

Juniorprofessor Dr. Matthias Bäcker, LL.M.

Mannheim, den 25. Mai 2009

Universität Mannheim
Schloss, Westflügel
68131 Mannheim

Stellungnahme

zu dem Entwurf eines Gesetzes zur Bekämpfung der Kinderpornographie in
Kommunikationsnetzen

(BT-Drs. 16/12850)

Gliederung

I. Kompetenzrechtliche Fragen

1. Keine Gesetzgebungskompetenz des Bundes
2. Zweifelhafte Verwaltungskompetenz des Bundes

II. Materiellrechtliche Fragen

1. Keine generelle Verfassungswidrigkeit von Sperren
2. Mängel des Gesetzentwurfs
 - a) Kein Ausschluss unverhältnismäßiger Sperren
 - aa) Fehlender Vorrang einer Löschung
 - bb) Fehlende Subsidiarität der Sperre von Verweisen
 - cc) Fehlender Ausschluss großflächiger Sperren
 - b) Unzulänglichkeit des behördlichen Verfahrens
 - aa) Fehlende Vorabkontrolle durch eine neutrale Stelle
 - bb) Fehlende Pflicht zur fortlaufenden Kontrolle der Liste
 - c) Ineffektiver Rechtsschutz wegen unzureichender Information der Betroffenen

d) Problematische Nutzung der Kommunikationsdaten zur Strafverfolgung

III. Ergebnisse

Ich behandle im Folgenden kompetenzrechtliche (I) und materielle rechtliche Probleme (II), die der Gesetzentwurf aufwirft. Abschließend fasse ich die wesentlichen Ergebnisse zusammen (III). Weitgehend außer Betracht bleiben die wirtschaftlichen Folgen der vorgesehenen Sperren für die Access Provider und die damit verbundenen rechtlichen Probleme, da ich davon ausgehe, dass die eingeladenen Branchenvertreter ihre Anliegen umfassend darlegen werden.

I. Kompetenzrechtliche Fragen

Ich habe bereits erhebliche Zweifel, ob das geplante Gesetz mit der Kompetenzordnung des Grundgesetzes vereinbar ist. Problematisch sind dabei sowohl die Gesetzgebungs- als auch die Verwaltungskompetenz des Bundes.

1. Keine Gesetzgebungskompetenz des Bundes

Meines Erachtens fehlt es an einer Gesetzgebungskompetenz des Bundes, so dass das Gesetz bereits aus diesem Grund vollständig verfassungswidrig wäre.

a) Entgegen der Gesetzesbegründung¹ ergibt sich eine Gesetzgebungskompetenz nicht aus Art. 74 Abs. 1 Nr. 11 GG, der eine solche Kompetenz für das Recht der Wirtschaft eröffnet.

Das Bundesverfassungsgericht legt diesen Kompetenztitel zwar weit aus. Das Recht der Wirtschaft umfasst danach alle Normen, die das wirtschaftliche Leben und die wirtschaftliche Betätigung regeln. Dies setzt einen „wirtschaftsregulierenden oder wirtschaftslenkenden Gehalt“ des jeweiligen Gesetzes voraus.² So können auch ordnungsrechtliche Normen im Sachzusammenhang mit dem Recht der Wirtschaft stehen und daher auf Art. 74 Abs. 1 Nr. 11 GG gestützt werden.³ Dagegen erstreckt sich die Gesetzgebungskompetenz nicht auf Vorschriften, die allein dazu dienen, die öffentliche Sicherheit und Ordnung zu schützen, auch wenn sie Auswirkungen auf die wirtschaftliche Tätigkeit haben mögen.⁴

Nach diesen Kriterien können die geplanten Regelungen über Internetsperren nicht mehr als Recht der Wirtschaft im Sinne des Art. 74 Abs. 1 Nr. 11 GG eingeordnet werden. Ihr Gegenstand ist weder das wirtschaftliche Verhalten der betroffenen Access Provider noch der Markt für Zugangsdienstleistungen insgesamt, sondern die Bekämpfung der Kinderpornographie und damit ein Anliegen der allgemeinen Gefahrenabwehr.⁵ Die Access Provider werden in die Pflicht genommen, um gegen Gefahren vorzugehen, die sie nicht selbst geschaffen haben und

¹ BT-Drs. 16/12850, S. 9 f.

² BVerfGE 55, 274 (308); 67, 256 (275); 68, 319 (330); 116, 202 (215 f.).

³ Vgl. etwa BVerfGE 41, 344 (355) – Gewerbeamt; BVerfGE 115, 276 (318 f.) – Glücksspielrecht.

⁴ BVerfGE 8, 143 (149 f.); 13, 367 (371 f.); 41, 344 (355).

⁵ Denkbar wäre noch, die geplanten Regelungen als Medienrecht einzustufen. Für die Frage der Gesetzgebungskompetenz ist diese Frage ohne Belang, da der Bund weder für die allgemeine Gefahrenabwehr noch für das Medienrecht zuständig ist.

denen sie auch ansonsten nicht nahe stehen. Darin unterscheidet sich das geplante Gesetz etwa von Regelungen, die eine potentiell gefährliche Wirtschaftstätigkeit regulieren und deshalb unter Art. 74 Abs. 1 Nr. 11 GG fallen. Das geplante Gesetz behandelt die Access Provider gewissermaßen als verlängerten Arm der staatlichen Gewalt, um gegen bestimmte Kommunikationsinhalte im Internet vorzugehen. Eine Norm, die Private in dieser Weise in Dienst nimmt, hat keinen wirtschaftsregulierenden Gehalt. Selbst wenn sie die wirtschaftliche Tätigkeit der betroffenen Privaten berührt, handelt es sich um eine bloße Nebenfolge.

