DEUTSCHER BUNDESTAG
16. Wahlperiode
Ausschuss für Wirtschaft
und Technologie

Ausschussdrucksache **16(9)1546**
25. Mai 2009

FREY RECHTSANWÄLTE

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

Deutscher Bundestag
Ausschuss für Wirtschaft
und Technologie

Platz der Republik 1
11011 Berlin

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

*Fachanwalt für Urheber- und Medienrecht

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

Köln, den 22. Mai 2009

Aktenzeichen: (09)K651
(Bitte bei Schriftverkehr angeben)

Stellungnahme

zum

Entwurf eines Gesetzes zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen (BT-Drucksache 16/12850)

Die Bundesregierung hat am 22. April 2009 den Entwurf eines Gesetzes zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen verabschiedet. Mit der vorliegenden Stellungnahme nehmen wir zu den Regelungen dieses Gesetzentwurfs Stellung. Vorab möchten wir – zur Vermeidung von Wiederholungen –auf unsere bereits im Februar 2009 unterbreitete Stellungnahme für den Unterausschuss Neue Medien zum Thema Kinderpornographie im Internet verweisen (http://www.bundestag.de/ausschuesse/a22/a22_nm/oeffentliche_Sitzungen/a22_uanm_to24/Stellungnahmen/Frey.pdf). Dort haben wir eine Reihe allgemeiner Anmerkungen angebracht, die auch für das vorliegende Gesetzgebungsverfahren von Bedeutung sind. Insbesondere haben wir bereits im Februar empfohlen, eine klare gesetzliche Sonderregelung im Zusammenhang mit der Bekämpfung von Kinderpornographie im Internet vorzusehen, um zu verhindern, dass Access-Provider zu „Gatekeepern des Rechts“ werden. Dieser Gefahr begegnet der Gesetzentwurf nur unzureichend (vgl. dazu unten Randnummern 77ff. dieser Stellungnahme).

Trotz des zu begrüßenden Ansatzes, die Materie nunmehr gesetzlich zu regeln, weist der vorliegende Gesetzentwurf noch beachtliche Schwächen auf, die es im Laufe des Gesetzgebungsverfahrens auszuräumen gilt, um insbesondere die vielfältigen verfassungsrechtlichen Fragestellungen der Implementierung von Zugangserschwerungen durch Access-Provider zu lösen.

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

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

A. Zusammenfassung

Zusammenfassend kann Folgendes festgehalten werden:

- *Insgesamt mangelt es dem Gesetzentwurf an der verfassungsrechtlich gebotenen Normenklarheit und Normenbestimmtheit*

  Die Tatbestandsvoraussetzungen für die Aufnahme eines Telemedienangebots in die Sperrliste durch das BKA bleiben unklar. Kinderpornographische Angebote sollen anhand unterschiedlicher Sperrkategorien (Internetprotokoll-Adresse, vollqualifizierter Domainname, Zieladresse) identifiziert werden. Dabei wird nicht geregelt, ob die genannten Kategorien alternativ oder gleichberechtigt nebeneinander zur Identifizierung eines inkriminierten Inhalts in der Liste vorliegen sollen. Dies ist jedoch von entscheidender Bedeutung, da die Gefahr einer versehentlichen (Mit-)Sperrung rechtmäßiger Inhalte je nach verwendeter Sperrkategorie unterschiedlich groß ist und zusätzlich auch auf inkriminierte Inhalte verweisende Angebote in die Sperrliste aufgenommen werden sollen.

  Außerdem bleiben die Access-Provider treffenden Verpflichtungen, den Zugang zu inkriminierten Inhalten und Verweisen zu erschweren, unklar. Den Access-Providern wird es als Privaten in einem grundrechtssensiblen Bereich überlassen, über die Eingriffsintensität einer Maßnahme zu entscheiden. Sie hätten darüber zu entscheiden, in welchem Umfang etwa die Sperrung rechtmäßiger Inhalte als unbeabsichtigter Nebeneffekt möglich ist. Dies wirkt sich schließlich auch auf die Verpflichtung von Access-Providern aus, einen Server mit Stoppmeldungen zu betreiben, auf den Nutzeranfragen zu den auf der Sperrliste enthaltenen Angeboten umgeleitet werden. Die bei der von Access-Providern gehosteten Stoppmeldung anfallenden Daten hängen entscheidend davon ab, auf welche der genannten Sperrkategorien die eingesetzte Sperrinfrastruktur aufsetzt. Würden etwa Internetprotokoll-Adressen zur Identifizierung inkriminierter Inhalte im Internet verwendet, wären die im Zusammenhang mit der Stoppmeldung anfallenden personenbezogenen Daten besonders umfangreich und unspezifisch, da die Anzahl der umzuleitenden Nutzer voraussichtlich größer ist und ein Zusammenhang mit dem Abruf kinderpornographischer Inhalte regelmäßig nicht hergestellt werden kann.

  Schließlich erfasst die Unbestimmtheit und Unklarheit der vorstehend skizzierten Eingriffsvoraussetzungen auch die mit § 8a Abs. 7 TMG-E intendierte Haftungsfreistellung für Access-Provider. Die Freistellung wird von der „*ordnungsgemäßen*“ Umsetzung der Sperrmaßnahmen abhängig gemacht. Wann eine solche ordnungsgemäße Umsetzung vorliegt, lässt sich aufgrund des Gesetzentwurfs nicht mit ausreichender Sicherheit beurteilen.

- *Die Verhältnismäßigkeit der aufgrund des Gesetzentwurfs in Frage stehenden Sperrungsmaßnahmen ist ebenfalls zweifelhaft*

  Der Gesetzentwurf verfolgt mit der Bekämpfung der Kinderpornographie in Kommunikationsnetzen ohne Zweifel einen legitimen Zweck. Dabei stehen zwei präventive Zielsetzungen, der Opferschutz und die Gefahrenabwehr im Vordergrund. Es soll verhindert werden, dass eine schwerwiegende Verletzung der Intimsphäre eines abgebildeten und im Sinne des § 176 Abs. 1 StGB missbrauchten Kindes durch die weitere Verbreitung von Bildnissen im Internet vertieft wird. Der Gesetzentwurf enthält dabei allerdings nur Regelungen zu den am wenigsten wirksamen Maßnahmen gegen die Perpetuierung der schwerwiegenden Verletzungen des allgemeinen

Persönlichkeitsrechts der dargestellten Kinder. Zugangserschwerungen tilgen weder kinderpornographische Angebote aus dem Internet noch eignen sich die intendierten technischen Manipulationen durch Access-Provider dazu, Straftäter aus Deutschland von solchen Angeboten wirksam abzuschneiden. Gerade mit krimineller Energie agierende Täter verwenden z.B. Verschlüsselungstechnologien, denen mit den derzeit diskutierten Methoden der Zugangserschwerung nicht beizukommen ist. Wesentlich wirksamer ist daher, die Verbreitung kinderpornographischer Inhalte an der Quelle zu bekämpfen. Dazu müsste zunächst gegen die Anbieter der Inhalte und gegebenenfalls gegen die Betreiber der Internetserver vorgegangen werden, bevor Zugangserschwerungen auf der Ebene von Access-Providern erwogen werden (sog. ultima ratio-Grundsatz). Der Gesetzentwurf lässt aber eine Gesamtstrategie zur Bekämpfung der Kinderpornographie im Internet vermissen. Er beschränkt sich auf die Verpflichtung der Access-Provider, über deren Netzinfrastruktur die Datenpakete übermittelt werden. Es handelt sich dabei um eine konzeptionelle Schwäche, die durch die Verpflichtung ausgeräumt werden könnte, vor der Aufnahme eines Inhalts auf die Sperrliste, die Löschung von den Inhalteanbietern und Host-Providern zu verlangen sowie in Kooperation mit den zuständigen ausländischen Strafverfolgungsbehörden Zwangsmaßnahmen gegen die Verantwortlichen einzuleiten.

Im Lichte des Vorgesagten erweisen sich Zugangserschwerungen durch Access-Provider bei Inlandssachverhalten als unverhältnismäßig, da hier Content-Anbieter und/oder Host-Provider in jedem Fall der deutschen Hoheitsgewalt unterliegen. Zugangserschwerungen, die Sachverhalte auf dem Territorium eines Mitgliedsstaats der Europäischen Gemeinschaft betreffen, dürften nicht erforderlich sein. Die justitielle Zusammenarbeit zur Bekämpfung von Kinderpornographie ist gemeinschaftsrechtlich geregelt. Auch bestehen aufgrund der Richtlinie über den elektronischen Geschäftsverkehr und der Richtlinie über audiovisuelle Mediendienste gemeinschaftsrechtlich vorgegebene Konsultations- und Prüfungsverfahren, die wesentliche Verfahrensvorschriften des Gemeinschaftsrechts darstellen, deren Missachtung die Unanwendbarkeit einer nationalen Maßnahme zur Folge hat.

- *Im Übrigen enthält der vorliegende Gesetzentwurf eine Reihe weiterer Schwächen, die ohne substantielle Nachbesserungen die Verhältnismäßigkeit im engeren Sinne in Frage stellen:*

  Es handelt sich stichpunktartig um die folgenden Aspekte:

  - Fehlende verfahrensrechtliche Absicherung der erstellten Sperrliste;
  - Auswertung des gesamten Datenverkehrs der Internetnutzer, ohne verfahrensrechtliche Absicherung;
  - Verwendung personenbezogener Daten der Internetnutzer zur Strafverfolgung ohne Festlegung zielgenauer Sperrkriterien und qualifizierter zusätzlicher Indizien für das Ergreifen von Ermittlungsmaßnahmen;
  - Keine ausreichenden Vorkehrungen zum Schutz rechtmäßiger Angebote im Rahmen des Verwaltungsverfahrens und durch effektiven gerichtlichen Rechtsschutz;
  - Fehlende Übergangsregelung für Access-Provider zur Implementierung der Sperrmaßnahmen;
  - Fehlende Regeln zur Kostenerstattung für Access-Provider.

Gliederung

B. Verfassungsrechtliche Betrachtung

1. Die in dem Gesetzentwurf vorgesehene Pflicht der Access-Provider, den Zugang zu kinderpornographischen Telemedienangeboten durch technische Vorkehrungen zu erschweren, berührt Grundrechte in unterschiedlichster Hinsicht. Neben dem in Art. 10 GG geschützten Telekommunikationsgeheimnis der Nutzer, der Berufsfreiheit gem. Art. 12 GG bzw. der Eigentumsgarantie gem. Art. 14 GG der Access-Provider und Webseitenbetreiber kann die Meinungs-, Presse-, Informations-, Kunst- und Wissenschaftsfreiheit gem. Art. 5 GG von Nutzern und Webseitenbetreibern betroffen sein; Access-Providern kommt in unserer heutigen Gesellschaft nicht nur im Hinblick auf die Informationsbeschaffung der Bürger, sondern auch für ihre berufliche und wirtschaftliche Betätigung eine herausragende Rolle zu.

2. Die nachfolgende verfassungsrechtliche Betrachtung zum Gesetzentwurf erfolgt im Lichte des Grundsatzes der Normenklarheit sowie Normenbestimmtheit, des Grundsatzes der Verhältnismäßigkeit und der im Gesetzentwurf vorgebrachten Gesetzgebungskompetenzen.

