

Stellungnahme

Gesetzentwurf der Bundesregierung zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen

7. Mai 2009

Seite 1

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

Die Bundesregierung hat am 22. April 2009 den Entwurf eines Gesetzes zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen beschlossen. Hiermit sollen die vom Kabinett am 25. März 2009 beschlossenen Eckpunkte umgesetzt und eine rechtliche Grundlage geschaffen werden für die von der Bundesregierung angestrebten Zugangshürden zu kinderpornographischen Inhalten im Internet. BITKOM hat bereits im Februar mit einer umfassenden Stellungnahme¹ seine Haltung zu den Plänen der Bundesregierung dargelegt und dabei ausdrücklich einen hinreichenden rechtlichen Rahmen eingefordert. Wir begrüßen daher, dass über die bereits geschlossenen Vereinbarungen hinaus nunmehr ein gesetzlicher Rahmen für das Ausnahmeinstrument technischer Zugangshürden geschaffen wird. Zur Vermeidung von Wiederholungen verweisen wir hinsichtlich der grundsätzlichen damit in Zusammenhang stehenden Fragestellungen auf unsere früheren Ausführungen und beschränken uns nachfolgend im Wesentlichen auf Anmerkungen zu den konkreten Regelungen des beabsichtigten Gesetzes.

Zusammenfassung der Forderungen des BITKOM

- Klarstellung in der Gesetzgebung, dass eine Ausweitung des Instrumentariums der Zugangshürde auf andere Inhaltskategorien nicht in Betracht kommt.
- Zusammenfassung der Regelungen in einem Spezialgesetz statt sachlich falscher und systemfremder Schwerpunktregelung im Telemediengesetz.
- Präzisierung der Begrifflichkeiten in Bezug auf die Adressaten der Regelung und die in der Sperrliste genutzten technischen Identifikations-Kategorien für die einzelnen Inhalte (§ 8a Abs. 1, 2 TMG-E).

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

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

Ansprechpartner

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

Präsident

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

Hauptgeschäftsführer

Dr. Bernhard Rohleder

¹ Abrufbar unter: http://www.bitkom.org/files/documents/090205_BITKOM-Stellungnahme_Expertengespraech_UA_neue_Medien_12_2_2009.pdf.

Stellungnahme

GE Bekämpfung der Kinderpornographie in Kommunikationsnetzen

Seite 2

- Beschränkung der Sperrliste auf Inhalte aus Drittländern außerhalb des Anwendungsbereiches der Richtlinie 2000/31/EG über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft.
- Klarstellung, dass das BKA nach § 8a Abs. 1 TMG-E zur permanenten Aktualisierung auch aller bestehenden Einträge in der Sperrliste verpflichtet ist, um die Ausweitung der Liste durch veraltete und fehlerhafte Einträge auszuschließen und zu verhindern, dass eine unnötigerweise immer umfangreichere Liste die Nutzung erschwert.
- Technische Implementierungspflicht für Zugangsanbieter beschränkt auf Werkzeuge.
- Streichung der objektiv nicht begründbaren und damit gleichheitswidrigen Bereichsausnahme für staatliche Anbieter von Zugangsdiensten, insbesondere Universitäten und Bibliotheken.
- Streichung des § 8a Abs. 5 TMG-E und Klarstellung, dass eine Verwertung anfallender personenbezogener Daten, sowie eine Erfassung, Speicherung, Nutzung und Übermittlung nicht stattfindet.
- Klarstellung, dass den nach § 8 Abs. 6 TMG-E zu übermittelnden statistischen Daten nur eine sehr begrenzte Aussagekraft zukommt.
- Präzisierung der Haftungsfreistellung nach § 8a Abs. 7 TMG-E im Sinne ausdrücklicher Hinweise, dass eine technisch bedingte Mitsperrung von Seiten, die nicht auf der Liste stehen, umfasst ist.
- Klarstellung im Gesetzestext, dass keine Verantwortlichkeit der Zugangsanbieter für fehlerhafte oder nicht mehr aktuelle Listeninhalte besteht.
- Klarstellung, dass die Haftungsfreistellung nach § 8a Abs. 7 TMG-E auch die Erfüllungsgehilfen des Access Providers mit umfasst, die bei der Erbringung der Zugangserschwerung mitwirken - Orientierung an § 110 TKG.
- Schaffung eines formalisierten, dem Verwaltungsrechtsschutz vorgelagerten formalisierten Beschwerdeverfahrens für Webseitenbetreiber zur schnellen Beseitigung zu Unrecht erfolgter Sperrungen.
- Schaffung eines Ausgleichs-Anspruchs für Webseiten-Betreiber gegenüber dem Bund für Vermögensschäden aufgrund der Sperrung legaler Seiten, sei es aufgrund fehlerhafter Listeneinträge oder technisch bedingter Mitsperrung.
- Klarstellung und Erweiterung der Auskunftspflicht nach § 8a Abs. 8 S. 2 TMG-E dahingehend, dass das BKA ausdrücklich auch die Erfüllung der Voraussetzungen des § 184b StGB gegenüber Diensteanbietern zu bestätigen und die Unternehmen im Falle rechtlicher Probleme zu unterstützen hat.
- Schaffung einer Regelung zur Kostenerstattung für die anfallenden Investitionskosten.
- Klarstellung, dass die technische Richtlinie nach § 8a Abs. 9 TMG-E in Zusammenarbeit mit den ISP erstellt wird.
- Klarstellung, dass die Evaluation nach Art. 3 des Entwurfs auch eine Beurteilung der Auswirkungen der Maßnahmen auf die Angebotslandschaft kinderpornografischer Inhalte im Internet umfasst.
- Schaffung einer Umsetzungsfrist von mindestens sechs Monaten.
- Klärung, dass Diensteanbieter nicht für technische Probleme ausländischer Dienstleister haften.

