Deutscher Bundestag ■ Wissenschaftliche Dienste

Sperrverfügung gegen Internet-Provider

- Ausarbeitung /aktualisierte Fassung-

Günter Pursch und Verena Bär

 WD 10 - 3000 - 010/2009

Wissenschaftliche Dienste des Deutschen Bundestages

Verfasser/in: Günter Pursch und Verena Bär

Sperrverfügung gegen Internet-Provider

Ausarbeitung WD 10 - 3000 - 010/2009

Abschluss der Arbeit: 27.01.2009

Fachbereich WD 10: Kultur, Medien und Sport

Telefon: +49 (30) 227-33735

Inhaltsverzeichnis **Seite**

W

1. Einleitung

Sperrverfügungen gegen Internetdienstanbieter im Zusammenhang mit kriminellen Handlungen geraten verstärkt in die öffentliche Diskussion. Seit dem Ende der 90er-Jahre wird das Internet von immer mehr Menschen genutzt. Es sollte nach Meinung vieler Nutzer weitgehend frei von staatlichen Regulierungen bleiben. Doch als mit dem und durch das Internet Geld verdient wird, wurde deutlich, dass klare gesetzliche Rahmen gegeben werden mussten. Ohne rechtliche Grundlagen hätte wohl kein Unternehmen in Geschäftsmodelle investiert, die im Zusammenhang mit dem Internet stehen. Formen der Kriminalität wurden sichtbar, die zwar schon zuvor bestanden, deren Begehung jedoch durch das Internet begünstigt wurden. Die Dynamik und die Geschwindigkeit, mit der sich das Internet entwickelt, bereiten der Rechtsprechung und dem Gesetzgeber erhebliche Schwierigkeiten. Es stellten sich viele neue Fragen. Das lag unter anderem daran, dass nun viele Privatpersonen als Dienstanbieter auftraten und eigene Webseiten erstellen konnten. Dezentralität und Internationalität des Internets machten es zudem schwer, einen konkreten Verantwortlichen zu benennen. Es fehlte an einer zentralen Instanz und es gab keine Stelle, von der die Anwendung bestimmter Regeln verlangt werden konnte.

Vor allem fehlte es an Referenzurteilen oder einer herrschenden Meinung in der Rechtsliteratur. So kam es dazu, dass in den Anfangsjahren des Internetrechts zahlreiche Fragen erst vom Bundesgerichtshof geklärt werden mussten. Dies kostete jedoch viel Zeit, in der sich das Internet wiederum stark weiterentwickelt hatte. Deswegen zeichnet sich das Internetrecht durch mehrere Besonderheiten aus. Es ist kein homogenes Rechtsgebiet, sondern setzt sich aus einer Vielzahl unterschiedlicher Rechtsgebiete zusammen. Beispielhaft sind hier zu nennen:

Auf dem Rechtsgebiet Zivilrecht hat das Internet Auswirkungen auf die Bereiche Vertragsschluss, Handel und E-Commerce, Gewährleistung und allgemeine Haftungsgrundsätze; gesetzliche Regelungen finden sich hierzu im BGB.

Beim Urheberrecht sind Auswirkungen beim Schutz des Urhebers, Verwertungsrecht, Rechteübertragung, Tauschbörsen und bei Privatkopien zu sehen; gesetzliche Regelungen finden sich hierzu im UrhG und im KunstUrhG.

Das Wettbewerbsrecht wirkt sich auf wettbewerbsrechtliche Abmahnungen und auf Werbung aus; gesetzliche Regelungen finden sich im UWG.

Im Strafrecht wirken sich Cracken, die Veröffentlichung pornographischer Inhalte sowie Volksverhetzung aus; gesetzliche Regelungen finden sich im StGB.
Für den Jugendschutz finden sich entsprechende Regelungen im Jugendschutzmedien-Staatsvertrag (JMStV).

Beim Namen- und Markenrecht wirken sich Domainregistrierung, Domainnutzung sowie auch Domainhandel und dem Domainnamensrecht aus; gesetzliche Regelungen finden sich im MarkenG und im BGB.

Beim Datenschutzrecht sind Auswirkungen auf E-Commerce, Rechte von Datenschutzbeauftragten sowie Informations- und Belehrungspflichten zu sehen; gesetzliche Regelungen finden sich im TMG und im BDSG sowie im Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (ZKDSG).

Beim Internationalen Privatrecht (IPR) wirken sich grenzüberschreitende Verträge und/oder Rechtsverletzungen aus; gesetzliche Regelungen finden sich im EGBGB und CISG, dem UN-Kaufrecht.

Das Internationale Zivilverfahrensrecht wirkt sich auf die Zuständigkeit der Gerichte aus; gesetzliche Regelungen finden sich hierzu in der EuGVVO und in diversen Abkommen.

Beim Telekommunikationsrecht sind Auswirkungen auf Impressum sowie Abrechnung von Telediensten zu sehen; gesetzliche Regelungen: TMG, TKG, IuKDG.

Beim Rundfunkrecht sind Auswirkungen im Zusammenhang mit der Erhebung von Rundfunk- und Fernsehgebühren für entsprechende Empfangsgeräte (Computer, Handy, PDA) festzustellen; gesetzliche Regelungen: RGebStV und RFinStV.

2. Begriffsbestimmungen

Zunächst gilt es, internetspezifische Fachtermina zu erläutern:

2.1. Internetdienstanbieter

Eine Antwort auf die Frage, wer als Internetdienstanbieter[1] zu qualifizieren ist, gibt § 2 S.1 Nr. 1 TMG.[2] Nach der in dieser Vorschrift enthaltenen Legaldefinition ist „Diensteanbieter“ jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt. Zur genaueren Einordnung der Dienstanbieter ist mithin nach wie vor je nach der technischen Funktion des Providers zwischen drei Anbietertypen zu unterscheiden. Die drei unterschiedlichen Providertypen, auf die einzugehen sein wird, sind folglich weiterhin entsprechend ihrer jeweiligen Funktion als Content-Provider, Host-Provider und Access-Provider zu bezeichnen.

2.2. Content-Provider

Der Content-Provider[3] zeichnet sich dadurch aus, dass es sich bei ihm um einen Anbieter handelt, dessen Dienste im Angebot eigener Informationen zur Nutzung durch Dritte bestehen. Maßgeblich ist insofern das Bereithalten von eigenen Tele- oder Mediendiensten, die beispielsweise in Onlineausgaben von Zeitungen und Zeitschriften bestehen kann. Zu den bekanntesten Content-Providern in Deutschland zählen u. a.. T-Online und AOL.

---

1 auch Internet Service Provider – kurz ISP - genannt. Im deutschsprachigen Raum auch oft nur Provider, weniger häufig auch nur Internetanbieter oder Internetprovider genannt.

2 Telemediengesetz (TMG) ersetzt das Teledienstegesetz (TDG), das Teledienstedatenschutzgesetz (TDDSG) sowie weitestgehend auch den Mediendienste-Staatsvertrag (MdStV) seit 1. März 2007.

3 dt. Inhaltsanbieter; auch ICP genannt.

