5. Kapitel: Zwischenergebnis: Das „Dilemma“ staatlicher Kontrolle von digitalen Kommunikationsinhalten

Die bisherigen Ausführungen haben die Grenzen staatlicher Kontrolle von digitalen Kommunikationsinhalten deutlich werden lassen: Die bestehenden Regeln sind in wesentlichen Gebieten des Inhaltskontrollrechts auf neue digitale Kommunikationsformen und ihre Akteure nicht zu übertragen[891]. Die neuen Regelungen des TDG und des MDStV erlangen insgesamt nur geringe Bedeutung; nur ihre Haftungsbegrenzungen haben wichtigen klarstellenden Charakter. Das Aufkommen neuer digitaler Kommunikationsformen führt dazu, daß auch die staatliche Inhaltsregulierung des herkömmlichen Mediums Rundfunk zunehmend ihre verfassungsrechtliche Grundlage verliert[892]. Die nationalstaatliche Regulierung ist durch die vereinfachte und daher zunehmende Direktzuspielung von digitalen Inhalten vom und ins Ausland überfordert.[893] Zudem steht jede danach noch anwendbare Regel des herkömmlichen Inhaltskontrollrechts im Bezug auf digitale Kommunikationsinhalte vor erheblichen Durchsetzungshindernissen, die durch die Struktur digitaler Kommunikationsformen bedingt und der Rechtsanwendung daher neu sind.[894]

Zusammenfassend läßt sich sagen, daß die Erfolgsaussichten gesetzlicher Inhaltskontrolle und ihrer hoheitlichen Durchsetzung sich in bei der Kommunikation digitaler Inhalte auf Einzelfälle aus zwei Fallgruppen beschränken:

(1) Die Rechtswidrigkeit der kommunizierten digitalen Inhalte war dem handelnden *content provider* nicht positiv bekannt; deshalb hat er sie weder anonym noch verschlüsselt kommuniziert und war folglich ermittelbar.

> Beispiel: A ermöglicht auf seiner *homepage* über einen *hyperlink* zu B den *download* von dessen Software „TelcoExplorer“. M hat sich den Namen „Explorer“ als Marke schützen lassen. A glaubt nicht, daß eine Verwechselungsgefahr im Sinne von § 14 Abs. 2 Nr. 2 MarkenG besteht.[895]

(2) Dem handelnden *content* oder *host provider* war die Rechtswidrigkeit zwar bekannt, er hat dennoch auf wirksame Schutzmaßnahmen verzichtet.

> Beispiel 1: A sendet dem B eine beleidigende *e-mail* unter Angabe seines Namens.

---

891 Vgl. oben *1. Kapitel: Übertragbarkeit herkömmlicher Inhaltsregulierung auf die Kommunikation digitaler Inhalte*, S. 25.

892 Vgl. *2. Kapitel: Schwindende Berechtigung bisheriger Rundfunkregulierung*, S. 129.

893 Vgl. *3. Kapitel: Bedeutungsverlust nationaler Regulierung*, S. 147.

894 Vgl. *4. Kapitel: Fehlende Durchsetzbarkeit staatlicher Regulierung der Kommunikation digitaler Inhalte*, S. 162.

895 Verwechselungsgefahr ablehnend LG München I, Az. 9 HKO 850/99 vom 25.05.1999, http://www.afs-rechtsanwaelte.de/urteile64.htm, für „*FTP*-Explorer“ anders OLG München, Az.: 6 W 1563/99 v. 30.04.99 http://www.afs-rechtsanwaelte.de/urteile65.htm.

> Beispiel 2: Der *host provider* P weiß, daß auf seinen Speichern jede Menge wettbewerbswidriger „Last-Minute-Reise"-Angebote zum Abruf bereitgehalten werden. Er tut nichts.[896]

In anderen bekannt gewordenen Fälle wurden wesentliche Fragen nach hier vertretener Auffassung nicht richtig gewertet, so daß sich eine Anwendbarkeit gesetzlicher Inhaltsbindungen zu Unrecht ergab. So wurden Seiten im *WWW* und in *newsgroups* kommunizierte Bilder als „Schriften" im Sinne des § 11 Abs. 3 StGB angesehen[897], ein nach hier vertretener Meinung nicht verantwortlich zu machender Akteur herangezogen[898]. Bei Beachtung rechtstaatlicher Grenzen durch die Ermittlungsbehörden, sowie der hier vertretenen Auslegung von § 5 TDG und des nachfolgend zu prüfenden Sachrechts ergeben sich nur wenige Fälle, in denen gesetzliche Inhaltsbindungen gegenüber rechtswidriger Kommunikation digitaler Inhalte wirksam angewandt und durchgesetzt werden können.

