Bundeskriminalamt

POSTANSCHRIFT Bundeskriminalamt · 65173 Wiesbaden

HAUSANSCHRIFT Thaerstraße 11, 65193 Wiesbaden
POSTANSCHRIFT 65173 Wiesbaden

TEL
FAX
BEARBEITET VON
E-MAIL
AZ
DATUM 09.02.2009

BETREFF Öffentliches Expertengespräch des Unterausschusses Neue Medien am 12.02.09

BEZUG Einladung des Vorsitzenden des Unterausschusses Neue Medien vom 26.01.09

Zu dem mit der o. g. Einladung des Vorsitzenden des Unterausschusses Neue Medien übermittelten Fragenkatalog nimmt das Bundeskriminalamt wie folgt Stellung:

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?*

   Eine solche Sperrung des Zugriffs auf entsprechende Inhalte kann grundsätzlich auf drei verschiedenen technischen Ebenen erfolgen. Diese sind

   a) der Computer des Nutzers,

   b) der Computer des Anbieters (Host) und

   c) das für den Abruf solcher Inhalte genutzte Verbindungsnetz (Internet).

   zu a) Auf dem Computer des Nutzers würde eine Sperrung z. B. durch Filterung in der Anwendungssoftware (z. B. dem Web-Browser) oder im Betriebssystem erfolgen. Solche Mechanismen sind bereits heute (kommerziell) verfügbar, um etwa die Nutzung des Internets durch Kinder zu beschränken. Für die Sperrung auf dem Computer

des Nutzers müssen regelmäßig aktuelle Listen dem Computer des Nutzers zur Verfügung gestellt werden, damit dieser den Zugriff auf die relevanten Seiten sperren kann. Dazu müssten möglichst alle Computer über standardisierte Mechanismen zur Sperrung und Verarbeitung der Sperrlisten verfügen, wofür die Anpassung der Anwendungssoftware oder des Betriebssystems erforderlich ist.
Eine Sperrung auf dem Computer des ist wegen der Möglichkeit ihrer Umgehung, der Schwierigkeit einer kurzfristigen Umsetzung und wegen des zu betreibenden Aufwands als Lösung eher ungeeignet.

zu b) Die Löschung von Internet-Inhalten auf Seiten des Anbieters erscheint als technisch beste Methode zur Unterbindung des Angebotes. Da viele der entsprechenden Inhalte jedoch aus dem außereuropäischen Ausland angeboten werden und Deutschland darauf nur eingeschränkt Einfluss nehmen kann (Rechtshilfe), scheidet diese Möglichkeit zumindest als kurz- bis mittelfristige Lösung aus.

zu c) Eine Sperrung des Zugangs im Rahmen der technischen Möglichkeiten des Internets erscheint derzeit am schnellsten und effizientesten realisierbar. Allerdings bestehen auch hier Umgehungsmöglichkeiten, die Zugangsanbieter können mit zusätzlichen Kosten belastet werden und möglicherweise kann die Effizienz und Integrität der Datenübertragung im Internet eingeschränkt werden. Dabei gibt es drei geläufige Ansätze:

- **Sperrung der Internet-Adresse (IP-Adresse)**

Die IP-Adresse im Internet hat eine ähnliche Funktion wie eine Telefonnummer. Die IP-Adresse bezeichnet zum einem einen Computer im Internet, zum anderen beschreibt sie aber auch den Weg, wie Daten von einem Quell- zu einem Zielcomputer vermittelt werden. Der Fachbegriff für die Vermittlung im Internet ist *Routing*. Die Sperrung auf Ebene der IP-Adresse würde typischerweise an den *Routern* ansetzen und diese z. B. veranlassen, den Datentransport zu einer gesperrten IP-Adresse abzulehnen.
Eine IP-Adresse kann einzelne Computer, aber auch ganze Computernetzwerke bezeichnen, deren Computer über eine einzige IP-Adresse erreicht werden können, ähnlich wie einer Telefonanlage eine einzige Telefonnummer zugeordnet sein kann.
Sperrt man im letzteren Fall ein ganzes Computernetzwerk, so werden neben den zu sperrenden Inhalten möglicherweise auch zahlreiche legale Inhalte und Dienste innerhalb dieses Netzwerks gesperrt. Bei großen Web-Hostern käme ein solches Vorgehen einer Stilllegung des Betriebs gleich, die in Regel als unverhältnismäßig anzusehen wäre.