I. Normenklarheit und Normenbestimmtheit

3. Gesetzliche Eingriffe in Grundrechte müssen dem Gebot der Normenklarheit und Normenbestimmtheit genügen, welches seine Grundlage im Rechtsstaatsprinzip gem. Art. 20, Art. 28 Abs. 1 GG (vgl. BVerfGE 110, 33 [53, 57, 70]; 112, 284 [301]; 113, 348 [375]; 115, 320 [365]) findet. Das Gebot soll sicherstellen, dass der demokratisch legitimierte Parlamentsgesetzgeber die wesentlichen Entscheidungen über Grundrechtseingriffe und deren Reichweite selbst trifft, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte die Rechtskontrolle durchführen können. Ferner sichern Klarheit und Bestimmtheit der Norm, dass der Betroffene die Rechtslage erkennen und sich auf mögliche belastende Maßnahmen einstellen kann (vgl. BVerfGE 110, 33 [52 ff.]; 113, 348 [375 ff.]). Der Gesetzgeber hat Anlass, Zweck und Grenzen des Eingriffs hinreichend bereichsspezifisch, präzise und normenklar festzulegen (vgl. BVerfGE 100, 313 [359 f., 372]; 110, 33 [53]; 113, 348 [375]; BVerfG, Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07 – *Online-Durchsuchung*, NJW 2008, S. 822 [828 Rn. 210]).

4. Die Kompatibilität des Gesetzentwurfs mit dem verfassungsrechtlichen Gebot der Normenklarheit und Normenbestimmtheit ist zweifelhaft. Die Tatbestandsvoraussetzungen für die Aufnahme eines Telemedienangebots in die Sperrliste durch das BKA bleiben in unterschiedlicher Hinsicht unklar. Gleiches gilt für den Inhalt und die Reichweite der Verpflichtungen von Diensteanbietern zur Umsetzung der von dem BKA erstellten Sperrliste sowie der von ihnen zu hostenden Stoppmeldung. Daraus resultiert schließlich, dass eine „*ordnungsgemäße*“ Umsetzung der von Diensteanbietern gem. § 8a Abs. 2 bis 6 TMG-E vorzunehmenden Maßnahmen nicht mit der notwendigen Klarheit und Bestimmtheit erkennbar ist, obwohl dies Voraussetzung für die angestrebte Haftungsfreistellung ist.

1. Erstellung der Sperrliste gem. § 8a Abs. 1 TMG-E

5. Gem. § 8a Abs. 1 TMG-E soll die Sperrliste – offensichtlich vor dem Hintergrund der angestrebten technologieneutralen Sperrverpflichtungen – einerseits

> „vollqualifizierte Domainnamen, Internetprotokoll-Adressen und Zieladressen von Telemedienangeboten, die Kinderpornographie nach § 184b StGB des Strafgesetzbuches enthalten".

Andererseits sollen in die Liste zusätzlich vollqualifizierte Domainnamen, Internetprotokoll-Adressen und Zieladressen aufgenommen werden, deren

> „Zweck darin besteht, auf derartige Telemedienangebote [Kinderpornographie nach § 184b StGB] zu verweisen".

a) Zugangserschwerung mittels „Zieladresse"

6. Die einzige Information der angedachten Sperrliste, die eine relativ genaue Zugangserschwerung zu einem inkriminierten Inhalte erlauben dürfte, ist die Zieladresse. Eine Zieladresse verweist auf Ressourcen im Internet und wird als URL („Uniform Resource Locator") bezeichnet. Sie könnte beispielweise wie folgt aussehen: *http://www.server.net/user1/evil/child.mov*.

b) Zugangserschwerung mittels „vollqualifizierten Domainnamen"

7. Der vollqualifizierte Domainname, der zur Namensauflösung im vorstehenden Beispiel verwendet wird, hieße: *www.server.net*. Allerdings wäre unter dem genannten vollqualifizierten Domainnamen nicht zwangsläufig nur die im Beispiel genannte Zieladresse mit dem inkriminierten Inhalt zu finden. Hinter dem Domainnamen könnten auch rechtmäßige Inhalte, die über andere Zieladressen aufzurufen wären, angeboten werden (z.B. *http://www.server.net/user2/nice/information.html).* Die Sperrung auf Ebene des vollqualifizierten Domainnamens *www.server.net* würde in dem vorstehenden Beispiel auch den rechtmäßigen Inhalt erfassen.

c) Zugangserschwerung mittels „Internetprotokoll-Adresse"

8. Die Auswirkungen einer Sperrung auf der Basis einer Internetprotokoll-Adresse gingen noch wesentlich weiter. Unter einer Internetprotokoll-Adresse (z.B. 217.79.215.140) werden häufig Webangebote von unterschiedlichen Domains gehostet. Es handelt sich um das sog. *Name-Based Virtual Hosting*, das es ermöglicht, im Rahmen großer Server mit nur einer oder weniger Internetprotokoll-Adressen, die Dienste für mehrere hundert oder gar tausende von Domains beherbergen zu können. Würde die Sperrung auf der Ebene einer Internetprotokoll-Adresse vorgenommen, besteht daher immer die Gefahr, dass nicht nur der Zugang zur Domain *server.net* erschwert wird, sondern auch die Domains *server1.net* bis *server1000.net* von der Sperrung mit erfasst werden, ohne dass hinter den genannten Domainnamen kinderpornographische Inhalte stehen (vgl. hierzu bereits Randnummer 21 unserer Stellungnahme vom 10. Februar 2009 zur öffentlichen Anhörung des Unterausschusses Neue Medien).

d) Verhältnis der Sperrkategorien zueinander

9. Das Gesetz schreibt keine zielgerichtete Zugangserschwerung vor, sondern lässt es zu, dass auf der Sperrliste gleichberechtigt, vollqualifizierte Domainnamen, Internetprotokoll-Adressen und Zieladressen aufgeführt werden. Es bleibt dabei im Dunkeln, in welchem Verhältnis die drei genannten Sperrkategorien stehen. Es wird beispielsweise nicht klargestellt, ob die genannten Sperrkategorien alternativ von dem BKA gesammelt und von den Access-Providern verwendet werden können oder sollen. Da eine relativ zielgenaue Zugangserschwerung nur anhand der URL, also der Zieladresse, denkbar ist, und die Verwendung des vollqualifizierten Domainnamens insbesondere aber der Internetprotokoll-Adresse zu ganz erheblichen Kollateralschäden im Hinblick auf rechtmäßige Inhalte führen kann, bleiben in dem Gesetzentwurf wesentliche Fragen der grundrechtlichen Eingriffsintensität offen.

e) Verweissperrung

10. Verschärft wird das Problem der Unbestimmtheit und Unklarheit des gesetzlichen Regelungsentwurfs noch durch den Umstand, dass das BKA nicht nur berechtigt sein soll, kinderpornographische Angebote anhand der drei oben beschriebenen Sperrkategorien in die Liste gem. § 8a Abs. 1 TMG-E aufzunehmen. Vielmehr sollen auch solche vollqualifizierten Domainnamen, Internetprotokoll-Adressen und Zieladressen in die Sperrliste aufgenommen werden, deren Zweck es ist, auf kinderpornographische Angebote zu verweisen.

11. Kinderpornographische Angebote werden indes nicht nur anhand der Zieladresse in die Sperrliste aufgenommen. Nach dem Gesetzentwurf können sie – wie vorstehend dargelegt – auch anhand vollqualifizierter Domainnamen und Internetprotokoll-Adressen identifiziert sein. Die sich bereits daraus ergebende Unklarheit und Unbestimmtheit der Eingriffsvoraussetzungen und nach dem Willen des Gesetzgebers ggf. zulässiger Kollateralschäden durch die Sperrung rechtmäßiger Angebote wird durch die Pflicht zur Sperrung von Verweisen weiter verschärft. Nach dem Wortlaut des Gesetzentwurfs wäre denkbar, dass die Internetprotokoll-Adresse eines Angebots, das auf die Internetprotokoll-Adresse eines kinderpornographischen Inhalts verweist, gesperrt wird. Damit würde die bereits auf der ersten Ebene möglicherweise erhebliche Zahl von rechtmäßigen Angeboten, die von der Sperrung erfasst werden, noch weiter gesteigert.

12. Zudem lassen der Gesetzentwurf und die Begründung zu § 8a Abs. 1 TMG-E offen, was unter dem „*Zweck*“ zu verstehen ist, „*auf derartige Telemedienangebote zu verweisen*“. Damit könnte beispielsweise auch ein journalistisches Angebot in die Sperrliste aufgenommen werden, das sich kritisch mit der Beurteilung eines vermeintlich kinderpornograhischen Angebots durch das BKA auseinandersetzt.

13. Zudem definiert das Gesetz nicht, was technisch unter einem „*Verweis*“ zu verstehen ist. Soll es sich um einen anklickbaren Hyperlink auf eine URL handeln oder rechtfertigt z.B. die Nennung eines Domainnamens oder einer Internetprotokoll-Adresse bereits die Aufnahme in die Sperrliste.

14. Die genannte Problematik würde weiter dadurch verschärft, dass je nach Sperrkategorie, d.h. vollqualifizierte Domainnamen, Internetprotokoll-Adressen und Zieladressen, die Gefahr der Sperrung rechtmäßiger Inhalte besteht. Ein im Sinne eines Kollateralschadens mitgesperrter rechtmäßiger Inhalt, auf den z.B. zum Zwecke der kritischen Auseinandersetzung mit der Praxis

des BKA verwiesen wird, müsste daher ebenfalls auf der Sperrliste geführt werden. Diese problematische Konstellation könnte auch erhebliche praktische Relevanz entfalten, da die Verweissperrung nicht nur Verweise auf die Sperrliste insgesamt erfassen soll, sondern jeder Verweis auch auf einzelne Einträge in die Sperrliste aufgenommen werden soll.

15. Die Eingriffsintensität der unklaren und unbestimmten Voraussetzungen des § 8a Abs. 1 TMG-E wird schließlich dadurch verstärkt, dass die Sperrliste aufgrund der präventiven Zielrichtung des Gesetzentwurfs heimlich erstellt werden soll.

2. Umsetzung der Sperrliste durch Access-Provider gem. § 8a Abs. 2 TMG-E

16. Gem. § 8a Abs. 2 TMG-E sollen Diensteanbieter nach § 8 TMG, die den Zugang zur Nutzung von Informationen über ein Kommunikationsnetz „*ermöglichen*“ *[§ 8 TKG spricht dagegen von „vermitteln“]*, „*den Zugang zu Telemedienangeboten, die in der Sperrliste aufgeführt sind*“, erschweren.