2.3. Host-Provider

Im Unterschied zum Content-Provider bietet der Host-Provider nicht eigene, sondern vielmehr fremde Informationen an.[4] Dieser stellt gewissermaßen nur das Tor zum Internet dar. Die bereitgehaltenen Informationen müssen jedoch ihrerseits nicht von professionellen, insbesondere Content-Providern stammen, vielmehr können diese fremden Informationen auch von Internet-Nutzern zur Verfügung gestellt werden.

2.4. Access-Provider

Der Access-Provider beschränkt sein Angebot nur auf die Vermittlung des Zugangs zur Nutzung fremder Teldienste durch das Bereitstellen eines Einwahlknotens.[5]

2.5. Endnutzer

Endnutzer sind diejenigen Personen, die einem im Internet angebotenen Service zur Kommunikation nutzen bzw. die angebotenen Informationen und Daten abrufen.

2.6. Router

Router[6] sind Verbindungssysteme zur Verknüpfung von Computersystemen, welche die unterschiedlichen Protokollschichten miteinander verbinden.[7] Durch das Routergerät werden Datenpakete auf höheren Protokollschichten übermittelt, wobei die grundlegenden Routingfunktionen im Internetprotokoll auf der Netzwerkschicht implementiert sind. Anhand der Adressierungsstruktur können die Router dann erkennen, welcher Transportweg und welche Datenpaketgröße optimal sind.

---

[4] Vgl. § 3 S. 1 Nr. 1, 2. Alt. TDG.

[5] Boßmanns, S. 32.

[6] von englisch to route – einen bestimmten Weg nehmen lassen.

2.7. World Wide Web

Das World Wide Web (www) ist ein verteiltes Softwaresystem, das auf dem Internet läuft.[8] Mithilfe dieser Informationsdarstellung können Texte und grafische Elemente kombiniert, unmittelbar dargestellt und einzelne HTML-Dokumente durch Hyperlinks miteinander verknüpft werden. Der Benutzer kann so mehrere unabhängig voneinander arbeitende Computer als kohärentes System wahrnehmen.[9] Hierdurch verschmelzen mehrere Einzeldokumente zu einem weltweiten Informationspool. 1,3 Milliarden Menschen – ein Fünftel der Weltbevölkerung – nutzen das www.[10] Allein in Deutschland werden zurzeit mehr als 42 Millionen Internetnutzer gezählt.

2.8. Proxy

Proxy ist ein Dienst im Internet, der zwischen einen Einzelrechner und das Gesamtnetz geschaltet ist. Proxy dient auch als Bezeichnung für den Rechner, auf dem die entsprechende Software läuft. Fordert eine Person an ihrem Rechner ein Dokument aus dem Internet an, dann sucht der Proxy-Server in seinen lokalen Daten, ob er eine gespeicherte Version dieses Dokuments besitzt, und leitet diese Kopie an den Nachfrager weiter; andernfalls gibt er die Anfrage weiter. Auf diese Weise können Proxy-Server, die gewöhnlich geografisch nah zum Kunden liegen und daher kurze Übertragungszeiten ermöglichen, Zugriffszeiten reduzieren. Außer einer eventuellen Beschleunigung kann ein Proxy-Server auch die Sicherheit erhöhen, indem er verhindert, dass Viren und ähnliche Schadprogramme an den Nutzer beziehungsweise das lokale Netz, das an ihn angeschlossen ist, weitergegeben werden.[11]

Da die strukturellen Eigenheiten des Internets aus seiner historischen Entwicklung resultieren, soll diese zur Ermöglichung eines besseren Verständnisses skizziert werden.

---

[7] Gets, S. 34.

[8] Tanenbaum, S. 16.

[9] Tanenbaum, S. 16.

[10] Belwe, Katharina; Internet und Kommunikation, in „Aus Politik und Zeitgeschehen (APuZ) – Beilage zur Wochenzeitung „Das Parlament“; Neue Medien (39/2008): S. 1.

11 www.brockhaus-enzyklopaedie.de

3. Historische Entwicklung des Internets

Der Ursprung des Internets liegt in den USA. Auslöser für seine Entwicklung war der Kalte Krieg[12]. Als eine von mehreren Reaktionen auf den Sputnikschock gründete das amerikanische Verteidigungsministerium 1958 die Forschungseinrichtung Advanced Research Projects Agency (ARPA), die innovative Technologien entwickeln sollte, um den vermeintlichen Rückstand der USA gegenüber der Sowjetunion aufzuholen. Insbesondere suchte man nach Methoden zur Datenübertragung in einem Netzwerk, die die Kommunikation auch noch bei einem Teilausfall des Netzes gewährleisten sollten.[13] 1969 gab das Verteidigungsministerium der USA ein Forschungsvorhaben bei der ARPA in Auftrag, das unter dem Namen ARPAnet bekannt wurde und heute als Vorläufer des Internets angesehen wird. Dieses Projekt hatte den Sinn, zwischen den unterschiedlichen über das Land verteilten, Computern Daten auszutauschen und von einem Rechner aus mit allen Programmen der anderen Rechner arbeiten zu können[14]. Die für das Militär wichtigste Eigenschaft sollte jedoch darin bestehen, trotz partieller Zerstörung des Kommunikationsnetzwerkes in einem Nuklearkrieg Datentransfer aufrecht zu erhalten.

Aus diesem Grund wurden spezielle Computer, sogenannte IMPs[15] entwickelt. Sie brachten die Nachrichten der unterschiedlichen Rechner in ein maschinenunabhängiges Format und übermittelten sie dann an entfernte IMPs. Durch die Verbindung eines IMP mit mehreren oder allen anderen IMPs wurde erreicht, dass bei eventuell stattfindender Zerstörung von Übertragungsstrecken eine Datenkommunikation weiterhin über die anderen IMPs gewährleistet war.

1971 waren 23 Computer des Militärs miteinander vernetzt. Heute sind es vergleichsweise weit mehr als 30 Millionen Rechner. 1983 hatte das ARPAnet eine solche Ausdehnung erfahren, dass es in einen zivilen, forschungsorientierten und einen militärischen Teil aufgeteilt wurde. Im zivilen Teil des Netzes nahm die Zahl der angeschlossenen Rechner im Verlauf der 1980er-Jahre extrem zu, woran die amerikanische National

---

[12] Boßmanns, S. 10 ff.

[13] Vgl. http://www.brockhaus-enzyklopaedie.de/be21_article.php#3.

[14] Hoeren, S. 9, 10.

[15] Interface Message Processor.

Science Foundation (NFS)[16] großen Anteil hatte. Um allen amerikanischen Universitäten den Zugang zum Netz zu gewährleisten, gründete sie das NSFnet und schuf ein leistungsstarkes System von Hauptleitungen,[17] das die bedeutendsten wissenschaftlichen Rechenzentren miteinander verband. Kleinere Rechnernetze oder auch einzelne Rechner konnten sich mit einem dieser Rechenzentren verbinden und über dieses andere Netze erreichen. Auf diese Weise entstand ein „Netz der Netze", für das sich in dieser Zeit der Begriff Internet durchsetzte.[18] 1985 wurde das ARPAnet in seiner Trägerfunktion durch das NSFnet abgelöst und 1990 abgeschaltet.

