Mit den Rezepten von gestern gegen die Probleme von morgen

Von Rechtsanwalt Dr. Hendrik Schöttle, Hambach & Hambach Rechtsanwälte

Zusammenfassung

Es gibt keine wirksame Möglichkeit für den Staat, unerwünschte Webseiten im Internet gegen den Zugriff aus Deutschland zu sperren. Die derzeit existierenden Methoden lassen sich ohne Spezialkenntnisse oder zusätzliche Hard- und Software mit zwei Mausklicks außer Kraft setzen. Zudem lässt sich technisch nicht ausschließen, dass durch eine Sperrung zahlreiche Angebote ebenfalls geblockt werden, die gar nicht Ziel der dahinter stehenden Verfügung sind. Sollen mehr als nur 1-2 Webseiten geblockt werden, ist darüber hinaus ein System erforderlich, welches regelmäßige automatische Aktualisierungen der Sperrlisten ermöglicht.

Angesichts des immensen finanziellen und personellen Aufwands, der hohen Kollateralschäden und der von jedermann einfach zu bewerkstelligenden Umgehung scheitert jede Sperrungsverfügung am Verhältnismäßigkeitsgrundsatz und ist daher rechtswidrig.

Die Diskussion um die Zukunft des deutschen Sportwetten- und Glücksspielmarktes reißt nicht ab. Die EU hat kürzlich erst deutlich gemacht, dass sie die geplante Neufassung des Lotterie-Staatsvertrags nicht akzeptieren werde. Das geplante Regelwerk widerspreche der Dienstleistungsfreiheit und sei deswegen EU-rechtswidrig, so der EU-Binnenmarkt-Kommissar Charlie McCreevy in einem Spiegel-Interview. Dennoch wollen die Länder an dem Vertragsentwurf festhalten. Am 13. Dezember 2006 soll über den Staatsvertrag abschließend beraten werden,

der – geht es nach den Ländern – zum 1. Januar 2008 in Kraft treten soll.

Ob es allerdings jemals so weit kommen wird, ist inzwischen mehr als fraglich. Der Staatsvertrag enthält in seiner zuletzt geänderten Fassung so viele Ausnahmen zugunsten der staatlichen Anbieter, dass von einem „konsequent am Ziel der Bekämpfung der Wettsucht“ ausgerichteten Angebot nicht mehr die Rede sein kann. Doch genau dies verlangt das Bundesverfassungsgericht in der Sportwetten-Entscheidung vom 28. März 2006.

Sperrungsverfügungen als Mittel zum Zweck?

Um die zahlreichen europäischen Online-Spieleanbieter vom deutschen Markt zu drängen, wird inzwischen überlegt, auch die deutschen Internet-Zugangsanbieter in die Pflicht zu nehmen. Ein Beispiel: Im Sportausschuss des deutschen Bundestags wurde überlegt, angesichts zahlreicher im EU-Ausland betriebener Online-Angebote auch die Anbieter von Internet-Zugängen in die Pflicht zu nehmen. In der letzten Sitzung des Bundestags-Sportausschusses wurde es auf den Punkt gebracht:

> *„Wenn ein klares gesetzliches Verbot für die Zukunft vorliegt, wird es auch durchsetzbar sein. Die Durchsetzbarkeit betrifft die Internetprovider auf der einen und die Banken, die den Zahlungsverkehr abwickeln, auf der anderen Seite.“*[1]

Auch im aktuellen Entwurf des Lotterie-Staatsvertrages wird daher in der Begründung von der Sperrung ausländischer Webseiten durch Internetprovider ausgegangen.[2]

Der Vorschlag klingt so einfach wie genial: Die deutschen Anbieter von Internetzugängen werden verpflichtet, die Webseiten ausländischer Glücksspielanbieter zu sperren. Damit ist den Interessenten in Deutschland ein Zugriff auf diese

Anbieter nicht mehr möglich und die – vor allem finanziell schmerzhafte – Abwanderung weg von staatlichen Angeboten zur privaten und meist günstigeren Konkurrenz gestoppt. Derartige Forderungen nach einer Kontrolle des Internet sind nicht neu. Bereits das Regierungspräsidium Düsseldorf hat versucht, mit Sperrungsverfügungen Webseiten mit rechtsextremistischen Inhalten auszublenden. In der jüngst wieder aufgenommenen Debatte um ein Verbot von „Killerspielen“ wurden ebenfalls Forderungen laut, *„auch eine Regelung zur Zugriffsbeschränkung für Internetseiten mit entsprechenden Inhalten zu erlassen“*[3] .