Diese Beobachtungen sind jedoch noch unvollständig. Denn danach kann der Eindruck entstehen, die Regulierung sei in der bestehenden Form einfach nicht scharf genug, um in den neuen, digitalen Kommunikationsformen ähnlich geordnete und „saubere" Verhältnisse herzustellen wie in den herkömmlichen[899], die Schwierigkeiten könnten durch eine Verschärfung der Inhaltskontrolle überwunden werden.

Dabei wird jedoch die andere Seite des „Dilemmas"[900] außer Acht gelassen, in dem sich staatliche Inhaltsregulierung befindet: Ein schärferer Durchgriff des Staates um einer effektiven Inhaltskontrolle willen ist einem überforderten Recht keineswegs vorzuziehen, denn er kann kaum dosiert werden und führt zu unerwünschten Nebeneffekten. Einige denkbare Maßnahmen seien hier zusammenfassend in Erinnerung gerufen, wobei zu betonen ist, daß die meisten davon derzeit nicht geplant und teilweise gesetzlich explizit ausgeschlossen sind:

(1) Eine umfassende Verantwortlichkeit von *host* und *access providern*[901] bedeutete zwangsläufig eine Pflicht zur proaktiven Kontrolle der auf ihren Rechnern gespeicherten oder kommunizierten Inhalte durch die *provider*. Damit wäre aber dort jede vertrauliche Kommunikation unmöglich und viele Anwendungen digitaler Kommunikationsformen ausgeschlossen.

---

896 Im Fall des OLG München, vgl. FN 543, wurde der *host provider* trotz fehlender Kenntnis der Rechtswidrigkeit verurteilt.

897 Dazu oben *b. Strafrecht*, S. 73; nicht problematisiert von *AG Berlin-Tiergarten*, Urteil von 30.6.97 260 DS 857/96 – „*Marquardt-Radikal*", über http://www.akademie.de; aA AG München vom 28.05.98, MMR 1998, 429ff – *Somm*.

898 AG München, a.a.O.; *Cour d'Appel de Paris*, Arrêt du 10 février 1999 Estelle Halliday / Valentin Lacambre, http://www.legalis.net/legalnet/judiciaire/decisions/ca_100299.htm.

899 In diesem Sinne wollen einzelne Strafrichter und Staatsanwälte in Deutschland „schärfer durchgreifen", vgl. „*CompuServe*"-Urteil des AG München vom 28.05.98, mit Anm. *Sieber*; *Generalbundesanwalt beim BGH*, Einstellungsverfügung im Verfahren 2 BJs 104/96-4, MMR 1998, 93.

900 Vgl. *Ladeur*, ZUM 1997, 372 (376).

901 Entgegen § 5 TDG / MDStV, Art 12ff. des Vorschlags für eine europäische E-Commerce-Richtlinie, Richtlinien der EG zum elektronischen Handel (Vorschlag KOM(1998)586 endg. (FN 14)).

(2) Eine Lizensierung der Anbieter digitaler Inhalte[902] würde eine Beseitigung der technischen Zugangsoffenheit (Telefonanschluß) der digitalen Kommunikationsformen erfordern. Verfassungsrechtlich begegnete sie den gleichen Bedenken wie eine Zulassungspflicht für Presseanbieter, die von Art. 5 Abs. 1 GG ausgeschlossen ist.[903] Das zwangsläufig damit verbundene Verbot von Anonymität beim Angebot digitaler Inhalte birgt erhebliche Gefahren für das Recht auf informationelle Selbstbestimmung.[904]

(3) Könnte die gesamte Kommunikation digitaler Inhalte technisch durch eine zentrale Stelle auf Rechtswidriges untersucht werden, liefe dies auf eine von konkretem Verdacht auf rechtswidriges Handeln unabhängige Totalüberwachung der gesamten *on-line* Kommunikation hinaus[905]. Eine zwangsläufig damit verbundene einschränkende Reglementierung der Verschlüsselung digitaler Inhalte ist ein Eingriff in die Meinungsäußerungsfreiheit, dessen Verhältnismäßigkeit bezweifelt werden muß. Denn ein Verschlüsselungsverbot kann angesichts der technischen Gegebenheiten[906] den Zweck, die Verbreitung illegaler digitaler Inhalte zu verhindern, kaum fördern. Jede Einschränkung von Verschlüsselung führt wiederum zu einer Gefährdung sicherer Kommunikation.

