FREY Rechtsanwälte • Kaiser-Wilhelm-Ring 40 • 50672 Köln

Deutscher Bundestag
Ausschuss für Kultur und Medien
Herrn MdB Christoph Pries,
Vorsitzender des UA Neue Medien
Platz der Republik 1
11011 Berlin

Rechtsanwälte
Dr. Dieter Frey, LL.M. (Brügge)*
Dr. Matthias Rudolph

*Fachanwalt für Urheber- und Medienrecht

Dr. Dieter Frey
Tel. +49 (0) 221 / 420 748 00
Fax +49 (0) 221 / 420 748 29
dieter.frey@frey.tv

Aktenzeichen: (09)K627
(Bitte bei Schriftverkehr angeben)

Köln, den 10. Februar 2009

Sehr geehrter Herr Pries,

gerne nehme ich die Einladung des Unterausschusses Neue Medien zu der Anhörung über die rechtlichen und technischen Möglichkeiten sowie Grenzen von Sperrungsverfügungen von Internetzugängen an und stehe Ihnen als Sachverständiger zur Verfügung.

Mit dem vorliegenden Schreiben erlaube ich mir, die Antworten auf die von Ihnen übermittelten Fragen vorab zusammenzufassen. Dabei werde ich mich auf die aufgeworfenen rechtlichen Fragestellungen konzentrieren. Auf ausführliche Quellennachweise wurde verzichtet. Zudem möchte ich auf das gemeinsam mit meinem Kollegen Herrn Dr. Matthias Rudolph erstellte *Rechtsgutachten zu Evaluierung des Haftungsregimes für Host- und Access-Provider im Bereich der Telemedien* hinweisen. Das Rechtsgutachten, das wir im Auftrag des Bundesverbandes Digitale Wirtschaft (BVDW) e.V. erarbeitet haben, behandelt viele von Ihnen angesprochene Problemkomplexe in größerer Detailtiefe. Sehr gerne übermitteln wir das Rechtsgutachten den Mitgliedern des Unterausschusses Neue Medien per Email.

Bitte erlauben Sie mir aufgrund der umfassenden Beschäftigung mit dem jugendmedienschutzrechtlichen und dem zivilrechtlichen Haftungsregime für Access-Provider folgende Vorbemerkung:

FREY Rechtsanwälte
Kaiser-Wilhelm-Ring 40
50672 Köln
Tel. +49 (0) 221 / 420 748 00
Fax +49 (0) 221 / 420 748 29
Internet : www.frey.tv

Bankverbindung:
Deutsche Bank Köln, BLZ 37070024
Konto-Nr. 114421100
Raiba Rosbach e.G., BLZ 37069639
Konto-Nr. 6900819011
USt.-ID-Nr.: DE 207 139 511

A. Vorbemerkung

1. Die Bekämpfung der Kriminalität im Zusammenhang mit Kinderpornographie sollte höchste Priorität haben. § 184b StGB schafft dazu eine aus meiner Sicht ausreichende strafrechtliche Grundlage, indem nicht nur die Verbreitung, sondern auch der Erwerb und der Besitz kinderpornographischer Schriften unter Strafe gestellt werden. Im Hinblick auf konsumierende Täterkreise kann damit durch eine effektive und intensive Strafverfolgung im Inland eine zielgerichtete Bekämpfung kinderpornographischer Straftaten erreicht werden. Gleiches gilt auch für Anbieter kinderpornographischer Inhalte, die sich im Territorium der Bundesrepublik Deutschland befinden. Im Hinblick auf Auslandssachverhalte wird mit vielen Ländern eine Kooperation der Polizeibehörden gepflegt, wobei insbesondere im Rahmen der Europäischen Gemeinschaft auf eine enge Zusammenarbeit bei der Bekämpfung von Kinderpornographie zu verweisen ist (vgl. nur den *Rahmenbeschluss 2004/68/JI des Rates vom 22. Dezember 2003 zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie*, Amtsblatt der EU vom 20.01.2004, L13, S. 44 ff.). Aufgrund des EU-Rahmenbeschlusses wurde die Strafverfolgung im Hinblick auf Kinderpornographie in der Europäischen Union harmonisiert und gleichzeitig eine möglichst breite justizielle Zusammenarbeit angestrebt (vgl. Erwägungsgrund 7 des Rahmenbeschlusses). Das Europäische Parlament hat erst am 3. Februar 2009 eine *Empfehlung zur Überarbeitung des genannten Rahmenbeschlusses* angenommen. Die Bekämpfung von Kinderpornographie im Internet ist in den letzten Jahren intensiviert worden (vgl. dazu auch die *Europaratskonvention zum Schutz von Kindern vor sexueller Ausbeutung und sexuellen Missbrauch)*. Trotzdem ist eine weitere Verbesserung der technischen und personellen Ausstattung der Strafverfolgungsbehörden sinnvoll und angezeigt, um dem Übel kinderpornographischer Inhalte an der Quelle zu begegnen.

2. Auch nach den Bestimmungen des Jugendmedienschutz-Staatsvertrags (JMStV) sind kinderpornographische Angebote im Internet (vgl. insb. § 4 Abs. 1 Nr. 10 JMStV) verboten und sind von den zuständigen Landesmedienanstalten, die durch die Kommission für Jugendmedienschutz (KJM) als funktional zuständigem Organ handeln, zu unterbinden. Kinderpornographische Angebote sind zudem auf Antrag der KJM (§ 18 Abs. 6 JuSchG) von der Bundesprüfstelle für jugendgefährdende Medien (BPjM) zu indizieren und in die Listenteile mit jugendgefährdenden Medien aufzunehmen, die ein absolutes Verbreitungsverbot betreffen (Teile B und D). Wird ein Internetangebot (Telemedium) mit jugendgefährdenden Inhalten aus dem Ausland in die Liste aufgenommen, sollen diese Informationen zum Zwecke der Einbeziehung in nutzerautonome Filterprogramme zur Verfügung gestellt werden (vgl. § 24 Abs. 5 JuSchG). Durch die Verwendung entsprechender nutzerseitiger Filtersoftware können Eltern ihre Kinder vor jugendgefährdenden Inhalten aus dem Ausland schützen.

3. Trotz der vorstehend kurz skizzierten, umfangreichen Möglichkeiten der Strafverfolgung und des Jugendmedienschutzes bei kinderpornographischen Internetinhalten, können sich bei Auslandssachverhalten Probleme ergeben, die insbesondere den Opferschutz betreffen. Die Verfügbarkeit kinderpornographischen Materials im Internet verletzt in besonders schwerwiegender Art und Weise die Persönlichkeitsrechte der missbrauchten Kinder. Die Probleme des Opferschutzes, die im Zusammenhang mit den schwerwiegenden Rechtsverletzungen an den missbrauchten Kindern bestehen, rechtfertigen m.E. Überlegungen, Kinderpornographie nicht nur an der Quelle, d.h. bei den Anbietern und Konsumenten, zu bekämpfen, sondern an der Rechtsverletzung unbeteiligte Access-Provider zur Unterstützung heranzuziehen. Dabei ist jedoch zu berücksichtigten, dass eine „Sperrung" des Zugangs zu ausländische Webseiten heute technisch nicht möglich ist (vgl. zur technischen Wirksamkeit die Antwort zu Frage 7). Weder lassen sich durch solche Maßnahmen ausländische kinderpornographische Angebote aus dem Internet tilgen, noch eignen sich technische Manipulationen durch Access-Provider dazu, Straftäter aus Deutschland von ausländischen Angeboten wirksam abzuschneiden. Gerade mit krimineller Energie agierende Täter werden z.B. Verschlüsselungstechnologien oder Anonymisierungsdienste verwenden, um ihrer pädophilen Neigung nachzugehen. Zufallskontakte mit Kinderpornographie werden sich durch Zugangsbeschränkungen eher eindämmen lassen. Es ist jedoch zu befürchten, dass sich die Verschaffungs- und Besitzkriminalität in eine technische Grauzone verschiebt, die von den Strafverfolgungsbehörden nur schwer kontrolliert werden kann. Zugangsbeschränkungen dürfen jedoch keinesfalls dazu führen, dass die Effektivität der Strafverfolgung leidet, wenn das Problem der Kinderpornographie durch vermeintliche Netzsperren aus der öffentlichen Wahrnehmung gerät.