In den 1980er-Jahren wurden weltweit immer mehr kleinere Netze von Universitäten und Forschungseinrichtungen an das Internet angeschlossen. Trotz seiner starken Ausweitung blieb das Internet bis Anfang der 1990er-Jahre fast ausschließlich ein Werkzeug, mit dem Wissenschaftler Daten und Forschungsergebnisse austauschten.

Zum heutigen Zeitpunkt versetzt das Internet den Menschen in die Lage Informationen zu fast jedem erdenklichen Thema zu bekommen. Es ist zum Netz der unbegrenzten Möglichkeiten mutiert. Aber auch hier gibt es keinen straffreien Raum und so wird es auch für die Begehung von Straftaten missbraucht, etwa zur Verbreitung von kinderpornographischen Inhalten, illegalem Glücksspiel, Werbung für terroristische Ziele, Betrug oder es werden Urheberrechtsverletzungen begangen. Das Simon-Wiesenthal-Center schätzt die Zahl rechtsextremer und volksverhetzender Webseiten auf mehr als 2000. Der Verfassungsschutz spricht von 1300 rechtsextremen Webseiten allein in deutscher Sprache.[19]

Oft stößt jedoch hierzulande das nationale Recht bei der Verfolgung und Verhinderung derartiger Straftaten an ihre Grenzen und die Frage der Rechtsdurchsetzung bereitet besondere Schwierigkeiten, da die Kompetenzen der nationalen Sicherheitsbehörden grundsätzlich an den Staatsgrenzen enden.

---

[16] eine Stiftung mit dem Auftrag, die Wissenschaft zu fördern.

[17] das sog. Backbone-Netz.

[18] Vgl. http://www.brockhaus-enzyklopaedie.de/be21_article.php.

[19] Engel, Christoph; Die Internet-Service-Provider als Geiseln deutscher Ordnungsbehörden, in MMR 4/2003, S. 16.

Wenn also nicht direkt gegen die auf ausländischen Servern gespeicherte Inhalte vorgegangen werden kann, so sollen wenigstens inländische Internetprovider einen Zugriff der Bürger durch technische Sperren im Internet[20] unterbinden. Die Frage, ob und auf welche Art und Weise ein Vorgehen gegen strafrechtlich relevante Inhalten gegenüber inländischen Internetanbietern überhaupt möglich ist, stellt nicht zuletzt auch ein technisches Problem dar. Daher wird die Architektur des Internets und die physikalische Struktur im Folgenden näher dargestellt.

4. Das Internet und seine Funktionsweise

Beim Internet[21] handelt es sich um ein Kommunikationsnetz in Form eines weltweiten Verbundes von Computernetzwerken und Rechnern durch das Daten ausgetauscht werden.[22] Es ermöglicht die Nutzung der Internetdienste wie E-Mail[23], Dateiübertragung, www, Telefonie, Radio und Fernsehen.

Im Prinzip kann dabei jeder Rechner weltweit mit jedem anderen Rechner verbunden werden. Der Datenaustausch zwischen den einzelnen Internet-Rechnern erfolgt über die technisch normierten Internetprotokolle. Umgangssprachlich wird „Internet“ häufig synonym zum www verwendet, da dieses einer der meistgenutzten Internetdienste ist, und im wesentlichen zum Wachstum und der Popularität des Mediums beigetragen hat.

4.1. Physikalische Struktur

Die physikalische Struktur des Internets wird aus einem komplexen Gemisch von hierarchisch strukturierten Datenleitungen gebildet. Transkontinentalkabel und Satelliten verbinden dabei die Hauptübertragungswege[24] der Kontinente, an die sich die Daten-

---

[20] Vgl. Punkt 7.3.

[21] wörtlich etwa Zwischennetz oder Verbundnetz; von englisch: interconnected Networks: untereinander verbundene Netzwerke.

[22] Eichhorn, S.19.

[23] Electronic Mail.

[24] sog. Backbones.

netze von nationalen Providern[25] ankoppeln. Über die Einwahlknoten der nationalen Provider sind wiederum kleinere, regional operierende Internetdienstleister und Endkunden (Firmen, Universitäten, auch Einzelpersonen) an das Internet angeschlossen. Zur Kommunikation auf dieser physikalischen Struktur dienen standardisierte Protokolle. Grundlegend sind die Protokolle IP[26], das die zu übertragenden Daten in Pakete aufteilt, adressiert und schließlich wieder zusammenführt, sowie TCP[27], das den Datentransport überwacht und Übertragungsfehler korrigiert. Beide werden zu TCP/IP zusammengefasst. Um TCP/IP möglich zu machen, besitzt jeder Computer im Internet eine eindeutige IP-Adresse.[28] Diese besteht aus vier Zahlen zwischen Null und 255[29], Der IP-Adresse kann ein eindeutiger, für die Nutzer gut merkbarer Name[30] zugeordnet sein. Die Umwandlung erfolgt vom Nutzer unbemerkt durch den Domain-Name-Service (DNS).[31] Die einzelnen Datenpakete werden unabhängig voneinander verschickt, eventuell sogar auf verschiedenen Wegen, wenn etwa eine Leitung während der Datenübertragung ausfällt oder überlastet ist. Die Verbindung zwischen den verschiedenen Teilnetzen leisten so genannte Router beziehungsweise Gateways. Diese müssen die Umsetzung zwischen dem TCP/IP-Protokoll und Protokollen in anderen Netzen durchführen.

5. Juristische Zuständigkeiten in Deutschland

In Deutschland ist die Staatsanwaltschaft zuständig, soweit mit der Verbreitung der Inhalte Straftaten verwirklicht werden. Mit In-Kraft-Treten des Jugendmedienschutz-Staatsvertrages[32] am 1. April 2003 sind seitdem bei unzulässigen und entwicklungsbeeinträchtigenden Angeboten gem. § 20 Abs. 4 JMStV, § 59 Abs. IV RStV (Rundfunkstaatsvertrag) die Kommission für Jugendmedienschutz (KJM) für Sperrverfügungen im

---

[25] auch Internet Service Provider – kurz ISP - genannt.

[26] Internet Protocol.

[27] Transmission Control Protocol.

[28] Vgl. Kapitel 8.

[29] http://www.brockhaus-enzyklopaedie.de/be21_article.php?document_id=0x06be04bd@be.

[30] Host-Name genannt; Bespiel: www.brockhaus.de.

[31] Domain Name System, vgl. Punkt 8.

[32] Vor dem 01.04.2003 waren im Bereich des Jugendschutzes von Internet-Diensten die Vorschriften des Gesetzes über die Verbreitung jugendgefährdender Schriften und Medieninhalte (GjSM), des Teledienstegesetzes (TDG) und des Mediendienste-Staatsvertrages (MDStV) zu beachten.

