Stellungnahme

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 Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.200 Unternehmen, davon 900 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Dr. Guido Brinkel
Rechtsanwalt
Bereichsleiter Medienpolitik
Tel. +49. 30. 27576-221
Fax. +49. 30. 27576-51-221
g.brinkel@bitkom.org

Präsident
Prof. Dr. Dr. h.c. mult.
August-Wilhelm Scheer

Hauptgeschäftsführer
Dr. Bernhard Rohleder

1 Allgemeine Anmerkungen

BITKOM bewertet die Verbreitung von Kinderpornografie im Internet als eines der größten Probleme der Webkriminalität (hier verstanden als Straftaten, deren Begehung mit Hilfe des Internets erheblich erleichtert und gefördert wird) überhaupt. Die Verbreitung von Kinderpornografie hat sich gerade im Internet über den Aspekt kriminell ausgelebter Pädophilie hinaus zu einem kommerziellen Markt entwickelt. Dieser trägt Züge organisierter Kriminalität. Die vom BITKOM repräsentierten Mitgliedsunternehmen unterstützen in jeder Hinsicht den Kampf gegen die Verbreitung solcher schwerstkrimineller Inhalte. Dies beinhaltet grundsätzlich auch die Bereitschaft, auf rechtlich sicherer Grundlage technische Mechanismen zur Erschwerung des Zugangs zu entsprechenden Inhalten im World Wide Web einzusetzen.

Wir betonen gleichzeitig, dass der Kampf gegen Kinderpornografie auf sämtlichen Ebenen geführt werden muss. Das Kernziel jeglicher Aktivitäten muss neben der Ermittlung der Täter die Stärkung des Opferschutzes, die Verhinderung weiterer Missbräuche und damit auch die Austrocknung des kommerziellen Marktes für entsprechende Inhalte, sei es offline oder online, sein. Vor diesem Hintergrund bewerten wir insbesondere die in den vergangenen Jahren erzielten Ermittlungsergebnisse deutscher Landeskriminalämter sowie des Bundeskriminalamtes als große Erfolge.

Zugangserschwernisse können stets nur ein flankierendes Mittel sein, da ihre Wirkung auf den kommerziellen Markt aus verschiedenen Gründen gering ist. Politische Initiativen sollten daher ein Gesamtpaket beinhalten, dass seinen Schwerpunkt auf die Stärkung der Täterermittlung legt. Wir schließen uns in diesem Zusammenhang ausdrücklich der Forderung an, die Ermittlungsbehörden sowohl in technischer als auch fachlicher Hinsicht besser auszustatten. Insgesamt warnen wir mit Nachdruck davor, die Bekämpfung der Kinderpornografie zu einem Wahlkampfthema zu stilisieren. Die Schwere der Verbrechen erfordert ein entschlossenes Handeln aller Beteiligten – jedoch keine politischen

Schnellschüsse. In diesem Zusammenhang muss insbesondere die nötige Rechtssicherheit für alle Beteiligten gewährleistet werden. Jüngste Bewertungen zeigen die mit Zugangssperrungen einhergehenden rechtlichen Probleme deutlich auf.

BITKOM legt schließlich großen Wert auf die Berücksichtigung der Einbettung der Debatte in den politischen und rechtlichen Gesamtkontext. Das Instrument der Zugangserschwerung auf Access-Ebene ist in Deutschland bereits seit mehreren Jahren nicht nur für kinderpornographische Inhalte in der Diskussion. Es ist klar erkennbar, dass von verschiedenen Seiten erhebliche Begehrlichkeiten bestehen, das Instrument der Zugangserschwerung auf weitere Inhalte auszudehnen. Entsprechende Forderungen gibt es für extremistische, insbesondere rechtsradikale Seiten, für einfache Pornografie, für urheberrechtlich relevante Inhalte sowie aktuell hinsichtlich ausländischer Glücksspielangebote. Diese Ausweitungsdiskussionen bilden einen maßgeblichen Unterschied zur Situation in anderen Staaten – insbesondere den im Bereich Kinderpornografie häufig als Beispiel genannten skandinavischen Ländern. Dort gibt es klare politische Signale, dass eine Ausweitung von Zugangserschwernissen auf andere Inhalte oder Sachlagen aufgrund der damit ebenfalls verbundenen tief greifenden rechtlichen Bedenken und technischen Eingriffe nicht in Betracht kommt.

BITKOM betont mit Nachdruck, dass eine Zugangserschwerung auf Access-Ebene ein Ultima-ratio-Instrument für schwerstkriminelle und international geächtete Inhalte wie Kinderpornografie ist, das sich für eine Ausweitung auf andere Konstellationen nicht eignet. Mit Sorge und tiefgreifender Skepsis bewerten wir daher die schon in der Vergangenheit geführte und jetzt im Zuge der zu Kinderpornografie stattfinden Diskussion noch stärker aufkommenden weiter reichenden Ansprüche und Begehrlichkeiten. Konsequent zu Ende gedacht, würden diese die Internet Service Provider (ISP; also alle Diensteanbieter, die Zugang zum Datennetz anbieten) in eine Überwacherrolle drängen, die konträr zur neutralen Natur der erbrachten Dienstleistung und damit auch konträr zu grundlegenden rechtlichen Wertungen ist, wie sie insbesondere in der EU-E-Commerce-Richtlinie sowie dem darauf basierenden Telemediengesetz (TMG) zum Ausdruck kommen.

2 Zu den vorgelegten Fragen

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?

BITKOM verweist zu diesem Punkt in den Details auf die umfangreichen Ausführungen des technischen Gutachtens von Prof. Pfitzmann im Auftrag der Kom-

mission für Jugendmedienschutz (KJM)[1], dessen Einschätzung wir in den wesentlichen Punkten teilen. Insbesondere verzichten wir unter Verweis auf die dortige umfassende Darstellung auf eine Beschreibung der verschiedenen denkbaren technischen Ansätze.