Doch ein solches Vorhaben krankt an gleich zwei Kardinalfehlern: Eine Sperrungsverfügung ist erstens aus technischer Sicht völlig ungeeignet und hält daher zweitens einer rechtlichen Verhältnismäßigkeitsprüfung nicht stand. Solche Forderungen offenbaren ein frappierendes Fehlverständnis von dem, was im Internet machbar ist und was nicht. Nachfolgend soll zur Verdeutlichung der technischen Problematik gezeigt werden, wie es mit zwei Mausklicks möglich ist, auch die stärkste Form der Website-Sperrung, die Blockade der IP-Adresse, zu umgehen – ohne jegliche Zusatzsoftware oder Spezialkenntnisse. Welche Auswirkungen das auf die rechtliche Zulässigkeit von Sperrungsverfügungen hat, soll in einem zweiten Teil untersucht werden.

Die technische Machbarkeit: nur Schein, kein Sein Um zu veranschaulichen, warum eine Sperrungsverfügung aus praktischer Sicht zum Scheitern verurteilt ist, muss die Technik, die hinter dem Internet steht, etwas genauer betrachtet werden. Das Internet wurde als ein Netzwerk entwickelt, dessen Stärke besonders eine hohe Ausfallsicherheit ist; diese Ausfallsicherheit wird vor allem durch eine dezentrale Organisation sicher gestellt. Und genau diese Stärke ist der große Schwachpunkt eines jeden Versuchs, bestimmte Informationen zu filtern oder zu blockieren.

Die DNS-Sperrung

Im Internet wird zur Adressierung von Rechnern – und damit auch von bestimmten Webseiten – das so genannte Domain Name System (DNS) verwendet. Es ermöglicht, im Browser (z.B. Firefox oder dem Internet Explorer) unter der Adresse http://www.bverfg.de die Website des Bundesverfassungsgerichts zu erreichen. Eine Methode zur Sperrung von Webseiten, die auch von staatlichen Stellen vorgeschlagen wird,[4] sieht daher vor, dass die Internet-Zugangsprovider (z.B. AOL, T-Online oder Arcor) Anfragen zu bestimmten Webseiten nicht weiterleiten. Der Benutzer erhält dann eine Fehlermeldung, wenn er die entsprechende Webseite aufruft.[5] Reicht es also, alle Anfragen nicht weiterzuleiten, welche die Seite www.bverfg.de anfordern? Mitnichten: Viele Websites segeln nicht nur unter einer Flagge im Internet, sondern sind auch über alternative Domainnamen erreichbar. Im Fall des Bundesverfassungsgerichts ist dies etwa die Adresse http://www.bundesverfassungsgericht.de/. Hinzu kommt übrigens noch, dass im Fall des Bundesverfassungsgerichts jeweils auch das „www.“ weggelassen werden kann, womit wir bereits bei vier Alternativen wären. Und das bei einer Website, die es noch nicht einmal darauf angelegt hat, durch verschiedene Schreibweisen möglichen Sperrungsverfügungen zu entgehen. In Italien hat man sich von derartigen Bedenken jedoch nicht abschrecken lassen und eine Liste mit zahlreichen ausländischen Glücksspielanbietern vorgelegt, die zu sperren sind.[6] Allerdings hat man nicht gerade besondere Sachkenntnis offenbart, als man die URL www2.sportwetten-gera.com aufnahm. Die meisten Internetnutzer wissen, worum es geht: Bei großen Providern ist es oft üblich, die Serverlast (den Datenverkehr) auf mehrere Rechner zu verteilen. So führt eine Einstiegsseite unter www.sportwetten-gera.com auf die Server www1-www4. Würde das Bundesverfassungsgericht dieselbe Technik einsetzen, wären wir mit unserem Beispiel schon bei zwölf zu sperrenden Domainnamen – wohlgemerkt für eine einzige Website.

Sperrung von IP-Adressen

Aber ist die Website wenigstens dann hinter Schloss und Riegel, wenn eine Sperrungsverfügung sämtliche Domainnamen umfasst? Wer diese Frage bejaht, offenbart fehlendes technisches Grundverständnis. Jeder Rechner besitzt eine eigene IP-Adresse, unter welcher er erreichbar ist. Im Fall des Bundesverfassungsgerichts führt auch die Eingabe von http://134.96.83.81/ in die Adresszeile des Browsers zum Ziel. Damit muss ein Schutz, der mehr sein soll als eine bloße Fassade, auch eine Sperrung der entsprechenden IP-Adressen umfassen.

