Landtag
Rheinland-Pfalz
Abteilung II
Wissenschaftlicher Dienst
und Parlamentsdienst

Mainz, 5.12.1996

Az.: II/52-1200

Gutachtliche Stellungnahme

Kinder- und Jugendschutz bei Online-Angeboten

A. Auftrag

Der Ausschuß für Kultur, Jugend und Familie hat in seiner Sitzung vom 24. September 1996 den Wissenschaftlichen Dienst um eine Ausarbeitung zu dem Thema Kinder- und Jugendschutz bei Online-Angeboten gebeten. Die Ausschußvorsitzende, Frau Abgeordnete Pepper konkretisierte den Auftrag wie folgt:

1. Welche rechtlichen Möglichkeiten gibt es zur Zeit, Kinder- und Jugendschutz bei Online-Angeboten durchzusetzen?
2. Welche Lücken bestehen, um Gewalt und Pornographie z.B. im Internet verhindern zu können?
3. Welche gesetzlichen Initiativen gibt es zur Zeit auf Bundes- und Länderebene, Kinder- und Jugendschutz im Bereich der neuen Medien zu verbessern?
4. Welche Initiativen werden auf europäischer Ebene verfolgt?

B. Einführung

Um die Weitergabe von pornographischen und gewaltverherrlichenden Informationen in Computernetzen rechtlich bewerten zu können, sind zunächt einige Erläuterungen zu den verschiedenen Online-Diensten sowie den damit zusammenhängenden speziellen Angeboten (vgl. I) notwendig. Außerdem ist maßgeblich, in welcher Funktion der jeweilige Anbieter innerhalb des Netzes tätig ist (vgl. II).

I. Online-Dienste

Der Begriff „online“ steht für die elektronische Verbindung eines Computers mit einem anderen oder einem Netzwerk von mehreren anderen Computern. Mittlerweile hat sich die Bezeichnung „Online-Dienste“ als Oberbegriff für die Datenfernübertragung durch Netzwerke durchgesetzt. Der aus einem Zusammenschluß von rund 43000 einzelnen Netzwerken in etwa 90 Ländern bestehende und mit rund 40 Millionen Teilnehmern größte Online-Dienst ist das **Internet**.[1] Andere Dienste sind zum Beipiel: T-online, MSN (Microsoft Network) und CompuServe. Im Hinblick auf die Fragestellung, die überragende Bedeutung des Internet und die zahlreichen unterschiedlichen rechtlichen Probleme der verschiedenen Dienste beziehen sich die folgenden Ausführungen nur auf das Internet.

Dabei handelt es sich um ein dezentral organisiertes Datennetz. Alle Informationen sind auf verschiedene Rechnern des Netzwerks verteilt, für das nur gewisse Koordinierungsfunktionen vorhanden sind. Lediglich die Übertragungsform der Daten ist einheitlich. Sie definiert das Internet als Verbund von Rechnern, die über das Netzwerkprotokoll TCP/IP[2] weltweit miteinander kommunizieren. Dieses Übertragunsprotokoll legt fest, wie ein einzelner Rechner im Netz erkannt und angesprochen wird und welche Wege (routes) die Daten von einem Rechner über verschiedene andere bis hin zum Zielrechner nehmen. Bei Ausfall verschiedener Netzabschnitte können die angeschlossenen Computersysteme selbständig alternative Datenverbindungen aufbauen. Wegen der fehlenden hierarchischen Struktur bestehen im Internet bis heute keinerlei Kontrollinstanzen, die gegenüber einzelnen Teilnehmern oder angeschlossenen Einzelnetzwerken ordnend eingreifen oder auch nur Anweisungen erteilen könnten. Allein die Vergabe von IP-Nummern und domain-Namen[3] wird durch übergeordnete Institutionen verwaltet.

Grundsätzlich eröffnet das Internet nur die Möglichkeit, andere Rechner im Internet ungeachtet ihres Aufstellungsortes anzusprechen.[4] Um sich auf diese Rechner einzuwählen oder Informationen von ihnen zu erlangen, bedarf es weiterer Vorrichtungen. Diese werden zumeist durch eine Software angesteuert und als **Internet-Dienste** bezeichnet. So-

---

1 Vgl. Die Welt vom 28. Februar 1996, S. 13. Aufgrund der dezentralen Struktur des Internet sind über die Teilnehmerzahlen allerdings immer nur grobe Schätzungen möglich.

2 TCP/IP steht für Transmission Control Protocol/Internet Protocol.

3 Anhand beider lassen sich die einzelnen Rechner im Internet eindeutig identifizieren.

4 Zum Internet erhält ein Nutzer dadurch Zugang, daß dieser über ein Modem[4] oder einen ISDN-Adapter[4] den Rechner eines Online-Anbieters anwählt. Dieser ist dann über Standleitungen mit den übrigen Rechnern eines Netzwerkes verbunden.[4]

weit es um den Datenaustausch per Internet oder im „Cyberspace“[5] geht, betrifft dies regelmäßig einen der im folgenden erläuterten Dienste.

Der **News-Dienst** hat den öffentlich zugänglichen Austausch von Nachrichten (news) zum Gegenstand. Die news stellen ein weltweites Diskussionsmedium bereit. Man kann es sich wie eine Vielzahl von elektrisch betriebenen schwarzen Brettern vorstellen. Zu jedem erdenklichen Thema exisitiert ein Diskussionsforum (newsgroup), in dem Beiträge zu einem vom Nutzer gewählten Thema ausgetauscht werden. Der News-Dienst bietet die Möglichkeit, öffentliche Nachrichten auf diesen „schwarzen Brettern“ zu lesen oder an sie zu senden. Aus technischer Sicht besteht ein news-Server aus einem im Internet erreichbaren Rechner, der alle im **Usenet**[6] ausgetauschten Nachrichten weiterleitet und eine ausgewählte Anzahl von News-Konferenzen selbst bereithält. Die von ihm angebotenen Nachrichten sind also dauerhaft gespeichert. Der Zugang zum News-Server kann jedem Nutzer des Internets oder nur ausgewählten Personen ermöglicht werden.

Ein weiterer Dienst sind die **Mailing Lists**. Sie enstehen aus einer zunächst privat per email[7] geführten Korrespondenz von Experten zu einem bestimmten Thema. Die einzelnen Themen werden anhand einer Liste, die mitunter mehrere 1000 Teilnehmer aufweisen kann, verschickt. Damit die Liste nicht zu stark ausufert, bieten einige Internet-Rechner das Abonnement einer Mailing-List an. Die Abonnenten können die einzelnen Beiträge lesen, ohne als individuell bezeichneter Teilnehmer hervorzutreten. Eine nicht öffentlich geführte Mailing List ist praktisch kaum zu kontrollieren.

Um nicht nur Texte, sondern auch Programme auszutauschen, wird im Internet zumeist auf das **file transfer protocol (ftp)** zurückgegriffen. Die sogenannten ftp-Server erlauben Nutzern die Einwahl auf dem Rechner, um dort Daten „herunterzuladen“ (sog. Download) als auch auf den ftp-Server „hochzuladen“ (sog. Upload). In der Regel sind die ftp-Server für jeden Nutzer des Internets anonym zugänglich. Vertrauliche Informationen oder schüt-

---

5 Die sich im Internet und den anderen Netzwerken auftuenden „virtuellen Welten“ werden häufig als „cyberspace“ bezeichnet, einem Kunstwort aus griechisch: kybernãn = steuern, leiten, regieren, und englisch: space = Raum.

6 Das Usenet ist ein Rechnerverbund, der sich nicht (wie das Internet) über die Übertragungsform der Daten, sondern den Inhalt der ausgetauschten Daten definiert: Er bezeichnet alle Rechner, die – oft nur zeitweilig miteinander verbunden – news austauschen. Die meisten zum Usenet gehörigen Rechner sind zugleich über das Internet miteinander verbunden.

7 Bei der electronic mail handelt es sich um die Übertragung von privaten Nachrichten in elektronischer Form.

zenswerte Daten sind jedoch nur für solche Nutzer erreichbar, denen der Betreiber einen Account[8] eingerichtet hat.

Der wohl bekannteste über Internet-Rechner erreichbare Dienst ist das **World Wide Web** (WWW)[9]. Er bezeichnet diejenigen Rechner, die Informationen über das hyper text transfer protocol (http) austauschen. Ein WWW-Server bietet zahlreiche Dokumente in der Seitenbeschreibungssprache HTML (HyperText Markup Language, kurz HTML) an. Ruft man diese mit einem speziellen Programm (dem sogenannten Browser) auf, stellt der Browser aus den enthaltenen HTML-Kommandos die grafisch aufbereiteten Informationen zusammen. Verweise auf bestimmte Fundorte lassen sich mit einem „Mausklick“ verfolgen. Auf diese Weise erfolgt die Weiterführung zu Informationen im WWW. Die einzelnen Dokumente im WWW stellen deshalb eine leicht bedienbare grafische Benutzeroberfläche dar und ermöglichen selbst Kindern das Auffinden von Informationen. Suchserver im WWW[10] halten überdies Abfragemechanismen bereit, mit denen sich das gesamte WWW nach Dokumenten zu einem bestimmten Thema absuchen läßt. Die von einem WWW-Server angebotenen Informationen bestehen aus Verweisen auf andere WWW-Server und lokal vorgehaltenen Informationen. Diese sind auf dem entsprechenden Server dauerhaft abgespeichert. Der Zugang zu einem WWW-Server ist zumeist öffentlich und anonym möglich, der Zugriff auf den gesamten Server oder einzelne Seiten kann aber auch einen Account erfordern.

