**DEUTSCHER BUNDESTAG**
16. Wahlperiode
Ausschuss für Wirtschaft
und Technologie

Ausschussdrucksache **16(9)1559(neu)**
3. Juni 2009

**Professor Dr. Dr. h.c. Ulrich Sieber**

Direktor am Max-Planck-Institut für
ausländisches und internationales Strafrecht
u.sieber@mpicc.de

# Sperrverpflichtungen und Protokollierungsmaßnahmen gegen Kinderpornographie im Internet

– Stellungnahme zum Entwurf eines Gesetzes zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen, BT-Drucks. 16/12850 v. 5.5.2009 –

– und

– Vorschläge für den Schutz gegen Kinderpornografie im Internet
– Mit einem subsidiären und sanktionsorientierten Sperrungskonzept

Erstellt für die Anhörung im
Ausschuss für Wirtschaft und Technologie
des Deutschen Bundestages
am 27.05.2009 in Berlin

- Ergänzte Fassung vom 02.06.2009 -

MAX-PLANCK-GESELLSCHAFT

# Inhalt

**I. Einführung** ..... 3

A. Problemstellung ..... 3

B. Lösungsansatz des Gesetzentwurfs ..... 5

C. Zentrale Fragen ..... 5

**II. Analyse der vorgeschlagenen Lösungsansätze** ..... 6

A. Sperrverpflichtung ..... 6

1. Prüfungsmaßstab und Prüfungsgegenstand ..... 6
2. Vorteile für den Kinderschutz ..... 7
3. Einschränkungen der Wirksamkeit des Kinderschutzes ..... 7
4. Mögliche Nachteile für den Kinderschutz ..... 8
5. Beeinträchtigung von Grundrechten und anderen Werten ..... 10
6. Abwägungen im Hinblick auf die Art der Sperrmaßnahmen ..... 11
7. Probleme bei der Beurteilung der illegalen Angebote und bei deren Aktualisierung ..... 12
8. Verfahrensrechtliche Garantien ..... 13

B. Weiterleitung von personenbezogenen Nutzerdaten an das BKA ..... 14

C. Evaluierungsverpflichtung ..... 16

**III. Zusammenfassende Bewertung und Konsequenzen** ..... 16

A, Bewertung des gegenwärtigen Entwurfs ..... 16

B. Ziele und Strategie eines Neuansatzes ..... 17

# L Einführung

## A. Problemstellung

Kinderpornografische Darstellungen werden in Kommunikationsnetzen über zahlreiche Dienste angeboten und abgerufen. Im Mittelpunkt der öffentlichen - und insbesondere der politischen - Diskussion steht der WWW-Dienst des Internets. Eine erhebliche und wohl noch sehr viel größere Bedeutung haben allerdings der Austausch von Daten über Peer-to-Peer-Protokolle, Newsgroups, Chaträume sowie - z.B. im Anschluss an eine Kontaktanbahnung im Internet - der persönliche und unmittelbare Austausch über E-Mail oder Offline-Medien wie CD-ROM und DVD.[1]

Die im Internet angebotenen Bilder zeigen die Vergewaltigung und den sonstigen Missbrauch von - teilweise nur wenige Jahre alten - Kindern. Sie verletzen die Menschenwürde der Abgebildeten und verursachen mit ihrer Stigmatisierung und Traumatisierung eine erneute Viktimisierung der Opfer. Das - teils im Tausch erfolgende, teils bezahlte und teils unentgeltliche - Angebot von kinderpornografischen Darstellungen stimuliert deren Nachfrage und damit auch den weiteren Missbrauch von Kindern. Darüber hinaus wird angenommen, dass die Bilder einzelne Konsumenten zu einem Missbrauch von Kindern veranlassen und die Bilder bisweilen auch genutzt werden, um entsprechende Verhaltensweisen bei Kindern als „normal" darzustellen und dadurch Hemmschwellen zu senken.[2]

Ein wirksamer *Schutz der Kinder gegen ihren Missbrauch als Darsteller* wird vor allem dann erreicht, wenn die Täter ermittelt und dadurch zukünftige Missbrauchsfälle verhindert werden. Dies kann z.B. über die Identifikation der Anbieter und ihrer Lieferanten erfolgen. Auf nationaler und internationaler Ebene wird auch am Aufbau von Bilddateien und weiteren Maßnahmen gearbeitet, die über eine Identifizierung der Opfer zu den Produzenten der Bilder führen.[3]

Ein effektiver *Schutz gegen die von kinderpornografischen Angeboten* verursachten schädlichen Wirkungen gelingt vor allem, wenn die entsprechenden Darstellungen auf den jeweiligen Host-Servern gelöscht werden. Dies wird insbesondere durch ein System von „Hotlines" gefördert, die Meldungen über rechtswidrige Inhalte entgegennehmen und - teilweise über die national zuständigen Meldestellen - an die betreffenden in- oder ausländischen Hostprovider weiterleiten. Die Hostprovider reagieren hierauf häufig mit einer kurzfristigen Löschung, da Kinderpornografie in vielen Ländern der Welt moralisch und auch strafrechtlich geächtet wird und die

---

[1] Zu den relevanten technischen Grundlagen und Begriffen *Sieber,* in: Hoeren/Sieber (Hrsg.), Handbuch des Multimediarechts, Loseblattsammlung, München, 21. Erg. Lfg. Dezember 2008, Teil 1, S. 1 ff.

[2] Zu den Folgen des Konsums von kinderpornografischen Darstellungen *König,* Kinderpornographie im Internet, Würzburg 2004, S. 60 ff.

[3] Zur Optimierung der Strafverfolgung gegen Kinderpornografie *Sieber,* in: Waltermann/Machill (Hrsg.), Protecting Our Children on the Internet, Gütersloh 2000, S. 319 (345-378).

Provider sich sonst strafbar machen würden.[4] Wenn ausländische Provider trotz Hinweisen untätig bleiben und die notice-and-take-down-Prozeduren der Hotlines nicht funktionieren, so bleibt nur die internationale Rechtshilfe, die im vorliegenden Bereich jedoch langsam und häufig erfolglos ist.

Diese Probleme der extraterritorialen Rechtsdurchsetzung haben in vielen Staaten zu dem Ansatz geführt, den Abruf von Kinderpornografie wenigstens auf dem eigenen Staatsgebiet zu verhindern oder zu erschweren. Viele Rechtsordnungen haben deswegen den - im Inland erfolgenden - Abruf von kinderpornografisehen Angeboten kriminalisiert. Nicht wenige Staaten versuchen oder diskutieren daneben auch eine *technische „Sperrung" der Angebote* gegen den Abruf auf ihrem Territorium. Im Mittelpunkt des Interesses stehen dabei Zwangssperrungen bei den Diensteanbietern, die den Nutzern den Zugang zum Internet ermöglichen (Accessprovider).

Solche Zwangssperrungen sind auf unterschiedlichen technischen Wegen realisierbar. Aufgrund der Natur des Internets sind jedoch alle Maßnahmen mehr oder weniger leicht umgehbar. Sie verursachen auch häufig schädliche Nebenwirkungen und „Kollateralschäden", z.B. wenn sie legale Angebote oder Unterseiten miterfassen. Ein besonderes Dilemma besteht darin, dass einfach durchzuführende Sperrmaßnahmen oft wenig wirksam sind,[5] während effektivere Sperrtechniken häufig mit einem massiven Overblocking verbunden sind,[6] von den Providern einen hohen Aufwand verlangen[7] oder eine komplexe Überwachungsarchitektur erfordern.[8] Sperrmaßnahmen im Internet sind darüber hinaus vor allem wegen der von ihnen verursachten Eingriffe in Grundrechte problematisch. Einschlägig sind dabei insbesondere die Berufsfreiheit und der Eigentumsschutz der Zugangsprovider, die Meinungsfreiheit der Anbieter von Inhalten und die Informationsfreiheit der Nutzer sowie -je nach eingesetzter Sperrtechnik - das Fernmeldegeheimnis.[9]

Die geringe Wirksamkeit der Internetsperren (bei denen die strafbaren Internetangebote weiterhin in vielen Staaten verfügbar bleiben) sowie ihre Nebenfolgen und Kollateralschäden haben deswegen eine in der Öffentlichkeit schwer verständliche Konsequenz: Obwohl es um Maßnahmen im Umfeld schwerster Kriminalität geht, kann die - auch verfassungsrechtlich erforderliche - Abwägung ihrer Vor- und Nachteile überaus problematisch sein. Wenn die Komplexität der technischen Gegebenheiten im Internet, die Folgewirkungen von Sperrmaßnahmen sowie die Möglichkeiten und Folgen von einschlägigen Umgehungsmaßnahmen nicht verstanden werden, so kann dies zu unglücklichen Konsequenzen führen. Der Kritik an Sperrkonzepten wird dann nicht selten der Vorwurf gemacht, Kinder nicht wirksam gegen Missbrauch zu schützen oder ein gesetzloses Internet zu verteidigen, obwohl die Kritik an wenig sinnvollen Sperrmaßnahmen eine Voraussetzung für die Entwicklung von wirksamen Präventionsansätzen ist.

---

[4] Zu den Chancen von notice-and-take-down-Prozeduren gegen die Hostprovider mit dem Ziel der Löschung von illegalen Daten *Sieber,* Verantwortlichkeit im Internet, München 1999, S. 100 f.; 241, 263 ff., *ders.*, in: Waltermann/Machill (Hrsg.) (Anm. 3), S. 389 ff.