Stellungnahme

GE Bekämpfung der Kinderpornographie in Kommunikationsnetzen

Seite 3

Inhalt	Seite
1 Zielsetzung und Reichweite des Gesetzentwurfes	5
1.1 Zielsetzung	5
1.2 Reichweite	5
2 Spezialgesetz statt TMG-Regelung	6
3 Artikel 1 - Änderungen des Telemediengesetzes.....	7
3.1 § 8a Abs. 1 TMG-E	7
3.1.1 Verortung.....	7
3.1.2 Technische Identifikationskategorien	7
3.1.3 Begrenzung auf Nicht-EU-Inhalte	8
3.1.4 Fehlende Aktualisierungspflicht	8
3.2 § 8a Abs. 2 TMG-E	9
3.2.1 Adressatenkreis der Regelung.....	9
3.2.2 Wahlfreiheit bzgl. des Sperrverfahrens	10
3.2.3 Reichweite der Verpflichtung.....	10
3.3 § 8a Abs. 3 TMG-E – Sicherung gegen Kenntnisnahme durch Dritte.....	10
3.4 § 8a Abs. 4 TMG-E – Stoppsseitenbetrieb	11
3.5 § 8a Abs. 5 TMG-E Verwendung und Übermittlung von personenbezogenen Daten	12
3.6 § 8a Abs. 6 TMG-E – statistische Daten	13
3.7 § 8a Abs. 7 TMG-E – Haftung der ISP.....	13
3.8 § 8a Abs. 8 TMG-E – Nachweisverfahren	15
3.9 § 8a Abs. 9 TMG-E – technische Richtlinie.....	16
4 Artikel 2 – Änderung des Telekommunikationsgesetzes.....	16
5 Artikel 3 – Evaluierung	16
6 Implementierungsfristen	17
7 Kostentragung.....	17

Stellungnahme

GE Bekämpfung der Kinderpornographie in Kommunikationsnetzen

Seite 4

1 Zielsetzung und Reichweite des Gesetzentwurfes

1.1 Zielsetzung

BITKOM legt großen Wert auf eine klare Festlegung der Zielsetzung der beabsichtigten gesetzlichen Regelung. Wie bereits vielfach betont, können technische Maßnahmen allenfalls einen flankierenden, in seiner Wirksamkeit beschränkten Beitrag zur Bekämpfung der Verbreitung von kinderpornographischen Inhalten im Internet leisten. Sie sind insbesondere nicht ausreichend, um wirksam gegen die Herstellung und die Verbreitung von Kinderpornographie vorzugehen. Hierfür bedarf es vielmehr verstärkter Anstrengungen zur Täterermittlung und Entfernung der eigentlichen Inhalte. Beides ist bereits heute in der großen Mehrzahl der hiervon betroffenen Länder möglich.

Wir begrüßen es daher, dass der nunmehr vorgelegte Entwurf bewusst von der Terminologie der „Sperrung“ weggeht und in Begründung und Gesetzestext von einer „Erschwerung des Abrufs“ spricht. Dies trägt sachgerecht dem Umstand Rechnung, dass sämtliche denkbaren technischen Verfahren mit gewissem technischem Know-How umgehbar sind und durch solche Maßnahmen keine Entfernung der eigentlichen Inhalte aus dem Netz erfolgt.

BITKOM weist daneben nochmals darauf hin, dass eine relevante Beeinträchtigung des weltweiten kommerziellen Angebots für kinderpornographische Inhalte durch Zugangshürden nicht zu erwarten ist. Die geplanten technischen Maßnahmen können daher allenfalls dazu dienen, den zufälligen Kontakt mit entsprechenden Inhalten zu beschränken. Soweit der Kabinettsbeschluss vom 25. März 2009 im Gegensatz zum jetzt vorgelegten Entwurf noch das Ziel verfolgte, den „kommerziellen Massenmarkt für Kinderpornographie im Internet empfindlich zu stören“ stehen wir diesem Ziel skeptisch gegenüber. BITKOM sieht stattdessen nach wie vor Bedarf für weitere politische Initiativen zur gezielten Verbesserung der weltweiten Täterverfolgung. Hierzu zählen insbesondere eine verbesserte technische und personelle Ausstattung der deutschen Ermittlungsbehörden sowie eine Verbesserung der internationalen Kooperation. Schließlich muss konsequent sichergestellt sein, dass auf in Deutschland befindlichen Servern entsprechende Inhalte nicht verfügbar gemacht werden. Dort wo Zugriffsmöglichkeiten der Behörden auf die konkreten Server bestehen, muss die Entfernung der Inhalte stets der Aufnahme in Sperllisten vorgehen.

Positiv bewerten wir, dass die Begründung des Entwurfs das bereits bestehende vielfältige Engagement der deutschen Internetwirtschaft ausdrücklich würdigt.

1.2 Reichweite

BITKOM begrüßt nachdrücklich, dass das vorliegende Gesetz in seinem Anwendungsbereich strikt auf kinderpornographische Inhalte beschränkt ist und die Bundesregierung mehrfach betont hat, dass eine Ausweitung auf andere Inhaltskategorien nicht geplant ist. Wir stehen weiterhin auf dem Standpunkt, dass es sich bei der Inanspruchnahme von Internet Service Providern zu technischen Zugangshürden um ein „Ultima-ratio“-Instrument handelt, welches nicht zu

Stellungnahme

GE Bekämpfung der Kinderpornographie in Kommunikationsnetzen

Seite 5

einem regulatorischen „Allheilmittel“ ausgebaut werden darf. Mit tiefer Skepsis bewerten wir daher die von den Innenministerien der Länder artikulierten Forderungen nach einer Sperrung ausländischer Glücksspielseiten zur Durchsetzung des staatlichen Lottomonopols, die nicht zuletzt grundlegenden Wertungen des europäischen Rechts zuwiderlaufen.

Die Gesetzesbegründung zum vorgelegten Entwurf lässt bedauerlicherweise eine deutliche Aussage zur mehrfach von den zuständigen Ministerien artikulierten Zielsetzung, Zugangshürden auf den klar abgrenzbaren Bereich kinderpornografischer Inhalte zu beschränken, vermissen. Es ist für uns nicht nachvollziehbar, dass diese Intention sich nicht in den Erläuterungen zum Gesetzentwurf wiederfindet.

2 Spezialgesetz statt TMG-Regelung

Vor dem Hintergrund dieser Erwägungen hält es BITKOM außerdem nach wie vor für sinnvoll und dringend geboten, die angedachten Mechanismen über eine spezialgesetzliche Regelung zu realisieren, um deren Ausnahmecharakter zu unterstreichen und deutlich zu machen, dass es sich um eine abschließende Regelung handelt. Die stattdessen gewählte Systematik über eine Verankerung sämtlicher maßgeblicher Regelungen im Telemediengesetz (TMG) führt zu schwerwiegenden Systembrüchen und lässt aufgrund des Querschnittscharakters des TMG befürchten, dass das Instrument künftig für weitere Inhaltskategorien fruchtbar gemacht werden soll. Dies lehnen wir klar ab.