4. Zudem ist zu berücksichtigen, dass Überlegungen zu Netzsperren durch Access-Provider nicht nur im Zusammenhang mit Kinderpornographie angestellt werden. Gleiche Ansinnen werden aktuell auch vor dem Hintergrund des am 1. Januar 2008 in Kraft getretenen *Glücksspiel-Staatsvertrags* vorgetragen. Auch von Seiten des Bundeskriminalamts ist laut Presseberichten zu hören, dass Access-Provider *Webseiten mit terroristischem, rechtsradikalem und antisemitischem Hintergrund* sperren sollen. Sperrungsforderungen sind auch im Lichte des *Privatrechts* bereits gerichtlich geltend gemacht worden. Ein deutscher Anbieter von Pornographie wollte beispielsweise ein US-amerikanisches Angebot von Access-Providern mit der Begründung sperren lassen, dass Access-Provider eine *wettbewerbsrechtliche Verkehrspflicht verletzen*, falls über ihre Internetzugangsinfrastruktur pornographische Angebote aus dem Ausland ohne Altersverifikationssystem nach deutschem Recht zugänglich sind. Schließlich wird von Verwertungsgesellschaften und anderen Rechteinhabern der Musikindustrie gefordert, *Webseiten mit urheberrechtsverletzenden Inhalten* zu sperren. Vergleichbare Argumentationsstränge

zur Sperrung von Webseiten aus dem Ausland liegen auch im Hinblick auf *markenrechtsverletzende Angebote* sowie bei *schwerwiegenden Persönlichkeitsrechtsverletzungen* nahe.

5. Werden (freiwillige) Sperrungsmechanismen im Hinblick auf ausländische Angebote mit Kinderpornographie erwogen, kann dies m.E. nicht ohne Beachtung der rechtlichen Konsequenzen für die weiteren gerade angeführten Rechtsmaterien erfolgen. Bisher gelten die Internetzugangsdienste von Access-Providern als gesellschaftlich besonders erwünschte, inhaltsneutrale Infrastrukturleistungen, die grundsätzlich blind gegenüber einer rechtlich qualitativen Bewertung der durchgeleiteten Daten und Kommunikationsvorgänge sind. Dieser Befund, der bereits aus dem Geschäftsmodell der Access-Provider folgt, wird zudem gesetzlich besonders abgesichert. Access-Provider haben das Fernmeldegeheimnis gem. Art. 10 GG und einfachgesetzlich gemäß § 88 TKG zu wahren, wonach sowohl die Inhalte als auch die näheren Umstände der Internetkommunikation geschützt sind. Soweit Access-Provider im Zusammenhang mit Sperrungsmaßnahmen diese inhaltsneutrale Rolle aufgeben (müssen), ist die nach bisherigem Recht anzunehmende Nichtverantwortlichkeit für die durchgeleiteten Informationen zu hinterfragen. § 8 TMG, der eine weitgehende Haftungsprivilegierung von Access-Providern regelt, würde zwar weiterhin Geltung beanspruchen; allerdings wären Sperrungsforderungen von Behörden und Personen des Privatrechts neu zu bewerten, wenn Access-Provider Zugangsbeschränkungen im Hinblick auf Kinderpornographie vornehmen würden.

6. Es liegt die Befürchtung nahe, dass Access-Provider zu *Gatekeepern des Rechts* werden; sie würden in unterschiedlichen Konstellationen zur Rechtsdurchsetzung herangezogen. Verfassungsrechtlich stellen sich hier zentrale Fragen, insbesondere im Hinblick auf die verfassungsrechtlich verbürgten Grundrechte der Bürger und das Rechtsstaatsprinzip. Sollen Access-Provider als Personen des Privatrechts Aufgaben der staatlichen Rechtsdurchsetzung und Gefahrenabwehr übernehmen?

7. Als weitere Konsequenz der Umsetzung unterschiedlichster Sperrungsanforderungen könnte es – im Interesse der Wahrung deutscher Rechtstraditionen und kultureller Vorstellungen im Internet – zu einer Art „Renationalisierung" des heute faktisch weltweit bestehenden Kommunikationsraumes kommen. Eine solche Renationalisierung würde zu einem Paradigmenwechsel führen, der verfassungsrechtlich nicht ohne einen umfassenden demokratischen Willensbildungsprozess vorstellbar ist. Die aus dem verfassungsrechtlichen Rechtsstaats- und Demokratieprinzip von dem BVerfG in ständiger Rechtssprechung abgeleitete Wesentlichkeitstheorie verpflichtet den Gesetzgeber in grundlegenden normativen Bereichen, insbesondere im Bereich der Grundrechtsausübung, alle wesentlichen Entscheidungen selbst zu treffen. Ergebnis des demokratischen Willensbildungsprozesses muss dabei der Ausgleich der konfligierenden Grundrechte

sein. Soweit Zugangsbeschränkungen zum Internet erwogen werden, müssen also z.B. auch die grundrechtlich verbürgte Meinungs- und Informationsfreiheit der Bürger, die Presse-, Wissenschafts- und Kunstfreiheit sowie die Berufs- und Eigentumsfreiheit berücksichtigt werden. Schließlich ist ein Eingriff in das Telekommunikationsgeheimnis durch Zugangsbeschränkungen in die Erwägungen einzubeziehen und gesetzlich anzuordnen (Zitiergebot).

8. Die vorstehend angestellten grundsätzlichen Erwägungen sprechen m.E. gegen *freiwillige Beschränkungen* des Zugangs zu Kinderpornographie durch Access-Provider in Deutschland. Da es sich bei Kinderpornographie um besonders schwerwiegende Rechtsverletzungen handelt, ist aber insbesondere aus Gründen des Opferschutzes eine gesetzliche Sonderregelung denkbar, die als *ultima ratio* Kinderpornographie *nicht an der Quelle* bekämpft, *sondern* den *Internetzugang beschränkt*. Dies sollte jedoch nur aufgrund einer eindeutigen rechtlichen Grundlage geschehen, die den Ausgleich konfligierender Grundrechte und rechtsstaatliche Verfahren sicherstellt. Auch vor dem Hintergrund der bereits technisch virulenten Gefahr, dass neben dem Zugang zu rechtswidrigen Inhalten auch der Zugang zu rechtmäßigen Inhalten beschränkt werden kann, wodurch die grundrechtlich verbürgten Freiheiten unbeteiligter Dritter schwerwiegend berührt werden können, sollte die Kontrolle der Exekutive durch die Judikative sichergestellt sein.

B. Fragen zur Technik

9. Fragen zur Technik werden nicht unmittelbar beantwortet, sondern können nur im Rahmen unserer rechtlichen Expertise berücksichtigt werden. Ich verweise insofern auf die Antworten zu den Fragen 6 – 12.