^ Z.B. die Manipulation der einschlägigen Domainnamen im DNS.

6 Z.B. bei der Sperrung von kompletten IP-Adressen.

^ Z.B. bei der URL-Sperrung durch Accessprovider, die auf der Internetschicht arbeiten.

8 Z.B. bei hybriden Sperrtechniken mit einem nationalen Proxyserver.

[9] Zu Sperrtechniken, Umgehungsmaßnahmen und relevanten Grundrechtseingriffen umfassend *Sieber/ Nolde,* Sperrverfügungen im Internet, Berlin 2008, S. 49 ff., 58 ff, 176 ff.

## B. **Lösungsansatz des Gesetzentwurfs**

Der aktuelle *„ Entwurf eines Gesetzes zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen"* v. *5.5.2009*^ zielt auf die Sperrung von Telemedienangeboten im WWW. Nach dem Entwurf des neuen § 8a Abs. 1 Telemediengesetz (im Folgenden: TMG-E) führt das Bundeskriminalamt eine Liste über „vollqualifizierte Domainnamen, Internetprotokoll-Adressen und Zieladressen von Telemedien, die Kinderpornografie nach § 184b des Strafgesetzbuchs enthalten oder deren Zweck darin besteht, auf derartige Telemedienangebote zu verweisen". Das Bundeskriminalamt stellt den größeren Accessprovidern arbeitstäglich eine aktuelle Sperrliste zur Verfügung, deren Inhalte die Provider geheim halten müssen. Diensteanbieter nach § 8 Telemediengesetz, die den Zugang zur Nutzung von Informationen über ein Kommunikationsnetz für mindestens 10.000 Teilnehmer in der Regel gegen Entgelt ermöglichen, haben dann nach § 8a Abs. 2 TMG-E unverzüglich und spätestens innerhalb von sechs Stunden „geeignete und zumutbare technische Maßnahmen zu ergreifen, um den Zugang zu Telemedien, die in der Sperrliste aufgeführt sind, zu erschweren". Für die Zugangserschwerung „dürfen vollqualifizierte Domainnamen, Internetprotokoll-Adressen und Zieladressen von Telemedienangeboten verwendet werden. Die Sperrung erfolgt mindestens auf der Ebene der vollqualifizierten Domainnamen, deren Auflösung in die zugehörigen Internetprotokoll-Adressen unterbleibt".

Die Diensteanbieter leiten die einschlägigen Nutzeranfragen nach § 8 Abs. 4 TMG-E auf ein von ihnen betriebenes und vom Bundeskriminalamt vorgegebenes Telemedienangebot mit einer „Stoppmeldung", welche die Nutzer über die Gründe der Sperrung sowie eine Kontaktmöglichkeit zum Bundeskriminalamt informiert. Die Diensteanbieter dürfen dabei nach Absatz 5, soweit dies für die Sperrmaßnahmen und die Anzeige der Stoppseite nach den Absätzen 2 und 4 erforderlich ist, personenbezogene Daten erheben und verwenden. § 8a Abs. 5 TMG-E bestimmt dazu weiter: „Diese Daten dürfen für Zwecke der Verfolgung von Straftaten nach § 184b des Strafgesetzbuches den zuständigen Stellen auf deren Anordnung übermittelt werden."

Der Entwurf enthält darüber hinaus anonymisierte Berichtspflichten der Provider gegenüber dem Bundeskriminalamt (§ 8 Abs. 6 TMG-E), Dokumentationspflichten des Bundeskriminalamts (Art. 8a Abs. 8 TMG-E), eine Haftungsfreistellung der Provider (§ 8a Abs. 7 TMG-E) sowie eine allgemein formulierte Berichts- und Evaluierungspflicht der Bundesregierung über die Anwendung des Gesetzes (Art. 3 TMG-E). Der Gesetzentwurf erfüllt auch das Zitiergebot für Eingriffe in das Fernmeldegeheimnis (Art. 8a TMG-E).

## C. **Zentrale Fragen**

Die vorgeschlagene Neuregelung enthält damit zwei unterschiedliche Maßnahmen zur Bekämpfung der Kinderpornografie: Im Mittelpunkt steht die Verpflichtung zur Sperrung der vom Bundeskriminalamt bestimmten Angebote. Hinzu kommt die Ermächtigung der Provider, den zuständigen Stellen auf deren Anordnung die für Sperrmaßnahmen erhobenen personenbezogenen Daten für die Verfolgung von Straftaten nach § 184b StGB zu übermitteln. Die vorliegende Stellungnahme prüft deswegen in ihrem folgenden zweiten Teil diese beiden Maßnahmen unter verfassungsrechtlichen sowie sonstigen rechtspolitischen Gesichtspunkten und geht anschließend noch kurz auf die Evaluierungsverpflichtung der Bundesregierung ein. Der abschließende dritte Teil der Stellungnahme gibt eine zusammenfassende Bewertung des Gesetzentwurfs und

---

[10] BT-Drucks. 16/12850 v. 5.5.2009.

macht Vorschläge für seine Optimierung im Rahmen eines integrierten Systems zur Eindämmung der Kinderpornographie mit einem subsidiären und sanktionsorientierten Sperrungskonzept. [1]

# II. Analyse der vorgeschlagenen Lösungsansätze

## A. Sperrverpflichtung

### 7. *Prüfungsmaßstab und Prüfungsgegenstand*

Die verfassungsrechtliche Zulässigkeit von Sperrverfügungen im Internet wurde ausführlich in einem Rechtsgutachten geprüft, das der Verfasser und seine Mitarbeiterin *Malaika Nolde* für die Kommission für Jugendmedienschutz (KJM) erstellt haben.[12] Als entscheidender verfassungsrechtlicher und damit auch rechtspolitischer Prüfungsmaßstab für Sperrmaßnahmen im Internet erwies sich dabei die Frage nach der Verhältnismäßigkeit und insbesondere der Angemessenheit von Sperrmaßnahmen. Dabei ist insbesondere der von den Sperrverfügungen erreichte Schutz gegen kinderpornografische Darstellungen mit den damit verbundenen Eingriffen in andere Rechtsgüter abzuwägen.

Eine solche Abwägung ist nur im konkreten Einzelfall möglich und hängt insbesondere von dem jeweiligen Angebot sowie der gewählten Sperrtechnik ab. Während das vorgenannte Gutachten für die KJM die Verhältnismäßigkeitsprüfung für die verschiedenen Sperrmaßnahmen in technischer und rechtlicher Hinsicht umfassend darstellt, behandelt die vorliegende Stellungnahme nur die im Mittelpunkt des Gesetzentwurfs stehenden Manipulationen der Domainnameserver. Diese Beschränkung ist vor allem dann begründet, wenn man den insoweit unklaren Gesetzentwurf (besonders vor dem Hintergrund der ihm vorausgegangenen Verhandlungen der Bundesregierung mit Industrieverbänden) so versteht, dass die Provider ihre Verpflichtung zur Zugangserschwerung mit der „mindestens" erforderlichen Domainname-Sperrung erfüllen, jedoch nicht zu hierüber hinausgehenden Sperrmaßnahmen verpflichtet werden können.[13]

Aufgrund des Wortlauts und der Systematik des Gesetzentwurfs kann § 8 TMG-E allerdings auch so interpretiert werden, dass er die Accessprovider zusätzlich zu hierüber hinausgehenden effektiveren Sperrtechniken (wie IP-Sperrungen oder hybriden Sperrmaßnahmen) verpflichtet. Bei einer solchen Auslegung stellen sich weitere Probleme, da die anderen in Betracht kommenden - meist effektiveren - Sperrtechniken nicht nur zu größeren Kollateralschäden führen können, sondern auch zu der Frage, ob die daraus resultierenden schwierigen Abwägungen weitergehender Sperrmaßnahmen vom Bundeskriminalamt oder von den Providern vorgenommen und verantwortet werden müssen. An der Notwendigkeit einer Prüfung der auch dann noch im

---

[1] * Die weiteren - nicht unproblematischen - Fragen der Bundes- oder Landeskompetenz für die gefahrenabwehrrechtlichen Sperrmaßnahmen können im Hinblick auf die notwendige Begrenzung dieses Beitrags nicht erörtert werden.

12 Siehe hierzu den Nachweis oben in Anm. 9.

[13] Die verschiedenen Sperrtechniken (z.B. IP-, DNS-, URL- oder hybride Sperren) stehen nicht grundsätzlich in einem Stufenverhältnis zueinander. Jede Umsetzung einer Sperranweisung hat individuelle Vor- und Nachteile für den Umsetzenden und die davon betroffenen Inhaltsanbieter. Die gesetzliche Formulierung, dass „mindestens" eine DNS-Sperrung erfolgen müsse, ist daher unklar, aber wohl im Hinblick auf die Effizienz der Sperrung zu verstehen. Vgl. dazu auch unten II.A.6.

Mittelpunkt des Entwurfs stehenden DNS-Sperrungen würde dies jedoch nichts ändern. Die folgenden Ausführungen konzentrieren sich deswegen - soweit dies möglich ist - auf eine Prüfung dieser DNS-Sperrungen.

