

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

Deutscher Bundestag  
Rechtsausschuss

Platz der Republik 1  
11011 Berlin

Köln, den 7. November 2010

**Rechtsanwälte**

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

\*Fachanwalt für Urheber- und Medienrecht

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

Aktenzeichen: (10)K866

## Stellungnahme

zu dem

- a) **Gesetzentwurf der SPD – Entwurf eines Gesetzes zur Aufhebung des Gesetzes zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen (BT-Drucksache 17/776)**
- b) **Gesetzentwurf der Abgeordneten Jörn Wunderlich, Dr. Petra Sitte, Agnes Alpers, Herbert Behrens, Nicole Gohlke, Dr. Rosemarie Hein, Dr. Lukrezia Jochimsen, Jan Korte, Kathrin Senger-Schäfer, Kersten Steinke, Halina Wawzyniak und der Fraktion DIE LINKE – Entwurf eines Gesetzes zur Aufhebung von Zugangsbeschränkungen in Kommunikationsnetzen (BT-Drucksache 17/646)**
- c) **Gesetzentwurf der Abgeordneten Dr. Konstantin von Notz, Volker Beck (Köln), Birgitt Bender, Katja Dörner, Kai Gehring, Ingrid Hönlinger, Memet Kilic, Sven Kindler, Maria Klein-Schmeink, Markus Kurth, Beate Müller-Gemmeke, Lisa Paus, Brigitte Pothmer, Tabea Rößner, Christine Scheel, Dr. Harald Terpe, Wolfgang Wieland, Josef Philip Winkler und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Entwurf eines Gesetzes zur Aufhebung des Gesetzes zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen und Änderung weiterer Gesetze (BT-Drucksache 17/772)**

Kern aller Gesetzentwürfe, die Gegenstand der Anhörung sind, ist die Aufhebung des Zugangerschwerungsgesetzes (ZugErschwG), welches am 18. Juni 2009 durch den Deutschen Bundestag beschlossen wurde<sup>1</sup> und am 23. Februar 2010 in Kraft getreten ist.

Zur Problematik der mit dem ZugErschwG eingeführten Internetsperren zur Bekämpfung kinderpornographischer Internetangebote sowie zu dem Entwurf des Gesetzes zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen haben wir im vergangenen Jahr bereits in Anhörungen des Unterausschusses Neue Medien sowie des Wirtschaftsausschusses des Deutschen Bundestages Stellung genommen. Zur Vermeidung von Wiederholung verweisen wir insbesondere auf unsere schriftliche Stellungnahme zum Entwurf des ZugErschwG (vgl. <http://webarchiv.bundestag.de/cgi/show.php?fileToLoad=1678&id=1134>), in der wir detailliert zu den verfassungsrechtlichen Bedenken Stellung genommen haben.

## **A. Zusammenfassung**

Trotz der während des Gesetzgebungsverfahrens vorgenommenen Verbesserungen ist es nach unserem Dafürhalten nicht gelungen, insbesondere die vielfältigen verfassungsrechtlichen Probleme der Implementierung von Zugangerschwerungen durch Access-Provider zu lösen. Wir empfehlen daher die Aufhebung des Gesetzes.

Wie nachfolgend näher gezeigt wird, mangelt es dem Gesetz insgesamt an der verfassungsrechtlich gebotenen Normenklarheit und Normenbestimmtheit. Sowohl die Tatbestandsvoraussetzungen für die Aufnahme eines Telemedienangebots durch das BKA in die Sperrliste als auch die Access-Provider treffende Verpflichtung, den Zugang zu inkriminierten Inhalten und Verweisen zu erschweren, bleiben diffus. Den Access-Providern wird es damit als Privaten in einem grundrechtssensiblen Bereich überlassen, über die Eingriffsintensität einer Maßnahme zu entscheiden. Sie hätten darüber zu entscheiden, in welchem Umfang etwa die Sperrung rechtmäßiger Inhalte als unbeabsichtigter Nebeneffekt möglich ist.

Die Verhältnismäßigkeit der aufgrund des ZugErschwG in Frage stehenden Sperrungsmaßnahmen ist ebenfalls zweifelhaft. Das Gesetz verfolgt mit der Bekämpfung der Kinderpornographie in Kommunikationsnetzen ohne Zweifel einen legitimen Zweck. Dabei stehen zwei präventive Zielsetzungen, der Opferschutz und die Gefahrenabwehr, im Vordergrund. Es soll verhindert werden, dass eine schwerwiegende Verletzung der Intimsphäre eines abgebildeten und im Sinne des § 176 Abs. 1 StGB missbrauchten Kindes durch die weitere Verbreitung von Bildnissen im Internet vertieft wird. Zentrale Regelungsgegenstände des Gesetzes beziehen sich aber auf die am wenigsten wirksamen Maßnahmen gegen die Perpetuierung der schwerwiegenden Verletzungen des Persönlichkeitsrechts der dargestellten Kinder. Zugangerschwerungen tilgen weder kinderpornographische Angebote aus dem Internet noch eignen sich die intendierten technischen Manipulationen durch Access-Provider dazu, Straftäter aus Deutschland von solchen Angeboten wirksam abzuschneiden. Gerade mit krimineller Energie agierenden Tätern ist mit den geregelten Methoden der Zugangerschwerung

---

<sup>1</sup> Am 10. Juli 2009 hat der Bundesrat beschlossen, den Vermittlungsausschuss (Art. 77 Abs. 2 GG) nicht anzurufen, vgl. BR-Drs. 604/09.

zum World Wide Web nicht beizukommen. Wesentlich wirksamer ist daher, die Verbreitung kinderpornographischer Inhalte an der Quelle zu bekämpfen. Dazu müssten insbesondere die Betreiber der Internetserver zur Löschung der Inhalte veranlasst werden. Dieses vordringliche Ziel regelt das ZugErschwG nicht bzw. nur unzureichend. Zugangerschwerungen haben lediglich ein (technisch leicht zu umgehendes) Verschleiern von weiter verfügbaren kinderpornographischen Inhalten im deutschen Kommunikationsraum zur Folge.

Kinderpornographie im Internet sollte wirksam bekämpft werden. Hierzu bedarf es eines abgestimmten Gesamtkonzeptes: In erster Linie gehört dazu eine wirksame, international koordinierte Strafverfolgung, die durch eine ausreichende technische und personelle Ausstattung der Strafverfolgungsbehörden zu gewährleisten ist. Daneben ist das Vorgehen an der Quelle, d.h. bei den Content- und Host Providern, die unmittelbaren Zugriff auf die inkriminierten Inhalte haben, zu intensivieren, um die Darstellung missbrauchter Kinder tatsächlich aus dem Netz zu verbannen. Die Mechanismen der grenzüberschreitenden Selbstregulierung sind dabei von großer Bedeutung.

Eine Reihe unzureichender Regelungen des ZugErschwG, insbesondere verfahrensrechtlicher Art, legen einen Verstoß gegen das Übermaßverbot nahe. Es handelt sich stichpunktartig um die folgenden Aspekte:

- Unzureichende verfahrensrechtliche Absicherung der geheimen Sperrlisten;
- Auswertung des gesamten Datenverkehrs der Internetnutzer, ohne verfahrensrechtliche Absicherung;
- Keine ausreichenden Vorkehrungen zum Schutz rechtmäßiger Angebote im Rahmen des Verwaltungsverfahrens und durch effektiven gerichtlichen Rechtsschutz.

Das ZugErschwG birgt schließlich die große Gefahr, dass es zu einem „Dambruch“ hin zu einem universellen Einsatz von Internetsperren im Internet kommt. Sperrungen werden mittlerweile in vielen Rechtsgebieten, insbesondere in den Bereichen des Online-Glücksspielrechts, des Wettbewerbsrechts und der Immaterialgüterrechte, verlangt. Uns sind beispielsweise rechtliche Auseinandersetzungen bekannt, bei denen Internetsperren unter Hinweis auf das ZugErschwG im Bereich des Urheberrechts gerichtlich geltend gemacht wurden. Auch im Bereich des Glücksspielrechts sind unter Berufung auf das ZugErschwG Sperranordnungen durch eine Verwaltungsbehörde gegen Access-Provider verfügt worden, die gegenwärtig Gegenstand gerichtlicher Auseinandersetzungen sind. Die beschriebene Entwicklung stellt den verfassungsrechtlich gebotenen *ultima ratio*-Charakter von Internetsperren in Frage und führt zu dem Missverständnis, es handele sich bei Internetsperren um ein beliebiges Mittel der Rechtsdurchsetzung.