Wirksamkeit & Effizienz:

Grundsätzlich lässt sich festhalten, dass sämtliche denkbaren Mechanismen – ungeachtet ihrer technischen Komplexität – für einen gezielt vorgehenden und mit Fachwissen ausgestatteten Nutzer umgehbar sind. Insbesondere bei Nutzung sog. Anonymisierungsdienste, die sowohl frei als auch als kommerzielle Dienstleistung angeboten werden, geraten sämtliche Methoden zur Zugangserschwerung an ihre Grenzen. Bei weniger komplexen Eingriffen, wie einer Modifikation des DNS bestehen für technisch versierte Nutzer noch einfacher zu handhabende Formen der Umgehbarkeit – konkret auf DNS-Modifikationen bezogen etwa die Nutzung eines freien DNS-Servers, z.B. www.opendns.org. BITKOM steht auf dem Standpunkt, dass diese Ausgangssituation maßgeblich die Erwartungshaltung an die beabsichtigten Maßnahmen prägen und die Zielvorstellungen einer möglichen Zugangserschwerung beeinflussen sollte. Konkret folgt aus der Umgehbarkeit, dass entsprechende Mechanismen allenfalls zufällige Aufrufe und Abrufe durch „Gelegenheitskonsumenten“ erschweren können. Dies entspricht auch der Bewertung des sog. Systems „Cleanfeed“ in Großbritannien.

Trotz der nicht geringfügigen Umgehungsmöglichkeiten steht BITKOM auf dem Standpunkt, dass Zugangshürden das Verhalten von Durchschnittsnutzern beeinflussen und Zufallskontakte begrenzen können und insgesamt ein richtiges gesellschaftspolitisches Signal im Kampf gegen Kinderpornografie sind. Inwieweit durch entsprechende Maßnahmen aber tatsächlich der kommerzielle Markt für Kinderpornografie eingedämmt werden kann, sollte Gegenstand einer entsprechenden Evaluation sein.

Ein Aspekt, der ebenfalls im Rahmen einer Evaluation dringend Beachtung finden sollte, sind etwaige kontraproduktive Auswirkungen von Access-Sperrungen auf die Täterermittlung im Bereich der Konsumenten. Professionell agierende Täter werden im Falle der Umsetzung von Sperrmaßnahmen möglicherweise verstärkt auf die Nutzung von Anonymisierungsdiensten setzen. Es besteht daher die Gefahr, dass hierdurch die konkrete Täterermittlung noch erschwert wird, weil die IP-Adresse als Ansatzpunkt zur Identifizierung nicht mehr ausgelesen werden kann. Derartige Negativeffektiv auf die eigentliche Täterverfolgung sollten in jedem Fall vermieden werden, da diese auch künftig das Hauptinstrument im Kampf gegen kinderpornografische Inhalte bilden muss. Ggf. sollte zu diesem Punkt auch auf Erfahrungen aus dem Ausland zurückgegriffen werden.

Wir verweisen hinsichtlich der Problematik der Wirksamkeit darüber hinaus auf die Antwort zu Frage 5.

[1] Abrufbar unter http://www.kjm-online.de/public/kjm/bogus.php?download_id=498.

Aufwand & Kosten:

Der konkrete Aufwand sowie die Kosten der verschiedenen Mechanismen einer Zugangserschwerung lassen sich aktuell nicht seriös benennen, da es in Deutschland hierzu an Erfahrungswerten fehlt. Überdies ist der konkrete Aufwand nicht allein vom gewählten technischen Verfahren abhängig, sondern von einer Vielzahl weiterer Faktoren, insbesondere der Anzahl der zu blockierenden Seiten, dem Verfahren der Einbindung der Blacklist, der bestehenden Netzstruktur des jeweiligen ISP, der Aktualisierungshäufigkeit sowie etwaiger weiterer Anforderungen an die ISP, etwa Dokumentationspflichten.

Folgende Grundaussagen lassen sich abstrakt treffen: Der Aufwand wird umso höher, je komplexer das eingesetzte technische System ist – den höchsten Komplexitätsgrad erreichen dabei hybride Methoden. Dabei ist zu bedenken, dass es sich in jedem Fall um anspruchsvolle, wenig erprobte Technik handeln wird, die in der Anfangszeit eine gewisse Fehlerträchtigkeit aufweist und deshalb einen hohen Pflegeaufwand erfordert. Außerdem wächst mit der Anzahl der zu blockierenden Seiten bei allen denkbaren Systemen der Administrationsaufwand.

Dies liegt nicht zuletzt daran, dass sobald eine nennenswerte Sperrwirkung erreicht würde, mit einer Gegenreaktion in Form von Denial-of-Service- und anderen Angriffen durch Anbieter oder Hacker zu rechnen wäre, gegen die entsprechende Leistungsreserven vorgehalten werden müssten. Da die Sperreinrichtungen bei Störungen, Fehlkonfiguration und sonstigem Versagen die Stabilität und Funktionsfähigkeit des Internets beeinträchtigen können, wäre für redundante, hochverfügbare Auslegung und entsprechend hohe technische und personelle Überwachung zu sorgen. Allgemein ist sowohl der Personal-, als auch der Sach-/Investitionsaufwand nicht zu vernachlässigen, der mit der Komplexität der Systeme steigt.

Ein weiteres Beispiel für die Abhängigkeit des Aufwandes von der bestehenden technischen Konfiguration des jeweiligen ISP sind Verfahren auf Proxy-Basis. Sofern ein ISP keine eigenen Proxy-Server betreibt, müsste er zur Umsetzung entsprechender Maßnahmen zunächst solche anschaffen und in die eigene Netzinfrastruktur einfügen. In diesem Falle wäre die Realisierung einer technischen Zugangshürde faktisch mit einer tiefgreifenden Veränderung der eigenen technischen Struktur verbunden. Das juristische Gutachten von Prof. Sieber im Auftrag der KJM[2] sieht aus unserer Sicht zu Recht in einem solchen Eingriff eine (unzulässige) Pflicht zur Veränderung des Geschäftsmodells.