II. Online-Provider

Bei den im Internet aktiven Personen lassen sich – im Hinblick auf die hier interessierende rechtliche Fragestellung – folgende Funktionen unterscheiden:

1. Der **Content-Provider** (Inhaltsanbieter) ist der Urheber der jeweiligen Information. Jedermann kann durch eine Beitrag in einer Newsgroup, auf einem ftp-Server oder durch eine eigene Web-Seite zum weltweiten Inhaltsanbieter werden.[11] Da die jeweilige Informati-

---

8 Individuell zu kontrollierende und abrechenbare Zugangsmöglichkeit, die zumeist durch Eingabe einer User-ID (dem Nutzer zugeordneter Name) sowie eines Passworts eröffnet wird.

9 Direkt übersetzt: weltweites Spinnennetz

10 Bekannt sind z.B. Yahoo und Altavista.

11 Beispielsweise erlaubt der Online-Dienst CompuServe jedem Mitglied, auf dem eigenen Web-Server nicht kommerziell ausgerichtete persönliche Web-Seiten pro Account bis zu einer Größe von 1 Megabyte abzulegen.

on von dem Content-Provider selbst stammt, ist er für mögliche strafbare Inhalte auch selbst verantwortlich.

2. Als (Mit-)Verantwortliche kommen darüber hinaus die **Service-Provider** (Dienste-anbieter) in Betracht, die ihren Teilnehmern eine Zugangsmöglichkeit zum Internet verschaffen.[12] Dabei kann es sich z.B. auch um Wirtschaftsunternehmen, Universitäten oder Schulen handeln. Im Hinblick auf die rechtliche Bewertung lassen sich verschiedene Tätigkeitsbereiche des Service-Providers unterscheiden. Sie werden im folgenden anhand der abnehmenden Einflußmöglichkeiten des Service-Providers auf die übertragenen Dateninhalte dargestellt:

- Vollen Einfluß hat der Service-Provider nur dann, wenn er auch als Content-Provider tätig wird. Dies ist lediglich in seltenen Konstellationen der Fall, z.B. wenn der Provider eigene Informationen im WWW zur Verfügung stellt.
- Begrenzten Einfluß auf den Dateninhalt hat der Service-Provider bei der Moderation (= Auswahl) fremder Daten. Dies ist insbesondere bei newsgroups und Mailing lists, die der Service-Provider selbst moderiert, sowie regelmäßig beim Betrieb eines ftp-Servers gegeben. In diesen Fällen sichtet der Service-Provider den Datenbestand und entscheidet, welche Daten er allgemein zugänglich machen will.
- Eine bloß formale technische Unterstützung bei der Verbreitung fremder Informationen übt der Service-Provider dagegen aus, wenn er seine Server für die Speicherung fremder Daten zur Verfügung stellt (sogenanntes „hosting“). Diese – für die meisten Service-Provider typische – Funktionstätigkeit erfolgt insbesondere beim Betrieb eines mail-Servers, beim Zugänglichmachen fremder newsgroups auf dem providereigenen news-Server und der Bereitstellung des eigenen list-Servers für fremde Mailing Lists.
- In vielen Fällen dient die Bereitstellung von Speicherplatz jedoch – ebenso wie die Bereitstellung von Leitungskapazitäten – nur dem technischen Transport von bereits gespeicherten Daten. Derartige Transportfunktionen erfüllen insbesondere Netzknotenrechner und Proxy-Cache-Server[13]. Die Einflußmöglichkeiten des Service-Providers auf die Daten sind in diesen Fällen gering.

---

[12] Vgl. Sieber, Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen, JZ 1996, S. 429, 433.

[13] Diese Computer erlauben eine Zwischenspeicherung von Web-Seiten, auf die von den Nutzern häufig zugegriffen wird. Ruft ein zweiter Nutzer dieselben Seiten ab, müssen sie nicht erneut von einem evtl. weit entfernten oder langsamen Rechner geholt werden.

- Ein weiterer – für alle Service-Provider zentraler – Tätigkeitsbereich ist die Bereitstellung des Zugangs zum Internet und seinen Diensten. Diese Funktion beinhaltet die technische Realisierung des Internet-Zugangs. Soweit ein Teilnehmer z.B. das WWW ohne Unterstützung eines Proxy-Cache-Servers nutzt, beschränkt sich die Funktion des Service-Providers auf das bloße Zurverfügungstellen des "Gateways"[14].

C. Stellungnahme

I. Frage 1

Bei den bestehenden rechtlichen Möglichkeiten des Kinder- und Jugendschutzes wird man zwischen präventivem (vgl. I 1) und repressivem Schutz (vgl. I 2) vor pornographischen und gewaltverherrlichenden Äußerungen in Computernetzen unterscheiden müssen.

1. Präventiver Schutz

a) Präventive Maßnahmen sind im Gesetz zum Schutze der Jugend in der Öffentlichkeit (JÖSchG) geregelt. Die obersten Landesbehörden prüfen Filme oder Bildträger, bevor diese der Öffentlichkeit zugänglich gemacht werden (vgl. §§ 6 und 7 JÖSchG). Ergebnis der Prüfung ist eine "Freigabeentscheidung", nach der ein Film beispielsweise ohne Altersbeschränkung oder erst ab 6 Jahren freigegeben ist. Der Veranstalter muß dann entsprechende Vorkehrungen zur Einhaltung dieses Gebotes treffen. Schutz der Kinder und Jugendlichen vor bedenklichen Informationen in Computernetzen bietet dieses Verfahren indes nur, wenn das JÖSchG auf derartige Fälle anwendbar ist. Aufschluß darüber geben die möglicherweise einschlägigen Tatbestände. So bezieht sich § 6 Abs. 1 JÖSchG auf Filme, die bei „öffentlichen Filmveranstaltungen“ gezeigt werden. § 7 Abs. 1 JÖSchG fordert die Vergleichbarkeit anderer "Bildträger" mit Videokassetten und Bildplatten. Daraus ergibt sich, daß nur ein kleiner Ausschnitt der auf Computernetzen enthaltenen Informationen vom JÖSchG erfaßt sein kann. In Bezug auf § 7 Abs. 1 JÖSchG handelt es sich etwa um Bilderfolgen und Videosequenzen, wie sie z.B. auf ftp-Servern oder WWW-Seiten bereitgehalten werden. Pornographische oder gewaltverherrlichende textliche Äußerungen

---

[14] Hierbei handelt es sich um ein Computersystem, welches den Zugang zum Internet und seinen Diensten ermöglicht. Allerdings ist ein Gateway nur erforderlich, wenn keine direkte Anbindung an das Internet besteht.

werden nicht erfaßt. Das gilt auch für das Bereithalten von Filmsequenzen in Computernetzen, da es sich dabei nicht um eine „öffentliche Filmveranstaltung“ i.S.d. § 6 Abs. 1 JÖSchG handelt.

b) Weitere Vorschriften zum präventiven Schutz von Kindern und Jugendlichen enthält das Gesetz über die Verbreitung jugendgefährdender Schriften (GjS). Es regelt ein Verfahren zur Prüfung der Frage, ob Schriften geeignet sind, Kinder oder Jugendliche sittlich zu gefährden. Die Bundesprüfstelle entscheidet auf Antrag im Wege einer Nachprüfung darüber, ob eine bereits im Verkehr befindliche Schrift in die Liste der jugendgefährdenden Schriften aufgenommen wird (vgl. §§ 1 Abs. 1 S. 1, 11 Abs. 1 GjS). Um in den hier maßgeblichen Fällen einen wirksamen Schutz von Kindern und Jugendlichen zu bieten, muß das GjS auf Computernetze anwendbar sein. Erforderlich ist, daß es sich bei den Abbildungen auf den Bildschirmen bzw. den Daten auf den Computern um "Schriften" i.S.d. § 1 Abs. 3 GjS handelt. Nach dieser Vorschrift stehen den Schriften Ton- und Bildträger, Abbildungen und andere Darstellungen gleich. Unter den Oberbegriff der Darstellungen fallen dabei Zeichen, die – auch unter Verwendung von Hilfsmitteln – sinnlich wahrnehmbar sind, einen gedanklichen Inhalt vermitteln und deren stoffliche Verkörperung von gewisser Dauer ist.[15] Bezüglich pornographischer oder gewaltverherrlichender Äußerungen im Internet ist das Vorhandensein einer dauerhaften Verkörperung problematisch. Die Anzeigen auf den Computerbildschirmen, die nach ihrem Sichtbarwerden ohne Spuren zu hinterlassen wieder verschwinden, reichen für die Bejahung einer dauerhaften Verkörperung nicht aus.[16] Anders hingegen ist die Speicherung der übertragenen Daten auf eigenen Datenträgern oder denen des Service Providers zu beurteilen.[17] Hier ist das Erfordernis einer dauerhaften Verkörperung zweifellos gegeben, sofern es sich nicht nur um flüchtige Speichervorgänge – z.B. bei einer transportbedingten Zwischenspeicherung auf einem Netzknotenrechner – handelt. Das GjS ist insoweit anwendbar[18] und kommt damit in Betracht, Kindern und Jugendlichen präventiven Schutz vor pornographischen und gewaltverherrlichenden Schriften zu bieten.[19]