Unabhängig von materiell-rechtlichen Gesichtspunkten bestehen zudem an der Gesetzgebungskompetenz des Bundes erhebliche Zweifel. Unter dem Blickwinkel der den Ländern traditionell zustehenden Gesetzgebungskompetenz zur Gefahrenabwehr sind die Länder und nicht der Bund für die Regelungsmaterie des ZugErschwG zuständig.

## B. Unzulänglichkeit des Zugängerschwerungsgesetz im Einzelnen

1. Das ZugErschwG leidet nicht nur unter einer Reihe handwerklicher Mängel, sondern ist auch durch unbestimmte und unklare Voraussetzungen geprägt, die die Erstellung der Sperrliste durch das BKA und die Umsetzung der Liste durch die Zugangsanbieter betreffen. Zweifel bestehen auch an der Verhältnismäßigkeit des ZugErschwG aufgrund einer unzureichenden rechtsstaatlichen Absicherung der Sperrmaßnahmen. Die Aufhebung des Gesetzes ist daher aus rechtlicher Sicht zu empfehlen.
2. Dazu im Einzelnen:

### I. Unzureichende Normenbestimmtheit und -klarheit im Hinblick auf die Erstellung der Sperrliste

3. Das verfassungsrechtliche Gebot der Normenbestimmtheit und -klarheit soll sicherstellen, dass der demokratisch legitimierte Parlamentsgesetzgeber die wesentlichen Entscheidungen über Grundrechtseingriffe und deren Reichweite selbst trifft, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte die Rechtskontrolle durchführen können. Ferner sichern Klarheit und Bestimmtheit der Norm, dass der Betroffene die Rechtslage erkennen und sich auf mögliche belastende Maßnahmen einstellen kann<sup>2</sup>. Der Gesetzgeber hat Anlass, Zweck und Grenzen des Eingriffs hinreichend bereichsspezifisch, präzise und normenklar festzulegen<sup>3</sup>. Dies geschieht in § 1 Abs. 1 ZugErschwG, der die Erstellung der Sperrliste durch das BKA regelt, nur unzureichend:
4. Kinderpornographische Telemedienangebote nach § 184b StGB sowie Verweise auf solche Angebote sollen gem. § 1 Abs. 1 ZugErschwG anhand unterschiedlicher technischer Identifikationskategorien (Internetprotokoll-Adresse, vollqualifizierter Domainname, Zieladresse) in der Sperrliste nachgewiesen werden. Das Gesetz regelt dabei nicht, ob die genannten Kategorien kumulativ zur Identifizierung eines inkriminierten Inhalts in der Liste vorliegen müssen oder ob bereits ein oder zwei der Kategorien zur Erfüllung der gesetzlichen Anforderungen ausreichen. Dies ist jedoch von entscheidender Bedeutung, da die Gefahr einer versehentlichen (Mit-)Sperrung – sog. „Overblocking“ – rechtmäßiger Inhalte je nach verwendeten Kategorien unterschiedlich groß ist.

#### 1. Zugängerschwerung mittels „Zieladresse“

5. Die einzige Information, die eine relativ genaue Zugängerschwerung zu einem inkriminierten Inhalt erlauben dürfte, ist die Zieladresse. Eine Zieladresse verweist auf

<sup>2</sup> Vgl. BVerfGE 110, 33, 52 ff.; 113, 348, 375 ff.

<sup>3</sup> Vgl. BVerfGE 100, 313, 359 f., 372; 110, 33, 53; 113, 348, 375; BVerfG, Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07 – *Online-Durchsuchung*, NJW 2008, S. 822, 828 Rn. 210.

Ressourcen im Internet und wird als URL („Uniform Resource Locator“) bezeichnet. Sie könnte beispielsweise wie folgt aussehen: <http://www.server.net/user1/evil/child.mov>.

## 2. Zugangserschwerung mittels „vollqualifizierten Domainnamen“

6. Der vollqualifizierte Domainname, der zur Namensauflösung im vorstehenden Beispiel verwendet wird, hieße: [www.server.net](http://www.server.net). Allerdings wäre unter dem genannten vollqualifizierten Domainnamen nicht zwangsläufig nur die im Beispiel genannte Zieladresse mit dem inkriminierten Inhalt zu finden. Hinter dem Domainnamen könnten auch rechtmäßige Inhalte, die über andere Zieladressen aufzurufen wären, angeboten werden (z.B. <http://www.server.net/user2/nice/information.html>). Die Sperrung auf Ebene des vollqualifizierten Domainnamens [www.server.net](http://www.server.net) würde in dem vorstehenden Beispiel auch den rechtmäßigen Inhalt erfassen. Die Sperrung des vollqualifizierten Domainnamens [www.youtube.com](http://www.youtube.com) würde etwa alle Inhalte der populären Videoplattform erfassen, auch wenn der inkriminierte Inhalt nur hinter einer Zieladresse wie beispielsweise der URL <http://www.youtube.com/watch?v=UtTtUwUKa44> verfügbar ist.

## 3. Zugangserschwerung mittels „Internetprotokoll-Adresse“

7. Die Auswirkungen einer Sperrung auf der Basis einer Internetprotokoll-Adresse gingen noch wesentlich weiter. Unter einer Internetprotokoll-Adresse (z.B. 217.79.215.140) werden häufig Webangebote von unterschiedlichen Domains gehostet. Es handelt sich um das sog. *Name-Based Virtual Hosting*, das es ermöglicht, im Rahmen großer Server mit nur einer oder weniger Internetprotokoll-Adressen, die Dienste für mehrere hundert oder gar tausende von Domains beherbergen zu können. Würde die Sperrung auf der Ebene einer Internetprotokoll-Adresse vorgenommen, besteht daher immer die Gefahr, dass nicht nur der Zugang zur Domain [server.net](http://www.server.net) erschwert wird, sondern auch die Domains [server1.net](http://www.server1.net) bis [server1000.net](http://www.server1000.net) von der Sperrung mit erfasst werden, ohne dass hinter den genannten Domainnamen kinderpornographische Inhalte stehen<sup>4</sup>.

## 4. Verweissperrung

8. Verschärft wird das Problem unklarer Eingriffsvoraussetzungen noch durch den Umstand, dass das *BKA* auch solche vollqualifizierten Domainnamen, Internetprotokoll-Adressen und Zieladressen in die Sperrliste aufnehmen soll, deren Zweck es ist, auf kinderpornographische Angebote zu verweisen. Da § 1 Abs. 1 ZugErschwG und die Gesetzesbegründung offen lassen, was unter dem „Zweck [...], „auf derartige Telemedienangebote zu verweisen“ zu verstehen ist, müsste etwa auch ein rechtmäßiger Inhalt, auf den z.B. zum Zwecke der kritischen Auseinandersetzung mit der Praxis des *BKA* verwiesen wird, auf der Sperrliste geführt werden. Zudem definiert das Gesetz nicht, was technisch unter einem „Verweis“ zu verstehen ist. Soll es sich um einen anklickbaren

---

<sup>4</sup> Medienberichten zufolge konnten im Zuge der durch einen Access-Provider im Fall „youporn“ vorgenommenen „IP-Sperre“ fast 3,5 Mio. Webseiten nicht mehr abgerufen werden.

Hyperlink auf eine URL handeln oder rechtfertigt z.B. die Nennung eines Domainnamens oder einer Internetprotokoll-Adresse bereits die Aufnahme in die Sperrliste?