C. Fragen zum Recht

Frage 6: Wie bewerten Sie die bestehenden Instrumente der Selbstregulierung in Deutschland und Europa?

10. Die Instrumente zur Selbstregulierung in Deutschland und Europa beurteile ich grundsätzlich positiv.

11. Die Selbstregulierung auf europäischer Ebene betrifft insbesondere die Alterskennzeichnung für Spiele. Es handelt sich um das von der Europäischen

Kommission auch finanziell unterstützte Altersklassifizierungs- und Alterseinstufungssystem PEGI (Pan-European Game Information) und PEGI-Online. Daneben kann auf den ebenfalls unter Mitwirkung der Europäischen Kommission von der Mobilfunkindustrie entwickelten *European Framework for Safer Mobile Use by Younger Teenagers and Children* verwiesen werden.

12. Der im Jahre 2003 in Kraft getretene JMStV hat für die Onlinesphäre erstmals in Deutschland das System der „regulierten Selbstregulierung" eingeführt. In diesem Zusammenhang ist in erster Linie die Freiwillige Selbstkontrolle Multimedia (FSM) zu nennen, die von der KJM im Jahre 2005 als Einrichtung der freiwilligen Selbstkontrolle anerkannt wurde und wertvolle Arbeit für den Jugendmedienschutz leistet. Schwachstellen im Hinblick auf Detailfragen habe ich mit meinem Kollegen Herrn Dr. Matthias Rudolph im Jahr 2007 im Rahmen eines Rechtsgutachtens zur Evaluierung des Jugendmedienschutz-Staatsvertrags untersucht. Die Einzelheiten unserer Analyse leite ich Ihnen auf Anfrage gerne zu.

13. Das System der „regulierten Selbstregulierung" in Deutschland betrifft vornehmlich Fragestellungen, die Inhalte und Angebote betreffen, welche von den Mitgliedsunternehmen von Selbstregulierungseinrichtungen rechtlich und tatsächlich kontrolliert werden können. Ein wichtiges Beispiel ist etwa die Alterskennzeichnung von Spielen und Filmen, welche von der Unterhaltungssoftware Selbstkontrolle (USK) und der Freiwilligen Selbstkontrolle der Filmwirtschaft (FSK) für Bildträger nach dem JuSchG vorgenommen wird und gem. § 12 JMStV auch für die Kennzeichnung in Onlinemedien übernommen werden muss. Bei den diskutierten Zugangsbeschränkungen durch Access-Provider mit Blick auf kinderpornographische Inhalte handelt es sich dagegen *nicht* um *Inhalte und Angebote*, die dem Zugriff und dem *Verantwortungsbereich der Access-Provider* unterliegen. Access-Provider können hier also keine rechtlichen und qualitativen Standards bezüglich eigener Angebote und Inhalte im Wege der Selbstregulierung umsetzen. Sie wären vielmehr zu Hilfsmaßnahmen bei der Durchsetzung des deutschen Rechts gegenüber rechtswidrigen Angeboten aus dem Ausland aufgerufen. Da keine unmittelbare Beziehung, weder faktischer noch rechtlicher Art, zwischen dem rechtswidrigen Auslandsangebot und den nationalen Access-Providern besteht, würden freiwillige Maßnahmen von Access-Providern im Rahmen der regulierten Selbstregulierung eine neue Qualität gewinnen. Access-Providern würde die Rolle eines Gatekeepers des Rechts zufallen, was im Lichte des verfassungsrechtlichen Rechtsstaatsprinzips kritisch zu untersuchen wäre. Auch wenn Selbstkontrolleinrichtungen für die ihnen angeschlossenen Access-Provider über die Rechtswidrigkeit von Inhalten Dritter im weltweiten Internet entscheiden würden, müsste die Frage nach einem effektiven Rechtsschutz gegen solche Entscheidungen geklärt werden.

14. Die Problematik illustriert anschaulich ein Beispiel, das die britische Internet Watch Foundation (IWF) betrifft: Aufgrund einer Entscheidung der IWF nahmen Access-Provider im Vereinigten Königreich Beschränkungen des Zugangs zu einem Artikel bei der Online-Enzyklopädie Wikipedia vor. Es handelte sich um einen Beitrag, der sich kritisch mit dem Original-Cover des bereits 1976 erschienen Albums „Virgin Killer" der Rockband „The Scorpions" befasst und ein nacktes, ungefähr 12 Jahre altes Mädchen zeigt. Der IWF entfernte die Webseite später wieder von seiner Blacklist, sodass die Zugangsbeschränkungen aufgehoben wurden. Eine rechtsstaatliche Kontrolle dieses Vorgangs fand offensichtlich nicht statt.

Frage 7: Wie bewerten Sie die unterschiedlichen technischen Möglichkeiten hinsichtlich ihrer Eingriffstiefe in Grundrechte, hinsichtlich ihrer Wirksamkeit und hinsichtlich ihrer Verhältnismäßigkeit?

15. An dieser Stelle möchte ich besonders auf das gemeinsam mit meinem Kollegen Herrn Dr. Rudolph erstellte Rechtsgutachten zur Evaluierung des Haftungsregimes für Host- und Access-Provider verweisen. Die nachfolgenden Ausführungen geben wesentliche Inhalte dieses Rechtsgutachtens zusammengefasst wieder. Die Ausführungen beziehen sich auf die geltende Rechtslage, die allgemein erörtert wird, ohne dabei auf die ggf. zu berücksichtigenden Besonderheiten kinderpornographischer Inhalte einzugehen.

16. Als denkbare Zugangsbeschränkungen werden in erster Linie drei technische Ansätze diskutiert: Zugangsbeschränkungen zu rechtswidrigen Informationen über in Routern gespeicherte IP-Adressen, Zugangsbeschränkungen zu rechtswidrigen Informationen über den Ausschluss von DNS-Namen in DNS-Servern sowie Zugangsbeschränkungen zu rechtswidrigen Informationen durch die Verwendung eines Zwangs-Proxy-Servers. Darüber hinaus werden hybride Sperransätze erwogen.

17. Zusammenfassend kann für alle technischen Ansätze der Zugangsbeschränkung zu Internetinhalten festgestellt werden, dass sie nur eine begrenzte Wirksamkeit entfalten: Alle Ansätze können durch Einstellungen, die der Nutzer selbständig vornehmen kann, umgangen werden. Diese technischen Ansätze dürften daher nur für technisch unversierte Nutzer den Zugang zu Inhalten im Internet beschränken. Generell können Zugangsbeschränkungen insbesondere die grundrechtlich verbürgte Meinungs- und Informationsfreiheit der Bürger, die Presse-, Wissenschafts- und Kunstfreiheit sowie die Berufs- und Eigentumsfreiheit betreffen. Schließlich ist bei allen diskutierten technischen Ansätzen das Telekommunikationsgeheimnis berührt.

18. Im Einzelnen ist Folgendes anzumerken:

I. Zugangsbeschränkungen zu rechtswidrigen Informationen über in Routern gespeicherte IP-Adressen

19. IP-Adressen nehmen eine zentrale Funktion im Internet ein, damit Informationen, die auf einem mit dem Internet verbundenen Server gespeichert sind, von einem anfragenden Rechner abgerufen werden können.