(4) Die zwingende Einführung eines *Rating*-Systems zur Inhaltskontrolle führte wegen der Schwierigkeit, im Einzelfall rechtswidrige von rechtmäßigen Inhalten zu unterscheiden zu weithin unbestimmbaren Eingriffen in die Meinungsfreiheit der Anbieter. Die Ausfilterung unbedenklicher Inhalte könnte kaum verhindert, der Eingriff daher nicht auf das erforderliche Maß begrenzt werden.[907]

(5) Eine Überprüfung oder gar Kappung des digitalen Datenverkehrs mit dem Ausland zur Verhinderung der grenzüberschreitenden Kommunikation rechtswidriger Inhalte oder der rechtswidrigen Verwendung kommunizierter Inhalte und Daten im Ausland[908] ist nicht durchsetzbar.

---

902 Entgegen § 4 TDG / MDStV.

903 Art. 5 Abs. 1 GG gewährleistet die freie Gründung von Presseorganen, BVerfGE 20, 162, 175f.

904 Vgl. oben *c. Weitreichende Folgen der Verhinderung von Anonymität*, S. 193.

905 Vgl. *Simitis*, (FN 263), S. 285ff. Bedenklich ist bereits die Verpflichtung von *providern*, jederzeit nutzbare Abhörmöglichkeiten vorzuhalten, die jetzt auf europäischer Ebene nach dem sog. ENFOPOL-Papier realisiert wird, vgl. *aa. Vertraulichkeitsschutz in Strafverfolgung und Strafrecht*, S. 107, bei FN 475ff.

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

907 Vgl. oben *c. Verpflichtung der provider zur Verwendung eines Rating-Systems*, S. 181.

908 Die Bestimmung des Art. 25 der Europäischen Datenschutzrichtlinie, vgl. FN 160, sieht eine derartige Kappung für den Fall vor, daß im Zielland kein „angemessenes Schutzniveau" hinsichtlich der Verwendung der kommunizierten personenbezogenen Daten besteht. In Art. 26 sind zahlreiche Ausnahmen normiert. Datenübertragungen sind insbesondere immer zulässig, wenn der Betroffene „ohne jeden Zweifel" einwilligt. Die Durchsetzungsmängel der Vorschrift sind evident: Es besteht keinerlei realistische Möglichkeit, daß die mitgliedsstaatlichen Umsetzungsregeln etwa die Übermittlung persönlicher Daten via *e-mail* oder *WWW* durch die betroffenen EU-Bürger selbst in Einzelfällen wirksam verhindern können, in denen gerade keine Ausnahme des Art. 26 RL greift.

Theoretisch denkbare Verschärfungen staatlicher Inhaltskontrolle führen somit nicht nur an die Grenzen des technisch Möglichen, sondern – mitunter dadurch bedingt – auch des verfassungsrechtlich Zulässigen. Mit einem solchen Vorgehen kann auf die Veränderungen nicht in rechtstaatlicher Weise reagiert werden.

Ist deshalb eine staatliche Kontrolle digitaler Kommunikationsinhalte mit herkömmlichem Inhaltskontrollrecht *nicht effektiv*, mit einem verschärften Inhaltskontrollrecht herkömmlicher Prägung aber außerdem *nicht rechtsstaatlich* möglich, so kann für diesen Bereich staatlicher Aktivität wenn auch nicht unbedingt von einer „Ohnmacht“[909], so doch jedenfalls von einer Schwäche des Staates gesprochen werden. Er steht der Präsenz rechtswidriger Inhalte und der rechtswidrigen Verwendung kommunizierter Inhalte und Daten etwa im Internet zunehmend schwächer gegenüber, wenn er sich nur auf das traditionelle Instrumentarium hoheitlicher Inhaltsregulierung und ihrer Durchsetzung verläßt.

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