Stellungnahme

Verband der deutschen Internetwirtschaft e.V.

Berlin, den 09.02.2009

Öffentliches Expertengespräch des Unterausschusses Neue Medien des Ausschusses für Kultur und Medien des Deutschen Bundestages zu den rechtlichen und technischen Möglichkeiten und Grenzen von Sperrungsverfügungen kinderpornographischer Inhalte im Internet

Donnerstag, 12. Februar 2009, 15:30 – ca. 16:30 Uhr

Der eco Verband der deutschen Internetwirtschaft vertritt die Interessen von mehr als 400 Mitgliedsunternehmen, die über 300.000 Mitarbeiter beschäftigen und einen Umsatz von ca. 75 Mrd. Euro jährlich erwirtschaften. Im eco-Verband sind unter anderem die ca. 230 „Backbones“ des deutschen Internet vertreten, also nahezu alle deutschen Internet Service Provider, die ein eigenes Netz betreiben.

eco versteht sich als Interessenvertretung der deutschen Internetwirtschaft gegenüber Politik und in internationalen Gremien. Als Expertennetzwerk befasst sich eco mit aktuellen Themen aus den Bereichen Internetrecht und Regulierung, Infrastruktur, Online Services und E-Business.

Einleitung

Der Kampf gegen Kinderpornografie und andere illegale Inhalte im Internet hat für eco und seine Mitgliedsunternehmen seit Jahren höchste Priorität. Die Zusammenarbeit und Kooperation mit dem Bundeskriminalamt, den Strafverfolgungsbehörden sowie der Betrieb von nationalen Beschwerdestellen und deren Einbindung in das internationale Netzwerk von Beschwerdestellen (INHOPE) leisten heute bereits einen wesentlichen Beitrag zur Bekämpfung der Kinderpornografie und anderer illegaler Inhalte sowie zu einer erfolgreichen Ermittlung und Strafverfolgung der Täter.

Vordringliches Ziel der gemeinsamen Bestrebungen von Strafverfolgungsbehörden und der Internetwirtschaft ist die effektive und nachhaltige Bekämpfung von sexueller Ausbeutung von Kindern sowie von Kinderpornografie. Hierzu ist eine Entfernung der inkriminierten Inhalte im Ursprungsland, ein konsequentes Vorgehen gegen den Anbieter der Inhalte und die Sicherstellung der Strafverfolgung der Täter erforderlich und hat höchste Priorität.

Demgegenüber kann die Implementierung technischer Maßnahmen, wie die derzeit diskutierte netzseitige Zugangserschwerung zu im Ausland liegenden Webseiten, anstelle dessen nur subsidiär und als Ultima ratio in Betracht

eco
Verband der deutschen
Internetwirtschaft e.V.
Marienstraße 12
10117 Berlin

Fon +49 (0) 30-24 08 36-96
Fax +49 (0) 30-24 08 36-97
info@eco.de
www.eco.de

kommen. Dementsprechend kann die Problematik bzw. die Frage nach Zugangserschwerungen nur dann auftreten, wenn die illegalen Inhalte im außereuropäischen Ausland gespeichert werden und nach der dortigen Rechtsordnung legal sind.

Sinnvollster Lösungsansatz bleibt daher die internationale Ächtung der Kinderpornografie und eine Verbesserung bei der internationalen Rechtsangleichung, Rechtsdurchsetzung und Strafverfolgung. Zugangserschwerungen können daher allenfalls flankierende Maßnahmen darstellen.

Die Implementierung derartiger Techniken ist nur auf den ersten Blick eine vermeintlich einfache Lösung. Denn sie führt zu keiner Beseitigung der Inhalte, sondern zu einer bloßen Erschwerung des Zugangs, da die Inhalte weiterhin verfügbar sind.

Aufgrund der Umgehungsmöglichkeiten ist eine voll wirksame Sperrung technisch nicht möglich. Die Implementierung technischer Maßnahmen leidet daher stets unter nicht unerheblichen Mängeln bei der Effektivität und Nachhaltigkeit.

Die derzeitige Diskussion über Zugangserschwerungen darf insbesondere nicht dazu führen, dass Access-Provider für die durchgeleiteten Inhalte verantwortlich gemacht werden, denn sie haben weder Kenntnis noch Einfluss auf die Inhalte. Dementsprechend schließen Telemediengesetz (TMG) und E-Commerce-Richtlinie (200/31/EG) die Verantwortlichkeit von Zugangsprovidern für durchgeleitete Inhalte grundsätzlich aus.

Darüber hinaus ist für Access-Provider eine Überwachung des Internetverkehrs bereits aufgrund des Fernmeldegeheimnisses verboten. Auch bestehen für Zugangsanbieter nach E-Commerce-Richtlinie und Telemediengesetz keine proaktiven Kontrollpflichten der durchgeleiteten Inhalte.

Nach der derzeitigen Rechtslage mit zahlreichen ungelösten Fragestellungen (insbesondere Haftungsfragen) und praktischen Umsetzungsschwierigkeiten besteht somit für die Zugangsanbieter kein Spielraum für eine Selbstverpflichtung/Vereinbarung zur Implementierung netzseitiger Sperrungen. Vielmehr muss eine entsprechende gesetzliche Regelung in einem Spezialgesetz getroffen werden.

Vor diesem Hintergrund beantworten wir die durch den Unterausschuss Neue Medien des Ausschusses für Kultur und Medien des Deutschen Bundestages aufgeworfenen Fragen gern wie folgt:

Technik:

1. WELCHE FORMEN DER SPERRUNG VON STRAFRECHTLICH RELEVANTEN INHALTEN GIBT ES UND WIE BEWERTEN SIE DIESE HINSICHTLICH IHRER WIRKSAMKEIT UND EFFIZIENZ, DEM DAMIT JEWEILS VERBUNDEN AUFWAND SOWIE DEN JEWEILIGEN KOSTEN?