Die - notwendig - sehr detaillierte Regelung zu den Zugangssperren gegen Kinderpornographie stört erheblich die Klarheit und Verständlichkeit des ansonsten einfach und prägnant strukturierten Telemediengesetzes. Eine solche Ergänzung würde die Handhabbarkeit des Gesetzes für alle von diesem sehr spezifischen Thema nicht betroffenen Gesetzesadressaten erheblich erschweren. Auch dies spricht unbedingt für die Auslagerung in ein Spezialgesetz.

Aus gesetzessystematischer Sicht kann insbesondere die Einordnung des gesamten Regelungskomplexes in § 8a TMG-E nicht überzeugen. Ziel war offenbar, die Regelung der allgemeinen Haftungsprivilegierung für Zugangsanbieter nach § 8 TMG zuzuordnen. Im Ergebnis finden sich nach dem vorgelegten Vorschlag nunmehr jedoch unter dem auf der europäischen E-Commerce-Richtlinie beruhenden Abschnitt „Verantwortlichkeit“ des TMG neben der eigentlichen Anordnung zur Implementation von Sperrlisten auch Regelungen zu Befugnissen des Bundeskriminalamtes, datenschutzrechtliche Regelungen und Übermittlungsbefugnisse, die Verpflichtung zum Betrieb einer Stoppseite, eine Haftungsregelung sowie Dokumentationspflichten für das BKA.

Diese Ansammlung verschiedenster Regelungen passt sich in keiner Weise in die allgemeine Systematik des 3. Abschnitts des TMG ein und verwässert dessen Regelungszweck. Die Bestimmungen des 3. Abschnitts regeln insgesamt die europarechtlich vorgegebene Haftungsbegrenzung von Internetdiensteanbietern; die hier nunmehr niedergelegten Regelungen regeln stattdessen das

Stellungnahme

GE Bekämpfung der Kinderpornographie in Kommunikationsnetzen

Seite 6

Gegenteil, nämlich spezifische Handlungspflichten für verschiedene Akteure, darunter mit dem BKA auch eine Institution, die weder vom allgemeinen Anwendungsbereich des TMG noch vom Anwendungsbereich der §§ 7 ff. TMG erfasst wird.

Angesichts dieser schwerwiegenden gesetzesystematischen Brüche scheint es dringend angezeigt, die verfolgten Pläne über eine spezialgesetzliche Regelung zu realisieren.

3 Artikel 1 - Änderungen des Telemediengesetzes

Vorbehaltlich der oben geäußerten generellen Bedenken gegen einen im TMG verankerten Regelungsansatz erlauben wir uns zu den konkreten Elementen des Entwurfs folgende Anmerkungen:

3.1 § 8a Abs. 1 TMG-E

3.1.1 Verortung

Die Regelung beinhaltet eine Befugnis des Bundeskriminalamtes zur Erstellung einer Sperrliste. Diese Regelung sollte daher entsprechend der oben vorgebrachten Erläuterungen einem Spezialgesetz vorbehalten sein.

3.1.2 Technische Identifikationskategorien

Offen bleibt nach der Formulierung des Entwurfs, worin der Unterschied zwischen „vollqualifizierten Domainnamen“ und „Zieladressen von Telemedienangeboten“ besteht. Der Begriff der „Zieladressen von Telemedienangeboten“ ist kein verbindlicher technischer Terminus und dürfte Auslegungsdiskussionen provozieren. Letztlich scheint der Begriff der Zieladressen einen Oberbegriff zu definieren, der auch vollqualifizierte Domainnamen enthält. Dies wirft allerdings die Frage auf, welche weiteren Kategorien hierunter ggf. gefasst werden können und sollen. Da auch die Begründung des Entwurfs hierzu keinerlei Erläuterungen enthält, bedarf es einer Klarstellung des Normwortlautes. Der Begriff „vollqualifizierte Domainnamen“ ist zwar insofern klar, als es sich um eine Eindeutigung des englischen „Fully Qualified Domain Name (FQDN)“ handelt. Selbst damit ist jedoch noch nicht festgelegt, ob nur ein Host oder eine ganze Domain zu sperren ist.

Unklar ist weiter, wie mit Hosts umzugehen ist, auf denen lediglich in bestimmten Pfaden Inhalte nach § 184b StGB verfügbar sind. Die Auswirkungen einer Sperre des gesamten vollqualifizierten Domainnamens sind in solchen Fällen üblicherweise besonders gravierend, weil extrem viele unbeteiligte Nutzer betroffen sein werden. Eine solche Sperrung wäre jedenfalls unverhältnismäßig und sollte daher ausgeschlossen sein.

Schließlich bleibt offen, ob die seitens des BKA zu erstellende Sperrliste für jedes der entsprechenden Angebote jeweils sämtliche technische Identifikationskategorien (etwa vollqualifizierte Domainnamen *und* Internetprotokolladressen) vorhalten soll oder das BKA befugt sein soll, eine spezifische Kategorie zu wählen. Auch hierzu gibt die Begründung des Entwurfs nichts her.

Stellungnahme

GE Bekämpfung der Kinderpornographie in Kommunikationsnetzen

Seite 7

3.1.3 Begrenzung auf Nicht-EU-Inhalte

Nach Auffassung der federführenden Ministerien handelt es sich bei den avisierten Maßnahmen um flankierende Maßnahmen für einen spezifisch abgrenzbaren Bereich. Die Täterverfolgung und echte Beseitigung der Angebote stehen ausweislich der entsprechenden Pressemitteilungen auch nach Auffassung der zuständigen Ressorts im Vordergrund.

Vor diesem Hintergrund ist es nicht nachvollziehbar, weshalb die in öffentlich gewordenen früheren Entwurfsversionen des Gesetzes vorgesehene Beschränkung auf Inhalte aus Nicht-EU-Staaten entfallen ist. Nach dem aktuellen Entwurf dürfte die Sperrliste des BKA sogar Inhalte aufführen, die auf deutschen Servern vorgehalten werden. Dies widerspricht zum einen dem bereits in der Arbeitsgruppe zur Thematik erzielten gemeinsamen Verständnis, dass derlei Inhalte nicht Gegenstand der Sperrliste sein dürfen.

Vor allem aber wird hierdurch der extrem kontraproduktive Eindruck vermittelt, dass künftig selbst dort, wo ein Zugriff auf die eigentlichen Inhalte und mithin eine echte Löschung derselben möglich wäre, stattdessen das Instrument der Zugangerschwerung eingreifen soll. Dies untergräbt die Akzeptanz des gesamten Vorhabens.

Da im Rahmen der Europäischen Union überdies Rechtshilfeabkommen sowie mit Interpol eine länderübergreifende agierende Polizeiinstitution existieren muss auch in diesem Rahmen stets die Löschung der Inhalte Vorrang haben. Die in der Vorversion enthaltene sachgerechte Beschränkung auf Inhalte aus Drittländern außerhalb des Anwendungsbereiches der Richtlinie 2000/31/EG über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft ist daher wieder in den Gesetzestext aufzunehmen.

