrem Eingang erfährt. Auch wer davon keinen Gebrauch macht, wird nicht sofort nach dem Abrufen seiner Nachrichten mit deren Inhalt konfrontiert, sondern sieht erst eine tabellarische Aufstellung der eingegangenen Post mit Angaben über den Sender, die Sendezeit und den Betreff der Nachricht. Den Inhalt einer bestimmten Nachricht oder eines bestimmten *attachment* kann der Nutzer erst wahrnehmen, nachdem er den Inhalt ausdrücklich geöffnet hat. Unerwünschte Inhalte erreichen ihn auch hier nur, wenn er Opfer einer gezielten Täuschung wird. Gegen *e-mail*-Inhalte, die weder bei der Normanwendung[941] noch bei der Durchsetzung die besonderen Schwierigkeiten neuer Kommunikationsformen aufweisen, – etwa beleidigende Ausfälle eines Geschäftspartners per *e-mail* statt per Brief [942] – verbleiben dem Empfänger die herkömmlichen Reaktionsmöglichkeiten, etwa die Strafanzeige.

Will ein Empfänger *Push*-Inhalte empfangen, muß er zunächst einen Kanal einrichten, auf dem ihn diese Inhalte erreichen. Dies geschieht in der Regel durch Öffnen eines neuen *browser*-Fensters, also einer weiteren Datenübertragungs-Verbindung zu einer bestimmten Adresse, deren Inhalt jedoch nicht statisch ist, sondern sich dauernd ändert. Der Nutzer hat, nachdem er einmal den Kanal eröffnet, keinen Einfluß mehr auf die sich ändernden Inhalte der Zieladresse. Insofern besteht die Möglichkeit, daß er von unerwünschten Inhalten überrascht wird. Dagegen kann er sich nur mittelbar durch die Auswahl eines Anbieters schützen, dem er vertraut, weil dieser sich selbst zur Einhaltung von inhaltlichen Standards verpflichtet hat, Nutzern Beschwerdemöglichkeiten einräumt und nicht anonym publiziert.

938 *Schmidt, Hans,* Robinson schlägt zurück, König Kunde (FN 220), S. 34.

939 Vgl. zu den teilweise mißverständlichen Vorgaben der EU-Fernabsatz- und der EU-E-Commerce-Richtlinien oben bei FN 369ff.

940 Gerade Werbemail-Versender schicken häufig Nachrichten, auf die der Empfänger nicht direkt antworten kann.

941 Vgl. oben bei FN 337.

942 Dies gilt jedenfalls dann, wenn der Inhalt nicht anonym und nicht aus dem Ausland verschickt wurde.

c. Zwischenergebnis

Technologisch stehen dem Empfänger wirksame Schutzmaßnahmen zur Verfügung, mit denen er sich der Risiken erwehren kann, die sich für seine Interessen und Rechtsgüter aus den ausdifferenzierten Formen digitaler Kommunikation ergeben. Um diese jedoch bestmöglich nutzen zu können, ist der Nutzer auf das Vorhandensein eines marktmäßigen Umfeldes angewiesen, in dem er eine Wahlfreiheit zwischen vielfältigen Anbietern von Inhalten, Diensten und Produkten hat, die miteinander im Wettbewerb stehen. Insbesondere der optimale Einsatz der *PICS*-Technologie erfordert eine Mehrzahl von *Rating*-Agenturen, aus deren Bewertungen der Nutzer seine persönliche Kombination zusammenstellen kann. Sieht er sich lediglich einem oder wenigen *Rating*-Konzepten gegenüber, wird er seine Präferenzen darin kaum wiederfinden und gegebenenfalls die Technologie gar nicht nutzen, obwohl er bestimmte rechtswidrige Inhalte gern ausgefiltert hätte. Deren Verbreitung wird dann insgesamt noch weniger verhindert.

Damit ein solcher Wettbewerb entstehen kann, ist die Teilnahme möglichst vieler Akteure an digitalen Kommunikationsformen notwendig. Diese müssen zudem über die notwendigen Kenntnisse verfügen, die ihnen zur Verfügung stehende Technologie nach ihren Interessen – und damit im Sinne verbesserter Inhaltskontrolle – einzusetzen. Damit sind die staatlichen Kooperationsbeiträge vorgezeichnet, die zur Schaffung kooperativer Inhaltskontrolle geboten sind.

2. Staatliche Unterstützungsmaßnahmen

Aufgaben, die bisher kaum dem Vorfeld der Kommunikationsinhaltskontrolle zugerechnet wurden, stellen sich im Rahmen der Kommunikation digitaler Inhalte als wichtige Kooperationsbeiträge des Staates zur Inhaltskontrolle dar. Sie gewinnen als notwendige Voraussetzungen einer wirksamen Selbstkontrolle verstärkte Bedeutung für die Verhinderung der Kommunikation rechtswidriger Inhalte insgesamt, die wegen der Schwäche rein hoheitlicher Maßnahmen auf die Ergänzung durch kooperative Inhaltskontrolle angewiesen ist.

a. Wettbewerbssicherung als Voraussetzung kooperativer Inhaltskontrolle

Die Digitalisierung der Inhaltsübertragung und die Möglichkeiten der Kompression digitaler Inhalte lassen gegenwärtig die technische Knappheit der Transportinfrastruktur für Kommunikationsinhalte verschwinden. Dieser Prozeß dauert an. Unabhängig davon entstehen jedoch neuartige Engstellen, an denen Inhaber proprietärer faktischer Stan-

dards den freien Kommunikationsfluß behindern können.[943] Die Offenhaltung dieser Engstellen ist für das Gelingen kooperativer Kontrolle von Bedeutung.

Drei Beispiele aus jüngerer Zeit sollen die Problematik verdeutlichen:

> *Beispiel 1:* Während auf der *server*-Seite der digitalen Kommunikation – noch – verschiedene Betriebssysteme anzutreffen sind[944], werden die Computer auf der Empfangsseite durch ein Produkt eines einzelnen Herstellers beherrscht.[945] Das Betriebssystem eines Computers bestimmt dessen Funktionalität. Durch die Koppelung des *Windows*-Betriebssystems mit dem Programm, das Auswahl, Abruf und Darstellung digitaler Inhalte kontrolliert, dem *browser*,[946] bestimmt der nichtöffentliche (proprietäre) Standard eines einzigen Herstellers die Kommunikationsmöglichkeiten der weitaus überwiegenden Zahl der Empfänger digitaler Inhalte weltweit. Die mit einer derartigen Stellung verbundenen Einfluß- und Mißbrauchsmöglichkeiten sind erheblich und schließen die Kontrolle von Inhalten ein.[947] So kann *Microsoft* auf jedem mit *Windows* ausgelieferten Rechner die Zugangssoftware zum *Microsoft-Network* vorinstallieren, die den Nutzer durch Anklicken eines Symbols auf der Benutzeroberfläche direkt zu von *Microsoft* ausgesuchten Inhalten führt.[948] Die zur Benutzung der *PICS-Ratings* einer bestimmten Firma nötigen Programmdateien können bereits im Betriebssystem eingearbeitet sein, während die Nachinstallation anderer Dateien, die nötig sind, um konkurrierende *Rating*-Systeme zu verwenden, für den Laien undurchführbar schwierig ist.[949] Mit Hilfe selbstausführender Programme, die von *WWW*-Seiten aus verschickt werden, kann *Microsoft* Einstellungen seiner Programme auf den Rechnern der Nutzer verändern oder

---

943 Vgl. *Holznagel, Bernd,* Der spezifische Funktionsauftrag des Zweiten Deutschen Fernsehens, ZDF-Schriftenreihe Nr. 55, 1999, S. 82f. m.w.N.; zur ökonomischen Bedeutung von Standards *Knorr, Henning,* Sieben Thesen zur Standardisierungspolitik in der Telekommunikation in Mestmäcker, Ernst-Joachim (Hrsg.), Kommunikation ohne Monopole II, 1995, S. 515 ff.; *OFTEL,* Beyond the telephone, the television and the PC, Second Submission, Section 6; http://www.oftel.gov.uk/ broadcast/dcms398 .htm.

944 Dies ist in der Tradition begründet, das UNIX-Betriebssystem auf der *server*-Seite zu verwenden, weil dafür das kostenlose *server*-Programmpaket *„Apache"* erhältlich ist.

945 Das *Microsoft* – Produkt *Windows* in den Versionen 3.x und 9x wird auf etwa 85 % aller PCs weltweit eingesetzt.

946 Die Rechtmäßigkeit der Koppelung des *Windows98*-Betriebssystems mit dem *Microsoft-browser Internet Explorer* ist derzeit in Washington D.C. Gegenstand des umfangreichsten wettbewerbsrechtlichen Gerichtsverfahrens der amerikanischen Geschichte, vgl. dazu *Moglen, Eben,* Microsoft Wants US (FN 185).

947 Der amerikanische Juraprofessor und Computerfachmann *Eben Moglen* schreibt a.a.O.: „When *Microsoft* claims for itself the right to determine ‚the Windows experience', it is really claiming the right to decide which newspapers are the easiest to read, which music is the simplest to listen to and which banks or brokerages are the most convenient places to put your money. [...] The most valuable location in the world is the spot in front of your eyeballs: at your desk, at home, on the airplane, when your kids sit down to do their homework. That's the location Gates claims his company has an unfettered right to control."