Da sämtlichen technischen Maßnahmen immanent ist, dass sie den Zugang zu Inhalten niemals zu 100% sperren, verwendet eco anstelle von „Sperrung“ den Begriff der Zugangserschwerung. Für solche Zugangserschwerungen kommen verschiedene technische Möglichkeiten in Betracht.

Im Hinblick auf die Effizienz sämtlicher Maßnahmen ist jedoch vorab hervorzuheben, dass sich im hier einschlägigen Bereich der Kinderpornografie nur ein Bruchteil der Inhalte auf Websites befindet, die Ziel sämtlicher Maßnahmen der Zugangserschwerung sind.

Die Erfahrungen der Strafverfolgungsbehörden und der Einrichtungen der Internetwirtschaft zeigen vielmehr, dass der weitaus größte Teil von Inhalten mit Bezug zu Kindesmissbrauch über Peer-to-Peer-Verbindungen, etwa durch IRC-Chats, Instant-Messaging-Clients oder auch Peer-to-Peer-Netzwerke ausgetauscht werden. Nur ein verhältnismäßig sehr geringer Anteil solcher Inhalte ist online frei zugänglich. Bereits insoweit ist die Geeignetheit und Effizienz solcher Maßnahmen zur Eindämmung der Verbreitung kinderpornografischer Inhalte im Internet sehr gering.

Aktuell werden folgende vier technische Ansätze für die Zugangserschwerung verfolgt:

- Manipulation am DNS-Server
- Einträge in Routing-Tabellen/ IP-Ausschluss durch Sperrung am Router
- Einsatz eines Proxy-Servers auf der Anwendungsschicht
- Hybride Sperrtechnologien

Bezüglich der Details der unterschiedlichen technischen Möglichkeiten des „Access-Blocking“ erlauben wir uns, auf das von der KJM in Auftrag gegebene **Gutachten von Prof. Dr. Pfitzmann** zu verweisen.

Ergänzend dazu ist auf folgendes hinzuweisen:

Access-Blocking führt spätestens dann, wenn es in der Breite gegen eine Vielzahl von Seiten eingesetzt wird, zu einer Beeinträchtigung des Internet insgesamt – und damit auch der Nutzung der wichtigsten globalen Informationsressource.

Erfahrungen aus bisherigen Sperrversuchen zeigen, dass die Anbieter von illegalen Inhalten in solchen Fällen innerhalb von wenigen Stunden reagieren und durch Änderungen die Sperrungen umgehen. Zudem werden kinderpornografische Inhalte verstärkt über sog. „Botnetze“ gesteuert, durch die automatisch ständig die Server gewechselt werden. Dadurch sind die technischen und personellen Anforderungen an eine ständig aktualisierte Liste mit illegalen Inhalten äußerst hoch.

2. LÄSST SICH VERHINDERN, DASS DIESE TECHNISCHEN MÖGLICHKEITEN NICHT NUR ZUR SPERRUNG VON KINDERPORNOGRAPHISCHEN INHALTEN, SONDERN ZUR SPERRUNG VON RECHTMÄßIGEN INHALTEN MISSBRAUCHT WERDEN KÖNNEN?

Für welche Inhalte die jeweils verwendete Technik verwendet wird, hängt ausschließlich von dem jeweiligen Betreiber bzw. den Personen ab, die bei dem jeweiligen Betreiber tätig sind. Insofern sind Missbrauchsmöglichkeiten grundsätzlich gegeben. Sobald eine entsprechende Technologie implementiert ist, kann diese für jede Art unerwünschter Inhalte verwendet werden. Umso wichtiger ist die Einbettung in ein rechtsstaatliches Verfahren und eine rechtsstaatliche Kontrolle.

3. WIE KANN VERHINDERT WERDEN, DASS DIE LISTEN DER ZU SPERRENDEN INHALTE BEKANNT WERDEN? WAS SIND DIE FOLGEN, WENN – WIE IN EINIGEN SKANDINAVISCHEN LÄNDERN – DIE LISTEN DER ZU SPERRENDEN INHALTE BEKANNT WERDEN?

Ein Bekanntwerden der Inhalte der zu sperrenden Listen hat erhebliche negative Folgen.

So wurden zuletzt auf dem anonym betriebenen Portal Wikileaks.org die Sperrlisten der Länder Dänemark und Thailand veröffentlicht, die dort nach wie vor abrufbar ist. Danach umfasst die dänische Liste allein 3863 Websites wobei sich herausgestellt hat, dass nur ein sehr geringer Teil der Websites tatsächlich kinderpornografisches Material aufgewiesen hat.

Durch derartige Vorfälle verkehrt sich nicht nur der eigentlich beabsichtigte Effekt ins Gegenteil. Dies zeigt auch, wie anfällig die Technologie ist.

Das Bekanntwerden von „Sperrlisten“ kann nicht ganz verhindert werden, aber durch den Einsatz von Verschlüsselungstechnologien beim Austausch der Daten zwischen Listenersteller und Provider verringert werden.

Darüber hinaus müsste der Austausch dieser Daten über eine gesicherte Serververbindung erfolgen.

Selbst unter Einsatz solcher Techniken verbleibt jedoch die Möglichkeit, die IP-Adressen der gesperrten Inhalte nachzuvollziehen. Im Fall des in Großbritannien eingesetzten Systems „CleanFeed“ ist diese Anfälligkeit durch das Gutachten von Prof. Dr. Pfitzmann bestätigt worden.[1]

4. MIT WELCHEN KOSTEN SIND DIE UNTERSCHIEDLICHEN FORMEN DER SPERRUNG VERBUNDEN? IN DEN MEDIEN WURDE BERICHTET, DASS DAS BMFSFJ MIT INVESTITIONSKOSTEN VON CA. 40.000 EURO RECHNET. WIE BEWERTEN SIE DIESE KOSTENABSCHÄTZUNG?