b) Eine Gesetzgebungskompetenz des Bundes ergibt sich weiter nicht aus Art. 73 Abs. 1 Nr. 10 GG. Danach kann der Bund unter anderem die Zusammenarbeit des Bundes und der Länder in der Kriminalpolizei und die internationale Verbrechensbekämpfung regeln. Das geplante Gesetz sieht jedoch keine Zusammenarbeit von Bund und Ländern vor, sondern weist eine bestimmte Maßnahme der Gefahrenabwehr ausschließlich einer Bundesbehörde zu. Die Sperren sind auch keine Maßnahmen der internationalen Verbrechensbekämpfung. Darunter ist nicht die „Bekämpfung internationaler Verbrechen“ zu verstehen, sondern es werden nur grenzüberschreitende Bekämpfungsmaßnahmen erfasst, insbesondere die Vernetzung in- und ausländischer Behörden.⁶ Der Gesetzentwurf soll dem Bundeskriminalamt hingegen eine neue rein national wirkende Aufgabe zuweisen, wenn sich diese auch auf ein weltweites Datennetz bezieht.

c) Das Gesetz lässt sich auch nicht auf Art. 73 Abs. 1 Nr. 7 GG stützen, nach dem der Bund die ausschließliche Gesetzgebung über die Telekommunikation hat. Dieser Kompetenztitel betrifft nur die Technik der Telekommunikationsinfrastruktur und der Informationsübermittlung, nicht aber Regelungen, die auf die übermittelten Inhalte ausgerichtet sind.⁷ Gerade um eine solche Inhaltsregulierung geht es dem geplanten Gesetz jedoch.

d) Schließlich kann das geplante Gesetz auch nicht dem Strafrecht zugeordnet werden, für das eine Gesetzgebungskompetenz des Bundes aus Art. 74 Abs. 1 Nr. 1 GG besteht. Die geregelten Zugangerschwerungen sollen in erster Linie nicht dazu dienen, Straftaten nach § 184b StGB aufzuklären, sondern sie sollen verhindern, dass Personen kinderpornographische Inhalte abrufen und sich damit gegebenenfalls strafbar machen. Dies ist ein Anliegen der Gefahrenabwehr und nicht der Strafverfolgung. Dass durch § 8a Abs. 5 Satz 2 TMG-E die Daten, die bei einer Sperre anfallen, in einem nächsten Schritt umgewidmet werden und für die Strafverfolgung genutzt werden können, ändert daran nichts. Nach der Konzeption des Gesetzes handelt es sich dabei nur um eine Nebenfolge der geregelten Abwehrmaßnahmen. Konsequenterweise regelt das Gesetz die strafprozessuale Nutzung der Daten nicht selbst, sondern öffnet den Datenbestand lediglich für eine solche Nutzung nach anderen (strafprozessualen) Normen.⁸

2. Zweifelhafte Verwaltungskompetenz des Bundes

Selbst wenn eine Gesetzgebungskompetenz des Bundes für das geplante Gesetz unterstellt wird, erscheint problematisch, ob es mit dem Grundgesetz vereinbar ist, dass das Gesetz das Bundeskriminalamt damit betraut, die Sperrliste zu führen. Der Bund kann nach Art. 83 GG Bundesgesetze nur dann durch eigene Behörden vollziehen lassen, wenn das Grundgesetz ihm

⁶ Vgl. BVerfGE 100, 313 (369); *Gärditz*, Strafprozeß und Prävention, S. 275 f.

⁷ BVerfGE 113, 348 (368).

⁸ Dazu unten II. 2. d).

dafür die Verwaltungskompetenz besonders zuweist. Eine solche Verwaltungskompetenz des Bundes kann meiner Ansicht nach jedenfalls nicht mit den Erwägungen begründet werden, die sich dem Gesetzentwurf indirekt entnehmen lassen.

Nach § 8a Abs. 1 TMG-E führt das Bundeskriminalamt die Sperrliste „im Rahmen seiner Aufgaben als Zentralstelle“ nach § 2 BKAG. Verfassungsrechtlich gewendet lässt sich dem entnehmen, dass die Verwaltungskompetenz des Bundes anscheinend aus Art. 87 Abs. 1 Satz 2 GG hergeleitet wird. Nach dieser Norm kann der Bund unter anderem eine Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei einrichten; dies ist nach § 2 BKAG das Bundeskriminalamt. Welche Aufgaben und Befugnisse einer solchen Zentralstelle genau verliehen werden können, ist in der Literatur umstritten und in der Rechtsprechung des Bundesverfassungsgerichts bislang nicht abschließend geklärt. Einigkeit besteht allerdings darin, dass die Tätigkeit der Zentralstelle in erster Linie eine Servicefunktion hat: Es geht darum, das Handeln anderer Behörden informationell zu verklammern und zu koordinieren.⁹ Auch ist weitgehend anerkannt, dass Art. 87 Abs. 1 Satz 2 GG dem Bund nicht ermöglicht, das Bundeskriminalamt – jenseits des hier nicht einschlägigen Sonderfalls der Terrorismusabwehr nach Art. 73 Abs. 1 Nr. 9a GG – mit präventivpolizeilichen Befugnissen zu unmittelbar außenwirksamen Maßnahmen auszustatten: Im Bereich der Gefahrenabwehr ist das Amt darauf beschränkt, die kriminalpolizeiliche Tätigkeit anderer Polizeibehörden zu unterstützen. Über diese Grenze der Verwaltungskompetenz des Bundes setzt sich der Gesetzentwurf hinweg, indem er dem Bundeskriminalamt ermöglicht, darüber zu entscheiden, welche Kommunikationsangebote im Internet es auf die Sperrliste setzt und damit blockieren lässt. Dem Zentralstellenbegriff entspräche es dagegen, wenn das Bundeskriminalamt – ähnlich wie bei der Strafverfolgung im Bereich der Kinderpornographie – lediglich Informationen über kinderpornographische Angebote sammelte und an die Landespolizeibehörden weitergäbe.