Internet funktionell zuständig[33], die von der zuständigen Landesmedienanstalt gem. § 14 II JMStV gebildet wird.
Die KJM prüft und bewertet demzufolge, ob Verstöße gegen Jugendschutzbestimmungen vorliegen und entscheidet auch, welche Sanktion dieser Verstoß zur Folge hat. Vollzogen werden diese Maßnahmen von den Landesmedienanstalten[34]. Gemäß § 6 der Geschäfts- und Verfahrensordnung der KJM (GVO-KJM) werden Einzelfallprüfungen und mögliche Verstöße gegen Jugendmedienschutz-Staatsvertrag in Prüfausschüssen der KJM behandelt. Die Entscheidungen der KJM-Prüfausschüsse werden im Umlaufverfahren oder in Präsenzprüfungen vorbereitet, indem die Prüfgruppen Entscheidungsempfehlungen abgeben. Die jeweiligen Maßnahmen stehen in Abhängigkeit zur Schwere der Strafe. Grundsätzlich sind für Verstöße gegen Jugendschutzbestimmungen in den Telemedien folgende Sanktionen möglich:

- Beanstandung gegen Content-Provider in Form eines Beanstandungsbescheides
- Untersagung gegen Content-Provider
- Sperrung gegen Content-Provider
- Aufforderung zur Sperrung gegen Host-Provider oder Access-Provider
- Sperrung gegen Host-Provider oder Access-Provider
- Ordnungswidrigkeitenverfahren (§ 24 JMStV): Einleitung eines Bußgeldverfahrens; bei Straftatbestand Abgabe an Staatsanwaltschaft.

Die örtliche Zuständigkeit ergibt sich aus § 20 Abs. 6 Satz 1 JMStV, wonach der Sitz des Anbieters von Telemedien maßgeblich ist. Ergibt sich danach keine Zuständigkeit, soll gemäß der Auffangregelung in Satz 2 der Ort entscheidend sein, an dem der Anlass für die Amtshandlung hervortritt. Nach der Begründung zum JMStV ist dabei „subsidiär der Ort entscheidend, an dem die Maßnahmen der Landesmedienanstalt wirksam werden sollen, also beispielsweise dort, wo eine Sperrungsverfügung auf einem Server umgesetzt werden kann.[35]

[33] der KJM angeschlossen worden ist auch die Internetseite www.jugendschutz.net.
[34] Vgl. http://www.kjm-online.de.
[35] Pfitzmann, Köpsell, Kriegelstein; S. 9.

6. Rechtliche Probleme der Sperrung

Die technischen Probleme der Umsetzung einer Sperrung werfen auch eine Reihe rechtlicher Fragen auf, die untersucht werden sollen. In die Frage nach einem Vorgehen gegen die Provider spielen vor allem verfassungsrechtliche Aspekte hinein, insbesondere ist die Vereinbarkeit mit dem Grundgesetz zu prüfen, die Zumutbarkeit der Sperrung und deren Verhältnismäßigkeit.

6.1. Rechtsgrundlage

Die Entwicklungen des Informations- und Multimediarechts spiegeln sich auch in der Veränderung der Rechtsgrundlage, welche die Bezirksregierung Düsseldorf 2002[36] für ihre Sperrverfügung herangezogen hat. Seit diesem Zeitpunkt hat es eine Reihe von Änderungen im Informations- und Multimediarecht gegeben.
Daher ist es vonnöten diese zunächst zu skizzieren, um dann die derzeitige Rechtsgrundlage für Zugangssperrungen gegen rechtswidrige Medieninhalte im Internet zu benennen.
Ursprünglich wurde als Rechtsgrundlage für Sperrverfügungen § 18 Mediendienstestaatsvertrag (MDStV) herangezogen[37]. Im April 2003 trat dann der Jugendmedienschutz-Staatsvertrag (JMStV) in Kraft, mit dem der erste Teil des Kompetenzkompromisses „Datenschutz gegen Jugendschutz“ zwischen Bund und Ländern umgesetzt wurde und es verschob sich erneut die Rechtsgrundlage. Bislang galt § 20 IV JMStV i.V.m. §§ 22 MDStV zur Sperrung des Zugriffs bei Verstößen gegen §§ 4, 5 JMStV. Außerhalb des JMStV-Anwendungsbereichs galt § 22 III MDStV bei Mediendiensten und bei den Teldiensten wurde auf die polizeiliche Generalklausel zurückgegriffen. Durch die jüngste Entwicklung des Telemedienrechts hat sich die Rechtsgrundlage erneut geändert. Mit dem zweiten Schritt des Kompetenzkompromisses zwischen Bund und Ländern traten zum 01.März 2007 der Mediendienstestaatsvertrag und das Tele-

---

[36] Bezirksregierung Düsseldorf erließ im Februar 2002 gegen zahlreiche Unternehmen, die den Zugang zum Internet vermitteln, eine Verfügung zur Sperrung des Zugangs zu bestimmten Internetangeboten von rechtsextremistischen Inhalten.

[37] Stadler, Thomas; Sperrungsverfügung gegen Access-Provider, in MMR (6/2002): S. 343 ff.

dienstgesetz (TDG) außer Kraft. Diese wurden durch das Telemediengesetz und den 9. Rundfunkänderungsstaatsvertrag abgelöst.[38]
Wirtschaftlich orientierte Regelungen und Vorschriften zum Datenschutz sind im Telemediengesetz (TMG) des Bundes zu finden. Inhaltliche Anforderungen wurden durch einen neuen Abschnitt VI in den Staatsvertrag für Rundfunk und Telemedien der Länder (RStV) einbezogen. Dies betrifft auch die Regelung zur Aufsicht. Die neue Rechtsgrundlage für Sperrungen illegaler Seiten ist daher jetzt in (§20 IV JMStV i.V.m.) § 59 III und IV RStV zu sehen.

7. Verfassungsrechtliche Aspekte

7.1. Verhältnismäßigkeit

Eine Sperrungsverfügung, welche z. B. die Sperrung von IP-Adressen vorsieht, ist nur dann rechtmäßig, wenn sie auch verhältnismäßig ist. Das ist dann der Fall, wenn der mit ihr erstrebte Zweck in angemessenem Verhältnis zur Beeinträchtigung des Adressaten - also des von der Verfügung betroffenen Zugangsproviders steht. Die Verhältnismäßigkeit ist dann gegeben, wenn die Maßnahme zur Erreichung des Zieles geeignet, erforderlich und angemessen ist.

7.2. Geeignetheit

Geeignet im Sinne des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes ist eine Sperrungsanordnung, wenn eine Sperrung überhaupt technisch möglich ist und darüber hinaus auch noch das Ziel erreichen kann, die Verbreitung bestimmter Inhalte zu verhindern oder zumindest einzuschränken.[39]

7.3. Technische Möglichkeiten der Sperrung

---

[38] Spindler, Gerald; Das neue Telemediengesetz, Computer und Recht (CR), 2007, S. 239 ff.

[39] Zimmermann, Andreas; Polizeiliche Gefahrenabwehr und das Internet, in: NJW (1999): S. 3145-3152; BVerfGE 67, 157, 173.