---

15 Vgl. Scholz, Jugendschutz, München 1985, § 1 GjS Ziff. 9.

16 So Jäger/Collardin, Die Inhaltsverantwortlichkeit von Online-Diensten, CR 1994, S. 236, 237; Stange, Pornographie im Internet, CR 1996, S. 424, 426; Sieber, aaO., S. 494, 495; aA. Dreher/Tröndle, Strafgesetzbuch 47. Aufl., München 1995, § 11 Rn. 44.

17 Sieber, aaO., S. 494, 495; im Ergbnis auch: Stange, Pornographie im Internet, CR 1996, S. 424, 426.

18 So hatte die Bundesprüfstelle jüngst über die Indizierung von Web-Seiten zu entscheiden, nachdem das Familienministerium die Ächtung von acht Seiten des Deutschkanadiers Ernst Zündel, der den nationalsozialistischen Völkermord leugnet, beantragt hatte. Vgl. Möcke/Heinson, Ein Krampf, C't 1996, S. 118.

19 Anderer Ansicht Sieber, aaO., S. 494, 497 mit Verweis auf die Rechtsprechung des Bundesverwaltungsgerichts zu der Anwendbarkeit des GjS auf Fersehsendungen und Btx (BVerwGE, 85, 169, 174). Im

c) Präventive Maßnahmen bieten auch Überwachungsprogramme wie "Surf-Watch", "Net Nanny" oder "Cyber-Patrol". Dabei handelt es sich um Software-Lösungen, mit deren Hilfe ein Teilnehmer z.B. verhindern kann, daß seine Kinder bestimmte Newsgroups, Bild- oder Videodateien abrufen. Im Gegensatz zum JÖSchG und zum GjS werden hier also keine staatliche Stellen präventiv schützend tätig.

2. Repressiver Schutz

Die Antwort auf die Frage, welche repressiven Möglichkeiten es beim Kinder- und Jugendschutz gibt, hängt zunächst davon ab, welche Regelungen einschlägig sind (vgl. a) und ob sie als deutsches Recht auf die maßgeblichen Sachverhalte anwendbar sind (b). Weiterhin ist maßgeblich, inwieweit Content- und Service-Provider für mögliche Rechtsverstöße zur Verantwortung gezogen (c) und Sanktionen durchgesetz werden können (d).

a) Im Mittelpunkt der Sanktionsmöglichkeiten steht das Strafgesetzbuch (StGB). Die in Betracht kommenden Tatbestände finden sich in § 131 StGB[20] und § 184 StGB[21]. In § 131 StGB geht es um gewaltverherrlichende[22], in § 184 StGB um pornographische[23] Dar-

---

Ergebnis jedoch nicht überzeugend, da eine Beschränkung des Adressatenkreises auf Erwachsene durch den Service-Provider möglich sein dürfte.

[20] § 131 StGB lautet:
"Wer Schriften (§ 11 Abs. 3), die grausame oder sonst unmenschliche Gewalttätigkeiten gegen Menschen in einer Art schildern, die eine Verherrlichung oder Verharmlosung solcher Gewalttätigkeiten ausdrückt oder die das Grausame oder Unmenschliche des Vorgangs in einer die Menschenwürde verletzenden Weise darstellt,
1. verbreitet,
2. öffentlich ausstellt, anschlägt, vorführt oder sonst zugänglich macht,
3. einer Person unter achtzehn Jahren anbietet, überläßt oder zugänglich macht oder
4. herstellt, bezieht, liefert, vorrätig hält, anbietet, ankündigt, anpreist, einzuführen oder auszuführen unternimmt, um sie oder aus ihnen gewonnene Stücke im Sinne der Nummern 1 und 3 zu verwenden oder einem anderen eine solche Verwendung zu ermöglichen,
wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
(…)

[21] Diese Vorschrift lautet:
"Wer pornographische Schriften (§ 11 Abs. 3)
1. einer Person untern achtzehn Jahren anbietet, überläßt oder zugänglich macht
2. an einem Ort, der Personen unter achtzehn Jahren zugänglich ist oder von ihnen eingesehen werden kann, ausstellt, anschlägt, vorführt oder sonst zugänglich macht,
(…)
5. öffentlich an einem Ort, der Personen unter achtzehn Jahren zugänglich ist oder von ihnen eingesehen werden kann, oder durch Verbreiten von Schriften außerhalb des Geschäftsverkehrs mit dem einschlägigen Handel anbietet, ankündigt oder anpreist,
(…)
wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
(…)

[22] Gewaltverherrlichende Darstellungen sind gemäß § 131 StGB solche, die "grausame oder sonst unmenschliche Gewalttätigkeiten gegen Menschen in einer Art schildern, die eine Verherrlichung oder Ver-

stellungen. Für die zuletzt im Jahre 1974 überarbeiteten Vorschriften stellt sich die Frage, inwieweit sie überhaupt auf Computernetze anwendbar sind. Eine gefestigte Rechtsprechung liegt dazu nicht vor. Erste Ausführungen existieren in der Rechtslehre.[24] Außerdem beginnen sich die Parlamente z.B. durch Anhörungen mit dem Problembereich zu beschäftigen.[25] Dabei wird eine Vielzahl von Rechtsfragen deutlich. Sowohl § 131 StGB als auch § 184 StGB knüpfen an ein bestimmtes Tätigwerden durch "Schriften" an. Die in § 11 Abs. 3 StGB enthaltene Definition entspricht inhaltlich der von § 1 Abs. 1 GjS. Wie dazu festgestellt, ist der Schriftenbegriff nicht bei Anzeigen auf Computerbildschirmen und bei flüchtigen Speichervorgängen, sondern nur bei einer dauerhaften Verkörperung der Daten auf einem Speicher erfüllt.[26] Nach § 131 Abs. 1 Nr. 3, § 184 Abs. 1 Nr. 1 und 2, Abs. 3 StGB müssen die Schriften Kindern und Jugendlichen zugänglich gemacht werden. Das ist der Fall, wenn diese von den pornographischen oder gewaltverherrlichenden Inhalten Kenntnis nehmen können.[27] Entsprechende Möglichkeiten vermitteln Content-Provider, die ihre Inhalte ohne eine Schutzvorkehrung gegen den Abruf durch Kinder oder Jugendliche in Computernetzen anbieten. Das gleiche gilt für Service-Provider, die durch die Zugangsmögichkeit zum Internet auch die Möglichkeit der Kenntnisnahme von den angebotenen Inhalten vermitteln. Das Tatbestandsmerkmal des "Zugänglichmachens" ist insoweit erfüllt.[28] Vom Ansatz her sind die die Strafvorschriften §§ 131 und 184 StGB deshalb geeignet, Kindern und Jugendlichen repressiven Schutz vor pornographischen und gewaltverherrlichenden Inhalten zu bieten. Allerdings setzt der enge Schriftenbegriff der Anwendbarbeit der Vorschriften enge Grenzen, so daß zahlreiche Sachverhalte, für die eine Bestrafung wünschenswert wäre, nicht erfaßt werden. Weitere Einschränkungen einer wirksamen Strafverfolgung ergeben sich zudem daraus, daß die Service-Provider - wie noch ausgeführt wird[29] - für mögliche Rechtsverstöße regelmäßig nicht verantwortlich sind.

---

harmlosung solcher Gewalttätigkeiten ausdrückt oder die das Grausame oder Unmenschliche des Vorgangs in einer die Menschenwürde verletzenden Weise darstellt".

23 Pornographie läßt sich definieren als "grobe und direkte Darstellung des Sexuellen, die in einer den Sexualtrieb aufstachelnden oder die Geschlechtlichkeit in den Schmutz ziehenden oder lächerlich machenden Weise den Menschen zum bloßen (auswechselbaren) Objekt geschlechtlicher Begierde oder Betätigung jedweder Art degradiert“, vgl. OLG Düsseldort NJW 1974, 1474; Dreher/Tröndle, aaO., § 184 Rn. 7.