2. Lässt sich verhindern, dass diese technischen Möglichkeiten nicht nur zur Sperrung von kinderpornographischen Inhalten, sondern zur Sperrung von rechtmäßigen Inhalten missbraucht werden können?

2.1 Missbrauch

[2] Abrufbar unter http://www.kjm-online.de/public/kjm/bogus.php?download_id=499.

Nach Auffassung des BITKOM können und dürfen ISP im Rahmen etwaiger technischer Zugangshürden allenfalls als rein technischer Mittler fungieren, die eine durch eine staatliche Institution erstellte und gepflegte Liste – möglichst automatisiert – einem technischen Mechanismus zuführt, so dass der Zugang zu den in der Liste hinterlegten Seiten für den Normalnutzer technisch erschwert ist. Dies bedeutet, dass die ISP an keiner Stelle einen Einfluss auf die Inhalte nehmen können, die ihnen über technische Schnittstellen seitens der zuständigen Behörde übermittelt werden. Konkret ist ein Verfahren zu bevorzugen, welches bis zu einem solchen Grad automatisiert ist, dass eine persönliche Kenntnis der Listenbestandteile durch Mitarbeiter der ISP nicht notwendig ist.

Dies zugrunde gelegt, kämen entsprechende Manipulationen allenfalls - was wir nicht unterstellen - auf Seiten der zuständigen Behörde in Betracht. Diese muss daher im Rahmen von IT-Sicherheitsstandards sicherstellen, dass ein Zugriff oder gar die Manipulation der Listenbestandteile, sei es von außen oder durch behördeninterne Vorgänge, ausgeschlossen ist. Angesichts der Brisanz der Inhalte und der Eingriffsintensität von Access-Sperrungen muss aus Sicht des BITKOM die Festlegung dieser Standards von vornherein Teil der Gesamtregelung entsprechender Zugangshürden sein.

Überdies ist verbindlich und abschließend festzulegen, dass Bestandteil einer entsprechenden Liste ausschließlich kinderpornografische Inhalte i.S.d. § 184b, Abs. 1 i.V.m. § 176 Abs. 1 StGB sein dürfen.

2.2 Kollateralschäden

Ein bedeutsamer Aspekt sind die mit einzelnen technischen Verfahren einhergehenden Kollateralschäden durch technisch bedingte Mitsperrung legaler Seiten. Insbesondere im Rahmen von IP-basierten Methoden sind von Zugangshürden bzgl. einer spezifischen IP-Adresse aufgrund des verbreiteten „Virtual Hostings“ fast zwangsläufig auch andere Webseiten betroffen. Außerdem hat – in manchen Fällen – ein derartiges Verfahren auch Auswirkungen auf alle anderen Dienste unter der genannten IP-Adresse, etwa FTP-, E-Mail- oder VoIP-Dienste. In einem konkreten Beispiel aus dem Jahr 2007 wurde auf Basis einer später aufgehobenen gerichtlichen Verfügung in einem wettbewerbsrechtlichen Verfahren eine IP-basierte Zugangshürde umgesetzt, was zur Mitsperrung verschiedener legaler Seiten führte.[3]

Diese Nebeneffekte bilden ein technisch bedingtes, spezifisches Haftungsrisiko, dessen Absicherung für den ISP einer der wesentlichen Bestandteile des notwendigen rechtlichen Rahmens sein muss.

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?

Eine vollständige Sicherheit ist aus unserer Bewertung nur schwer zu gewährleisten; sie ist letztendlich angesichts der Architektur des Internets sogar illuso-

[3] S. dazu Spiegel-Online, 17.9.2007, http://www.spiegel.de/netzwelt/web/0,1518,506143,00.html.

risch. Alle denkbaren Systeme ermöglichen faktisch zumindest die Abfrage von Listenbestandteilen durch Testanfragen bzgl. spezifischer Domains. Dies gilt selbst für hochkomplexe Technologien wie das in Großbritannien verwendete „Cleanfeed“, für welches diese Möglichkeit nachgewiesen wurde und einen der Kernkritikpunkte bildet.

Grundsätzlich liegt die Verantwortung für die Geheimhaltung der zugrundeliegenden Liste bei der zuständigen staatlichen Behörde, die entsprechend auch die Sicherheitsstandards der notwendigen technischen Schnittstelle, die höchsten professionellen Ansprüchen genügen müsste, zu gewährleisten hat. Die Frage des Bekanntwerdens einer entsprechenden Liste bzw. einzelner Listenbestandteile ist überdies ein Aspekt der Haftungsproblematik, da hier unter anderem ein strafrechtliches Risiko für entsprechende organisatorisch verantwortliche Personen innerhalb der eingebundenen ISP droht. Da eine vollständige Absicherung, wie beschrieben, technisch nach unserer Einschätzung nicht möglich ist, muss diese strafrechtliche Haftungsproblematik gesetzlich abgesichert sein.

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?

Seitens der Internetwirtschaft ist eine Schätzung der tatsächlich anfallenden Kosten aktuell nicht seriös möglich. Die vom BMFSFJ genannte Größenordnung kann aus diesem Grund nicht bestätigt werden, erscheint auf den ersten Blick aber für deutsche Verhältnisse zu niedrig – zugrunde lagen hier offenbar Zahlen aus Skandinavien, die jedoch mangels weitergehender Informationen für uns nicht verifizierbar sind.