Eine Verpflichtung zum Ausschließen einer bestimmten Webseite oder eines bestimmten verlinkten Inhalts besteht nur, wenn dies technisch möglich ist, eine Sperre also nach dem aktuellen Stand der Entwicklung überhaupt durchführbar ist. Seit den Düsseldorfer Sperrungsverfügungen aus dem Jahr 2002, in dem die Bezirksregierung Düsseldorf noch als Aufsichtsbehörde nach dem Mediendienstestaatsvertrag (MDStV)[40] für das Land Nordrhein-Westfalen fungierte und Sperrungsverfügungen gegen eine Reihe von Access-Provider erlassen hat, sind drei verschiedene Sperrungsmöglichkeiten bekannt. Die Manipulation der DNS-Einträge am DNS-Server des Access-Providers, die Benutzung eines Proxy-Servers oder die Sperrung der IP-Adresse am Router. Diese Verfahren sollen nachfolgend analysiert werden:

8. DNS Sperren

Das DNS ist einer der wichtigsten Dienste im Internet. Hauptsächlich wird das DNS zur Umsetzung von Domainnamen in IP-Adressen benutzt.[41] Das DNS ist also dem Telefonbuch vergleichbar, das die Namen der Teilnehmer in ihre Telefonnummer auflöst. Das DNS bietet somit eine Vereinfachung, weil Menschen sich Namen weitaus besser merken können als Zahlenkolonnen. So kann man sich einen Domainnamen wie www.bundestag.de in der Regel leichter merken als die dazugehörende IP-Adresse 217.79.215.140. Die Umwandlung ist dabei für den Benutzer nicht sichtbar, das heißt, die IP-Adresse wird nicht angezeigt. Rechner, auf denen dieser Dienst läuft, werden als DNS-Server oder Name-Server bezeichnet. Ein solcher Server nutzt eine dezentral im Internet verteilte Datenbank; jede einzelne Datenbank ist für einen bestimmten Namensbestandteil zuständig. Der Host-Name wird immer von rechts nach links aufgelöst: Die erste Datenbankauskunft betrifft die Top-Level-Domain (z. B. „de“ für Deutschland) und wird an den zuständigen DNS-Server (in diesem Falle bei der DENIC e. G.[42]) gesandt. Dieser DNS-Server gibt die IP-Adresse des Servers zurück, der für die Second-Level-Domain (im obigen Beispiel „bundestag“) zuständig ist. Dieser Prozess wird so lange fortgeführt, bis der ganz links stehende Namensbestandteil „www“ erreicht ist.

---

[40] Der MDStV ist seit dem 01.03.2007 außer Kraft.

41 vgl. auch S. 11

[42] Die DENIC eG ist die zentrale Registrierungsstelle für alle Domains unterhalb der Top Level Domain .de.

8.1. Sperrungsverfahren

Das Sperrungsverfahren funktioniert insofern, als das derjenige, der im DNS-Server den gesuchten Eintrag nachschlägt, eine fehlerhafte numerische Adresse erhält und somit die Verbindung misslingt[43] und die Endnutzer dann die Meldung „Host not found“ erhalten.

8.2. Verwendung eines Proxy-Servers

Eine weitere Möglichkeit um den Abruf von Informationen mit strafbarem Inhalt zu verhindern, besteht darin, Proxy-Server zur Filterung der abgerufenen Informationen einzusetzen[44]. Um eine zu naive Interpretation des Begriffs eines Proxy-Servers zu verhindern, muß zunächst die Technologie näher erläutert werden:
Weitverkehrsnetze werden stark belastet, wenn viele Nutzer immer und immer wieder dieselben Informationen von entfernten Rechnern abrufen. Daher wurden auch im Bereich des http-Protokolls Proxy-Server zur Zwischenspeicherung vor Ort entwickelt. Ein Proxy-Server ist ein Dienst im Internet, der zwischen einen Einzelrechner und das Gesamtnetz geschaltet ist[45]. Wenn ein Browser über die technische Möglichkeit verfügt, so kann der Benutzer über das Browser-Optionsmenü einstellen, daß statt des für die URL[46] zuständigen Servers zunächst der vom Nutzer eingetragene Proxy befragt wird, ob dieser die gewünschte Information in seinem Cache[47] vorrätig hat. Falls dies der Fall ist, wird diese Information sofort vom Proxy an den Browser ausgeliefert, und eine Entlastung der Datenleitungen ist die gewünschte Folge. Ist die Information nicht vorhanden, wird der Proxy versuchen, diese zu beschaffen, um sie zum einen dem anfragenden Browser zur Verfügung zu stellen und um sie zum anderen für weitere Anfragen eine gewisse Zeit vorrätig zu halten. Insofern sieht es auf den ersten Blick so aus, als könne am Proxy mittels Negativlisten eine Filterung implementiert werden, die Informationen mit strafbarem Inhalt nicht an Client-Rechner weiterleitet. Derzeitige Proxy-Server sind allerdings in Hinblick auf eine effiziente Bearbeitung von Negativlisten nicht optimiert.

---

[43] Pfitzmann, Köpsell, Kriegelstein; S. 52.

[44] ebenda, S. 54.

[45] Brauner, Raible-Besten,Weigert; S. 179.

46 Uniform Resource Locator (URL) bezeichnet die genormte Adressierung für Multimedia-Dokumente im WWW oder auf dem eigenen Rechner.

8.3. IP-Sperren

Die dritte Möglichkeit besteht darin, dass eine Sperrung des Zugangs zur IP-Adresse stattfindet. Im Falle einer IP-Sperre werden demzufolge Anfragen, die sich auf eine der IP-Adressen beziehen, unter der ein strafrechtlich relevantes Angebot zur Verfügung gestellt wird, am vom Access-Provider betriebenen Router aussortiert und nicht weitergeleitet.[48] Somit ist dieses Angebot für den Kunden des Providers nicht mehr erreichbar.

8.4. Umgehungsmaßnahmen

Festzuhalten bleibt, dass es zwar technisch möglich ist, die drei genannten Sperrverfahren einzurichten. Allerdings existiert eine Reihe von Umgehungsmaßnahmen für jede der genannten Sperrmaßnahmen. Bezüglich der IP-Sperre ist zu berücksichtigen, dass sie weit mehr sperrt als beabsichtigt und keine zielgenaue Blockade der inkriminierten Inhalte bewirkt. Dieser Fall tritt zum Bespiel dann ein, wenn sich mehrere Webseiten dieselbe IP-Adresse teilen. Aufgrund der Adressknappheit ist es also üblich, dass für eine öffentliche IP-Adresse mehrere Hosts gehalten werden. Dies hat zur Folge, dass eine Sperrung, die an der IP-Adresse ansetzt, äußerst ungenau ist und dazu führen kann, dass mehrere andere legale Webseiten automatisch mitgesperrt werden.[49] Das VG Düsseldorf[50] stellte dazu fest: „Dass mit der Sperrung einer IP-Adresse wegen Rechtswidrigkeit eines Angebots auch andere legale Angebote mit betroffen sein können, macht diese Methode nicht im Rechtssinne zur Gefahrenabwehr ungeeignet. Im Übrigen wird es wegen der hohen Verbreitung getrennter Domains für unterschiedliche Angebote durchaus die Möglichkeit geben, nicht rechtswidrige Angebote auf nicht gesperrte IP-Adressen auszulagern, ohne dass sich die von den Kunden eingesetzten Adressen ändern.“

---

[47] Cache ist eine besondere Art von Speicher, die den Zugriff auf Daten beschleunigen soll.