1. Bewertung der Wirksamkeit

20. In Netzknoten (Routern) sind in Routingtabellen die Informationen hinterlegt, auf welchem Weg welche Server im Internet erreichbar sind. Befindet sich in der Routingtabelle eines Knotens, der in die Übertragung eines IP-Paketes involviert ist, kein entsprechender Eintrag zu einem Server, ist er für diesen Knoten nicht erreichbar. Werden Router derart konfiguriert, dass der Datenverkehr zu bestimmten IP-Adressen nicht mehr weitergeleitet wird, lässt sich erreichen, dass die auf den entsprechenden Servern befindlichen Informationen von mit dem Internet verbundenen Rechnern nicht mehr abgerufen werden können.

21. Zwar lässt sich mit dem vorstehend beschriebenen Vorgehen herbeiführen, dass rechtswidrige Informationen auf bestimmten Servern im Internet nicht mehr erreichbar sind. Allerdings wird dabei regelmäßig nicht nur eine bestimmte Webseite erfasst, sondern es werden *in nicht unerheblichem Umfang auch völlig legale Informationen beeinträchtigt*. Die Manipulation der Router kann alle unter der betroffenen IP-Adresse angebotenen Dienste, also z.B. nicht nur den Datenverkehr über HTTP, sondern auch E-Mail-Dienste usw. berühren. Da das Verfahren des virtuellen Hostings weit verbreitet ist, lässt sich eine Manipulation der Router im vorstehend beschriebenen Sinn z.B. nur selten auf eine konkrete Webseite unter einem DNS-Namen begrenzen. Beim Einsatz des virtuellen Hosting-Verfahrens werden durch eine Manipulation der Router alle einer IP-Adresse zugeordneten DNS-Namen erfasst. Wie die Praxis in Bezug auf das pornographische Angebot Youporn zeigt, vermag eine Manipulation von Routern im Hinblick auf einzelne IP-Adressen zu einem erheblichen „Kollateralschaden" zu führen. Medienberichten zufolge konnten im Zuge der durch einen Access-Provider im vorstehenden Fall vorgenommenen „IP-Sperre" fast 3,5 Mio. Webseiten nicht mehr abgerufen werden.

22. Außerdem kann die IP-Adresse von dem Content-Provider leicht verändert werden. Nutzt ein Content-Provider beispielsweise für einen von ihm betriebenen Web-Server einen breitbandigen Internetanschluss mit hoher Upstream-Bandbreite, kann er die IP-Adresse seines Web-Servers mittels dynamischer IP-Adresse bekannt machen.

23. Nutzer könnten diesen technischen Ansatz z.B. durch den Einsatz von Anonymisierungsdiensten umgehen.

24. Eine Verhinderung des Zugangs zu rechtswidrigen Informationen können Manipulationen an Routern im Hinblick auf IP-Adressen folglich nicht bewirken; eine Sperrung im eigentlichen Sinne können sie daher nicht herbeiführen. Manipulationen an Routern im Hinblick auf IP-Adressen können allenfalls zu einer Erschwerung des Zugangs zu Informationen führen.

2. Bewertung der Verhältnismäßigkeit

25. Die Frage der Verhältnismäßigkeit hängt eng mit der nach der geltenden Rechtlage verlangten technischen Möglichkeit und Zumutbarkeit einer „Sperrung" (§ 20 Abs. 1 und Abs. 4 JMStV i.V.m. § 59 Abs. 4 RStV) zusammen.

a) Technische Möglichkeit einer „Sperrung"

26. Die erwogene technische Möglichkeit einer Sperrung muss geeignet sein, rechtswidrige Informationen isoliert zu sperren. Dabei ist auf den vorhandenen technischen Realitäten aufzusetzen, vor allem auf der bestehenden (Netz-) Infrastruktur. Eine Sperrungsverfügung darf eine Sperrung nur anordnen, die technisch möglich ist, nicht indes die Sperrung technisch erst ermöglichen.

27. Solange sich mittels der Manipulationen im Zusammenhang mit IP-Adressen der Zugang zu einer zu sperrenden rechtswidrigen Information isoliert beschränken lässt, wird man im Ergebnis eine solche Zugangsbeschränkung in *technischer Hinsicht* als möglich erachten. Etwas anders gilt jedoch, wenn es gleichzeitig zu der Beschränkung des Zugangs zu zahlreichen legalen Angeboten kommt. Wie das unter Randnummer 20 wiedergegebene Beispiel belegt, wird sich oftmals eine Zugangsbeschränkung mittels dieses technischen Ansatzes nicht auf die rechtsverletzenden Informationen beschränken lassen, sondern eine erhebliche Anzahl rechtmäßiger Informationen ebenfalls erfassen. In diesem Fall wird man die Manipulation an Routern im Hinblick auf IP-Adressen nicht als eine technisch mögliche Zugangsbeschränkung erachten können.

b) Zumutbarkeit der „Sperrung"

28. Sollte sich eine Zugangsbeschränkung mittels Manipulationen im Zusammenhang mit IP-Adressen noch als technisch möglich erweisen, stellt sich gleichwohl die Frage nach der Zumutbarkeit einer solchen Maßnahme.

29. Angesichts der bestehenden Umgehungsmöglichkeiten sowie der für den betroffenen Access-Provider entstehenden Belastungen ist dabei zunächst zu betrachten, ob der Aufwand für eine Sperrung außer Verhältnis zu der mit ihr erzielten moderaten Wirkung steht, wobei auf die Verhältnisse des jeweiligen Access-Providers abzustellen sein wird, für den die Maßnahme je nach Organisation seines Betriebes unterschiedlich belastend sein kann. Die Grenze der Zumutbarkeit dürfte jedenfalls überschritten sein, wenn ein Access-Provider zur Umsetzung einer Sperrungsverfügung Hard- und Softwarekomponenten erst erwerben, entsprechend Personal einstellen und gegebenenfalls die eigene Netztopologie ändern müsste. Der Eingriff in die Berufsfreiheit und das Eigentum von Access-Providern im Hinblick auf solche staatlich erzwungenen Investitionen wäre insbesondere einem „nicht störenden" Access-Provider unzumutbar. Sperrungsverfügungen stellen Eingriffe in die gem. Art. 12 GG geschützte Berufsfreiheit sowie in das gemäß Art. 14 GG geschützte Eigentum dar.

30. Gleichzeitig ist bei der Beurteilung der Zumutbarkeit die Meinungs-, Presse-, Informations-, Kunst- und Wissenschaftsfreiheit gem. Art. 5 GG zu berücksichtigen; Access-Providern kommt in unserer heutigen Gesellschaft nicht nur im Hinblick auf die Informationsbeschaffung der Bürger, sondern auch für ihre berufliche und wirtschaftliche Betätigung eine herausragende Rolle zu. Sollte eine Maßnahme auch legale Informationen und Angebote treffen, kann dies zu schwerwiegenden Eingriffen in die Grundrechte von unbeteiligten Dritten führen. Das Internet stellt einen beachtlichen Wirtschaftsfaktor dar. Nicht wenige Personen bestreiten heutzutage mittels des Internets ihren Lebensunterhalt z.B. durch den Betrieb von Online-Shops. Die Bewerbung und das Angebot von Waren und Dienstleistungen über das Internet sind für die Wirtschaft in einer zunehmend digital und konvergent geprägten Gesellschaft von größter Bedeutung. Erfassen „Sperren" legale Angebote, können diese in vielerlei Hinsicht sehr weitreichende wirtschaftliche Folgen nach sich ziehen. Gleiches gilt im Hinblick auf die Informationsbeschaffung und den Meinungsbildungsprozess als konstitutive Elemente unserer freiheitlich demokratischen Grundordnung. Auch eine global vernetzte Wissenschaft würde entsprechend tangiert. Darüber hinaus gilt es zu berücksichtigen, dass Zugangsbeschränkungen, die an die IP-Adresse anknüpfen, in das Telekommunikationsgeheimnis gem. Art. 10 Abs. 1 GG eingreifen.