Die Kosten für die unterschiedlichen Formen der Sperrung hängen unter anderem von dem jeweiligen Geschäftsmodell, der Netzstruktur sowie der Kundenzahl eines Providers ab. Die Implementierung beispielsweise einer DNS-Lösung stellt sich für einen national oder regional tätigen Provider anders dar als für ein europaweit tätiges Unternehmen, dass DNS-Server in mehreren Ländern betreibt.

Bei einer DNS-Lösung dürfte es sich um diejenige Maßnahme handeln, die mit den geringsten Kosten verbunden ist. Selbst hier bedeutet dies z.B. für ein europaweit tätiges Unternehmen mit eigenem Netz in mehreren europäischen Ländern reine Investitionskosten in Höhe von ca. EUR 800.000,-.[2] Hinzu kommen selbstverständlich die Kosten des laufenden Betriebes.

Für die weiteren technischen Möglichkeiten des IP-Blockings, dem Einsatz eines Proxy-Servers oder hybriden Methoden sind die Investitionskosten ungleich höher. Einzelheiten sind derzeit nicht bekannt, da in Deutschland keine Erfahrungen mit der Implementierung derartiger Maßnahmen bestehen.

[1] Prof. Dr. Pfitzmann, Gutachten „Sperrungsverfügungen gegen Access-Provider“, S. 57
[2] Diese Angabe beruht auf einem konkreten, aktuellen Angebot, das von einem Unternehmen für die Umsetzung eines DNS-Blocking im eigenen Netz eingeholt wurde.

Bereits vor dem Hintergrund der Kostenschätzung für eine DNS-Lösung bewerten wir die Kostenabschätzung des BMFSFJ jedoch als zu gering, insbesondere aber als zu wenig differenziert. Keinesfalls sind darin die Kosten für den laufenden Betrieb der jeweiligen Maßnahme enthalten.

5. WIE BEWERTEN SIE DIE ERFAHRUNGEN BEZÜGLICH DER WIRKSAMKEIT DERARTIGER SPERREN IN ANDEREN VERGLEICHBAREN STAATEN?

Erfahrungen bezüglich der Wirksamkeit von Sperrungen in anderen vergleichbaren Staaten liegen kaum vor.

Zwar existieren Zahlen darüber, wie viele Seitenaufrufe in einigen Ländern geblockt werden. Dabei ist aber zum einen zu berücksichtigen, dass die Listen teilweise nicht nur bzw. wenig kinderpornografisches Material beinhalten. Zum anderen lassen sich daraus keine Rückschlüsse darauf ziehen, ob ein „geblockter Nutzer“ sich möglicherweise auf anderem Wege Zugang zu der jeweiligen Website verschafft hat.

Insbesondere ist kaum nachzuvollziehen, ob und – wenn ja – welche Auswirkungen solche Maßnahmen auf die Verfügbarkeit und Anzahl kinderpornografischer Angebote insgesamt haben.

RECHT:

6. WIE BEWERTEN SIE DIE BESTEHENDEN INSTRUMENTE DER SELBSTREGULIERUNG IN DEUTSCHLAND WIE AUCH IN EUROPA?

a) Internet-Beschwerdestelle

Gemeinsam mit der Freiwilligen Selbstkontrolle Multimedia e.V. (FSM) betreibt eco die von der Europäischen Kommission durch den „Safer Internet Action Plan“ geförderte Internetbeschwerdestelle, bei der Nutzer illegale Inhalte im Internet melden können (www.internet-beschwerdestelle.de). Hier werden nicht nur Inhalte von Websites gemeldet und von den Mitarbeitern der Einrichtung überprüft, sondern z.B. auch illegale Inhalte aus den Bereichen E-Mail, Tauschbörsen, Chats, Newsgroups.

Die Einrichtung stößt bei der deutschen Internet-Öffentlichkeit auf großen Zuspruch. Im Jahr 2006 wurde die Internet-Beschwerdestelle insgesamt über 70.000 Mal von Internet-Nutzern kontaktiert. eco geht gemeinsam den

Beschwerden nach, prüft den Anlass der Beschwerde und den Sitz des für die inkriminierten Inhalte Verantwortlichen und leitet gegebenenfalls die Beschwerde entweder an Kooperationspartner im Ausland weiter oder unternimmt selbst Schritte, um der Beschwerde abzuhelfen. Ziel ist dabei stets, den Inhalt am Ursprungsort zu bekämpfen und aus dem Netz zu entfernen.

Internetwirtschaft und BKA kooperieren seit vielen Jahren erfolgreich bei der Eindämmung strafbarer – insbesondere kinderpornografischer Inhalte. Ende 2007 haben die Freiwillige Selbstkontrolle Multimedia (FSM), jugendschutz.net und der Verband der deutschen Internetwirtschaft (eco) ihre langjährige und erfolgreiche Zusammenarbeit mit dem Bundeskriminalamt durch den Abschluss einer Kooperationsvereinbarung untermauert.

b) INHOPE

Die Internet Beschwerdestelle kooperiert im Rahmen der internationalen Dachorganisation von Beschwerde-Hotlines INHOPE (www.inhope.org) mit derzeit 33 Partnerorganisationen aus 29 Ländern weltweit. Diese Einrichtung besteht bereits seit 1999.

Das Netzwerk ermöglicht die Weiterleitung von Beschwerden, damit illegale Inhalte in deren Ursprungsland bekämpft werden können. Die effiziente internationale Zusammenarbeit der INHOPE-Hotlines hat in der Vergangenheit bereits vielfach großen Fahndungserfolgen insbesondere im Bereich der Bekämpfung der Kinderpornographie geführt.

Im Rahmen dieses eines „Trusted Networks“ von Beschwerdestellen werden Beschwerden von Internetnutzern über rechtswidrige und schädliche Inhalte im Netz entgegengenommen und an die zuständigen Behörden unmittelbar oder über eine der internationalen Partnerhotlines weitergeleitet und unverzüglich bearbeitet. Die Einrichtung „ziviler“ Beschwerdestellen, die in den Ländern der Europäischen Union ebenfalls durch das Safer Internet Programm teilweise kofinanziert werden, entlastet Strafverfolgungsbehörden bei der Prüfung von Beschwerden erheblich und sorgt für eine Absenkung der nachgewiesenen Hemmschwelle bei der Meldung rechtlich kritischer Inhalte.