Denkbar wäre dagegen, auf der Grundlage von Art. 87 Abs. 3 Satz 1 GG eine selbstständige Bundesoberbehörde einzurichten, die die Sperrliste führt. Solche Bundesoberbehörden können anders als Zentralstellen mit Exekutivkompetenzen ausgestattet werden. Dass in einem bestimmten Sachbereich gemäß Art. 87 Abs. 1 Satz 2 GG eine Zentralstelle geschaffen werden kann, hindert den Rückgriff auf Art. 87 Abs. 3 Satz 1 GG nicht, da zwischen beiden Kompetenztiteln kein Spezialitätsverhältnis besteht.¹⁰ Es wäre meines Erachtens auch möglich, das Bundeskriminalamt mit dieser Aufgabe zu betrauen.¹¹ Allerdings setzt die Einrichtung einer selbstständigen Bundesoberbehörde einen besonderen gesetzlichen Errichtungsakt voraus,¹² an dem es hier fehlt, da das Amt die Sperrliste gerade im Rahmen seiner Zentralstellentätigkeit führen soll.¹³

⁹ In diese Richtung BVerfGE 110, 33 (51); ausführlich zum Zentralstellenbegriff und seinen (unklaren) Grenzen *Bäcker*, Terrorismusabwehr durch das Bundeskriminalamt (erscheint demnächst), Teil 1, I. 1. und 2. a).

¹⁰ BVerfGE 110, 33 (50 ff.).

¹¹ Vgl. *Pieroth*, in: Jarass/Pieroth, GG, Art. 87 Rn. 14.

¹² Vgl. *Lerche*, in: Maunz/Dürig/Herzog, GG, Art. 87 Rn. 172 ff.

¹³ Auch die anderen Aufgabenzuweisungen des BKA-Gesetzes wurden bislang nicht auf Art. 87 Abs. 3 Satz 1 GG gestützt, vgl. § 1 Abs. 1 BKAG.

II. Materiellrechtliche Fragen

Inhaltlich kann eine Sperrpflicht für kinderpornographische Inhalte verfassungsgemäß sein. Der Gesetzentwurf weist jedoch bei der konkreten Ausgestaltung dieser Sperrpflicht Mängel auf, die auch verfassungsrechtliche Bedenken begründen.

1. Keine generelle Verfassungswidrigkeit von Sperren

Eine Sperrliste, mit der Access Provider angewiesen werden, den Zugriff auf kinderpornographische Inhalte im Internet zu erschweren, muss nicht notwendigerweise gegen das Grundgesetz verstoßen. Die Aufnahme eines Kommunikationsangebots in die Liste greift zwar in die Grundrechte von Contentanbietern,¹⁴ Internetnutzern¹⁵ und Access Providern¹⁶ ein.¹⁷ Der Grundrechtseingriff kann jedoch grundsätzlich verfassungsrechtlich gerechtfertigt werden.

Die Sperrliste ist keine Zensurmaßnahme, die nach Art. 5 Abs. 1 Satz 3 GG generell verboten wäre. Nach der Rechtsprechung des Bundesverfassungsgerichts erfasst der Zensurbegriff nur eine Vorzensur,¹⁸ während hier bereits publizierte Inhalte gesperrt werden sollen. Wollte man den Zensurbegriff weiter fassen und darunter allgemein eine staatliche Inhaltsprüfung verstehen, die von hinreichenden Anzeichen konkreter Rechtsgutsgefährdungen unabhängig ist,¹⁹ käme man letztlich zu keinem anderen Ergebnis, solange nicht staatliche Stellen das Internet anlasslos und großflächig auf mögliche verbotene Inhalte durchsuchen.²⁰

Internetsperren zur Bekämpfung der Kinderpornographie können auch dem Verhältnismäßigkeitsgrundsatz genügen.

¹⁴ Betroffen ist zumindest die allgemeine Handlungsfreiheit nach Art. 2 Abs. 1 GG. Je nach den Umständen des Einzelfalls können auch andere Grundrechte einschlägig sein: „Sprechendes“ Bildmaterial, das eine Meinungsäußerung vermittelt, fällt in den Schutzbereich der Meinungsfreiheit, vgl. BVerfGE 30, 336 (352); 102, 347 (359); 107, 275 (280). Fiktive und verfremdete (kinder-)pornographische Inhalte wie Romane oder Animationsfilme können auch durch die Kunstfreiheit geschützt sein, vgl. BVerfGE 83, 130 (138 f.) – „Josefine Mutzenbacher“. Wird der Contentanbieter an einer wirtschaftlichen Tätigkeit gehindert, liegt darin ein Eingriff in seine Berufsfreiheit.

¹⁵ Die Sperre ist insoweit an der Informationsfreiheit des Art. 5 Abs. 1 Satz 1 GG zu messen, wie hier etwa *Sieber/Nolde*, Sperrverfügungen im Internet, S. 77 ff.; *Neumann*, Ordnungsrechtliche Sperrungsverfügungen und die Informationsfreiheit nach Art. 5 Abs. 1 S. 1 2. Alt. GG, URL: <http://www.artikel5.de/artikel/sperrunginffreiheit.html>. Hingegen greift die Sperre als solche entgegen einer verbreiteten Auffassung nicht in das Fernmeldegeheimnis nach Art. 10 GG ein, da dieses Grundrecht als Eingriffsabwehrrecht nur davor schützt, dass staatliche Stellen Inhalte oder Umstände der Telekommunikation zur Kenntnis nehmen oder eine solche Kenntnisnahme vorbereitet wird, vgl. BVerfGE 100, 313 (366). Eine derartige Kenntnisnahme ist jedoch mit der bloßen Sperre nicht verbunden und auch nicht Zweck der Maßnahme. Allerdings fordert Art. 10 GG, den staatlich veranlassten Umgang der Access Provider mit Kommunikationsdaten auf das erforderliche Maß zu begrenzen, näher *Bäcker*, Die Vertraulichkeit der Internetkommunikation, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, S. 99, unter II. 1. b) aa). Diese Begrenzung ist in § 8a Abs. 5 Satz 1 TMGE und § 96 Abs. 1 TKG-E enthalten.