31. Im Rahmen der Zumutbarkeit wird erschwerend zu berücksichtigen sein, wenn eine Vielzahl von Sperrungsverfügungen gleicher Art angeordnet wird. Bereits das OVG Münster führt im Hinblick auf die „Düsseldorfer Sperrungsverfügungen" hierzu wörtlich aus (Beschluss v. 19.03.2003, Az.: 8 B 2567/02):

> „Erst in künftigen Verfahren werden sich die Fragen stellen, ob die Praxis der Aufsichtsbehörden zu einer unzulässigen Umkehrung des „Regel/Ausnahmeverhältnisses" bzw. des Subsidiaritätsgrundsatzes des § 22 Abs. 2

> und 3 MDStV führt und welche Anforderungen im Einzelnen an die Zumutbarkeit einer Inanspruchnahme eines Access-Providers unter **Berücksichtigung ihrer „Gesamtbelastung"** zu stellen sein werden." [Hervorhebungen hinzugefügt]

32. Sollte es zu systematischen und anlassunabhängigen Kontrollen von Informationen nach deren Veröffentlichung im Internet kommen, dürfte sich eine beachtliche Gefahr für die Informations- und Meinungsäußerungsfreiheit realisieren, die durch ein Verbot der *Zensur* abgewendet werden soll. Nach gegenwärtigem Verständnis des Zensurverbots wird nur eine Vor-Zensur erfasst. Ein erweitertes Verständnis des verfassungsrechtlichen Zensurverbots erschiene bei systematischen und anlassunabhängigen Kontrollen der Internetkommunikation naheliegend.

II. Zugangsbeschränkungen zu rechtswidrigen Informationen über den Ausschluss von DNS-Namen in DNS-Servern

33. Das Domain Name System (DNS) dient in erster Linie dazu, durch die Anfrage bei einem DNS-Server für DNS-Namen – wie sie typischerweise in den URLs der Webseiten Verwendung finden – die dazugehörige numerische IP-Adresse zu ermitteln, um den gewünschten Server im Internet ansprechen zu können. Würde man Manipulationen im Hinblick auf die DNS-Einträge in DNS-Servern vornehmen, so ließe sich hierdurch erreichen, dass der Anfragende die einem DNS-Namen zugehörige IP-Adresse nicht bzw. nur eine fehlerhafte IP-Adresse erhält.

1. Bewertung der Wirksamkeit

34. Die Wirksamkeit solcher Manipulationen erscheint zweifelhaft. Kennt der Anfragende bereits die numerische IP-Adresse des zu kontaktierenden Servers, kann er mit dem entsprechenden Server durch unmittelbare Eingabe der IP-Adresse in seinem Browser in Verbindung treten. Es sei in diesem Zusammenhang angemerkt, dass es eine Reihe von Angeboten im World Wide Web gibt, die zur Auflösung von DNS-Namen, mithin zur Ermittlung von IP-Adressen, genutzt werden können. Darüber hinaus kann der Nutzer mit wenigen Schritten den „manipulierten" DNS-Server des Access-Providers auf einfache Weise umgehen, indem er einen anderen bzw. einen zusätzlichen DNS-Server nutzt. Eine DNS-Manipulation ist wirkungslos, wenn der Content-Provider bei der Umgehung dieser Manipulation „mithilft". So kann er seine rechtswidrigen Informationen jederzeit ohne große Schwierigkeiten unter einem neuen DNS-Namen im Internet zugänglich machen. Gleichzeitig erfolgen aber auch automatische Spiegelungen der Inhalte im Internet, so z.B. durch die Speicherung von Inhalten durch Suchmaschinen und Web-Archiven. Darüber hinaus kommt weiter erschwerend hinzu, dass die Inhalte nicht nur auf anderen Webseiten gespiegelt werden können, sondern auch in anderen Content-Verteil-Systemen, z.B. in P2P-Netzen, verfügbar sind.

2. Bewertung der Verhältnismäßigkeit

35. Wie bereits ausgeführt, hängt die Frage der Verhältnismäßigkeit eng mit der nach der geltenden Rechtlage verlangten technischen Möglichkeit und Zumutbarkeit einer Sperrung zusammen.

a) Technische Möglichkeit einer „Sperrung"

36. Auch diese erwogene technische Möglichkeit einer Sperrung muss geeignet sein, rechtswidrige Informationen unter den vorhandenen technischen Realitäten, insbesondere der bestehenden (Netz-)Infrastruktur, isoliert zu sperren. Zwar erweist sich eine Zugangsbeschränkung zu Informationen – auch insoweit ist eine vollständige Sperrung von rechtswidrigen Informationen nicht möglich – über den Ausschluss von DNS-Namen in DNS-Servern als nicht sehr effektiv, jedoch zumindest als technisch möglich.

b) Zumutbarkeit der „Sperrung"

37. Im Hinblick auf die Zumutbarkeit von DNS-Sperren kann auf die Ausführungen zu den Zugangsbeschränkungen zu rechtswidrigen Informationen mittels einer Manipulation im Hinblick auf IP-Adressen unter Randnummer 29ff. verwiesen werden.

38. Ergänzend sei erwähnt, dass m.E. – entgegen der von *Sieber/Nolde* vertretenen Ansicht (Sperrverfügungen im Internet, S. 85) – auch Manipulationen im Zusammenhang mit dem DNS das Telekommunikationsgeheimnis gem. Art. 10 Abs. 1 GG berühren. Der Schutzbereich des Telekommunikationsgeheimnisses erfasst die Kommunikation über und mittels der gesamten Netzinfrastruktur des Internets, unabhängig davon, welche Aufgabe und welche Funktion einzelne Bestandteile der Netzinfrastruktur ausfüllen. Daher ist m.E. sowohl die Kommunikation mit Web-Servern als auch mit DNS-Servern vom Schutz des Telekommunikationsgeheimnisses eingeschlossen. Die Manipulation des DNS-Servers hat zum Ergebnis, dass die mit der URL korrespondierende IP-Adresse nicht an den Anfragenden zurück übermittelt wird. Vielmehr übergibt er nach Auswertung der DNS-Anfrage eine IP-Adresse, die zu einem anderen Web-Server als dem angefragten führt. Die Manipulation von DNS-Einträgen in DNS-Servern greift insoweit in einen laufenden Kommunikationsvorgang ein, der durch das Telekommunikationsgeheimnis geschützt ist. Eine möglicherweise nicht unter das Telekommunikationsgeheimnis fallende Verhinderung des Kommunikationsvorgangs in Gänze erfolgt dadurch nicht. Vielmehr wird eine weiterhin

mögliche und bereits initiierte Kommunikation durch die Manipulation verfälscht und umgeleitet.

III. Zugangsbeschränkungen zu rechtswidrigen Informationen durch die Verwendung eines Zwangs-Proxy-Servers

39. Als weitere Möglichkeit der Sperrung von rechtswidrigen Informationen wird die Verwendung eines Zwangs-Proxy-Servers diskutiert.