## II. Verhältnismäßigkeitsgrundsatz durch die Einführung des Prinzips „Löschen vor Sperren“ nicht ausreichend gewahrt

9. Der Grundsatz der Verhältnismäßigkeit verlangt, dass ein Grundrechtseingriff einem legitimen Zweck dient und als Mittel zu diesem Zweck geeignet, erforderlich und angemessen ist<sup>5</sup>. Wie nachfolgend gezeigt, erlangen Sperrungsmaßnahmen in vielerlei Hinsicht grundrechtliche Relevanz. Einschlägig sind dabei insbesondere die Berufsfreiheit und der Eigentumsschutz der Zugangsprovider, die Meinungsfreiheit der Anbieter von Inhalten und die Informationsfreiheit der Nutzer sowie das Fernmeldegeheimnis.
10. Mit § 1 Abs. 2 und 3 ZugErschwG wird angestrebt, den Grundsatz „Löschen vor Sperren“ als Ausfluss des Verhältnismäßigkeitsprinzips einzuführen. § 1 Abs. 2 S. 1 ZugErschwG regelt allgemein, dass „die Aufnahme in die Sperrliste [nur] erfolgt [...], soweit zulässige Maßnahmen, die auf die Löschung des Telemedienangebots abzielen nicht oder nicht in angemessener Zeit erfolgversprechend sind“ und lehnt sich damit an § 59 Abs. 4 RStV an. Die Sperrung soll nach diesem Ansatz *ultima ratio* bleiben und nur subsidiär gegenüber einer zielgenauen und für die breite Öffentlichkeit weniger eingriffsintensiven Löschung inkriminierter Inhalte eingesetzt werden.
11. Dieser verfassungsrechtlich gebotene Ansatz<sup>6</sup>, ist im ZugErschwG jedoch nur unzureichend umgesetzt. Dies zeigt bereits der Umstand, dass eine Internetsperrung bei Inlandssachverhalten nicht ausgeschlossen wird. Hier ist ein behördlicher Zugriff auf Content- oder Host-Provider ohne Probleme möglich, sodass das Löschen eines kinderpornographischen Inhalts immer ohne rechtsstaatlich relevanten Zeitverzug durchgesetzt werden kann. Zugangerschwerungen bei Inlandssachverhalten würden daher jedenfalls nicht dem verfassungsrechtlichen Gebot der Erforderlichkeit genügen.
12. Als Reaktion auf die Kritik in der Expertenanhörung<sup>7</sup> des Wirtschaftsausschusses wurden zudem in § 1 Abs. 2 S. 2 ZugErschwG die Verpflichtungen des in der Richtlinie über den elektronischen Geschäftsverkehr vorgeschriebenen Konsultations- und Prüfungsverfahrens zutreffend umgesetzt<sup>8</sup>. Für Drittstaaten außerhalb der *Europäischen Union* wird in § 1 Abs. 2 S. 3 ZugErschwG dann jedoch vorgesehen, dass ein Telemedienangebot sofort in die Sperrliste aufgenommen wird, wenn „nach Einschätzung des *BKA* davon auszugehen ist, dass in dem betroffenen Staat andere Maßnahmen, insbesondere Mitteilungen an die für den polizeilichen Informationsaustausch zuständigen

<sup>5</sup> Vgl. BVerfGE 109, 279, 335 ff.; 115, 320, 345; BVerfG, Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07 – *Online-Durchsuchung*, NJW 2008, S. 822, 828 Rn. 218, stRspr.

<sup>6</sup> Vgl. Stellungnahme zum Gesetzentwurf, S. 3, Ausschussdrucksache 16(9)1546; vgl. auch *Frey/Rudolph*, Haftungsregime für Host- und Access-Provider im Bereich der Telemedien, Rn. 112.

<sup>7</sup> Stellungnahme zum Gesetzentwurf, Rn. 46 ff., Ausschussdrucksache 16(9)1546.

<sup>8</sup> Vgl. zum Konsultations- und Prüfungsverfahren *Frey/Rudolph*, Der Jugendmedienschutzstaatsvertrag im Lichte des Gemeinschaftsrechts, ZUM 2008, S. 564, 576 f.



Stellen nicht oder nicht in angemessener Zeit zu einer Löschung des Telemedienangebots führen“. Die Anwendung des Grundsatzes „Löschen vor Sperren“ wird damit im Hinblick auf Sachverhalte, die Drittstaaten außerhalb der *EU* betreffen, allein der Einschätzung des *BKA* überlassen. Durch die Verwendung des Begriffs „Einschätzung“ wird der objektiv formulierte Maßstab des § 1 Abs. 2 S. 1 ZugErschwG durch die subjektive Beurteilung einer Behörde ersetzt. Anders als in der Begründung der Beschlussempfehlung des Wirtschaftsausschusses<sup>9</sup>, die insofern von einer Ermessensentscheidung spricht, widerspricht der Wortlaut des Gesetzes der Annahme, dass die Entscheidung des *BKA* justitiabel ist.

13. In der Praxis ist zudem zu befürchten, dass beispielsweise sprachliche Probleme oder eine nur schleppende Behördenkommunikation mit der für den polizeilichen Informationsaustausch zuständigen Stelle das *BKA* veranlassen wird, den Grundsatz „Löschen vor Sperren“ nicht in Erwägung zu ziehen. Die Verhältnismäßigkeit einer Maßnahme von der Beurteilung einer Behörde abhängig zu machen, erscheint nach rechtsstaatlichen Maßstäben bedenklich. Dem hätte dadurch begegnet werden können, z.B. einen Hinweis gegenüber Host-Providern auf inkriminierte Inhalte gesetzlich zu regeln. Von diesem im Gesetzgebungsverfahren diskutierten Ansatz wurde abgesehen, um die Möglichkeit unzulässiger Eingriffe in die Hoheitsrechte anderer Staaten auszuschließen<sup>10</sup>. In der Tat würde ein hoheitliches Handeln des *BKA* im ausländischen Sitzstaat des Host-Providers in dessen Souveränität eingreifen<sup>11</sup>. Allerdings sind Maßnahmen unterhalb der Schwelle befehlender Verwaltungsakte nicht grundsätzlich ausgeschlossen. Solange kein konkretes Tun, Dulden oder Unterlassen verlangt wird, wäre ein rein informierender Hinweis, dass sich auf den Servern des angeschriebenen Host-Providers kinderpornographische Inhalte befinden, daher zulässig<sup>12</sup>. Insoweit sei darauf hingewiesen, dass deutsche Gerichte in ständiger Rechtsprechung davon ausgehen, dass die einfache Bekanntgabe eines Verwaltungsaktes im Ausland in allen Staaten unabhängig von ihrer Zustimmung, völkerrechtlich zulässig ist, weil die deutsche Behörde in diesem Fall nicht selbst im Ausland tätig wird<sup>13</sup>.
14. Gleichzeitig hätte die Möglichkeit eröffnet werden können, Organisationen der freiwilligen Selbstkontrolle in die Löschbemühungen einzubeziehen. Bereits heute werden in vielen Staaten Beschwerdestellen, sog. Hotlines, (in Deutschland z.B. eco-Verband, FSM und jugendschutz.net) betrieben und international über das INHOPE-Netzwerk verbunden. Eine Reihe von Versuchen privater Organisationen hat zudem gezeigt, dass der

<sup>9</sup> Vgl. BT-Drs. 16/13411, S. 12.

<sup>10</sup> Vgl. BT-Drs. 16/13411, S. 12.

<sup>11</sup> Das Spannungsverhältnis zwischen der Souveränität ausländischer Staaten und der Verfolgung kinderpornographischer Angebote nach § 184b StGB wird im StGB im Übrigen zugunsten des sogenannten Weltrechtsprinzips gemäß § 6 Nr. 6 StGB entschieden: Die Verbreitung von Kinderpornographie ist strafrechtlich danach ohne Rücksicht auf einen ausländischen Tatort, das Recht des Tatorts und die Staatsangehörigkeit des Täters zu verfolgen.

<sup>12</sup> So ausdrücklich die Ausarbeitung des Wissenschaftlichen Dienstes des Deutschen Bundestag, WD 3 – 3000 – 211/09, S. 8, abrufbar unter <http://netzpolitik.org/wp-upload/090616-211-09-a.pdf> (Abrufdatum: 9.9.2009).