24 Vgl. z.B. Sieber, aaO., S. 494ff.

25 Vgl. gemeinsamen öffentlichen Anhörung des Ausschusses für Familie, Senioren, Frauen und Jugend und der Enquete-Kommission "Zukunft der Medien in Wirtschaft und Gesellschaft - Deutschlands Weg in die Informationsgesellschaft" vom 9. Oktober 1996.

26 Siehe S. 7.

27 Lenckner in: Schönke/Schröder, Kommentar zum Strafgesetzbuch, 24. Aufl. München 1991, § 184 Rn. 9.

28 Auch ein "öffentliches" Zugänglichmachen i.S.d. § 131 Abs. 1 Nr. 3 StGB liegt vor, wenn die Darstellung einem größeren, individuell nicht feststehenden oder jedenfalls durch persönliche Beziehungen nicht verbundenen Personenkreis zugänglich gemacht wird.

29 Vgl. S. 15.

Andere Sanktionsnormen finden sich im Gesetz zum Schutze der Jugend in der Öffentlichkeit (GjS) und im Gesetz über die Verbreitung jugendgefährdender Schriften (JÖSchG). Nach § 12 Abs. 1 Nr. 6 JÖSchG handelt ordnungswidrig, wer als Gewerbetreibender entgegen § 7 Abs. 1 JÖSchG[30] einem Kind oder einem Jugendlichen einen bespielten Bildträger, der nicht für seine Altersstufe freigegeben ist, zugänglich macht. Diese Voraussetzungen erfüllen die Content- und die Service-Provider, die mit den von ihnen angebotenen Diensten einen finanziellen Gewinn erzielen wollen und Kindern und Jugendlichen die Möglichkeit bieten, von strafbaren Inhalten im Computernetz Kenntnis zu nehmen[31]. Nach § 21 Abs. 1 Nr. 1 GjS wird mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft, wer von der Bundesprüfstelle verbotene Schriften einem Kind oder Jugendlichen zugänglich macht. Entsprechend dem zuvor Gesagten ist ein "Zugänglichmachen" jugendgefährdender Inhalte durch die Content- und die Service-Providerzu bejahen. Ihre Bestrafung gemäß § 12 Abs. 1 Nr. 6 JÖSchG bzw. § 21 Abs. 1 Nr. 1 GjS ist also möglich. Allerdings werden wegen der ggf. erforderlichen Gewerbsmäßigkeit des Handelns und des engen Schriftenbegriffs wiederum viele Fälle nicht erfaßt.

Weitere repressive Regelungen finden sich in speziellen medienrechtlichen Vorschriften: dem Rundfunkstaatsvertrag[32], dem Landespressegesetz Rheinland-Pfalz[33] und dem Bildschirmtext-Staatsvertrag[34].

Nach § 2 Rundfunk-Staatsvertrag (Rundf-StV) ist Rundfunk "die für die Allgemeinheit bestimmte (...) Verbreitung von Darbietungen aller Art in Wort, in Ton und in Bild unter Benutzung elektrischer Schwingungen ohne Verbindungsleitung oder längs oder mittels eines Leiters“. § 3 Rundf-StV erklärt gewaltverherrlichende, pornographische, Kinder schwer gefährdende oder die Menschenwürde verletzende Sendungen für unzulässig. Soweit Sendungen unzulässig sind, ist ihre vorsätzliche oder fahrlässige Verbreitung gemäß § 32 Rundf-StV ordnungswidrig. Wiederum stellt sich die Frage, ob der Rundf-StV auf Computernetze anwendbar ist. Grundsätzlich handelt es sich bei den gängigen On-

---

30 Siehe S. 6.

31 Vgl. Scholz, Jugendschutz, München 1985, § 7 JÖSchG, Ziff. 2.

32 Der Rundfunkstaatsvertrag v. 31. August 1991, GVBl. S. 369, 371 findet sich als Art. 1 im "Staatsvertrag über den Rundfunk im vereinten Deutschland" vom 10. Dezember 1991, GVBl. S. 369.

33 Gesetz vom 14. Juni 1965, GVBl. S. 107.

34 Der Bildschirmtext-Staatsvertrag findet sich als Art. 6 im "Staatsvertrag über den Rundfunk im vereinten Deutschland" v. 31. August 1991, GVBl. S. 369, 399.

line-Diensten nicht um Rundfunk.[35] Wie sich aus der in § 2 Rundf-StV enthalteten Definition ergibt, umfaßt der Rundfunkbegriff nämlich nur die simultane Verbreitung von Signalen und beruht nicht – wie praktische alle Online-Dienste – auf dem Abrufprinzip. Etwas anderes dürfte nur im Hinblick auf die jüngst in Mode kommenden Einspeisung ganzer Radioprogramme in das WWW gelten, die mittels Plug-Ins genannter Erweiterungen bestimmter Browser hörbar gemacht werden.

Das Landespressegesetz orientiert sich hinsichtlich seines Anwendungsbereichs am Begriff des "Druckwerks". Gemäß § 7 Abs. 1 PresseG sind Druckwerke im Sinne des Gesetzes "alle mittels eines zur Massenherstellung geeigneten Vervielfältigungsverfahrens hergestellten und zur Verbreitung bestimmten Schriften (...)". Erscheint ein so definiertes Druckwerk mit jugendgefährdendem Inhalt, ist unter bestimmten Voraussetzungen eine Bestrafung des Verantwortlichen möglich.[36] Obwohl sich des Pressegesetz deshalb grundsätzlich zur Durchsetzung von Kinder- und Jugenschutz eignet, scheitert seine Heranziehung in hier relevanten Fällen schon an den Tatbestandsvoraussetzungen des Druckwerks. Ein zur Massenherstellung geeignetes Vervielfältigungsverfahren liegt den in Computernetzen ausgetauschten Daten nämlich nicht zugrunde.[37]

§ 1 Btx-Staatsvertrag (Btx-StV) enthält eine Definition von Bildschirmtext[38], woraus sich ergibt, daß es sich dabei um ein geschlossenes, hierarchisches und textbasiertes System handelt. Auch wenn das Bereithalten gewaltverherrlichender oder pornographischer Angebote gemäß § 15 Abs. 1 Nr. 3 Btx-StV ordnungswidrig ist, kommt eine Bestrafung von Content- oder Service-Providern nach dieser Vorschrift nicht in Betracht, da die Voraussetzungen von Bildschirmtext beim Datenverkehr im Internet nicht erfüllt sind. [39]

Zusammenfassend läßt sich damit feststellen, daß sich gesetzliche Vorschriften zum Schutz von Kindern und Jugendlichen vor Pornographie und Gewalt in Computernetzen

---

35 Vgl. das Rechtsgutachten von Prof. Dr. Bullinger und Prof. Dr. Mestmäcker, abrufbar unter der URL http://www.iid.de/aktuelles.

36 Vgl. z.B. § 19 Abs. 2 PresseG R.-P., wonach der Redakteur mit Freiheitsstrafe bis zu einem Jahr bestraft werden kann, wenn er vorsätzlich oder fahrlässig seine Verpflichtung verletzt hat, Druckwerke von strafbarem Inhalt freizuhalten.

37 Im Ergebnis ebenso: Schaar, Datenschutzfreier Raum Internet?, CR 1996, S. 160, 175.

38 Danach ist "Bildschirmtext ein für jeden als Teilnehmer und als Anbieter zur inhaltlichen Nutzung bestimmtes Informations- und Kommunikationssystem, bei dem Informationen und andere Dienste für alle Teilnehmer oder Teilnehmergruppen (Angebote) und Einzelmitteilungen elektronisch zum Abruf gespeichert, unter Benutzung des öffentlichen Fernmeldenetzes und von Bildschirmtextvermittlungsstellen oder vergleichbaren technischen Vermittlungseinrichtungen individuell abgerufen und typischerweise auf dem Bildschirm sichtbar gemacht werden".