➢ Sperrung über das Domain Name System (DNS)

Das Domain Name System ist funktional vergleichbar mit einem Telefonbuch. Über DNS werden leicht zu merkende Adressbezeichnungen (www.bmi.bund.de), so genannte Domainnamen, in schwer zu merkende dafür aber technisch verarbeitbare IP-Adressen (77.87.229.1) aufgelöst.
Ebenso wie die Löschung eines Teilnehmers aus einem Telefonbuch nicht zur Sperrung seines Telefonanschlusses führt, kann auf Inhalte (z. B. einer Web-Seite) auch nach einer Löschung oder Veränderung des DNS-Eintrags nach wie vor zugegriffen werden, wenn die IP-Adresse des Computers mit den inkriminierten Inhalten bekannt ist.
Der Zugang zu einem DNS-Server wird von den Internetzugangsanbietern zumeist gemeinsam mit dem Internetzugang angeboten. In den Ländern, die das Access Blocking auf Ebene des DNS durchführen, werden die Tabellen der DNS-Server der großen Zugangsanbieter modifiziert, so dass bei Aufruf einer gesperrten Seite dem Nutzer ein Hinweis gegeben wird, das der vom Nutzer angeforderte Inhalt kinderpornographisches Material enthält. Im DNS wird also zu dem Domain-Namen statt der ursprünglichen IP-Adresse die IP-Adresse einer entsprechenden Hinweisseite hinterlegt.
Eine der Umgehungsmöglichkeiten der DNS-basierten Sperrung besteht daher in der Nutzung „freier DNS-Server“ im Ausland, auf denen die auf deutschen DNS-Servern durch Umleitung gesperrten Seiten nicht entsprechend gesperrt sind.
Im Gegensatz zur vorangehend genannten Sperre von IP-Adressen lässt die DNS-basierte Sperre eine gezieltere Auswahl der zu sperrenden Inhalte zu. So verwenden z. B. große Web-Hoster so genannte Subdomains, um ihren Nutzern möglichst individuelle Domainnamen zu ermöglichen (z.B. im Bereich des Bundes: bmi.bund.de; bmj.bund.de; bmf.bund.de – „bmi“, „bmj“ und „bmf“ sind Subdomains von „bund.de“). Eine Vielzahl von Subdomains verweist dabei auf eine kleine Menge von IP-Adressen eines Web-Hosters (so könnten z. B. die Internettauftritte des BMI und des BMJ unter einer einzigen IP-Adresse vorgehalten werden). Würden diese IP-Adressen gesperrt, wäre, wie vorangehend ausgeführt, kein Nutzer des Web-Hosters mehr erreichbar. Der Vorteil der Sperrung auf DNS-Ebene ist also im Gegensatz zur Sperrung der IP-Adresse, dass nur die Inhalte des Nutzers eines Web-Hosters der auch illegale Inhalte anbietet, gesperrt werden.

➢ Sperrung über den Uniform Resource Identifier (URI)

Einzelne Ressourcen im Internet werden über einen URI gekennzeichnet. Bei diesen Ressourcen handelt es sich beispielsweise um Web-Seiten, Bilder usw. So steht etwa

der URL[1] http://www.bundestag.de/layout/bilder/logo.gif für das Logo des Deutschen Bundestages auf seiner Homepage. Auch Dienste wie Email, Filetransfer, Newsfeed usw. werden über den URI benannt. Der URI ist somit eine der genauesten Möglichkeiten, um illegale Internet-Inhalte zu bezeichnen und nachfolgend zu sperren.
Aufgrund des technischen Aufbaus des Internets ist eine Filterung auf Ebene von URIs sehr aufwendig und würde, falls flächendeckend eingeführt, zum Zusammenbruch des Internets führen. Daher hat man sich z. B. in GBR entschlossen, ein Hybridverfahren einzusetzen, das wie ein mehrstufiges Sieb arbeitet. Im ersten Schritt werden IP-Adressen mit potentiell zu sperrenden Inhalten mit Hilfe einer Liste identifiziert. Die an diese IP-Adressen gesendeten Daten werden in einem zweiten Schritt näher analysiert und falls sie an eine zu sperrende URI bzw. URL gerichtet sind, wird die Verbindung oder der Datentransport abgebrochen. Eine Umleitung auf eine Hinweisseite wäre ebenfalls möglich.
Die Methode ist sehr zielsicher und beschränkt den Zugang zu nicht zu sperrenden Inhalten minimal im Vergleich zu den vorangehend genannten Sperrverfahren. Allerdings ist die hybride Technik bei bestimmten verschlüsselten Internetverbindungen wirkungslos.