948 Gegen die Zusage, auf dem *Windows* Desktop plaziert zu werden hat z.B. der *access* und *content provider America Online (AOL)* den *Microsoft Internet Explorer* als voreingestellten *WWW*-Browser für seinen Online-Dienst akzeptiert. Vgl. http://www.techweb.com/printableArticle ?doc_id= TWB19981028S0027.

949 Vgl. zu dieser Praxis von *Microsoft*, dessen *Internet Explorer* werksseitig nur die *RSACi-Ratings* (an *RSACi* ist *Microsoft* beteiligt) unterstützte *Weinberg, Jonathan,* 19 Hastings Comm/Ent L.J. 453 (1997).

– gegebenenfalls ohne Wissen der Öffentlichkeit in die Programme eingebaute – Funktionen aktivieren.[950]

Beispiel 2: Zunehmend wird erwartet, daß sich das Breitbandkabelnetz zu einem wichtigen Übertragungsmedium für digitale Inhalte entwickelt.[951] Bei der Benutzung des Kabelnetzes für die digitale Kommunikation entsteht nicht nur bei der Entscheidung über den Zugang von Anbietern zum Netz eine Engstelle, deren Kontrolle heftig umstritten ist.[952] Auch der Computer, der auf der Empfängerseite die Dekodierung, Angebotsdarstellung und Abrechnung erledigt, sowie über die interaktiven Möglichkeiten der Kabelkommunikation mittels Fernsehgerät entscheidet *(Set-Top*-Box*)*, erlaubt einem Quasi-Monopolisten eine durchgreifende Einflußnahme auf Kommunikationsinhalte. Während die politische Aufmerksamkeit sich vor allem auf den Kompetenzstreit zwischen Bund und Ländern um die Multimediadienste konzentrierte, hatten die *Kirch*-Gruppe, *Bertelsmann* und die *Deutschen Telekom* die *Multimedia-Betriebsgesellschaft (MMBG)* als Gemeinschaftsunternehmen zur Verbreitung digitalen Kabelfernsehens und zur Durchsetzung des proprietären *d-(Set-Top-)* Box–Standards gebildet. Auch die Untersagung dieser Allianz durch die EU-Kommission[953] hat die Etablierung eines – nun allein von *Kirch* kontrollierten – Standards nicht verhindern können.

Mitte 1999 sieht es so aus, als werde der Standard der *Set-Top*-Box in Zukunft ebenfalls durch *Microsoft* bestimmt. Nach einer Beteiligung in Höhe von fünf Milliarden US$ an *AT&T*, nach Übernahme von *MediaOne* Amerikas größter Kabelbetreiber, und dem Einstieg bei den britischen Kabelkonzernen *Telewest*, *NTL* und *Cable & Wireless* beabsichtigt die Firma, gemeinsam mit *Bertelsmann* das deutsche Fernsehkabelnetz zu erwerben[954] und dort – wie schon in den USA- ihr Betriebssystem *Windows CE*[955] in den *Set-Top*-Boxen einzusetzen. Damit wäre das Unternehmen *Microsoft* in der Lage, sich auf die Kommunikation digitaler Inhalte über den Fernseher ähnliche Einflußmöglichkeiten zu verschaffen, die es bereits heute beim PC ausüben kann.

Beispiel 3: Als zentraler Baustein des technologischen Selbstschutzes vor rechtswidrigen digitalen Kommunikationsinhalten und damit der kooperativen Inhaltskon-

---

950 Vgl. oben FN 254.

951 Diese Entwicklung wird auch europarechtlich durch die Richtlinie 95/51/EG der Kommission vom 18.10.1995 zur Änderung der Richtlinie 90/388/EWG hinsichtlich der Aufhebung der Einschränkung bei der Nutzung von Kabelfernsehnetzen für die Erbringung bereits liberalisierter Telekommunikationsdienste, ABl. EG Nr. L 256/49 vom 26.10.1995 vorgegeben.

952 Vgl. *Bullinger*, ZUM 1997, 281; *Engel*, ZUM 1997, 309; *Gersdorf, Hubertus*, Regelungskompetenzen bei der Belegung digitaler Kabelnetze, 1996. Zuletzt haben nach Presseberichten die Landesmedienanstalten die Kabelnetzbetreiber aufgefordert, bis zum 7. September 1999 einen konkreten Vorschlag zur künftigen Belegung der digitalen Hyperbandkanäle vorzulegen. Die Regelung soll am 1. April 2000 in Kraft treten. Danach sei der Netzbetreiber verpflichtet, bei einem Drittel seiner für die digitale Verbreitung vorgesehenen Kapazitäten ein „vielfältiges Programmangebot an Vollprogrammen, nicht entgeltfinanzierten Programmen, Spartenprogrammen und Fremdsprachenprogramme sowie Mediendienste angemessen zu berücksichtigen", vgl. Berichte vom 30.6.1999 über http://www. newsroom.de.

953 *Europäische Kommission*, Mitteilung v. 13.3.98 Fall Nr. IV/M.1027, CR 1998, 424.

954 *Schulzki, Haddouti, Christiane*, Bill Gates auf dem Weg zur Herrschaft über das Internet, Telepolis v. 18.5.1998, unter http://www.heise.de/tp/deutsch/inhalt/te/2857/1.html.

955 *Windows CE* ist wie das bereits auf dem PC-Markt führende *Windows 95/98* ein proprietärer, also nicht offener, Standard. Dieses System ist bereits weit verbreitet in Kleinstcomputern wie etwa *Personal Digital Assistants*, *Palmtops* und anderern Geräten, die in Zukunft Kommunikationsfunktionen wahrnehmen werden (etwa Küchengeräte).

trolle insgesamt ist ein auf dem *PICS*-Standard basierendes System der Filterung von Inhalten beschrieben worden. Dabei ist deutlich geworden, daß ein solches System in besonderem Maße auf ein Nebeneinander verschiedener Anbieter von *Ratings* angewiesen ist.[956] Am 12. Mai 1999 haben sich führende Inhalte-, Dienste- und Technologieanbieter zur Gründung eines *Rating*-Anbieters zusammengeschlossen. *AOL Europe*, die *Bertelsmann-Stiftung, British Telecom, Cable & Wireless, Demon Internet,* die *EuroISPA*[957]*, IBM, Internet Watch Foundation, T-Online* und wiederum *Microsoft* wollen über die *Internet Content Rating Association (ICRA)* mit Sitz in London eine auf dem 1994 von der *Software Publishers Association* geschaffenen und von *Microsoft* und *IBM* finanzierten *RSACi*-System basierende Filtersoftware entwickeln und kostenlos abgeben.[958]

Kann ein einzelnes Unternehmen durch seine Kontrolle über das Betriebssystem bestimmen, welche Software auf den Kommunikationsgeräten der Nutzer funktioniert, so kann dieses Unternehmen maßgeblich darüber entscheiden, welche Inhalte diese Geräte kommunizieren. Kann dieses Unternehmen zusätzlich erreichen, daß die Mehrzahl der Nutzer faktisch ausschließlich Inhalte auswählt, die durch ein von ihm kontrolliertes Filtersystem vorselektiert sind, so entsteht aus dieser Stellung zunächst Markt- und daraus auch Meinungsmacht.[959] Staatliche Intervention dagegen erscheint wegen der sich daraus für den Wettbewerb und den Prozeß der freien Meinungsbildung ergebenden Gefahren wettbewerbs[960]- und medienpolitisch geboten.

Fraglich sind die geeigneten Instrumente. In den beschriebenen Beispielen ergibt sich die für die Inhaltskontrolle bedeutsame Meinungsmacht zum einen aus der vorentstandenen starken Stellung in verschiedenen Märkten für Produkte (Betriebssysteme, Software) und Dienstleistungen (*Rating*-Agenturen), die für Vorgänge digitaler Kommunikation bedeutsam sind und von ihr abhängen. Zum anderen kann die Möglichkeit der Meinungskontrolle dadurch entstehen, daß ein marktbeherrschendes Unternehmen Zusatzfunktionen in seine Produkte einbaut, die der Nutzer nicht selbst oder unter Zuhilfenahme anderer Produkte verändern oder verhindern kann, weil die dazu nötigen technischen Informationen (Standards, Schnittstellen) von dem marktbeherrschenden Unternehmen nicht offengelegt werden.

Nutzt ein Akteur seine wirtschaftliche Stellung in dieser Weise zur Beeinflussung digitaler Inhalte und ihrer Erreichbarkeit aus, liegt es nahe, darin den Mißbrauch einer marktbeherrschenden Stellung zu sehen und dagegen mit Mitteln des Wettbewerbsrechts vorzugehen. Fraglich ist, ob dieses in der Lage ist, den speziellen Meinungsbezug dieses Verhaltens ausreichend zu berücksichtigen.[961]

---

956 Vgl. *1. Schutzmöglichkeiten des Kommunikationsempfängers gegen unerwünschte digitale Inhalte*, S. 206.

957 Die *EuroISPA* ist der europaweite Zusammenschluß der Internet *service provider*.

958 *Rötzer, Florian*, Ein globales Bewertungssystem für Online-Inhalte, Telepolis v. 13.5.1999, über http://www.heise.de/tp/deutsch/inhalte/te/2842/1.html und oben FN 259.