[48] Schneider, Gerhard; Die Wirksamkeit der Sperrung von Internet-Zugriffen, in MMR (1999): S. 571, 572.

[49] Volkmann; S. 243.

[50] VG Düsseldorf, Urt. vom 10.05.2005, 27 K 5968/02.

So waren vor einigen Jahren zahlreiche Webseiten der Schweizer Hochschulen in der Schweiz nicht erreichbar, weil der Rechner, auf welchem die Webseiten betrieben wurden, eine IP-Adresse zugeteilt bekam, unter welcher vorher ein rechtsextremes Internet-Portal erreichbar war.[51] Da die Sperrlisten nicht aktuell waren, wurden auch die Hochschulseiten gesperrt, obwohl sie mit den Rechtsextremen weder den Domainnamen, noch den Inhalt teilten. Zudem kann die IP-Blockade relativ einfach umgangen werden. Der Betreiber des Zielrechners muss lediglich die IP-Adresse ändern und die Maßnahme läuft ins Leere.

Auch im Falle der DNS-Sperre gibt es Umgehungsmöglichkeiten. In einer Anleitung zur Konfiguration der DNS-Einstellungen[52] beschreibt der Chaos Computer Club (CCC), wie jeder Nutzer diese Einstellungen am eigenen PC ohne große Mühen ändern und auf einen alternativen DNS-Server ausweichen kann. Außerdem bleibt der Eingriff am DNS-Server auch dann wirkungslos, wenn der Nutzer anstatt der URL direkt die IP-Adresse in den Browser einträgt.

Um eine DNS-Sperre zu umgehen, könnte der Nutzer auch einen Proxy verwenden, um über diesen auf die gesperrte Seite zu gelangen[53]. Eine weitere einfache Möglichkeit, die Sperrung zu umgehen, ist ferner den Anbieter zu wechseln. Notfalls kann zu einem ausländischen Provider gewechselt werden. Der sperrende Router des lokalen Providers wird dann nicht mehr verwendet und die Sperrung ist demzufolge wirkungslos.[54] Auch eine Sperrung von Inhalten durch Einsatz von Proxy-Servern lässt sich ähnlich leicht wie die zuvor beschriebene DNS-Sperre umgehen. Dabei kommen die gleichen Umgehungsmaßnahmen zum Einsatz. Der Content-Provider kann seine Inhalte einfach unter einer anderen Adresse anbieten, so dass eine adressbasierte Filterung im Zwangs-Proxy mißlingt.[55] Zudem wäre ein weiterer Nachteil, dass der Einsatz von Proxy-Servern einen erheblichen technischen Aufwand erfordern würde[56].

---

[51] Vgl. www.heise.de/tp/r4/artikel/12/12249/1.html.

[52] Vgl. http://www.ccc.de/censorship/dns-howto/index.xml.

[53] Pfitzmann, Köpsell, Kriegelstein, S. 53.

[54] Köhntopp, Seeger; Sperrungen im Internet, in DuD (1997): S. 629.

[55] Pfitzmann, Köpsell, Kriegelstein, S. 53.

[56] Stadler,Thomas; Sperrungsverfügung gegen Access-Provider, in: MMR, 6/2002, S. 346.

Bei der Betrachtung der Umgehbarkeit einer Maßnahme ist außerdem der Kenntnisstand der jeweiligen Zielgruppe nicht außer Acht zu lassen. Es kann und muss davon ausgegangen werden, daß dieser Kenntnisstand in jüngeren Bevölkerungsschichten wesentlich höher ist als bei denen, die eine Umgehbarkeit auf ihre Schwierigkeit hin zu beurteilen versuchen.

Daher ist zum einen festzuhalten, dass Sperrungen durch die Access-Provider zwar technisch möglich sind, jedoch kann jede der drei aufgeführten Sperrtechniken mit einem vergleichsweise geringen Aufwand von dem Nutzer oder den Anbietern der Inhalte umgangen werden.[57] Zum anderen bleibt bezüglich der Verhinderung des Zugangs zu bestimmten Webseiten festzuhalten, dass eine dauerhafte, zielgerichtete Sperrung ohne erhebliche Nebenwirkungen auf der Grundlage der gegebenen Internetstruktur nahezu unmöglich ist[58]. Um im Internet Sperrverfügungen sinnvoll und effektiv umsetzen zu können, müsste die Struktur des Internets komplett neu gestaltet werden.

8.5. Erforderlichkeit

Aus den genannten Gründen ist auch die Erforderlichkeit einer Sperrungsanordnung fraglich. Denn als erforderlich im Sinne des Verhältnismäßigkeitsgrundsatzes gilt ein Eingriff nur dann, wenn kein milderes, zugleich aber ebenso effektives Mittel zur Zielerreichung zur Verfügung steht. Zu denken wäre etwa an gezielte Aufklärungsmaßnahmen in der Öffentlichkeit mit Hilfe der Medien.
Eine Erklärung der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) aus dem Jahre 2005, die sich im Juni desselben Jahres mit der Meinungsfreiheit im Internet befasste, sprach sich dafür aus, die Inhaltskontrolle allein den Nutzern zu überlassen. Besondere Bedeutung sollten danach Filtermaßnahmen durch die Eltern zukommen.

Das VG Köln[59] nahm dennoch in einem Urteil aus dem Jahre 2005 an[60], dass eine Sperre, deren Wirksamkeit in der Regel vom Zufall abhängt, ein wirksames Mittel darstellt,

---

[57] Horster, S. 55.
[58] Schneider, Gerhard; Die Wirksamkeit der Sperrung von Internet-Zugriffen, in MMR 1999, S. 571 ff.
[59] VG Köln, Urt. v. 3.3. 2005 , 6 K 7603/02.

da nicht erwiesen sei, dass es „praktisch überhaupt keinen Zugriff auf die in Rede stehenden Seiten verhindert".