39 Vgl. Sieber aaO., S. 494, 498; Scholz, aaO., S. 8.

im StGB sowie im GjS und für bestimmte Dienste im JÖSchG, in Ausnahmefällen auch im Rundfunk-Staatsvertrag befinden. Allerdings ist der Wirkungskreis dieser Gesetze relativ eng, so daß viele gängige Angebote jugendgefährdender Inhalte nicht erfaßt werden.

b) Eine Verfolgung aufgrund der genannten Vorschriften setzt voraus, daß deutsches Recht im konkreten Fall überhaupt anwendbar ist. Probleme ergeben sich, wenn die betreffenden Informationen von einem im Ausland tätigen Provider nach Deutschland gelangen. So stellt sich die Frage der Strafbarkeit zum Beispiel dann, wenn ein deutscher Staatsangehöriger von den Niederlanden aus über das Internet für Kinder und Jugendliche zugänglich Pornographie anbietet und er sich damit am Ort der Handlung nicht strafbar macht.[40] Die Anwendbarkeit des deutschen Strafrechts[41] ergibt sich in derartigen Fällen aus § 3 i.V.m. § 9 StGB. Nach § 3 StGB gilt das deutsche Strafrecht für Taten, die im Inland begangen werden. Das ist dann der Fall, wenn der Täter im Inland gehandelt hat oder hätte handeln müssen bzw. wenn der zum Tatbestand gehörende Erfolg im Inland eingetreten ist (vgl. § 9 StGB). Daneben gilt das deutsche Strafrecht nach § 6 Nr. 6 StGB unabhängig vom Recht des Tatorts für die Verbreitung pornographischer Schriften aus dem Ausland in den Fällen des § 184 Abs. 3 StGB[42]. Hinsichtlich der Verfolgung von Ordnungswidrigkeiten nach dem JÖSchG und dem Rundf-StV enthalten die § 5 i.V.m. § 7 OWiG Regelungen, die mit denen der § 3 i.V.m. § 9 StGB entsprechen. Anknüpfungspunkt ist deshalb zum einen der Ort der Handlung und zum anderen der Ort des tatbestandlichen Erfolges.

c) Die oben dargestellten Tatbestände des StGB sowie des GjS, des JÖSchG und des Rundf-StV gelten im Internet zunächst für den Urheber strafbarer Äußerungen. Dabei handelt es sich um den **Content-Provider** (Inhaltsanbieter), der beispielsweise Datenbanken erstellt, einen Beitrag verfaßt oder als Verleger Teile seiner Zeitschriftenausgabe im Internet anbietet. Als Urheber der strafbaren Äußerung kennt er ihren Inhalt und speist

---

[40] So ist beispielsweise das Zugänglichmachen sog. "harter" Pornographie (Darstellungen, die den sexuellen Mißbrauch von Kindern oder sexuelle Handlungen von Menschen mit Tieren zum Gegenstand haben) in Deutschland einer erhöhten Strafdrohung unterworfen. In Schweden und den Niederlanden hingegen ist die Verbreitung derartiger Medien nicht verboten.

[41] Darunter ist die Gesamtheit aller Normen der Bundesrepublik Deutschland und ihrer Länder zu verstehen, soweit sie Voraussetzungen und Rechtsfolgen rechtswidriger Taten regeln, vgl. Dreher/Tröndle, aaO., vor § 3 Rn. 3.

[42] Diese Vorschrift betrifft die sogenannte "harte" Pornographie. Darunter sind solche Darstellungen zu verstehen, „die Gewalttätigkeiten, den sexuellen Mißbrauch von Kindern oder sexuelle Handlungen von Menschen mit Tieren zum Gegenstand haben, vgl. Dreher/Tröndle, aaO., § 184 Rn. 7.

sie wissentlich und willentlich in das Computernetz ein, so daß er insoweit vorsätzlich handelt. Auch ergeben sich aus der Informations- und Meinungsfreiheit des Art. 5 Abs. 1 S. 1 GG[43] keine Rechtfertigungsgründe, weil der Content-Provider mit seinen strafbaren Äußerungen gegen Jugendschutzbestimmungen verstößt (vgl. Art. 5 Abs. 2 GG[44]). Die Verfolgung des Content-Providers wegen des Verstoßes gegen §§ 131, 184 StGB sowie § 21 GjS und ggf. § 12 JÖSchG und § 32 Rundf-StV ist also möglich.

Der **Service-Provider**, der seinen Teilnehmern eine Zugangsmöglichkeit zum Internet verschafft, kommt als (Mit-) Verantwortlicher in Betracht. Anknüpfungspunkt für die Vorwerfbarkeit ist das Unterlassen von Kontrollmaßnahmen.[45] Insoweit kommt eine Strafbarkeit des Service-Providers nur in Betracht, wenn er eine "Garantenstellung" i.S.d. § 13 Abs. 1 StGB[46] inne hat.[47] Dazu müßte er zur Überwachung des Internet und zur Kontrolle der darüber zugänglichen jugendgefährdenden Schriften verpflichtet sein. Inwieweit das der Fall ist, hängt von den konkret angeboteten Diensten ab.[48] Letztlich ist eine Garantenpflicht des Service-Providers aber jedenfalls deshalb zu verneinen, weil er nicht für selbständiges Handeln dritter Personen verantwortlich gemacht werden kann.[49] Etwas anderes gilt nur für den Fall, daß sich der Service-Provider am Verhalten des – für die strafbare Informationsverbreitung primär verantwortlichen – Haupttäters beteiligt. Dies kann jedoch nur angenommen werden, wenn der Beitrag des Service-Providers ausdrücklich oder

---

43 Art. 5 Abs. 1 S. 1 lautet:
"Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten."

44 Art. 5 Abs. 2 GG lautet:
"Diese Rechte finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend ..."

45 Etwas anderes kann nur bei eigenmoderierten Newsgroups, selbst zusammengestellten Mailing Lists oder nach Prüfung übernommener Homepages einzelner Nutzer durch den Service-Provider gelten. Hier gelangen die Daten nämlich erst nach inhaltlicher Prüfung durch eine aktive Handlung an die Öffentlichkeit. Trifft der Service-Provider in diesen Fällen eine falsche Auswahlentscheidung, liegt der Vorwurf eines positiven Tuns nahe. Letztlich stellt sich jedoch auch hier - ähnlicn wie bei den Unterlassungsdelikten - die Frage nach dem „Zurechnungszusammenhang“.

46 Diese Vorschrift lautet:
"Wer es unterläßt, einen Erfolg abzuwenden, der zum Tatbestand eines Strafgesetzes gehört, ist nach diesem Gesetz nur dann strafbar, wenn er rechtlich dafür einzustehen hat, daß der Erfolg nicht eintritt, und wenn das Unterlassen der Verwirklichung des gesetzlichen Tatbestandes durch ein Tun entspricht."

47 Eine entsprechende Regelung für Ordnungswidrigkeiten enthält § 8 OWiG.

48 Während eine tatsächliche Einflußnahmemöglichkeit für solche Daten, die der Service-Provider nicht auf seinem Rechner gespeichert hat, wegen unüberschaubaren Vielzahl der täglich über das Internet ausgetauschten E-Mails und News-Beiträge nicht mögich ist, muß etwas anderes bei großen und öffentlich zugänglichen ftp-Servern gelten. Hier ist es nämlich beispielsweise möglich, daß Uploads erst nach Kontrolle und Freigabe durch den Service-Provider zum öffentlichen Download freigegeben werden.

49 So macht sich z.B. auch der Hauseigentümer nicht wegen Unterlassens strafbar, wenn er beleidigende Parolen an seinem Haus beläßt, die eine andere Person dort angebracht hat, vlg. auch Dreher/Tröndle, aaO., vor § 13 Rn. 17 a.

konkludent auf die Anstiftung[50] oder Beihilfe[51] zu einer Straftat gerichtet ist.[52] Das wird – schon wegen der erforderlichen vorsätzlichen Tatbeteiligung – in den allermeisten Fällen zu verneinen sein. Zusammenfassend ist demnach festzustellen, daß eine strafrechtliche Verfolgung des Service-Providers regelmäßig bereits wegen des Fehlens der erforderlichen Garantenstellung ausscheidet.

Selbst wenn es im Zuge einer Gesetzesänderung nicht mehr auf das Vorliegen der zuvor beschriebenen Garantenstellung ankäme, stünden der strafrechtlichen Verfolgung des Service-Provider nach der heutigen Rechtslage zahlreiche weitere Probleme entgegen, die im folgenden kurz angesprochen werden. So muß der Service-Provider die verlangte Handlung tatsächlich vornehmen können.[53] Sind bestimmte Kontroll- oder Selektionsmechanismen technisch unmöglich oder praktisch undurchführbar, kann ihr Unterlassen dem Service-Provider nicht vorgeworfen werden. Die bisher entwickelten Kontroll- oder Selektionsmechanismen haben den Zugriffs auf bestimmte Daten durch Kinder und Jugendliche nicht vollständig ausschließen können. Zwar kann der Provider in den Fällen, in denen Daten auf seinem eigenen Server gespeichert sind – etwa bei E-Mails oder News-Beiträgen – bestimmte Daten sperren oder löschen. Die für den Austausch von News üblichen Routingverfahren bewirken jedoch, daß die Daten auf anderen News-Servern gespeichert und abgerufen werden. Um dies zu verhindern, wäre ein Befehl an alle News-Server erforderlich, einen ausgetauschten Beitrag wieder zu löschen und diese Anordnung weiterzugeben. Ein solcher Befehl ist im Rahmen des den Austausch von News regelnden nntp (net news transport protocol) zwar vorgesehen, allerdings haben viele News-Server die Ausführung dieses Befehls deaktiviert. Selbst wenn ein Service-Provider die Weiterleitung strafbaren Materials verhindern will, kann ihm dies aufgrund der Verweigerungshaltung zahlreicher anderer Provider im Internet nicht gelingen. Insoweit ist eine effektive Weiterleitungskontrolle durch den Service-Provider bereits technisch nicht möglich.[54]

---

50 Nach § 26 StGB wird als Anstifter bestraft, "wer vorsätzlich einen anderen zu dessen vorsätzlich begangener rechtswidriger Tat bestimmt hat".