Fazit:

Die unter c) genannten Sperrverfahren erfordern Eingriffe in die Weiterleitungs- und Vermittlungsstrukturen des Internets. Diese Eingriffe verlangen Investitionen auf Seiten der deutschen Netzbetreiber. Ob die Eingriffe zu Sicherheitslücken oder Betriebsstörungen im deutschen Teil des Internet führen können, bedarf der weiteren Prüfung.
Keines der vorgestellten Verfahren bietet hohe Umgehungssicherheit, so dass voraussichtlich nur der „normale Nutzer“ am Zugang zu illegalen Inhalten gehindert wird, nicht jedoch derjenige, der den Zugang gezielt sucht.
Eine Filterung[2] auf Ebene der IP-Adresse ist dabei technisch eher einfach herzustellen, da die Analyse der IP-Adresse und die darauf aufbauende Entscheidung, an welchen Router die Daten weitergeleitet werden, bereits Bestandteil der Datenvermittlung im Internet (Routing) ist. Aufgrund der damit verbundenen Nachteile für Nichtbetroffene (Sperrung auch anderer Inhalte) begegnet dieses Vorgehen allerdings Bedenken.

---

[1] Ein Uniform Resource Locator ist eine Unterkategorie der URI

[2] Filtern bedeutet hier eine IP-Adresse mit einer „schwarzen Liste“ abzugleichen und bei Übereinstimmung den Datenverkehr abzubrechen. Routing bedeutet eine IP-Adresse mit einer Routingliste abzugleichen und die Daten an die in der Routingliste bezeichnete Netzwerkverbindung weiterzuleiten.

Bezogen auf kinderpornografische Inhalte werden in einer Reihe von Staaten die oben beschriebene DNS-Sperre, in Großbritannien die sog. Hybride Sperrtechnik eingesetzt.

Es liegen folgende Erfahrungswerte aus dem Ausland vor:
In Norwegen, wo auf Vertragsbasis zwischen polizeilicher Zentralstelle und Internetserviceprovidern (ISP) seit 2004 Sperrungen über DNS-Server erfolgen, werden arbeitstäglich 15.000 – 18.000 Zugriffsversuche auf kinderpornografische Webseiten gesperrt.

Nach Mitteilung der dänischen kriminalpolizeilichen Zentraldienststelle hat der größte dänische Provider bei Implementierung der technischen Voraussetzungen für eine dem norwegischen Modell entsprechende Zugangssperrung ca. 40.000 Euro aufgewendet. In Dänemark erfolgt Access-Blocking kinderpornografischer Webseiten seit 2005.

In Großbritannien sind nach hier vorliegenden Informationen im Jahr 2006 täglich 35.000 Zugriffe auf kinderpornografische Webseiten abgewehrt worden.

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

Der Missbrauch verfügbarer Sperrtechnologien sowie die versehentliche Sperrung rechtmäßiger Inhalte lassen sich nicht völlig ausschließen. Durch eine möglichst präzise Bestimmung der zu sperrenden Inhalte kann diese Gefahr jedoch eingedämmt werden. Nach derzeitigen Vorstellungen sollen Verträge zwischen dem Bundeskriminalamt und den einzelnen Internetserviceprovidern geschlossen werden, die die Sperrung des Zugangs ausschließlich zu kinderpornografischen Webseiten zum Gegenstand haben. Dabei soll die Bewertung, ob eine Webseite kinderpornographische Inhalte umfasst und damit die Festlegung der zu sperrenden Seiten durch das Bundeskriminalamt erfolgen, während die Sperrung als solche von den ISP vorgenommen wird.

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?

Um das Bekanntwerden der Listen nach Möglichkeit zu verhindern, soll in Verträgen zwischen Bundeskriminalamt und Providern u.a. die Nutzung von Verschlüsselungstechniken und eine Begrenzung des damit befassten Personenkreises festgeschrieben werden.

Nach Aussage des Vertreters einer skandinavischen polizeilichen Zentraldienststelle ist nach dortiger Überzeugung davon auszugehen, dass die in Skandinavien in die Öffentlichkeit gelangte Liste nicht durch einen mit deren Umgang Betrauten bekannt gegeben worden ist. Es sei davon auszugehen, dass die in die Öffentlichkeit gelangte Liste rückwärts generiert worden ist, zum Zeitpunkt der Veröffentlichung aber bereits veraltet gewesen sei.