17. Die im Zusammenhang mit der Listenerstellung durch das BKA konstatierte Unklarheit und Unbestimmtheit des Gesetzentwurfs erfasst auch § 8a Abs. 2 TMG-E. Die hier verpflichteten gewerblichen Access-Provider (vgl. zur unpräzisen Verweisformulierung bereits vorstehend Randnummer 16) müssen die in ihrer Struktur und inhaltlichen Reichweite unklare Sperrliste des BKA „*unverzüglich*“ umsetzen, vgl. Satz 4. Sie haben gem. Satz 1-3 dazu

> „geeignete und zumutbare technische Maßnahmen zu ergreifen […]. Für die Sperrung dürfen vollqualifizierte Domainnamen, Internetprotokoll-Adressen und Zieladressen von Telemedienangeboten verwendet werden“.

a) Access-Provider entscheiden über Eingriffstiefe von Zugangserschwerungen

18. Hier bleibt unklar, welche konkreten Verpflichtungen Access-Provider im Hinblick auf inkriminierte Inhalte und Verweise treffen sollen. Nach der Gesetzesbegründung zu Abs. 2 ist dies darin begründet, dass es aufgrund der rasanten Fortentwicklung der Technik nicht zweckmäßig erscheint,

> „den Zugangsvermittlern vorzugeben, wie die Sperrung technisch zu erfolgen hat. Vor diesem Hintergrund ist das Gesetz technologieneutral, dass heißt, es können alle vorhandenen technischen Möglichkeiten in Betracht gezogen werden, soweit diese den Diensteanbietern zuzumuten sind.“

19. Die angestrebte Technologieneutralität überlässt es indes in einem grundrechtssensiblen Bereich Privaten über die Eingriffsintensität von Maßnahmen zu entscheiden, die nach dem Gesetzentwurf zudem rechtmäßige Angebote erfassen können. Die ggf. notwendige, in dem Gesetzentwurf aber unbestimmt gehaltene Beschränkung des Aktionsradius von Access-Providern auf *geeignete und zumutbare technische Maßnahmen* soll darüber hinaus von diesen selbst beurteilt werden. Dabei sollen Access-Provider hinsichtlich der aufzubauenden Sperrinfrastrukturen frei sein, auf welche der in der Liste geführten Sperrkategorien sie zugreifen möchten. Wie bereits angeführt, dürfen für die Sperrung nach dem Gesetzentwurf ausdrücklich und offensichtlich gleichberechtigt vollqualifizierte Domainnamen, Internetprotokoll-Adressen und Zieladressen von Telemedienangeboten verwendet werden. Damit würde Access-Providern auch die Entscheidung darüber überlassen, in welchem Umfang etwa die Sperrung rechtmäßiger Inhalte als

unbeabsichtigter Nebeneffekt möglich ist. Fragestellungen von solcher Grundrechtsrelevanz können aber nicht Privaten zur Entscheidung übertragen werden, sondern sind nach der von dem Bundesverfassungsgericht entwickelten Wesentlichkeitstheorie durch den Gesetzgeber zu entscheiden.

b) DNS-Sperre unverbindlich

20. Die kritisierte Unbestimmtheit des Entwurfs in § 8a Abs. 2 TMG-E wird auch nicht durch Satz 3 der Regelung geheilt. Danach erfolgt die

> „Sperrung […] mindestens auf der Ebene der vollqualifizierten Domainnamen, deren Auflösung in die zugehörigen Internetprotokoll-Adressen unterbleibt".

21. In der Gesetzesbegründung heißt es dazu:

> „In der bloßen Verhinderung des Zugangs zu einer Seite mit kinderpornographischem Inhalt auf der DNS-Ebene liegt nach einhelliger Auffassung die geringste Eingriffstiefe. Den Diensteanbietern ist es jedoch unbenommen, sich für eine andere Sperrtechnik mit größerer Eingriffstiefe zu entscheiden."

22. Damit wird unterstrichen, dass der Gesetzgeber die sog. DNS-Sperre nicht als verbindliche Lösung regeln will. Dadurch ist auch der Pflichtenkreis für die betroffenen Access-Provider nur unzureichend konkretisiert. Der Gesetzentwurf lässt nämlich offen, ob die normierte Mindestanforderung `DNS-Sperre` vor dem Hintergrund der in der Gesetzesbegründung angeführten technologischen Entwicklung zukünftig nicht mehr als ausreichend erachtet wird, um eine *„ordnungsgemäße"* (vgl. § 8a Abs. 7 TMG-E) Umsetzung der Sperrliste sicherzustellen. Ist die Ordnungsgemäßheit der Umsetzung nicht gewährleistet, verlieren Access-Provider aber die intendierte Haftungsfreistellung.

23. Schließlich ist es eine Frage der Perspektive, ob die DNS-Sperre auf Basis vollqualifizierter Domainnamen die geringste Eingriffsintensität aufweist. Dies mag für Access-Provider zutreffen. Wie unter Randnummer 6 dieser Stellungnahme erläutert, ist dies bezogen auf Webseitenbetreiber und Nutzer aber regelmäßig nicht der Fall. Hier dürfte die Eingriffsintensität dann am geringsten sein, wenn auf Basis der Zieladresse gesperrt wird. Die Verwendung von Zieladressen (d.h. URL's) erlaubt eine relativ zielgenaue Zugangserschwerung im Hinblick auf kinderpornographische Inhalte und dürfte daher seltener zu Kollateralschäden, also zur (unbeabsichtigten) (Mit-)Sperrung rechtmäßiger Inhalte, führen. Wie oben unter Randnummer 6 gezeigt, kann dies auf der Basis vollqualifizierter Domainnamen nicht sichergestellt werden. Folgendes plakatives Beispiel zur Illustration: Die Sperrung des vollqualifizierten Domainnamens www.youtube.com würde alle Inhalte der populären Videoplattform erfassen, auch wenn der inkriminierte Inhalte nur hinter einer Zieladresse wie beispielsweise der URL http://www.youtube.com/watch?v=UtTtUwUKa44 verfügbar ist.

3. Geringe Aussagekraft der personenbezogenen Daten auf dem Server mit gehosteter Stoppmeldung

24. Die unklaren und unbestimmten Eingriffsvoraussetzungen des § 8a Abs. 1 und 2 TMG-E wirken sich mittelbar auch auf die Verpflichtung aus, dass Access-Provider gem. § 8a Abs. 4 und 5 TMG-

E einen Server aufsetzen sollen, auf den die Nutzeranfragen zu den Telemedienangeboten, die auf der Sperrliste enthalten sind, umgeleitet und den betreffenden Nutzern eine sog. Stoppmeldung angezeigt werden soll.

25. Gem. § 8a Abs. 5 S. 2 TMG-E dürfen Access-Provider die personenbezogenen Daten, die bei der Umleitung auf die von ihnen gehostete Stoppseite anfallen, den Strafverfolgungsbehörden übermitteln. Die bei Access-Providern im Zusammenhang mit der von ihnen gehosteten Stoppmeldung anfallenden personenbezogenen Daten sind aber entscheidend davon abhängig, auf welche der genannten Sperrkategorien die eingesetzte Sperrinfrastruktur aufsetzt. Während der Rückgriff auf die Zieladresse zumindest eine Zuordnung zu einem kinderpornographischen Inhalt erlauben dürfte, würde insbesondere eine Bezugnahme auf eine Internetprotokoll-Adresse wegen der damit regelmäßig einhergehenden Sperrung rechtmäßiger Seiten wohl nur eine äußerst geringe oder gar keine Aussage darüber zulassen, ob tatsächlich ein kinderpornographischer Inhalt angesteuert werden sollte. Vielmehr würden in diesem Fall in der Regel auch eine Reihe von Nutzern umgeleitet, die rechtmäßige Inhalte ansteuern wollten, die unter derselben Internetprotokoll-Adresse wie inkriminierte Inhalte im Internet zugänglich gemacht werden. Die im Hinblick auf die Stoppmeldung anfallenden personenbezogenen Daten würden sich hier als besonders umfangreich und unspezifisch darstellen, da die Anzahl der umzuleitenden Nutzer voraussichtlich größer ist und ein Zusammenhang mit dem Abruf kinderpornographischer Inhalte regelmäßig nicht hergestellt werden kann.

4. Haftungsfreistellung für Access-Provider gem. § 8a Abs. 7 TMG-E

26. Wie bereits unter Randnummer 22 dieser Stellungnahme angedeutet, würden sich die unklaren und unbestimmten Eingriffsvoraussetzungen des § 8 Abs. 1 und 2 TMG-E auch auf die mit § 8a Abs. 7 TMG-E intendierte Haftungsfreistellung für Access-Provider auswirken. Letztere haften nach der genannten Bestimmung

> „nur, wenn und soweit sie die Sperrliste durch Maßnahmen nach den Absätzen 2 bis 6 nicht ordnungsgemäß umsetzen".

27. Wie eine *„ordnungsgemäße"* Umsetzung einer Sperrliste auszusehen hat, ist – wie dargelegt – aufgrund der Regelungen des Gesetzentwurfs nur schwer zu beurteilen.

28. Aufgrund der erheblichen Eingriffsintensität der geforderten Sperrungsmaßnahmen liegt es darüber hinaus nahe, dass Nutzer und Webseitenbetreiber zunächst die unmittelbar agierenden Access-Provider in Anspruch nehmen. Die Sperrung einer rechtmäßigen Webseite mit der Umleitung der anfragenden Nutzer auf einen Server mit Stoppmeldung führt bei dem Betreiber der rechtmäßigen Webseite regelmäßig zu erheblichen materiellen und immateriellen Schäden (z.B. Imageverlust). Es ist wahrscheinlich, dass zunächst Access-Provider (im Rahmen des einstweiligen Rechtschutzes) auf Unterlassung in Anspruch genommen werden. Die unklaren und unbestimmten Regelungen des Gesetzentwurfs dürften auch zur Folge haben, dass Schadensersatzansprüche gegen Access-Provider mit dem Argument einer nicht ordnungsgemäßen Umsetzung der Sperrungsmaßnahmen geltend gemacht werden.

II. Verhältnismäßigkeit

29. Der Grundsatz der Verhältnismäßigkeit verlangt, dass ein Grundrechtseingriff einem legitimen Zweck dient und als Mittel zu diesem Zweck geeignet, erforderlich und angemessen ist (vgl. BVerfGE 109, 279 [335 ff.]; 115, 320 [345]; BVerfG, Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07 – *Online-Durchsuchung*, NJW 2008, S. 822 [828 Rn. 218] stRspr.). Wie bereits unter Randnummer 1 der Stellungnahme skizziert, erlangen Sperrungsmaßnahmen in vielerlei Hinsicht grundrechtliche Relevanz.

30. Die Verhältnismäßigkeit der aufgrund des Gesetzentwurfs in Frage stehenden Sperrungsmaßnahmen ist ebenfalls zweifelhaft.

1. Legitimer Zweck

31. Gemäß dem Titel des Entwurfs zielt das Gesetz auf die Bekämpfung der Kinderpornographie in Kommunikationsnetzen. Kinderpornographie nach § 184b StGB ist strafrechtlich sanktioniert. Sowohl die Verbreitung als auch die Besitzverschaffung kinderpornographischer Schriften stehen unter Strafe. Es gilt gem. § 6 Nr. 6 StGB das sog. Weltprinzip; strafrechtlich ist Kinderpornographie daher ohne Rücksicht auf einen ausländischen Tatort, das Recht des Tatorts und die Staatsangehörigkeit des Täters zu verfolgen. Der Gesetzentwurf verfolgt aber unmittelbar keinen repressiven Zweck. Mit dem Opferschutz und der Gefahrenabwehr dürften zwei präventive Zielsetzungen im Vordergrund stehen, mit denen verhindert werden soll, dass eine schwerwiegende Verletzung der Intimsphäre eines abgebildeten und i.S.d. § 176 Abs. 1 StGB missbrauchten Kindes durch die weitere Verbreitung von Bildnissen im Internet vertieft wird. Der so intendierte Schutz vor der Perpetuierung der Verletzung des allgemeinen Persönlichkeitsrechts i.S.d. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG stellt einen legitimen Zweck dar.