959 Vgl. *Moglen, Eben*, Microsoft Wants US, The Nation (1998), FN 185.

960 Vgl. *OFTEL*, http://www.oftel.gov.uk/broadcast/dcms398.htm.

961 Vgl. dazu *II. Wettbewerbsrecht als Instrument der Inhaltskontrolle*, S. 243.

b. Förderung allgemeiner Teilnahme an digitalen Kommunikationsformen als Voraussetzung kooperativer Inhaltskontrolle

Kooperative Inhaltskontrolle basiert auf einem offenen Wettbewerb der Anbieter und einem ständigen Diskussionsprozeß aller Akteure über die Inhalte digitaler Medien. Folglich liegt ein zentraler Beitrag des Staates zur kooperativen Inhaltskontrolle darin, die Teilnahme möglichst vieler an diesen Prozessen zu fördern. Dies gilt um so dringender, je mehr sich wesentliche Kommunikationsprozesse in digitale Medien verlagern. Nicht nur Inhalte der innergesellschaftlichen Kommunikation[962] werden zunehmend exklusiv in digitalen Kommunikationsformen erreichbar sein.[963] Mit einem Bedeutungszuwachs digitaler Medien für Kommunikationsvorgänge zwischen Staat und Bürger bis hin zur politischen Willensbildung ist zu rechnen.[964]

Die staatliche Förderung allgemeiner Teilnahme an digitalen Kommunikationsformen kann nicht nur durch die Aufnahme dieser Dienste in ein gesetzliches Universaldienstregime[965], sondern auch durch direkte finanzielle Förderung allgemein zugänglicher digitaler Infrastruktur im staatlichen Aufgabenbereich[966] erfolgen.

c. Vermittlung von Kenntnissen über die Möglichkeiten privaten Selbstschutzes

Die Nutzer digitaler Kommunikationsformen können sich nur wirksam selbst gegen unerwünschte Inhalte schützen, wenn sie mit den ihnen zur Verfügung stehenden technischen Schutzmöglichkeiten vertraut sind. Nur dann können sie im Wettbewerb der Anbieter eigenverantwortliche Entscheidungen treffen. Die Vermittlung von Kenntnissen über die Möglichkeiten privaten Selbstschutzes ist mithin von zentraler Bedeutung für

962 Vgl. zur Unterscheidung von Informationsbeziehungen im staatlichen und gesellschaftlichen Bereich *Schoch*, VVDStRL 57 (1998), S. 158 (160ff.).

963 Zahlreiche aktuelle Meldungen aus Einzelbranchen oder Spezialthemengebieten werden ausschließlich etwa im Internet verbreitet, vgl. etwa die Informationsdienste „*Telepolis*“ , http://www.heise.de /tp oder „*Futurezone*“, http://futurezone.orf.at. Immer mehr Waren und Dienstleistungen sind ausschließlich im *online*-Handel erhältlich.

964 Bereits heute nutzen Parlamentarier das Internet, um Stimmungbilder der Wähler zu erhalten, Stadtnetze können Bürgern Beteiligungsmöglichkeiten eröffnen, etwa bei der Bauleitplanung, vgl. *Spannowsky*, DÖV 1997, 757 (760).

965 Vgl. § 17 ff. TKG. § 17 Abs. 2 S. 2 TKG bestimmt zwar, daß „die Bestimmung der Universaldienstleistungen [...] der technischen und gesellschaftlichen Entwicklung nachfragegerecht anzupassen“ ist, bisher jedoch sieht die Telekommunikations-Universaldienstverordnung (TUDLV v. 30.1.1997, BGBl. I, 141) nur einen Sprachtelefondienst mit ISDN-Leistungsmerkmalen, ein Auskunftssystem, Teilnehmerverzeichnis und die flächendeckende Bereitstellung öffentlicher Telefonzellen vor.

966 Etwa durch die umfassende Vernetzung von Schulen und Hochschulen, öffentlichen Einrichtungen. Davon wird immernoch sehr zurückhaltend Gebrauch gemacht, vgl. zum Programm „Schulen ans Netz“, *Moser, Heinz*, Schulen ans Netz – Top oder Flop ?, http://www.heise.de/ tp/deutsch/inhalt/ te/1163/1.html; überzeugender in dieser Hinsicht die Pläne Bayerns, jedem Bürger einen Internet-Zugang zur Verfügung zu stellen.

das Funktionieren kooperativer Inhaltskontrolle. Während es in den USA vor allem kommerzielle Anbieter von Filtersoftware und Verbände als ihre Aufgabe begreifen, über den Umgang mit dieser Technologie zu informieren[967], wird darin in Europa und Deutschland ein Teilaspekt der Vermittlung von Medienkompetenz in staatlicher Verantwortung gesehen.[968]

In diese Richtung gehende Ankündigungen von politischer Seite[969] haben aber bisher kaum den Charakter konkreter Beiträge zur kooperativen Inhaltskontrolle erreicht, während wesentlich konkreter versucht wird, eigene staatliche Kontrollaktivitäten auszubauen.[970] Es stellt sich die Frage, ob in der Vermittlung von Kenntnissen über die Möglichkeiten privaten Selbstschutzes nicht nur ein rechtspolitisches Anliegen zur Förderung kooperativer Inhaltskontrolle, sondern eine rechtliche Verpflichtung des Staats liegt.[971]

3. Schutzmöglichkeiten des Anbieters gegen die unerwünschte Verwendung der von ihm kommunizierten digitalen Inhalte oder personenbezogenen Daten

Inhaltskontrollregeln dienen nicht nur dem Schutz des Empfängers vor der Konfrontation mit rechtswidrigen Inhalten, sondern haben auch den Schutz des Inhalteanbieters vor rechtswidriger Verwendung der von ihm kommunizierten Inhalte zum Ziel.[972] Welche technologischen Möglichkeiten des Selbstschutzes Akteuren in dieser Konstellation bei der Kommunikation digitaler Inhalte zugute kommen können, soll im Folgenden an zwei Problemlagen untersucht werden, die herkömmlich durch Inhaltsbindungen des Urheber- und des Datenschutzrechts geregelt werden.

---

967 Vgl. die *WWW*-Angebote der bei *Faith Cranor/ Resnick/ Gallo*, a.a.O., (FN 830) genannten Anbieter und etwa der *American Civil Liberties Union*, http://www.aclu.org und der *American Library Association*, http://www.ala.org.

968 *Hoffmann-Riem, Wolfgang*, RuF 1995, 125 (129), *Depenheuer*, AfP 1997, 669; *Bertelsmann Stiftung*, Kommunikationsordnung 2000, 1997, S. 40ff.; *Wehrt, Christoph H.*, Die Herausforderungen des Staates in der Informationsgesellschaft, Aus Politik und Zeitgeschichte B 40/98 v. 25.9.98, S. 22 (27f.); *Trute*, VVDStRL 57 (1998), 218 (254); *Eudes, Yves*, „Censorware" – la censure privatisée, Le Monde, Télévision, Radio, Multimédia, 12./13.10.97.

969 *Europäische Kommission*, Illegale und schädigende Inhalte im Internet, KOM(96)487endg., 25ff.; *dies.*, Grünbuch über die Liberalisierung der Telekommunikationsinfrastruktur und der Kabelfernsehnetze (Teil 2), BR-Drs. 101/95, 86; *Schröder, Gerhard*, Alter Kontinent und neue Medien-Chancen und Perspektiven für Europas Medienwirtschaft, Rede am 16. Juni 1998 beim Medienforum NRW 98 in Köln; Bericht der Bundesregierung, „Info 2000", BT-Drs. 13/4000, S. 89ff.

970 Vgl. die Aktivitäten zur Entwicklung eines Softwareprogramms zum Aufspüren rechtswidriger Inhalte, FN 750 und die Bestrebungen zur Verabschiedung des ENFOPOL-Programms zum Abhören digitaler Kommunikation, FN 17, 475ff.

971 Vgl. *III. Rechtliche Verpflichtung des Staates zur Vermittlung von Kenntnissen über den Umgang mit Möglichkeiten des technologischen Selbstschutzes*, S. 254.

972 Dazu dienen etwa die Regeln zum Urheberrechts- und Datenschutz. Zu deren Übertragbarkeit auf die Kommunikation digitaler Inhalte vgl. *a. Urheberrecht*, S. 68, *g. Privatheit der Kommunikation*, S. 105.

a. Schutz vor unerwünschter Verwendung kommunizierter digitaler Inhalte

Um Inhalte, die an bestimmte Empfänger kommuniziert werden, vor dem unerwünschten Zugriff Dritter zu schützen, steht bei der digitalen Kommunikation die Verschlüsselung als technologische Schutzmöglichkeit zur Verfügung.[973] Inhalte, die wegen ihrer hohen Vertraulichkeit oder weil sie vom berechtigten Empfänger bezahlt werden, nicht für Dritte nutzbar sein sollen, können so effektiv vor dieser unerwünschten Verwendung geschützt werden.[974]

Anders liegt es, wenn eine bestimmte Verwendung durch den an sich berechtigten Kommunikationsempfänger selbst unterbunden werden soll. Wie gezeigt, führt jede telekommunikative Verbreitung digitaler Inhalte dazu, daß beim Empfänger ein vom Original nicht zu unterscheidendes Exemplar des Inhalts entsteht, das von diesem beliebig genutzt werden kann.[975] Insbesondere kann der Empfänger gegen den Willen bzw. gegen eine entsprechende vertragliche Vereinbarung mit dem Erstverbreiter den Inhalt kommerziell oder unkommerziell weitergeben, ohne daß der Zweiterwerber von seiner Nichtberechtigung oder der Erstverbreiter von dieser Weitergabe erfahren. Will der Anbieter dies wirksam verhindern, muß er dafür sorgen, daß der kommunizierte Inhalt entweder technologisch nicht erneut übertragbar ist oder daß er für den Empfänger in einer Weise gekennzeichnet wurde, die eine Weitergabe für den Nichtberechtigten oder den Zweiterwerber unattraktiv macht.