Die Kosten einer Zugangshürde hängen im Wesentlichen vom einzusetzenden technischen Verfahren, der Architektur des zugrunde liegenden Netzes (z.B. Kabelnetze, Mobilfunkzugang oder Festnetz), dem Umfang der Sperrung sowie insbesondere den Administrations- und Personalkosten innerhalb des Unternehmens ab. Grob lässt sich sagen, dass hybride Mechanismen einen erheblichen Komplexitätsgrad aufweisen und damit auch mit Abstand am kostenintensivsten sind. Die vom BMFSFJ genannte Größenordnung ist daher jedenfalls für eine hybride Technologie nach unserer Einschätzung keinesfalls haltbar.

Den geringsten Aufwand dürfte eine Sperrung von Einträgen im Domain-Name-System (sog. DNS-Sperre) nach sich ziehen. Die konkrete Kostenbelastung ist allerdings auch hier davon abhängig, wie viele Einträge eine entsprechende Blacklist enthält, da auch bei DNS-basierten Verfahren das Problem der Skalierbarkeit besteht.

Bedeutsam ist außerdem, dass die Kosten einer technischen Zugangshürde sich nicht in technischen Investitionskosten erschöpfen. Die Umsetzung eines entsprechenden Verfahrens muss innerhalb eines Unternehmens projektiert werden. Nach der eigentlichen technischen Implementierung entstehen weitere Kosten durch die notwendige Administration und das Personal. Die Frage der Kostenbelastung ist daher insbesondere auch abhängig von der konkreten

Ausgestaltung des Gesamtmechanismus. Stellschrauben bilden die Aktualisierungsintervalle, die Ausgestaltung der technischen Schnittstelle zur Implementierung der Liste sowie etwaige Dokumentations- oder Mitwirkungspflichten seitens der Unternehmen. Außerdem bildet die Struktur und Größe des konkret betroffenen Netzes einen maßgeblichen Einflussfaktor auf die Kostenbelastung. Auch aus diesem Grund sind die Zahlen aus Skandinavien nicht uneingeschränkt übertragbar. Nach unserer Einschätzung würden daher allein die jährlichen Administrations- und Personalkosten den seitens des BMFSFJ genannten Betrag – zumindest bei einigen Unternehmen – erheblich übersteigen.

5. Wie bewerten Sie die Erfahrungen bezüglich der Wirksamkeit derartiger Sperren in anderen vergleichbaren Staaten?

Dem BITKOM liegen keine Detailinformationen zu den Effekten bzw. der Wirksamkeit der Zugangshürden in anderen Staaten vor. Bewerten lässt sich bislang daher allenfalls die Zahl der absolut geblockten Zugriffe. Entsprechend der bekannten Informationen liegen diese etwa in Dänemark bei täglich 1700, in Norwegen bei 15000 – 18000 Blockings.

Ein Fazit dieser Zahlen dürfte sein, dass offenbar auch abseits abgeschlossener Räume in Newsgroups und abseits von Peer-to-Peer-Systemen entsprechende Inhalte konsumiert werden, mithin neben einem harten Kern kriminell organisiert agierender Konsumenten kinderpornografische Inhalte auch von „Gelegenheitskonsumenten“ abgerufen werden.

Die Interpretation der Zahlen ist gleichwohl mit zahlreichen Fragen versehen, die berücksichtigt werden müssen. Zum einen lässt die Gesamtzahl der erfolgten Blockings keinen Rückschluss darauf zu, zu welchem Anteil die Abrufe vom Nutzer auch intendiert waren. Es ist davon auszugehen, dass ein Teil der so erfassten Abrufe entstehen, indem Nutzer auf der Suche nach einfacher Pornografie unbeabsichtigt auf Seiten mit kinderpornografischen Inhalten gelangen. Nach unseren Informationen ist dies ein Grund, weshalb in Skandinavien von einer Verwendung der anfallenden Informationen für Strafverfolgungszwecke bewusst abgesehen wird.

Denkbar ist überdies, dass Abrufe bzw. Blockings durch Pop-Up-Fenster generiert wurden, deren Aufruf vom Nutzer nicht aktiv gesteuert wird. Auch hierüber geben die zirkulierenden Zahlen naturgemäß keine Auskunft.

In der Gesamtbewertung ist aus Sicht des BITKOM außerdem die Zielsetzung der Maßnahmen zu berücksichtigen und ihre Effizienz an dieser Zielsetzung zu messen. Soll eine Zugangshürde der Austrocknung des kommerziellen Marktes und damit im Ergebnis dem Schutz potentieller Opfer dienen, so muss eine Evaluation sich weniger an der Zahl der konkreten Blockingvorgänge orientieren, sondern in erster Linie die Auswirkungen auf die entsprechende Angebotslandschaft untersuchen.

BITKOM spricht sich daher jedenfalls für eine umfassende Evaluation aus, die insbesondere den zuletzt betonten Aspekt einbezieht.

Recht:

6. Wie bewerten Sie die bestehenden Instrumente der Selbstregulierung in Deutschland wie auch in Europa?

Selbstregulierung findet in Deutschland vor allem im Bereich des Presserechts sowie des Jugendmedienschutzes statt. In beiden Bereichen bewertet BITKOM die entsprechenden Ansätze als klares Erfolgsmodell. Insbesondere im Jugendmedienschutz ist über das mit dem JMStV etablierte Modell der regulierten Selbstregulierung in den vergangenen Jahren ein Schutzniveau entstanden, das im internationalen Vergleich als führend beurteilt werden kann. Wir bewerten es daher als positiv, dass auch die Europäische Union Selbstregulierungsmodelle verstärkt in politische Überlegungen einbezieht und dabei gerade auf die deutschen Erfahrungen im Bereich Jugendmedienschutz zurückgreift.