2. Geeignetheit

32. Die in dem Gesetz vorgesehenen Sperrmaßnahmen müssten des Weiteren zur Erreichung des Zwecks geeignet sein. Bei der Beurteilung der Eignung ist dem Gesetzgeber ein beträchtlicher Einschätzungsspielraum eingeräumt (vgl. BVerfGE 77, 84 [106]; 90, 145 [173]; 109, 279 [336]). Im Rahmen der Eignungsprüfung ist nicht zu fordern, dass die Maßnahmen, welche der Gesetzentwurf vorsieht, stets oder auch nur im Regelfall Erfolg versprechen. Die gesetzgeberische Prognose darf aber nicht offensichtlich fehlsam sein (vgl. BVerfG, Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07 – *Online-Durchsuchung*, NJW 2008, S. 822 [828 Rn. 222]).

33. Zur Verhinderung der Perpetuierung schwerwiegender Verletzungen des allgemeinen Persönlichkeitsrechts der dargestellten Kinder sind – aufbauend auf die intensive Verfolgung der Straftäter – unterschiedliche Maßnahmen möglich.

a) Kein Vorgehen an der „Quelle“ von Kinderpornographie

34. Ein Vorgehen gegen die Verbreitung kinderpornograhischer Inhalte an der Quelle, d.h. dort wo sie von den Internet-Servern gelöscht werden können, stellt den effektivsten Ansatz zur

Zweckerreichung dar. Dazu müsste gegen die Anbieter der Inhalte (sog. Content-Provider) und ggf. gegen die Betreiber der Internet-Server (sog. Host-Provider) vorgegangen werden, auf deren Rechnern die inkriminierten Inhalte zum Abruf über das Internet bereitgehalten werden. Solche Maßnahmen regelt der Gesetzentwurf jedoch nicht.

b) Umgehbarkeit

35. Der Gesetzentwurf beschränkt sich auf die Inanspruchnahme von Zugangsvermittlern (sog. Access-Provider), über deren Netzinfrastruktur die Datenpakete zum Nutzer gelangen.

36. Teilweise wird der Nutzen solcher Zugangserschwerungen gänzlich in Frage gestellt. Je nach verwendeter Sperrtechnik lassen sich die Maßnahmen mit mehr oder weniger großem Aufwand umgehen. Dies gilt insbesondere für die sog. DNS-Sperre. Zur gegenüber einem Access-Provider geltend gemachten Forderung der Sperrung einer Webseite mit urheberrechtsverletzenden Inhalten hat beispielsweise des LG Hamburg mit Urteil vom 12. November 2008 (Az.: 308 O 548/08) festgestellt (soweit ersichtlich bisher nur Online veröffentlicht unter http://openjur.de/u/30638-308_o_548-08.html):

> „Die Eignung einer „DNS-Sperre“ zur Verhinderung des Zugriffs auf einen Internetauftritt ist aufgrund von Umgehungsmöglichkeiten, etwa durch Eintragung eines anderen Nameservers, nur beschränkt (vgl. LG Kiel, MMR 2008, 123, 124; Gehrke, MMR 2008, 291). Ohne Erfolg verweisen die Antragstellerinnen darauf, dass die Mehrzahl der durchschnittlichen Internetnutzer durch eine DNS-Sperre davon abgehalten würden, einen anderen Weg zu dem gesperrten Internetauftritt zu suchen. Dem Gericht ist es in wenigen Minuten gelungen, eine Internetseite mit einer Anleitung zur Umgehung mit den verfügbaren Name-Servern zu finden. Den Nutzern solcher Filmdownloadseiten wie „...“, es dürften im Wesentlichen internetaktive Jugendliche und junge Erwachsene sein, wird das im Zweifel noch schneller gelingen.“

37. Zweifel an der Geeignetheit der mit dem Gesetzentwurf angeordneten Zugangserschwerungen können daher einerseits die technische Umsetzung und andererseits die inhaltliche Beschränkung auf die am wenigsten wirksame Form der Bekämpfung kinderpornographischer Inhalte, nämlich die Zugangserschwerungen durch Access-Provider, betreffen. DNS-Sperren betreffen jedoch nur eine mögliche Form zur Umsetzung der Sperrliste. Da sie als gesetzliche Mindestanforderung im Entwurf festgeschrieben sind und auch die öffentliche Diskussion über Zugangserschwerungen beherrschen, ist davon auszugehen, dass DNS-Sperren in der Praxis das Mittel der Wahl sein würden.

38. Allerdings muss trotz der leichten Umgehbarkeit der DNS-Sperre im Hinblick auf die Bewertung der Geeignetheit der beträchtliche Einschätzungsspielraum des Gesetzgebers beachtet werden. In der Begründung des Gesetzentwurfs zu § 8a Abs. 2 TMG-E heißt es insofern:

> „Die Vorschrift ist auf eine Handlungspflicht ausgerichtet, nicht auf einen Erfolg, denn es ist nach dem gegenwärtigen Stand der Technik nicht auszuschließen, dass der Zugang zu kinderpornographischen Inhalten trotz der Sperrmaßnahmen der Anbieter nicht vollständig verhindert werden kann. Es ist aber bereits viel erreicht, wenn solche Angebote nicht ohne Weiteres zugänglich sind.“

39. Diese Beurteilung dürfte in technischer Hinsicht verfassungsrechtlich nicht zu beanstanden sein, da insbesondere nur von einer Handlungspflicht ausgegangen wird.

c) Keine Gesamtkonzept zur Bekämpfung von Kinderpornographie

40. Der Gesetzentwurf erhält aber keine Ausführungen zur Beschränkung der Maßnahmen zur Bekämpfung der Kinderpornographie im Internet auf Zugangserschwerungen durch Access-Provider. Die auch vor dem Hintergrund der technischen Schwächen von Zugangserschwerungen effektiveren Maßnahmen gegen Content- und Host-Provider werden in den vorgeschlagenen Bestimmungen weder geregelt noch wird in der Begründung erläutert, warum der legitime Zweck der Bekämpfung der Kinderpornographie nur auf der Ebene des Internetzugangs erfolgen soll.

41. Die angedachten Zugangserschwerungen sind auch nicht auf Fälle beschränkt, in denen sich die verantwortlichen Content-Provider und die Host-Provider im Ausland befinden. Daher kann aufgrund des intendierten Gesetzes – auch nicht bei Inlandssachverhalten – zwischen den möglichen Instrumenten zur Bekämpfung der Kinderpornographie gewählt werden, sondern es muss das häufig am wenigsten wirksame Instrumente der Zugangserschwerung durch Access-Provider verwandt werden. Dies ist eine offensichtliche Schwäche des Gesetzentwurfs.

42. Vor dem Hintergrund der Einschätzungsprärogative des Gesetzgebers wird man den intendierten Zugangserschwerungen aber jedenfalls dann nicht die Geeignetheit zur Erreichung des legitimen Zwecks grundsätzlich absprechen können, falls der Zugriff auf die Quelle kinderpornographischer Angebote nur im Ausland möglich ist. In dieser Konstellation kann eines der möglichen Instrumente – wenn auch in der Wirksamkeit beschränkt – durch ein unilaterales Handeln eingesetzt werden.

3. Erforderlichkeit

43. Die in dem Gesetzentwurf vorgesehenen Sperrungsmaßnahmen sind im Sinne des Verhältnismäßigkeitsgrundsatzes erforderlich, wenn keine milderen Mittel zur Erreichung des Zwecks vorliegen.

a) Inlandssachverhalte

44. Nach dem vorstehend zur Geeignetheit der ausschließlich auf Zugangserschwerungen durch Access-Provider zugeschnittenen Regeln Gesagten steht die Erforderlichkeit zunächst bei Inlandssachverhalten in Frage. Hier können kinderpornographische Angebote problemlos an der Quelle, d.h. bei den verantwortlichen Content-Providern und/oder den Host-Providern, bekämpft werden. Ein rechtsstaatlich relevanter Zeitverlust dürfte ebenfalls nicht eintreten. Ein entsprechender Mechanismus zur Untersagung bzw. Löschung der Angebote an der Quelle könnte auch im Lichte der erheblichen strafrechtlichen Relevanz kinderpornographischer Angebote gesetzlich geregelt werden, ohne auf das in der gegenwärtigen Form häufig langwierige jugendmedienschutzrechtliche Verfahren nach § 20 Abs. 4 JMStV i.V.m. § 59 Abs. 3 u. 4 RStV zurückgreifen zu müssen. Durch ein zielgerichtetes Vorgehen an der Quelle würden die mit Zugangserschwerungen einhergehenden vielfältigen Grundrechtseingriffe beschränkt. Auch die betroffenen Grundrechtsträger wären bei Maßnahmen an der Quelle im Vorfeld klar identifiziert. Dagegen werden nach dem Gesetzentwurf zur Umsetzung der Sperrmaßnahmen Access-Provider als polizei- und ordnungsrechtliche „Nicht-Störer“ in Anspruch genommen.

45. Die intendierten Sperrmaßnahmen setzen daneben voraus, dass die durch das Fernmeldegeheimnis geschützte Internetkommunikation aller Internetnutzer ausgewertet wird. Schließlich wird die Eingriffsintensität auch gegenüber Webseitenbetreibern dadurch verstärkt, dass aufgrund der unbestimmten gesetzlichen Regelung die konkrete Gefahr des (Mit-)Sperrens rechtmäßiger Inhalte besteht (vgl. dazu bereits Rn. 5 ff. dieser Stellungnahme). Zugangserschwerungen würden bei Inlandssachverhalten daher jedenfalls nicht dem Gebot der Erforderlichkeit genügen.

b) Auslandssachverhalte

46. Die vorstehenden Erwägungen gelten grundsätzlich auch bei Auslandssachverhalten. Maßnahmen gegen Content- oder Host-Provider im Ausland setzen die Bereitschaft zur Kooperation ausländlicher Behörden voraus, soweit die betreffenden Diensteanbieter kinderpornographische Inhalte nicht freiwillig löschen. Tatsächlich wird mit vielen Staaten eine Kooperation der Polizeibehörden gepflegt, wobei insbesondere im Rahmen der Europäischen Gemeinschaft auf eine enge Zusammenarbeit bei der Bekämpfung von Kinderpornographie zu verweisen ist (vgl. nur den *Rahmenbeschluss 2004/68/JI des Rates vom 22. Dezember 2003 zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie*, ABl. der EU vom 20.01.2004, L13, S. 44 ff.). Aufgrund des EU-Rahmenbeschlusses wurde die Strafverfolgung im Hinblick auf Kinderpornographie in der Europäischen Union harmonisiert und gleichzeitig eine möglichst breite justizielle Zusammenarbeit angestrebt (vgl. Erwägungsgrund 7 des Rahmenbeschlusses). Dies könnte als Beleg dafür angeführt werden, dass jedenfalls die justizielle Zusammenarbeit innerhalb der Europäischen Gemeinschaft als milderes Mittel gegenüber Sperrungen bezogenen auf Sachverhalte, die andere EU-Mitgliedstaaten betreffen, gilt.