<sup>13</sup> Vgl. OVG Münster, Beschluss v. 03.12.2009 - 13 B 776/09, Rn. 104; Beschluss v. 08.12.2009 - 13 B 958/09 Rn 103; Beschluss v. 12.11.2009 - 13 B 959/09 Rn 81.

unmittelbare Kontakt zu Host-Providern – auch im Rahmen sog. Notice and Take Down-Verfahren – einen effektiven Weg zur Löschung inkrimierter Inhalte darstellt<sup>14</sup>.

### III. Expertengremium erfüllt rechtsstaatliche Anforderungen nicht

15. Als rechtsstaatliches Korrektiv für die von dem *BKA* in alleiniger Verantwortung erstellte und geheim gehaltene Sperrliste sieht § 9 ZugErschwG die Einrichtung eines Expertengremiums bei dem *Bundesdatenschutzbeauftragten* vor. Das fünfköpfige Gremium ist jederzeit zur Kontrolle, d.h. einer nachträglichen Überprüfung, der Sperrliste berechtigt. Verpflichtet ist es allerdings nur, mindestens einmal pro Quartal eine relevante Anzahl von Stichproben zu überprüfen. Inwieweit das Expertengremium einen im Lichte des Verfassungsrechts ggf. indizierten Richtervorbehalt kompensieren kann, erscheint allerdings zweifelhaft.
16. Das BVerfG hat in seiner Entscheidung zu Online-Durchsuchungen<sup>15</sup> geurteilt, dass sich bei einem Grundrechtseingriff von besonders hohem Gewicht – wie dem heimlichen Zugriff auf ein informationstechnisches System – der Spielraum des Gesetzgebers dahingehend reduziert, die Maßnahme grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Richter könnten aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Betroffenen im Einzelfall am besten und sichersten wahren<sup>16</sup>. Die Kontrolle diene insoweit der „kompensatorischen Repräsentation“ der Interessen des Betroffenen im Verwaltungsverfahren<sup>17</sup>. Nach der Rechtsprechung des BVerfG darf der Gesetzgeber eine andere Stelle nur dann mit der Kontrolle betrauen, wenn diese gleiche Gewähr für ihre Unabhängigkeit und Neutralität bietet wie ein Richter. Auch von ihr müsse eine Begründung zur Rechtmäßigkeit gegeben werden<sup>18</sup>.
17. Betrachtet man die verfahrensrechtliche Ausgestaltung des ZugErschwG, dürfte es den vorstehenden Kriterien des BVerfG nicht gerecht werden. Bei der Beurteilung der grundrechtlichen Relevanz der durch das Gesetz vorgesehenen Verpflichtung für Zugangsanbieter zur Sperrung kinderpornographischer Inhalte ist zu beachten, dass neben dem in Art. 10 GG geschützten Telekommunikationsgeheimnis der Nutzer, der Berufsfreiheit gem. Art. 12 GG bzw. der Eigentumsgarantie gem. Art. 14 GG der Zugangsanbieter und Webseitenbetreiber, die Meinungs-, Presse-, Informations-, Kunst- und Wissenschaftsfreiheit gem. Art. 5 GG von Nutzern und Webseitenbetreibern betroffen sein können; Zugangsanbietern kommt in unserer heutigen Gesellschaft nicht nur im Hinblick auf die Informationsbeschaffung der Bürger, sondern auch für ihre berufliche und wirtschaftliche Betätigung eine herausragende Rolle zu. Insbesondere Maßnahmen, die

<sup>14</sup> Vgl. dazu auch *Sieber*, Sperrungsverpflichtungen gegen Kinderpornographie im Internet, JZ 2009, S. 653, 656f.

<sup>15</sup> BVerfG, Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, S. 822, 832 f. Rn. 257 ff.

<sup>16</sup> Vgl. BVerfGE 103, 142 [151]; 107, 299 [325], BVerfG, Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, S. 822, 832 f. Rn. 259.

<sup>17</sup> Vgl. SächsVerfGH, Urteil v. 14.05.1996 - Vf.44-II-94 -, JZ 1996, S. 957, 964, BVerfG, Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, S. 822, 832 Rn. 258.

<sup>18</sup> BVerfG, Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, S. 822, 833 Rn. 260.



auch legale Informationen und Angebote treffen, führen zu schwerwiegenden Eingriffen in die Grundrechte von unbeteiligten Dritten.

18. Zwar ist das Expertengremium unabhängig und drei der fünf Mitglieder müssen über die Befähigung zum Richteramt verfügen. Jedoch ist nur eine nachträgliche noch dazu stichprobenmäßige Kontrolle der Sperrliste vorgesehen. Eine Begründungspflicht für Entscheidungen des Expertengremiums sieht das ZugErschwG nicht vor. Angesichts der grundrechtlich vielschichtigen Relevanz der durch das ZugErschwG vorgesehenen, heimlichen Zugangerschwerungen durch Zugangsanbieter dürfte die eingeschränkte Kontrolle der Sperrliste durch das Expertengremium den verfahrensrechtlichen Anforderungen des BVerfG nicht gerecht werden. Es besteht keine Möglichkeit, rechtlich bereits im Vorfeld gegen die Aufnahme in die Sperrliste vorzugehen, etwa gerichtlichen Rechtsschutz in Anspruch zu nehmen. Außerdem gibt es bei heimlich vorgenommenen Maßnahmen faktisch keinen Weg, durch das eigene Verhalten auf den Gang eines Verfahrens einzuwirken. Der Ausschluss dieser Einflusschancen verstärkt das Gewicht des Grundrechtseingriffs<sup>19</sup>.
19. Nach dem Wortlaut des § 9 ZugErschwG prüft das Expertengremium zudem nur, ob die Einträge auf der Sperrliste die Voraussetzungen des § 1 Abs. 1 ZugErschwG erfüllen. Die – gerade im Lichte des Verhältnismäßigkeitsgrundsatzes – besonders wichtige Kontrolle des Prinzips „Löschen vor Sperren“ gemäß § 1 Abs. 2 und 3 ZugErschwG gehört dagegen nicht zu der Kompetenz des Expertengremiums. Das ZugErschwG regelt auch nicht die materielle Ausstattung des Expertengremiums. Ein nur ehrenamtlich tätiges Gremium wird kaum in der Lage sein, die täglich aktualisierte Sperrliste des *BKA* effektiv zu kontrollieren und einem „Overblocking“, also dem (Mit-)Sperren rechtmäßiger Inhalte, entgegenzuwirken.
20. Darüber hinaus fehlt es an einem formalisierten Verfahren, mit dem sich zu Unrecht durch Zugangerschwerungen Betroffene gegen die Maßnahme zur Wehr setzen können. Der in § 8 Abs. 2 ZugErschwG vorgesehene Auskunftsanspruch gegen das *BKA* und der Verweis auf den Verwaltungsrechtsweg in § 12 ZugErschwG genügen nicht. Der Auskunftsanspruch gewährt bereits keine Auskunft darüber, ob sich hinter dem Listeneintrag überhaupt Kinderpornographie verbirgt und aufgrund welcher Annahmen und Unterlagen ein Angebot in die Liste aufgenommen wurde.

#### **IV. Inhalt und Reichweite der Sperrungsverpflichtung unbestimmt**

21. Gem. § 2 Abs. 1 S. 1 ZugErschwG sollen Diensteanbieter nach § 8 TMG, die den Zugang zur Nutzung von Informationen über ein Kommunikationsnetz „ermöglichen“<sup>20</sup>, „den Zugang zu Telemedienangeboten, die in der Sperrliste aufgeführt sind“, erschweren. Die im Zusammenhang mit der Listenerstellung durch das *BKA* konstatierte Unklarheit und

<sup>19</sup> Vgl. hierzu BVerfG, Urteil v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, S. 822, 830 Rn. 238.

<sup>20</sup> § 8 TKG spricht dagegen von Diensteanbietern, die den Zugang zur Nutzung fremder Informationen „vermitteln“. Diese begriffliche Divergenz scheint ein redaktionelles Versehen zu sein.