Die Zielrichtung bei der Bekämpfung der Kinderpornografie ist indes eine grundsätzliche andere. Kinder und Jugendliche sind hier weniger als Rezipienten von Medieninhalten Schutzobjekt etwaiger Initiativen (wenngleich auch der Konsum von Kinderpornografie durch Jugendliche denkbar ist). Vielmehr steht hier das Ziel des Opferschutzes in Bezug auf Schwerstkriminalität im Vordergrund.

Die unterschiedliche Schutzrichtung beider Rechtsmaterien sollte auch in der politischen Debatte berücksichtigt werden. Sie beeinflusst nicht nur rechtliche Zuständigkeiten, sondern auch die konkrete Zielrichtung, Zulässigkeit und Reichweite gesetzlicher oder freiwilliger Initiativen. Aus Sicht des BITKOM sollte daher auch in Bezug auf die Diskussion zu Zugangserschwerungen auf Access-Ebene zunächst die konkrete Zielrichtung solcher Maßnahmen eingehend diskutiert werden, um zu verhindern, dass eine falsche öffentliche Erwartungshaltung und im schlimmsten Fall ein allgemeines Gefühl einer letztlich trügerischen Scheinsicherheit verursacht wird.

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

BITKOM verweist zur Beantwortung dieser Frage zunächst auf die eingehenden Analysen der Rechtsgutachten von Prof. Sieber sowie Frey Rechtsanwälten. Zur Frage der Wirksamkeit verweisen wir außerdem auch auf die Beantwortung der Frage 1.

BITKOM bewertet etwaige Zugangshürden nicht als „Zensur“ im formaljuristischen Sinne. Wir folgen insoweit der Einschätzung des Gutachtens von Prof. Sieber.

Technische Zugangshürden auf Access-Ebene greifen allerdings grundsätzlich in das Fernmeldegeheimnis, die Berufsfreiheit bzw. das Eigentumsrecht der betroffenen ISP, die Informationsfreiheit der Nutzer sowie schließlich in die Meinungsfreiheit der jeweiligen Content-Provider ein.

Unabhängig von der konkreten juristischen Bewertung von DNS-basierten Zugangshürden in Bezug auf das Fernmeldegeheimnis (s. Frage 8) halten wir eine klarstellende Regelung schon deshalb für notwendig und sinnvoll, um für alle Beteiligten die notwendige Rechtssicherheit zu gewährleisten.

Hinsichtlich der Eingriffstiefe bewerten wir Zugangshürden auf Access-Ebene als besonders belastend. Durch die entsprechenden Maßnahmen werden zum einen sehr grundlegende Eingriffe in die technische Netzstruktur der Provider hervorgerufen, zum anderen bildet die Errichtung von Zugangshürden einen Einschnitt in die Informationsfreiheit der Endnutzer, die mehr und mehr durch die Möglichkeit geprägt wird, sich aus dem bewusst dezentral organisierten Internet frei zu informieren. Schließlich können sie unter Umständen die technische Funktionsweise des Internet an sich beeinträchtigen.

Die Schwere des aktuell diskutierten Anlasssachverhaltes – die Verbreitung von Kinderpornografie – darf daher nicht dazu verleiten, die notwendige gründliche Verhältnismäßigkeitsprüfung ausnahmsweise für entbehrlich zu halten. Dies gilt insbesondere vor dem Hintergrund der bekannten Ausweitungswünsche, da ansonsten eine Präjudizwirkung für das Instrument technischer Zugangshürden als solchem droht.

Im Hinblick auf die Verhältnismäßigkeit bewerten wir technische Zugangserschwerungen wie folgt:

- Die Geeignetheit einer technischen Zugangshürde wird durch die zahlreichen Umgehungsmöglichkeiten nicht gänzlich ausgeschlossen, jedoch sind diese in die Betrachtung einzubeziehen. Wir betonen außerdem, dass sich die Geeignetheit einer Maßnahme nur beurteilen lässt, wenn deren Ziel konkretisiert ist. Es bedarf daher auch für die derzeit diskutierten Konstellationen eines klar festgelegten Verständnisses, was konkret mit der Implementierung technischer Zugangshürden erreicht werden soll. Soweit der Zugriff von Gelegenheitsnutzern beschränkt werden soll, bewerten wir insbesondere DNS-basierte Verfahren als geeignet. Auch im Hinblick auf eine beabsichtigte gesellschaftspolitische Signalwirkung können Zugangshürden als geeignet bewertet werden.
- Die Erforderlichkeit hängt von mehreren Faktoren ab. Zum einen ist hier zwischen verschiedenen technischen Modellen zu differenzieren, da diese eine unterschiedliche Eingriffsintensität beim betroffenen Provider zur Folge haben. Insbesondere verursachen hochkomplexe hybride Verfahren erhebliche Aufwände und grundlegende technische Strukturveränderungen, ohne ein wesentlich höheres Maß an Umgehungssicherheit zu bieten. Umso komplexer das einzusetzende Verfahren ausgestaltet ist, umso eher steht aus unserer Sicht daher die Erforderlichkeit in Frage.

  Einen weiteren, die Erforderlichkeit beeinflussenden Aspekt bildet die Frage, inwieweit gegen Inhalteanbieter ggf. auch mit anderen Mitteln vorgegangen werden kann. Eine Rolle kann dies etwa spielen, wenn Blacklists Inhalte enthalten, die auf Servern in Ländern vorgehalten werden, in denen die Verbreitung von Kinderpornografie ähnlich wie in Deutschland sanktioniert ist und mit denen belastbare Rechtshilfeabkommen oder ähnliche Kooperati-

onsmodelle bestehen. In diesen Fällen bildet die Entfernung des eigentlichen Inhalts nicht nur das geeignetere, sondern auch das weniger belastende Mittel.