Da die entsprechenden Inhalte in der Regel sehr „flüchtig“ sind, also nur kurze Zeit unter einer URI (Uniform Resource Identifier) vorgehalten werden, sind die Gefahren, die von der Veröffentlichung einer rückwärts generierten Liste ausgehen, begrenzt.

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?

Zu den Kosten wird auf die Antwort zu 1. verwiesen. Die Kostenabschätzung des BMFSFJ basiert auf der Aussage der dänischen polizeilichen Zentralstelle.

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

Die Erfahrungen der Staaten bezüglich der Wirksamkeit derartiger Sperren sind nach Auskunft der zuständigen kriminalpolizeilichen Zentraldienststellen positiv und werden seitens des Bundeskriminalamtes entsprechend bewertet. Hinsichtlich der Anzahl der gesperrten Zugriffsversuche wird auf die Ausführungen zu 1. verwiesen. Darüber hinaus hat es nach Auskunft der zuständigen norwegischen und dänischen kriminalpo-

lizeilichen Zentraldienststellen dort bislang nur in ganz vereinzelten Fällen Beschwerden gegen die vorgenommenen Sperrungen gegeben, was für die Zielgenauigkeit und Akzeptanz der durchgeführten Sperrmaßnahmen spricht.

Recht:

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

Die Internetserviceprovider in Deutschland wie in Europa haben wie alle Wirtschaftsbeteiligten grundsätzlich die Möglichkeit, ihre Geschäftsaktivitäten unter Berücksichtigung bestehender gesellschaftspolitischer Zielsetzungen zu gestalten. Dies gilt natürlich auch für die Sperrung des Zugriffs auf kinderpornographische Internetseiten. Jedenfalls in Deutschland haben die Internetserviceprovider hiervon bislang keinen Gebrauch gemacht. Zu den im europäischen Ausland bestehenden Instrumenten der Selbstregulierung kann das Bundeskriminalamt keine abschließende Bewertung abgeben. In einer Reihe von anderen europäischen Staaten wird Access Blocking jedenfalls nicht allein auf der Grundlage freiwilliger Selbstverpflichtungen durchgeführt, sondern auf der Basis von Verträgen bzw. gesetzlichen Bestimmungen.

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

Die unter 1. Buchstabe c) genannten Sperrmaßnahmen sind nach hiesiger Einschätzung **verfassungsrechtlich grundsätzlich zulässig**.

Zwar kann in der Sperrung einer Internetseite ein Eingriff in die Informationsfreiheit der Nutzer liegen (Art. 5 Abs. 1 Satz 1 GG), da diese die entsprechenden Seiten nicht mehr aufrufen können. Dieser Eingriff wäre jedoch gerechtfertigt. Das Recht auf Informationsfreiheit wird durch die Schranke der allgemeinen Gesetze nach Artikel 5 Abs. 2 GG sowie durch andere Wertentscheidungen des Grundgesetzes begrenzt. Die

Verbreitung kinderpornographischer Inhalte im Internet stellt eine massive Verletzung der Menschenwürde der betroffenen Kinder dar. Die Sperrung solcher Inhalte dient folglich dem Schutz eines überragend wichtigen Rechtsguts. An dem Empfang von kinderpornographischem Material kann dagegen kein schützenswertes Interesse bestehen, so dass die Meinungsfreiheit demgegenüber zurücktreten muss. Gleiches gilt im Hinblick auf die Kommunikationsfreiheit des Anbieters entsprechender Inhalte.

Auch handelt es sich bei der in Aussicht genommenen Sperrung kinderpornographischer Inhalte um keine nach Art. 5 Abs. 1 Satz 3 GG unzulässige Zensur. Literatur und Rechtsprechung sind sich darin einig, dass hierunter zunächst die so genannte Vorzensur zu verstehen ist (vgl. BVerfGE 87, 209, 230), eine Nachzensur sollte vom Verfassungsgeber nicht ausgeschlossen werden. Vorzensur ist bereits dem Wortlaut nach ein staatliches Eingreifen vor der eigentlichen Veröffentlichung. Hier geht es indessen um die Sperrung des Zugangs zu bereits existierenden Angeboten im Internet. Nach der Definition des Bundesverfassungsgerichts liegt keine Vorzensur mehr vor, wenn „das Geisteswerk erst einmal an die Öffentlichkeit gelangt“ ist und Wirkungen auszuüben vermag (BVerfGE 33, 52, 72). Die fraglichen Internetseiten haben ihre Öffentlichkeit bereits gefunden, was nicht zuletzt dadurch dokumentiert ist, dass sie auf der Sperrliste des Bundeskriminalamtes geführt werden. Eine nach Art. 5 Abs. GG unzulässige Vorzensur liegt aus diesem Grund bereits nicht vor (VG Köln Urteil vom 3. März 2005, Juris, Rn. 78; Dietlein/Heinemann, K&R 2004, 418, 421; im Ergebnis ebenso OVG NW Beschluss vom 19. März 2003, Juris, Rn. 29 *Greiner*, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, S. 144f).