¹⁶ Einschlägig ist insoweit die Berufsfreiheit des Art. 12 GG.

¹⁷ Rechtsdogmatisch handelt es sich für Contentanbieter und Internetnutzer um einen sogenannten mittelbaren Grundrechtseingriff, da eine staatliche Stelle (das Bundeskriminalamt) bestimmte Private (die Access Provider) rechtlich bindend veranlasst, grundrechtliche Freiheit zu beeinträchtigen. Strukturell ähnelt die Maßnahme der Erhebung von Telekommunikationsdaten bei einem Telekommunikationsunternehmen, vgl. dazu BVerfGE 107, 299 (313 f.).

¹⁸ Vgl. BVerfGE 33, 52 (71 ff.); 87, 209 (230).

¹⁹ So *Hoffmann-Riem*, Kommunikationsfreiheiten, S. 141.

²⁰ Eingehend *Sieber/Nolde*, Sperrverfügungen im Internet, S. 99 ff.

Zwar bestehen Zweifel, ob solche Sperren ein wirksames und sinnvolles Mittel sind, um die Herstellung und Verbreitung kinderpornographischen Materials zu bekämpfen: Die derzeit diskutierten Sperrtechniken lassen sich durchweg mit vergleichsweise geringem Aufwand umgehen.²¹ Hinzu kommt, dass die Sperren sich technisch bedingt vor allem gegen Angebote im World Wide Web richten, während sie die Verbreitung kinderpornographischen Materials über andere Kommunikationsdienste des Internet wie Filesharingnetze, geschlossene Chats oder das Usenet nicht verhindern. Gleichwohl lassen sich Sperren angesichts des weiten Einschätzungsspielraums des Gesetzgebers²² noch nicht als schlechthin ungeeignet und deshalb unverhältnismäßig ansehen.

Es ist auch nicht generell unangemessen, den Zugriff auf kinderpornographische Inhalte im Internet zu erschweren. Zwar ermöglicht § 8a Abs. 1 Satz 1 TMG-E nicht lediglich, solche Kommunikationsinhalte zu sperren, denen ein tatsächliches Missbrauchsgeschehen zugrunde liegt. Die strafrechtliche Verbotsnorm in § 184b Abs. 1 StGB erfasst auch fiktive Darstellungen, selbst wenn diese – wie etwa Romane oder Animationsfilme – nicht wirklichkeitsnah sind.²³ Die Einschränkung der Informationsfreiheit²⁴ kann daher nicht in jedem Fall mit der Erwägung gerechtfertigt werden, die Persönlichkeitsrechte von Missbrauchsoffern müssten geschützt werden. Jedoch lässt sich der Strafnorm entnehmen, dass bestimmte Formen einer Sexualisierung von Kindern allgemein tabuisiert werden sollen. Dies begegnet keinen Bedenken und kann auch eine Unterdrückung derartiger Inhalte tragen, die bei dem Empfänger ansetzt.

2. Mängel des Gesetzentwurfs

Jedoch weist der Gesetzentwurf Mängel auf, die teilweise verfassungsrechtliche Bedenken begründen, teilweise den Nutzen der geplanten Sperren weiter verringern dürften.

a) Kein Ausschluss unverhältnismäßiger Sperren

In bestimmten Fallkonstellationen kann eine Sperre unnötig oder unangemessen sein. Eine solche Maßnahme verletzt den Verhältnismäßigkeitsgrundsatz und muss unterlassen werden. Der Gesetzentwurf enthält jedoch keine Vorkehrungen, um solche Sperren zu verhindern. Er deckt damit auch Sperren, die den verfassungsrechtlichen Anforderungen nicht genügen:

aa) Fehlender Vorrang einer Löschung

Der Eingriff in die Grundrechte der Access Provider, der mit einer Sperre verbunden ist, ist nicht erforderlich, um einen Zugriff zu verhindern, wenn das betroffene kinderpornographische Material zuverlässig aus dem Netz entfernt werden kann. Dies ist zumindest in aller Regel dann anzunehmen, wenn sich der Rechner, auf dem das Material gespeichert ist, in der Bundesrepublik oder einem anderen Mitgliedstaat der Europäischen Union befindet. In einem solchen Fall kann eine Sperre allenfalls für einen Übergangszeitraum bis zur Entfernung gerechtfertigt werden. Auch wenn der betroffene Rechner sich außerhalb der Europäischen Uni-

²¹ Dazu im Überblick *Murdoch/Anderson*, in: Deibert u.a., *Access Denied: The Practice and Policy of Global Internet Filtering*, S. 57 (67 f.).

²² Vgl. zu „Online-Durchsuchungen“ BVerfGE 120, 274 (320 f.).

²³ Vgl. *Lenckner/Perron*, in: Schönke/Schröder, StGB, § 184b Rn. 3.

²⁴ Zu den Anforderungen an die Eingriffsrechtfertigung BVerfGE 27, 71 (85 f.); *Hoffmann-Riem*, Kommunikationsfreiheiten, S. 159 f.

on befindet, muss aber zumindest versucht werden, eine Löschung des kinderpornographischen Inhalts zu erreichen.

Sollen kinderpornographische Inhalte aus ermittlungstaktischen Gründen im Netz belassen werden, ist eine Sperre unangemessen, da sie Wertungswidersprüche erzeugt: Das Bundeskriminalamt kann nicht einerseits entscheiden, dass ein Zugriff auf die betroffenen Inhalte um eines Ermittlungserfolgs willen hingenommen werden kann, andererseits aber unbeteiligte Dritte in die Pflicht nehmen, um einen solchen Zugriff zu verhindern. Nach allgemeinen polizeirechtlichen Grundsätzen kann ein Nichtstörer nur dann zur Gefahrenabwehr herangezogen werden, wenn Maßnahmen gegen den Verantwortlichen nicht möglich sind oder keinen Erfolg versprechen,²⁵ nicht aber, wenn eine Inanspruchnahme des Nichtstörers aus taktischen Gründen wünschenswert erscheint.