Derartige technologische Schutzsysteme werden als *Electronic Copyright Management Systems (ECMS)* bezeichnet[976]. Zum Kopierschutz sind vor allem Systeme bekannt, die Kopien verkörperlichter digitaler Datenträger verhindern sollten. So erlaubt das *Digital Audio Tape (DAT)* zwar unbegrenzte Kopien vom Originalband, nicht aber Kopien von der Kopie. Ein von der *MiniDisc* von *Sony* verwendetes System sorgt dafür, daß Kopiebrennungen nicht mehr die Originalqualität erreichen. Derartige Technologien können grundsätzlich auch auf die *online*-Übertragung digitaler Inhalte übertragen werden.[977] Nach einem von *Disney Inc.* vorgeschlagenen System muß ein spezieller Chip im Empfangsgerät des Nutzers dem angefragten *server* erst bestätigen, daß keinerlei Aufnahmegeräte angeschlossen sind, bevor mit der Inhaltsübertragung begonnen wird.[978]

---

973 Vgl. oben *bb. Technische Unmöglichkeit der Identifizierung bei verschlüsselten Inhalten*, S. 177 und *ACLU,* Big Brother in the Wires, 1998, über http://www.aclu.org.

974 Zur Funktionsweise von Verschlüsselungssoftware FN 184.

975 Vgl. oben *a. Urheberrecht*, S. 68.

976 Vgl. *Bechtold, Stefan,* Multimedia und das Urheberrecht, Seminararbeit abrufbar als pdf-Dokument unter http://www.jura.uni-tuebingen.de/student/stefan.bechtold/sem97, dort S. 33ff.; teilweise veröffentlicht in GRUR 1998, 18ff.

977 *Wand, Peter,* GRUR Int. 1996, 897 (899).

978 Information von *Eben Moglen* im Kurs „Computers, Privacy and the Constitution", Columbia Law School, Früjahrssemester 1998.

Mittels „Digitaler Wasserzeichen“[979] können dem Inhalt Informationen etwa über den Urheber, den berechtigten Empfänger und die vertraglichen Nutzungsbedingungen beigefügt werden, die so „robust“ sind, daß sie der Erstempfänger nicht entfernen oder verändern kann. Dadurch kann eine Authentifizierung des berechtigten Übertragungsvorgangs durch den Urheber erreicht werden, die der unbefugt Weitergebende dem Zweiterwerber nicht bieten kann. Dessen Inhalt wäre immer als „Raubkopie“ erkennbar und damit weniger attraktiv. „Digitale Wasserzeichen“ lassen sich auch in Audio- und Videoinhalten verbergen.[980]

Bedenklich sind dagegen Lösungen, bei denen der auf einem vernetzten Computer benutzte digitale Inhalt – meist Computersoftware – von sich aus mit „seinem“ Urheber Kontakt aufnimmt oder ein Dritter vom Nutzer unbemerkt mit dessen Rechner kommuniziert, um das Vorhandensein von Raubkopien festzustellen.[981] Hierbei könnten in vom Nutzer unkontrollierbarer Weise persönliche Daten kommuniziert werden, wovor sich dieser gerade auch durch technologische Mittel schützen möchte.

b. Schutz vor unerwünschter Verwendung kommunizierter personenbezogener Daten

Gegen den Fall, daß die unerwünschte Verwendung kommunizierter personenbezogener Daten darin besteht, daß ein Dritter die an sich bestimmungsgemäß kommunizierten Daten unbefugt abhört, bieten sich wiederum die Möglichkeiten der Verschlüsselung. Um als Versender vertraulicher Informationen zu verhindern, daß Dritte Zugriff auf die eigene Absenderadresse erhalten, können Inhalte über sogenannte *anonymous remailer* versandt werden, die die Adreßinformationen der kommunizierten Datenpakete abtrennen.[982]

---

979 Zur Technologie digitaler Wasserzeichen vgl. *Lacy, Jack / Quackenbush, Schuyler R. / Reibman, Amy R. / Snyder, James H.*, Intellectual Property Protection Systems and Digital Watermarking, Optics Express 1998, 478, unter http://epubs.osa.org/oearchive/pdf/7085.pdf; *Mintzer, Fred / Lotspiech, Jeffrey / Morimote, Norishige*, Safeguard Digital Library Contents and Users – Digital Watermarking, D-Lib Magazine, December 1997, unter http://www.dlib.org/dlib/december97 /ibm/ 12lotspiech.html.

980 Zu den verschiedenen Verfahren, die sich teilweise noch in der Entwicklung befinden, vgl. die umfangreichen *hyperlinks* auf der *WWW*-Seite des *Laboratorio Communicazioni & Immagini* der Universität Florenz, http://cosimo.die.unifi.it/~piva/Watermarking/watermarking.html und unter http://www-sal.cs.uiuc.edu/~l-qiao/copyright-q2.html.

981 Es ist etwa möglich, daß frei zugängliche Internet-Inhalte im *Microsoft*-Network (*msn*) kleine Programme (*ActiveX-Applets*) enthalten, die die Festplatte des Nutzers nach raubkopierten *Microsoft*-Produkten absuchen und beim nächsten Besuch auf dem *msn-server* an *Microsoft* zurückgeschickt werden.

982 Zur Funktionsweise von *anonymous remailern* vgl. *Froomkin*, (FN 871). Es handelt sich allerdings um einen begrenzten Schutz, da die Information auf der Strecke bis zum *anonymous remailer* abhört werden kann.

Zu differenzieren ist wiederum für den Fall, daß sich der Anbieter gegen eine unerwünschte Verwendung seiner Daten durch den Kommunikationspartner schützen möchte.

Ist der Nutzer an sich zur Weitergabe seiner persönlichen Daten bereit, etwa weil diese zur Abwicklung des beabsichtigten *online*-Geschäfts nötig ist oder er dadurch Nutzungs- (Preis-)vorteile erlangt, möchte er dennoch die Kontrolle darüber behalten, ob der Empfänger die Daten darüber hinaus noch für andere Zwecke verwendet. Zu diesem Zweck ist er darauf angewiesen, von einer glaubwürdigen Stelle Informationen über die Datenverwendungspraktiken seines Kommunikationspartners zu erlangen, anhand derer er entscheiden kann, ob er das *online*-Geschäft unter diesen Bedingungen mit ihm abwickeln möchte oder es vorzieht, sich einen anderen Partner zu suchen.

Derartige „glaubwürdige Stellen" (*Trust Center*) können ihrerseits wieder miteinander im Wettbewerb stehen und kontrollieren sich so selbst.[983] Technologische Verfahren für das automatisierte Zustandebringen eines solchen „Datenschutzübereinkommens" zwischen einem Nutzer und dem Anbieter etwa eines Dienstes im *WWW* bestehen bereits. Dabei vergleicht der Computer des Nutzers die Selbstverpflichtungen von Diensteanbietern hinsichtlich der Sammlung, Verarbeitung und Weitergabe von Daten mit den voreingestellten Präferenzen des Nutzers.[984]

Die besondere Gefahr der unkontrollierten Kommunikation persönlicher Daten besteht darin, daß an verschiedenen Stellen zu an sich legitimen Zwecken gespeicherte Datensätze immer anhand der gleichen Angaben (Name, Geburtsdatum, Photo o.ä.) einer bestimmten Person zuzuordnen sind und damit eine Verbindung dieser einzelnen Datensätze (Abgleich) möglich ist, die dem Abgleichenden eine größere Menge personenbezogener Informationen verschafft, als er allein durch seine Kommunikation mit der betreffenden Person erreichen könnte und die er zu deren Abwicklung unmittelbar auch nicht benötigt (sogenanntes „Datenprofil").

Ist die Übermittlung auf die Identität einer bestimmten Person bezogener persönlicher Daten zur Nutzung eines digitalen Angebotes nicht erforderlich, so kann der Nutzer technologische Schutzmaßnahmen verwenden, die ihm erlauben, gar keine oder nur ein Minimum an personenbezogenen Daten zu kommunizieren. Den effektivsten Schutz vor unerwünschter Verwendung von Daten durch den Kommunikationspartner bietet die anonyme oder pseudonyme Kommunikation.

983 Vgl. zu Funktionsweise und Selbstverständnis eines solchen *Trust Centers*, http://www. truste.org.

984 *Reagle, Joseph / Faith Cranor, Lorrie*, The Platform for Privacy Preferences, http://www.w3.org /TR/ 1998/NOTE-P3P-CACM-19980731.