Hiesigen Erachtens liegt auch kein **Eingriff in das Fernmeldegeheimnis der Nutzer aus Art.10 Abs. 1 GG** vor. Nach Auffassung von *Sieber* greifen Sperrtechnologien in das Grundrecht aus Art. 10 Abs. 1 GG ein, soweit sie die vom Nutzer übermittelten IP-Adressen, Port-Nummern und URls analysieren. In der Rechtsprechung ist ein Eingriff in Art. 10 Abs. 1 GG dagegen bisher nicht angenommen worden.

Grundsätzlich schützt Art. 10 GG nicht nur den Inhalt der Telekommunikation, sondern auch die näheren Umstände der Telekommunikation (st. Rspr., vgl. etwa BVerfGE 107, 299, 312). Dazu gehört insbesondere, ob, wann und wie oft zwischen wel-

chen Personen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist. Daher kann grundsätzlich jede Kenntnisnahme von Daten, die einen Rückschluss auf eine von Art. 10 GG geschützte Telekommunikation zulässt, ein Eingriff in Art. 10 Abs. 1 GG darstellen. Hiervon sind allerdings zwei Ausnahmen zu machen:

- Zunächst ist **umstritten, wie weit der Schutzumfang Art. 10 GG im Bereich des Internet reicht**. Während für den Bereich der Individualkommunikation dies mittlerweile zwar unstreitig der Fall ist (daher ist die Überwachung eines Voice over IP-Gesprächs ein Eingriff in Art. 10 GG, vgl. BVerfG Urteil vom 27. Februar 2008, Rn. 190), ist dies für den Fall der Massekommunikation im Internet (etwa dem Aufruf einer Website mit allgemeinen Informationen) umstritten, da es hier an einer Kommunikation zwischen zwei (oder mehreren) Personen fehlt. Zum Teil wird daher vertreten, auf die Differenzierung von Individual- und Massenkommunikation vollständig zu verzichten, da anderenfalls der Staat erst unter Umständen in Art.10 GG eingreifen müsste, um festzustellen, ob dieser einschlägig ist (so auch *Sieber* in seinem Gutachten). Aus hiesiger Sicht sollte indes an der grundsätzlichen Unterscheidung zwischen Individual- und Massenkommunikation festgehalten werden (ebenso *Löwer*, in: *von Münch/Kunig*, GG, Art. 10, Rn. 18; *Pagenkopf*, in: Sachs, GG, Art. 10, Rn. 14a; *Badura*, in: BK, GG, Art. 10 fordert einen individuellen Kommunikationsvorgang“ und auch das BVerfG hat in seinem Urteil vom 27. Februar 2008 ausgeführt, „Die Gewährleistung des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG schützt die unkörperliche Übermittlung von Informationen an *individuelle Empfänger* mit Hilfe des Telekommunikationsverkehrs“, Rn. 182), um den Schutzbereich des Art.10 GG nicht übermäßig auszudehnen. Es ist daher abzulehnen, dass Fernmeldegeheimnis auf alle telekommunikationstechnischen Übertragungswege (und damit das Internet insgesamt) zu erstrecken, nur weil hierauf möglicherweise individuelle Kommunikationswege abgewickelt werden können (so aber *Seitz*, Strafverfolgungsmaßnahmen im Internet, S. 258 m.w.N.). Auch das Bundesverfassungsgericht hat im Zusammenhang mit dem Einsatz des IMSI-Catchers von der Erforderlichkeit des Personenbezugs einer Kommunikation gesprochen (BVerfG Beschluss vom 22. August 2006). Der bloße Aufruf einer Seite im Internet ist daher nicht durch Art. 10 Abs.

1 GG geschützt. Kommt es daher zu einer Sperrung, die an Daten aus Massenkommunikationsvorgängen anknüpft, ist bereits aus diesem Grund zweifelhaft, ob hierdurch in Art. 10 GG eingriffen werden kann.