1. Bewertung der Wirksamkeit

40. Technisch ist es denkbar, dass ein Access-Provider den Datenverkehr des Nutzers automatisch – gleichsam „zwangsweise" – über einen Proxy-Server leitet. Durch die Festlegung von Filterregeln auf dem Zwangs-Proxy-Server kann der Access-Provider bestimmen, welche URLs nicht erreichbar sein sollen. Mittels der URL lassen sich durch die Verwendung eines Zwangs-Proxy-Servers rechtswidrige Informationen, die für die Nutzer im Internet nicht mehr erreichbar sein sollen, festlegen.

41. Allerdings lässt sich ein Zwangs-Proxy-Server ähnlich leicht umgehen, wie eine Zugangsbeschränkung mittels einer Manipulation an DNS-Servern. Der Content-Provider kann die Filterung umgehen, indem er für den Server, auf dem seine Inhalte gespeichert sind, eine andere IP-Adresse bzw. einen anderen DNS-Namen verwendet. Außerdem kann der Nutzer selbst einen Proxy verwenden – z.B. einen Anonymisierungsdienst. Je nach Art des verwendeten Proxy lässt sich das verwendete Protokoll nicht dem Web-Traffic zuordnen und daher nicht von dem Zwangs-Proxy-Server analysieren; die Übertragung findet gleichsam an dem Zwangs-Proxy-Server vorbei statt. Auch verschlüsselte Daten kann der Zwangs-Proxy-Server nicht sinnvoll analysieren, da sowohl Inhalt als auch Adressinformationen verschlüsselt übertragen werden.

2. Bewertung der Verhältnismäßigkeit

42. Auch insoweit hängt die Frage der Verhältnismäßigkeit eng mit der nach der geltenden Rechtlage verlangten technischen Möglichkeit und Zumutbarkeit einer Sperrung zusammen.

a) Technische Möglichkeit einer „Sperrung"

43. Wie die bereits erwähnten technischen Sperransätze, muss auch dieser erwogene technische Sperransatz rechtswidrige Informationen unter den vorhandenen

technischen Realitäten, insbesondere der bestehenden (Netz-)Infrastruktur, isoliert sperren können. Eine vollständige Sperrung von rechtswidrigen Informationen ist auch hierdurch nicht möglich. Zwar erweist sich eine Zugangsbeschränkung zu Informationen mittels des Einsatzes eines Zwangs-Proxy-Servers als technisch möglich, aber auch als umgehbar.

b) Zumutbarkeit der „Sperrung"

44. Im Hinblick auf die Zumutbarkeit kann auf die Ausführungen zu den Zugangsbeschränkungen zu rechtswidrigen Informationen mittels einer Manipulation im Hinblick auf IP-Adressen unter Randnummer 29ff. verwiesen werden.

IV. Zugangsbeschränkungen zu rechtswidrigen Informationen durch hybride Sperransätze

45. Als weitere Möglichkeit der Sperrung von rechtswidrigen Informationen werden außerdem hybride Filtersysteme diskutiert, wie das in Großbritannien verwendeten „CleanFeed"-System.

1. Bewertung der Wirksamkeit

46. British Telecom (BT), einer der größten Access-Provider in Großbritannien, nahm im Juni 2004 ein System zum Sperren von Web-Inhalten in Betrieb, das als „CleanFeed" bezeichnet wird. CleanFeed implementiert einen zweistufigen Entscheidungsprozess: Zunächst wird mittels der Ziel-IP-Adresse einer Verbindung überprüft, ob diese Verbindung potentiell zu einer in einer Datenbank gespeicherten URL (Blacklist) gehören kann. Dazu werden mit Hilfe des DNS die IP-Adressen aller in den URLs enthaltenen Domainnamen ermittelt. Gehört eine Verbindung zu den „verdächtigen" Verbindungen, wird sie nicht sofort geblockt, sondern über Web-Proxies umgeleitet. Diese Web-Proxies untersuchen nun die innerhalb der Verbindung abgerufenen URLs auf Übereinstimmung mit der Blacklist. Erst wenn es hier zu einem Treffer kommt, wird die Verbindung tatsächlich gesperrt.

47. Allerdings lässt sich das System durch die üblichen Umgehungsmaßnahmen, z.B. durch den Einsatz von Proxys und Tunnels, umgehen. Im Ergebnis erweist sich eine Zugangsbeschränkung zu Inhalten – auch insoweit ist eine vollständige Sperrung von rechtswidrigen Inhalten nicht möglich – über den Einsatz hybrider Systeme zwar als technisch möglich, aber ebenfalls als umgehbar.

2. Bewertung der Verhältnismäßigkeit

48. Wie bereits ausgeführt, hängt die Frage der Verhältnismäßigkeit eng mit der nach der geltenden Rechtlage verlangten technischen Möglichkeit und Zumutbarkeit einer Sperrung zusammen.

a) Technische Möglichkeit einer „Sperrung"

49. Auch dieser erwogene technische Sperransatz muss geeignet sein, rechtswidrige Informationen unter den vorhandenen technischen Realitäten, insbesondere der bestehenden (Netz-)Infrastruktur, isoliert zu sperren. Eine vollständige Sperrung von rechtswidrigen Informationen lässt sich mittels dieses technischen Ansatzes nicht herbeiführen. Eine Zugangsbeschränkung zu Informationen über den Einsatz eines Zwangs-Proxy-Servers ist hierdurch zwar technisch möglich, nicht aber unumgehbar.

b) Bewertung der Zumutbarkeit der „Sperrung"

50. Im Hinblick auf die Zumutbarkeit kann auf die Ausführungen zu den Zugangsbeschränkungen zu rechtswidrigen Informationen mittels einer Manipulation im Hinblick auf IP-Adressen unter Randnummer 29ff. verwiesen werden.

Frage 8: Auf welcher rechtlichen Grundlage und durch wen könnten welche Inhalte und mit welchen Mitteln gegen einen Zugriff von Endnutzern gesperrt werden?

51. Im Bereich des Jugendmedienschutzes sind Sperrungsverfügungen der Landesmedienanstalten, die durch die KJM entscheiden, denkbar: Rechtliche Grundlage für entsprechende jugendmedienschutzrechtliche Verfügungen gegen Access-Provider bilden § 20 Abs. 1 und Abs. 4 JMStV mit seinen Verweisen auf §§ 7 – 10 TMG sowie auf § 59 Abs. 2 – 4 RStV. Es handelt sich dabei um eine komplexe Verweiskette, die im Einzelnen erhebliche Auslegungsschwierigkeiten bereitet. Im Ergebnis dürfen Access-Provider aufgrund eines Systems abgestufter Verantwortlichkeiten im Bereich des Jugendmedienschutzes erst in Anspruch genommen werden, wenn ein Vorgehen gegen Content- und Host-Provider wegen eines rechtswidrigen Inhalts ausscheidet. Zudem ist es ausgeschlossen Access-Providern allgemeine Überwachungs- und Nachforschungspflichten aufzugeben. Insgesamt dürfen Access-Provider nur als *ultima ratio* in Anspruch genommen werden. Daher ist bei Inlandssachverhalten generell von einer Unzulässigkeit der Inanspruchnahme von Access-Providern auszugehen, da hier Content- und Host-

Provider zur Gefahrenabwehr herangezogen werden können. Auch bei Sachverhalten, die Mitgliedsstaaten der EU betreffen, wird eine Inanspruchnahme von Access-Providern infolge des in der Richtlinie über audiovisuelle Mediendienste und der Richtlinie über den elektronischen Geschäftsverkehr vorgesehenen Konsultations- und Prüfungsverfahrens nur ausnahmsweise zulässig sein.