Die nachfolgenden Ausführungen analysieren dazu im Hinblick auf die verfassungsrechtliche Verhältnismäßigkeitsprüfung zunächst die Vor- und Nachteile der Sperrmaßnahmen: insbesondere ihre Auswirkungen auf den Kinderschutz sowie ihre Eingriffe in Grundrechte und andere Werte (unten 2 - 5). Diese Analyse zeigt, dass die Bestimmung von zulässigen Sperrmaßnahmen im konkreten Einzelfall zu schwierigen Abwägungen und erheblichen Abgrenzungsschwierigkeiten sowohl bei der Festlegung der Art der Sperrmaßnahmen als auch bei der Erstellung und Aktualisierung der Sperrlisten führen kann (unten 6 - 7). Eine Bewältigung dieser Probleme erfordert daher sowohl verbesserte Verfahrensgarantien als auch die Verankerung des Subsidiaritätsprinzips im Hinblick auf das Verhältnis von Sperr- und Löschungsmaßnahmen (unten 8).

### *2. Vorteile für den Kinder schütz*

Für alle vorgesehenen Sperrmaßnahmen spricht zunächst der hohe Rang des geschützten Rechtsguts. Dabei kann allerdings nicht - wie gelegentlich in der Presse - auf die unmittelbare Verhinderung von Kindesmissbrauch abgestellt werden, der durch die Verhinderung oder Unterdrückung der Darstellungen weder rückgängig gemacht noch zukünftig unmittelbar unterbunden werden kann. Die von den Sperrmaßnahmen erstrebte Zugriffsverhinderung schützt - soweit sie wirksam ist - jedoch mit der Menschenwürde der missbrauchten Kinder ebenfalls ein wichtiges Gut, da die öffentliche Zurschaustellung der Bilder für die Opfer durch Stigmatisierung und Traumatisierung zu einer Zweitviktimisierung führt. Hinzu kommen die Einschränkung der bereits genannten Nachfragestimulierung und der Verleitung zum Kindesmissbrauch mit Hilfe der Darstellungen. Auch kann sich die Stoppschild-Funktion des Gesetzentwurfs positiv auswirken, indem sie auf zahlreiche Betroffene eine kontextnahe Abschreckungswirkung haben und bewusstseinsbildend wirken wird. Schließlich kann für die vorgeschriebenen Maßnahmen der Zugangserschwerung angeführt werden, dass sie zu einem Schutz gegen die ungewollte Konfrontation mit Kinderpornografie führt; in der praktischen Erfahrung wird diese zufällige Konfrontationsgefahr im Internet allerdings als wenig realistisch eingeschätzt.

### *3. Einschränkungen der Wirksamkeit des Kinderschutzes*

Die vorgeschlagene Regelung erreicht den angestrebten Schutz der Menschenwürde der Kinder allerdings nur in einem sehr begrenzten Umfang. Dies beruht zunächst darauf, dass der Gesetzentwurf nur kinderpornografische Darstellungen im WWW erfasst. Der Zugang zu kinderpornografischen Bildern über E-Mail, Newsgroups, Peer-to-Peer-Tauschbörsen, Chaträume und andere der oben aufgezeigten Wege wird durch das Gesetz nicht tangiert. Nach Einführung der Sperren dürfte sich der von den Zugangserschwerungen erfasste Teilbereich kinderpornografischer Angebote im WWW noch weiter vermindern, weil die Täter verstärkt auf andere Dienste und Bereiche des Internets ausweichen werden. Auch wegen dieser bereits seit Jahren erfolgenden Verlagerungen erscheint es fraglich, ob sich die WWW-Sperren auf Angebot und Nachfrage kinderpornografischer Darstellungen spürbar auswirken werden.

Hinzu kommt, dass die angeordneten Mindestmaßnahmen für Zugangserschwerungen leicht *umgehbar* sind. Durch die im Entwurf als Mindestanforderung genannte Manipulation der DNS-Server wird die sprachlich umschriebene Domain eines erfragten Angebots nicht mehr in

die korrekte numerische IP-Adresse aufgelöst, sondern in die Adresse der Stoppseite. Der Nutzer kann eine solche Sperrung durch das Eintragen eines nicht kontrollierten DNS-Servers in seinen Computer umgehen, was ihm im Internet durch ein knapp halbminütiges Video erklärt wird.[14] Spätestens die erste Umleitung ihrer Anfrage auf die Stoppseite dürfte daher zahlreiche Nutzer zum Wechsel des bisher genutzten DNS-Servers veranlassen und somit kontraproduktiv wirken, wenn die Nutzer die Zugangserschwerung - ähnlich wie einen nutzerbasierten Filter - generell und auf Dauer abschalten werden. Aufgrund dieser „Opt out"-Lösung wirkt die DNS-Sperre nicht viel stärker als ein nutzerbasiertes Filterkonzept. In diesem Zusammenhang ist auch die vielfach geäußerte Hoffnung unberechtigt, dass ein solches „Umgehungsverhalten" bei einem späteren Zugriff des Nutzers auf eine kinderpomografische WWW-Seite den Tätervorsatz belegen kann. Denn jeder Internetnutzer hat die Freiheit, seinen Domainnameserver selbst auszusuchen und z.B. den DNS-Server eines nicht-sperrpflichtigen kleinen Accessproviders in Deutschland oder eines ausländischen Providers auszuwählen. Wenn mehrere „Stopplistentreffer" der gleichen Absenderadresse bei den Ermittlungsbehörden zu einer Verdachtsabklärung wegen des Verschaffens von Kinderpornografie führen, dann wäre es sogar verständlich, wenn nicht nur Konsumenten von erlaubter Erwachsenenpornografie, sondern auch viele andere Netznutzer die kontrollierten Domainnameserver vermeiden, um beim versehentlichen Anklicken der falschen Links erst gar nicht in den Fokus von Ermittlungsmaßnahmen geraten zu können. Auf andere Sperrtechniken könnte in ähnlicher Weise reagiert werden, z.B. wenn URL- und IP-Sperrungen mit Hilfe eines verschlüsselten „Tunnels" und eines ausländischen Providers umgangen werden.

Letztlich ist die Wirkung aller Sperrtechniken aber vor allem deswegen schwach, weil sie nicht auf die Entfernung der illegalen Angebote „an der Quelle" ausgerichtet sind, sondern lediglich als eine Art „Sichtschutz" für das eigene Territorium fungieren.[15] Diese Beschränkung des Schutzes ist vor allem für die auf den Bildern dargestellten Opfer ein Problem: Die Sperrverfügung schützt ihre Menschenwürde nur gegen einen Bildabruf über die großen deutschen Domainnameserver; dem Abruf ihrer Fotos durch Nutzer aus dem Ausland oder über ausländische Server sind sie weiter schutzlos preisgegeben. Dieser Aspekt stellt nicht nur eine wesentliche Relativierung und Minderung des Sperrschutzkonzepts dar, sondern kann bei einer Betrachtung des Gesamtschutzsystems sogar zu einer Verschlechterung der Opferposition und damit zu einem echten Nachteil führen.

### *4. Mögliche Nachteile für den Kinderschutz*

Nachteile für den Schutz der abgebildeten Opfer können sich bei Sperrverfügungen dadurch ergeben, dass der von den Behörden leichter umsetzbare Sperransatz gegen die Accessprovider das bisher im Vordergrund stehende Löschungskonzept gegen die Hostprovider ersetzen oder schwächen könnte. Das vorrangige Bemühen um eine - weltweit wirksame - Datenlöschung statt einer nur national und damit begrenzt wirksamen Datensperrung oder Zugangserschwerung

---

[14] Zu den DNS-Sperrungen und ihrer Umgehung *Sieber/Nolde* (Anm. 9), S. 50, 182 ff. Leicht verständliche Anleitungen zur Umstellung des DNS-Servers finden sich z.B. auf den Webseiten des CCC (http://www.ccc.de/censorship/dns-howto/) oder bei OpenDNS (https://www.opendns.com/start/). Zu dem im Text genannten Video siehe http://www.youtube.com/watch?v=lNNG5I6DBmO. Vgl. dazu auch die Einschätzung des LG Hamburg, K&R 2009, 272 ff.

[15] Unter anderem deswegen wehren sich auch die Missbrauchsopfer im Internet ausdrücklich gegen Internetsperren, vgl. http://mogis.wordpress.com/2009/04/05/hallo-welt/ (abgerufen am 02.06.2009).

ist dabei nicht nur dem bereits genannten Schutz der Menschenwürde des Opfers geschuldet. Die vorrangige Inanspruchnahme des Störers vor dem Nichtstörer stellt auch einen allgemeinen polizeirechtlichen Grundsatz dar. Dieser ist verfassungsrechtlich verankert, da ein eingriffsintensives Vorgehen gegen die Accessprovider dann nicht mehr „erforderlich" ist, wenn ein Vorgehen gegen die Hostprovider effektiver und weniger eingriffsintensiv ist. Für das Vorgehen der Jugendschutzbehörden bestimmt § 59 Abs. 4 Rundfunkstaatsvertrag daher auch, dass Sperrverfügungen gegen Diensteanbieter fremder Inhalte (d.h. Accessprovider) nur dann möglich sind, wenn Maßnahmen gegenüber dem Verantwortlichen (d.h. insbesondere dem Hostprovider) „nicht durchführbar oder nicht Erfolg versprechend" sind.