47. Allerdings hat die Europäische Kommission am 25. März 2009 einen Vorschlag für einen neuen Rahmenbeschluss vorgelegt, der folgenden Art. 18 enthält (KOM(2009) 135 endg.; vgl. http://dip21.bundestag.de/dip21/brd/2009/0297-09.pdf):

> **„Artikel 18 - Sperrung des Zugangs zu Webseiten, die Kinderpornografie enthalten**
> Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, damit die zuständigen Justiz- oder Polizeibehörden vorbehaltlich angemessener Schutzvorschriften die Sperrung des Zugangs von Internet-Nutzern zu Webseiten, die Kinderpornografie enthalten oder verbreiten, anordnen oder auf ähnliche Weise erwirken können; insbesondere soll sichergestellt werden, dass die Sperrung auf das Nötige beschränkt wird, dass die Nutzer über die Gründe für die Sperrung informiert werden und dass Inhalteanbieter darüber unterrichtet werden, dass sie die Entscheidung anfechten können."

48. Danach werden – jedenfalls nach dem Wortlaut des Entwurfs – ebenfalls Internetsperren im Zusammenhang mit Kinderpornographie angedacht, die nicht auf Sachverhalte außerhalb der Europäischen Gemeinschaft beschränkt sind. Der betreffende Rahmenbeschluss ist bisher nicht vom Rat verabschiedet worden. Trotzdem kann die Haltung der Europäischen Kommission als Argument dafür herangezogen werden, dass die Mitgliedstaaten die ihnen gebührende Einschätzungsprärogative durch Sperrungsmaßnahmen für alle Auslandssachverhalte nicht überschreiten.

49. Trotzdem dürften Zugangserschwerungen, die Sachverhalte auf dem Territorium eines Mitgliedsstaats der Europäischen Gemeinschaft betreffen, hinsichtlich des Gebots der Erforderlichkeit in Frage stehen. Die justitielle Zusammenarbeit zur Bekämpfung von Kinderpornographie ist gemeinschaftsrechtlich geregelt. Zudem bestehen aufgrund der Richtlinien

über den elektronischen Geschäftsverkehr und über audiovisuelle Mediendienste gemeinschaftsrechtlich vorgegebene Konsultations- und Prüfungsverfahren, die wesentliche Verfahrensvorschriften des Gemeinschaftsrechts darstellen, deren Missachtung die Unanwendbarkeit einer nationalen Maßnahme zur Folge hat (vgl. *Frey/Rudolph*, ZUM 2008, 564 [567 ff.].

4. Angemessenheit

50. Das Gebot der Verhältnismäßigkeit im engeren Sinne – auch als Angemessenheit bezeichnet – verlangt, dass die Schwere der Eingriffe bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen darf (vgl. BVerfGE 90, 145 [173]; 109, 279 [349 ff.]; 113, 348 [382]; stRspr des Bundesverfassungsgerichts).

a) Problem der unzureichenden Normenbestimmtheit und Normenklarheit

51. Leidet eine Eingriffsermächtigung bereits an dem Mangel hinreichender Normenbestimmtheit und Normenklarheit kann sich dies nach der Rechtsprechung des Bundesverfassungsgerichts auch auf die Verhältnismäßigkeit im engeren Sinne auswirken (vgl. BVerfGE 110, 33 [55]). In solchen Fällen kann die notwendige Abwägung zwischen dem gesetzlichen Schutzgut und der Schwere des Eingriffs nicht auf einer nachvollziehbaren Tatsachenbasis vorgenommen werden (vgl. zu einer ähnlichen Erwägung BVerfG, Urteil v. 27.07.2005, 1 BvR 668/04, Rn. 147).

52. Während das gesetzliche Schutzgut im Hinblick auf Kinderpornographie gem. § 184b StGB klar zu identifizieren ist (Probleme ergeben sich ggf. im Hinblick auf ebenfalls vorgesehene Verweissperrungen), hängt die Eingriffsintensität der intendierten Sperrmaßnahmen maßgeblich von der Sperrkategorie (vollqualifizierte Domainnamen, Internetprotokoll-Adressen und Zieladressen) ab, die nach § 8a Abs. 1 TMG-E gleichberechtigt nebeneinander stehen sollen (vgl. dazu oben Rn. 9). Gleichzeitig wird Access-Providern als Privaten gem. § 8a Abs. 2 TMG überlassen, welche konkreten Maßnahmen sie ergreifen (vgl. dazu oben Rn. 19). Dadurch lässt sich der Rahmen einer „*ordnungsgemäßen*“ Durchführung der Sperrmaßnahmen durch Access-Provider nur schwer voraussehen. Damit steht die indendierte Haftungsfreistellung für Access-Provider in Frage und es besteht die Gefahr der (Mit-)Sperrung einer erheblichen Zahl rechtmäßiger Angebote (vgl. dazu oben Rn. 5 ff.). Schließlich ist der Umfang, der am Server mit der gehosteten Stoppmeldung anfallenden personenbezogenen Daten unklar. Insofern fehlt es für eine nachvollziehbare Abwägung der geschützten Rechtsgüter der Kinder (insbesondere die Verhinderung der Perpetuierung der schwerwiegenden Persönlichkeitsverletzung durch die Abbildung des Missbrauchs) gegenüber den Eingriffen in die Grundrechte von Access-Providern, Webseitenbetreibern und Nutzern derzeit an einer belastbaren Tatsachengrundlage.

b) Fehlende verfahrensrechtliche Absicherung und Heimlichkeit

53. Nach dem Gesetzentwurf leiten Diensteanbieter Nutzeranfragen zu in der Sperrliste aufgeführten Telemedienangeboten auf ein von ihnen betriebenes Telemedienangebot – eine Stoppmeldung – um, das die Nutzer über die Gründe sowie eine Kontaktmöglichkeit zum Bundeskriminalamt informiert (§ 8a Abs. 4 TMG-E). Das Bundeskriminalamt soll Diensteanbietern im Sinne des TMG – also Content-, Host- und Access-Providern –, die ein berechtigtes Interesse darlegen, auf Anfrage

Auskunft darüber erteilen, ob und in welchem Zeitraum ein Telemedienangebot in der Sperrliste enthalten ist oder war. Einen darüber hinausgehenden verfahrensrechtlichen Rahmen enthält der Gesetzentwurf nicht. Es darf bezweifelt werden, dass die genannte Regelung des Gesetzentwurfs verfassungsrechtlichen Anforderungen genügt:

54. Das Bundesverfassungsgericht hat in seiner Entscheidung zu Online-Durchsuchungen (BVerfG, Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, S. 822 [832 f. Rn. 257 ff.]) entschieden, dass sich bei einem Grundrechtseingriff von besonders hohem Gewicht – wie dem heimlichen Zugriff auf ein informationstechnisches System – der Spielraum des Gesetzgebers dahingehend reduziert, die Maßnahme grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Richter könnten aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Betroffenen im Einzelfall am besten und sichersten wahren (vgl. BVerfGE 103, 142 [151]; 107, 299 [325], BVerfG, Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, S. 822 [832 f. Rn. 259). Vorausgesetzt ist allerdings, dass sie die Rechtmäßigkeit der vorgesehenen Maßnahme eingehend prüfen und die Gründe schriftlich festhalten. Nach der Rechtsprechung des Bundesverfassungsgerichts darf der Gesetzgeber eine andere Stelle nur dann mit der Kontrolle betrauen, wenn diese gleiche Gewähr für ihre Unabhängigkeit und Neutralität bietet wie ein Richter. Auch von ihr müsse eine Begründung zur Rechtmäßigkeit gegeben werden (BVerfG, Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, S. 822 [833 Rn. 260]). Ein Richtervorbehalt könne bedeutsames Element eines effektiven Grundrechtsschutzes sein. Er könne gewährleisten, dass die Entscheidung über eine heimliche Maßnahme auf die Interessen des Betroffenen hinreichend Rücksicht nimmt, wenn der Betroffene selbst seine Interessen aufgrund der Heimlichkeit der Maßnahme im Vorwege nicht wahrnehmen kann. Die Kontrolle diene insoweit der „*kompensatorischen Repräsentation*“ der Interessen des Betroffenen im Verwaltungsverfahren (vgl. SächsVerfGH, Urteil vom 14. Mai 1996 - Vf.44-II-94 -, JZ 1996, S. 957 [964], BVerfG, Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, S. 822 [832 Rn. 258]).

55. Betrachtet man den vorliegenden Gesetzentwurf, dürfte er den vorstehenden Kriterien des Bundesverfassungsgerichts nicht gerecht werden. Bei der Beurteilung der grundrechtlichen Relevanz der durch den Gesetzentwurf vorgesehenen Verpflichtung für Access-Provider zur Sperrung kinderpornographischer Inhalte ist zu beachten, dass neben dem in Art. 10 GG geschützten Telekommunikationsgeheimnis der Nutzer, der Berufsfreiheit gem. Art. 12 GG bzw. der Eigentumsgarantie gem. Art. 14 GG der Access-Provider und Webseitenbetreiber die Meinungs-, Presse-, Informations-, Kunst- und Wissenschaftsfreiheit gem. Art. 5 GG von Nutzern und Webseitenbetreibern betroffen sein können; Access-Providern kommt in unserer heutigen Gesellschaft nicht nur im Hinblick auf die Informationsbeschaffung der Bürger, sondern auch für ihre berufliche und wirtschaftliche Betätigung eine herausragende Rolle zu. Sollte eine Maßnahme auch legale Informationen und Angebote treffen, kann dies zu schwerwiegenden Eingriffen in die Grundrechte von unbeteiligten Dritten führen. Das Internet stellt einen beachtlichen Wirtschaftsfaktor dar. Nicht wenige Personen bestreiten heutzutage mittels des Internets ihren Lebensunterhalt z.B. durch den Betrieb von Online-Shops. Die Bewerbung und das Angebot von Waren und Dienstleistungen über das Internet sind für die Wirtschaft in einer zunehmend digital und konvergent geprägten Gesellschaft von größter Bedeutung. Erfassen „Sperren“ legale Angebote, können diese in vielerlei Hinsicht sehr weitreichende wirtschaftliche Folgen nach sich ziehen. Gleiches gilt im Hinblick auf die Informationsbeschaffung und den Meinungsbildungsprozess als konstitutive Elemente unserer freiheitlich demokratischen

Grundordnung. Auch eine global vernetzte Wissenschaft könnte entsprechend tangiert werden. Außerdem gilt es zu berücksichtigen, dass die Zugangserschwerungen, die auch legale Informationen und Angebote treffen, für die Betreiber dieser Angebote heimlich erfolgen. Es besteht zum einen keine Möglichkeit, rechtlich bereits im Vorfeld hiergegen vorzugehen, etwa gerichtlichen Rechtsschutz in Anspruch zu nehmen. Zum anderen gibt es bei heimlich vorgenommenen Maßnahmen faktisch keine Möglichkeit, durch das eigene Verhalten auf den Gang eines Verfahrens einzuwirken. Der Ausschluss dieser Einflusschancen verstärkt das Gewicht des Grundrechtseingriffs (vgl. hierzu BVerfG, Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, S. 822 [830 Rn. 238]).