Um eine unverzügliche Löschung der Kommunikationsinhalte zu gewährleisten, muss das Bundeskriminalamt daher verpflichtet werden, parallel zu der Sperre alles ihm Mögliche zu unternehmen, um die Löschung zu veranlassen. Das Gesetz muss zudem klarstellen, dass Inhalte, die auf Rechnern innerhalb der Europäischen Union gespeichert sind, nur übergangsweise gesperrt werden dürfen.

bb) Fehlende Subsidiarität der Sperre von Verweisen

Soweit der Gesetzentwurf ermöglichen soll, auch Angebote zu sperren, die selbst kein kinderpornographisches Material enthalten, wenn sie auf solche Angebote verweisen, ist es unklar formuliert und geht teilweise über das zur Gefahrenabwehr erforderliche Maß hinaus.

Unklar ist der Entwurf, soweit verlangt wird, dass der Zweck des Angebots darin bestehen muss, auf kinderpornographische Angebote zu verweisen. Diese Formulierung zwingt dazu, zweckgerichtete und nicht zweckgerichtete Verweise voneinander abzugrenzen, was wenig sinnvoll erscheint: Wird in ein Kommunikationsangebot im Internet ein technischer Verweis auf ein anderes Angebot (etwa ein Hyperlink) aufgenommen, so ist dieser Verweis immer insofern zweckgerichtet, als der Anbieter weiß und will, dass der Verweis auf das andere Angebot führt. Zudem stellt sich bei Kommunikationsangeboten, die neben dem Betreiber auch durch Dritte gestaltet werden können (beispielsweise Foren, soziale Netzwerke oder Online-Enzyklopädien), die Frage, wer über die Zweckrichtung von Verweisen bestimmt. Angesichts dessen liegt es nahe, die Norm weit auszulegen, so dass letztlich jeder Verweis auf ein kinderpornographisches Angebot erfasst wird.

Es wäre jedoch unangemessen, wenn jeder solche Verweis ohne weiteres gesperrt werden könnte. Ein Angebot, das auf ein anderes Angebot verweist, muss dann nicht gesperrt werden, wenn bereits dieses andere Angebot gesperrt und dadurch die Gefahr, dass Kinderpornographie verbreitet wird, abgewehrt werden kann. In einem solchen Fall ist die Sperre des Verweises nicht erforderlich und daher unverhältnismäßig. Eine Sperre des Verweises kommt daher nur in Betracht, wenn entweder der Inhalt, auf den verwiesen wird, nicht gesperrt werden kann²⁶ oder eine Sperre dieses Inhalts zur Gefahrenabwehr nicht ausreicht.²⁷

²⁵ Vgl. etwa § 20 Abs. 1 Nr. 2 BPolG.

²⁶ Vorstellbar wäre etwa, eine Indexierungsseite für ein Filesharing-Netzwerk (wie thepiratebay.org) zu sperren, wenn eine Sperre des Datenaustauschs im Netzwerk nicht möglich ist. Eine solche Sperre wird allerdings vielfach wegen drohender Kollateralschäden unverhältnismäßig sein, siehe dazu sogleich im Text.

Statt des kaum handhabbaren Zweckerfordernisses sollte daher geregelt werden, dass verweisende Angebote nur subsidiär gesperrt werden dürfen.

cc) Fehlender Ausschluss großflächiger Sperren

Schließlich können Sperren zu (absehbaren) Nebenfolgen führen, die den Betroffenen nicht zumutbar sind. Das Gesetz enthält keine hinreichenden Schutzvorkehrungen, um solche Nebenfolgen zu vermeiden.

Hinsichtlich der technischen Ausgestaltung der Sperre²⁸ ist § 8a Abs. 2 TMG-E technologie-neutral formuliert. „Mindestens“ wird allerdings eine Sperre auf Domainnamenebene (DNS-Sperre) gefordert. Nach der gesetzlichen Konzeption ist daher damit zu rechnen, dass die meisten Access Provider die Sperrliste auf diese Weise umsetzen.

DNS-Sperren erfassen alle Inhalte, die mit einem bestimmten Domainnamen verbunden sind. Bei Domains, unter denen Dienste mit Beteiligung zahlreicher Personen betrieben werden (beispielsweise de.wikipedia.org, www.facebook.com, www.rapidshare.com oder www.youtube.com), kann es sich dabei um Beiträge von Millionen von Nutzern handeln, von denen allenfalls ein verschwindend geringer Teil kinderpornographisches Material enthält. Eine derartig weitgehende Sperre unverfänglicher Inhalte lässt sich vor den Grundrechten der Betroffenen nicht rechtfertigen. Insbesondere können sie nicht als Nichtstörer in Anspruch genommen werden, da das öffentliche Interesse an der Sperre eines einzelnen kinderpornographischen Angebots schon wegen der geringen Wirksamkeit dieses Instruments ihr kommunikatives Entfaltungsinteresse nicht überwiegt. Wenigstens aber müsste eine Entschädigung gewährt werden,²⁹ die das Gesetz nicht vorsieht.

Ein Listeneintrag, bei dem die Gefahr eines solchen Kollateralschadens besteht, darf daher nicht mittels DNS-Sperre umgesetzt werden. Da diese Gefahr noch steigt bei Sperren, die den Zugriff auf bestimmte IP-Adressen blockieren,³⁰ und die Einrichtung eines Proxy-Servers, mit dessen Hilfe gezielt einzelne URL gesperrt werden könnten, von den Access Providern nicht generell verlangt wird,³¹ dürfte es in manchen Fällen zumindest einzelnen Providern unzumutbar im Sinne des § 8a Abs. 2 Satz 1 TMG-E sein, die Sperrliste vollständig zu implementieren.