3.1.4 Fehlende Aktualisierungspflicht

Die Regelung des § 8a Abs. 1 TMG-E lässt in der jetzigen Fassung eine ausdrückliche Aktualisierungspflicht vermissen. Nach Aussagen aller Experten im Rahmen der Beratungen zur Thematik wechseln Anbieter entsprechender Inhalte nahezu im Tagesrhythmus die Server bzw. die entsprechenden Zieladressen. Da der Zielsetzung des Entwurfs zufolge die Sperrlistenbefugnis des BKA strikt auf kinderpornographische Inhalte beschränkt ist, muss ausdrücklich klargestellt werden, dass Listeneinträge, die aufgrund einer Veränderung der hinterlegten Inhalte nicht mehr auf kinderpornographische Inhalte verweisen, sofort aus der Liste entfernt werden. Andernfalls droht ein permanentes Anwachsen der Sperrliste ohne Rückabgleich, was systemtechnisch bedingt auch zu Performanz-Problemen führen kann.

BITKOM ist sich bewusst, dass eine dauernde Pflicht, auch bereits bestehende Einträge erneut zu prüfen und zu aktualisieren, eine deutliche Mehrbelastung darstellt, sie ist jedoch unabdingbar nötig. Allein der Grundsatz der Vermeidung unnötiger und der Berichtigung falsche Daten gebietet die Aktualisierung. Es ist

Stellungnahme

GE Bekämpfung der Kinderpornographie in Kommunikationsnetzen

Seite 8

in jedem Fall zu vermeiden, dass die Liste innerhalb kurzer Zeit ein nicht mehr handhabbares Ausmaß annimmt.

Für die Unternehmen sollte eine Pflicht zur Implementierung der Liste nur werktags zu den Geschäftszeiten festgeschrieben werden. Ein 24/7-Erreichbarkeit wäre mit erheblichem organisatorischem und kostentechnischem Aufwand verbunden, der nur einen unerheblichen Mehrwert darstellen würde.

3.2 § 8a Abs. 2 TMG-E

3.2.1 Adressatenkreis der Regelung

Das Gesetz verpflichtet nach der gewählten Terminologie zunächst „Diensteanbieter i.S.v. § 8 TMG“. § 8 TMG enthält allerdings keine eigenständige Definition, sondern spricht im Ausgangspunkt selbst nur von Diensteanbietern – ein Begriff der wiederum legaldefiniert ist in § 2 Nr. 1 TMG. Danach ist Diensteanbieter *„jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt“*. Es bleibt daher der genaue Anwendungsbereich von § 8a Abs. 2 TMG-E unklar. Gemeint ist wohl „Diensteanbieter in Ausübung der in § 8 TMG beschriebenen Tätigkeit“ – jedoch ist dies durch den Wortlaut nicht eindeutig. Der Verweis auf § 8 TMG lässt insbesondere auch die Frage offen, ob auch reine Resale-Dienstleister erfasst werden. Dies wirft schon deswegen Probleme auf, weil diese in der Regel keinen Einfluss auf das Netz und insbesondere die DNS-Server haben werden. In einem solchen Fall müsste eine dem § 110 TKG angelehnte Regelung geschaffen werden, mit deren Hilfe sich der Diensteanbieter des Netzbetreibers bedienen kann. Spiegelbildlich müsste auch die Haftungsregelung des § 8a Abs. 7 TMG-E auf diese Netzbetreiber, die nicht zugleich Diensteanbieter im oben genannten Sinne sind, erweitert werden.

BITKOM weist überdies darauf hin, dass mit der Herausnahme staatlicher Einrichtungen, die als Zugangs-Provider tätig werden, die ohnehin begrenzte Wirksamkeit der avisierten Maßnahmen weiter geschmälert wird. Der Gesetzentwurf erläutert in seiner Begründung nicht, weshalb überhaupt staatliche Einrichtungen aus dem Anwendungsbereich ausgeklammert werden; objektiv lässt sich hierfür keinerlei Rechtfertigung finden. Da es sich um eine Ungleichbehandlung handelt, muss diese jedoch sachlich begründet werden, um Art. 3 GG standzuhalten. Soweit die Ausklammerung, wie zu vermuten steht, aus Kostengründen erfolgt, kann dies die Ungleichbehandlung nicht rechtfertigen, da auch bei den betroffenen privatwirtschaftlichen Anbietern erhebliche Belastungen entstehen, die jedenfalls nach dem vorgelegten Entwurf nicht entschädigt werden würden. Soweit ferner ein unverhältnismäßiger Aufwand bei staatlichen Einrichtungen vermieden werden soll, kann dies über die allgemeine Einschränkung auf Anbieter mit mindestens 10000 Nutzern bewirkt werden. Vor dem Hintergrund dieser Erwägungen bewerten wir § 8a TMG-E in seiner jetzt vorgelegten Form als gleichheitswidrig.

Stellungnahme

GE Bekämpfung der Kinderpornographie in Kommunikationsnetzen

Seite 9

3.2.2 Wahlfreiheit bzgl. des Sperrverfahrens

Positiv bewerten wir dagegen die durch § 8a Abs. 2 TMG-E grundsätzlich bewirkte Wahlfreiheit bezüglich der konkreten technischen Umsetzung des Sperrverfahrens durch eine technologieneutrale Ausgestaltung. Hiermit wird den unterschiedlichen technischen Ausgangsvoraussetzungen in den verschiedenen Netzen Rechnung getragen.

Dabei ist bedeutsam, dass der Gesetzentwurf ausdrücklich ein DNS-basiertes Verfahren als technische Lösungsoption vorsieht. BITKOM betont, dass in den vorangegangenen Vertragsverhandlungen stets allein diese Lösung diskutiert wurde und in den abgeschlossenen Verträgen auch die Umsetzung über ein DNS-basiertes Verfahren verbindlich vereinbart wurde. Aufgrund dieser Vorarbeit ist die Umsetzung via DNS Sperre das naheliegende Mittel für die involvierten Provider.

3.2.3 Reichweite der Verpflichtung

Wir begrüßen, dass § 8a Abs. 2 TMG auch ausweislich der Begründung als reine Handlungspflicht ausgestaltet ist, die zudem direkt die Kriterien der Zumutbarkeit und technischen Möglichkeit aufgreift. Hiermit wird verdeutlicht, dass eine vollständige Blockade spezifischer Inhalte nach keinem bekannten Verfahren technisch realisierbar ist.