Ein Großteil der im Rahmen digitaler Kommunikationsformen heute üblichen Kommunikationsvorgänge kann technisch problemlos anonym durchgeführt werden.[985] Dazu gehört auch die anonyme Bezahlung von digitalen Inhalten und in digitalen Diensten. Die theoretischen Grundlagen[986] und die ersten praktischen Umsetzungen verschiedener Modelle anonymer elektronischer Bezahlformen[987] sind bereits seit Mitte der 90er Jahre bekannt[988] und können heute als ausgereift angesehen werden. Sie werden jedoch noch selten angeboten. Daran haben auch §§ 4 Abs. 1 TDDSG und § 13 Abs. 1 MDStV nichts ändern können, die die Möglichkeit anonymer Bezahlung von Tele- und Mediendiensten bei technischer Möglichkeit und Zumutbarkeit ausdrücklich vorschreiben.

Nicht nur für die Bezahlung, sondern auch für die *online*-Abwicklung zahlreicher weiterer Kommunikationsvorgänge des täglichen Lebens bestehen technische Lösungen, die die Kommunikation persönlicher Daten fast vollständig vermeiden helfen. So hat *David Chaum* bereits 1992 ein praktikables Konzept einer *Smart Card* vorgeschlagen, die persönliche Daten nur in dem benötigten Umfang und grundsätzlich durch „blinde" digitale Signaturen pseudonymisiert bekanntgibt. Mit diesem „digitalen Repräsentanten" kann dem berechtigten Datenbedarf von Banken, Ärzten, Steuerbehörden und Verkäufern als auch den Privatheitsinteressen der Nutzer gleichermaßen Rechnung getragen werden, wobei der Nutzer allein die vollständige Kontrolle über seine persönlichen Daten behält.[989]

---

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

986 Vgl. jeweils mit zahlreichen weiteren Nachweisen *Froomkin*, (FN 871); *Chaum*, (FN 871).

987 Die Firma *DigiCash* von *D. Chaum* lizensiert Software an Banken, mit der sogenannte *„blinded coins"* ausgegeben werden können. Als weltweit erste Bank hat die *Mark Twain Bank of St. Louis, Missouri* am 23.10.1995 derartige *„blinded coins"* ausgegeben, heute ist etwa auch die *Deutsche Bank* Lizenznehmerin von *DigiCash*, vgl. http://www.digicash.com/ecash/issuers/db/; die britische *Mondex Bank* hat 1996 mit der Ausgabe sogenannter *„electronic purses"* begonnen. Dies sind intelligente Chipkarten, mit denen eine anonyme *online*-Bezahlung möglich ist, ohne daß es des gesonderten *clearing* jeder Bezahlung durch eine Bank bedürfte, vgl. die Informationen unter http://www.mondex.com/mec_ noflash.html. Zusammenfassend *O'Mahony, Donald / Peirce, Michael / Tewari, Mitesh*, Electronic Payment Systems, Norwood, MA, 1997. Eine Sammlung von *hyperlinks* zu Dutzenden verschiedener *online*-Zahlungstechnologien unter http://ganges.cs.tcd.ie /mepeirce/Project/oninternet.html. Die – soweit ersichtlich – ergiebigste akademische Zusammenstellung in deutscher Sprache bietet *Rott, Christian*, E-Cash: Bestandsaufnahme, http://stud1.tuwien. ac.at/~e8525020/preecash.html.

988 Auch die Europäische Union unterstützt mit dem sog. *Conditional Access for Europe (CAFE)*-Projekt die Entwicklung anonymer *online*-Zahlungsmöglichkeiten, vgl. CAFE—Conditional Access For Europe, http://www.informatik.uni-hildesheim.de/FB4/Projekte/sirene/projects /cafe/index.html; The CAFE Project, http://www.cwi.nl/cwi/projects/cafe.html; *DigiCash*, DigiCash products—the CAFE project, http://www.digicash.com/projects/cafe.html.

989 *Chaum, David*, Achieving Electronic Privacy, Scientific American, August 1992, 96; http:// ganges.cs.tcd.ie/mepeirce/Project/Chaum/sciam.html.

4. Staatliche Unterstützungmaßnahmen

Bezogen auf die genannten Kommunikationssituationen bestehen zahlreiche Möglichkeiten des Staates, die Schutzmöglichkeiten des Anbieters gegen die unerwünschte Verwendung der von ihm kommunizierten digitalen Inhalte oder personenbezogenen Daten zu unterstützen und so einen Beitrag zur kooperativen Kontrolle von Kommunikationsinhalten zu leisten. Es handelt sich zum Teil um Maßnahmen, deren Bezug zum Inhaltskontrollrecht bisher noch wenig herausgestellt wurde. Einige Beispiele sollen hier genannt sein:

a. Lockerung urheberrechtlicher Strukturen

Die Anwendung des klassischen Urheberrechts auf digitale Kommunikationsinhalte bereitet zahlreiche Schwierigkeiten.[990] Es wird zunehmend gefragt, ob der Grundgedanke des Urheberrechts, Kreativität und Schöpfergeist durch die Einräumung von Ausschlußrechten zu fördern, bei digitalen Inhalten überhaupt noch seine Berechtigung hat.[991] Auch die Annahme, Urheber könnten eine angemessene Vergütung für ihre Leistungen nur durch ein gesetzlich geregeltes Verwertungssystem erhalten, erweist sich im Lichte der dargestellten technischen Möglichkeiten selbstkontrollierter Direktverbreitung von Inhalten als zweifelhaft.[992] Hinsichtlich digitaler Werke, die der Urheber zu selbstgewählten Bedingungen direkt kommunizieren kann, ist vielmehr zu befürchten, daß einem gesetzlich durchregulierten Verfahren, in dem faktische Verwertungsmonopole[993] nach einem pauschalierten Vergütungssystem[994] viele Einzelurheberrechte gesamthaft verwerten, die nötige Flexibilität fehlt[995]. Es könnte die Rechte und Interessen zahlreicher, global agierender Urheber verschiedenster Größe, die Werke unter-

990 Vgl. *a. Urheberrecht*, S. 68.

991 *Moglen, Eben*, Anarchism Triumphant: Free Software and the Death of Copyright, http://old.law. columbia.edu/my_pubs/anarchy.htm; *Eudes, Yves*, La deuxième révolution Gutenberg, Le Monde v. 13.8.98, S. 9; *Lutterbeck, Bernd*, Klassische Regelungsansätze werden der Wirklichkeit nicht mehr gerecht, Das Parlament Nr. 40 v. 25.9.98, S. 13; diese Diskussion wird verstärkt durch den zunehmenden Erfolg des kostenlosen Betriebssystems *Linux*, das durch urheberrechtsfreie, weltweite Kooperation entstanden ist, dazu *Krempl, Stefan*, Software muß frei sein – Interview mit Richard Stallman, Telepolis v. 19.5.99 über http://www.heise.de/tp/deutsch/inhalt/te/2860/1.html.

992 Vgl. *a. Schutz vor unerwünschter Verwendung kommunizierter digitaler Inhalte*, S. 216.

993 Wegen des Monopolcharakters der Verwertungsgesellschaften in ihrem Tätigkeitsbereich (nur im Bereich der Filmverwertung konkurrieren vier Gesellschaften) unterliegen sie einer Erlaubnispflicht und einer staatlichen Aufsicht, vgl. Schricker-*Reinbothe*, Vor §§ 1ff. WahrnG Rn. 7, 11. Dies wurde seinerzeit als für alle Beteiligten nützlich und zweckmäßig angesehen, vgl. Begründung zum WahrnG, BT-Drs. IV/271, S. 11, 9.

994 Vgl. § 7 Urheberrechtswahrnehmungsgesetz v. 9. 9. 1965 (BGBl. I, 1294), zuletzt geändert durch das 4. Gesetz zur Änderung des Urheberrechtsgesetzes vom 8. 5. 1998 (BGBl. I, 902).

995 Verständlicherweise sind die Verwertungsgesellschaften selbst anderer Meinung, vgl. *Kreile, Reinhold / Becker, Jürgen*, Verwertungsgesellschaften in der Informationsgesellschaft, FS Mestmäcker, 1996, S. 77; kritisch auch *Reinbothe, Jörg* a.a.O.,Vor §§ 1ff. WahrnG, Rn. 16.

schiedlichster Art schaffen und digital verbreiten, kaum ausreichend zur Geltung bringen; eine schwache Staatsaufsicht könnte das sich herausbildende Netz kooperierender nationaler „Weltmonopol"-Gesellschaften kaum kontrollieren.[996] Es beseitigte eher den durch die Technologie ermöglichten Flexibilitätsgewinn, weckte Erwartungen an staatlichen Schutz, die immer weniger durchsetzbar sind und wirkte zugleich hemmend auf die dynamische Weiterentwicklung technologischen Schutzes (etwa *copyright management*-Systeme[997]).[998]

Es wäre ein rechtspolitisch überlegenswerter Beitrag des Staates zur kooperativen Inhaltskontrolle, Regelungen hier zu unterlassen oder sogar abzuschaffen. Fraglich ist, inwiefern eine Lockerung urheberrechtlichen Schutzes für digitale Kommunikationsinhalte rechtlich zulässig wäre.[999]

b. Sicherung der freien Benutzung von Verschlüsselung

Verschlüsselung bietet die wirksamste Garantie gegen die unbefugte Kenntnisnahme Dritter von digitalen Kommunikationsinhalten. Ihre freie Benutzbarkeit für jedermann ohne die mit einer Schlüsselhinterlegungspflicht verbundenen Risiken ist ein wesentliches Element privaten Selbstschutzes.[1000] Weltweit setzt sich zunehmend die Auffassung durch, daß gerade das Unterlassen jeglicher Kryptographieregulierung ein sinnvoller staatlicher Beitrag zur Kommunikationsinhaltskontrolle ist.[1001] In jüngerer Zeit haben auch Frankreich und die USA ihre vormals strengen Regulierungen ausgesetzt bzw. gelockert.[1002]

---

996 Die internationale Zusammenarbeit von Verwertungsgesellschaften verstärkt sich stetig, etwa durch die Einrichtung von *clearing*-Stellen, vgl. *Kreile, Reinhold / Becker, Jürgen*, a.a.O. Kritisch schon zum heutigen nationalen System, das zu unangemessenen Wahrnehmungsbedingungen führe und von der Staatsaufsicht nicht wirksam kontrolliert werden könne *Rehbinder, Manfred*, DVBl. 1992, 216.