51 Wegen Behilfe wird nach § 27 Abs. 1 StGB bestraft, "wer vorsätzlich einem anderen zu dessen vorsätzlich begangener rechtswidriger Tat Hilfe geleistet hat".

52 Bei Ordnungswidrigkeiten gibt es eine derartigen Unterscheidung zwischen Täter und Teilnehmer nicht. Es gilt der Begriff des "Einheitstäters". Nach § 14 Abs. 1 OWiG handelt jeder, der sich an einer Ordnungswidrigkeit beteiligt, ordnungswidrig.

53 Vgl. Dreher/Tröndle, aaO., § 13 Rn. 14.

54 Daran ändern auch Überwachungsprogramme wie "Surf-Watch", "Net Nanny" oder "Cyber-Patrol" nichts. Hierbei handelt es sich um Software-Lösungen, mit deren Hilfe ein Teilnehmer z.B. verhindern kann, daß seine Kinder bestimmte Newsgroups, Bild- oder Videodateien abrufen. Eine solche "Kindersicherung" vor Ort setzt jedoch die aktive Mithilfe des erwachsenen Teilnehmers voraus und kann vom Provider nicht kontrolliert werden. Seit Anfang 1996 entwickelt die "Platform for Internet Content Selection" (PICS), ein

Aus den gerade genannten Gründen sind auch die Kausalität und der Zurechnungszusammenhang zu verneinen.[55] Wegen des Ausweichens auf eine andere Verbindungsstrecke und der Weigerung zahlreicher anderer Service-Provider, bestimmte News-Beiträge zu löschen, würde der Servide-Provider die Weiterleitung der problematischen Daten durch das Sperren der von ihm vermittelten Zugangsmöglichkeit zum Internet nicht verhindern.[56]

Auch in subjektiver Hinsicht ist dem Service-Provider regelmäßig kein Vorwurf zu machen. Er stellt meist nur Speicherplatz zur Verfügung oder vermittelt eine Zugangsmöglichkeit zum Internet. Dabei hat er auf die Daten, deren Übermittlung programmgesteuert und automatisiert erfolgt, keinen Einfluß. Er kennt weder diese noch deren Inhalt, so daß ihm - angesicht von 40 Millionen potentiellen Dateiverfassern - auch kein „billigendes Inkaufnehmen“ im Rahmen des Eventualvorsatzes vorzuwerfen ist. Etwas anderes gilt jedoch, wenn der Service-Provider eigene Informationen wissent- und willentlich zur Verfügung stellt und damit auch als Content-Provider handelt. In diesen Fällen ist direkter Vorsatz zu bejahen.[57] Das gilt auch für die Moderation fremder Daten (im Rahmen der Auswahl von newsgroups und ftp-Uploads), bei der der Service-Provider die jeweiligen Inhalte kennt und die entsprechenden Daten bewußt auswählt.

Zusammenfassend ist deshalb festzustellen, daß die Verfolgung des Service-Providers regelmäßig schon deshalb ausscheidet, weil er keine Garantenstellung inne hat, effektive Kontroll- und Selektionsmöglichkeit nicht bestehen und darüber hinaus Zurechnungszusammenhang und Vorsatz fehlen.

d) Das Problem der rechtlichen Durchsetzbarkeit der Sanktionsnormen stellt sich nur bei dem Content-Provider, da der Service-Provider für Gesetzesverstöße nicht verantwortlich ist. Durchsetzungsschwierigkeiten bestehen im Hinblick auf die unterschiedlichen internationalen Sanktionsnormen. Speist beispielsweise ein deutscher Content-Provider sog.

---

freiwilliger Zusammenschluß von Industrieunternehmen, jedoch Kontrollösungen, die nicht nur auf der Ebene des Netznutzers, sondern auch auf dem Server des Providers eingesetzt werden können. PICS muß sich in der Praxis jedoch noch bewähren.

55 Auf das schwierige dogmatische Problem, daß das gefährdete Rechtsgut vorliegend durch das Unterlassen mehrerer Personen bedroht wird, soll hier nicht weiter eingegangen werden, zumal dazu keine gefestigte Rechtsprechung vorliegt. Sieber, aaO., S. 494, 503 kommt über einen Vergleich mit der Rechtsfigur der alternativen Kausalität beim positiven Tun zu dem Ergebnis, daß letztlich schwierige Einzelfeststellungen getroffen werden müßten, um zu einer angemessenen Lösung zu gelangen.

56 Vgl. BGH NJW 1987, 2940; BGH JZ 1973, 173.

57 Siehe S. 13.

„harte“ Pornographie von den Niederlanden aus in das Computernetz ein und können die Inhalte in Deutschland zur Kenntnis genommen werden, hat er sich nach deutschem, nicht aber nach niederländischem Recht strafbar gemacht.[58] Hier scheidet die Verfolgung aus, da die deutschen Strafverfolgungsbehörden grundsätzlich nur auf deutschem Staatsgebiet tätig werden dürfen. Auch ein Auslieferungsersuchen nach dem Europäischen Auslieferungsübereinkommen (EuALÜbk)[59] hat wenig Aussicht auf Erfolg, weil nach Art. 2 EuALÜbk eine Auslieferung nur wegen solcher Handlungen erfolgt, die in beiden Staaten strafbar sind.[60]

II. Frage 2

Die Beantwortung des Frage, welche Lücken bestehen, um Gewalt und Pornographie im Internet verhindern zu können, erfordert die Differenzierung zwischen Content- und Service-Providern.

Die Strafbarkeit der **Service-Provider** scheitert - wie oben bereits dargelegt - an verschiedenen Voraussetzungen. Insoweit bestehen Lücken, um Gewalt und Pornographie im Internet verhindern zu können. Zu nennen ist das regelmäßige Fehlen der Garantenpflicht zur Überwachung der Daten in den Computernetzen. Darüber hinaus ist den Service-Providern die unterlassene Handlung wegen der besonderen Strukturen des Internet und des Verhaltens anderer Provider nicht zuzurechnen. Auch der Vorsatz ist regelmäßig zu verneinen. Wollte man die angesprochenen Lücken schließen, ist bei den zu erlassenden Normen jedoch zu beachten, daß unmögliche Handlungen nicht Gegenstand eines Normbefehls sein können.[61]

Die **Content-Provider** hingegen können sich nach dem Strafgesetzbuch und dem GjS strafbar machen sowie nach dem JÖSchG und dem Rundf-StV Ordnungswidrigkeiten begehen. Allerdings ist die Bestrafung bestimmter Handlungen wegen des relativ engen Schriftenbegriffs in § 11 Abs. 3 StGB nicht möglich, obwohl dies zum Jugendschutz erfor-

---

58 Vgl. S. 12.

59 Vom 13. Dezember 1957, BGBl. 1964 II 1369; 1976 II 1778.

60 Art. 2 Abs. 1 S. 1 EuAlÜbk hat folgenden Wortlaut:
„Ausgeliefert wird wegen Handlungen, die sowohl nach dem Recht des ersuchenden als auch nach dem des ersuchten Staates mit einer Freiheitsstrafe oder die Freiheit beschränkenden Maßregel der Sicherung und Besserung im Höchstmaß von mindestens einem Jahr oder mit einer schwereren Strafe bedroht sind.