Weltweit haben INHOPE Beschwerdestellen im Jahr 2007 über 93.000 Beschwerden bearbeitet und über 6000 Meldungen an Strafverfolgungsbehörden weitergeleitet. Die Beschwerdestelle des eco bearbeitete davon mehr als 4.300 Beschwerden und informierte in 141 Fällen deutsche Strafverfolgungsbehörden, in 130 Fällen INHOPE Partnerhotlines, und in allen Fällen – einschließlich derer mit nicht strafrechtlich relevanten, sondern lediglich rechtswidrigen Inhalten – die

involvierten Internetdienstleister, die sodann für eine unverzügliche Sperrung des Zugangs zu den Inhalten Sorge tragen.

Im Fall "Marcy" konnte die deutsche eco Hotline im Mai 2002 einen entscheidenden Hinweis auf eine einschlägige, geschlossene Nutzergruppe in einem „Bulletinboard“ an die spanische Partner-Hotline im Rahmen des INHOPE-Netzwerkes weitergeben. Unmittelbar nach Überprüfung der Inhalte wurde das Bundeskriminalamt informiert. Nach rund einem Jahr Ermittlungstätigkeit ist es der Polizei infolgedessen gelungen, 38 international tätige kinderpornografische Zirkel im Internet zu sprengen. Von den Ermittlungen in 166 Ländern waren rund 26.500 tatverdächtige Internet-Nutzer betroffen, darunter 530 Bundesbürger. Der eco-Verband hat damit eine der bislang bedeutendste Aktion gegen die internationale Kinderpornografie-Szene ausgelöst. Allein in Deutschland wurden von der Polizei 745 Computer, mindestens 35.500 CDs, 8.300 Disketten sowie 5.800 Videos beschlagnahmt.

7. WIE BEWERTEN SIE DIE UNTERSCHIEDLICHEN TECHNISCHEN MÖGLICHKEITEN HINSICHTLICH IHRER EINGRIFFSTIEFE IN GRUNDRECHTE, HINSICHTLICH IHRER WIRKSAMKEIT UND HINSICHTLICH IHRER VERHÄLTNISMÄßIGKEIT?

a) Eingriffstiefe

Die Eingriffstiefe in die Grundrechte hängt zum einen von der verwendeten Technologie ab, zum anderen von den Umständen des Einzelfalls auf Seiten des in die Pflicht genommenen Providers.

So stellt sich zum Beispiel für einen kleinere Access-Provider, der keinen eigenen Proxy-Server betreibt, der Einsatz eines „Zwangs-Proxy-Servers“ als stärkeren Eingriff in die Berufsausübungsfreiheit (Art. 12 GG) dar.

Auf Seiten der Nutzer sind bei allen technischen Maßnahmen Eingriffe in die Informationsfreiheit (Art. 5 Abs. 1 S. 1 Alt. 2 GG) zu befürchten.

Nach den vorliegenden Gutachten ist darüber hinaus bei Maßnahmen des IP-Blockings, dem Einsatz eines Proxy-Servers und dem hybriden Verfahren ein Eingriff in das Fernmeldegeheimnis (Art. 10 GG und dessen einfachgesetzliche Ausformung in § 88 TKG) gegeben. Nach dem Gutachten der Rechtsanwälte Dr. Frey liegt ein solcher Eingriff auch bei einem DNS-Blocking vor.

b) Wirksamkeit

Sämtlichen technischen Möglichkeiten ist gemeinsam, dass sie niemals eine 100%ige Sperrung, sondern immer nur eine Erschwerung des Zugangs ermöglichen. Die Höhe der technischen Hürde kann dabei nicht isoliert betrachtet werden, sondern muss ins Verhältnis gesetzt werden zu dem technischen Aufwand der Implementierung, dem Eingriff in Grundrechte, den Kosten des Betriebes und dem jeweils erforderlichen Eingriff in die Netzinfrastruktur des Providers.

Dennoch lässt sich für IP-Sperren sagen, dass diese sehr ungenau sind und eine zielgenaue Blockade der illegalen Inhalte daher nur schwer möglich ist. Es besteht daher bei dieser Technik die erhebliche Gefahr, dass legale Webseiten mitgesperrt werden.

c) Verhältnismäßigkeit

Bei der Frage nach der Verhältnismäßigkeit sind nach Auffassung von eco insbesondere die „Geeignetheit“ und die „Angemessenheit“ der technischen Möglichkeiten zu berücksichtigen.

aa) Geeignetheit

Bei der Frage nach der Geeignetheit ist insbesondere die Skalierbarkeit der technischen Maßnahme von Bedeutung.[3] Denn die gewählte Sperrmethode muss daraufhin geprüft werden, wie geeignet sie auch angesichts wachsender Datenmengen ist und inwiefern der Ressourcenbedarf steigt. Angesichts der aktuell diskutierten BKA-Liste mit einer derzeit nicht konkret zu bestimmenden Anzahl von Einträgen (anfänglich dürfte von etwa 1000 Adressen auszugehen sein, die Anzahl wird aber in kurzer Zeit rapide anwachsen (vgl. Frage 10)), die Gegenstand von Sperrmaßnahmen sein sollen, ist auch dies nicht unproblematisch. Insbesondere ist fraglich, wie dem sowohl in den technischen und rechtlichen Gutachten, als auch in der Rechtsprechung zu Sperrungsverfügungen immer wieder hervorgehobenem Grundsatz Rechnung getragen werden soll, nach dem die Rechtmäßigkeit einer Sperrung im Hinblick auf Eingriffsintensität und Effektivität immer anhand des konkreten Einzelfalls zu beurteilen ist.