Ebenso unterstützen wir den Ansatz, die Verpflichtung auf die rein technische Implementation der staatlichen Sperrliste zu beschränken, womit klargestellt ist, dass die Provider keinerlei eigene Prüfungspflicht bzgl. kinderpornographischer Inhalte trifft. Allerdings könnte diese Zielrichtung der Verpflichtung durch folgende Formulierung noch besser verdeutlicht werden:

„...haben geeignete und zumutbare technische Maßnahmen zu ergreifen, um durch technische Einbindung der Sperrliste nach Absatz 1 den Zugang zu Telemedienangeboten, die Kinderpornographie nach § 184b des Strafgesetzbuchs enthalten, zu erschweren.“

Angesichts der von uns insgesamt abgelehnten Integration der Regelungen in das TMG muss § 8a Abs. 2 TMG-E außerdem um die Klarstellung ergänzt werden, dass § 7 Abs. 2 S. 1 und § 8 Abs. 1 TMG unberührt bleiben.

3.3 § 8a Abs. 3 TMG-E – Sicherung gegen Kenntnisnahme durch Dritte

Hinsichtlich der Sicherung vor Kenntnisnahme durch Dritte plädieren wir zunächst für folgende präzisere Formulierung des Begriffs des Dritten:

“...durch Dritte ~~die an den technischen Maßnahmen zur Vornahme von Sperrungen nicht beteiligt sind.~~ Dritter in diesem Sinne ist, wer nicht an der technischen Erbringung der Zugangerschwerung nach § 8a Abs. 2 TMG mitwirkt.“

Stellungnahme

GE Bekämpfung der Kinderpornographie in Kommunikationsnetzen

Seite 10

Die Frage der Anforderungen an die Sicherungsmechanismen der Provider sollte aus Gründen der Rechtssicherheit außerdem Gegenstand der technischen Richtlinie sein und in Zusammenarbeit mit den Providern erarbeitet werden.

Außerdem muss zumindest in der Begründung klargestellt werden, dass eine etwaige Ermittlung von Listenbestandteilen durch systematische Abfragen und Abgleich mit der Stopp-Seite nicht in den Verantwortungsbereich der Provider fällt, da dieser Gefahr bei der gesetzlich festgelegten Methodik der Einbindung einer Stopp-Seite faktisch nicht begegnet werden kann, weshalb zu befürchten steht, dass auf diesen Weg zumindest Teile der Liste bekannt werden. Anders ausgedrückt: Da die Rückübermittlung einer Stoppseite per Definition öffentlich ist, schließen sich Stoppseitenbetrieb und Geheimhaltung der Liste faktisch gegenseitig aus.

3.4 § 8a Abs. 4 TMG-E – Stoppseitenbetrieb

Für BITKOM bleibt nach der Neufassung das Verhältnis von Stoppseitenbetrieb und den datenschutzrechtlichen Erwägungen im Zusammenhang mit dem Gesetz unklar. Sowohl das BKA als auch das Bundesfamilienministerium hatten in den Arbeitsgruppensitzungen argumentiert, dass ein Betrieb seitens einer staatlichen Stelle ausscheide, weil eine solche nicht über Zugriffsdaten verfügen dürfe. Der Grund dafür, dass die Provider die Stoppseite betreiben sollen, lag danach in erster Linie darin, dass eine Weiterreichung von Zugriffsdaten möglichst vermieden werden sollte. Nach dem aktuellen Vorschlag zu § 8a Abs. 5 TMG-E sollen die Daten nun jedoch gesetzlich verpflichtend weitergegeben und die Stoppseite gleichwohl durch die Zugangsanbieter betrieben werden. Da die Bundesregierung eine solche Weitergabe offenbar für zulässig hält, muss daher auch der Stoppseitenbetrieb selbst durch das BKA erfolgen können. Es bleibt daher für uns offen, wieso der Gesetzentwurf hierfür pauschal die Zugangsanbieter verpflichtet wissen will.

Im Übrigen bestimmt § 8a Abs. 4 TMG-E lediglich allgemein, dass die in der Filterliste aufgeführten Telemedienangebote auf Stoppseiten umzulenken sind. Hierbei wird übersehen, dass Internet auch auf Protokollen abseits von HTTP beruht. Bei Verwendung des HTTPS-Protokolls ist eine Umleitung gerade nicht möglich, weil HTTPS eben gegen solche Umlenkungen schützen soll. Aber auch bei dem Standard-Protokoll HTTP gibt es erhebliche Probleme, weil der Stopp-Server nicht erraten kann, welchen Datentyp der Browser erwartet.

Wir weisen außerdem darauf hin, dass sich der Stoppseitenbetrieb nicht mit den kommenden Regelungen über die Signatur von DNS-Datenbanken und die Sicherheit der DNS-Auflösung gegen Manipulation vereinbaren lässt. Eine Technik wie die hier vorgeschlagene Umleitung auf eine Stoppseite dürfte nicht mit dem Ziel der DNS-Reformen in Einklang zu bringen sein, eben solche Arten von Umleitungen, Domain-Hijacking und verwandte Techniken auszuschließen. Dies würde dazu führen, dass Zugangsanbieter nur noch die DNS-Auflösung unterbinden, aber nicht mehr auf eine Stopp-Seite umleiten können, sobald die neuen Regelungen über die Authentifizierung im DNS wirksam werden.

Stellungnahme

GE Bekämpfung der Kinderpornographie in Kommunikationsnetzen

Seite 11

Da Internetzugangsanbieter nicht zu technisch Unmöglichem verpflichtet werden können, bedarf es auch in § 8 Abs.4 TMG-E somit jedenfalls des allgemeinen Vorbehalts „soweit technisch möglich und zumutbar“.

3.5 § 8a Abs. 5 TMG-E Verwendung und Übermittlung von personenbezogenen Daten

Mit der Regelung des § 8a Abs. 5 TMG-E wird die Befugnis für Internetzugangsanbieter geschaffen, im Rahmen der Implementierung der Sperrliste und des Betriebs der sog. Stopp-Seite anfallende personenbezogene Daten zu erheben und zu verwenden, um auf Anordnung zuständiger Stellen diese Daten zum Zwecke der Strafverfolgung zu übermitteln. Die Regelung zielt damit darauf ab, die im Rahmen von Zugangshürden anfallenden Daten für strafrechtliche Ermittlungen nutzen zu können. Formal betrachtet ist § 8a Abs. 5 TMG allerdings in sich selbst widersprüchlich. Zunächst heißt es, personenbezogene Daten dürfen nur erhoben und verwendet werden, *soweit* dies für Maßnahmen nach Abs. 2 und 4 notwendig ist. Im Anschluss aber heißt es, dass Daten auch an die Strafverfolgung weitergeleitet werden dürfen, somit auch für darüberhinausgehende Zwecke verwendet werden können.