61 Dreher/Tröndle, aaO., § 13 Rn. 14.

derlich wäre. So bleibt das Zugänglichmachen von pornographischen oder gewaltverherrlichenden Darstellungen mangels einer dauerhaften stofflichen Verkörperung straflos, wenn die betreffenden Darstellungen zwar auf dem Bildschirm betrachtet werden können, eine Speicherung jedoch nicht erfolgt. Zudem scheitert eine strafrechtliche Verfolgung häufig bei im Ausland begangenen Taten. Hier bestehen nach wie vor Mängel in der internationalen Zusammenarbeit sowie bei der Harmonisierung der unterschiedlichen nationalen Sanktionsnormen. So ist beispielsweise das Zugänglichmachen sog. "harter" Pornographie in Deutschland einer erhöhten Strafdrohung unterworfen. In Schweden und den Niederlanden hingegen ist die Verbreitung derartiger Medien nicht verboten.[62] Auch hinsichtlich der Definition von einfacher Pornografie bestehen beträchtliche Unterschiede zwischen den einzelnen Ländern Europas.[63]

Wegen der dezentralen Struktur des Internet, der weithin fehlenden Kontrollstrukturen und der technischen Möglichkeit, unter fremder Identität Beiträge einzuspeisen, ist es im übrigen schwierig, den tatsächlichen Urheber zu ermitteln und ihm den Gesetzesverstoß nachzuweisen.[64] Vor diesem Hintergrund ergibt sich ein weiteres Problem: die Jugendmedienschutzdienststellen der Landeskriminalämter verfügen nur vereinzelt über Internet-Zugänge. Insoweit gestaltet sich die Verfolgung schon aufgrund tatsächlicher Umstände als schwierig. Auch in rechtlicher Hinsicht bestehen Probleme, z.B. wenn sich ein Anbieter verdächtig gemacht hat. Die Strafverfolgungsbehörden haben gegenwärtig keine rechtlichen Möglichkeiten, zum Zwecke der Beweisführung auf den durch Verschlüsselungen gesicherten Datenbestand des verdächtigen Anbieters aus dem Netz zuzugreifen. Es gibt nämlich keine Rechtsgrundlage zur Beantragung eines Gerichtsbeschlusses, der die Überwachung einer Computeranlage des Beschuldigten anordnet.[65] Den Strafverfolgungsbehörden bleibt daher nur der Ausweg der klassischen Durchsuchung am Standort der Anlage und deren Beschlagnahme. Diese Maßnahme bleibt jedoch meist wirkungslos,

---

62 Siehe S. 16.

63 Vgl. dazu den Antrag der Staatskanzlei Rheinland-Pfalz vom 29. November 1996. Darin wird gebeten, in die geplante Stellungnahme des Bundesrates zu der Mittelung der Kommission der Europäischen Gemeinschaften an den Rat und das Europäische Parlament über schädliche und illegale Inhalte im Internet vom 16. Oktober 1996 folgendes aufzunehmen:
„Der Bundesrat hält es für erforderlich, Überlegungen anzustellen, durch einheitliche EG-Bestimmungen die Maßstäbe für den Kinder- und Jugendschutz im Bereich der neuen Dienste festzulegen“.

64 Vgl. Sieber, aaO., S. 429, 431; Stange, aaO., S. 424, 426.

65 Darauf verweist auch Gunter Hauch, Ltd. Kriminaldirektor in seiner schriftlichen Stellungnahme in der gemeinsamen öffentlichen Anhörung des Ausschusses für Familie, Senioren, Frauen und Jugend und der Enquete-Kommission "Zukunft der Medien in Wirtschaft und Gesellschaft - Deutschlands Weg in die Informationsgesellschaft" vom 9. Oktober 1996, unkorrigiertes Wortprotokoll, S. 182, 187.

da Daten schnell gelöscht, bestimmte Datenbestände unidentifizierbar verschlüsselt[66] sind oder der Computer so programmiert wird, daß sich bei unbefugter Inbetriebnahme der Festplattenspeicher automatisch formatiert.

Darüber hinaus scheitern die meisten Kontrollmaßnahmen an dem Routingverfahren des Internet und der Möglichkeit der verschlüsselten oder versteckten Datenübertragung. Ferner bedeutet eine flächendeckende Anwendung von Textfiltern bei E-Mail-Diensten einen unzumutbaren Aufwand. Sie könnte zudem durch Verschlüsselungssoftware leicht umgangen werden, außerdem würde sie Bild- und andere Binärdateien nicht erfassen. Auch bei einem extensiven Einsatz von Filtern im News-Dienst könnten strafbare Daten nur auf einzelnen Servern gesperrt werden und wären über andere Rechner weiter verfügbar. Gleiches gilt für den Bereich des WWW-Dienstes, bei dem die multimedialen Fähigkeiten des Dienstes und die schier unendliche Zahl der Web-Seiten Kontrollen zusätzlich erschweren.

Diese Probleme machen auch eine präventive Kontrolle nach den Vorschriften des JÖSchG schwierig: auf die Kommunikation im Internet angewandt, dürften Daten nicht ohne die Freigabe nach § 7 Abs. 1 und 2 S. 1 JÖSchG in Computernetze eingespeist werden. Angesichts der unüberschaubaren Datenmengen und des ständig wechselnden Datenbestandes erscheint es nahezu ausgeschlossen, daß die oberste Landesbehörde die beim Service-Provider vorhandenen Datenträger vor dem Zugänglichmachen im Netz überprüft.[67]

Aus den dargestellten Lücken resultiert zumindest faktisch der von vielen Netzbenutzern reklamierte "rechtsfreie Raum im Cyberspace". Diese Situation ist offensichtlich unbefriedigend. Aufgrund des "nullum crimen sine lege"-Grundsatzes von Art. 103 Abs. 2 GG[68] ist eine Abhilfe jedoch nicht durch die Rechtsprechung möglich. Erforderlich ist vielmehr eine Lösung durch den Gesetzgeber, die den speziellen technischen, rechtlichen und internationalen Herausforderungen des Internet Rechnung tragen muß.

---

66 Dem Problem der Verschlüsselung versucht eine Bonner Expertengruppe im Innenministerium im Rahmen eines „Kryptogesetzes“ zu begegnen.

67 Darauf verweist auch: Scholz, aaO., S. 8, 9.

68 Art. 103 Abs. 2 GG lautet:
"Eine Tat kann nur bestraft werden, wenn die Strafbarkeit gesetzlich bestimmt war, bevor die Tat begangen wurde."

III. Frage 3

Bei der Frage, welche gesetzlichen Initiativen es zur Zeit gibt, um Kinder und Jugendschutz im Bereich der neuen Medien zu verbessern, ist zwischen Bund- und Länderebene zu differenzieren. Auf beiden Ebenen gibt es entsprechende Aktivitäten. Jedoch bestand über die Gesetzgebungskompetenzen längere Zeit Streit. Es ging darum, ob der Bund mit dem neuen Bundesgesetz für Informations- und Kommunikationsdienste[69] (IuKDG, oft als Multimediagesetz bezeichnet) in die Rundfunkhoheit der Länder eingreift oder ausschließlich von seinem Recht zur Regelung der Wirtschaft Gebrauch macht. Mitte dieses Jahres verständigten sich Bund und Länder dann beim sog. Multimedia-Gipfel offenbar auf einen Kompromiß: Sowohl im neuen Multimediagesetz wie in einem entsprechenden Länderstaatsvertrag wird die Zugangsfreiheit für Multimedia-Dienste festgelegt. Der Bund ist zuständig für Bereiche wie Datendienste, insbesondere Online-Dienste und elektronische Post. Die Länder behalten ihre Zuständigkeiten in den Bereichen Pay-TV, Pay-per-view, und Video-on-demand, soweit es sich um Unterhaltungsangebote handelt. Die Länder pochen auf ihre im Grundgesetz verankerte Zuständigkeit für den Rundfunk. Sie werden deshalb einen Medienstaatsvertrag abschließen. Eine Kommission soll Gesetz und Vertrag aufeinander abstimmen.

1. Zum Informations- und Kommunikationsdienste-Gesetz lag Mitte September der zweite Referentenentwurf vor, der in Abstimmung mit Wirtschafts- und Verbraucherverbänden sowie der Gesellschaft für Informatik entstanden ist.[70] Zum Schutz der Jugend ist geplant, die **Verantwortlichkeit** der Diensteanbieter[71] danach zu unterscheiden, ob es sich um eigene oder fremde Programme handelt und welche Inhaltskenntnis der Provider hat (Art. 1 § 5 des Referentenentwurfs). Nach wie vor sind die Content-Provider für ihre Inhalte, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich. Sie können sich deshalb strafbar machen, ihrer Verfolgbarkeit stehen jedoch unverändert vor allem tatsächliche Hindernisse entgegen.[72] Die Service-Provider sind künftig für fremde Inhalte, die sie zur Nutzung bereithalten verantwortlich, wenn sie von diesen Inhalten Kenntnis

---

69 An der praktischen Wirksamkeit des Gesetzes werden bereits jetzt Zweifel laut. Die Süddeutsche Zeitung schreibt am 29. August 1996 zu kriminellen Darstellungen im Internet:" Mit Paragraphen wie in dem für 1997 geplanten Multimediagesetz läßt sich da wenig ausrichten – sie scheitern bereits an der ungeordneten elektronischen Struktur."

70 Das parlamentarische Verfahren dazu wird voraussichtlich im Sommer 1997 abgeschlossen sein.

71 Gemäß § 3 Nr. 1 des Referentenentwurfs sind "Diensteanbieter" natürliche oder juristische Personen oder Personenvereinigungen, die eigene oder fremde Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln.