Zudem weist Prof. Sieber in seinem Gutachten zu „Sperrungsverfügungen“ zu Recht darauf hin, dass nach der Rechtsprechung des Bundesverfassungsgerichts bei der Frage der Geeignetheit zunehmend auch der sogenannte „additiven Grundrechtseingriff“ in die Abwägung einzubeziehen ist:

[3] Prof. Sieber Gutachten „Sperrverfügungen im Internet“, S. 183.

„*Eine nur punktuelle Betrachtung der Einzelfälle wird den vielfältigen staatlichen Inpflichtnahmen, denen sich die Privatwirtschaft ausgesetzt sieht, deswegen nicht mehr gerecht. Gerade die Berufsgruppe der Internet-Service-Provider wird vom Staat immer umfassender herangezogen*."[4]

Unabhängig von der Frage nach dem Umfang einer Liste, die Gegenstand von Sperrungen sein soll, ist vor diesem Hintergrund bei der Frage nach der Geeignetheit auch zu berücksichtigen, dass bereits heute gegenüber Providern durch verschiedene Interessengruppen Wünsche nach netzseitigen Zugangserschwerungen herangetragen werden.[5] Wenn daher im Bereich Kinderpornografie eine gesetzliche Regelung zur Zugangserschwerung gewollt ist wird diese nur dann dem Verhältnismäßigkeitsgrundsatz gerecht, wenn der Gesetzgeber diese Maßnahmen eindeutig und als Ausnahme auf strafrechtliche relevante Inhalte im Sinne des § 184 b StGB (Verbreitung, Erwerb und Besitz kinderpornographischer Schriften) beschränkt und allen anderen Begehrlichkeiten eine klare Absage erteilt.

bb) Angemessenheit

Die Angemessenheitsprüfung erfordert stets eine Abwägung im Einzelfall. Insoweit ist es schwierig, die im Gegensatz zu einzelnen Sperrungsverfügungen konkreter Angebote nunmehr geplante generelle Verpflichtung zur Zugangserschwerung einer Liste mit einer derzeit konkret nicht zu bestimmenden Anzahl von Einträgen auf ihre Angemessenheit hin zu beurteilen.

Im Hinblick auf die verschiedenen technischen Möglichkeiten ist jedenfalls festzuhalten, dass mit höherer Eingriffsintensität die Zumutbarkeit gegenüber dem Provider zunehmend problematisch wird. Sofern – wie beim Einsatz eines Proxy-Servers – durch eine Maßnahme das Wesen des Geschäftsmodells des Providers tangiert wird, ist diese mit Blick auf Art. 12, 14 GG nicht mehr zumutbar[6] und damit unverhältnismäßig.

Ein weiteres Kriterium für die Angemessenheit aller technischen Maßnahmen ist die Frage der Kostentragung. Mehr noch als im Falle einzelner Sperrungs-verfügungen durch Aufsichtsbehörden ist diese Frage von Bedeutung, wenn die dauerhafte Zugangserschwerung einer listenmäßig zusammengestellten, variierenden Anzahl von Webseiten von den Unternehmen implementiert werden soll.

---

[4] Prof. Sieber Gutachten „Sperrverfügungen im Internet", S. 184.
[5] Details siehe unten, Ausführungen zu Ziff. 14.
[6] Prof. Sieber Gutachten „Sperrverfügungen im Internet", S. 217.

Da bereits eine unentgeltliche Inanspruchnahme der Provider – die hier als Nichtstörer zur Erfüllung hoheitlicher Aufgaben herangezogen werden – dann nicht mehr angemessen ist, wenn sie über die Grenze der Geringfügigkeit hinaus geht[7], hat zur Wahrung der Verhältnismäßigkeit nach Auffassung von eco eine Kostenerstattung zu erfolgen.

8. AUF WELCHER RECHTLICHEN GRUNDLAGE UND DURCH WEN KÖNNTEN WELCHE INHALTE UND MIT WELCHEN MITTELN GEGEN EINEN ZUGRIFF VON ENDNUTZERN GESPERRT WERDEN?

a) Rechtsgrundlage

Nach derzeitiger Rechtslage kämen für Sperrungsverfügungen die Ermächtigungsgrundlagen im Jugendmedienschutz-Staatsvertrag (§ 20 Abs. 4 JMStV iVm. § 59 Abs. 2-4 RStV) und im Rundfunk-Staatsvertrag (§ 59 Abs. 2-4 RStV) in Betracht. Allerdings müsste jeweils für den Einzelfall geprüft werden, ob eine Sperrverfügung erlassen werden kann. Hierbei müssten insbesondere die Schwere der Rechtsverletzung wie auch die Umstände beim Provider berücksichtigt werden.

b) Zuständigkeit

Für Sperrungsanordnungen innerhalb des JMStV – Anwendungsbereichs ist für Anbieter von Telemedien gem. § 20 Abs. 4 JMStV die „zuständige Landesmedienanstalt durch die KJM“ zuständig.

Außerhalb des JMStV – Anwendungsbereichs bestimmt sich die Zuständigkeit nach § 59 Abs. 2 RStV, die auf „nach Landesrecht bestimmte Aufsichtsbehörden“ abstellt.

c) Adressierte Inhalte

Die Ermächtigungsgrundlage des § 20 Abs. 4 JMStV bezieht sich gem. § 20 Abs. 1 JMStV auf Verstöße gegen Bestimmungen „dieses Staatsvertrages“. In Frage kommen hierfür § 4 Abs. 1 JMStV (absolut unzulässige Angebote), § 4 Abs. 2 JMStV (Angebote nur für Kinder und Jugendliche unzulässig) und § 5 JMStV (Angebote, die nur für Kinder und Jugendliche bestimmter Altersstufen möglichst unzugänglich zu machen sind).

[7] Prof. Sieber Gutachten „Sperrverfügungen im Internet“, S. 224.