- Im Bereich der Angemessenheit bedarf es schließlich einer nochmaligen Gesamtabwägung der zahlreichen konfligierenden Rechtsgüter. Hierbei ist für den Bereich Kinderpornografie grundsätzlich zu berücksichtigen, dass es sich um einen Bereich der Schwerstkriminalität handelt. Dem stehen in der Abwägung etwaige Kollateralschäden, die für Provider entstehenden Aufwände sowie die begrenzte Wirksamkeit gegenüber.

Nach alledem bewerten wir Zugangshürden auf Access-Ebene als Ultima ratio zur Bekämpfung schwerstkrimineller Inhalte, in Fällen in denen ein Zugriff auf den eigentlichen Inhalteanbieter nicht möglich ist. Die Frage, welches technische Verfahren für die betroffenen ISP noch angemessen ist, hängt überdies auch von etwaigen Entschädigungsregelungen ab. Jedenfalls darf der zu wählende technische Ansatz nicht den Charakter der Diensteerbringung verändern.

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

Nach den Ergebnissen der beiden bekannten rechtlichen Analysen kommen technische Zugangshürden auf Access-Ebene nur als Instrument ultima ratio Betracht. Beide Gutachten kommen – mit Ausnahme einer abweichenden Bewertung DNS-basierter Verfahren – zu dem Ergebnis, dass bei Zugangserschwerungen auf Access-Ebene in der Regel ein nicht gesetzlich legitimierter Eingriff in das Fernmeldegeheimnis vorliegt. Je nach juristischer Bewertung beschränkt sich damit der Kreis der denkbaren Verfahren auf DNS-Sperrungen oder deren Implementierung ist rechtlich vollständig ausgeschlossen.

Selbst unter der Annahme der Zulässigkeit einzelner Verfahren lassen sich weitergehende abstrakte Aussagen zur rechtlichen Zulässigkeit von Zugangshürden nur schwer treffen, weil die stets notwendige intensive Verhältnismäßigkeits-Prüfung, wie sie beide juristischen Bewertungen fordern, letztlich nur am Einzelfall entschieden werden kann. Es ist daher insbesondere relevant, zu welchen Inhalten konkret eine Zugangshürde errichtet werden soll und welche Maßnahme hierfür eingesetzt werden muss. BITKOM steht auf dem Standpunkt, dass auf Basis von Verhältnismäßigkeitserwägungen kinderpornografische Inhalte den einzigen denkbaren Anwendungsfall für technische Zugangshürden auf Access-Ebene bilden.

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

Die konkrete Ausgestaltung hängt grundlegend davon ab, welche Rollen den verschiedenen Beteiligten in dem zu installierenden Gesamtverfahren zugeordnet sind. Zu beachten ist zunächst die oben angesprochene Einordnung solcher Verpflichtungen nicht in den Bereich des Jugendmedienschutzes, sondern in den Bereich der Straftaten-Prävention und des Opferschutzes. Diskutiert wurden

bislang behördliche Sperrverfügungen, freiwillige Selbstverpflichtungen, Verträge mit staatlichen Behörden sowie spezifische spezialgesetzliche Regelungen.

Aus Sicht des BITKOM kommt den ISP lediglich die Rolle des rein technischen Umsetzers zu. Sie bewerkstelligen lediglich die technische Realisierung innerhalb eines ansonsten zwingend in der Verantwortung des Staates bzw. seiner dazu bestimmten Behörden anzusiedelnden Verfahrens. Aus diesem Grundverständnis ergeben sich mindestens die folgenden Anforderungen an den notwendigen rechtlichen Rahmen:

- Die notwendige Blacklist muss seitens einer staatlichen Behörde in einem rechtsstaatlichen, ggf. gerichtlichen Verfahren erstellt bzw. bestätigt und gepflegt werden. Die in die Liste aufzunehmenden Inhaltskategorien sind – sinnvollerweise gesetzlich – verbindlich und abschließend festzulegen.
- Ein Verfahren sollte im Idealfall derart automatisiert und professionell ausgestaltet sein, dass seitens des ISP eine persönliche Kenntnisnahme von Listeninhalten durch Mitarbeiter weder nötig noch möglich ist.
- Ein etwaiger Eingriff in das Fernmeldegeheimnis muss ausdrücklich gesetzlich legitimiert sein. In diesem Zusammenhang sollte auch der Bundesbeauftragte für Datenschutz in die Diskussion einbezogen werden.
- Sämtliche Haftungsrisiken auf Seiten des ISP, seien sie strafrechtlicher, öffentlich-rechtlicher oder zivilrechtlicher Natur müssen umfassend abgesichert sein. Zu präferieren ist dabei grundsätzlich eine gesetzliche Privilegierung statt einer vertraglichen Lösung, da letztere zum einen lediglich zu einem schwachen Schutz des ISP über Regressansprüche führt und zum anderen strafrechtliche Verantwortlichkeiten von vorneherein nicht erfasst werden können.
- Um eine unbeabsichtigte öffentliche Verbreitung der Blacklist zu verhindern, sollte die technische Absicherung durch festgelegte Standards festgehalten werden. Hierbei sollte das BSI einbezogen werden.
- Es ist eine Regelung zur Verteilung der Kostenlast bzw. Kompensation zu treffen, soweit die technische Umsetzung absehbar über vernachlässigbare Aufwände hinausgeht.

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?

Hierbei handelt es sich bisher um einen Vorschlag des BMFSJ und anderer, über den derzeit mit den Verbänden und wichtigen Branchenunternehmen intensiv diskutiert wird. Aus Sicht der Unternehmen besteht hier noch Diskussions- und Klarstellungsbedarf. Für den BITKOM ist es ungeachtet der Gesamtausgestaltung einer technischen Zugangshürde unerlässlich, dass die konkrete Suche sowie Indexierung der fraglichen Inhalte durch eine staatliche Behörde - ggf. durch Einbindung von Gerichten - in einem rechtsstaatlich abgesicherten

Verfahren erfolgt. Unabhängig von den anderen zu diskutierenden Parametern ist es für Provider ausgeschlossen, selbst eine solche Listenerstellung vorzunehmen. Dies gilt schon allein aufgrund der strafrechtlichen Relevanz des Abrufes entsprechender Inhalte sowie des Vorhaltens einer entsprechenden Zusammenstellung.