52. Unabhängig von den einzelnen Voraussetzungen der Ermächtigungsgrundlage für Sperrungsverfügungen gegen Access-Provider erweist sich derzeit als zentraler Hinderungsgrund, dass das Gesetz keinen Eingriff in das Telekommunikationsgeheimnis regelt. Daher sind Sperrungsverfügungen, die in das Telekommunikationsgeheimnis eingreifen, auf der Basis des § 20 Abs. 1 und Abs. 4 JMStV i.V.m. § 59 Abs. 3 u. 4 RStV nicht zulässig. Mangels entsprechender gesetzlicher Regelungen würden Zugangsbeschränkungen von Access-Providern zu rechtswidrigen Informationen durch Manipulation im Zusammenhang mit Umständen der Telekommunikation rechtswidrig sein.

53. Der grundgesetzlich und einfachgesetzlich angeordnete Schutz des Telekommunikationsgeheimnisses lässt m.E. gegenwärtig auch keine netzbasierten „Sperren" durch Access-Provider auf DNS-Basis zu (vgl. Randnummer 38). Unabhängig davon, wie der insofern bestehende juristische Meinungsstreit im Ergebnis von Gerichten entschieden würde, ist bereits die damit einhergehende Rechtsunsicherheit Access-Providern, die ordnungs- und polizeirechtlich als Nicht-Störer zu qualifizieren sind, nicht zumutbar. Es gilt insoweit zu berücksichtigen, dass Access-Provider bei Verletzung des Telekommunikationsgeheimnisses empfindlichen Sanktionen ausgesetzt sind. Die Verletzung des Telekommunikationsgeheimnisses ist gem. § 206 StGB sogar mit Strafe bedroht.

54. Sperrungen im Sinne einer nutzerautonomen Beschränkung des Zugangs sind indes jederzeit möglich.

Frage 9: Wie sollte eine solche Regelung zur Verpflichtung zur Sperrung von kinderpornographischen Inhalten konkret ausgestaltet werden?

55. Dem *ultima ratio*-Gedanken folgend sollte eine gesetzliche Regelung zunächst klarstellen, dass Zugangsbeschränkungen zum Internet ausschließlich im Hinblick auf kinderpornographische Inhalte vorgenommen werden sollen. Damit würde der Ausnahmecharakter einer insbesondere aus Gründen des Opferschutzes eingeführten gesetzlichen Regelung unterstrichen und gleichzeitig die Ausweitung von Zugangsbeschränkungen im Hinblick auf andere Regelungsgegenstände (z.B.

Glücksspiel, Urheberrecht etc.) unterbunden. Dies kann m.E. nur durch eine Sonderregelung im Hinblick auf Kinderpornographie sichergestellt werden, die klarstellt, dass die rechtliche Bewertung der gesellschaftlich erwünschten inhaltsneutralen Infrastrukturleistung der Access-Provider nicht grundsätzlich infrage gestellt werden soll, sondern überragende Rechtsgüter im Hinblick auf missbrauchte Kinder geschützt werden.

56. Die rechtliche Grundlage zur Zugangsbeschränkung zu kinderpornographischen Inhalten im Ausland sollte zum Ausdruck bringen, dass Adressaten von Maßnahmen zunächst immer die für rechtswidrige Inhalte verantwortlichen Content- und Host-Provider sein müssen. Nur wenn sich die Bekämpfung kinderpornographischer Inhalte an der Quelle als nicht durchführbar erweist, dürfen Sperrungsmaßnahmen gegenüber Access-Providern erwogen werden. Darüber hinaus ist das europarechtlich vorgesehene Konsultations- und Prüfungsverfahren zu berücksichtigen. Im Ergebnis dürften daher Maßnahmen gegenüber Access-Providern, unbeschadet besonders dringender Fälle, nur dann in Betracht kommen, wenn die rechtswidrigen Informationen von außerhalb der EU stammen. Das Gesetz sollte zudem ausdrücklich regeln, dass Access-Provider keine Überwachungs- und Nachforschungspflichten treffen. Angesichts des Umstands, dass Access-Providern eine Sperrung des Zugangs zu Informationen im Internet faktisch nicht möglich ist – ihre Manipulationsmöglichkeiten erschöpfen sich in der Erschwerung des Zugangs zu Informationen – sollte eine gesetzliche Regelung außerdem von der weiteren Verwendung des Begriffs „Sperrung" absehen.

57. In dem grundrechtssensiblen Bereich von Zugangsbeschränkungen durch Access-Provider ist im Rahmen der Schaffung einer gesetzlichen Grundlage weiterhin sicherzustellen, dass eine rechtliche Einstufung von Informationen als Kinderpornographie, zu denen Access-Provider den Zugang als *ultima ratio* erschweren sollen, in einem rechtsstaatlichen Verfahren erfolgt. Bereits die Abgrenzung zwischen Kinder- (§ 184b StGB) und Jugend-Pornographie (§ 184c StGB) dürfte nicht immer eindeutig vorzunehmen sein. Darüber hinaus besteht generell die Gefahr einer Überblockade, bei der auch rechtmäßige Inhalte von Zugangsbeschränkungen erfasst werden. Betroffenen muss daher insbesondere die Möglichkeit einer gerichtlichen Überprüfung von Maßnahmen eröffnet werden.

58. Eine gesetzliche Regelung muss außerdem den Umfang bestimmen, in dem Access-Provider zu Eingriffen in das Telekommunikationsgeheimnis berechtigt sind. Das Zitiergebot ist dabei zu wahren. Es sollte hinreichende Normklarheit und Normbestimmtheit angestrebt werden. Aufgrund der vielschichtigen Rechtspositionen, die durch die Erschwerung des Zugangs zum Internet berührt werden, sollte eine gesetzliche Regelung in Bezug auf alle Handlungen, die Access-Provider als polizei- und ordnungsrechtliche Nichtstörer in Erfüllung der von ihnen verlangten

Zugangsbeschränkungen vornehmen, auch eine umfassende Freistellung von Haftungsansprüchen regeln. Schließlich sollten dem nichtstörenden Access-Provider die anfallenden Kosten erstattet werden.

Frage 10: Medienberichten zufolge soll nach den Planungen des BMFSJ das Bundeskriminalamt nach kinderpornographischen Internetseiten und Inhalten suchen und diese in eine ständig aktualisierte Liste aufnehmen und den Internetanbietern zuleiten. Wie bewerten Sie diesen Vorschlag aus rechtlicher Sicht?

59. Aus rechtlicher Sicht ist nichts dagegen einzuwenden, dass das Bundeskriminalamt im Internet nach kinderpornographischen Inhalten sucht. Bei Kinderpornographie handelt es sich um schwerwiegende Offizialdelikte, die von Amts wegen zu verfolgen sind, was m.E. auch anlassunabhängige Ermittlungstätigkeiten rechtfertigt. Im Vordergrund sollte dabei die Strafverfolgung stehen, die durch eine Verbesserung der technischen und personellen Ausstattung der Strafverfolgungsbehörden unterstützt werden kann.

60. Eine alleinige Zuständigkeit des Bundeskriminalamts zur Festlegung einer Liste mit Inhalten, zu denen der Zugang im Internet durch Access-Provider zu beschränken ist, wäre dagegen m.E. rechtlich problematisch. Einer solchen Liste des Bundeskriminalamts käme nämlich ohne rechtsstaatliche Verfahrensgarantien autoritativer Charakter in einem grundrechtssensiblen Bereich zu. Daher halte ich es für notwendig, dass eine von dem Bundeskriminalamt erstellt Liste vor der Umsetzung von Zugangsbeschränkungen durch Access-Provider richterlich überprüft oder durch einen pluralistisch besetzten Beschlusskörper wie die BPjM nach einer Kontrolle freigeben wird.