997 Vgl. oben *a. Schutz vor unerwünschter Verwendung kommunizierter digitaler Inhalte*, S. 216.

998 Vgl. die gleichlautenden Bedenken der *Internet Society* gegen den Entwurf einer EG-Copyright-Richtlinie, *Krempl, Stefan*, Copyright-Richtlinie überdenken, Telepolis v. 1.3.1999, unter http://www.heise.de/tp/deutsch/inhalt/te/1936/1.html.

999 Dazu unten *IV. Mögliche Verletzung rechtlicher Bindungen durch die Lockerung urheberrechtlicher Strukturen und die Rücknahme von strafrechtlichen Inhaltsverboten*, S. 258.

1000 Vgl. *bb. Technische Unmöglichkeit der Identifizierung bei verschlüsselten Inhalten*, S. 176.

1001 *Global Internet Liberty Campaign*, Cryptography and Liberty - An International Survey of Encryption Policy, Über http://www.gilc.org.

1002 Vgl. *Lorenz-Meyer, Lorenz*, Europa: Anderswo ist Kryptographie Chefsache, SPIEGEL ONLINE v. 27. Mai 1999, http://www.spiegel.de/netzwelt/politik/0,1518,24693,00.html; *Gabriel, Susanne*, Frankreich: Hürden für die Lauscher, SPIEGEL online v. 9.2.99; *Messmer, Ellen*, White House changes Encryption Tune, a Smidge, Network World v. 19. Oktober 1998, S. 60; zu neueren US-Gerichtsentscheidungen, die Verschlüsselungsoftware als vom *First Amendment* erfaßte Rede („*speech*") ansehen, *Cunard, Jeffrey P. / Coplan, Jennifer B.*, 15 Computer Law Strategist Vol. 4, S. 5 (August 1998).

Die Bundesregierung hat sich nach zunächst anderen Überlegungen[1003] am 2. Juni 1999 in den „Eckpunkte der deutschen Kryptopolitik" für eine vollständige Freigabe von Kryptographieprodukten entschieden. Sie beabsichtigt nicht, „die freie Verfügbarkeit von Verschlüsselungsprodukten in Deutschland einzuschränken. Die Bundesregierung wird [...] die Verbreitung sicherer Verschlüsselung in Deutschland aktiv unterstützten. Dazu zählt insbesondere die Förderung des Sicherheitsbewußtseins bei den Bürgern, der Wirtschaft und der Verwaltung."[1004] Darin liegt ein wesentlicher Beitrag des Staates zur kooperativen Inhaltskontrolle.

c. Förderung technischer Möglichkeiten zur datensparsamen Kommunikation als Ergänzung herkömmlicher Datenschutzregulierung

Die Sorge vor freiheitsgefährdender *staatlicher* Datenerhebung, -sammlung und -verarbeitung gab den Anlaß zur Schaffung des heutigen Datenschutzrechts[1005], das den Staat zu datensparsamer Aufgabenerfüllung anhält.[1006] Letztlich haben Datenschutzgesetze jedoch die zunehmende Ansammlung personenbezogener Daten sowohl in den Händen des Staates und Privater nicht verhindern können.[1007] Von den staatlichen Datenschutzbeauftragten selbst werden weitgehende Reformen gefordert.[1008] Erst durch heute bestehende technologische Möglichkeiten können zahlreiche Kommunikationsvorgänge wirklich mit einem Minimum an Datenanfall und zudem ohne die Möglichkeit eines Datenabgleichs abgewickelt werden.[1009]

Diese Technologie ist nicht auf Kommunikation im gesellschaftlichen Bereich beschränkt, sondern eignet sich auch für Kommunikationsvorgänge zwischen Staat und Bürger. Zur datensparsamen Kommunikation trügen etwa Systeme bei, die es dem Bürger erlauben, etwa bei der Beantragung staatlicher Leistungen das Vorhandensein erfor-

1003 Zu dem Modell des ehemaligen Bundesinnenministers *Kanther*, das die Hinterlegung von Nachschlüsseln auch im Inland erfordert hätte, *Schulzki-Haddouti, Christiane,* Verschlüsselungstechniken sicherheitspolitisch umstritten, Handelsblatt v. 26.10.98, http://www.handelsblatt.de/cgi-bin/hbi.exe?SH=&iPV=0&FN=hb &SFN=news_ct_artcomputer&iID=42158.

1004 Vgl. *Pressemitteilung des BMI / BMWi*, http://www.bmwi.de/presse/1999/0602prm1.html.

1005 Vgl. BVerfGE 49, 1 – *Volkszählung*.

1006 Vgl. § 13 Abs. 1 BDSG, der die staatliche Datenerhebung für zulässig erklärt, die zur „Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist".

1007 Vgl. *Bäumler, Helmut*, Der neue Datenschutz in ders., Der neue Datenschutz, S. 1(2): Die Verarbeitungswünsche der Verwaltung seien „mehr oder weniger ungeschmälert in Dutzende von Gesetzen" aufgenommen worden, mit „akribischem Fleiß" hätten „Verwaltung und Gesetzgeber die Realität der Datenverarbeitung und zusätzlich das Wünschenswerte in Gesetzestexten aufgeschrieben". Zur Kritik an den „weitgehend auf Generalklauseln" beschränkten Regeln für die Datenverarbeitung durch Private *Hoffmann-Riem, Wolfgang*, Informationelle Selbstbestimmung als Grundrecht kommunikativer Entfaltung, in Bäumler, a.a.O., S. 11 (16) mwN.

1008 *Schulzki-Haddouti, Christiane*, Bürgerrechte für die Informationsgesellschaft, Telepolis v. 10.11.98 http://www.heise.de/tp/deutsch/inhalt/te/1637/1.html.

1009 Vgl. oben *b. Schutz vor unerwünschter Verwendung kommunizierter personenbezogener Daten*, S. 217.

derlicher gesetzlicher Voraussetzungen nachzuweisen, ohne dabei überflüssige, für den konkreten Kommunikationsvorgang nicht benötigte persönliche Daten preiszugeben. Mit Hilfe eines „digitalen Repräsentanten“[1010] könnte ein Bürger etwa bei der Beantragung von Kindergeld für jedes Kind bloß bestätigen, *daß* sie eine bestimmte Altersgrenze nicht überschritten haben bzw. *daß* sie sich in der Ausbildung befinden sowie *daß* für ein bestimmtes Kind und einen bestimmten Zeitraum Leistungen nicht bereits gewährt wurden, ohne dabei auch seinen eigenen Namen und die seiner Kinder, deren Geburtsdatum und Ausbildungsstelle angeben zu müssen. Die Richtigkeit der gemachten Angaben würde durch die auf dem Repräsentanten fälschungssicher gespeicherten Informationen etwa des Einwohnermeldeamts oder der Schule des Kindes glaubhaft bestätigt. Eine Überprüfung aller Angaben durch die Behörde und die damit verbundene unnötige Kommunikation zusätzlicher persönlicher Daten würde vermieden.

Noch weniger als die Datenverarbeitung durch öffentliche Stellen läßt sich die mit Hilfe vernetzter Computer jedermann mögliche und zunehmend grenzüberschreitende Datenverarbeitung durch Private aussichtsreich mit gesetzlichen Regeln kontrollieren.[1011] Dagegen kann der Staat Private – nötigenfalls unter Androhung gesetzlicher Intervention – dazu auffordern, ihren Kunden freiwillig und gegebenenfalls im Wege von Selbstverpflichtungen Anonymität, Pseudonymität oder die Benutzung datensparsamer Technologien anzubieten. Die bereits bestehende Verpflichtung der Anbieter zum Angebot anonymer Nutzungs- und Bezahlformen in §§ 4 Abs. 1 TDDSG und 13 Abs. 1 MDStV hat bisher keinen Lenkungseffekt erzielen können, weil wirksame Sanktionen bei ihrer Nichteinhaltung fehlen.[1012] Daneben bestehen zahlreiche, viel konkretere Möglichkeiten, die der Staat den Anbietern nahelegen könnte.[1013]

Beim Schutz vor unerwünschter Verwendung personenbezogener Daten leistet der Staat durch die technikgerechte Gestaltung von Kommunikationsvorgängen einen wertvolleren Beitrag als durch Regulierung.

d. Vermittlung von Kenntnissen

Auch die technologischen Maßnahmen zum Selbstschutz vor unerwünschter Verwendung von kommunizierten Inhalten und persönlichen Daten erfordern erhebliche Kenntnisse, ohne die ihre Nutzung kaum zweckmäßig möglich ist.