BITKOM betont nochmals mit Nachdruck, dass der ISP im Rahmen der Gesamtsystematik entsprechender Zugangshürden gegen kinderpornografische Inhalte allenfalls die Rolle eines technischen Dienstleisters einnehmen kann, der entsprechend klarer, ggf. zu schaffender rechtsstaatlicher Grundlagen die technische Umsetzung im Auftrag der entsprechenden Behörde vornimmt. Aus dieser Grunderwägung ergeben sich weitere Anforderungen an den rechtlichen Rahmen. Die rein technische Rolle des ISP bedingt insbesondere, dass er haftungsrechtlich vollständig von sämtlichen denkbaren Konstellationen freigestellt werden muss. Dies kann am effektivsten durch einen gesetzlichen Privilegierungstatbestand erfolgen, da eine vertragliche Freistellung durch die entsprechende Behörde als Vertragspartner allenfalls einen Regressanspruch begründen könnte, so dass in der Praxis Durchsetzungsstreitigkeiten drohen.

Zugangshürden, welche das Fernmeldegeheimnis berühren müssen außerdem rechtsstaatlich abgesichert sein. Dies kann aus unserer Bewertung allein durch eine gesetzliche Regelung erfolgen kann. Eine solche Klarstellung ist auch aus rechtspolitischer Sicht wünschenswert und notwendig, um zu verdeutlichen, dass der entsprechende Grundrechtseingriff vom Gesetzgeber nach Abwägung der betroffenen Rechtsgüter als geeignet, erforderlich und angemessen bewertet wird.

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?

In den bislang geführten Gesprächen wurde dem BITKOM ein solcher Vorschlag noch nicht unterbreitet. Die Fragestellung zielt offenbar auf den von der Bundesprüfstelle für jugendgefährdende Medien (BPJM) gepflegten Index ab.

Hierzu ist zunächst zu betonen, dass auf Basis der BPJM-Liste derzeit keinerlei Zugangshürden auf Access-Ebene realisiert werden und sich diese Liste nicht auf kinderpornografische Inhalte bezieht. Eine technische Umsetzung findet aktuell im Bereich Suchmaschinen statt, in welchen die von der BPJM indexierten Inhalte nicht angezeigt werden. Es ist daher zu betonen, dass die Ausdehnung der BPJM-Liste auf kinderpornografische Inhalte mit dem Ziel, auf dieser Basis Zugangserschwerungen auf Access-Ebene zu realisieren eine grundsätzliche Veränderung des Charakters der BPJM-Liste und damit auch der BPJM als Institution zur Folge hätte.

Wir halten dies für nicht sinnvoll. Wie bereits zu Frage 6 dargelegt, ist die Zielrichtung der aktuell diskutierten Maßnahmen eine andere als die Zielrichtung des klassischen Jugendmedienschutzes. Zwar beinhaltet auch die BPJM-Liste strafrechtlich relevantes Material, jedoch kann dies nicht mit der Schwere der

Verbrechen im Bereich Kinderpornografie gleichgesetzt werden. Es bleibt daher aus unserer Sicht unklar, welchen Vorteil die Einbeziehung einer weiteren Institution in ein solches System erbringen soll. Wir sehen in einer solchen Verknüpfung beider Themenkomplexe eher die Gefahr einer Aufweichung der aktuell beabsichtigten klaren Beschränkung technischer Zugangshürden auf den Bereich Kinderpornografie.

Aus Sicht des BITKOM sollte die Listenerstellung und die technische Schnittstelle somit zentral bei einer staatlichen Behörde gebündelt werden.

12. Welche rechtstaatlichen Absicherungen sind darüber hinaus notwendig? Welche Rechtschutzmöglichkeiten müssen vorgesehen werden, beispielsweise bei versehentlicher Sperrung?

Wir verweisen hierzu zunächst auf die Ausführungen zu Frage 9.

Zur Haftungsproblematik sind folgende Konstellationen relevant:

- Ein Listeninhalt ist trotz Umsetzung des festgelegten technischen Verfahrens außerhalb der Verbindungswege zwischen staatlicher Stelle und Unternehmen im Internet oder in sonstiger Weise frei verfügbar – entweder aufgrund der grundsätzlichen Charakteristika des Verfahrens und den darauf folgenden Umgehungsmöglichkeiten oder aufgrund einer technischen Fehlfunktion. Hier droht insbesondere eine strafrechtliche Verantwortlichkeit für Beschäftigte des ISP. Daneben kommt aber auch eine öffentlich-rechtliche Haftung des ISP in Betracht.
- Kinderpornografische Inhalte sind verfügbar, da sie schon nicht Gegenstand der Liste sind. Auch hier bedarf es einer Klarstellung, dass der ISP nicht abseits des zu etablierenden Verfahrens zur Implementierung einer Zugangshürde verpflichtet werden kann.
- Aufgrund der Charakteristika des technischen Verfahrens oder aufgrund einer Fehlfunktion wird der Zugang zu legalen Seiten erschwert, die nicht Gegenstand der Liste sind. Hier drohen zivilrechtliche Ansprüche gegen den ISP.
- Aufgrund nachträglicher Veränderungen von Inhalten oder Versehen bei der Erstellung der Blacklist wird der Zugang zu Inhalten erschwert, die legal sind. Auch hier besteht die Gefahr, dass sich Seitenbetreiber mit Haftungsansprüchen an den ISP wenden.