Unbestimmtheit der Tatbestandsvoraussetzungen erfasst auch § 2 Abs. 1 S. 1 ZugErschwG. Die hier verpflichteten Zugangsanbieter<sup>21</sup> müssen die in ihrer Struktur und inhaltlichen Reichweite unklare Sperrliste des BKA „unverzüglich“, spätestens jedoch sechs Stunden nach der Übermittlung umsetzen, vgl. § 2 Abs. 3 ZugErschwG. Sie haben dazu „geeignete und zumutbare technische Maßnahmen zu ergreifen [...]“. Zugangsanbieter sollen hinsichtlich der aufzubauenden Sperrinfrastrukturen frei sein, auf welche der in der Liste geführten Sperrkategorien sie zugreifen möchten<sup>22</sup>.

### **1. Zugangsanbieter entscheiden über Eingriffstiefe von Zugangserschwerungen**

22. Da die Zugangsanbieter für die Sperrung alternativ vollqualifizierte Domainnamen, Internetprotokoll-Adressen und Zieladressen von Telemedienangeboten verwenden dürfen, wird Privaten in einem grundrechtssensiblen Bereich die Entscheidung darüber überlassen, in welchem Umfang etwa die Sperrung rechtmäßiger Inhalte als unbeabsichtigter Nebeneffekt möglich ist. Fragestellungen von solcher Grundrechtsrelevanz können aber nicht Privaten zur Entscheidung übertragen werden, sondern sind nach der von dem BVerfG entwickelten Wesentlichkeitstheorie durch den Gesetzgeber zu entscheiden.

### **2. DNS-Sperre unverbindlich**

23. Die kritisierte Unbestimmtheit des § 2 Abs. 2 ZugErschwG wird auch nicht durch Satz 2 der Regelung geheilt. Danach erfolgt die „Sperrung [...] mindestens auf der Ebene der vollqualifizierten Domainnamen, deren Auflösung in die zugehörigen Internetprotokoll-Adressen unterbleibt“. In der Gesetzesbegründung heißt es dazu: „In der bloßen Verhinderung des Zugangs zu einer Seite mit kinderpornographischem Inhalt auf der DNS-Ebene liegt nach einhelliger Auffassung die geringste Eingriffstiefe. Den Diensteanbietern ist es jedoch unbenommen, sich für eine andere Sperrtechnik mit größerer Eingriffstiefe zu entscheiden.“<sup>23</sup>
24. Damit wird unterstrichen, dass die sog. DNS-Sperre nicht als verbindliche Lösung geregelt werden soll. Dadurch ist auch der Pflichtenkreis für die betroffenen Zugangsanbieter nur unzureichend konkretisiert. Das Gesetz lässt nämlich offen, ob die normierte Mindestanforderung `DNS-Sperre` vor dem Hintergrund der in der Gesetzesbegründung angeführten technologischen Entwicklung zukünftig nicht mehr als ausreichend erachtet wird, um eine „ordnungsgemäße“ (vgl. § 7 Abs. 1 ZugErschwG) Umsetzung der Sperrliste sicherzustellen. Ist die Ordnungsgemäßheit der Umsetzung schuldhaft nicht gewährleistet, verlieren Zugangsanbieter die intendierte

<sup>21</sup> Siehe zu den möglichen Ausnahmen § 2 Abs. 1 S. 2 ZugErschwG und die Beschlussempfehlung des Wirtschaftsausschusses, BT-Drs. 16/13411, S. 12.

<sup>22</sup> Vgl. BT-Drs. 16/12850, S. 7 der Gesetzesbegründung.

<sup>23</sup> BT-Drs. 16/12850, S. 7.

Haftungsprivilegierung gegenüber zivilrechtlichen Ansprüchen von Content- und Host-Providern, die von einer Sperrung betroffen sind.

25. Aufgrund der erheblichen Eingriffsintensität der geforderten Sperrungsmaßnahmen liegt es darüber hinaus nahe, dass Nutzer und Webseitenbetreiber zunächst die unmittelbar agierenden Zugangsanbieter in Anspruch nehmen. Die Sperrung einer rechtmäßigen Webseite mit der Umleitung der anfragenden Nutzer auf einen Server mit Stoppmeldung führt bei dem Betreiber der rechtmäßigen Webseite regelmäßig zu erheblichen materiellen und immateriellen Schäden (z.B. Imageverlust). Es ist daher absehbar, dass Zugangsanbieter (im Rahmen des einstweiligen Rechtsschutzes) auf Unterlassung in Anspruch genommen werden<sup>24</sup>.

## V. Keine Nutzung von Verkehrs- und Nutzungsdaten für Zwecke der Strafverfolgung

26. Verkehrs- und Nutzungsdaten, die aufgrund der Zugangserschwerung bei der Umleitung auf die Stopp-Meldung anfallen, dürfen nicht für Zwecke der Strafverfolgung verwendet werden, § 5 ZugErschwG. Aufgrund der unspezifischen Sperrkriterien sowie wegen der Möglichkeit eines ungewollten Anklickens kinderpornographischer Angebote<sup>25</sup> wären die anfallenden personenbezogenen Daten für die Strafverfolgung wenig aussagekräftig gewesen.
27. Die Begründung der Beschlussempfehlung des Wirtschaftsausschusses hebt insofern hervor, dass durch § 5 ZugErschwG „die sog. „Echtzeitüberwachung“ von Verkehrsdaten am Stopp-Server nach dem TKG gem. § 100g StPO unzulässig“ ist<sup>26</sup>. Der Hinweis auf den Stopp-Server ist in diesem Zusammenhang missverständlich, da dort nur die Stoppmeldung gehostet wird. Eine „Echtzeitüberwachung“ nach TKG wäre dagegen eher an der von den Zugangsanbietern aufzubauenden Sperrinfrastruktur in Betracht gekommen, da an dieser Stelle in einen laufenden Telekommunikationsvorgang eingegriffen und die Kommunikation zu einem anderen Ziel, dem Server mit Stoppmeldung, umgeleitet wird. Nach dem Wortlaut scheint dies der mit der Norm intendierte Zweck zu sein, da gerade auf die „Umleitung“ Bezug genommen wird. Die Umleitung erfolgt z.B. über den Einsatz eines Routers oder die Manipulation eines DNS-Servers während der laufenden Kommunikation. Bei den dort anfallenden Daten handelt es sich um Verkehrsdaten im Sinne des TKG, deren Nutzung nach dem Wortlaut der Norm für Zwecke der Strafverfolgung ausdrücklich gesperrt ist.
28. Zu unterscheiden von dem Eingriff in die Telekommunikation durch die „Umleitung“ sind die Daten, die daran anschließend nach Abschluss der Telekommunikation am Stopp-Server, auf dem die Stoppmeldung gehostet ist, anfallen<sup>27</sup>. Dabei handelt es sich um

<sup>24</sup> Siehe zu einem ersten Verfügungsverfahren wegen der zwischen BKA und einigen Zugangsanbietern geschlossenen Sperrungsverträgen, OLG Frankfurt, Beschluss v. 11.08.2009 - Az. 3 W 45/09.

<sup>25</sup> Vgl. dazu *Sieber*, JZ 2009, S. 653, 655.

<sup>26</sup> Vgl. BT-Drs. 16/13411.

<sup>27</sup> Vgl. zur Abgrenzung von Verkehrs- und Nutzungsdaten die Stellungnahme des Bundesrats zum TMG, BT-Drs. 16/3078, S. 18.

Nutzungsdaten in Bezug auf ein Telemedium, deren Schutz § 15 TMG regelt. Die Anordnung zur Herausgabe der am Stopp-Server im Zusammenhang mit der dort gehosteten Stoppmeldung angefallenen Nutzungsdaten durch eine Ermittlungsbehörde gegenüber einem Zugangsanbieter nach § 15 Abs. 5 S. 4 i.V.m. § 14 Abs. 2 TMG ist daher nach dem Wortlaut der Norm nicht ausgeschlossen. Auf der Grundlage solcher Nutzungsdaten könnte beispielsweise eine ermittelnde Staatsanwaltschaft von dem Zugangsanbieter das Zusammenführen der Nutzungsdaten mit den bei ihm geführten Bestandsdaten seiner Kunden verlangen und diese Informationen zur Strafverfolgung einsetzen.