§ 4 JMStV	
Abs. 1	*Nicht mehr Generalklausel mit Bezugnahme auf StGB, sondern Verstöße werden gesondert umschrieben; subjektive Voraussetzungen des StGB müssen nicht erfüllt sein („unbeschadet strafrechtlicher Verantwortlichkeit“)*
Nr. 1	*Ausdrückliche Bezugnahme auf §§ 86 StGB, Propagandadelikte*
Nr. 2	*Ausdrückliche Bezugnahme auf § 86a StGB, Verwendung von Kennzeichen verfassungswidriger Organisationen*
Nr. 3	*Volksverhetzung (entsprechend § 130 Abs. 2 StGB)*
Nr. 4	*Leugnen/Verharmlosen von Verbrechen unter der Herrschaft des Nationalsozialismus*
Nr. 5	*Schildern von grausamen und sonst unmenschlichen Gewalttätigkeiten gegen Menschen (entsprechend § 131 StGB)*
Nr. 6	*Anleitung zu einer in § 126 Abs. 1 StGB genannten Tat (Landfriedensbruch, Mord, schwere Körperverletzung usw.)*
Nr. 7	*Kriegsverherrlichende Angebote*
Nr. 8	*Angebote, die gegen die Menschenwürde verstoßen (z.B. „snuff“-Videos)*
Nr. 9	*Kinder und Jugendliche in unnatürlich geschlechtsbetonter Körperhaltung*
Nr. 10	*Harte Pornographie (entsprechend §§ 184a ff. StGB)*
Nr. 11	*Teile B und D der Bundesprüfstellen-Liste (öffentliche Liste sowie nicht-öffentliche Liste der Trägermedien mit absolutem Verbreitungsverbot) oder im Wesentlichen inhaltsgleich*

Abs. 2	*Angebote im Rundfunk unzulässig; in Telemedien jedoch nur für Jugendliche aller Altersgruppen unzulässig; für Erwachsene zulässig, sofern diese in geschlossenen Benutzergruppen angeboten werden*
Nr. 1	*Pornographische Angebote, die nicht schon nach Abs. 1 unzulässig sind;*
Nr. 2	*Teile A und C der Bundesprüfstellen-Liste (keine strafrechtliche Relevanz, aber Gefährdungspotential) oder im Wesentlichen inhaltsgleich*
Nr. 3	*Schweres Gefährdungspotential für die Entwicklung von Kindern und Jugendlichen, Berücksichtigung der besonderen Wirkungsform des Verbreitungsmediums*

9. WIE SOLLTE EINE SOLCHE REGELUNG ZUR VERPFLICHTUNG ZUR SPERRUNG VON KINDERPORNOGRAPHISCHEN INHALTEN KONKRET AUSGESTALTET WERDEN?

Zu den Anforderungen einer derartigen Regelung verweisen wir auf die Ausführungen zu Ziff. 10, 12 und 14.

10. MEDIENBERICHTEN ZUFOLGE SOLL NACH DEN PLANUNGEN DES BMFSJ DAS BUNDESKRIMINALAMT NACH KINDERPORNOGRAFISCHEN INTERNETSEITEN UND INHALTEN SUCHEN UND DIESE IN EINE STÄNDIG AKTUALISIERTE LISTE AUFNEHMEN UND DEN INTERNET-ANBIETERN ZULEITEN. WIE BEWERTEN SIE DIESEN VORSCHLAG AUS RECHTLICHER SICHT?

Dieser Vorschlag wird zurzeit in einer Arbeitsgruppe beim BMFSJ gemeinsam mit Vertretern der großen Provider, der Verbände und mit BMWi, BMI und BKA diskutiert.

Aus Sicht von eco sind dabei insbesondere folgende Punkte zu diskutieren:

a) Judikative Kontrolle
In dem Moment, indem eine ursprünglich zu Strafverfolgungszwecken von einer Strafverfolgungsbehörde erstellte Liste mit strafrechtlich relevanten Inhalten als Basisdokument für die Erschwerung des Zugangs zu derartigen Inhalten dient, verlässt die erstellende Behörde ihren eigentlichen Aufgabenbereich. Das Bundeskriminalamt als Strafverfolgungsbehörde kann daher nicht ohne Einbindung in ein rechtsstaatliches Verfahren und ohne Kontrollinstanzen darüber verfügen, welche medialen Inhalte über deutsche Zugangsprovider abgerufen werden können und welche nicht. Auch von den präventiven Befugnissen des BKA ist die Erstellung einer Liste, die Gegenstand von Zugangserschwerungen sein soll, nicht umfasst.

Der Gesetzgeber müsste vor diesem Hintergrund bei einem derartigen Verfahren sicherstellen, dass die Gewaltenteilung auch bei dem Verfahren der Listenerstellung greift. Hierzu kann es erforderlich sein, dass das BKA als Strafverfolgungsbehörde bei der Listenerstellung einer judikativen Kontrolle unterliegt. Es muss in einem rechtsstaatlich anerkannten Verfahren geregelt sein, wer darüber entscheidet, was unter welchen Voraussetzungen in die Liste aufgenommen wird.

b) Technische Umsetzung
Aufgrund der stark divergierenden Netzinfrastrukturen und unterschiedlichen technischen Gegebenheiten muss die konkrete Umsetzung und Implementierung netzseitiger Zugangserschwerungen den Telekommunikationsunternehmen vorbehalten bleiben. Aus Gründen der Rechts- und Planungssicherheit ist jedoch klarzustellen, dass eine Zugangserschwerung auf Basis des Domain Name Systems (sog. „DNS-Blocking“) als geeignet erachtet wird.

Die technischen Einzelheiten, insbesondere die Datenbank zur Vorhaltung der Listeneinträge, Definition der Schnittstelle und Schutzmaßnahmen zur

Verhinderung des Zugriffs Dritter, sollten in einer zu treffenden Vereinbarung festgelegt werden. Die Festlegung der technischen Einzelheiten sollte im Einvernehmen unter Beteiligung der Unternehmen und der Verbände erfolgen, um einen reibungslosen Ablauf und eine problemlose Implementierung zu gewährleisten.