Das Gegenargument, dass es auf eine Unterscheidung zwischen Individual- und Massenkommunikation nicht ankommen könne, weil hierzu bereits eine Auswertung der Nachrichteninhalte erforderlich sei (so *Sieber*, Sperrverfügungen im Internet, S. 80f), übersieht, dass das Bundesverfassungsgericht selbst in der Frage, ob Daten (noch) von Art. 10 Abs. 1 GG geschützt sind, danach unterscheidet, ob der Kommunikationsvorgang abgeschlossen ist (BVerfGE 115, 166ff). Eine solche Feststellung wird sich aber oftmals erst bei und nach einem Zugriff auf diese Daten feststellen lassen. Gleichwohl hat das Bundesverfassungsgericht davon abgesehen, diese Daten insgesamt und pauschal dem Schutz des Art. 10 Abs. 1 GG zu unterstellen.

- Zudem stellt sich die **Frage der Eingriffsqualität einer Analyse der entsprechenden Daten**. Zwar erstreckt sich die Schutzwirkung von Artikel 10 GG grundsätzlich auf den gesamten Prozess der Informations- und Datenverarbeitung, der die erlangten Daten betrifft. Art. 10 GG entfaltet seine Schutzwirkungen schon in einem frühen Stadium des technischen Übertragungsvorgangs: Nicht erst die Kenntnisnahme vom Inhalt der Kommunikation oder Kommunikationsumstände kann einen Eingriff in das Grundrecht beinhalten, sondern schon die Erfassung der Daten selbst (vgl. BVerfGE 100, 313, 366 – G 10). Auch jeder weitere Datenverarbeitungsprozess, der sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließt und in dem Gebrauch von den erlangten Kenntnissen gemacht wird, stellt einen eigenständigen Eingriff in das durch Artikel 10 GG geschützte Grundrecht dar (BVerfGE 100, 313, 359; 110, 33, 68f.; 113, 348, 365).

  Eine Ausnahme hiervon ist aber anzunehmen, wenn Telekommunikationsvorgänge **ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Signalaufbereitung technisch wieder spurenlos ausgesondert werden** (BVerfGE 100, 313, 366; 107, 299, 328; ähnlich zur Erfassung von durch Ar-

tikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG geschützten Daten: BVerfGE 115, 320, 343f. – Rasterfahndung; BVerfG Urteil vom 11. März 2008, Rn. 68 – Automatisierte Kennzeichenerfassung). Das Bundesverfassungsgericht hat damit für bestimmte Fallgestaltungen anerkannt, dass es hinsichtlich solcher Datenverarbeitungsvorgänge an einem Grundrechtseingriff fehlt.

In der bloßen **Verhinderung des Zugangs** zu einer bestimmten Information (der Seite mit kinderpornographischem Inhalt) liegt ohnehin kein Eingriff in Art. 10 Abs. 1 GG (*Jarass*, in: *Jarass/Pieroth*, GG, Art. 10, Rn. 12 m.w.N.; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, S. 445).

Zur Frage der Wirksamkeit wird auf die Antwort zu Frage 1 verwiesen.

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

Die Inanspruchnahme inländischer Zugangsanbieter auf Sperrung des Zugangs zu bestimmten Webseiten, die inkriminierte Inhalte zum Gegenstand haben, ist bereits nach geltendem Recht auf der Grundlage von § 20 Abs. 4 des Staatsvertrags über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien (Jugendmedienschutz-Staatsvertrag –JMStV) i.V.m. § 59 Abs. 4 des Staatsvertrags für Rundfunk und Telemedien (Rundfunkstaatsvertrag – RStV) und § 59 i.V.m. § 54 Abs. 1 RStV sowie unter bestimmten Voraussetzungen auf der Grundlage der Generalklausel der Polizeigesetze der Länder möglich. Allerdings ist dieses Verfahren recht umständlich und zeitaufwändig, weshalb es sich beim Vorgehen gegen die Verbreitung der sehr flüchtigen kinderpornographischen Inhalte im Internet als nicht ausreichend erwiesen hat (s. hierzu im Einzelnen die Ausführungen zu 13.). Es wird derzeit nach wirksameren Methoden gesucht, um die Verbreitung entsprechender Inhalte im Internet entgegenzuwirken. Die derzeitigen Überlegungen beschränken sich dabei auf die Sperrung kinderpornographischer Inhalte im Sinne von § 184b StGB. Die oben unter 1. c) beschriebene Sperrung auf Ebene des Internet kann nur durch den Internet Servi-

ce Provider (ISP) vorgenommen werden. Eine solche Sperrmaßnahme könnte beispielsweise auf entsprechende Regelungen in den AGB des ISP für die Vertragsbeziehungen mit seinen Kunden in Verbindung mit einem öffentlich-rechtlichen Vertrag gestützt werden. Ferner käme die Schaffung einer spezifischen gesetzlichen Rechtsgrundlage in Betracht, die den Besonderheiten des ins Auge gefassten Verfahrens Rechnung trägt.