## VI. „Dambruch“ – Sperrungsforderungen gegen Access-Provider im Hinblick auf diverse Rechtsverletzungen Dritter im Internet

29. Mit § 7 Abs. 2 ZugErschwG soll ausgeschlossen werden, dass die nach dem Gesetz von Zugangsanbietern aufzubauende Sperrinfrastruktur auch dazu verwendet werden muss, zivilrechtlich begründete Sperrungsforderungen umzusetzen. Damit sollte der befürchtete „Dambruch“ verhindert werden, dass Gerichte zukünftig etwa wettbewerbsrechtlich oder urheberrechtlich begründete Ansprüche wegen einer neuen Beurteilung der technischen Möglichkeit und der Zumutbarkeit einer Sperrung bejahen<sup>28</sup>. Dieser Ansatz ist zu begrüßen, wenngleich nach Aufhebung oder Auslaufen des Gesetzes am 31.12.2012 auch diese gesetzliche Beschränkung zur Nutzung der Sperrinfrastruktur enden würde. Außerdem ist nicht ausgeschlossen, dass Sperrforderungen unabhängig von der einzusetzenden Sperrinfrastruktur geltend gemacht werden. Gerade im Bereich des Urheber- und Wettbewerbsrechts sind solche Forderungen bereits mehrfach gerichtlich vorgetragen worden<sup>29</sup>.
30. Nicht ausgeschlossen durch das ZugErschwG ist dagegen die Nutzung der Sperrinfrastruktur für weitere öffentlich-rechtlich begründete Sperrungsforderungen. Es ist zu erwarten, dass sowohl *de lege lata* als auch *de lege ferenda* die Stimmen, die eine Sperrung z.B. rechtsradikaler sowie allgemein jugendgefährdender Inhalte fordern, lauter werden. Schließlich sind Sperrungsverfügungen gegen deutsche Access-Provider zur Erschwerung des Zugangs zu ausländischen Glücksspielangeboten im Internet unter Hinweis auf die Sperrinfrastruktur für Kinderpornographie bereits ergangen und sind gegenwärtig Gegenstand rechtlicher Auseinandersetzungen.
31. Das ZugErschwG leitet damit eine verfassungsrechtlich bedenkliche Entwicklung ein. Eine Internetsperre wird nicht mehr einer auf den äußersten Einzelfall beschränkten, besonders rechtsstaatlich abgesicherten *ultima ratio*-Entscheidung vorbehalten. Im Gegenteil wird der Aufbau einer universell einsetzbaren Sperrinfrastruktur gesetzlich angeordnet, die die Umsetzung geheim gehaltener Sperrlisten ermöglichen soll. Dabei stellt sich die für die Rechtsdurchsetzung im Internet zentrale Frage, ob die Bundesrepublik Deutschland mit ihrer besonderen Verfassungstradition durch den listenbasierten Einsatz

<sup>28</sup> Vgl. dazu Frey, Netzsperrn: Werden Access-Provider die neuen Gatekeeper des Rechts?, MMR 2009, S. 221, 222; Stellungnahme zum Gesetzentwurf, Rn. 81 ff., Ausschussdrucksache 16(9)1546.

<sup>29</sup> Vgl. z.B. LG Hamburg, Urteil v. 12.3.2010 - Az. 308 O 640/08, MMR 2010, S. 488ff.

von Internetsperren eine Renationalisierung des digitalen Kommunikationsraumes versuchen sollte herbeizuführen. Wir sind der Ansicht, dass dies keine Option sein kann, da dazu das Surfverhalten der gesamten Bevölkerung kontrolliert werden müsste und die tatsächlichen Rechtsverletzungen, die bekämpft werden sollen, nicht beseitigt, sondern lediglich verschleiert werden können.

32. Access-Provider würden zudem dazu verpflichtet, die Inhaltsneutralität ihrer Infrastrukturdienste aufzugeben. Bisher gelten die Internetzugangsdienste von Access-Providern als gesellschaftlich besonders erwünschte, inhaltsneutrale Infrastrukturleistungen, die grundsätzlich blind gegenüber einer rechtlich qualitativen Bewertung der durchgeleiteten Daten und Kommunikationsvorgänge sind. Dieser Befund, der bereits aus dem Geschäftsmodell der Access-Provider folgt, wird derzeit gesetzlich besonders abgesichert. Die Internetkommunikation ist durch das Fernmeldegeheimnis gem. Art. 10 GG geschützt. Eine entsprechende Verpflichtung trifft Access-Provider einfachgesetzlich gem. § 88 TKG. Der Schutzbereich beider Bestimmungen umfasst dabei sowohl die Inhalte als auch die näheren Umstände der Internetkommunikation.

## VII. Auswertung des gesamten Datenverkehrs der Internetnutzer

33. Eine Zugangserschwerung zu kinderpornographischen Angeboten im Internet auf der Basis der von dem *BKA* erstellten Sperrlisten setzt voraus, dass der gesamte Datenverkehr der Internetnutzer ausgewertet wird. Die Identifikation des Ansurfens kinderpornographischer Internetinhalte kann nur erfolgen, wenn ein Selektionsmechanismus auf der Basis der adressierten Sperrkategorien vorgenommen wird. Internetsperren führen so zu Eingriffen in das Telekommunikationsgeheimnis.
34. Internetsperren erfordern in Hinblick auf alle angesprochenen Sperrkategorien eine zielgerichtete Überwachung der Telekommunikation der Internetnutzer, da die Identifikation von Internetangeboten anhand der eingegebenen URL, des Domainnamens oder der IP-Adresse unabdingbare Voraussetzung für die Zugangsbeschränkung ist. Dies hat mittlerweile das LG Hamburg in Bezug auf alle diskutierten Filter- und Sperrmaßnahmen – insbesondere auch bezogen auf die Einrichtung einer DNS-Sperre – ausdrücklich festgestellt<sup>30</sup>:

„Die in Frage stehenden Filter- und Sperrmaßnahmen setzen voraus, dass der Access-Provider sich Kenntnisse von Umständen der Telekommunikation zu Nutzen macht. Das greift in das Fernmeldegeheimnis ein, was nur bei einer gesetzlichen Beschränkung i.S.d. Art. 10 Abs. 2 Satz 1 GG erlaubt ist, die den Anforderungen des Art. 19 GG genügt.“

35. Auch das ZugErschwG – wie sich anhand von § 11 ZugErschwG<sup>31</sup> zeigt – unterstellt, dass alle Sperrkategorien – auch Manipulationen an DNS-Servern – Eingriffe in das

<sup>30</sup> LG Hamburg, aaO., MMR 2010, 488 [490].

<sup>31</sup> vgl. LG Hamburg, MMR 2010, 488 [490]; *Rehart*, MMR-Aktuell 2010, 303415; *Frey/Rudolph*, CR 2009, S. 644, 646.

Telekommunikationsgeheimnis darstellen. Das Grundrecht des Fernmeldegeheimnisses dient der freien Entfaltung der Persönlichkeit durch einen Kommunikationsaustausch mit Hilfe des Fernmeldeverkehrs<sup>32</sup>. Bei der Nutzung von Telekommunikationseinrichtungen ist die Kommunikation besonderen Gefährdungen der Kenntnisnahme durch Dritte ausgesetzt und unterliegt deshalb besonderem Schutz<sup>33</sup>. Das Fernmeldegeheimnis soll gegen eine vom Betroffenen ungewollte Informationserhebung schützen und die Privatheit auf Distanz gewährleisten<sup>34</sup>. Nach der Rechtsprechung des BVerfG<sup>35</sup> soll mit der grundrechtlichen Verbürgung der Unverletzlichkeit des Fernmeldegeheimnisses zudem vermieden werden, dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen. Das Fernmeldegeheimnis dient damit indirekt dem Schutz der ebenfalls betroffenen Informationsfreiheit.

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

## VIII. Gesetzgebungskompetenz

37. Nicht nur im Hinblick auf Bestimmtheit und Verhältnismäßigkeit des ZugErschwG bestehen erhebliche verfassungsrechtliche Zweifel. Bereits die Gesetzgebungskompetenz des Bundes dürfte nicht vorliegen. Es ist vielmehr davon auszugehen, dass unter dem Blickwinkel der den Ländern traditionell zustehenden Gesetzgebungskompetenz zur Gefahrenabwehr<sup>36</sup>, letzteren die Gesetzgebungskompetenz für die Zugangserschwerungen zu kinderpornographischen Telemedien durch Zugangsanbieter zukommt.