56. Angesichts dieser grundrechtlich vielschichtigen Relevanz der durch den Gesetzentwurf vorgesehenen Zugangserschwerungen durch Access-Provider, die zu Grundrechtseingriffen von besonders hohem Gewicht führen können, über die zudem die Betroffenen – bis auf die Nutzer – keine Mitteilung erhalten, dürfte sich der verfahrensrechtliche Spielraum des Gesetzgebers dahingehend reduzieren, die Sperrliste unter einen Richtervorbehalt zu stellen. Darüber hinaus fehlt es an einem formalisierten Verfahren, mit dem zu Unrecht durch Zugangserschwerungen Betroffene sich gegen die Maßnahme zur Wehr setzen können. Der in § 8a Abs. 8 S. 2 TMG-E vorgesehene Auskunftsanspruch genügt insoweit nicht. Der Auskunftsanspruch gewährt bereits keine Auskunft darüber, ob sich hinter dem Listeneintrag überhaupt Kinderpornographie verbirgt und aufgrund welcher Annahmen und Unterlagen ein Angebot in die Liste aufgenommen wurde.

c) Auswertung des gesamten Datenverkehrs der Internetnutzer

57. Eine Zugangserschwerung zu kinderpornographischen Angeboten im Internet auf der Basis der von dem BKA erstellten Sperrlisten setzt voraus, dass der gesamte Datenverkehr der Internetnutzer ausgewertet wird. Die Identifikation des Ansurfens kinderpornographischer Internetinhalte kann nur erfolgen, wenn ein Selektionsmechanismus auf der Basis der adressierten Sperrkategorien (vollqualifizierte Domainnamen, Internetprotokolladresse oder Zieladresse) vorgenommen wird.

58. Das Grundrecht des Fernmeldegeheimnisses dient der freien Entfaltung der Persönlichkeit durch einen Kommunikationsaustausch mit Hilfe des Fernmeldeverkehrs (BVerfGE 106, 28 [35f.]). Bei der Nutzung von Telekommunikationseinrichtungen ist die Kommunikation besonderen Gefährdungen der Kenntnisnahme durch Dritte ausgesetzt und unterliegt deshalb besonderem Schutz (BVerfGE 106, 28, [36]; vgl. bereits BVerfGE 67, 157 [171f.]; 85, 386 [396]). Das Fernmeldegeheimnis soll gegen eine vom Betroffenen ungewollte Informationserhebung schützen und die Privatheit auf Distanz gewährleisten (BVerfGE 115, 166 [182]; Beschluss vom 22.08.2006, 2 BvR 1345/03 – IMSI-Catcher, NJW 2007, 351 [353 – Rn. 51]). Nach der Rechtsprechung des Bundesverfassungsgerichts (vgl. BVerfGE 107, 299 [313]) soll mit der grundrechtlichen Verbürgung der Unverletzlichkeit des Fernmeldegeheimnisses zudem vermieden werden, dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen. Das Fernmeldegeheimnis dient damit indirekt dem Schutz der ebenfalls betroffenen Informationsfreiheit.

59. Gegen Fernmeldegeheimnis und Informationsfreiheit müssen der Opferschutz und die legitime Erwägung präventiver Maßnahmen gegen Kinderpornographie im Internet abgewogen werden. Diese im Allgemeininteresse stehenden Schutzgüter können Eingriffe rechtfertigen. Allerdings sind die vorgeschlagenen gesetzlichen Eingriffsvoraussetzungen unbestimmt und mit potentiell weitreichenden Kollateralschäden im Hinblick auf rechtmäßige Inhalte verbunden, sodass die Gefahr eines erheblichen Streuverlusts entsteht, der dazu geeignet ist, das Vertrauen des Einzelnen in die Fernkommunikation zu erschüttern. Hier wirkt sich erschwerend aus, dass die Entscheidung des BKA über die Aufnahme eines Inhalts in die Sperrliste heimlich erfolgen soll und zudem keine verfahrensrechtliche Absicherung einer solchen Entscheidung erfolgt. Vor diesem Hintergrund ist davon auszugehen, dass der Gesetzentwurf in der derzeitigen Form das Übermaßverbot im Hinblick auf die Auswertung des gesamten Internetverkehrs der Nutzer verletzt.

d) Verwendung personenbezogener Daten der Internetnutzer zur Strafverfolgung

60. Am Server, der die Stoppmeldung hostet, würden aufgrund der intendierten Umleitung der Internetkommunikation in erheblichem Umfang personenbezogene Daten anfallen. Diese Daten sollen nach dem Gesetzentwurf zur Strafverfolgung genutzt werden können (vgl. § 8a Abs. 5 S. 2 TMG-E). Die effektive Verfolgung der schwerwiegenden Straftaten gemäß § 184b StGB liegt im Allgemeininteresse. Zudem handelt es sich bei den betreffenden Straftaten um Offizialdelikte, die von den Strafverfolgungsbehörden nach dem Legalitätsprinzip verfolgt werden müssen. Die am Stopp-Server anfallenden Nutzungsdaten könnten wichtige Indizien zur Aufklärung der Straftaten sein. Allerdings stellt sich aufgrund der unklaren Eingriffsvoraussetzungen hinsichtlich der Aufnahme in die Sperrliste und der Umsetzung der Liste durch Access-Provider wiederum das Problem, dass Nutzungsdaten von unbescholtenen Bürgern in großem Umfang am Stopp-Server anfallen können. Dabei ist zu berücksichtigen, dass es sich bei Kinderpornographie im Sinne des § 184b StGB um ein sog. Unternehmensdelikt handelt, wonach neben der Vollendung bereits der Versuch der Besitzverschaffung strafbar ist (vgl. § 11 Nr. 6, § 184b Abs. 4 StGB).

61. Nur im Falle zielgenauer Zugangserschwerungen könnten nach dem Vorgesagten Ermittlungstätigkeiten wie der Abgleich der am Stopp-Server anfallenden IP-Adresse mit der durch den Access-Provider für einen Kunden zu einem bestimmten Zeitpunkt vergebenen dynamischen IP-Adresse erwogen werden. Weitergehende Maßnahmen wie Durchsuchungen und Beschlagnahmen von Computern dürften aufgrund der Fehleranfälligkeit erst dann angemessen sein, wenn anderweitige qualifizierte Anhaltspunkte für kinderpornographische Straftaten vorliegen. Die genannten weiteren Maßnahmen sind mit erheblicher grundrechtlicher Eingriffsintensität verbunden und können bereits für sich genommen zu einer sozialen Ächtung des Betroffen führen.

62. Da die Eingriffsvoraussetzungen für die Aufnahme in die Sperrliste sowie die Umsetzungsverpflichtung für Access-Provider allerdings gänzlich unklar und unbestimmt sind, besteht generell die erhebliche Gefahr, dass in großem Umfang an den Stopp-Servern personenbezogene Daten unbescholtener Bürger anfallen. Der Gesetzentwurf führt daher in der derzeitigen Form nicht nur zu einem Eingriff in das Recht auf informationelle Selbstbestimmung, sondern zu der Gefahr von weiteren Grundrechtseingriffen, die in Ausmaß und Rechtsfolgen nicht voraussehbar sind. Auch insofern würde die Verabschiedung des Gesetzes in der gegenwärtigen Fassung zu einer Verletzung des Übermaßverbots führen.

e) Keine ausreichenden Vorkehrung zum Schutz rechtmäßiger Angebote

63. Wie bereits mehrfach angeführt, hat die Unbestimmtheit der Eingriffsvoraussetzungen zur Folge, dass die konkrete Gefahr einer (Mit-)Sperrung rechtmäßiger Angebote besteht. Der Entwurf wirkt dem auch nicht durch gesetzliche Vorkehrungen entgegen, die den Schutz rechtmäßiger Angebote verfahrensmäßig absichern.

64. Die Prüfung der in die Sperrliste aufzunehmenden Angebote erfolgt alleine durch das BKA. Der Gesetzentwurf sieht weder eine vorherige noch eine nachträgliche Kontrolle dieser Entscheidung durch einen Richter vor. Auch werden Webseitenbetreiber nicht über die beabsichtigte Aufnahme in die Sperrliste im Vorfeld informiert. Der Gesetzentwurf überlässt den konkreten Rahmen und die Intensität des unmittelbaren Eingriffs in die Rechte der Betroffenen zudem den Access-Providern. Er verlagert damit einen Teil der Verantwortung für fehlerhafte Maßnahmen auf Private.

65. Der Gesetzentwurf regelt auch keine Verpflichtung des BKA zu regelmäßigen Kontrollen der in der Sperrliste enthaltenen Sperrkategorien im Hinblick auf Telemedienangebote. Pflichten zur nachträglichen Überprüfung der Einträge auf Richtigkeit und gesetzliche Kriterien, die zu einer Löschung eines Eintrags der Sperrlisten verpflichten, fehlen.

66. Effektiven Rechtsschutz der betroffenen Webseitenbetreiber gewährt der Gesetzentwurf ebenfalls nicht. Betreiber erfahren allenfalls zufällig davon, dass ihre Webseiten von der (ob gewollt oder ungewollt) Sperrliste erfasst werden. Sie haben im Vorfeld der Aufnahme in die Sperrliste keine rechtliche Handhabe, um sich gegen die Maßnahme des BKA (und sich daran anschließende Maßnahme der Access-Provider) zur Wehr zu setzen. Die gleiche Problematik dürfte auch für die Effektivität des nachträglichen Rechtsschutzes bestehen, da der Gesetzentwurf kein Verfahren vorsieht, mit dem der betroffene Webseitenbetreiber die Löschung des ihn belastenden Eintrags von der Liste durchsetzen kann. Daher dürfte der Gesetzentwurf in der derzeitigen Form auch insofern das Übermaßverbot verletzen.

f) Unzureichende Haftungsfreistellung für Access-Provider

67. Die Haftungsfreistellung für Access-Provider nach § 8a Abs. 7 TMG-E greift nur bei „*ordnungsgemäßer*“ Umsetzung der Sperrliste. Was unter einer „*ordnungsgemäßen*“ Umsetzung der Sperrmaßnahmen zu verstehen ist, lässt sowohl der regelnde Teil als auch die Begründung des Gesetzentwurfs offen. Wie bereits unter Randnummern 5 ff. dieser Stellungnahme ausgeführt, bergen die unbestimmten Eingriffsvoraussetzungen ein erhebliches Fehlerpotential. So bleibt etwa offen, ob und inwieweit die Haftungsfreistellung auch die technisch bedingte (Mit-)Sperrung rechtmäßiger Angebote erfassen soll. Außerdem enthält der Gesetzentwurf keine Regelung zu fehlerhaften oder veralteten Listeneinträgen, die ebenfalls zur Sperrung rechtmäßiger Angebote führen können. Die damit einhergehende Rechtsunsicherheit ist Access-Providern als verwaltungs- und polizeirechtlichen Nichtstörern nicht zuzumuten. Der Gesetzentwurf würde in der derzeitigen Form insofern ebenfalls das Übermaßverbot verletzen.

g) Fehlende Übergangsregelung für Access-Provider

68. Der Gesetzentwurf enthält keine Übergangsregelung für die Implementierung der nach § 8a Abs. 2 TMG-E geforderten Sperrinfrastruktur durch Access-Provider. Dabei handelt es sich um technisch

anspruchsvolle Prozesse, die dem gegenwärtigen Geschäftsmodell und den aktuellen gesetzlichen Verpflichtungen (Telekommunikationsgeheimnis) von Access-Providern widersprechen. Wie von Access-Providern zu hören ist, erfordert die Implementierung der Sperrinfrastruktur mindestens sechs Monate. Ohne gesetzliche Bestimmung einer Übergangsfrist würde das Gesetz daher gegen das Gebot der Verhältnismäßigkeit verstoßen.

h) Fehlende Kostenerstattung

69. Der Gesetzentwurf enthält keine Kostenerstattungsregeln zu Gunsten von Access-Providern. Access-Provider sind polizei- und ordnungsrechtliche Nichtstörer. Sie sollen zur Umsetzung staatlicher Aufgaben der Gefahrenabwehr verpflichtet werden. Eine angemessene gesetzliche Regelung müsste daher die Erstattung der Kosten für die Einrichtung und den Betrieb der Sperrungsinfrastruktur vorsehen.