BITKOM ist überrascht von diesem Regelungsvorschlag, da er diametral der mehrfach explizit in den Arbeitsgruppensitzungen geäußerten Absicht der federführenden Ressorts widerspricht, das Instrument der Zugangshürden nicht mit strafrechtlichen Ermittlungsmaßnahmen zu verbinden. Diese Absicht spiegelt sich nicht zuletzt im Text der Stoppseite wider, welche die Bundesfamilienministerin anlässlich der Vertragsunterzeichnung am 17. April 2009 vorstellte. Dort heißt es ausdrücklich:

„Weder Informationen zu Ihrer IP-Adresse noch andere Daten anhand derer Sie identifiziert werden könnten, werden vom Bundeskriminalamt gespeichert, wenn diese Seite erscheint. Die Sperrung dieser Webseiten erfolgt ausschließlich, um die kriminelle Verbreitung von Darstellungen sexuellen Missbrauchs und die weitere Ausbeutung der Kinder zu erschweren.“

Soweit dieser vorgestellte Text lediglich davon spricht, dass die Daten nicht „vom Bundeskriminalamt“ gespeichert werden, ist mit Nachdruck darauf hinzuweisen, dass in den Vorbesprechungen innerhalb der Arbeitsgruppe seitens sämtlicher beteiligter Ministerien versichert wurde, dass keinerlei Speicherung, somit insbesondere auch keine Speicherung auf Seiten der Zugangsanbieter zur Nutzung für Strafverfolgungszwecke erfolgen darf und soll. ISP dürfen keinesfalls zur Einbindung eines Stoppseitentextes verpflichtet werden, welcher die Nutzer faktisch über die Verwertung der anfallenden Log-Daten in die Irre führt.

Die mit § 8a Abs. 5 TMG-E geplante Regelung bedeutet eine vollständige Abkehr von der bisher verfolgten Linie und unterstellt faktisch, dass jeder Zugriff auf die Stopp-Seite eine Straftat darstellt. Das ist sachwidrig und rechtlich bedenklich, da es viele Methoden gibt, einen Internet-Nutzer ohne dessen Willen

Stellungnahme

GE Bekämpfung der Kinderpornographie in Kommunikationsnetzen

Seite 12

und ohne dass es ihm bewusst wird, zur unterschwelligeren dauerhaften Abfrage von Webseiten zu bringen, die dann auch im Browser-Cache lägen und bei einer Hausdurchsuchung zum „Beweismittel“ würden. Insbesondere sehen wir die Gefahr, dass Dritte, die darauf aus sind, Unbeteiligte zu schädigen, diese Situation ausnutzen könnten, etwa durch gezieltes Verbreiten entsprechender Links innerhalb öffentlicher Internet-Foren.

BITKOM lehnt die in § 8a Abs. 5 TMG-E enthaltene Befugnis ab. Sie drängt die ISP in eine Rolle, die klar über die eines rein technischen Mittlers zur Umsetzung der Zugangshürden hinausgeht und macht sie zum Beteiligten in den entsprechenden Ermittlungsverfahren. Zwar ist § 8a Abs. 5 TMG-E als Befugnis, nicht als Verpflichtung ausgestaltet – bereits dies beinhaltet jedoch ein aus unserer Sicht falsches Signal. In den Arbeitsgruppengesprächen bestand – auch vor dem Hintergrund der Erfahrungen aus dem Ausland, wo auf eine Speicherung und Übermittlung der IP-Adressen verzichtet wird – Einigkeit, dass angesichts der Ausrichtung der Zugangshürden auf „Zufallskonsumenten“ eine Identifizierungsmöglichkeit mit anschließenden strafrechtlichen Ermittlungen unverhältnismäßig sei. Der vorgelegte Gesetzentwurf lässt diese Einschätzung fallen, ohne dass der Grund hierfür in der lediglich kursorischen Begründung dargelegt wird. Im Übrigen ist eine Speicherung der IP-Adressen abseits der geltenden Regelungen im Telekommunikationsgesetz nie Gegenstand der Diskussion gewesen. BITKOM fordert daher, § 8a Abs. 5 TMG-E ersatzlos zu streichen.

Vorbehaltlich dieser grundsätzlichen Ablehnung weisen wir darüber hinaus darauf hin, dass bei Beibehaltung der entsprechenden Regelung für die zu erwartenden Auskunftersuchen eine Entschädigung nach Maßgabe des TK-Entschädigungs-Neuordnungsgesetzes zu erfolgen hätte.

3.6 § 8a Abs. 6 TMG-E – statistische Daten

Diensteanbieter sollten aus Sicht des BITKOM keinerlei personenbezogene Daten erheben, nutzen und übermitteln dürfen. Wir begrüßen daher, dass § 8a Abs. 6 TMG-E die Übermittlung statistischer Daten nur anonymisierter Form vorsieht.

Gleichzeitig betonen wir, dass aussagekräftiger als die abstrakte Anzahl blockierter Abrufe Erkenntnisse darüber wären, wie viele Seiten durch internationale Kooperationsverfahren auf Veranlassung des BKA außer Betrieb gesetzt werden konnten. Die Übermittlung abstrakter statistischer Abrufzahlen lässt beispielsweise keinerlei Aussagen darüber zu, in welchem Maße diese Abrufe durch automatisiert generierte Anfragen, etwa über Suchmaschinencrawler oder Bot-Netze, verursacht wurden.

3.7 § 8a Abs. 7 TMG-E – Haftung der ISP

Mit § 8a Abs. 7 TMG-E sollen die ISP ausweislich der Begründung des Gesetzentwurfs von Haftungsrisiken für den Fall befreit werden, dass durch die von ihnen ordnungsgemäß durchgeführten Maßnahmen ein Schaden entsteht. Mit der gesetzlichen Haftungsfreistellung wird auf eine zentrale Forderung der

Stellungnahme

GE Bekämpfung der Kinderpornographie in Kommunikationsnetzen

Seite 13

Internetwirtschaft eingegangen, die einen der Kerndiskussionspunkte auch in den vorangegangenen Arbeitsgruppensitzungen bildete. Insofern begrüßt BITKOM grundsätzlich den in § 8 Abs. 7 TMG-E verankerten Gedanken.

