Sachstand
EZPWD – Anfrage Nr. 3038
Internetsperren in Deutschland

1. Einleitung

Sperrverfügungen gegen Internetdiensteanbieter 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 seitdem mit dem und durch das Internet Geld verdient wird, wurde deutlich, dass klare gesetzliche Rahmen gegeben werden mussten. Gerade für Unternehmen, die in Geschäftsmodelle, die im Zusammenhang mit dem Internet stehen, investieren, sind rechtliche Grundlagen elementar. 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 noch immer erhebliche Schwierigkeiten.

2. Technische Voraussetzungen an die Sperrung von Internetseiten in Deutschland

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) (Der MDStV ist seit dem 01.03.2007 außer Kraft. Zudem gab es in Deutschland mit dem gescheiterten Zugangserschwerungsgesetz von 2009 den Versuch, Verpflichtungen zur technischen Sperrung von Inhalten durchzusetzen. Der Gesetzgeber strebte damit die Verpflichtung von Zugangsprovidern zur Sperrung vom Bundeskriminalamt indizierten kinderpornographischen Seiten an. Durch einen im April 2011 ergangenen Kabinettsbeschluss wurde das Gesetz jedoch wieder außerkraftgesetzt.) für das Land Nordrhein-Westfalen fungierte und Sperrungsverfügungen gegen eine Reihe von Access-Provider erlassen hat, sind drei verschiedene Sperrungsmöglichkeiten bekannt. Diese spielen auch gegenwärtig eine zentrale Rolle.

- Die Manipulation der DNS-Einträge am DNS-Server des Access-Providers,
- die Benutzung eines Proxy-Servers, mit dem Anfragen auf die unzulässigen Angebote gefiltert oder aber auf eine andere vordefinierte Seite im Browser umgeleitet würden
- oder die Sperrung der IP-Adresse am Router.

Diese Verfahren sollen nachfolgend analysiert werden.

3. DNS Sperren

Das DNS ist einer der wichtigsten Dienste im Internet. Hauptsächlich wird das DNS zur Umsetzung von Domainnamen in IP-Adressen benutzt. 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.) 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.

3.1. 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 und die Endnutzer dann die Meldung „Host not found“ erhalten.

3.2. 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. 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. Wenn ein Browser über die technische Möglichkeit verfügt, so kann der Benutzer über das Browser-Optionsmenü einstellen, dass statt des für die URL zuständigen Servers zunächst der vom Nutzer eingetragene Proxy befragt wird, ob dieser die gewünschte Information in seinem Cache (eine besondere Art von Speicher, die den Zugriff auf Daten beschleunigen soll) 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.

3.3. 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. Somit ist dieses Angebot für den Kunden des Providers nicht mehr erreichbar.

3.4 Umgehungsmöglichkeiten

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. Das VG Düsseldorf 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.“

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. 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 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. 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. 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. Zudem wäre ein weiterer Nachteil, dass der Einsatz von Proxy-Servern einen erheblichen technischen Aufwand erfordern würde.

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. 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. Um im Internet Sperrverfügungen sinnvoll und effektiv umsetzen zu können, müsste die Struktur des Internets komplett neu gestaltet werden.

4. Rechtliche Voraussetzungen an die Sperrung von Internetseiten in Deutschland

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.

5. Verfassungsrechtliche Aspekte

5.1. 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.

5.2. 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.

5.3 Erforderlichkeit

Aus den genannten Gründen (Umgehungsmaßnahmen der Sperrmaßnahmen, vgl. 2.4) 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 nahm dennoch in einem Urteil aus dem Jahre 2005 an, dass eine Sperre, deren Wirksamkeit in der Regel vom Zufall abhängt, ein wirksames Mittel darstellt, da nicht erwiesen sei, dass es „praktisch überhaupt keinen Zugriff auf die in Rede stehenden Seiten verhindert".

5.4. 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. 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.

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. Dass dies auch bei der Düsseldorfer Bezirksregierung angeordneten Maßnahme aus dem Jahre 2002 der Fall war, dürfte jeden-falls 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 kinder-pornographischen Inhalten, illegalem Glücksspiel, Werbung für terroristische Ziele, Volksverhetzung oder Betrug durchzusetzen, durch die Sperrung von einigen Internetseiten nur unwesentlich vergrößert werden dürften. 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 sich für die Adressaten aus der Auflage ergeben, einen Proxy-Server zu installieren. Sie bildet deshalb einen Hauptkritikpunkt der Sperrungstechnologie. Insbesondere für die Zugangsvermittler auf der Internetschicht, die keinen Proxy betreiben, würden sich enorme Kosten ergeben. Die Branche geht von einem Gesamtaufwand von vielen Millionen Euro aus. Unterschiedlich leistungsfähige Proxyserver sind zwar auch unter-schiedlich 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. Selbst bei einem vergleichsweise kostengünstigen Sperransatz wie der DNS-Manipulation ist problematisch, dass – anders als im allgemeinen Polizei- und Ordnungs-recht – im Jugendmedienschutzvertrag (JMStV) und im Rundfunkstaatsvertrag (RStV) keine Kostenerstattung zur Entschädigung der herangezogenen Diensteanbieter vorgesehen ist.