Die technologie neutrale Ausrichtung des § 8a Abs. 2 TMG-E kann das Bundeskriminalamt nicht davon entlasten, so weitgehend wie möglich sicherzustellen, dass neue Einträge auf der

²⁷ So kann es etwa bei umfangreichen Linksammlungen liegen, die regelmäßig aktualisiert werden.

²⁸ Kurze Darstellungen der derzeit diskutierten Sperrtechniken bei *Murdoch/Anderson*, in: Deibert u.a., *Access Denied: The Practice and Policy of Global Internet Filtering*, S. 57 (58 ff.); *Sieber/Nolde*, *Sperrverfügungen im Internet*, S. 49 ff.

²⁹ Vgl. zur Entschädigung von Nichtstörern etwa § 51 Abs. 1 BPolG.

³⁰ Problematisch ist daran vor allem, dass in vielen Fällen über eine IP-Adresse zahlreiche Domain-Namen erreichbar sind. So soll die IP-Sperre dreier pornographischer Websites durch einen deutschen Access Provider mehrere Millionen weiterer Webseiten blockiert haben, Quelle: <http://www.spiegel.de/netzwelt/web/0,1518,506143,00.html>. Die IP-Sperre eines niederländischen Host Providers soll neben einer extremistischen Publikation die Web-Auftritte von mehr als 6000 Anbietern betroffen haben, Quelle: *Sieber/Nolde*, *Sperrverfügungen im Internet*, S. 186.

³¹ Im Übrigen können auch proxybasierte Maßnahmen im Einzelfall unerwünschte Auswirkungen haben. So wird von einem Fall aus Großbritannien berichtet, in dem die Sperre eines einzelnen Artikels der englischsprachigen Wikipedia dazu führte, dass britische Nutzer ohne Anmeldung keine Einträge mehr bearbeiten konnten, Quelle: <http://www.heise.de/newsticker/meldung/120048>.

Sperrliste nicht zu derartigen Kollateralschäden führen. Das Amt muss daher gesetzlich verpflichtet werden, für jeden neuen Eintrag zu prüfen, ob bei einzelnen Sperrmethoden solche Schäden drohen. Gegebenenfalls müssen diese Sperrmethoden ausgeschlossen werden, auch wenn dann die gewünschte Sperre nicht mehr flächendeckend durchgeführt werden kann. Zudem muss das Bundeskriminalamt verpflichtet werden, die Adresse des betroffenen Kommunikationsangebots so genau wie möglich anzugeben, um den Access Providern zu ermöglichen, dieses Angebot so präzise wie möglich zu erfassen. § 8a Abs. 2 Satz 2 TMG-E, der so gelesen werden kann, als habe das Bundeskriminalamt ein Wahlrecht, wie es die zu sperrenden Inhalte bezeichnet, ist zumindest missverständlich.

b) Unzulänglichkeit des behördlichen Verfahrens

Der Gesetzentwurf begegnet weiter insoweit Bedenken, als er keine hinreichenden verfahrensrechtlichen Absicherungen zum Schutz der betroffenen Grundrechtsträger vor unverhältnismäßigen Eingriffen enthält.

aa) Fehlende Vorabkontrolle durch eine neutrale Stelle

Das Gesetz enthält keine Vorgaben für das Verfahren, in dem das Bundeskriminalamt die Sperrliste erstellt. Solche Verfahrensanforderungen erscheinen jedoch geboten:

Zunächst führt die Geheimhaltung der Sperrliste – für die es gute Gründe gibt – dazu, dass die Liste in ihrer Gesamtheit nicht von unabhängigen Stellen darauf kontrolliert werden kann, ob die erfassten Kommunikationsangebote die Voraussetzungen einer Sperre erfüllen. Auch eine öffentliche Debatte über den Umfang der Sperrliste und die genauen Kriterien für eine Aufnahme in die Liste ist nicht möglich. Zu einer Kontrolle kann es nur punktuell in Fällen kommen, in denen Betroffene hinsichtlich einzelner gesperrter Kommunikationsangebote gerichtliche Verfahren anstrengen. Wegen des mit jedem Prozess verbundenen Kostenrisikos und der Stigmatisierungswirkung, die von einer Aufnahme in die Liste ausgeht, ist damit zu rechnen, dass es zu solchen Verfahren nur selten kommen wird.

Weiter kann die Entscheidung, ob ein bestimmter Kommunikationsbeitrag als verbotene Kinderpornographie im Sinne des § 184b StGB anzusehen ist, in Grenzfällen erhebliche Schwierigkeiten aufwerfen. Das strafbewehrte Verbot erfasst gerade nicht nur Darstellungen, die tatsächliche Missbrauchsfälle in Bild und Ton dokumentieren, sondern auch fiktive und verfremdete Schilderungen, die als Meinungsäußerung oder Kunstwerk besonderen grundrechtlichen Schutz genießen können.³² Die Frage, ob eine solche Darstellung unter das Verbot fällt, kann sich als komplexe Abwägungsentscheidung darstellen.³³ Es liegt eher fern, eine solche Abwägungsentscheidung ausschließlich einer Polizeibehörde zu überlassen, die nach ihrem Aufgabenkreis nur begrenzt Gewähr für eine neutrale Begutachtung bietet.

Diese Gesichtspunkte legen nahe, die Aufnahme eines Angebots in die Liste vorab von einer neutralen und sachkundigen Stelle, etwa einem Gericht, kontrollieren zu lassen. Ein Kontrollvorbehalt könnte zudem dazu beitragen, die oben angeführten problematischen Fallkonstellationen zu bewältigen. Er ist daher rechtspolitisch dringend zu empfehlen, wenn er auch nicht zwingend verfassungsrechtlich geboten sein mag.

³² Siehe oben Fn. 14.