Wir sehen allerdings sowohl in der Formulierung des Gesetzeswortlautes als auch in der Begründung noch erheblichen Überarbeitungs- und Ergänzungsbedarf. Insbesondere bedarf es einer ausdrücklichen Klarstellung dahingehend, dass die Freistellung tatsächlich diejenigen Konstellationen erfasst, die in den bisher geführten Diskussionen im Zentrum standen. Es ist für uns nicht nachvollziehbar, dass der Entwurf trotz der umfangreichen Vorberatungen nicht zumindest in der Begründung ausführlich auf die in Rede stehenden konkreten Fallkonstellationen eingeht, sondern sich stattdessen faktisch auf die Wiederholung des Normwortlauts beschränkt. Im Einzelnen sehen wir zu folgenden Aspekten dringenden Überarbeitungsbedarf:

- Klargestellt werden muss ausdrücklich, dass die Haftungsfreistellung auch die Konstellation einer technisch bedingten Mitsperrung legaler Seiten erfasst, welche nicht Gegenstand der Sperrliste sind. Die generalklauselartige Formulierung des § 8a Abs. 7 TMG-E lässt dies nicht in ausreichendem Maße erkennen. Die Formulierung führt stattdessen absehbar zu der Frage, ob in Fällen solch technisch bedingter Kollateralschäden noch eine „ordnungsgemäße Umsetzung“ vorliegt. Stattdessen muss explizit klargestellt werden, dass Diensteanbieter von jeglicher Haftung frei sind, soweit die die Implementierung der Sperrliste "prozesskonform" im Sinne des § 8a Abs. 2 TMG-E sowie der Vorgaben der technischen Richtlinie ist, selbst wenn aus dieser Umsetzung eine Zugangerschwerung bzgl. Drittseiten erfolgt.
- Wir betonen in diesem Zusammenhang, dass es für technische Zugangshürden keinen „Stand der Technik“ gibt, an welchem sich messen ließe, ob eine Mitsperrung legaler Seiten durch einen „Fehler“ oder schlicht technisch bedingt erfolgt ist. Der Begriff der Ordnungsgemäßheit läuft jedoch auf eine solche Einschätzung hinaus und ist damit untauglich. In jedem Fall muss klargestellt sein, dass einfache Fahrlässigkeit keine Haftung begründet.
- Die Haftungsfreistellung muss in jedem Fall auch gelten, wenn sich der Diensteanbieter eines Netzbetreibers bedient, der für ihn die technische Implementierung der Zugangerschwerungen vornimmt. Hier könnte sich eine Regelung an § 110 Abs. 1 TKG orientieren.
- Darüber hinaus bedarf es einer ausdrücklichen Regelung, die klarstellt, dass etwaig fehlerhafte Listeneinträge nicht in den Verantwortungsbereich des ISP fallen. Wir schlagen folgende Formulierung vor:

„Den Diensteanbieter nach § 8a Abs. 2 TMG trifft keine Verantwortlichkeit für die falsche Bewertung einer Internetadresse als kinderpornographisch durch das Bundeskriminalamt oder bei anderen Fehlern aufgrund der Aufnahme einer Internetadresse in die Liste oder einer gebotenen, aber nicht erfolgten Löschung einer Internetadresse aus der Liste. Er ist

Stellungnahme

GE Bekämpfung der Kinderpornographie in Kommunikationsnetzen

Seite 14

insbesondere nicht dafür verantwortlich, dass aufgrund einer fehlerhaften Sperrliste legale Seiten gesperrt werden.“

- Schließlich lässt die Haftungsregelung offen, welche Ansprüche ein der Betreiber eines legalen Angebots geltend machen kann, dessen Seite aufgrund fehlerhafter Listenbestandteile oder technisch bedingter Mitsperrungen nicht erreichbar ist. Ein derlei betroffener Anbieter muss die Möglichkeit haben, einen Schaden, den er aufgrund dieses – jedenfalls mittelbar – staatlichen Handelns erleidet beim Bund liquidieren zu können. Hierzu bedarf es einer ausdrücklichen Regelung. Wir verweisen außerdem auf unsere weiteren Ausführungen unter Punkt 3.8.

3.8 § 8a Abs. 8 TMG-E – Nachweisverfahren

BITKOM begrüßt, dass der Gesetzentwurf eine Regelung vorsieht, die sicherstellt, dass im Falle von Streitfällen der Nachweis geführt werden kann, dass eine spezifische Seite berechtigterweise Bestandteil der Sperrliste war.

Unklar ist jedoch das Verhältnis von § 8a Abs. 8 S. 1 zu S. 2 TMG-E. Die Auskunftspflicht gegenüber den Diensteanbietern nach S. 2 muss sich auf alle Feststellungen nach S. 1 beziehen. S. 2 betrifft nach der jetzt vorgeschlagenen Formulierung jedoch nur die Übermittlung der Information „Domain XXX war in der Liste“. Er umfasst damit gerade nicht die ebenso bedeutsame Information „im fraglichen Zeitraum befand sich unter der Domain XXX kinderpornographisches Material“. Wir unterbreiten daher folgenden Formulierungsvorschlag:

„Das Bundeskriminalamt ist verpflichtet, Unterlagen vorzuhalten und im Falle gerichtlicher Auseinandersetzungen an das befassende Gericht zu übermitteln, mit denen der Nachweis geführt werden kann, dass die in der Liste aufgeführten VDN zum Zeitpunkt ihrer Bewertung durch das Bundeskriminalamt die Voraussetzungen des § 184b StGB erfüllten.

Für den Fall, dass der Diensteanbieter im Rahmen von außergerichtlichen oder gerichtlichen Auseinandersetzungen mit Dritten der fachlichen Unterstützung des Bundeskriminalamtes bedarf, leistet das BKA diese Unterstützung in der erforderlichen Form unter weitestgehender Berücksichtigung der Interessen des Diensteanbieters. Es erteilt insbesondere Diensteanbietern im Sinne dieses Gesetzes, die ein berechtigtes Interesse darlegen, auf Anfrage Auskunft darüber, ob und in welchem Zeitraum ein Telemedienangebot in der Sperrliste enthalten ist oder war und bestätigt gegenüber dem Diensteanbieter, dass das Angebot während des gesamten Zeitraumes die Voraussetzungen des § 184b StGB erfüllte.