III. Gesetzgebungskompetenz des Bundes

70. Der Begründung des Gesetzentwurfs zufolge steht dem Bund die Gesetzgebungskompetenz für die angedachten Regelungen zur Bekämpfung von kinderpornographischen Inhalten in Kommunikationsnetzen zu.

1. Gesetzgebungskompetenz für Zugangserschwerungen durch Access-Provider zu kinderpornographischen Inhalten

71. In der Begründung des Gesetzentwurfs wird die Pflicht der Access-Provider gem. §8a Abs. 2 TMG-E, den Zugang zu kinderpornographischen Telemedienangeboten durch technische Vorkehrungen zu erschweren, auf den zur konkurrierenden Gesetzgebung gehörenden Kompetenztitel des Art. 74 Abs. 1 Nr. 11 GG gestützt. Zur Begründung wird angeführt, dass nach der Rechtsprechung des Bundesverfassungsgerichts Art. 74 Abs. 1 Nr. 11 GG alle Regelungen abdeckt, die das wirtschaftliche Leben und die wirtschaftliche Betätigung als solche regeln und dass diese Kompetenznorm Gesetze mit wirtschaftsregulierenden oder wirtschaftslenkenden Inhalten umfasst. Die Pflicht zur Erschwerung des Zugangs zu kinderpornographischen Telemedienangeboten sei als solche wirtschaftslenkende Maßnahme zu qualifizieren, da sie die Diensteanbieter in der Ausübung ihrer wirtschaftlichen Tätigkeit reglementiere. Im Übrigen stütze sich das TMG auch schon bislang auf Art. 74 Abs. 1 Nr. 11 GG (vgl. Seite 7 der Begründung des Gesetzentwurfs).

72. Die Pflicht zur Erschwerung des Zugangs zu kinderpornographischen Telemedienangeboten als rein wirtschaftslenkende Maßnahme zu qualifizieren, da sie die Diensteanbieter in der Ausübung ihrer wirtschaftlichen Tätigkeit reglementiere, erscheint zweifelhaft. Der in das TMG neu einzufügende § 8a TMG-E trägt die Überschrift „*Erschwerung des Abrufs von Kinderpornographie in Kommunikationsnetzen*“. Bereits hiernach wird man annehmen dürfen, dass der Gesetzentwurf vorrangig das Ziel verfolgt, Gefahren durch Kinderpornographie in Kommunikationsnetzen, die dem Einzelnen und der Allgemeinheit drohen, zu bekämpfen. Zu diesem Zweck sollen Access-Provider

verpflichtet werden, den Zugang zu Telemedienangeboten, die in einer Sperrliste aufgeführt sind, zu erschweren. In der Begründung des Gesetzentwurfs wird ausgeführt, dass gegen die sexuelle Ausbeutung von Kindern im Internet mit allen Mitteln vorgegangen werden soll. Es sei nicht hinnehmbar, dass bekannte kinderpornographische Telemedienangebote teilweise wochen- oder jahrelang weiter genutzt werden können. Durch die Zugangserschwerung sollen Access-Provider ausweislich der Gesetzesbegründung ihren Beitrag dazu leisten, die Verbreitung und Besitzverschaffung von Kinderpornographie zu erschweren. Insbesondere im Lichte des Titels und der Begründung des Gesetzentwurfs wird man daher als Regelungsgegenstand und Normzweck des Gesetzentwurfs die Abwehr von Gefahren, namentlich die Abwehr von Gefahren durch Telemedien im Hinblick auf die Besitzverschaffung und Verbreitung von Kinderpornographie, identifizieren können, nicht hingegen wirtschaftslenkende Maßnahmen im Sinne des Art. 74 Abs. 1 Nr. 11 GG.

73. Allerdings ließe sich eine konkurrierende Gesetzgebungskompetenz des Bundes für die Pflicht zur Zugangserschwerung zu kinderpornographischen Telemedienangeboten unter Bezugnahme auf Art. 74 Abs. 1 Nr. 11 GG begründen, wenn sich die angedachten Zugangserschwerungen als ordnungsrechtlicher Annex des Rechts der Wirtschaft erweisen würden. Nach der Rechtsprechung des Bundesverfassungsgerichts kann die Ordnungsgewalt als Annex des Sachgebiets erscheinen, auf dem sie tätig wird; die Zuständigkeit zur Gesetzgebung in einem Sachbereich umfasst dann auch die Regelung der Ordnungsgewalt (Polizeigewalt) in diesem Sachbereich (vgl. BVerfGE 8, 143 [149]). Soweit der Bund ein Recht zur Gesetzgebung auf einem bestimmten Lebensgebiet hat, muss er demnach auch das Recht haben, die dieses Lebensgebiet betreffenden spezialpolizeilichen Vorschriften zu erlassen (vgl. BVerfGE 3, 407 [433]; 8, 143 [149 f.]). Normen, die der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung in einem bestimmten Sachbereich dienen, sind daher jeweils dem Sachbereich zuzurechnen, zu dem sie in einem notwendigen Zusammenhang stehen (vgl. BVerfGE 8, 143 [149 f.]; 28, 119 [146]). Nur solche Regelungen, bei denen die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung den alleinigen und unmittelbaren Gesetzeszweck bildet, können einem selbständigen Sachbereich zugerechnet werden, der als Polizeirecht im engeren Sinne bezeichnet wird und in die Zuständigkeit der Landesgesetzgebung fällt (BVerfGE 8, 143 [150]).

74. Zwar lässt sich argumentieren, dass durch die vorgesehene Zugangserschwerung das wirtschaftliche Betätigungsfeld der Access-Provider in ordnungsrechtlicher Hinsicht beschränkt wird. Hiergegen lässt sich jedoch einwenden, dass durch die angedachte Regelung im Kern Gefahren, die durch kinderpornographische Inhalte in Kommunikationsnetzen für den Einzelnen und für die Allgemeinheit entstehen, begegnet werden soll, mithin dem Problem der Kinderpornographie. Dass Access-Provider durch die ihnen nach dem Gesetzentwurf auferlegte Verpflichtung, den Zugang zu kinderpornographischen Inhalten zu erschweren, auch in ihrer wirtschaftlichen Freiheit betroffen sind, stellt dann nur einen logischen Reflex der durch die Regelung bezweckten Gefahrenabwehr dar. Es würde sich in Wahrheit um eine ordnungsrechtliche Sonderregelung der Regelungsmaterie Kinderpornographie handeln, nicht hingegen um eine wirtschaftsrechtliche Regelung von kinderpornographischen Telemedien. Unter dem Blickwinkel der den Ländern traditionell zustehenden Gesetzgebungskompetenz zur Gefahrenabwehr (vgl. z.B. BVerfG, Urteil v. 27.07.2005, Az. 1 BvR 668/04, Rn. 94), würde die Gesetzgebungskompetenz für die beabsichtigten Zugangserschwerungen zu kinderpornographischen Telemedien durch Access-Provider dann den Ländern zustehen.

2. Gesetzgebungskompetenz für Sperrliste des BKA

75. Die Befugnis des BKA gem. § 8a Abs. 1 TMG-E, eine Liste über voll qualifizierte Domainnamen, Internetprotokoll-Adressen und Zieladressen von Telemedienangeboten zu führen, die Kinderpornographie nach § 184 b StGB enthalten oder deren Zweck darin besteht auf derartige Telemedienangebote zu verweisen (Sperrliste) und den zur Zugangserschwerung verpflichteten Access-Providern zur Verfügung zu stellen, wird in der Gesetzesbegründung auf Art. 73 Abs. 1 Nr. 10 GG, eine der ausschließlichen Gesetzgebungskompetenzen des Bundes, gestützt. Eine Erläuterung enthält die Begründung des Gesetzentwurfs hierzu nicht (vgl. Seite 8 der Begründung des Gesetzentwurfs).

76. Durch § 8a Abs. 1 TMG-E wird nicht die Zusammenarbeit des Bundes und der Länder im Rahmen der Kriminalpolizei, des Verfassungsschutzes oder auswärtiger Belange geregelt, wie es der Kompetenztitel des Art. 73 Abs. 1 Nr. 10 GG vorsieht. Darüber hinaus dürfte dem Bund auch keine Kompetenz im Hinblick auf die in dem Kompetenztitel des Art. 73 Abs. 1 Nr. 10 genannte internationale Verbrechensbekämpfung zukommen. Darunter ist nicht die Bekämpfung internationaler Verbrechen, sondern die internationale Bekämpfung von Verbrechen, also etwa die Zusammenarbeit deutscher mit ausländischen Stellen in kriminalpolizeilichen Fragen, zu verstehen (BVerfG, Urteil v. 14.07.1999, 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Rn. 199; vgl. *Degenhardt* in Sachs, Art. 73, Rdnr. 53, der hierzu die Verhütung und Verfolgung von Straftaten in internationaler Zusammenarbeit, durch Amtshilfe, wechselseitige Informationen u.ä. zählt). Im Übrigen fällt das Polizeirecht als Gefahrenabwehrrecht in die Zuständigkeit der Länder (BVerfG, Urteil v. 14.07.1999, 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Rn. 199). Dem Zweck einer internationalen Bekämpfung von Kinderpornographie dient die in dem Gesetzentwurf vorgesehene Regelung nicht. Der Gesetzentwurf sieht nicht vor, dass Kinderpornographie im Rahmen internationaler Zusammenarbeit verhütet oder verfolgt werden soll. Vielmehr wird dem BKA die Befugnis zugewiesen, kinderpornographische Telemedienangebote in einer Sperrliste zu führen sowie die Befugnis, diese Sperrliste Access-Providern für Zugangserschwerungsmaßnahmen zur Verfügung zu stellen. Hierbei handelt es sich um die nationale Abwehr von Gefahren durch Kinderpornographie, nicht hingegen um deren internationale Bekämpfung. Dies gilt umso mehr als der Gesetzentwurf auch die Zugangserschwerung zu nationalen kinderpornographischen Inhalten durch Access-Provider vorsieht. Im Ergebnis erscheint eine Gesetzgebungskompetenz des Bundes gem. Art. Art. 73 Abs. 1 Nr. 10 GG für § 8a Abs. 1 TMG-E daher problematisch.