³³ Vgl. *Hörnle*, in: Münchener Kommentar zum StGB, § 184b Rn. 11.

bb) Fehlende Pflicht zur fortlaufenden Kontrolle der Liste

Nicht nur rechtspolitisch, sondern auch verfassungsrechtlich zu beanstanden ist, dass der Gesetzentwurf die Aktualität der Sperrliste nicht verfahrensrechtlich gewährleistet. Dies kann dazu führen, dass die Liste mit der Zeit mehr und mehr Adressen aufführt, unter denen keine kinderpornographischen Inhalte mehr abgerufen werden können. Die Access Provider gleichwohl mit dem Sperraufwand zu belasten, ist nicht erforderlich und daher unverhältnismäßig. Zudem ist möglich, dass Domainnamen oder IP-Adressen, die auf der Liste enthalten sind, nach Entfernung des Angebots an Anbieter legaler Inhalte vergeben werden. Die weitere Sperre einer solchen Adresse kann gleichfalls nicht gerechtfertigt werden. Adressen, die nicht mehr zur Verbreitung kinderpornographischen Materials genutzt werden, müssen daher von der Liste genommen werden. Dies liegt in der Verantwortung des Bundeskriminalamts. Das Gesetz muss regelmäßige Überprüfungen vorsehen, die dies gewährleisten.

c) Ineffektiver Rechtsschutz wegen unzureichender Information der Betroffenen

Da eine Sperre in Grundrechte der Contentanbieter wie auch der Internetnutzer eingreift, müssen diese Personen nach Art. 19 Abs. 4 GG gegen die Sperre effektiven³⁴ Rechtsschutz erlangen können. Probleme wirft unter diesem Gesichtspunkt § 8a Abs. 8 Satz 2 TMG-E auf. Nach dieser Norm muss das Bundeskriminalamt Diensteanbietern, die ein berechtigtes Interesse darlegen, auf Anfrage Auskunft darüber erteilen, ob und in welchem Zeitraum ein Angebot in der Sperrliste enthalten ist oder war.

Die geregelte Auskunftspflicht ist in zweierlei Hinsicht unzureichend: Zum einen muss dem Contentanbieter, der gegen eine Sperre vorgehen will, auch mitgeteilt werden, weshalb bestimmte Inhalte auf die Sperrliste gesetzt wurden. Anderenfalls reicht sein Informationsstand nicht aus, um beurteilen zu können, ob weitere behördliche³⁵ und gerichtliche Behelfe Erfolg versprechen. Zum anderen müssen auch Internetnutzer, die bestimmte gesperrte Informationsangebote wahrnehmen wollen, einen entsprechenden Auskunftsanspruch haben.

d) Problematische Nutzung der Kommunikationsdaten zur Strafverfolgung

Problematisch ist weiter die in § 8a Abs. 5 Satz 2 TMG-E vorgesehene Möglichkeit, die Kommunikationsdaten, die anlässlich der Sperre erhoben und genutzt werden, für Strafverfahren zu verwenden. Nach meiner Einschätzung läuft die Vorschrift in der derzeit geplanten Fassung weitgehend leer. Eine Erweiterung wäre hingegen verfassungsrechtlich bedenklich.

Die geplanten Regelungen in § 8a Abs. 5 Satz 1 TMG-E und § 96 Abs. 1 TKG-E sehen vor, dass die Access Provider Kommunikationsdaten ihrer Kunden erheben und verwenden dürfen, soweit dies für die Durchführung der Sperre erforderlich ist. Die Vorschriften enthalten hingegen weder eine Pflicht noch auch nur ein Recht der Provider, solche Daten darüber hinaus zu speichern. Daraus ergibt sich, dass diese Daten zu löschen sind,³⁶ sobald ein Zugriffsversuch auf ein gesperrtes Kommunikationsangebot blockiert worden und der betroffene Nutzer

³⁴ BVerfGE 100, 313 (364); 101, 106 (122).

³⁵ Die Aufnahme in die Sperrliste ist als Verwaltungsakt anzusehen, gegen den nach der VwGO Widerspruch und Anfechtungsklage eröffnet sind.

³⁶ Die Löschung nicht mehr benötigter Kommunikationsdaten ist auch ein grundrechtliches Gebot, vgl. BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 27. Oktober 2006 - 1 BvR 1811/99 -, NJW 2007, S. 3055 f.

auf die Stoppmeldung (§ 8a Abs. 4 Satz 1 TMG-E) umgeleitet worden ist. Kommunikationsdaten über Zugriffsversuche sind daher nur sehr kurze Zeit verfügbar.

Der strafprozessuale Zugriff auf diese Kommunikationsdaten richtet sich nach § 100g StPO.³⁷ Diese Norm ermöglicht einen Datenzugriff nur dann, wenn der Verdacht besteht, dass in der Vergangenheit eine bestimmte Straftat begangen wurde, die durch den Zugriff möglicherweise aufgeklärt werden kann. Die einzige Straftat, die mit Hilfe der Daten über einen erfolglosen Zugriffsversuch aufgeklärt werden kann, ist der Bezug von Kinderpornographie (§ 184b Abs. 1 Nr. 3 oder Abs. 4 StGB). Ein Verdacht auf eine solche Straftat mag bestehen, wenn ein Zugriffsversuch bereits stattgefunden hat. In dieser Situation werden allerdings keine Verkehrsdaten mehr verfügbar sein, mit denen der Zugriffsversuch nachgewiesen werden könnte, da diese Daten unmittelbar nach der Weiterleitung zu löschen waren. Hingegen kommt eine vorherige gerichtliche Anordnung, die Zugriffsdaten in Echtzeit an die Strafverfolgungsbehörden weiterzuleiten, nicht in Betracht, da es vor dem Zugriffsversuch an einem Straftatverdacht fehlt. § 100g StPO ermöglicht hingegen nicht, eine Datenerhebung anzuordnen, um Straftaten aufzuklären, die im Zeitpunkt der Anordnung noch gar nicht begangen worden sind.