Aktuelle Berichte über einschlägige Experimente im Internet bestätigen die Bedenken, dass die Verfolgung eines Sperransatzes die Bemühungen um eine Löschung der kinderpornografischen Angebote schwächen kann: Ein Nutzer schrieb im Mai 2009 insgesamt 348 Provider an, deren Angebote auf den bekanntgewordenen europäischen Sperrlisten standen, und informierte sie per E-Mail über die bei ihnen festgestellte Kinderpornografie. Innerhalb der ersten zwölf Stunden nach dem Versand der Mail löschten zehn Provider freiwillig 60 Webauftritte, darunter auch von drei Servern in Deutschland. 250 Provider antworteten auf das Anschreiben, dass sie hauptsächlich legale Inhalte gefunden hätten.[16] Die Erfolgschancen eines Löschungsansatzes werden auch durch die im Internet veröffentlichte finnische Liste deutlich, bei der die meisten gesperrten Angebote aus den USA stammten, d.h. aus einem Land, in dem aufgrund ähnlicher Wertvorstellungen Möglichkeiten einer Datenlöschung gegeben sein sollten.[17] Die Subsidiarität des Sperransatzes gegenüber dem Löschungsansatz ist daher in hohem Maße plausibel und sollte - sowohl aus verfassungsrechtlichen Gründen als auch im Hinblick auf einen effektiven Opferschutz - im Gesetz verankert werden. Da Kinderpornografie in fast allen Staaten geächtet und bestraft wird, dürfte ein entsprechender notice-and-take-down-Ansatz in diesem Deliktsbereich auch wesentlich erfolgreicher sein als bei der einfachen (d.h. in geschlossenen Benutzergruppen für Erwachsene zulässigen) Pornografle, für deren Strafbarkeit ein internationaler Konsens sehr viel schwieriger zu erreichen ist.

Eine Schwächung des Löschungsansatzes durch den Sperransatz kann und muss daher in dem Gesetzentwurf ähnlich wie in § 59 Abs. 4 RStV ausgeschlossen werden. Dies braucht - wie ich zusammen mit *Nolde* bereits zur Auslegung von § 59 Abs. 4 RStV ausgeführt habe[18] - nicht zwingend zu sinnlosen Löschungsversuchen bei bestimmten Providern oder in bestimmten Ländern zu führen, wenn die Erfolglosigkeit von Maßnahmen bereits von vornherein feststeht. Ob darüber hinaus alle europäischen Angebote (auch im Hinblick auf das Konsultationsverfahren der e-commerce-Richtlinie) aus der Listung herausgenommen werden sollten, hängt unter anderem von den bisherigen praktischen Erfahrungen mit der Frage ab, inwieweit und warum notice-and-take-down-Prozeduren für kinderpornografische Angebote im europäischen Ausland nicht funktionieren. Es spricht aber viel dafür, dass mit einer richtig formulierten Subsidiaritätsregelung die Problematik besser als mit territorialen Ausschlüssen gelöst wäre, weil dann gegen die Provider in unkooperativen Staaten noch flexibel reagiert werden könnte.

---

[16] Siehe http://ak-zensur.de/2009/05/loeschen-funktioniert.html. Zu möglichen Erklärungen unten im Text bei Anm. 25.

[17] Vgl. http://scusiblog.org/7p-463 (abgerufen am 2.6.2009).

[x]% *SieberfNolde* (Anm. 9), S. 154.

Im Übrigen zeigen die Erfahrungen mit dem Bekanntwerden der Sperrlisten in anderen Staaten, dass eine Geheimhaltung dieser Listen dauerhaft kaum möglich ist.[19] Auch in der Zukunft dürften Sperrlisten nicht geheim gehalten werden können.

### 5. *Beeinträchtigung von Grundrechten und anderen Werten*

Sperrmaßnahmen im Internet sind darüber hinaus vor allem wegen ihrer *Eingriffe in Grundrechte* problematisch. Einschlägig sind hier insbesondere die Berufsfreiheit und der Eigentumsschutz der Zugangsprovider (Art. 12 und 14 GG) sowie die Meinungsfreiheit der Anbieter von Inhalten und die Informationsfreiheit der Nutzer (Art. 5 Abs. 1 GG). Die Beeinträchtigung dieser Grundrechte hängt dabei im Einzelfall stark von der technischen Zugangsvermittlung der betroffenen Provider sowie der jeweiligen Sperrtechnik ab.[20]

Die *Berufsfreiheit und der Eigentumsschutz der Zugangsprovider* werden vor allem dann tangiert, wenn Accessprovider Sperrmaßnahmen auf der Anwendungsschicht vornehmen sollen, obwohl sie diese für die Erbringung ihrer (in erster Linie Transport-)Dienstleistung ansonsten nicht nutzen. Für die Accessprovider problematisch sind auch die hybriden Sperrtechniken. Die von dem Gesetzentwurf präferierten leicht durchführbaren DNS-Sperrungen stellen die Accesprovider hingegen vor keine großen Probleme.

Die *Meinungsfreiheit der Inhaltsanbieter sowie die Informationsfreiheit der Nutzer* wird nicht durch die Sperrung der kinderpornografischen Angebote verletzt, sondern durch die bei vielen Sperrmaßnahmen mitblockierten legalen Angebote tangiert. Ein solches Overblocking ergibt sich vor allem bei der Sperrung von IP-Adressen.[21] Es ist allerdings auch bei DNS-Sperrungen leicht möglich, vor allem wenn unter einer Domain umfangreiche Verzeichnisse mit einer Vielzahl von Daten gespeichert sind. Dieser Effekt des Overblocking zeigte sich deutlich im Jahr 1996, als der Zugriff auf das Online-Magazin *radikal* unterhalb der Domain http://www.xs4all.nl vor allem über die entsprechende IP-Adresse gesperrt wurde. Durch die Sperrmaßnahme wurde auch der Zugriff auf mehrere tausend legale Angebote unmöglich gemacht. Auch heute noch sind viele Angebote (wie YahoolGroups) nicht unter einer eigenen (und damit vergleichsweise einfach zu sperrenden) Subdomain verfügbar, sondern unter einer gemeinsamen Domain, welche die verschiedenen Angebote erst auf der Ebene der (mit DNS-Sperren nicht mehr differenzierbaren) Verzeichnisnamen unterscheidet. Die als gesetzliche Mindestanforderung vorgesehene DNS-Sperre kann daher - z.B. wenn kinderpornografische Angebote über gehackte WWW-Seiten angeboten werden - zu einem massiven Overblocking führen und im Einzelfall unzumutbar sein.

Zu diesen Problemen kommen mögliche Einschränkungen der Funktionalität des Internets durch Sperrmaßnahmen, die bei DNS-Manipulationen auftreten können. So sind unter bestimmten Umständen nicht nur WWW-Angebote von einer DNS-Sperre betroffen, sondern auch ande-

---

[19] Zum Bekanntwerden der australischen Liste, vermutlich durch einen Hackerangriff auf einen Anbieter von Internet-Filterlösungen siehe http://www.heise.de/newsticker/meldung/139492 (abgerufen am 02.06.2009).

[20] Zu den Eingriffen der verschiedenen Sperrverfügungen in Grundrechte ausführlich *Sieber/Nolde* (Anm.9), S. 58 ff., 212 ff.

[2*] Viele Hostprovider vergeben eine IP-Adresse für zahlreiche Domains (sog. shared hosting). Wird diese IP-Adresse gesperrt, so sind nicht nur die illegalen Angebote betroffen, sondern auch alle anderen Domains, die unter dieser IP-Adresse abrufbar waren.

re Dienste.[22] Wenn die Sperrlisten einen größeren Umfang annehmen, stellt sich darüber hinaus das Problem der Skalierbarkeit der Maßnahmen, d.h. der Umsetzbarkeit und der Performanceverluste bei großen Datenmengen. Hinzu kommen finanzielle Aufwendungen der Provider, die bei den DNS-Sperren vergleichsweise gering sind, bei hybriden Sperrmaßnahmen der (auf der IP-Protokollebene arbeitenden) Accessprovider jedoch unzumutbar sein und zu Änderungen des Geschäftsmodells führen können.

### *6. Abwägungen im Hinblick auf die Art der Sperrmaßnahmen*

Der Gesetzentwurf wird diesen differenzierten Abwägungsprozessen nicht gerecht, wenn er die einfach durchzuführenden DNS-Sperrungen stets als zumutbar ansieht und als Mindestmaßnahme verlangt. Auch bei DNS-Sperrungen kann - vor allem für inhaltsreiche Domains und Subdomains mit zahlreichen Verzeichnissen - die Umsetzung der Sperrliste im Einzelfall schwierige Abwägungen erfordern und aus rechtlichen Gründen ausscheiden. Bei anderen Sperrtechniken (wie IP-Sperrungen oder hybriden Sperrtechniken) sind diese Abwägungen teilweise noch komplexer.