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

Zunächst gilt es, die zu sperrenden Inhalte präzise zu definieren. Ferner sollten Mindeststandards in Bezug auf die zu verwendende Sperrtechnik festgelegt werden. Schließlich müssen die Verantwortlichkeiten auch unter haftungsrechtlichen Gesichtspunkten klar bestimmt werden. Derzeit wird unter Federführung des BMFSFJ und Einbeziehung weiterer Bundesministerien und des Bundeskriminalamtes mit Providern unter Beteiligung von Verbänden mit dem Ziel des Abschlusses von Verträgen i.S. der Antwort zu Frage 8 verhandelt. Wesentliche Eckpunkte des Vertrages werden neben der Begrenzung auf Kinderpornografie i.S. von § 184 b StGB die Pflichten der Provider und des Bundeskriminalamt sowie Aspekte der konkreten Durchführung und Zusammenarbeit sein.

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?*

Das Bundeskriminalamt unterstützt als Zentralstelle die Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder sonst erheblicher Bedeutung. Grundlage für die Wahrnehmung dieser Aufgabe ist § 2 Abs. 1 BKAG. Beim Bundeskriminalamt läuft in Wahrnehmung dieser Aufgabe schon heute eine Vielzahl von Informationen zu strafbaren Inhalten im Internet, insbesondere auch zu kinderpornographischen Inhalten zusammen. Zum Teil gewinnt das Bundeskriminalamt seine Erkenntnisse aus eigenen Nachfor-

schungen im Netz, teilweise erhält es aber auch Hinweise von anderen Polizeidienststellen im In- und Ausland sowie aus der Bevölkerung. Die so gewonnenen Erkenntnisse zu kinderpornographischen Inhalten im Internet wird das Bundeskriminalamt den derzeitigen Planungen nach künftig in einer „Sperrliste“ zusammenführen und den ISP als Grundlage für die von ihnen durchzuführenden Sperrmaßnahmen zur Verfügung stellen.

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 Bundesprüfstelle für jugendgefährdende Medien (BPjM) indiziert nach dem Jugendschutzgesetz Träger- oder Telemedien, die jugendgefährdend sind. Ziel des Indizierungsverfahrens ist es, Kinder und Jugendliche vor jugendgefährdenden Medieninhalten zu schützen, nicht jedoch den Zugang zu diesen Inhalten gänzlich zu sperren.

Für Webseiten mit kinderpornographischen Inhalten gilt demgegenüber § 184 b des Strafgesetzbuchs (StGB). Mit umfassenden Verbreitungs- sowie Besitzverschaffungs- und Besitzverboten soll der Markt für kinderpornographische Produkte ausgetrocknet werden. Dieses Ziel ist mit einer (zusätzlichen) Indizierung durch die BPjM nicht zu erreichen.

Ausländische jugendgefährdende Internetangebote, die von der BPjM indiziert werden, werden in das so genannte „BPjM-Modul“ eingestellt. Um Kindern und Jugendlichen den Zugang zu verwehren, kann dieses Modul z. B. in nutzerautonome Filterprogramme für jugendbeeinträchtigende Inhalte integriert werden. Die Nutzer kinderpornographischer Webseiten dürften jedoch gerade kein Interesse an der Implementierung entsprechender Filterprogramme auf ihrem Rechner haben, so dass die Aufnahme kinderpornographischer Webseiten in das „BPjM-Modul“ insofern leer laufen würde. Zudem ist die Zeitspanne zwischen der Anregung zur Indizierung und der tatsächlichen Indizierung, Aufnahme in das „BPjM-Modul“ und nutzerseitigen Aktualisierung des Moduls in Anbetracht der Kurzlebigkeit der entsprechenden Webseiten zu

groß (kommerzielle kinderpornographische Webseiten sind in der Regel nur wenige Tage unter der gleichen Adresse verfügbar).