Frage 11. Wie bewerten Sie den Vorschlag, dass das BKA entsprechende Inhalte sucht, diese aber dann an die zuständigen Jugendschutzbehörden weiterleiten sollte, damit diese – wie ja bereits nach geltendem Recht möglich – über die Aufnahme in entsprechende Listen entscheiden und diese dann an den Provider weiterleiten?

61. Im Lichte der vorstehenden Antwort zur Frage 10 ist die Einbeziehung der BPjM aus rechtlicher Perspektive ein gangbarer Weg, um rechtstaatliche Verfahrensgarantien im Rahmen einer gesetzlichen Regelung für Zugangsbeschränkungen zu Kinderpornographie einzuführen. Der BPjM würde als pluralistisch besetztem Beschlusskörper mit großer Erfahrung im Bereich jugendgefährdender Medien die

Letztentscheidung über Zugangsbeschränkungen vorbehalten bleiben. Dies hätte zudem den Vorteil, dass die BPjM bereits heute wegen § 18 Abs. 3 JuSchG (sog. Tendenzschutzklausel) gesetzlich zur Beachtung entgegenstehender Grundrechte verpflichtet ist.

62. Eine gesetzliche Neuregelung könnte entsprechend der bestehenden Regelungslogik des JuSchG einen gesonderten Listenteil für die Zugangsbeschränkung zu Kinderpornographie vorsehen, in die nach abgeschlossener Prüfung die Informationen eingestellt werden, die sich als kinderpornographisch erweisen und zu denen Access-Provider als *ultima ratio* den Zugang erschweren sollen.

63. Die Rechtsschutzmechanismen des JuSchG wären gegebenenfalls im Hinblick auf die besondere Problematik netzseitiger Zugangsbeschränkungen zu ergänzen.

Frage 12: Welche rechtstaatlichen Absicherungen sind darüber hinaus notwendig? Welche Rechtsschutzmöglichkeiten müssen vorgesehen werden, beispielsweise bei versehentlicher Sperrung?

64. Durch die vorstehend angeregten rechtsstaatlichen Verfahrensgarantien (vgl. Fragen 10 und 11) sollten bereits im Vorfeld von Zugangsbeschränkungen rechtlich und technisch fehlerhafte Anordnungen minimiert werden. Trotzdem müssen m.E. auch effektive Rechtsschutzmechanismen gegen umgesetzte Anordnungen von Zugangsbeschränkungen vorgesehen werden, um fehlerhafte Anordnungen nachträglich gerichtlich überprüfen zu können. Je nach Ausgestaltung des Systems, d.h. richterliche Überprüfung der vom Bundeskriminalamt recherchierten Liste oder Letztentscheidung des BPjM, wäre der ordentliche Rechtsweg oder der Verwaltungsrechtsweg indiziert. Für ein System unter Einbeziehung des BPjM enthielte das JuSchG bereits eine Reihe von Verfahrensregeln, auf die aufgebaut werden könnte und die für den Sonderfall der Anordnung von Zugangsbeschränkungen zu kinderpornographischen Inhalten im Ausland ggf. zu ergänzen wären.

65. Zugunsten von Access-Providern muss – wie bereits angeführt – gesetzlich eine umfassende Haftungsfreistellung vorgesehen werden. Dies muss sowohl im Hinblick auf zivilrechtliche Ansprüche Geschädigter, im Hinblick auf verwaltungsrechtliche Maßnahmen sowie auch im Hinblick auf das Strafrecht gelten.

Frage 13: Bestehen Defizite im bestehenden (Jugendschutz-)Recht, um den Zugang zu kinderpornographischen Inhalten im Internet zu verhindern und wenn ja, wo genau?

66. Derzeit wird vornehmlich über netzseitige Zugangsbeschränkungen zu kinderpornographischen Inhalten im Internet diskutiert. Nutzerautonome Filtermöglichkeiten, auf die das bestehende Jugendschutzrecht in unterschiedlichem Zusammenhang Bezug nimmt, werden dabei nicht weiter in die Abwägung einbezogen. Nutzerautonome Filtersoftware stellt m.E. einen Schlüssel für den effektiven Jugendmedienschutz im Internet dar, da Erziehungsberechtigte durch ihren Einsatz den Schutz von Kindern und Jugendlichen, die ihrer Personensorge unterliegen, altergerecht bestimmen können. Dabei ist selbstverständlich zu berücksichtigen, dass nutzerautonome Filtermöglichkeiten in erster Linie der Zielvorgabe Jugendmedienschutz dienen, während der Opferschutz für netzseitige Zugangsbeschränkungen zu kinderpornographischen Inhalten entscheidender Gesichtspunkt ist. Trotzdem ist m.E. zu empfehlen, durch die Verbesserung der gesetzlichen Rahmenbedingungen sowie durch die Förderung von Forschung und Entwicklung für nutzerautonome Filtersoftware zumindest begleitende Maßnahmen zu ergreifen, um Kinder und Jugendliche vor der Konfrontation mit kinderpornographischen Inhalten im Internet zu schützen.

Frage 14: Teilen Sie die Auffassung, dass es einer spezialgesetzlichen Regelung für die Sperrung von kinderpornographischen Internetangeboten bedarf? Könnte durch eine Erweiterung des JuSchG bzw. des JMStV das gleiche gewünschte Ergebnis erzielt werden?

67. Eine spezialgesetzliche Regelung zu Zugangsbeschränkungen im Hinblick auf kinderpornographische Inhalte im Internet erscheint empfehlenswert, um den Ausnahmecharakter einer solchen Maßnahme zu unterstreichen. Dies könnte m.E. durch präzise und unzweideutige Neuregelungen im JuSchG ebenfalls erreicht werden. Sowohl im Rahmen einer gesetzlichen Spezialregelungen als auch bei einer Erweiterung bestehender Gesetze wäre durch den Gesetzgeber klarzustellen, dass nur kinderpornographische Inhalte als so schwerwiegende Verletzungen herausragender Rechtsgüter qualifiziert werden, dass hier als *ultima ratio* ausnahmsweise eine netzseitige Zugangsbeschränkung zu Angeboten aus dem Ausland zulässig ist. Gleichzeitig sollte klargestellt werden, dass aufgrund einer solchen gesetzlichen Neuregelung die Verantwortlichkeit von Access-Providern in anderen Rechtsmaterien (z.B. Glücksspiel, Urheberrecht) nicht erweitert werden darf.

Frage 15: **Da die Anbieter der entsprechenden Angebote sich im Ausland befinden und nicht strafrechtlich verfolgt werden können, werden die Internetzugangsanbieter mit der Verpflichtung zur Sperrung als sog „Nichtstörer" in Anspruch genommen. Wie ist daher die Kostenerstattung für Investitionen und Inanspruchnahme der Internetzugangs-Provider auszugestalten?**

68. Da derzeit streitig ist, ob verwaltungsrechtliche Kostenerstattungsansprüche im diskutierten Fall Anwendung finden, sind spezialgesetzliche Kostenerstattungsansprüche zu schaffen, die Access-Providern eine umfassende Kostenerstattung für Investitionen und Inanspruchnahme für Sperrungsmaßnahmen gewähren.

Dr. Dieter Frey
(Rechtsanwalt)