1010 Dies ist eine von *David Chaum* vorgeschlagene *SmartCard*, die zwei sich gegenseitig kontrollierende Mikrochips enthält. Vgl. oben FN 989.

1011 Die etwa in §§ 3, 4 TDDSG niedergelegten Grundsätze und Pflichten sind zwar wegweisend, aber kaum durchsetzbar, vgl. oben *bb. Datenschutzrechtlicher Vertraulichkeitsschutz*, S. 109. Für Angebote aus dem Ausland kann das TDDSG keine Verbindlichkeit beanspruchen.

1012 Vgl. oben *bb. Datenschutzrechtlicher Vertraulichkeitsschutz*, S. 109.

1013 Zahlreiche Verschläge werden dazu von den Landesdatenschutzbeauftragten selbst gemacht, vgl. Achtzehnter Bericht des Landesbeauftragten für den Datenschutz Baden-Württemberg 1997, http://www.datenschutz.bawue.de/tb/tb97.doc, unter 1.2.2.

An deren Vermittlung an möglichst weite Bevölkerungskreise muß dem Staat um so mehr gelegen sein, je wirkungsvoller er verhindern will, daß auf Dauer nur wenige Bürger von den erweiterten Möglichkeiten digitaler Kommunikation profitieren können. Leistet der Staat diesen Beitrag zur kooperativen Inhaltskontrolle nicht, riskiert er, daß seine Bürger gegen die Risiken der neuen Kommunikationsformen nur durch gesetzliche Vorschriften geschützt sind, deren Wirksamkeit begrenzt ist.[1014]

III. Zwischenergebnis

Die Ziele von Kommunikationsinhaltskontrolle umfassen den Schutz der Akteure vor Rechtsverletzungen durch die Konfrontation mit unerwünschten Inhalten und die unerlaubte Verwendung kommunizierter Inhalte und persönlicher Daten. Konnten diese Ziele in herkömmlichen Medien befriedigend durch gesetzliche Inhaltsbindungen verwirklicht werden, bietet sich in ausdifferenzierten digitalen Kommunikationsformen eher eine Aufgabenverteilung zwischen privatem Selbstschutz durch die Akteure und präzisierten staatlichen Schutzleistungen im Vorfeld der Kommunikationsinhaltskontrolle an.

Die Kooperation zwischen dem Staat und Privaten bei der Kontrolle digitaler Kommunikationsinhalte verschiebt den Schwerpunkt staatlicher Aktivität in erheblicher Weise. Statt der unmittelbaren Garantie bestimmter Inhalte und allgemeinverbindlicher Schutzregime eröffnen sich ihm darin Aufgaben der Förderung privaten Selbstschutzes. Nach dem bisher Dargestellten vermögen kooperative Kontrollformen staatliche Inhaltskontrolle auch dort wirkungsvoll zu ergänzen, wo diese schwächer wird.

Die beschriebenen Formen kooperativer Kontrolle können jedoch die Kommunikation von Inhalten nur dann verhindern, wenn entweder der Empfänger oder der Anbieter dies wünscht. Gegen den Willen beider an einem digitalen Kommunikationsvorgang beteiligter Akteure kann ein auf ökonomischen Anreizen und verantwortungsbewußtem Verhalten der Akteure im Wettbewerb basierendes Kooperationsmodell die digitale Kommunikation eines heute als rechtswidrig definierten Inhalts nicht unterbinden.

IV. Stimulierung gesellschaftlicher Selbststeuerung durch Lockerung von Inhaltsbindungen

Es gibt danach einen Anteil digitaler Kommunikation rechtswidriger Inhalte, den zunächst weder gesetzliche Inhaltsregulierung noch kooperative Kontrolle aussichtsreich verhindern können. Zu ihm gehört zum einen die Kommunikation rechtswidriger digi-

1014 Vgl. *Bäumler,* (FN 1007).

taler Inhalte, die für Außenstehende unzugänglich[1015] zwischen zwei oder mehr Gleichgesinnten stattfindet *(zugangsbeschränkte kollusive Kommunikation)*, etwa der Austausch von Informationen via *e-mail* oder in einer geschlossenen Benutzergruppe. Zum zweiten ist nicht wirksam zu verhindern, daß rechtswidrige Inhalte aus offenen Angeboten aus dem Ausland oder gleichartigen anonymen Angeboten im Inland von Nutzern abgerufen werden, die von technischen Schutzmöglichkeiten keinen Gebrauch machen wollen[1016] und dazu auch nicht gezwungen werden können[1017] *(offene kollusive Kommunikation)*.

Bisher sind zur Lösung dieses Problems vornehmlich Vorschläge gemacht worden, die mit einer Verschärfung gesetzlicher Inhaltskontrollregeln und einer Erleichterung ihrer hoheitlichen Durchsetzbarkeit einhergehen, zu deren rechtlichen und technischen Schwierigkeiten schon Stellung genommen wurde.[1018] Diese läuteten zudem einen Wettlauf zwischen Recht und Technik ein, der Gefahr liefe, die inhaltliche Auseinandersetzung mit Anbietern und Nutzern rechtswidriger Inhalte aus dem Auge zu verlieren und statt dessen auch Unbeteiligte zur Entwicklung immer neuer Umgehungstechniken herausfordert, weil sie die „Nebenwirkungen" der Regulierung nicht akzeptieren, von denen sie staatliche Zensur befürchten.[1019]

Auch andere Ansätze sind denkbar. Vor allem im US-amerikanischen Verfassungsrecht besteht die Vorstellung, nachhaltige Inhaltskontrolle sei eher im Rahmen einer gesellschaftlichen Auseinandersetzung mit kontroversen Inhalten erreichbar, einem Wettstreit der Meinungen, in dem sich das Gute durchsetzt.[1020] Die Vorzugswürdigkeit eines öffentlichen Diskurses gegenüber staatlichen Inhaltsverboten beschreibt *Justice Brandeis* in Whitney v. California[1021] mit den Worten: *„If there be time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the re-*

1015 Machen die Teilnehmer dieser Kommunikation nicht nur von ihren Möglichkeiten zur Inhaltsfilterung, sondern auch von ihren Möglichkeiten zur Verschlüsselung keinen Gebrauch, können sie durch rechtmäßiges Abhören ihrer Kommunikation im Rahmen gesetzlicher Inhaltskontrollvorschriften zur Verantwortung gezogen werden.

1016 Frühere Vorschläge, den Nutzer selbst verstärkt für die Verletzung gesetzlicher Inhaltsbindungen verantwortlich zu machen, vgl. *Engel*, AfP 1996, 220 (227); ihn zitierend *von Bonin/Köster*, ZUM 1997, 821 (dort FN 50), sind letztlich nicht aufgegriffen worden.

1017 Arbeitgeber haben die Möglichkeit, Filtermaßnahmen auch gegen den Willen ihrer Arbeitnehmer in Geräten am Arbeitsplatz einzusetzen; Gleiches gilt im Verhältnis zwischen Eltern und Kindern.

1018 Vgl. *5. Kapitel: Zwischenergebnis: Das „Dilemma" staatlicher Kontrolle von digitalen Kommunikationsinhalten*, S. 197.

1019 Vgl. die Reaktion von *MIT*-Mitarbeitern auf deutsche Inhaltskontrollaktivitäten, oben *bb. Access provider*, S. 186.

1020 Vgl. zuerst *Supreme Court of the United States*, Abrams v. United States, 250 U.S. 616 (1919), J. Holmes (dissenting): „But when men have realized that the time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reaches by free trade in ideas – that the best test of truth is the power of the thought to get itself accepted in the competition of the market...".

1021 274 U.S. 357, 377 (1927) (J. Brandeis concurring).

medy to be applied is more speech, not enforced silence." Danach stehen Inhaltskontrolle durch staatliche Gesetze und Inhaltskontrolle durch öffentlichen Diskurs zumindest teilweise in einem Widerspruchs-, wenn nicht Ausschlußverhältnis zueinander. Denn, so legt *Brandeis* nahe, die *discussion* und der *process of education* können ihre Überzeugungskraft nur dann entfalten, wenn einerseits die gegen *falsehood, fellacy* und *evil* eingestellten gesellschaftlichen Kräfte nicht in dem Bestehen einer gesetzlichen Inhaltsbindung eine Vollzugsgarantie des Staates und damit eine Freizeichnung von eigener Überzeugungsarbeit erblicken können, sondern sich gerade durch die sichtbare Präsenz mißbilligter Inhalte zur Intervention angespornt sehen.[1022] Andererseits soll den Vertretern einer mißbilligten Haltung nicht durch ein gesetzliches Verbot der Rückzug vom öffentlichen Diskurs durch die oft mit einer Radikalisierung verbundene Flucht in den Untergrund ermöglicht werden.