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

Zunächst ist für ein hohes Maß an Transparenz zu sorgen, weshalb die Anzeige einer sog. „Stoppseite“ geplant ist, auf der der Grund (kinderpornografischer Inhalt im Sinne des §184 b StGB) für die Sperrung angegeben. und eine E-Mail-Adresse des Bundeskriminalamtes aufgeführt werden soll, an die sich der Betroffene wenden kann, wenn er der Auffassung ist, dass die Sperrung des Zugriffs zu Unrecht erfolgt ist. Auch betroffene Anbieter können sich zur Klärung an das Bundeskriminalamt wenden. Das Bundeskriminalamt prüft sodann, ob die Sperrung zu Recht erfolgt ist. Sollte sich herausstellen, dass dies nicht der Fall ist, wird der Fehler unverzüglich behoben und der Beschwerde damit abgeholfen. Darüber hinaus kann der Betroffene den Zivilrechtsweg beschreiten, um gegen eine Sperrmaßnahme eines ISP vorzugehen. Gegen die Aufnahme einer Internetseite auf die vom BKA geführte Sperrliste steht zudem der Verwaltungsrechtsweg offen. Weitere rechtsstaatliche Absicherungen bedarf es h. E. nicht.

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

Auch heute schon ist die Inanspruchnahme inländischer Zugangsanbieter auf Sperrung des Zugangs zu bestimmten Webseiten, die inkriminierte Inhalte zum Gegenstand haben, möglich. Als Rechtsgrundlage kommt hierfür vorrangig § 20 Abs. 4 des Staatsvertrags über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien (Jugendmedienschutz-Staatsvertrag –JMStV) i.V.m. § 59 Abs. 4 des Staatsvertrags für Rundfunk und Telemedien (Rundfunkstaatsvertrag – RStV) sowie § 59 i.V.m. § 54 Abs. 1 RStV in Betracht sowie unter bestimmten Voraussetzungen die Generalklausel der Polizeigesetze der Länder.

Das gegenwärtige Verfahren ist jedoch dadurch gekennzeichnet, dass es des gesonderten Erlasses eines Verwaltungsaktes, nämlich der Sperrverfügung, gegenüber jedem einzelnen in Deutschland ansässigen Internet-Zugangsanbieter bedarf. Dieses Verfahren ist umständlich und zeitraubend, zumal jede einzelne dieser Sperrverfügungen der vollen verwaltungsgerichtlichen Kontrolle mit allen Folgen (aufschiebende Wirkung der Rechtsmittel, die das Gericht ggf. auch wiederherstellen kann, jahrelange Prozesse in mehreren Instanzen) unterliegt. Es trägt damit nach Expertenansicht, die sich auch auf Erfahrungen aus früheren einzelnen Verfahren stützen kann, der Tatsache, dass die inkriminierten Seiten unter der betreffenden Internet-Adresse nicht selten nur kurze Zeit (häufig nur wenige Tage) im Netz eingestellt sind, nicht ausreichend Rechnung.

Erforderlich ist daher eine spürbare Verfahrensverkürzung und -beschleunigung: Statt des herkömmlichen Erlasses einer Sperrverfügung als Verwaltungsakt i.S.v. § 35 VwVfG soll es künftig ausreichen, dass eine autorisierte Stelle – das BKA – als Hinweis-, Sammel- und Prüfzentrale für Deutschland fungiert, aus seinen Prüfergebnissen Listen sperrwürdig erachteter Webseiten erzeugt und diese zeitnah elektronisch an die Zugangsanbieter übermittelt. Diese setzen die erhaltenen Informationen unverzüglich in technische Sperrmaßnahmen um. Auf diese Weise könnte durch die Polizei und Zugangsanbieter sehr aktuell und flexibel auf neue Erkenntnisse reagiert werden.

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?*

Ergänzend zu den obigen Ausführungen ist festzustellen, dass die Frage ob und wo eine gesetzliche Regelung erfolgen müsste, durch die zuständigen Ressorts zu entscheiden ist. Nach Auffassung des Bundeskriminalamtes könnte eine Regelung im Telemediengesetz ggf. auch im Telekommunikationsgesetz erfolgen.

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?

Derzeit wird der Abschluss eines Vertrags zwischen ISP und Bundeskriminalamt über die Zusammenarbeit bei der Sperrung kinderpornographischer Inhalte diskutiert. Hierbei handelt es sich also nicht um eine Inanspruchnahme als Nichtstörer. Die Frage der Kostentragung ist jedoch auch in diesem Zusammenhang noch nicht abschließend geklärt.

Im Auftrag
Maurer [gez. 09.02.09]