<sup>32</sup> BVerfGE 106, 28, 35f.

<sup>33</sup> BVerfGE 106, 28, 36; vgl. bereits BVerfGE 67, 157, 171f.; 85, 386, 396.

<sup>34</sup> BVerfGE 115, 166, 182; Beschluss vom 22.08.2006, 2 BvR 1345/03 – IMSI-Catcher, NJW 2007, 351, 353 – Rn. 51.

<sup>35</sup> Vgl. BVerfGE 107, 299, 313.

<sup>36</sup> Vgl. z.B. BVerfG, Urteil v. 27.07.2005, Az. 1 BvR 668/04, Rn. 94.



## 1. Gesetzgebungskompetenz für Zugangserschwerung

38. In der Gesetzesbegründung wird die Pflicht der Zugangsanbieter, den Zugang zu kinderpornographischen Telemedienangeboten durch technische Vorkehrungen zu erschweren, auf den Kompetenztitel des Art. 74 Abs. 1 Nr. 11 GG der konkurrierenden Gesetzgebung gestützt<sup>37</sup>. Dass dieser Kompetenztitel einschlägig ist, darf bezweifelt werden. Schon nach dem Titel des Gesetzes besteht der Gesetzeszweck darin, Gefahren durch Kinderpornographie in Kommunikationsnetzen, die dem Einzelnen und der Allgemeinheit drohen, zu bekämpfen. Durch die Zugangserschwerung sollen Zugangsanbieter ihren Beitrag dazu leisten, die Verbreitung und Besitzverschaffung von Kinderpornographie zu erschweren. Der Regelungsgegenstand und Normzweck des ZugErschwG besteht daher in der Abwehr von Gefahren im Zusammenhang mit der Kinderpornographie, nicht hingegen in wirtschaftslenkenden Maßnahmen im Sinne des Art. 74 Abs. 1 Nr. 11 GG.
39. Eine konkurrierende Gesetzgebungskompetenz des Bundes für die Zugangserschwerungen unter dem Gesichtspunkt eines ordnungsrechtlichen Annexes des Rechts der Wirtschaft erscheint ebenfalls nur schwer zu begründen. Nach der Rechtsprechung des BVerfG kann die Ordnungsgewalt als Annex des Sachgebiets erscheinen, auf dem sie tätig wird; die Zuständigkeit zur Gesetzgebung in einem Sachbereich umfasst dann auch die Regelung der Ordnungsgewalt (Polizeigewalt) in diesem Sachbereich<sup>38</sup>. Nur solche Regelungen, bei denen die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung den alleinigen und unmittelbaren Gesetzeszweck bildet, können einem selbständigen Sachbereich zugerechnet werden, der als Polizeirecht im engeren Sinne bezeichnet wird und in die Zuständigkeit der Landesgesetzgebung fällt<sup>39</sup>. Im Kern geht es beim ZugErschwG nicht darum, das wirtschaftliche Betätigungsfeld der Zugangsanbieter in ordnungsrechtlicher Hinsicht zu beschränken, sondern Gefahren, die durch kinderpornographische Inhalte in Kommunikationsnetzen entstehen, zu begegnen. Dass Zugangsanbieter durch die Verpflichtung zur Zugangserschwerung auch in ihrer wirtschaftlichen Freiheit betroffen sind, stellt nur einen logischen Reflex der bezweckten Gefahrenabwehr dar. Es handelt sich daher um eine ordnungsrechtliche Sonderregelung der Regelungsmaterie Kinderpornographie, nicht hingegen um eine wirtschaftsrechtliche Regelung von kinderpornographischen Telemedien.

## 2. Gesetzgebungskompetenz für Sperrliste des BKA

40. Die Befugnis des BKA, die Sperrliste zu erstellen und den Zugangsanbietern zur Verfügung zu stellen, wird in der Gesetzesbegründung auf Art. 73 Abs. 1 Nr. 10 GG gestützt. Eine Erläuterung hierzu fehlt<sup>40</sup>.

---

<sup>37</sup> Vgl. BT-Drs.16/12850, S. 5 f.

<sup>38</sup> Vgl. BVerfGE 8, 143, 149.

<sup>39</sup> BVerfGE 8, 143, 150.

<sup>40</sup> Vgl. BT-Drs.16/12850, S. 6 f.

41. Durch § 1 Abs. 1 ZugErschwG wird aber nicht die Zusammenarbeit des Bundes und der Länder im Rahmen der Kriminalpolizei, des Verfassungsschutzes oder auswärtiger Belange geregelt, wie es der Kompetenztitel des Art. 73 Abs. 1 Nr. 10 GG vorsieht. Darüber hinaus dürfte dem Bund auch keine Kompetenz im Hinblick auf die in Art. 73 Abs. 1 Nr. 10 GG genannte internationale Verbrechensbekämpfung zukommen. Darunter ist nicht die Bekämpfung internationaler Verbrechen, sondern die internationale Bekämpfung von Verbrechen, also etwa die Zusammenarbeit deutscher mit ausländischen Stellen in kriminalpolizeilichen Fragen, zu verstehen<sup>41</sup>. Im Übrigen fällt das Polizeirecht als Gefahrenabwehrrecht in die Zuständigkeit der Länder<sup>42</sup>. Dem Zweck einer internationalen Bekämpfung von Kinderpornographie dient die im ZugErschwG vorgesehene Regelung nicht. Das Gesetz sieht nicht vor, dass Kinderpornographie im Rahmen internationaler Zusammenarbeit verfolgt werden soll. Vielmehr wird dem BKA die Befugnis zugewiesen, kinderpornographische Telemedienangebote in einer Sperrliste zu führen sowie die Befugnis, diese Sperrliste Zugangsanbietern für Zugangsschwerungsmaßnahmen zur Verfügung zu stellen. Hierbei handelt es sich um die nationale Abwehr von Gefahren durch Kinderpornographie, nicht hingegen um deren internationale Bekämpfung. Dies gilt umso mehr als das ZugErschwG auch die Zugangsschwerung zu nationalen kinderpornographischen Inhalten durch Zugangsanbieter vorsieht. Im Ergebnis erscheint eine Gesetzgebungskompetenz des Bundes gem. Art. 73 Abs. 1 Nr. 10 GG im Hinblick auf die Sperrliste daher problematisch.

### C. Erlass zur Nicht-Umsetzung des ZugErschwG

42. CDU/CSU und FDP habe sich im Koalitionsvertrag vom 26. Oktober 2009 darauf geeinigt, dass es notwendig ist, kinderpornographische Angebote schnellstmöglich zu löschen statt diese zu sperren. Es sollen daher zunächst für ein Jahr kinderpornographische Inhalte auf der Grundlage des ZugErschwG nicht gesperrt werden. Nach einem Jahr soll dann Erfolg und Wirksamkeit von Löschbestrebungen evaluiert werden. Vor Abschluss der Neubewertung sollen weder nach dem ZugErschwG noch auf Grundlage der zwischen den Providern und BKA abgeschlossenen Verträge über Internetsperren Sperrlisten des BKA geführt und Providern übermittelt werden<sup>43</sup>.
43. In Ausführung des Koalitionsvertrages ordnete das Bundesinnenministerium nach dem bekannt gewordenen Erlass vom 17. Februar 2010 gegenüber dem BKA an, keine Sperrlisten zu erstellen, sodass Zugangssperren unterbleiben. Durch das BKA sollen nur Benachrichtigungen an ausländische Staaten mit der nachdrücklichen Bitte um Löschung der als kinderpornographisch identifizierten Inhalte erfolgen. Der Erlass wird damit begründet, dass die Bundesregierung beabsichtige, eine Gesetzesinitiative zur Löschung kinderpornographischer Inhalte im Internet zu schaffen. Bis zum Inkrafttreten dieser Neuregelung wolle sich die Bundesregierung auf der Grundlage des ZugErschwG

<sup>41</sup> BVerfG, Urteil v. 14.07.1999, 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Rn. 199; vgl. *Degenhardt* in Sachs (Hrsg.), Grundgesetz, 5. Auflage 2009, Art. 73, Rdnr. 53, der hierzu die Verhütung und Verfolgung von Straftaten in internationaler Zusammenarbeit, durch Amtshilfe, wechselseitige Informationen u.ä. zählt.