Besondere Probleme und Fragen treten bei einer vergleichenden Bewertung unterschiedlicher Sperrtechniken auf, etwa wenn über die mildeste Eingriffsmaßnahme zu entscheiden ist. Ist dies im konkreten Fall z.B. die DNS-Sperre (die finanzielle Interessen der Provider nur wenig berührt, aber aufgrund eines massiven Overblockings die Meinungs- und Informationsfreiheit der Nutzer stark belasten kann) oder aber die URL-Sperrung des speziellen Angebots (die wegen ihrer Zielgenauigkeit für die Meinungs- und Informationsfreiheit unproblematisch ist, jedoch einen auf der IP-Ebene arbeitenden Accessprovider zur Anschaffung eines Proxyservers zwingt)? Der Entwurf lässt insoweit auch offen, ob diese - sowohl von den Spezifika des illegalen Angebots als auch von der technischen Infrastruktur des jeweiligen Providers abhängigen - Abwägungsfragen vom Bundeskriminalamt oder vom Accessprovider entschieden werden sollen. Soweit es nur um DNS- oder IP-Sperrungen geht, können die entsprechenden Abwägungen von der staatlichen Behörde in allgemeiner Weise geprüft werden. Bei andern (z.B. URL-Sperrungen hängt die Verhältnismäßigkeitsprüfung dagegen auch von der technischen Infrastruktur der Provider ab. Die Effektivität des polizeilichen Listenverfahrens stößt daher hier an Grenzen, wenn nicht ein Verstoß gegen das verfassungsrechtliche Verhältnismäßigkeitsprinzip vorprogrammiert werden soll.

Der Entwurf klärt auch nicht die Frage, ob der Accessprovider bei rechtsfehlerhaften Entscheidungen über die Art der eingesetzten Sperrmaßnahmen seine Haftungsprivilegierung aus § 8a TMG-E für eine „ordnungsgemäße" Umsetzung der Sperrmaßnahmen verliert. Offen bleibt weiter, ob die - im Rahmen der Gesamtabwägung rechtmäßig oder rechtswidrig mitgeblockten - Informationsanbieter gegen die Bundesrepublik Deutschland Schadensersatzansprüche stellen können, die beim „Mitblockieren" von rechtmäßigen Angeboten leicht hohe Summen erreichen könnten. Der Gesetzgeber kann sich auch nicht darauf verlassen, dass Anbieter von Kinderpornografie ihre Angebote stets auf leicht isolierbare Domains und Subdomains ohne zusätzliche rechtmäßige Inhalte (in einzelnen Unterverzeichnissen) abspeichern werden.

---

[22] DNS-Anfragen sind nicht WWW-spezifisch, Eine Veränderung der DNS-Einträge kann daher Auswirkungen auf die Funktionsfähigkeit anderer Dienste haben, die unter der gleichen Domain angeboten werden, z.B. Chat oder in bestimmten Konstellationen sogar E-Mail.

### 7. *Probleme bei der Beurteilung der illegalen Angebote und bei deren Aktualisierung*

Die Umsetzungsprobleme von Sperrentscheidungen machen bereits deutlich, dass es sich bei Sperrmaßnahmen nicht um einfache Maßnahmen handelt, die wegen der leichten Erkennbarkeit von Kinderpornografie ohne verfahrensrechtliche Sicherungen möglich sind. Ähnlich schwierige Abgrenzungsfragen sind auch bei der Beurteilung des kinderpornografischen Charakters der Angebote und bei der Aktualisierung der Sperrlisten erforderlich.

Schwierige Grenzziehungen können sich vor allem bei den in § 8a TMG-E genannten kinderpornografischen Angeboten ergeben, „deren Zweck darin besteht, auf derartige Telemedienangebote zu verweisen". Dabei stellt sich etwa die Frage, ob hiervon nur eine direkte anpreisende Verlinkung oder auch eine mittelbare Verlinkung über mehrere Ebenen (die in der Regel auch zum Overblocking führt) erfasst ist. Ein eindrucksvolles Beispiel für eine entsprechende unzutreffende Rechtsanwendung ist die unten genannte (sogar gerichtliche) Entscheidung, in der ein von rechtswidrigen Inhalten weit entfernter Link als strafbar beurteilt wurde.[23]

Auch bei der Beurteilung der kinderpornografischen Darstellungen selbst ergeben sich schwierige Entscheidungen, z.B. im Hinblick auf das Alter der Darsteller, den erforderlichen Sexualbezug oder die Bewertung von verbalen literarischen Darstellungen. Die oben genannten Berichte und Experimente werden dabei häufig als Beleg für entsprechende Falschsperrungen herangezogen: Wie bereits erwähnt antworteten bei der oben genannten E-Mail-Aktion[24] 250 Provider, dass bei der Überprüfung der gesperrten Inhalte nur legale Seiten gefunden wurden. Stichproben sollen dies bestätigt haben und sogar belegen, dass die „überwiegende Mehrheit der Webseiten ... kein kinderpornographisches, teils überhaupt kein irgendwie beanstandbares Material" enthielten und die Sperreinträge daher zu Unrecht erfolgten. Auch die finnische Sperrliste soll überwiegend legale Angebote betreffen.[25] Die Schlussfolgerungen aus diesen Befunden sind allerdings nicht zwingend, da der Zeitpunkt der Sperranordnung und der Zeitpunkt der Inhaltsanalyse nicht identisch gewesen sein dürften und die Sperrungen auch zur Löschung oder Verlagerung von Angeboten geführt haben könnten. Die Zahlen können daher auch nur ein Beleg für die erheblichen Angebotsänderungen auf den jeweiligen WWW-Seiten sein.

Die hieraus resultierende Frage einer Aktualisierung der Sperrliste ist im vorliegenden Gesetzentwurf allerdings ebenfalls ungeklärt. Insoweit muss nicht nur berücksichtigt werden, dass die Inhalte unter einem bestimmten Domainnamen sich ständig verändern können.[26] Domains können auch aufgegeben oder verkauft werden und der neue Inhaber kann ausschließlich legale Inhalte unter einer Domain anbieten, die sich nach wie vor auf der Sperrliste befindet. Ein Domainwechsel erfolgt - wie die bisherigen Sperrmaßnahmen zeigen - vor allem auch als Gegenmaßnahme zu Sperrverfügungen.

---

[23] Näher dazu Anm. 35.

[24] Vgl. Anm.16.

[25] Dies zeigt z.B. die Analyse auf der Webseite „The filtering list and its contents" (abgerufen am 28.05.2009). Die einschlägige URL wird hier nicht angegeben, da sie auch *Links* zu Seiten enthält, die nach Angaben der Ersteller als kinderpornografisch eingeordnet werden könnten und den Verfasser nach LG Karlsruhe (unten Anm. 35) möglicherweise in die Gefahr einer Hausdurchsuchung bringen könnte.

[26] Im Rahmen der oben erwähnten E-Mail-Aktion (Anm.16) wurden auch gesperrte Angebote entdeckt, bei denen Hacker eine Sicherheitslücke ausgenutzt und den fremden Server anschließend zur Verbreitung von illegalem Material missbraucht hatten. Die Betreiber waren über diese Tatsache (ebenso wie über die Filterung) nicht informiert und zeigten sich „sehr dankbar für die Hinweise".

### 8. *Verfahrensrechtliche Garantien*

Damit ist offensichtlich, dass die Eingriffsintensität der Sperrungen und die im Einzelfall schwierigen Abgrenzungsprobleme des Listenverfahrens sowohl für die Erstellung als auch für die Umsetzung der Sperrlisten prozedurale Garantien erfordern Hier zeigt der Entwurf zwei - sich gegenseitige verstärkende - gravierende Probleme:

Das erste verfahrensrechtliche Defizit des Entwurfs besteht in der fehlenden Benachrichtigung der Informationsanbieter, die vor der Sperrung weder *rechtliches Gehör* noch die Möglichkeit einer Löschung oder (insbesondere bei Links) einer Umgestaltung ihrer Angebote erhalten, bevor die Sperrung möglicherweise unberechtigt in ihre Rechtspositionen eingreift. Diese Forderung nach rechtlichem Gehör folgt aus dem rechtsstaatlichen Gebot eines fairen Verfahrens und aus der Menschenwürde.[27] Die bloße Möglichkeit des Informationsanbieters, zufällig und nachträglich von der Sperrung zu erfahren und dann im normalen Verwaltungsverfahren gegen die polizeiliche Sperrung zu klagen, reicht insoweit als rechtsstaatliche Sicherung nicht aus. Das vom Gesetzentwurf vorgesehene Verfahren ist mit rechtsstaatlichen Anforderungen vor allem dann nicht vereinbar, wenn die polizeiliche Sperrliste geheim gehalten werden soll (vgl. § 8a Abs. 3 TMG-E und § 16 Abs. 2 N. 1b TMG-E). Es lässt sich auch kaum mit dem kriminalistischen Interesse an einer Geheimhaltung der ermittelten kinderpornografischen Angebote bis zur Identifikation der Hersteller und Anbieter rechtfertigen. In entsprechenden Fällen können die Ermittlungen vor der Indizierung der Angebote erfolgen, von der die Anbieter im Übrigen auch über die Stoppschildfunktion (z.B. mittels automatisierter Testabfragen) leicht Kenntnis bekommen können.