BITKOM vermisst außerdem die Festlegung eines formalisierten Beschwerdeverfahrens, mit dem ein Seitenbetreiber oder ein sonst Betroffener die Löschung eines zu Unrecht erfolgten Eintrags aus der Sperrliste erzwingen kann. Im Hinblick auf Art. 19 Abs. 4 GG wurde in den Vorbereitungen im Rahmen der Arbeitsgruppe seitens der zuständigen Ressorts stets betont, die Schaffung

Stellungnahme

GE Bekämpfung der Kinderpornographie in Kommunikationsnetzen

Seite 15

eines solchen Verfahrens sei notwendiger Bestandteil einer Gesamtregelung. Aus Sicht des BITKOM ist gegen Einträge in der Sperrliste jedenfalls der Rechtsweg vor die Verwaltungsgerichte und damit auch der verwaltungsgerichtliche Eilrechtsschutz gegeben, da die Aufnahme in die Sperrliste ein hoheitlicher Akt mit Eingriffsqualität ist. Angesichts der immensen Auswirkungen einer Aufnahme in die Sperrliste bedarf es jedoch eines zusätzlichen formalisierten Verfahrens, innerhalb dessen eine noch schnellere Entfernung etwaiger Falscheinträge ermöglicht wird. Dies ist auch im Interesse des Bundes, der andernfalls das Haftungsrisiko für entsprechende Nichterreichbarkeitszeiten tragen muss.

3.9 § 8a Abs. 9 TMG-E – technische Richtlinie

Die zu schaffende technische Richtlinie sollte in Zusammenarbeit mit den betroffenen Providern festgelegt werden, da die dort zu regelnden technischen Einzelheiten wesentlich auf die Architektur des Diensteanbieters bzw. Netzbetreibers ausgerichtet sein müssen.

4 Artikel 2 – Änderung des Telekommunikationsgesetzes

Mit Artikel 2 wird eine begrenzte datenschutzrechtliche Ermächtigung im Rahmen des § 96 Abs. 1 TKG geschaffen. Danach gilt:

„Der Diensteanbieter darf nur folgende Verkehrsdaten und nur für die in diesem Abschnitt oder in § 8a Abs.2 oder Abs. 4 des Telemediengesetzes genannten Zwecke erheben und längstens bis zum Ende der Verbindung verwenden: “

Diese Norm enthält zum einen ein offensichtliches Redaktionsversehen, da die fraglichen Datenkategorien nicht aufgezählt sind, hier also offenbar diese Beschränkung vergessen wurde.

Vor allem aber steht die Regelung in unmittelbarem Konflikt zur viel weiterreichenden Ermächtigung nach § 8a Abs. 5 TMG-E, der faktisch für die gleichen Daten eine Ermächtigung enthält, die keinen der in § 96 Abs. 1 TKG-E aufgeführten oder angedeuteten Beschränkungen enthält.

Damit werden gerade im kritischen Bereich des Datenschutzes zwei gegenläufige Regelungen geschaffen und es bleibt unklar, welches Konzept die Bundesregierung an dieser Stelle verfolgt. Aus Sicht des BITKOM ist der in § 96 Abs. 1 TKG-E angedeutete Gedanke einer strikten Begrenzung der Datenverwendung auf das technisch Unvermeidbare richtig. Auch aus diesem Grund bedarf es der vollständigen Streichung des § 8a Abs. 5 RMG-E und insbesondere einer Streichung der Übermittlungsbefugnis gegenüber Strafverfolgungsbehörden.

5 Artikel 3 – Evaluierung

BITKOM begrüßt, dass der Gesetzentwurf eine Evaluation der vorgesehenen Mechanismen vorsieht. Es muss jedoch klargestellt werden, dass die Evaluation auch eine Untersuchung beinhalten muss, welche Auswirkungen die Sperrmaßnahmen auf die – insbesondere kommerzielle – Angebotslandschaft für kinderpornographische Inhalte im Internet tatsächlich zeitigen. Hierzu gibt es auch aus

Stellungnahme

GE Bekämpfung der Kinderpornographie in Kommunikationsnetzen

Seite 16

dem Ausland keinerlei Bewertungen, auf die verwiesen werden kann. Die bisherige, auch in der Begründung wiederholte Formulierung der Evaluation der „Anwendung des Gesetzes“ lässt andernfalls befürchten, dass sich die Evaluation auf die Benennung von versuchten Zugriffen beschränkt, die als solche isoliert keinen Aussagegehalt hat. Wegen der Neuartigkeit der Regelung sollte außerdem in jedem Fall eine frühere Evaluierung angestrebt werden, um die Auswirkungen bewerten zu können. Der BITKOM schlägt einen Zeitraum von einem Jahr vor.

— Dies gilt umso mehr, als die Bundesregierung offenbar bereits jetzt beabsichtigt, auch die sog. Jugendpornographie einzubeziehen. Abgesehen davon, dass in dieser Kategorie erhebliche Abgrenzungsschwierigkeiten drohen, ist eine solche Ausdehnung überhaupt nur dann gerechtfertigt, wenn die vorangehende Evaluation belegt, dass Zugangshürden einen relevanten Einfluss auf die Angebotslandschaft zeitigen.

6 Implementierungsfristen

— Der Gesetzentwurf muss dringend Umsetzungsfristen für die Diensteanbieter vorsehen. Die Implementierung der notwendigen technischen Maßnahmen und die Schaffung der für die Umsetzung notwendigen Prozesse und Sicherungsvorkehrungen nimmt Zeit in Anspruch. Gerade im Interesse der strengen Vertraulichkeit der Listeninhalte und einer reibungslosen technischen Abwicklung bedarf es daher einer mindestens sechsmonatigen Implementierungsfrist für die Service Provider. Dies folgt überdies auch daraus, dass zunächst die technischen Standards für Schnittstellen zwischen BKA und ISP festgelegt und im Anschluss technisch umgesetzt werden müssen. Die Vorberatungen im Rahmen der Arbeitsgruppe haben deutlich aufgezeigt, dass es sich bei den anstehenden Maßnahmen um komplexe technische Fragen handelt, die nicht innerhalb weniger Wochen lösbar sind.

7 Kostentragung

Zusätzlich geregelt werden muss die Entschädigung des Kostenaufwands der Diensteanbieter. Da es sich bei der Täterermittlung und Verfolgung von Straftaten nach § 184b StGB um eine hoheitliche Maßnahme handelt, werden die Diensteanbieter als Hilfspersonen bei der Erfüllung dieser Maßnahmen tätig. Die Situation ist vergleichbar mit der Vorratsdatenspeicherung. Wir verweisen insoweit auf die jüngst ergangenen verwaltungsgerichtlichen Entscheidungen, wonach die Abwälzung originär hoheitlicher Aufgaben ohne entsprechende Erstattung auch der Investitionskosten als verfassungswidrig zu bewerten ist.