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 Fall-konstellationen ergeben können. Die Prüfung ist auch in den jeweiligen unterschiedlichen Fallgestaltungen problematisch, da meist mehrere Grundrechtsträger und unter-schiedliche Grundrechte betroffen sind. Schwierig ist schließlich auch die Angemessenheit einer Sperrungsanordnung im Verhältnis zu dem mit ihr verfolgten Ziel. Denn während 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 gegen-über staatlichen Einschränkungen der Kommunikationsfreiheit. 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.

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 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 teilweise angenommen, eine Sperrungsanordnung sei nur dann angemessen, wenn sie allen in Deutschland tätigen Zugangsanbietern auferlegt wird.

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.

6. Statistiken bezüglich Inhalt und Häufigkeit gesperrter Internetseiten in Deutschland

Umfassende Statistiken bezüglich Inhalt und Häufigkeit gesperrter Internetseiten sind in Deutschland nicht zu finden. Exemplarisch soll daher auf die Listenführung der Bundesprüfstelle für jugendgefährdende Medien (BPjM) eingegangen werden. (Vgl. auch die Google- Transparenzberichte, in denen eine Auflistung von Löschanfragen von Regierungsstellen gegen Inhalte auf Google-Diensten zu finden ist).

Die BPjM ist zuständig für die Indizierung von Träger- und Telemedien mit jugendgefährdendem Inhalt. Das Jugendschutzgesetz (JuSchG) verpflichtet die BPjM eine Liste der jugendgefährdenden Medien zu führen.

Die Veröffentlichung der Indizierungen aus Listenteil A und B erfolgt im Bundesanzeiger. Die BPjM gibt darüber hinaus alle drei Monate das amtliche Mitteilungsblatt "BPjM-Aktuell" heraus. Es enthält die Liste aller indizierten Trägermedien und eine Übersicht aller der BPjM mitgeteilten Medien, die beschlagnahmt oder eingezogen worden sind, sowie einen redaktionellen Teil. Aus Gründen des Jugendschutzes erfolgt keine Bereitstellung der amtlichen Indizierungsdaten im Internet.

Die Liste der indizierten Telemedien (Teile C und D) ist jedoch nicht öffentlich. Im Juli 2014 verschaffte sich ein anonymer Hacker Zugang zu einer von der BPjM erstellten digitalen Sperrliste. Der Inhalt der vertraulichen Datei: Mehr als 3000 Links zu Internetseiten mit pornografischen, kinderpornografischen, sowie rechtsradikalen Inhalten. Das BPjM-Modul wurde von der Prüfstelle nur als verschlüsselte Datei bereitgestellt. Den genauen Inhalt verteidigte das BPjM bisher als geheim. Im Jahre 2013 gab das Verwaltungsgericht Köln den Jugendschützern in dem Punkt Recht, dass die Liste geheim gehalten werden müsse. Die Richter begründeten dies mit der Gefahr der Bereitstellung einer Anleitung für das Ansurfen der Inhalte.

7. Statistiken über die Wirksamkeit von Internetsperren

Statistiken über die Wirksamkeit von Internetsperren in Deutschland existieren nicht. Dennoch lässt sich festhalten, dass die Wirksamkeit von Sperrlisten vielerorts bezweifelt wird. So vertritt der Förderverein Informationstechnik und Gesellschaft die Auffassung, dass im Kampf gegen Kinderpornographie Internet-Sperren wirkungslos seien. An anderer Stelle wird beispielsweise darauf verwiesen, dass es in Norwegen eine Initiative gegeben hat, der sich auch andere Länder angeschlossen hätten, bei der Providern eine DNS-Sperre angeboten wurde. Da letztendlich aber zahlreiche Provider diese Maßnahme nicht unterstützen wollten, wird die Maßnahme insgesamt

als nicht wirkungsvoll beurteilt. Auch ein Vertreter der schwedischen Polizei hat die Wirksamkeit der dort seit circa vier Jahren eingerichteten Internetsperren gegen Kinderpornographie infrage gestellt, da es dort ebenfalls problemlose Umgehungsmöglichkeiten gibt. Gegner von Internetsperren verweisen darauf, dass mit Sperrlisten nicht nur illegale Inhalte wie gewünscht gesperrt würden, sondern teilweise auch andere Inhalte betroffen seien. Um Nebenwirkungen zu vermeiden, sei das Löschen bzw. die Beseitigung von illegalen Angeboten vorzuziehen.