<sup>42</sup> BVerfG, Urteil v. 14.07.1999, 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Rn. 199.

<sup>43</sup> Vgl. S. 79 Koalitionsvertrag.

ausschließlich und intensiv für die Löschung derartiger Seiten einsetzen, Zugangssperren aber nicht vornehmen. Im Ergebnis ordnet die Exekutive, namentlich das Verfassungsorgan Bundesregierung, mit dem Erlass an, dass ein wirksam zustande gekommenes, verkündetes und in Kraft getretenes Gesetz der Legislative durch die Verwaltung nicht vollzogen wird.

44. Ein solches Vorgehen der Bundesregierung dürfte verfassungswidrig sein. Denn durch die Anordnung an das BKA, keine kinderpornographischen Inhalte in die Sperrliste aufzunehmen, um Zugangssperren zu verhindern, setzt sich die Exekutive über das von der Legislative verabschiedete ZugErschwG, mithin über ein demokratisch legitimiertes Gesetz, hinweg. Zwar bestimmt der Bundeskanzler die Richtlinien der Politik und trägt dafür die Verantwortung, und innerhalb dieser Richtlinien leitet der Bundesminister seinen Geschäftsbetrieb selbstständig und unter eigener Verantwortung (Art. 65 Abs. 1 GG). Als Spitze der Exekutive unterliegt die Bundesregierung jedoch der Gesetzesbindung gem. Art. 20 Abs. 3 GG. Es steht ihr daher nicht zu, wesentliche Regelungen eines in Kraft getretenen Gesetzes durch Erlass faktisch einer Anwendbarkeit durch die Verwaltung zu entziehen. Selbst wenn die Bundesregierung das ZugErschwG für verfassungswidrig halten sollte – wofür die vorstehend aufgeführten Gründe sprechen – darf die Bundesregierung als Staatsorgan das ZugErschwG nicht ohne weiteres außer Anwendung lassen<sup>44</sup>. Dass die Bundesregierung das ZugErschwG als verfassungswidrig ansieht, bringt sie jedoch nicht einmal zum Ausdruck. Die Verpflichtungswirkung des Gesetzes begründet vielmehr die Pflicht, die Anordnung des Gesetzes zu befolgen und sonst in ihrer Wirksamkeit zu respektieren<sup>45</sup>. Will die Bundesregierung an dem von den Gesetzgebungsorganen beschlossenen ZugErschwG nicht festhalten, muss sie über das ihr zustehende Gesetzesinitiativrecht ein von den Gesetzgebungsorganen zu beschließendes Gesetz herbeiführen, das das ZugErschwG aufhebt. Die Anordnung der Nichtanwendung hingegen verstößt gegen den Grundsatz der Gesetzesbindung der Exekutive.

#### **D. Bedarf es neben der Aufhebung des ZugErschwG einer gesetzlichen Neuregelung zur Bekämpfung der Kinderpornographie in Internet?**

45. Aufgrund der vorstehend dargestellten, vielfältigen verfassungsrechtlichen Probleme des ZugErschwG empfehlen wir seine Aufhebung.
46. Gleichzeitig halten wir es für wichtig, eine Gesamtstrategie zu entwickeln, mit der kinderpornographische Inhalte in Kommunikationsnetzen zielgerichtet und wirksam bekämpft werden. In erster Linie gehört dazu eine wirksame Strafverfolgung, die durch eine ausreichende technische und personelle Ausstattung der Strafverfolgungsbehörden sowie eine effektive internationale Kooperation zu gewährleisten ist. Daneben ist das Vorgehen an der Quelle, d.h. bei den Content- und Host-Providern, die unmittelbaren Zugriff auf die inkriminierten Inhalte haben, zu intensivieren, um die Darstellung missbrauchter Kinder tatsächlich aus dem Netz zu verbannen.

<sup>44</sup> Vgl. zu dieser Problematik *Sachs* in *Sachs*, a.a.O., Art. 20 Rn. 96.

<sup>45</sup> *Sachs*, a.a.O., Art. 20 Rn. 110.

47. Wir sind der Ansicht, dass es für die Entwicklung einer Gesamtstrategie keines spezifischen Löschgesetzes bedarf, auch wenn eine entsprechende gesetzliche Festlegung, die der Dynamik der digitalen Welt Rechnung tragen müsste, unseres Erachtens nicht schadet. Dabei sollte zunächst die Einbindung der Organisationen der freiwilligen Selbstkontrolle, die bereits innerhalb des INHOPE-Netzwerkes international organisiert sind, intensiviert und die unmittelbare Ansprache von Host-Providern verstärkt werden. Unsere Erfahrungen in der Kommunikation mit ausländischen Host-Providern, z.B. in der Ukraine oder in Indien, im Zusammenhang mit anders gearteten Rechtsverletzungen Dritter zeigen, dass diese durchaus gewillt sind, schnell und unkonventionell auf substantiiert vorgetragene Beschwerden zu reagieren.
48. Die bessere technische und personelle Ausstattung der Strafverfolgungsbehörden hilft nach unserem Dafürhalten nicht nur dabei, den Verfolgungsdruck auf inländische Straftäter zu erhöhen, sondern erleichtert die Kooperation im Rahmen internationaler Strafverfolgungsanstrengungen. Dabei ist auch zu berücksichtigen, dass gem. § 6 Nr. 6 StGB im Hinblick auf Kinderpornographie das sog. Weltprinzip gilt: Strafrechtlich ist Kinderpornographie daher ohne Rücksicht auf einen ausländischen Tatort, das Recht des Tatorts und die Staatsangehörigkeit des Täters zu verfolgen. Soweit dabei ein Spannungsverhältnis zur Souveränität anderer Staaten entsteht, ist dieses am besten durch eine intensive Kooperation mit den Strafverfolgungsbehörden im Ausland aufzulösen.
49. Gesetzliche Ermächtigungen für Maßnahmen gegen kinderpornographische Inhalte bestehen zudem bereits heute auf der Grundlage des Jugendmedienschutzstaatsvertrags in Verbindung mit dem Rundfunkstaatsvertrag (vgl. § 20 Abs 4 JMStV i.V.m. § 59 Abs. 2 bis 4 RStV). Nach den Bestimmungen des JMStV sind kinderpornographische Angebote im Internet (vgl. insb. § 4 Abs. 1 Nr. 10 JMStV) verboten und sind von den zuständigen Landesmedienanstalten, die durch die Kommission für Jugendmedienschutz (KJM) als funktional zuständigem Organ handeln, zu unterbinden. Kinderpornographische Angebote sind zudem auf Antrag der KJM (§ 18 Abs. 6 JuSchG) von der Bundesprüfstelle für jugendgefährdende Medien (BPjM) zu indizieren und in die Listenteile mit jugendgefährdenden Medien aufzunehmen, die ein absolutes Verbreitungsverbot betreffen (Teile B und D). Wird ein Internetangebot (Telemedium) mit jugendgefährdenden Inhalten aus dem Ausland in die Liste aufgenommen, sollen diese Informationen zum Zwecke der Einbeziehung in nutzerautonome Filterprogramme zur Verfügung gestellt werden (vgl. § 24 Abs. 5 JuSchG). Durch den Rückgriff auf die Ermächtigungsgrundlagen des JMStV i.V.m. dem RStV werden die Länderkompetenzen zur Gefahrenabwehr gewahrt. Dabei ist allerdings zu berücksichtigen, dass die bestehenden Ermächtigungsgrundlagen keine Eingriffe in das Telekommunikationsgeheimnis und damit keine Internetsperren zulassen.

Dr. Dieter Frey, LL.M.  
(Rechtsanwalt)

Dr. Matthias Rudolph  
(Rechtsanwalt)