Zu den weiteren rechtlichen Bewertungen siehe die Ausführungen zu Ziff. 12.

11. WIE BEWERTEN SIE DEN VORSCHLAG, DASS DAS BKA ENTSPRECHENDE INHALTE SUCHEN, 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?

Die derzeit im Fokus stehenden kinderpornografischen Inhalte sind nach Auffassung von eco zumindest nicht primär im Lichte des Jugendschutzes zu beurteilen. Vielmehr stehen die Verfolgung internationaler, organisierter Schwerstkriminalität und der Opferschutz im Vordergrund. Ob in diesem Zusammenhang Jugendschutzbehörden über die Aufnahme von Inhalten in eine Liste entscheiden sollen, ist fraglich.

Nach Auffassung von eco ist unabhängig davon weniger wichtig die Frage des „wer“, als vielmehr die Frage „wie“. Von grundlegender Bedeutung ist, dass die Listenerstellung eingebettet ist ein rechtsstaatliches Verfahren, dass unter anderem Rechtsmittel für den Fall der Sperrung legaler Angebote vorsieht.

Wie oben bereits dargelegt verfügt das BKA nicht über die Kompetenz bzw. gehört es nicht in den Zuständigkeitsbereich des BKA, eine Liste zu erstellen, die Gegenstand von Zugangserschwerungen sein könnte. Die Erstellung einer Liste, die Gegenstand von Zugangserschwerungen sein könnte, sollte in die Zuständigkeit einer Bundesbehörde gehören. Denkbar wäre beispielsweise eine Zuständigkeit der BPJM, für die bereits ein rechtsstaatlich anerkanntes gesetzliches Verfahren der Indizierung von Medien existiert.

12. WELCHE RECHTSTAATLICHEN ABSICHERUNGEN SIND DARÜBER HINAUS NOTWENDIG? WELCHE RECHTSSCHUTZMÖGLICHKEITEN MÜSSEN VORGESEHEN WERDEN, BEISPIELSWEISE BEI VERSEHENTLICHER SPERRUNG?

Die Umsetzung des Vorschlags des BMFSJ setzt völlig losgelöst von großen technischen Herausforderungen gleich eine ganze Reihe von rechtsstaatlichen Absicherungen voraus, die gesetzlich zu regeln wären.

a) Gesetzliche Regelung über Umgang, Verwendung und Zugriff auf die Liste

Da bereits der Besitz einer Liste mit kinderpornografischen Websites potentiell strafbar ist, muss auch die Zurverfügungstellung, der Umgang und die Verwendung einer solchen Liste geregelt werden.

b) Rechtsbehelfe gegen unberechtigte Listeneinträge

Die Liste muss einer regelmäßigen Aktualisierung und Überprüfung unterliegen, damit sichergestellt ist, dass ungültige Listeneinträge oder zwischenzeitlich rechtmäßige Inhalte nicht zu Unrecht einer Sperrung unterliegen. Diese Aktualisierung kann nicht den Unternehmen obliegen, die von den Inhalten keine Kenntnis nehmen dürfen.

Weiterhin muss die Entscheidung über die Aufnahme eines Telemedienangebotes in die Liste justiziabel sein. Es müssen Rechtsschutzmöglichkeiten für den Fall vorgesehen werden, dass sich rechtmäßige oder zwischenzeitlich rechtmäßig gewordene Inhalte auf der Liste befinden.

c) Subsidiarität der Maßnahme

Die Implementierung netzseitiger Zugangserschwerungen muss sich aus Gründen der Verhältnismäßigkeit ausschließlich auf Webseiten mit kinderpornografischen Inhalten beschränken und kann neben einer Entfernung der inkriminierten Inhalte, konsequenten Täterermittlung und Strafverfolgung nur subsidiär und als Ultima ratio in Betracht kommen kann.

Bereits Sperrungsanordnungen bzgl. einzelner Telemedienangebote nach geltendem Recht dürfen nur ergehen, wenn sich Maßnahmen gegenüber dem eigentlich Verantwortlichen nach § 7 TMG als nicht durchführbar oder nicht erfolgversprechend erweisen. Zur Wahrung der Subsidiarität ist es daher mindestens erforderlich, dass das unmittelbare Vorgehen gegen den Inhaltsanbieter auf rechtliche Hindernisse stößt.[8]

Es muss daher gesetzlich geregelt sein, dass zunächst wenigstens der Versuch unternommen wird, Inhalte am Ursprungsort zu bekämpfen, bevor ein Inhalt auf die Liste gesetzt wird. Dies gilt insbesondere für Inhalte, die im europäischen Raum gehostet werden. Anderenfalls droht die als Ultima Ratio vorgesehene Möglichkeit zur Sperrung zur Regel zu werden.

---

[8] vgl. Prof. Sieber, Gutachten „Sperrverfügungen im Internet“, S. 152.

d) Zitiergebot
Im Hinblick darauf, dass durch netzseitige Zugangserschwerungen der einfachgesetzlich und verfassungsrechtlich geschützte Bereich des Datenschutzes erheblich tangiert werden - Eingriff in das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung – muss das Zitiergebot beachtet werden.

e) Verantwortlichkeitsregelungen gem. TMG und E-Commerce Richtlinie
Telemediengesetz (TMG) und E-Commerce-Richtlinie (200/31/EG) schließen die Verantwortlichkeit von Zugangsprovidern für durchgeleitete Inhalte grundsätzlich aus. Die Implementierung netzseitiger Zugangserschwerungen darf daher nicht dazu führen, dass Access-Provider für die durchgeleiteten Inhalte verantwortlich gemacht werden. Ebenso muss klargestellt sein, dass die Implementierung netzseitiger Sperrungen weder zu einer Kenntniserlangung noch zu einer Auswahl von Inhalten führen kann. Zur Vermeidung von Rechtsunsicherheiten ist insoweit ebenfalls eine gesetzliche Klarstellung erforderlich.