Ideengeschichtlich ist diese Auffassung vor allem beeinflußt von den Thesen *John Stuart Mills*. Dieser nennt in seiner Schrift *On Liberty*[1023] im wesentlichen drei Argumente, mit denen er belegt, warum jegliches staatliche Verbot von Meinungen schädlich ist und vielmehr die freie Diskussion von Meinungen zur Durchsetzung der Wahrheit führt. Erstens könne die Wahrheit nur dadurch gefunden werden, daß trotz jeder Freiheit sie zu bestreiten die Gegenargumente nicht überzeugen.[1024] Nur durch dauernde Offenheit für Gegenargumente könne sich eine gesicherte Überzeugung von der Wahrheit bilden.[1025] Zweitens, benötige gerade eine wahre Auffassung ständige Herausforderung durch und die intime Kenntnis von Gegenauffassungen. Andernfalls verkomme die Wahrheit zum bloßen Dogma, verliere ihre Überzeugungskraft[1026], wird reflexionslos geglaubt und habe letztlich keinen Bezug mehr mit dem „inneren Leben" des Menschen.[1027] Die Gegenargumente müßten aber von ihren Verfechtern selbst angebracht

1022 In gesellschaftlicher *self-governance* wird ein wesentlicher Geltungsgrund der Meinungsfreiheit gesehen, vgl. oben FN 34.

1023 *Mill, John Stuart*, On Liberty, abrufbar etwa unter http://coombs.anu.edu.au/Depts/RSSS/ Philosophy/Texts/MilllibertyTOC.html.

1024 *Mill, John Stuart*, a.a.O., Chapter 2: „There is the greatest difference between presuming an opinion to be true, because, with every opportunity for contesting it, it has not been refuted, and assuming its truth for the purpose of not permitting its refutation. Complete liberty of contradicting and disproving our opinion, is the very condition which justifies us in assuming its truth for purposes of action; ..."

1025 *Mill*, a.a.O.: „The beliefs which we have most warrant for, have no safeguard to rest on, but a standing invitation to the whole world to prove them unfounded."

1026 *Mill*, a.a.O.: „However unwillingly a person who has a strong opinion may admit the possibility that his opinion may be false, he ought to be moved by the consideration that however true it may be, if it is not fully, frequently, and fearlessly discussed, it will be held as a dead dogma, not a living truth."

1027 *Mill*, a.a.O.: „But when it has come to be an hereditary creed, and to be received passively, not actively-[...] there is a progressive tendency to forget all of the belief except the formularies, [...] , as if accepting it on trust dispensed with the necessity of realizing it in consciousness, or testing it by personal experience; until it almost ceases to connect itself at all with the inner life of the human being."

werden können.[1028] Würden diese unterdrückt, bildete sich, drittens, eine Wissenselite derer heraus, die dennoch Zugang dazu haben, während der Masse Erkenntnismöglichkeiten vorenthalten werden.[1029] Diese Argumente *Mills* sind in jüngerer Zeit unter dem Stichwort der „Diskursethik" wieder aufgenommen worden.[1030]

Sie gewinnen auch für das deutsche und europäische Recht der Kommunikationsinhaltskontrolle zunehmend an Sinn, je schwächer der Staat bei der Kontrolle digitaler Kommunikation wird: Die beschriebenen Konstellationen kollusiver Kommunikation rechtswidriger Inhalte können von kooperativer Inhaltskontrolle letztlich nur dadurch erreicht werden, daß Anbieter oder Nutzer von der Schädlichkeit dieser Inhalte überzeugt werden und daraufhin freiwillig das Angebot unterlassen oder zu den beschriebenen Schutzmaßnahmen greifen. Sind Inhaltsverbote nach *Mill* ohnehin einer Überzeugungsbildung eher abträglich, so verlieren ihre materiellen Wertentscheidungen auch die ihnen verbliebene generalpräventive[1031] Überzeugungskraft[1032], je weniger ihre Sanktionen angewendet und durchgesetzt werden können.

Länger bestehen bleibt dagegen die Suggestivwirkung vorhandener Normen auf die schädliche Inhalte ablehnende Mehrheit.[1033] Diese verharrt in der Annahme, der Staat werde schon dafür sorgen, daß mißbilligte Inhalte verhindert und ihre Anbieter bestraft

---

1028 *Mill,* a.a.O.: „Nor is it enough that he should hear the arguments of adversaries from his own teachers, presented as they state them, and accompanied by what they offer as refutations. [...] He must be able to hear them from persons who actually believe them; who defend them in earnest, and do their very utmost for them. He must know them in their most plausible and persuasive form; he must feel the whole force of the difficulty which the true view of the subject has to encounter and dispose of, else he will never really possess himself of the portion of truth which meets and removes that difficulty."

1029 *Mill,* a.a.O. (als Kritik an der katholischen Kirche): „This discipline recognizes a knowledge of the enemy's case as beneficial to the teachers, but finds means, consistent with this, of denying it to the rest of the world: thus giving to the elite more mental culture, though not more mental freedom, than it allows to the mass. By this device it succeeds in obtaining the kind of mental superiority which its purposes require; for though culture without freedom never made a large and liberal mind, it can make a clever nisi prius advocate of a cause."

1030 *Hellesnes, Jon,* Toleranz und Dissens – Diskurstheoretische Bemerkungen über Mill und Rorty, in: Apel, Karl-Otto / Kettner, Matthias, Zur Anwendung der Diskursethik in Politik, Recht und Wissenschaft, 1992, S. 187ff.

1031 Nach strafrechtlichem Verständnis handelt es sich um den „positiven" Aspekt der Generalprävention, unter dem gemeinhin die Erhaltung und Stärkung des Vertrauens in die Bestands- und Durchsetzungskraft der Rechtsordnung gesehen wird; Enttäuscht wird sowohl der ‚Vertrauenseffekt, der sich ergibt, wenn der Bürger sieht, daß das Recht sich durchsetzt', als auch der ‚Befriedungseffekt, der sich einstellt, wenn das allgemeine Rechtbewußtsein sich aufgrund der Sanktion über den Rechtsbruch beruhigt und den Konflikt mit dem Täter als erledigt ansieht', vgl. *Roxin, Claus* (FN 56), § 3 Rn. 26ff mwN.

1032 Zum Wert der materiellen Überzeugungskraft von Normen und den Gefahren eines Vertrauensverlustes in ihren materiellen Gehalt, der nur durch einen gesellschaftlichen Diskurs vermieden werden kann *Chambers, Simone,* Zur Politik des Diskurses: Riskieren wir unsere Rechte?, in: Apel, Karl-Otto/ Kettner, Matthias, Zur Anwendung der Diskursethik in Politik, Recht und Wissenschaft, S. 168 (179, 185).

1033 Diese Suggestivwirkung entsteht, wenn eine Wahrheit zur „ererbten Überzeugung", zum „Dogma" wird, vgl. *Mill,* a.a.O.

werden, ohne sich selbst zu eigener Überzeugungsarbeit veranlaßt zu sehen.[1034] So treffen immer mehr schädliche Inhalte auf eine Öffentlichkeit, die nicht darauf vorbereitet ist, sich einem Diskussionsprozeß über diese Inhalte stellen zu müssen. Dieser Diskussions- und Überzeugungsprozeß, der an die Stelle einer zunehmend unwirksamen gesetzlichen Sanktionsdrohung treten müßte, ist eine Form der gesellschaftlichen Selbstregulierung, die zu aktivieren ein wünschenswerter Beitrag des Staates zur kooperativen Inhaltskontrolle ist.

Ein solcher Beitrag kann in Einzelfällen – *Mill* folgend - darin bestehen, die zunehmend trügerische Suggestivwirkung von Inhaltskontrollvorschriften zu beenden, indem diese gelockert oder sogar ganz zurückgenommen werden. Dadurch würde der Konflikt um Meinungen aus dem Staat-Bürger-Verhältnis der Rechtsanwendung und -durchsetzung an die Oberfläche des gesellschaftlichen Meinungsbildungsprozesses inhaltlicher Auseinandersetzung gehoben. Statt die Not geschwächter Staatskontrolle zu verheimlichen, könnte die Tugend demokratischer Fähigkeiten der Bürgergesellschaft eingeübt werden. Auf diese ist der Bürger ohnehin in steigendem Maße angewiesen. Insbesondere bei digitalen Inhalten, die in Deutschland, nicht aber in anderen wichtigen Anbieterländern verboten sind, können in Zeiten vereinfachter grenzüberschreitender Kommunikation besondere Zuwächse erwartet werden. Ein im Zusammenhang mit dem Internet bereits kontrovers diskutiertes Beispiel sind die deutschen Strafvorschriften gegen nationalsozialistisches Gedankengut.[1035]

Fraglich ist, ob und wieweit eine auf die digitale Kommunikation nationalsozialistischen Inhalts oder Gedankenguts begrenzte Rücknahme strafrechtlicher Inhaltsverbote[1036] als staatlicher Beitrag zur kooperativen Kontrolle digitaler Kommunikationsinhalte verfassungsrechtlich zulässig wäre.[1037]

1034 Zu dieser Gefahr bei „symbolischer Gesetzgebung", *Roxin, Claus* (FN 56), § 2 Rn. 23.

1035 Spiegelbildlich wird in den USA eine Freigabe der dort besonders strikten Pornographieregelungen verlangt, vgl. *Meyer, Carlin,* 83 Geo. L.J. 1969 (1995).

1036 Zur ohnehin zweifelhaften Anwendbarkeit dieser Bindungen auf die Verbreitung digitaler Inhalte, vgl. oben *b. Strafrecht*, S. 73.

1037 Vgl. unten *b. Strafrecht*, S. 262.