Für alle beschriebenen Konstellationen bedarf es einer umfassenden Haftungsfreistellung für den ISP bzw. dessen Mitarbeiter. Andernfalls besteht die Gefahr aufgrund der Mitwirkung an Zugangshürden im Sinne eines technischen Dienstleisters rechtlich zur Verantwortung gezogen zu werden.

Gleichzeitig sollte ein formalisiertes Beschwerde- bzw. Rechtsschutzverfahren etabliert werden, welches sicherstellt, dass Betreiber von Seiten, die sich unberechtigterweise von einer Zugangshürde beeinträchtigt sehen, Rechtsschutz gewährt wird. Das entsprechende Verfahren darf nicht bei den ISP, sondern muss bei der zuständigen Behörde angesiedelt werden.

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

Wie bereits oben dargelegt, bildet die Bekämpfung von Kinderpornografie kein klassisch jugendmedienschutzrechtliches Problem, da die Zielrichtung weniger Rezipientenschutz als Kriminalitätsbekämpfung ist. Im Bereich Kinderpornografie stehen also der Opferschutz und die präventive Verbrechensbekämpfung im Vordergrund. Zwar beinhaltet gerade § 4 JMStV einen unmittelbaren Bezug zu strafrechtlich relevanten Inhalten – jedoch geht es auch hier in erster Linie darum, Kinder und Jugendliche vom Konsum entsprechender Medien zu schützen.

Daraus folgt, dass das klassische Jugendschutzrecht nicht der richtige Ansatzpunkt zur Bekämpfung der Kinderpornografie sein kann – insofern sind aus unserer Sicht auch keine Defizite des aktuellen Jugendschutzrechts zu beklagen.

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?

Soweit eine gesetzliche Regelung der Materie für erforderlich gehalten wird, spricht sich BITKOM - auch aus vorgenannten Erwägungen (Frage 13) - grundsätzlich für eine *spezialgesetzliche* Verankerung entsprechender Regelungen aus. Jugendschutzgesetz und Jugendmedienschutzrecht sind aus unserer Sicht aufgrund der schwerpunktmäßig anderen Zielrichtung nicht der geeignete Ansatzpunkt.

Die Frage der gesetzlichen Systematik hängt überdies vom Umfang und Regelungsgehalt einer etwaigen gesetzlichen Regelung ab. Soweit nur Teilaspekte, wie etwa der Eingriff in das Fernmeldegeheimnis oder die Haftung gesetzlich verankert würden, legt dies eine andere gesetzliche Systematik nahe, als bei einer vollständigen gesetzlichen Regelung des gesamten Komplexes.

Die Frage der Gesetzessystematik wird aus Sicht des BITKOM durch folgende Ausgangsüberlegung präjudiziert: Access-Sperrungen bilden grundsätzlich einen tiefgreifenden Eingriff in die Informationsfreiheit sowie in die technische Struktur des Internet. Sie müssen aus diesem Grund in jedem Fall ein Ultima-ratio-Instrument bilden und sind nur bei schwerstkriminellen Inhalten, wie etwa im Bereich Kinderpornografie überhaupt zu rechtfertigen. Hieraus ergibt sich, dass das Instrument der Access-Sperrung nur auf einen engstmöglich begrenzten Kreis von Inhalten angewendet werden darf.

Schon dies spricht dafür, entsprechende Regelungen in einem eigenständigen Spezialgesetz niederzulegen. Dies gilt auch deshalb, da nur durch Regelung in einem Spezialgesetz die konkrete Zielrichtung der angestrebten Eingriffe hinreichend präzise dargelegt werden kann. Insbesondere das Telemediengesetz scheidet daher als gesetzlicher Rahmen für eine etwaige Regelung aus, da das Telemediengesetz seiner Natur nach als Querschnittsmaterie angelegt ist, was

der Ultima-ratio-Funktion Access-bezogener Zugangshürden grundlegend widerspricht.

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?

Die Frage der Kostentragung steht für die Internetwirtschaft angesichts des vorrangigen gemeinsamen Ziels der Zurückdrängung kinderpornografischer Inhalte im Internet nicht im Vordergrund. Allerdings sollte bei der Diskussion um die Umsetzung eines entsprechenden Rahmens darauf geachtet werden, übermäßige Kostenbelastungen möglichst zu vermeiden. Derartige Belastungen drohen insbesondere bei hybriden Verfahren, die technisch sehr komplex sind. BITKOM begrüßt in diesem Zusammenhang das frühzeitige Signal seitens der Bundesfamilienministerin, ggf. Entschädigungslösungen vorzusehen.

In rechtlicher Hinsicht wurde die Frage der Kostentragung ausführlich im Rahmen des von der KJM beauftragten Gutachtens von Prof. Sieber untersucht, so dass weitgehend hierauf verwiesen werden kann. Nach unserem Verständnis hängt daher die Frage einer rechtlichen Entschädigungspflicht des Staates stark davon ab, wie intensiv die Belastung der ISP konkret ist. Wir weisen in diesem Zusammenhang auch auf die jüngst ergangenen verwaltungsgerichtlichen Entscheidungen im Bereich der Vorratsdatenspeicherung hin, wonach aus einer fehlenden Regelung zur Kostenerstattung die Unzumutbarkeit einer Inanspruchnahme folgen kann.[4]

Die Frage einer angemessenen Entschädigungsregelung sollte daher aus Sicht des BITKOM ein Diskussionspunkt bei der Schaffung des notwendigen rechtlichen Rahmens für technische Zugangshürden sein. Entschädigungsregelungen sollten im Ergebnis eingreifen, wenn die konkret von ISP umzusetzenden Maßnahmen absehbar eine mehr als geringfügige Belastung zur Folge haben.

[4] S. zuletzt VG Berlin - Az.: VG 27 A 321.08. Hierzu Heise-Online vom 3. Februar 2009: http://www.heise.de/newsticker/QSC-speichert-Internetdaten-nicht-auf-Vorrat--/meldung/126797.