Die zweite verfahrensrechtliche Schwachstelle des Entwurfs liegt darin, dass die angestrebten Sperrentscheidungen durch eine *Polizeibehörde* und nicht durch einen Richter erfolgen. Das Grundgesetz geht davon aus, dass Richter aufgrund ihrer persönlichen und sachlichen Unabhängigkeit die Rechte der Betroffenen im Einzelfall am besten wahren können.[28] Für eine richterliche Entscheidung oder Bestätigung spricht vor allem auch wieder, dass die Sperrentscheidungen mit ihren teilweise schwierig zu beurteilenden Eingriffen in die Meinungs- und Informationsfreiheit den Anbietern und Hostprovidern nicht mitgeteilt werden und das hieraus resultierende Kontrolldefizit deswegen durch einen unabhängigen richterlichen Sachwalter kompensiert werden muss.[29] Denn die fehlende Anhörung des Betroffenen und die Heimlichkeit einer in Grundrechte eingreifenden staatlichen Ermittlungsmaßnahme erhöhen deren Eingriffsintensität und damit die Notwendigkeit eines Richtervorbehalts.[30]

Die verfassungsrechtlichen Implikationen der beiden Probleme sind allerdings nicht so strikt, dass für die schwierigen Verfahrensprobleme der Sperrverfügungen keine *praktikablen Lösungen* möglich sind.[31] Diese Probleme bei der Durchsetzung von Sperrverfügungen bestehen vor allem in dem massenhaften Auftreten und in der raschen Veränderung der kinderpornografi-

---

[27] *Stdkens/BonWSachsf Bonk/Kallerhoff,* Verwaltungsverfahrensgesetz, 7. Aufl. München 2008, § 28 Rn. 2 ff., 12.

[28] BVerfGE 103, 142 ff. (Rn. 33); 107, 299 ff. (Rn. 90).

[29] VerfG Sachsen JZ 1996, 957 (964).

[30] BVerfGE 103, 142 ff. (Rn. 34); BVerfGE 115, 320 ff. (Rn. 113); BVerfGE 120, 378 ff. (Rn. 79); VerfG Sachsen JZ 1996, 957, (963) sowie - für einen besonders eingriffsintensiven Spezialfall - BVerfG 120, 274 ff. (Rn. 257).

[31] Zur Flexibilität der Verfahrensgestaltung VerfG Sachsen JZ 1996, 957 (964).

sehen Angebote, die - insbesondere bei der Prüfung der Listenaktualität - nicht alle tagesaktuell von einem Richter geprüft werden können. Diese Probleme können deswegen dadurch gelöst werden, dass den Betroffenen - so weit dies möglich und zumutbar ist - die aufgefundenen kinderpornografischen Angebote mitgeteilt werden, sie zur Löschung der Angebote aufgefordert werden, und ihnen gleichzeitig die Möglichkeit zu einem Widerspruch gegeben wird. Eine richterliche Prüfung kann sich dann auf diese Widerspruchsfälle und möglicherweise auch auf bestimmte andere kritische Fälle beschränken. Ein solches „Widerspruchsmodell" entspräche dem deutschen Ordnungswidrigkeitenrecht oder dem Strafbefehlsverfahren, bei dem die richterliche Prüfung auch nur im Fall eines Widerspruchs oder Einspruchs erfolgt. Die Prüfung von Angebotsveränderungen könnte dabei ebenso wie ihre ordnungsgemäße Löschung durch ein Computersystem unterstützt werden, das den zuständigen Beamten täglich alle Veränderungen an den gesperrten Angeboten mitteilt. Für die Benachrichtigung der in unterschiedlichen Rollen Betroffenen und die Beschreibung eventueller Ausnahmen vom Grundsatz der richterlichen Entscheidung sollte eine gewisse Flexibilität vorgesehen werden, um in besonderen Fallgestaltungen und bei besonderen Gegenstrategien von Straftätern (etwa bei der ständigen Änderung in der Lozierung von Angeboten) noch angemessen reagieren zu können.

Die verfahrensrechtlichen Probleme lassen sich insbesondere durch eine konsequente Umsetzung des unten entwickelten sanktionsorientierten Sperransatzes lösen. Dieser Ansatz zielt vor allem auch auf das bereits oben angesprochene gravierendste Problem des Gesetzentwurfs, das in der fehlenden *Normierung der Subsidiarität* des Löschungsansatzes gegenüber dem Sperrungsansatz liegt.

### B. Weiterleitung von personenbezogenen Nutzerdaten an das BKA

Die nicht anonymisierte Protokollierung von Nutzerdaten durch die Provider und die Ermächtigung zur Weitergabe dieser Daten auf Anordnung der Strafverfolgungsbehörden nach § 8a Abs. 5 TMG-E entsprechen der neueren rechtspolitischen Tendenz, die Strafverfolgung durch die Nutzung von Daten zu verbessern, die bei einer präventiven Tätigkeit von Behörden oder Unternehmen (etwa zur Verhinderung von Geldwäsche) erlangt werden.[32] Eine solche Zwecksetzung kann daher in geeigneten Fällen eine verfassungsrechtlich relevante und zutreffende Zielsetzung sein.

Gegen die vorgeschlagene Regelung bestehen allerdings ebenfalls verfassungsrechtliche und sachliche Bedenken: Die Vorschrift ist zwar nicht als *WelXergabeverpflichtung* ausgestaltet. Da die protokollierten IP-Adressen zur Identifizierung der anfragenden Nutzer herangezogen werden können, ermächtigt die Regelung die Provider allerdings zu Eingriffen in das informationeile Selbstbestimmungsrecht der Nutzer. Grundrechtlich relevante Eingriffe liegen dabei auch in der Speicherung der personenbezogenen Daten, in ihrer Übersendung an die Ermittlungsbehörden sowie in der eventuellen Herstellung des Personenbezugs der IP-Adressen durch die Behörden. Diese Eingriffe müssen - vor allem wegen der damit verbundenen strafrechtlichen Zielsetzung und der auf behördliche Anforderung erfolgenden Datenübermittlung - den staatlichen Stellen wie eigene Eingriffsmaßnahmen zugerechnet und nach den gleichen Grundsätzen wie staatliche Eingriffe beurteilt werden.

---

[32] Dazu *Böse*, ZStW 119 (2007), 848 ff.

Für die rechtliche Beurteilung dieser Eingriffe ist deswegen relevant, dass die WWW-Anfrage nach einem kinderpornografischen Internetangebot nur einen geringen Verdacht auf die Begehung einer Straftat ergibt. Dies beruht auf mehreren Gründen: Die Anfrage kann ein mitgeblocktes legales Angebot betreffen. In vielen Fällen kennt der einen Link anklickende Internetnutzer auch den strafrechtlich relevanten Inhalt der aufgerufenen WWW-Seite noch nicht, sodass mangels Vorsatz selbst das Unternehmensdelikt des Sichverschaffens von kinderpornografischen Seiten noch nicht gegeben ist; die Einlassung des Verdächtigen, er habe nur für Erwachsene erlaubte Pornografie gesucht, wird in den meisten Fällen nicht zu widerlegen sein. Bei der Verabschiedung des Entwurfs werden sich viele Nutzer auch - wie oben erwähnt - einen (unter strafrechtlichen Gesichtspunkten nicht unproblematischen) „Spaß" daraus machen, über Links in E-Mails und auf WWW-Seiten Politiker und andere Personen zum - eventuell für diese gar nicht sichtbaren - Aufruf von kinderpornografischen Seiten zu veranlassen. Dies führt dann nicht nur dazu, dass diese Personen mit häufigen Zugriffsversuchen auf kinderpornografische Inhalte registriert werden. Es kann auch zur Folge haben, dass die den Link anklickenden Personen die Bilder der abgerufenen Seiten - eventuell unbemerkt - in ihrem Cache speichern. Falsche Ermittlungen und Rufmorde können dadurch vorprogrammiert werden, vor allem wenn der geringe Verdachtsgrad einer Erfassung von Anfragen auf der Stoppseite in der Praxis nicht richtig beurteilt wird.

Entsprechende Datenrasterungen von „etwas" verdächtigen Vorgängen sind - auch durch Private zum Zwecke der Strafverfolgung - gleichwohl unter bestimmten Bedingungen möglich, wie z.B. auch die Geldwäschebekämpfung der Finanzinstitute zeigt. Nach der Rechtsprechung des Bundesverfassungsgerichts muss die Verwendung dieser Daten dann jedoch nicht nur materielle Voraussetzungen (z.B. einem konkreten Tatverdacht) erfüllen, sondern auch in bestimmter und klarer Weise gesetzlich geregelt sein. Das BVerfG verlangt eine Schaffung eingriffsbeschränkender Maßstäbe durch den Gesetzgeber nicht nur zur Bindung der Verwaltung, sondern auch, damit „die betroffene Person grundsätzlich erkennen kann, bei welchen Anlässen und unter welchen Voraussetzungen ein Verhalten mit dem Risiko der Überwachung verbunden ist".[33] Verdachtslose oder an diffuse Anhaltspunkte anknüpfende Grundrechtseingriffe mit großer Eingriffstiefe sind wegen ihres Einschüchterungseffekts für die Ausübung von Grundrechten besonders problematisch.[34] Der bisherige Entwurf wird diesem verfassungsrechtlich gebotenen Bestimmtheitsgrundsatz in keiner Weise gerecht. Da die Unbestimmtheit der Regelung über die - geheim gehaltene - Datenauswertung der Strafverfolgungsbehörden das legale Nutzerverhalten beeinflussen und damit zu einem „Chilling effect" für die Informationsfreiheit führen dürfte, verstößt sie in der vorliegenden Form klar gegen verfassungsrechtliche Vorgaben.