f) Haftungsfreistellung
Ebenfalls aus Gründen der Rechtssicherheit und um ein Haftungsrisiko zu vermeiden, müssen die Zugangsanbieter vollumfänglich von einer Haftung freigestellt werden. Die Haftungsfreistellung muss sich sowohl auf die Implementierung netzseitiger Zugangserschwerungen als auch auf den Fall der unbeabsichtigten Sperrung rechtmäßiger Inhalte und daraus erwachsender Ansprüche Dritter erstrecken.

g) Evaluierung
Da bislang in Deutschland keinerlei Erfahrungswerte hinsichtlich der Auswirkungen und der Funktionsweise netzseitiger Zugangserschwerungen vorliegen, sollte innerhalb eines Zeitraumes von 12 Monaten ein Evaluierungsprozess eingeleitet werden, in dem insbesondere die technischen Auswirkungen auf die Netzinfrastruktur, die Effektivität im Hinblick auf die Erschwerung des Zugangs zu den entsprechenden Websites im Verhältnis zu dem damit verbundenen technischen, organisatorischen und administrativen Aufwand sowie die erfolgte Eindämmung der Verbreitung von Kinderpornografie überprüft werden.

13. BESTEHEN DEFIZITE IM BESTEHENDEN (JUGENDSCHUTZ-) RECHT, UM DEN ZUGANG ZU KINDERPORNOGRAPHISCHEN INHALTEN IM INTERNET ZU VERHINDERN UND WENN JA, WO GENAU?

Kinderpornografische Inhalte können als absolut unzulässige Inhalte zwar auch Gegenstand des Jugendmedienschutz-Staatsvertrages sein. Nach Auffassung

von eco steht bei der aktuellen Diskussion jedoch die Strafverfolgung bzw. –prävention im Vordergrund, so dass eine Debatte über mögliche Defizite im bestehenden Jugendschutzrecht hier nicht geführt werden sollte.

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?

Insbesondere aus den zu Ziff. 12 vorgebrachten Gründen kann die automatisierte Sperrung von kinderpornografischen Internetangeboten nicht ohne gesetzliche Änderungen implementiert werden. Hierzu reicht es jedoch nicht aus, das JuSchG oder den JMStV zu erweitern.

Ebenso darf die erforderliche Änderung keinesfalls im Telemediengesetz erfolgen, wie es derzeit teilweise gefordert wird. Das Telemediengesetz setzt unter anderem die E-Commerce-Richtlinie um und enthält bezüglich der Verantwortlich-keitsregeln der Provider ein sensibles Haftungsgefüge. Insbesondere verweist es bezüglich der Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen ausdrücklich auf die allgemeinen Gesetze (§ 7 Abs. 2 TMG). Mit dieser Regelung ist die hier einschlägige „Nicht-Störer-Verantwortlichkeit“ adressiert.

Darüber hinaus ist zu berücksichtigen, dass die §§ 7 – 10 Telemediengesetz gerade keine eigenen Verantwortlichkeiten des Diensteanbieters begründen und gerade keine Anspruchsgrundlagen oder öffentlich-rechtliche Eingriffsermächtigungen begründen. Diese bereits im Teledienstegesetz enthaltene Konstruktion einer „horizontalen Regelung“ diente der Vermeidung eines Änderungsbedarfs bezüglich unzähliger Gesetze.[9] Daher verweist das TMG auf die jeweils spezialgesetzliche Norm, deren Anspruchsvoraussetzungen zunächst erfüllt sein müssen.

Die erforderlichen gesetzlichen Änderungen müssen daher nach Auffassung von eco eine eigene, **spezialgesetzliche Regelung** erfahren. Da vorliegend nicht der Jugendschutz, sondern die Strafverfolgung bzw. –prävention im Vorderund steht, müsste ein neues Bundesgesetz, z.B. in Gestalt eines „Gesetzes zur Eindämmung der Verbreitung von Kinderpornografie über das Internet“ geschaffen werden.

[9] Hoffmann in Spindler, Recht der elektronischen Medien, TMG Vorb. §§ 7 ff., Rn. 25.

Damit wird zudem einem weiteren, wichtigen Punkt Rechnung getragen:

Bereits heute sehen sich die Provider auch mit Sperrungswünschen anderer Interessengruppen konfrontiert. So hat das Hessische Innenministerium Ende 2008 diverse Access-Provider zu einem Gespräch geladen, in denen die Sperrung eines ausländischen Glücksspielangebotes diskutiert werden sollte. Darüber hinaus äußert auch die Kommission für Jugendmedienschutz (KJM) den Wunsch nach der freiwilligen Sperrung jugendgefährdender Inhalte auf Basis einer Liste der Bundesprüfstelle für jugendgefährdende Medien und hat diesbezüglich zuletzt im Oktober Provider und Verbände zu einem Gespräch geladen. Selbst im Falle von Urheberrechtsverletzungen werden durch die Film- und Musikwirtschaft Vorschläge unterbreitet, die die Sperrung auf Access-Ebene zum Gegenstand haben.

Es steht daher zu befürchten, dass eine gesetzliche Regelung insbesondere dann weitere Begehrlichkeiten auch anderer Interessengruppe weckt, wenn nicht durch eine spezialgesetzliche Regelung klar zum Ausdruck kommt, dass ausschließlich und abschließend für den Bereich kinderpornografischer Inhalte als ultima ratio und unter engen Voraussetzungen technische Zugangserschwerungen in Betracht kommen.

Überdies ist eine spezialgesetzliche Regelung auch unter Verhältnismäßigkeits-gesichtspunkten von Bedeutung, vgl. die Ausführungen zu Ziff. 7a), cc).

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 INTERNETZUGANGSPROVIDER AUSZUGESTALTEN?

Wir beziehen uns insoweit auf die Ausführungen zu Ziff. 7 c), bb).