72 Vgl. S. 17 ff.

haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern. Für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, sind sie nicht verantwortlich. Die geplanten Regelungen knüpfen damit an die verschiedenen Funktionen der Service-Provider an.[73] Darüber hinaus wird den bereits angesprochenen Problemen des tatsächlich Möglichen, der Kausalität, der Zumutbarkeit und des Vorsatzes Rechnung getragen.[74] Den tatsächlichen Schwierigkeiten der Strafverfolgung bei **anonym** arbeitenden Content- und Service-Providern soll die neue Regelung in Art. 1 § 6 des Referentenentwurfs begegnen. Danach haben Diensteanbieter für ihre geschäftsmäßigen Angebote Namen und Anschrift anzugeben. Die große Gruppe der privaten Einspeiser pornographischer und gewaltverherrlichender Inhalte kann jedoch nach wie vor aus dem Verborgenen heraus agieren.

Art. 4 und 6 des Referentenentwurfs enthalten weitere Änderungen, die den Schutz von Kindern und Jugendlichen verbessern sollen. So ist geplant, den **Schriftenbegriff** in GjS und StGB auf Datenspeicher auszuweiten (Art. 4 § 1 und Art. 6 § 2 des Referentenentwurfs[75]). Insoweit soll den oben genannten Bedenken, hinsichtlich des zu enge Schriftenbegriffs Rechnung getragen werden.[76] Bloße Bildschirmdarstellungen ohne eine Datenspeicherung dürften jedoch nach wie vor nicht erfaßt sein. Art. 6 § 4 des Referentenentwurfs sieht darüber hinaus eine Ausnahme von dem Verbot, indizierte Schriften zugänglich zu machen vor, wenn durch **technische Vorkehrungen** Vorsorge getroffen ist, daß das Angebot im Inland auf volljährige Nutzer beschränkt werden kann. Ob es sich bei den "technischen Vorkehrungen" um solche handelt, die der Anbieter selbst handhabt oder um solche, bei denen er auf die Mithilfe der Eltern angewiesen ist[77], wird nicht deutlich. In beiden Fällen ist ein wirksamer Jugendschutz eher zweifelhaft. Sind die Eltern verantwortlich, hängt der Erfolg von ihrem Verantwortungsbewußtsein ab. Trifft der Service-Provider technische Vorkehrungen, so ist ein wirksamer Jugendschutz nur bei Mitwirkung aller Service-Provider gewährleistet, da die indizierten Inhalte sonst auf anderen Servern gespeichert und abgerufen werden können.[78] Vor dem Hintergrund einer freiwilligen Selbstkontrolle schließlich sollen bei gewerbsmäßigen Anbietern von Informations- und Kommunikationsdiensten unter bestimmten Voraussetzungen **Jugendschutzbeauftragte** bestellt werden, die als interne Berater tätig werden (Art. 6 § 7 a des Referentenentwurfs). Diese

---

[73] Dazu vgl. S. 5.
[74] Siehe zu diesen Problemen die Ausführungen auf S. 13 ff.
[75] Im Internet unter der URL http://www.iid.de/aktuelles abrufbar.
[76] Vgl. S. 10.
[77] Dabei handelt es sich um Sofware-Programme wie "Surf-Watch", "Net Nanny" oder "Cyber-Patrol".

sind vom Anbieter bei der Angebotsplanung und der Gestaltung der Allgemeinen Nutzungsbedingungen zu beteiligen. Dabei können sie Beschränkungen bestimmter Angeboten vorschlagen und üben so eine gewisse Kontrollfunktion aus. Die geplante Regelung erfaßt allerdings wiederum nur die gewerbsmäßigen Anbieter.

2. Was den geplanten Medienstaatsvertrag anbelangt, so liegt dem Landtag noch kein Entwurf vor. Nach den ersten bekannt gewordenen Vorentwürfen sollen jedoch z.B. solche Angebote unzulässig sein, die pornographisch oder offensichtlich geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden (§ 7 Abs. 1 Nr. 3 und 4). Offenbar sollen Verstöße gegen dieses Verbot als Ordnungswidrigkeit geahndet werden. Über den Mediendienste-Staatsvertrag werden die Länder voraussichtlich im Dezember auf der Konferenz der Ministerpräsidenten in Bonn beraten.

IV. Frage 4

Im Hinblick darauf, welche Initiativen auf europäischer Ebene verfolgt werden, ist zunächst auf das am 16. Oktober 1996 von der Kommission verabschiedete Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in den audiovisuellen Diensten und den Informationsdiensten hinzuweisen. Es besteht aus drei Kapiteln. In Kapitel I werden die inhaltlichen Kategorien analysiert, die zu Problemen für Jugendschutz und Menschenwürde führen können. Kapitel II widmet sich der Analyse des bestehenden rechtlichen und konstitutionellen Rahmens. Die aktuelle Lage in der Europäischen Union mit Blick auf das Gemeinschaftsrecht und die Zusammenarbeit in den Bereichen Inneres und Justiz wird in Kapitel III des Grünbuchs untersucht. Insbesamt ist es Ziel, eine ausführliche Debatte über Lösungen einzuleiten, die die Entwicklung der Dienstleistungen im audiovisuellen Bereich und gleichzeitig den Schutz der Minderjährigen und die Achtung der Menschenwürde ermöglichen. In diesem Zusammenhang machte Kommissar Oreja deutlich, daß jetzt noch nicht gesagt werden könne, ob die Europäische Union gesetzliche Vorschriften brauche. Gegenwärtig komme es viel mehr darauf an, die Möglichkeiten zu einer Harmonisierung nationaler Gesetze zu überprüfen. Parallel müßten im Hinblick auf einen effektiven Kinder- und Jugendschutz die neuen technischen Kontrollmöglichkeiten analysiert werden.

---

[78] Siehe S. 14.

Ebenfalls am 16. Oktober 1996 verabschiedete die Kommission die Mitteilung "Schädliche und illegale Inhalte im Internet". Darin wurden folgende Schlußfolgerungen getroffen:

- Die Zusammenarbeit zwischen den EU-Staaten muß so ausgeweitet werden, daß die Durchsetzung schon bestehender Vorschriften möglich ist. Geprüft werden soll, welche rechtlichen Maßnahmen fehlen.
- Internet-Anbieter haben in einigen EU-Staaten bereits begonnen, ein System der Selbstkontrolle beim Zugang zu illegalem Material zu entwickeln. Dies soll überall geschehen.
- Filtersoftware und Systeme zur Blockierung des Zugangs zu bestimmten Mitteilungen, die es schon gibt, sollen weiterentwickelt und europaweit eingeführt werden. So kann ein Computerbesitzer sein Gerät so einstellen, daß es bestimmte Internet-Seiten nicht mehr empfangen kann.
- Es sollen nationale Sensibilisierungsmaßnahmen für Eltern und Lehrer geprüft werden.
- Die Bekämpfung illegaler Inhalte muß weltumspannend sein – wie die Funktionsweise des Internets. Deswegen seien internationale Übereinkünfte nötig. Internationale Organisationen wie die Vereinten Nationen sollen eingeschaltet werden.

Die Mitteilung der Europäischen Kommission liegt dem Bundesrat vor. Dem Vernehmen nach dort soll sie im Januar 1997 beraten werden.

D. Ergebnis

Es bestehen präventive und repressive Rechtsvorschriften, die dem Schutz von Kindern und Jugendlichen vor pornographischen und gewaltverherrlichenden Inhalten in Computernetzen dienen können. Diese Vorschriften stammen allerdings aus einer Zeit, als Online-Dienste keine oder wenig Bedeutung besaßen. Demgemäß wird nur ein kleiner Teil der computerrelevanten Vorgänge, deren strafrechtliche Ahndung wünschenswert wäre, erfaßt. Das gilt insbesondere für die repressiven Rechtsvorschriften, bei denen verschiedene Strafbarkeitsvoraussetzungen zu eng sind. Dazu gehört beispielsweise der Schriftenbegriff im StGB und im GjS. Um diese Defizite auszugleichen, sieht der Referentenentwurf zum Informations- und Kommunikationsdienste-Gesetz verschiedene Neuerungen vor. So soll der Schriftenbegriff auf Datenspeicher ausgeweitet werden, um einen größeren Anwendungsbereich bei Computernetzen zu erlangen. Insgesamt ist allerdings eher fraglich,

ob das geplante Gesetz Kindern und Jugendlichen ausreichenden Schutz vor Pornographie und Gewalt in Computernetzen bieten kann. Vor allem in zweierlei Hinsicht ergeben sich Bedenken. So bestehen die tatsächlichen Schwierigkeiten einer effektiven Strafverfolgung fort. Zu nennen sind beispielsweise die Anonymität des privaten Anbieters und die nach wie vor nicht mögliche Kontrolle aller Daten durch die Service-Provider. Hinzu kommt, daß in den verschiedenen Staaten der Europäischen Union unterschiedliche Strafbarkeitsbestimmungen bestehen und auch insoweit die Durchsetzbarkeit eines möglichen Rechtsverstoßes häufig scheitert.

Wissenschaftlicher Dienst