C. Spezialgesetz statt Ergänzung des Telemediengesetzes

77. Die beabsichtigte Integration des § 8a TMG-E in das TMG erweist sich nicht nur als gesetzessystematischer Mangel, sondern schwächt auch die in der Begründung zum Gesetzentwurf angeführte Zielrichtung, dass eine Ausweitung auf andere Zwecke als dem Kampf gegen kinderpornographische Seiten nicht beabsichtigt ist.

I. Gesetzessystematischer Mangel

78. Der Abschnitt 3 des TMG regelt die Haftungsprivilegierung für Diensteanbieter. Er dient der Umsetzung der Richtlinie über den elektronischen Geschäftsverkehr, die detaillierte Regeln über die Verantwortlichkeit von Diensteanbietern vorgibt, in deutsches Recht. Nach der Gesetzesbegründung des TMG sollen die §§ 7 ff. TMG der Vollharmonisierung dienen, d.h. die Mitgliedsstaaten dürfen weder weitere noch engere Regeln im nationalen Recht treffen.

79. Die Bestimmungen sind als Filter konzipiert, der selbst weitergehende Verantwortlichkeiten von Diensteanbietern weder begründet noch die Haftung nach den allgemeinen Gesetzen erweitert. Die dogmatische Einordnung der Filterfunktion der §§ 7 bis 10 TMG ist im Einzelnen umstritten. Am Treffendsten lassen sich die Bestimmungen als tatbestandsintegrierter Vorfilter charakterisieren, der eine rechtsgebietsübergreifende Querschnittsregelung für das Straf-, Zivil- und Verwaltungsrecht darstellt (vgl. zum Ganzen *Frey/Rudolph*, Rechtsgutachten zur Evaluierung des Haftungsregimes für Host- und Access-Provider im Bereich der Telemedien, Rdnr. 4 ff.). Das TMG enthält folglich weder verwaltungsrechtliche Befugnisnormen noch zivilrechtliche Anspruchsgrundlagen. Diese können sich nach der Konzeption des Gesetzes aus den allgemeinen Gesetzen ergeben und unter bestimmten Voraussetzungen auch Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Internetinhalten regeln (vgl. § 7 Abs. 2 S. 2 TMG).

80. Der vorgeschlagene § 8a TMG-E widerspricht diesem systematischen Ansatz grundlegend. Er stellt eine vertikale Sonderregelung dar, der Zuständigkeiten und Befugnisse des BKA regelt, Access-Providern die Verpflichtungen zum Aufbau einer Sperrinfrastruktur sowie zur Einrichtung eines Stopp-Servers auferlegt. Die Bestimmung stellt damit einen Fremdkörper innerhalb der abstrakt und horizontal wirkenden Haftungsprivilegierung für Diensteanbieter dar. Vergleichbare Regelungen sind nach der Konzeption des Gesetzes nur außerhalb der Verantwortlichkeitsbestimmungen des dritten Abschnitts zu finden.

II. Gefahr der Ausweitung von Zugangserschwerungen auf andere Rechtsmaterien

81. Nach dem Gesetzentwurf ist eine Ausweitung der Zugangserschwerungen durch Access-Provider über kinderpornographische Seiten hinaus nicht beabsichtigt. Es ist allerdings zweifelhaft, ob diese in der Gesetzesbegründung zum Ausdruck gebrachte Intention in der Praxis Bestand haben wird.

82. Zugangserschwerungen durch Access-Provider werden nicht nur im Zusammenhang mit Kinderpornographie gefordert. Gleiche Ansinnen werden aktuell auch vor dem Hintergrund des am 1. Januar 2008 in Kraft getretenen Glücksspiel-Staatsvertrags vorgetragen. Von Seiten des BKA ist laut Presseberichten zu hören, dass Access-Provider Webseiten mit terroristischem,

rechtsradikalem und antisemitischem Hintergrund sperren sollen. Die Kommission für Jugendmedienschutz fordert allgemein Sperrungen im Hinblick auf jugendgefährdende Inhalte im Internet. Auch im Lichte des Zivilrechts sind Sperrungsforderungen bereits gerichtlich geltend gemacht worden. Der Fall Youporn hat eine Reihe von Instanzgerichten beschäftigt: Ein deutscher Anbieter von Pornographie wollte ein US-amerikanisches Angebot von Access-Providern mit der Begründung sperren lassen, dass Access-Provider eine wettbewerbsrechtliche Verkehrspflicht verletzen, falls über ihre Internetzugangsinfrastruktur pornographische Angebote aus dem Ausland ohne Altersverifikationssystem nach deutschem Recht zugänglich sind. Schließlich wird von Rechteinhabern der Musik- und Filmindustrie gefordert, Webseiten mit urheberrechtsverletzenden Inhalten zu sperren. Entsprechende Ansprüche werden auf die immaterialgüterrechtliche Störerhaftung gestützt (vgl. zuletzt LG Hamburg, U. v. 12.11.2008 -- 308 O 548/08). Bisher wurden allerdings alle zivilrechtlich begründeten Sperrungsforderungen von den Gerichten abgelehnt.

83. Die Umsetzung des Gesetzentwurfs hätte nicht nur den Aufbau einer universell einsetzbaren Sperrinfrastruktur zur Folge, sondern Access-Provider würden auch dazu verpflichtet, ihre Inhaltsneutralität aufzugeben. Bisher gelten die Internetzugangsdienste von Access-Providern als gesellschaftlich besonders erwünschte, inhaltsneutrale Infrastrukturleistungen, die grundsätzlich blind gegenüber einer rechtlich qualitativen Bewertung der durchgeleiteten Daten und Kommunikationsvorgänge sind. Dieser Befund, der bereits aus dem Geschäftsmodell der Access-Provider folgt, wird derzeit gesetzlich besonders abgesichert. Access-Provider haben das Fernmeldegeheimnis gem. Art.10 GG und einfachgesetzlich gem. § 88 TKG zu wahren, wonach sowohl die Inhalte als auch die näheren Umstände der Internetkommunikation geschützt sind. Soweit Access-Provider im Zusammenhang mit Sperrungsmaßnahmen kinderpornographischer Inhalte zur Aufgabe ihrer inhaltsneutralen Rolle verpflichtet sind, ist insbesondere im Zivilrecht, die nach bisherigem Recht anzunehmende Nichtverantwortlichkeit für die durchgeleiteten Informationen zu hinterfragen. § 8 TMG, der eine weitgehende Haftungsprivilegierung von Access-Providern regelt, würde zwar weiterhin Geltung beanspruchen; allerdings wären Sperrungsforderungen, die nach § 7 Abs. 2 S. 2 TMG bereits heute nicht grundsätzlich ausgeschlossen sind, neu zu bewerten. Bisher sind gerade die inhaltsneutralen Leistungen sowie die Unzumutbarkeit des Aufbaus einer Sperrinfrastruktur wichtige Gründe im Zivilrecht für das Ablehnen der Verantwortung von Access-Providern für rechtswidrige Inhalte gewesen, die sich in den Weiten des Internets befinden. Die dogmatischen Ansätze für die zivilrechtliche Haftung von Access-Providern, es handelt sich um eine täterschaftliche Haftung wegen des Verstoßes gegen wettbewerbsrechtliche Verkehrspflichten und die immaterialgüterrechtliche Störerhaftung, wären nach Inkrafttreten des Gesetzentwurfs neu zu justieren (vgl. zum Ganzen *Frey/Rudolph*, Rechtsgutachten zur Evaluierung des Haftungsregimes für Host- und Access-Provider im Bereich der Telemedien, Rdnr. 309 ff. u. Rdnr. 361 ff.). Die Bestätigung entsprechender Sperrforderungen gegenüber Access-Providern durch die Gerichte ist dann nicht mehr auszuschließen.

D. Detailfragen:

I. Art. 2 – Änderung des Telekommunikationsgesetzes

84. Der Gesetzentwurf sieht eine Änderung des § 96 Abs. 1 TKG vor. Neben der Änderung des § 96 TKG wäre aber auch eine Änderung des § 88 Abs. 3 TKG notwendig.

85. Gem. § 88 Abs. 3 S. 1 TKG ist es den Diensteanbietern untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in § 88 Abs. 3 S. 1 TKG genannten Zweck verwenden (§ 88 Abs. 3 S. 2 TKG). Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist gem. § 88 Abs. 3 S. 3 TKG nur zulässig, soweit das Telekommunikationsgesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht.

86. Die Sperrungsmaßnahmen setzen voraus, dass sich die Access-Provider außerhalb der geschäftsmäßigen Erbringung ihrer Dienste Kenntnisse über Inhalte und/oder die näheren Umstände der Kommunikation verschaffen. Gleichzeitig würden Kenntnisse über Tatsachen, die dem Telekommunikationsgeheimnis unterliegen, zu anderen Zwecken als der Erbringung von Telekommunikationsdiensten verwendet. Sowohl die Kenntnisverschaffung als auch die zweckfremde Verwendung dieser Kenntnis ist ohne eine entsprechende Ergänzung durch §88 Abs. 3 S. 1 u. 2 TKG untersagt. Die Auswertung der Telekommunikation zum Zwecke der Selektion von inkriminierten Inhalten ist für die geschäftsmäßige Erbringung von Internetzugangsdiensten nicht erforderlich. Zudem stellt die Verwendung der Selektionsergebnisse für die Umleitung auf die geplante Stoppmeldung keinen Zweck dar, der für die geschäftsmäßige Erbringung der Access-Leistungen notwendig ist.

87. Daher bedarf die im Sinne des Telekommunikationsgesetzes zweckfremde Verschaffung und Verwendung einer ergänzenden gesetzlichen Grundlage.

II. Widersprüchlichkeit des Gesetzentwurfs hinsichtlich der Verpflichteten

88. Im Hinblick auf die Verpflichteten gem. § 8a Abs. 2 TMG-E sind insbesondere staatliche Einrichtungen (Behörden, Bibliotheken, Universitäten, Schulen) von den Sperrungsverpflichtungen ausgenommen. Eine solche Ausnahme dürfte mit der Zielsetzung des Gesetzes, Kinderpornographie im Internet durch Zugangserschwerungen zu bekämpfen, nicht vereinbar sein. Daher ist das Gesetz in diesem Punkt widersprüchlich. Die gesetzliche Verpflichtung müsste auch auf staatliche Einrichtungen erstreckt werden, um einen umfassenden Schutz zu gewährleisten.

III. § 3 – Evaluierung

89. Mit dem Gesetzentwurf zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen wird Neuland betreten. Die Wirksamkeit und die Verhältnismäßigkeit solcher Maßnahmen sind vielfach in Frage gestellt worden. Daher sollte die Evaluierung dazu dienen, die notwendigen wissenschaftlichen Grundlagen hinsichtlich der Effektivität und Notwendigkeit der Zugangserschwerung durch Access-Provider zur Verhinderung von kinderpornographischen Angeboten in Kommunikationsnetzen zu sammeln. Keinesfalls dürfte insofern ausreichend sein, die Zahl der Umleitungen auf die Stoppmeldung zu zählen. Aufgrund der Gefahr des Mitsperrens rechtmäßiger Inhalte und des Abrufs der Seite etwa durch Suchmaschinen dürfte die Zahl der Abrufe hinsichtlich der Wirksamkeit des Instruments wenig aussagekräftig sein.

Dr. Dieter Frey
(Rechtsanwalt)

Dr. Matthias Rudolph
(Rechtsanwalt)