8.6. Angemessenheit

Ob eine Sperrung angemessen ist, muss aufgrund einer Abwägung anhand unterschiedlicher Kriterien entschieden werden. Zu diesen Kriterien zählen etwa die durch die unzähligen Inhalte verletzten Rechtsgüter auf der einen und durch die Kontrollmaßnahmen tangierten Rechtsgüter auf der anderen Seite.[61] Die Betroffenen dürfen nicht übermäßig oder unzumutbar belastet werden. Bei einer Gesamtabwägung zwischen der Schwere des Eingriffs und dem Gewicht und der Dringlichkeit der ihn rechtfertigenden Gründe muss die Grenze des Zumutbaren gewahrt bleiben.[62]

Als unzumutbar werden insbesondere Maßnahmen anzusehen sein, die einen erheblichen Aufwand erfordern, die jedoch durch einen Zugriff auf entsprechende Informationsangebote im Ausland oder über andere Netzverbindungen mit einem vergleichsweise geringen Aufwand umgangen werden können.[63] Dass dies auch bei der Düsseldorfer Bezirksregierung angeordneten Maßnahme aus dem Jahre 2002 der Fall war, dürfte jedenfalls keine unvertretbare Einschätzung sein. Denn selbst wenn die Sperrungen geeignet sind, den Zugang von 70 bis 80 Prozent der Nutzer zu den gesperrten Inhalten zu verhindern, so befinden sich noch zahlreiche weitere vergleichbare Inhalte im Netz, so dass die Chancen, den Schutz der deutschen Bevölkerung vor der Verbreitung von kinderpornographischen Inhalten, illegalem Glücksspiel, Werbung für terroristische Ziele, Volksverhetzung oder Betrug durchzusetzen, durch die Sperrung von einigen Internetseiten nur unwesentlich vergrößert werden dürften[64]. Zudem ist im Rahmen der Angemessenheit anzubringen, dass die Sperrungen erhebliche Kosten bei den Internet-Providern verursachen. Die intensivste finanzielle Belastung der Access-Provider würde

---

[61] Sieber, Ulrich; Die rechtliche Verantwortlichkeit im Internet, MMR 2/1999, Rn. 410 ff, München.

[62] BVerfGE 113, 167 ff.

[63] Sieber, Ulrich; Die rechtliche Verantwortlichkeit im Internet, MMR 2/1999, Rn. 423 ff, München.

[64] Kritische Würdigung der Anordnung von Sperrungen des Zugangs zur rechtswidrigen Internetinhalten gegenüber Zugangsvermittlern, Ausarbeitung WD 10 06/02.

sich für die Adressaten aus der Auflage ergeben, einen Proxy-Server zu installieren.[65] Sie bildet deshalb einen Hauptkritikpunkt der Sperrungstechnologie. Insbesondere für die Zugangsvermittler auf der Internetschicht, die keinen Proxy betreiben, würden sich enorme Kosten ergeben.[66] Die Branche geht von einem Gesamtaufwand von vielen Millionen Euro aus.[67] Unterschiedlich leistungsfähige Proxyserver sind zwar auch unterschiedlich teuer. Der Mindestaufwand ist aber auch nicht unbeträchtlich. Ebenso liegt es bei den Personalkosten. Sobald Sperrverlangen keine seltene Ausnahme mehr sind, müsste ein Access-Provider dafür besonderes Personal einstellen. Ein Teil der zusätzlichen Kosten ist also fix. Seine Höhe hängt nicht vom Geschäftsvolumen des Access-Providers ab. Deshalb sind kleine Access-Provider besonders betroffen. Einige müssten sogar ganz aus dem Markt ausscheiden. Bezüglich der DNS-Sperrungen können die Kosten nicht beziffert werden.

Für die Durchführung von DNS-Sperrungen wurden im Hinblick auf die Umstellung am Server in den bereits drei aufgezählten Verfahren zur Sperrungsverfügung der Düsseldorfer Bezirksregierung ein Kostenumfang von einem halben Arbeitstag berechnet.[68] Selbst bei einem vergleichsweise kostengünstigen Sperransatz wie der DNS-Manipulation ist problematisch, dass – anders als im allgemeinen Polizei- und Ordnungsrecht – im JMStV und im RStV keine Kostenerstattung zur Entschädigung der herangezogenen Diensteanbieter vorgesehen ist.[69]

Die Angemessenheitsprüfung gestaltet sich jedoch auch aus dem Grund als problematisch, weil sich bei der Normanwendung aufgrund der diversen illegalen Inhalte – wie Volksverhetzung, Pornografie, Gewaltdarstellungen –, des Tätigkeitsschwerpunkts der Provider und der einsetzbaren technischen Sperrmaßnahmen sehr unterschiedliche Fallkonstellationen ergeben können. Die Prüfung ist auch in den jeweiligen unterschiedlichen Fallgestaltungen problematisch, da meist mehrere Grundrechtsträger und unterschiedliche Grundrechte betroffen sind. Schwierig ist schließlich auch die Angemessenheit einer Sperrungsanordnung im Verhältnis zu dem mit ihr verfolgten Ziel. Denn wäh-

---

[65] Engel, Christoph; Die Internet-Service-Provider als Geiseln deutscher Ordnungsbehörden, in: MMR 4/2003, S. 20, Pfitzmann, Köpsell, Kriegelstein, S. 216.

[66] Pfitzmann, Köpsell, Kriegelstein; S. 188.

[67] Engel, Christoph; Die Internet-Service-Provider als Geiseln deutscher Ordnungsbehörden, in: MMR 4/2003, S. 20.

[68] Pfitzmann, Köpsell, Kriegelstein; S. 185.

rend das mit ihr verfolgte Ziel nach den bereits gemachten Ausführungen einerseits allenfalls unvollständig erreicht wird, schränkt die Sperrung von Web-Seiten mit Hilfe eines DNS-Filters eine ganze Reihe von verfassungsrechtlich bedeutsamen Belangen ein.

An erster Stelle ist dabei die Kommunikationsfreiheit des Art. 5 GG zu nennen, die zwar nicht unbeschränkt garantiert wird, insbesondere durch die mittelbaren Wirkungen einer Sperrungsandrohung aber auf eine Weise gefährdet werden kann, die bedenklich erscheint. Denn wenn auch zuzugeben ist, dass Belange des Jugendschutzes im Allgemeinen und der öffentlichen Sicherheit und Ordnung Beschränkungen der Kommunikationsfreiheit legitimieren können, muss dennoch berücksichtigt werden, dass die Gefahr weitergehender Beeinträchtigungen besteht, wenn Access-Provider Geldbußen befürchten müssen, weil sie bestimmte Inhalte nicht hinreichend ausfiltern können. Dann nämlich besteht die Gefahr, dass diese Provider zur Vermeidung möglicher Nachteile auch Inhalte sperren, die an sich unbedenklich sind. Im Ergebnis würden dadurch private Unternehmen zu einer Art Zensurstelle, die darüber entscheidet, welche Informationen zu den Bürgern gelangen können und welche nicht, ohne dass die gleichen rechtsstaatlichen Vorkehrungen gegen einen Missbrauch dieser Macht bestehen würden wie gegenüber staatlichen Einschränkungen der Kommunikationsfreiheit.[70] Hält man sich das große Missbrauchspotenzial, das gerade bei zentralen technischen Filtersystemen besteht, und die Bedeutung der Kommunikationsfreiheit für eine freiheitliche Demokratie vor Augen, so muss diese Gefahr als besonders schwerwiegend angesehen werden. Eben mit dieser Begründung sind im Interesse des Jugendschutzes eingeführte Bestimmungen in den Vereinigten Staaten von Amerika durch den Supreme Court für verfassungswidrig erklärt worden.[71]

Hinzu kommen Einschränkungen der Freiheit der wirtschaftlichen Betätigung der Access-Provider. Insbesondere für kleine Provider kann die Einrichtung einer Sperrung unter Umständen einen erheblichen technischen Aufwand bedeuten, zumal in vielen Fällen aufgrund der oben genannten technischen Umgehungsmöglichkeiten eine ständige Aktualisierung der technischen Einstellungen notwendig sein wird. Erschwerend

---

[69] Pfitzmann, Köpsell, Kriegelstein; S. 216.