8. Weiterführende Informationen im Internet

- Vgl. zum Abstimmungsergebnis des Zugangserschwerungsgesetzes von 2009: http://www.bundestag.de/parlament/plenargeschehen/abstimmung/20090618_kinderpornografie.pdf.
- Vgl. http://www.ccc.de/censorship/dns-howto/index.xml.
- ://www.kjm-online.de/public/kjm/downloads/juristisches%20Gutachten%20Sperrverfuegungen.pdf
- http://www.bundespruefstelle.de/bpjm/Aufgaben/Listenfuehrung/bekanntmachung.html
- Transparenzbericht Google: https://www.google.com/transparencyreport/?hl=de

9. Literatur

- Boßmanns, Claudia; Urheberrechtsverletzungen im Online Bereich und strafrechtliche Verantwortlichkeit der Internet-Provider, 2003.
- Brühl, Jannis, Janisch, Wolfgang, Gema gegen Telekom: Dieses Urteil ermöglicht das Sperren von Internetseiten, Süddeutsche Zeitung vom 26.11.2015.
- Aufgaben und Struktur der BPjM abrufbar unter: http://www.bundespruefstelle.de/bpjm/Aufgaben/Listenfuehrung/bekanntmachung.html
- Eichhorn, Bert; Internetrecht – Ein Lehrbuch für das Recht im World-Wide-Web, 2000.
- FITUG e.V. Pressemeldung und Hintergrundinformationen Kinderpornographie und Internet-Sperren vom März 2009, abrufbar unter: http://www.fitug.de/news/pes/fitug-20090325.de.Pressemeldung-Internet-Sperren.pdf.
- Fuest, Benedikt, Hacker knackt Internetsperrseite des Jugendschutzes, welt.de vom 12.07.2014, abrufbar unter: http://www.welt.de/print/die_welt/wirtschaft/article130073764/Hacker-knackt-Internet-Sperrliste-des-Jugendschutzes.html
- Gercke, Marco, in: Spindler, Gerald/Schuster, Fabian, Recht der elektronischen Medien, 3. Auflage 2015, § 184b.
- Kriegelstein, Thomas; Sperrverfügungen gegen Access-Provider, abrufbar unter: http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf, 2008.
- Kuhlmann, Nico, Störerhaftung von Access-Providern bei Urheberrechtsverletzungen, in: Gewerblicher Rechtsschutz und Urheberrecht. Praxis im Immaterialgüter- und Wettbewerbsrecht 2016.
- Lüthi, Nick, Access denied als Kollateralschaden, heise online, 05.04.2002, abrufbar unter: www.heise.de/tp/r4/artikel/12/12249/1.html
- Meister, Andre, Liste indizierter Webseiten geleakt: Bundesprüfstelle bestätigt Netz-Sperren-Kritik wie Overblocking, netzpoliti.org vom 08.07.2014, abrufbar unter: https://netzpolitik.org/2014/liste-indizierter-webseiten-geleakt-bundespruefstelle-bestaetigt-netz-sperren-kritik-wie-overblocking/
- Schneider, Gerhard; Die Wirksamkeit der Sperrung von Internet-Zugriffen, in MMR (1999): S. 571
- Schwedens Polizei: Kinderpornofilter sind wenig wirksam, abrufbar unter: http://www.golem.de/0903/66188.html. Die schwedische Filterliste ist im Internet verfügbar unter: http://maraz.kapsi.fi/sisalto-en.html.
- Volkmann, Christian, Der Störer im Internet, Schriftenreihe Information und Recht, 2005.
- Wissenschaftliche Dienste des Deutschen Bundestages (WD 10 – 010/09) Sperrverfügung gegen Internet-Provider.
- Wissenschaftliche Dienste des Deutschen Bundestages (WD 10 – 042/010) Internetsperren für kinderpornographische Inhalte.
- Verwaltungsgericht Düsseldorf , Urteil vom 10.05.2005 – 27 K 5968/02.

– Verwaltungsgericht Köln, Urteil vom 13.09.2013 - 19 K 3559/11.