§ 8a Abs. 5 Satz 2 TMG-E hätte daher nur dann einen sinnvollen Anwendungsbereich, wenn der Gesetzentwurf um eine Pflicht der Access Provider ergänzt würde, Kommunikationsdaten zu speichern. So könnten die Provider verpflichtet werden, die Zugriffe auf die Stoppmeldung in einem Logfile zu speichern. Eine solche Speicherungspflicht würde allerdings einen schwerwiegenden Eingriff in das Fernmeldegeheimnis des Art. 10 GG darstellen. Ich bezweifle, dass dieser Eingriff verfassungsrechtlich gerechtfertigt werden könnte: In aller Regel wird allenfalls der Verdacht einer Straftat nach § 184b Abs. 4 StGB (Verschaffung des Besitzes von kinderpornographischen Schriften) im Raum stehen. Nach der Einschätzung des Gesetzgebers handelt es sich dabei um ein Bagatelldelikt, wie sich insbesondere an der niedrigen Strafdrohung zeigt (Freiheitsstrafe bis zwei Jahre oder Geldstrafe). Schon deshalb ergäben sich Zweifel an der Verhältnismäßigkeit einer Speicherpflicht. Zudem erscheint fragwürdig, ob ein erfolgloser Zugriffsversuch auf ein kinderpornographisches Kommunikationsangebot überhaupt für sich genommen wenigstens in der Regel den Verdacht einer solchen Straftat begründet.³⁸ Zum einen ermöglicht § 8a Abs. 1 Satz 1 TMG-E, auch solche Inhalte auf die Sperrliste zu setzen, die kein tatsächliches oder wirklichkeitsnahes Geschehen wiedergeben und deren Bezug daher nicht nach § 184b Abs. 4 StGB strafbar ist. Zum anderen kann selbst ein Zugriffsversuch auf solche Inhalte Gründe haben, die nicht zu einer Strafbarkeit nach dieser Vorschrift führen. Der Zugriffsversuch kann etwa auf einem Versehen oder auf Handlungen Dritter beruhen.³⁹

Angesichts dieser Bedenken sollte davon abgesehen werden, die Kommunikationsdaten, die bei den Sperren erhoben und genutzt werden, auch für Zwecke der Strafverfolgung verfügbar zu machen.

³⁷ § 8a Abs. 5 Satz 2 TMG-E öffnet die erhobenen Daten lediglich für Zwecke der Strafverfolgung, verleiht den Strafverfolgungsbehörden jedoch keine eigenständige Ermittlungsbefugnis, so implizit auch die Entwurfsbegründung, BT-Drs. 16/12850, S. 14.

³⁸ Vgl. zu den Anforderungen an den Anfangsverdacht einer mittels des Internet begangenen Straftat nach § 184b Abs. 4 StGB etwa LG Aachen, Beschluss vom 8. Juli 2008 - 68 Qs 56/08 - "Operation Himmel".

³⁹ Beispielhaft seien genannt: Links über Kurz-URL-Dienste; Vorausladen verlinkter Webseiten durch das Browserprogramm (Link-Prefetching); Missbrauch eines „gekaperten“ Rechners im Rahmen eines Botnetzes; manipulatives Umleiten von Anfragen (Iframe-Angriffe).

III. Ergebnisse

1. Dem Bund fehlt die Gesetzgebungskompetenz für das geplante Gesetz. Das Gesetz wäre daher insgesamt formell verfassungswidrig.
2. Das Bundeskriminalamt kann in seiner Funktion als Zentralstelle nicht mit der Führung der Sperrliste betraut werden, da dem Bund insoweit die Verwaltungskompetenz fehlt.
3. Inhaltlich verstößt ein Gesetz, nach dem Access Provider den Zugriff auf kinderpornographische Inhalte im Internet erschweren müssen, nicht notwendigerweise gegen das Grundgesetz. Der Gesetzentwurf enthält jedoch Mängel:
 - a) Der Gesetzentwurf gewährleistet nicht hinreichend, dass unverhältnismäßige Sperren unterbleiben:
 - i. Die Sperre von Inhalten, die von einem Mitgliedstaat der Europäischen Union aus angeboten werden, darf nur übergangsweise vorgesehen werden, bis diese Inhalte entfernt worden sind. In jedem Fall muss zugleich mit der Sperre alles Mögliche unternommen werden, um das gesperrte kinderpornographische Angebot aus dem Netz zu entfernen.
 - ii. Kommunikationsbeiträge, die auf kinderpornographische Angebote verweisen, dürfen nur dann gesperrt werden, wenn eine Sperre dieser kinderpornographischen Angebote selbst nicht möglich ist oder zur Gefahrenabwehr nicht ausreicht.
 - iii. Es muss sichergestellt werden, dass eine Sperre keine technisch bedingten Nebenfolgen erzeugt, durch die unbeteiligte Dritte übermäßig beeinträchtigt werden. Insbesondere muss verhindert werden, dass die Sperre sich auf legale Kommunikationsangebote erstreckt.
 - b) Der Gesetzentwurf enthält keine verfahrensrechtlichen Regelungen, um die Grundrechte der Betroffenen vor unverhältnismäßigen Eingriffen zu schützen. Die Aufnahme eines Kommunikationsangebots in die Sperrliste sollte vorab durch eine unabhängige Stelle kontrolliert werden. Es muss sichergestellt werden, dass die Sperrliste regelmäßig überprüft und veraltete Einträge entfernt werden.
 - c) Den betroffenen Contentanbietern und Internetnutzern muss über den Gesetzentwurf hinaus Auskunft über den Grund einer Aufnahme in die Sperrliste erteilt werden, um einen effektiven Rechtsschutz sicherzustellen.
 - d) Es sollte davon abgesehen werden, die Kommunikationsdaten, die zum Zweck der Sperre erhoben und genutzt werden, für Zwecke der Strafverfolgung zu nutzen. Die derzeit vorgesehene Regelung läuft leer.