[70] Hoffmann-Riem, Wolfgang: Wider die Geistespolizei, in: Die Zeit 20/2001.

[71] Engel, Keller; S. 115 f.

wirkt zudem, dass aufgrund der dezentralen Aufsichtsstruktur in der Bundesrepublik Deutschland wahrscheinlich ist, dass in vielen Fällen nicht alle Provider den gleichen Sperrungsanordnungen unterliegen. Das birgt für den einer Anordnung unterliegenden Provider nicht nur aufgrund der zahlreichen „Internet-by-Call"-Angebote die Gefahr, dass Kunden zu einem anderen Anbieter wechseln und die mit einer Sperrung angestrebte Wirkung verpufft. Entsprechend wird von Zimmermann angenommen, eine Sperrungsanordnung sei nur dann angemessen, wenn sie allen in Deutschland tätigen Zugangsanbietern auferlegt wird.[72]

Stellt man diese negativen Auswirkungen den vermutlich nur geringen positiven Effekten gegenüber, muss mit einer im Schrifttum zunehmend vertretenen Auffassung auch die Angemessenheit einer Sperrungsanordnung gegenüber Access-Providern als problematisch angesehen werden.[73]

9. China als ein Fallbeispiel für Sperrmaßnahmen

Während der Ming Dynastie (14. – 17. Jahrhundert) bauten die Chinesen das größte Befestigungswerk der Erde mit einer Gesamtlänge von 7.200 km. Seit einigen Jahren feilt die chinesische Regierung mit der Unterstützung westlicher Suchmaschinenbetreiber am Aufbau einer undurchlässigen Internetzensur, auch sog. Great Firewall of China genannt, die gerade im Rahmen der Olymischen Spiele weltweit Aufsehen erregte. Da es von offizieller chinesischer Seite keine Beschreibung für die in China angewendete System zur Sperrung des Zugriffs auf unliebsame, ausländische Internetinhalte gibt, kann nur auf Literatur zurückgegriffen werden, die sich eingehend damit beschäftigt hat, den Aufbau und die Funktionsweise des Systems zu rekonstruieren. So haben Wissenschaftler der Universität von Cambridge ermittelt („Ignoring the great firewall of China, 2006, Clayton), wie chinesische Internet-Nutzer vor missliebigen Inhalten geschützt werden.

---

[72] Zimmermann, Andreas; Polizeiliche Gefahrenabwehr und das Internet, in: NJW 1999, S. 3150.

[73] ebenda

Zunächst werden die Datenpakete durch die chinesischen Access-Provider ungehindert weitergeleitet, wobei jedoch Kopien an ein Intrusion Detection System (IDS) geleitet werden. Das IDS analysiert den Datenstrom auf zu sperrende Inhalte. Wird ein zu sperrender Inhalt aufgespürt, so werden die Router instruiert, TCP-Reset (RST)-Pakete an die beiden Endpunkte der Kommunikation zu senden. Dies hat zur Folge, dass die beteiligten Geräte – in den meisten Fällen Rechner des Endnutzers und Webserver – die Verbindung als beendet ansehen. Gleichzeitig speichert das IDS für eine gewisse Zeit die IP-Adressen der an der geblockten Verbindung beteiligten Endpunkte. Auf diese Weise kann das IDS zukünftige Verbindungen sofort sperren, ohne eine Inhaltsanalyse durchführen zu müssen (Gutachten Technik, S. 59).

Das bemerkenswerte an dieser Lösung ist, dass nicht etwa die zu sperrenden IP-Adressen in einer Firewall bzw. den Routern hinterlegt werden, sondern diese Lösung quasi „stateless“ funktioniert, da sie die beteiligten Kommunikationspartner dazu bringt, von einer beendeten Kommunikation auszugehen. So wird das Skalierbarkeitsproblem gelöst, da im Allgemeinen davon auszugehen ist, dass eine zustandsbasierte Filterung zu aufwendig ist, als das sie unter praktischen Gesichtspunkten in den Firewalls/Routern der Access-Provider durchführbar wäre.
Dieses Filtersystem hat sich in Tests zwar als nicht perfekt erwiesen, da auch hier Möglichkeiten bestehen die Sperrmaßnahmen zu umgehen. Dennoch lässt sich feststellen, dass diese Methode eine effektive Maßnahme zur Sperrung darstellt.

Gerade am Beispiel China zeigt sich, dass Sperrungen durchaus wirksam durchgesetzt werden können, allerdings mit einem erheblichen Aufwand an Kosten, Zeit und Human Resources. Um Sperrungen effektiv handhaben zu können, müsste das Internet ganzheitlich umstrukturiert werden und insbesondere seine ursprüngliche Intention, nämliche die dezentrale Vernetzung von Computern, aufgegeben werden.

Günter Pursch gez. Verena Bär

10. Literaturverzeichnis

Boßmanns, Claudia; Urheberrechtsverletzungen im Online Bereich und strafrechtliche Verantwortlichkeit der Internet-Provider, Verlag Peter Lang, Frankfurt/Main, 2003

Brauner, Detlef; Raible-Besten, Robert; Weigert, Martin; Internetlexikon, R. Oldenbourg Verlag, München, 1997

Eichhorn, Bert; Internetrechrecht – Ein Lehrbuch für das Recht im World-Wide-Web, Beuth-Verlag, Berlin, 2000

Engel, Christoph; Keller, Ken; Global Networks and Local Values: A Comparative Look at Germany and the United States, Nomos, Baden-Baden, 2001

Gets, Marina; Meinungsäußerungs- und Informationsfreiheit im Internet aus der Sicht des Völkerrechts, Berliner Wissenschafts-Verlag, 2000

Hoeren, Thomas; Grundzüge des Internetrechts, C. H. Beck, München, 2002

Horster, Patrick; Datenschutz und Datensicherheit : Konzepte, Realisierungen, rechtliche Aspekte, Anwendungen, Vieweg + Teubner, Wiesbaden, 1999

Kriegelstein, Thomas; Sperrverfügungen gegen Access-Provider, http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf, 2008

Tanenbaum, Andrew:, Computernetzwerke, Pearson Studium, München, 2003

Volkmann, Christian; Der Störer im Internet, C. H. Beck, München, 2005

Links zu Gutachten:

Gutachten über Glückspiele in Rundfunk und Telemedien

http://www.kjm-online.de/public/kjm/index.php?show_1=154,58

Juristisches Gutachten:

http://www.kjm-online.de/public/kjm/downloads/juristisches%20Gutachten%20Sperrverfuegungen.pdf

Technisches Gutachten

http://www.kjm-online.de/public/kjm/downloads/technisches_Gutachten_Sperrverfuegung_2.pdf