Diesen „Chilling effect" für die Informationsfreiheit zeigte der Hinweis eines meiner Mitarbeiter, der mir sagte, die dänische Sperrliste sei zusammen mit einer kritischen Beurteilung auf einer bestimmten Internetseite gespeichert, er wolle den (m.E. noch eindeutig legalen) Abruf dieser Seite jedoch nicht versuchen, da ein solches Verhalten kürzlich zu Hausdurchsuchungen geführt habe.[35]

---

[33] BVerfGE 113, 348 ff. (Rn. 117).

[34] BVerfGE 115, 320 ff. (Rn. 117); ähnlich BVerfG NVwZ 2007, 688 ff. (691); BVerfG NJW 2008, 822 ff. (831).

[35] Vgl. dazu die unzutreffenden Beschlüsse des AG Pforzheim v. 30.01.2009, Az. 8 Gs 7/09 (http://www.internet-law.de/ag_pforzheim.pdf) und des LG Karlsruhe v. 23.02.2009, Az. Qs 45/09 (http://www.internet-law.de//lg_karlsruhe.pdf). In diesen Entscheidungen wird eine Hausdurchsuchung

Die gegenwärtige Regelung des § 8a Abs. 5 TMG-E muss deswegen entfallen. Ihre Problematik sollte in dem allgemeineren - vor allem für terroristische WWW-Seiten relevanten - Kontext einer Verrechtlichung der heimlichen Überwachung von WWW-Abrufen diskutiert werden.

### C. Evaluierungsverpflichtung

Die Evaluierungsverpflichtung des Entwurfs ist zu begrüßen. Sie sollte jedoch nicht nur präzisiert, sondern auch durch die laufende Begleituntersuchung eines unabhängigen Gremiums ergänzt werden. Dieses Gremium sollte den beteiligten Institutionen auch Vorschläge oder Vorgaben über die im aktuellen Betrieb möglichen anonymisierten Auswertungen machen können. Eine entsprechende Begleitforschung kann es dann ermöglichen, das Sperrverfahren in ein oder zwei Jahren realistisch zu bewerten.

## III. Zusammenfassende Bewertung und Konsequenzen

### A. Bewertung des gegenwärtigen Entwurfs

Zu der im Mittelpunkt des Entwurfs stehenden Sperrung von WWW-Seiten ist zusammenfassend festzustellen: Die als Mindesterfordernisse genannten DNS-Sperrungen werden nur eine sehr begrenzte Wirkung für den Schutz der missbrauchten Kinder haben. Ihre Bedeutung dürfte darin liegen, dass der noch öffentlich wahrnehmbare Bereich der Kinderpomografie im WWW von Deutschland aus weniger sichtbar ist, dass ein symbolisches Zeichen gegen Kinderpomografie gesetzt wird und dass mit den Stoppschildern eine kontextnahe Einwirkung auf die Nutzer erfolgen kann. Inwieweit diese Wirkungen dadurch aufgehoben werden, dass einzelne oder viele Benutzer ihre Computer dauerhaft auf nicht Sperrpflichtige DNS-Server im In- oder Ausland umstellen werden, ist schwer vorauszusagen. Es ist auch nicht auszuschließen, dass der mit dem Entwurf geregelte Sperransatz den bisher verfolgten, potentiell effektiven und weniger eingriffsintensiveren Löschungsansatz von notice-and-take-down-Verfahren schwächt, indem er Ressourcen anders zuordnet und die gravierende Problematik der in vielen Staaten weiterhin abrufbaren Opferbilder aus dem Sichtfeld der deutschen Öffentlichkeit und Politik bringt. Die Sperrmaßnahmen können darüber hinaus durch ein Overblocking in die Meinungs- und Informationsfreiheit eingreifen sowie negative technische und finanzielle Auswirkungen haben. Die Effektivität der vorgeschlagenen Regelung ist daher fragwürdig.

Auch die - nur „halbherzig" und in unklarer Weise verfolgte - repressive Speicherermächtigung und Befugnis zur Datenweiterleitung an das BKA führen zu keinem großen Sicherheitszuwachs. Es ist zweifelhaft, ob diese Regelungen den Strafverfolgungsbehörden die für eine erfolgreiche Tätigkeit notwendigen Daten überhaupt zur Verfügung stellen kann. Die Vorschrift wird im Hinblick auf potentielle Täter - spätestens nach der ersten Stoppschildwamung - auch dazu führen, dass die „verwarnten" oder „gewarnten" Personen einen anderen DNS-Server in ihren Computer oder Router eintragen und damit für ihren Computer das gesamte Sperr- und Proto-

---

wegen der (nicht unmittelbaren, sondern über mehrere WWW-Seiten vermittelten) Verlinkung auf die dänische Sperrliste angeordnet. Das LG Karlsruhe führt dabei aus, dass „aufgrund der netzartigen Struktur des World Wide Web [...] jeder einzelne Link im Sinne der conditio-sine-qua-non-Formel kausal für die Verbreitung krimineller Inhalte [sei], auch wenn diese erst über eine Kette von Links anderer Anbieter erreichbar sind". Siehe dazu auch http://www.heise.de/news/meldung/135461.

kollierungssystem dauerhaft abschalten, soweit dies auf DNS-Sperrungen beruht. Im Netz der Datenauswertung können allerdings unschuldige Personen hängen bleiben, die nicht wussten, welche Angebote in den von ihnen angesteuerten Domains (mit-)gespeichert waren.

Der gegenwärtige Entwurf kollidiert vor allem mehrfach mit verfassungsrechtlichen Garantien: Die fehlende Subsidiaritätsregelung und die damit gegebene Möglichkeit eines sofortigen eingriffsintensiven und nur begrenzt wirksamen Vorgehens gegen den „Nichtstörer" unter Verzicht auf ein oft einfaches und effektives Vorgehen gegen den Störer verstoßen gegen das verfassungsrechtliche Verhältnismäßigkeitsprinzip (insbesondere das Gebot der Erforderlichkeit/ Die unterbleibende Benachrichtigung der betroffenen Hostprovider (und eventuell auch der Inhaltsanbieter) verletzt den Grundsatz des rechtlichen Gehörs und tangiert damit vor allem den Grundsatz des fairen Verfahrens. Die Zuständigkeit einer Polizeibehörde für Eingriffe in die Informations- und Meinungsäußerungsfreiheit in Verbindung mit der Geheimhaltung der Sperrlisten ist im Hinblick auf die Verhältnismäßigkeit des Eingriffs in diese Grundrechte kritisch. Die Anordnung der DNS-Umleitung als Mindestsperrmaßnahme kann in einzelnen Fällen aufgrund eines Overblockings das Verhältnismäßigkeitsprinzip verletzen. Die unklare Befugnis zur Speicherung der Daten und ihrer Weiterleitung an das Bundeskriminalamt kollidiert mit dem Bestimmtheitsprinzip und - wegen ihres „Chilling effects" für die freie Kommunikation - mit der Meinungs- und Informationsfreiheit.

Diese Kollisionen müssen durch Änderungen des Entwurfs beseitigt werden. Aufgrund der verfassungsrechtlich anerkannten Einschätzungsprärogative des Gesetzgebers lässt sich das Risiko der Verfassungswidrigkeit des Entwurfs damit im weiteren Gesetzgebungsverfahren wesentlich mindern. Angesichts der geringen Effektivität der vorgeschlagenen Regelung und ihren gravierenden verfassungsrechtlichen Implikationen wäre es jedoch vorzugswürdig, das Gesetz noch einmal grundlegend zu überdenken.

## B. Ziele und Strategie eines Neuansatzes

Ziel der Überarbeitung des Entwurfs sollte es sein, die Bekämpfung der Kinderpornografie effektiver *und* verfassungsverträglicher zu regeln als der bisherige Gesetzentwurf. Der Entwurf muss auch die spezifischen Charakteristika des Internets besser berücksichtigen. Eine Regelung gegen die technische Natur des Internets ist wenig aussichtsreich. Das Gesetz sollte auch so effektiv und rechtsstaatlich ausgestaltet werden, dass es nicht wieder von einem großen Teil der fachkundigen Internet-Community abgelehnt wird, wie dies die kürzlich vorgelegte Petition von über 100.000 Internetnutzern gegen den Gesetzentwurf zeigt.[36]

Eine technisch angemessene, rechtsstaatliche und effektive Regelung kann nicht nur verhindern, dass die beabsichtigten Zugriffserschwerungen durch kollektive Gegenmaßnahmen der Internetnutzer ad absurdum geführt werden. Eine verbesserte Akzeptanz bietet auch die Chance, dass mehr Nutzer sich an der Bekämpfung der Kinderpornografie - z.B. in Zusammenarbeit mit Hotlines zur Meldung von kinderpornografischen Inhalten - beteiligen. Letzteres ist von essentieller Bedeutung: Die Eindämmung von Kinderpornografie in einem Netz mit weltweit 1,2 Milli-

[36] Vgl. https://epetitionen.bundestag.de/index.php?action=petition;sa=details;petition^3860. Die Online-Petition wurde am 22.04.2009 gestartet und hatte am 29.05.2009 bereits 102.616 Mitzeichner.

arden Nutzern und über 200 Millionen Websites[37] kann nur mit der und nicht gegen die Mehrheit der Nutzer erfolgreich sein.

Die Zielsetzung eines effektiven und rechtsstaatlichen Kinderschutzes erfordert weiterhin einen nationalen, regionalen und internationalen Gesamtansatz, der sowohl auf die Ermittlung der Kinderschänder als auch auf die Löschung der die Menschenwürde der Opfer verletzenden Bilder zielt. Bei dem Vorgehen gegen die Opferbilder ist der Vorrang der Löschung vor der partiellen (weil nur länderspezifischen) Sperrung klar im Gesetz zu verankern. Im Mittelpunkt des neuen Ansatzes gegen die pornografischen Internetangebote muss daher eine nationale, regionale und internationale Optimierung und Koordinierung der notice-and-take-down-Prozeduren stehen.[38]

Sperrungen dürfen in diesem System aus Gründen des Verfassungsrechts und der praktischen Effizienz nur ultima ratio sein. Ein neuer erfolgversprechender und die rechtlichen Probleme minimierender Ansatz zur Verwirklichung dieses Subsidiaritätsprinzips könnte darin liegen, die Sperrung der Seiten mit einem *sanktionsähnlichen Ansatz* erst dann vorzunehmen, wenn eine Löschung in vorwerfbarer Weise unterlassen wurde. Eine solche Handhabung der Subsidiarität von Sperrungen setzt voraus, dass die betroffenen Hostprovider und Informationsanbieter zunächst zur Löschung der gespeicherten Daten aufgefordert werden.[39] Besondere Aufmerksamkeit gebührt dabei der Aufforderung an diejenigen Personen, deren IP-Adressen oder Domains Gegenstand einer Sperrung sein können, die Inhalte selbst löschen oder eine Löschung veranlassen können und die deswegen eine Motivation zur Beseitigung der illegalen Inhalte haben, wenn sie sonst von der Sperrmaßnahme betroffen wären. Reagieren die Betroffenen nicht oder weigern sie sich, Daten zu löschen oder entsprechende Aufträge zu geben, so ist nicht nur die Sperrung der kinderpomografischen Inhalte sehr viel besser legitimiert und dem Grundsatz des rechtlichen Gehörs Rechnung getragen. Die in das Verfahren einbezogenen Akteure könnten sich dann in der Regel auch nicht mehr überzeugend gegen ein Overblocking ihner Inhalte wenden, wenn sie deren Sperrung durch eine Löschung der illegalen Angebote hätten verhindern können. Aus den gleichen Gründen wäre das Risiko von nachträglichen Schadensersatzansprüchen gegen die Stelle vermindert, welche die Sperrung angeordnet hat. Aufgrund der Mitteilung der rechtswidrigen Inhalte gegenüber den verantwortlichen Hostprovidern könnte teilweise auch die Prüfung der Aktualität von späteren Sperrverfügungen auf die angeschriebenen Hostprovider übertragen werden, die aufgrund ihres Antwortverhaltens eine EntSperrung veranlassen können. Bei dieser Lösung ist allerdings zu bedenken, dass die Sperrung auch andere Contentprovider betreffen kann. Ein entsprechendes Vorgehen muss daher weiterhin den Verhältnismäßigkeitsgrundsatz berücksichtigen, bei dessen Prüfung jedoch die Interessen der vorwerfbar die Sperrung von Kinderpornografie verweigernden Personen geringer bewertet werden dürfen. Den anderen „Mitbetroffenen" steht im Fall der „Mitsperrung" nur der Weg offen, sich gegen ihren Hostprovider zu wenden, der die Sperrung durch sein Verhalten hätte verhindern können. Eine solche Konsequenz würde den Druck auf den Hostprovider zur Löschung verstärken.

Es darf nicht verkannt werden, dass auch ein solcher sanktionsorientierter Löschungsansatz bei der Umsetzung von - als ultima ratio angeordneten - Sperrungen ebenfalls mit der begrenzten

---

[37] http://ne\vs.netcraftxoTn/archives/2009/05/27/may_2009_webserver_survey.htrril.

[38] Siehe bereits *Sieber*, in: Waltermann/Machill (Hrsg.) (Anm. 3), S. 320 ff.

[39] In bestimmten Fällen kann es erforderlich sein, diese Aufforderung auch auf andere Personen auszudehnen, welche die Daten löschen können, etwa auf einen Domaininhaber.

Wirksamkeit und den typischen Effektivitätsproblemen von Sperrmaßnahmen belastet wäre. Dies gilt vor allem in den Fällen, in denen kinderpornografische Inhalte von den Anbietern auf mehrere Server verteilt gespeichert werden. Der Vorteil eines solchen Vorgehens läge jedoch über die genannten rechtlichen Gesichtspunkte hinausgehend darin, dass - wie oben gezeigt[4]^ — ein großer Teil der Angebote nicht gesperrt, sondern gelöscht würde. Der kleinere Teil der verbleibenden Angebote, bei denen mangels Löschung Sperrmaßnahmen in Betracht gezogen werden, dürfte vor allem Angebote in „Oasenstaaten" betreffen, bei denen wegen des geringeren Verkehrsaufkommens Sperrungen leichter erfolgen können.

Wenn ein solches sanktionsorientiertes System zur Eindämmung kinderpomografischer Angebote nicht nur in einem einzelnen Staat, sondern in einer überregionalen Gemeinschaft angewandt würde, so könnte dies zu einem Machtpotential führen, das ausreichend Druck in (und auch auf) sperrunwillige(n) Staaten produziert. Die hier entwickelte Integration von Sperrverfügungen in einen sanktionsorientierten Löschungsansatz könnte damit erstmals auch eine Lösung für die schwierige Rechtsdurchsetzung in kooperationsunwilligen oder kooperationsunfähigen „Oasenstaaten" bilden. Der neue Ansatz müsste dann national erprobt und danach über die Europäische Union und weitere Kooperationen international ausgedehnt werden, um ihn wirkungsmächtig zu machen.

Ein solches Gesamtkonzept des Kinderschutzes im Internet kann nicht mehr in dem - damit überfrachteten und systematisch wenig passenden - Telemediengesetz normiert werden, sondern sollte eigenständig z.B. in einem „Gesetz zur Verhinderung der Kinderpornografie im Internet" geregelt werden. Dieses Gesetz könnte dann vier Regelungsbereiche oder Paragrafen enthalten:

- Es könnte in einem ersten Teil - ebenso wie ein späteres internationales Abkommen - den einschlägigen Kindesmissbrauch (§ 184 b, 176 Abs. 1 StGB) benennen sowie die im Internet verbotenen illegalen kinderpornografischen Inhalte definieren (letztere sollten im Hinblick auf Links präziser geregelt werden als in dem gegenwärtigen Entwurf).
- In einem zweiten Teil sollten die Verfahren zur konkreten Einordnung von Angeboten als Kinderpornografie und die Prozedur der notice-and-take-down-Verfahren gegenüber den Hostprovidern und Inhaltsanbietern normiert werden (auch mit vereinfachten Verfahren bei fehlender Reaktion der Hostprovider, Widerspruchsfristen, Rechtsmittel, Eilverfahren, sowie mögliche Sonderregelungen zur erleichterten Reaktion auf bestimmte Umgehungsstrategien von Straftätern).
- Auf dieser Grundlage kann der dritte Teil den Einsatz von Sperrmaßnahmen als ultima ratio und Sanktionen für den Fall vorsehen, dass die angezeigten kinderpornografischen Angebote nicht beseitigt werden. Dabei sollte auch geprüft werden, inwieweit die Accessprovider — eventuell in anonymisierter Form - den listenführenden Behörden bestimmte Daten (wie eventuell vorhandene „referer" auf verlinkende Listen) zur Optimierung der erfassten Seiten mitzuteilen hätten.
- Ein vierter Teil des Gesetzes könnte sich - auch erst später - mit der internationalen Zusammenarbeit befassen und insbesondere die gegenseitige Anerkennung von nationalen Verfahren und Entscheidungen regeln.[41]

---

[40] Anm. 16.

[41] Zu den maßgeblichen Gesichtspunkten *Sieber*, ZStW 2009 (121), 1 ff. 16 ff.

Die im Mittelpunk dieses Ansatzes stehende notice-and-take-down-Prozedur dürfte dabei aufgrund der erwartbaren Datenlöschungen den Umfang der notwendigen Sperren wesentlich reduzieren und die Opfer dadurch besser schützen. Wenn eine entsprechende Regelung in rechtsstaatlicher und überzeugender Weise ausgestaltet wäre, könnte sie auch zur Motivation der Netznutzer beitragen, von ihnen aufgefundene illegale Inhalte an die Hotlines zu melden, die als Public Private Partnerships betrieben und vernetzt sein könnten. Die Qualität von Public Domain Software, die von Internetnutzern gemeinsam geschaffenen Wikipedia-Werke oder die oben genannte Petition gegen den vorliegenden Gesetzentwurf zeigen, welche Leistungen eine Zusammenarbeit der Internetnutzer erbringen kann. Auf eine ähnliche Weise sollte das Netz zur Eindämmung von kinderpomografischen Angeboten unter Berücksichtigung seiner technischen Besonderheiten nicht gegen einen Großteil der Nutzer geregelt werden, sondern in einer neuen gemeinsamen Allianz von Nutzern, Internetindustrie und Ermittlungsbehörden.[42]

[42] Vgl. zu entsprechenden Vorschlägen die Nachweise oben Anm. 3 und 4.