Allerdings werden mit einem derart brachialem Vorgehen nicht selten auch die Falschen getroffen. Hinter einer einzigen IP-Adresse verbergen sich oftmals tausende von Webseiten auf einem „Multi-Domain-Server“, die mit dem einen schwarzen Schaf, dem Ziel der Sperrungsverfügung, nicht das geringste zu tun haben. Auch ist zu bedenken, dass das Internet keine statische Menge an Servern mit unveränderlichen IP-Adressen darstellt: So waren vor vier 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.[7] Da die Sperrlisten nicht aktuell waren, wurden auch die Hochschulseiten gesperrt, obwohl sie mit den Rechtsextremen weder den Domainnamen, noch den Inhalt teilten. Wer eine Sperrungsverfügung verhängt, müsste also regelmäßig die Liste der gesperrten Websites auf ihre Aktualität überprüfen. Dies übrigens nicht nur, um Unschuldige vor Sperrungen zu bewahren: Denn auch die Spieleanbieter werden nicht schlafen. Für sie ist es ein leichtes, sich innerhalb weniger Stunden einen anderen Domainnamen und eine andere IP-Adresse zuzulegen. Die Blockade der ursprünglich verwendeten Website liefe damit ins Leere. Es müsste also ein System eingerichtet werden, welches es ermöglicht, die Sperrliste täglich zu ändern und diese Änderungen automatisch an alle Provider weiterzugeben. Man muss sich nur die deutschen „Leuchtturmprojekte“ Autobahnmaut

und elektronische Gesundheitskarte vor Augen halten, um sich auszumalen, in welchem Jahrzehnt und zu welchen Kosten ein solches System fertig gestellt wäre. Dennoch würden dann immer noch andere, hinter derselben IP-Adresse stehende Anbieter zu unrecht ebenfalls gesperrt werden: Wer wegen eines einzigen rechtswidrigen Angebotes bei T-Online deren IP-Adresse sperren will, sperrt nahezu alle anderen Webseiten, die auch bei T-Online liegen.

Das Umgehen einer Website-Sperrung: ein Sache von zwei Mausklicks

Doch selbst wenn man derartige Kollateralschäden und explodierende Kosten für eine tägliche Aktualisierung der Sperrliste in Kauf nähme und die stärkste Form der Sperrung wählte – Blockierung der IP-Adresse und des DNS-Eintrages wäre der „Schutzwall" für den durchschnittlichen Internetnutzer so unüberwindlich wie eine rote Fußgängerampel. Die Nutzer können einen derartigen Schutz mit einfachsten Mitteln umgehen. Wie eingangs geschildert, sind dazu weder aufwändige Software, noch Programmierkenntnisse erforderlich. Im Gegenteil, der Beweis, wie kinderleicht eine solche Sperre umgangen werden kann, ist lediglich zwei Mausklicks entfernt.

Eines Vorweg: Die nachfolgende „Anleitung" ist kein vertrauliches Insiderwissen aus kriminellen Internetforen, in denen Hacker ihre neuesten Erkenntnisse austauschen. Nein, der Staat selbst erklärt, wie die „Zensur" umgangen werden kann, nachzulesen im 26. Tätigkeitsbericht 2004 des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD)[8]:

> *„Die chinesische Regierung betreibt eine rigide Zensur des Internet-Verkehrs von Nutzern in China, sodass zahlreiche Internet-Angebote gesperrt werden. Dies betrifft auch deutsche Firmen, die in China tätig sind. Mittels AN.ON ist es ihnen möglich, diese Zensur zu umgehen und auch auf von der Regierung nicht überwachte Internet-Angebote zuzugreifen."*

AN.ON ist ein Anonymisierungsdienst, auch Anonymizer genannt. Ein Anonymizer funktioniert als Proxy, also als Zwischenrechner, über welchen die Kommunikation mit dem eigentlichen Rechner abgewickelt wird. Ursprünglich zu dem Zweck entwickelt, anonymes Surfen zu ermöglichen, lässt er sich auch zum Umgehen von gesperrten Websites verwenden, wie vom Landesdatenschutzzentrum Schleswig-Holstein aufgezeigt. Das Prinzip ist denkbar einfach: Der Nutzer ruft den Anonymizer in seinem Browser auf, gibt die Website ein, die er besuchen möchte – fertig! Um keine Erwartungen zu enttäuschen, sei hier der Beweis angetreten, dass das ganze eine Sache von zwei Mausklicks ist:

Wenn Sie die Seite http://www.wieistmeineip.de/ aufrufen (erster Mausklick), sehen Sie Ihre IP-Adresse, also die Adresse, unter welcher Ihr Rechner gerade im Internet erreichbar ist. Gleichzeitig dürfte auch noch das von Ihrem Rechner verwendete Betriebssystem sowie Ihr Browser angezeigt werden. Schalten Sie nun einen Anonymizer davor, indem Sie die Seite http://anonymouse.org/cgi-bin/anon-www_de.cgi/http://www.wieistmeineip.de aufrufen (zweiter Mausklick), werden Sie feststellen, dass sich Ihre IP-Adresse geändert hat. Außerdem werden Ihre Betriebssystem und Ihr Browsertyp nicht mehr erkannt. Mit diesem zweiten Mausklick haben sie bereits sämtliche DNS- und IP-Sperren erfolgreich hinter sich gelassen. Selbstverständlich können Sie anstelle der Seite www.wieistmeineip.de jede beliebige andere Webseiten aufrufen[9] – auch solche, die in Deutschland eigentlich nicht erreichbar sein sollen.

Da die meisten dieser Anonymisierungsdienste außerhalb Deutschlands betrieben werden, können Sie ungefiltert auf die in Deutschland gesperrten Webseiten zugreifen. Fazit: Wer eine Website wirklich sperren will, muss auch sämtliche Anonymizer kontrollieren, bzw. sperren. Das sind jedoch hunderte von Rechnern, die weltweit verteilt sind und über ständig

wechselnde Adressen erreicht werden können. Ein Ding der Unmöglichkeit. Professor Dr. Gerhard Schneider, Mitglied des Verwaltungsrates des Deutschen Forschungsnetzes, kommt daher zu einem eindeutigen Ergebnis:

> *„In Wirklichkeit handelt es sich [bei Website-Sperrungen] lediglich um einen Versuch, den direkten Datenaustausch aus einem Rechtsraum mit einem sich außerhalb befindenden Rechner zu unterbinden. Auf die indirekten Wege hat dies keinen Einfluss und solange der eigene Rechtsraum klein ist im Verhältnis zur Ausdehnung des Internet, sind indirekte Wege zahllos vorhanden. Der einzige Weg, eine sog. Vollsperrung wirklich durchzusetzen, ist daher, sich vollständig vom Internet und allen anderen Kommunikationswegen (inklusive Telefon) abzukoppeln.“*[10]

Dass es dabei keinen Unterschied macht, welche Art von Webseiten gesperrt werden, liegt auf der Hand:

> *„Ob Sie dabei gegen Rechtsradikale oder gegen ausländische Spieleseiten vorgehen wollen – die Mittel sind gleich wirkungslos, denn die Bits sind dieselben“, so Schneider in einem telefonischen Interview vom 20.11.2006.*

Nach der oben dargestellten kleinen Demonstration dürfte klar sein, dass jeder Durchschnittsnutzer mit einem Anonymizer umgehen kann. Im übrigen gibt es genügend Bestrebungen, auch staatlicherseits, den Einsatz von Anonymizern zu fördern. Dieses Ziel hat sich etwa das bereits erwähnte ULD mit dem Projekt AN.ON gesetzt – immerhin gefördert vom Bundeswirtschaftsministerium. Auch wenn die Meinungsfreiheit in China dabei auf der Strecke bleibt, dürften solche Projekte nach den derzeitigen Plänen wohl keine Zukunft mehr haben, da mit derselben Technik auch das staatliche Glücksspielmonopol zumindest finanziell ausgehebelt werden könnte. Doch selbst, wenn der Staat den Spielern nicht mehr selbst mit Anleitungen

unter die Arme greift – entsprechende Tipps kursieren heute schon überall im Internet.

Der Vollständigkeit halber sei noch angemerkt, dass die hier dargestellte Technik nur eine von zahlreichen Möglichkeiten ist, die Sperre zu umgehen. Ob durch Verwendung eines Proxys, durch die Einrichtung eines Virtual Private Network (VPN) oder einfach durch die Modem-Einwahl bei einem ausländischen Internet-Provider – es gibt etliche andere Möglichkeiten, um trotz der roten Fußgängerampel auf die andere Straßenseite zu gelangen.

Neben der Technik das Recht: Zur (Un)verhältnismäßigkeit im weiteren Sinn

Wie gezeigt wurde, stellt selbst die stärkste Form der Website-Blockade, die Sperrung der IP-Adresse, eine Hürde dar, die mit zwei Mausklicks von jedem Internetnutzer problemlos genommen werden kann. Damit drängt sich die Frage auf, ob die Anordnung solcher Maßnahmen überhaupt rechtmäßig sein kann. Im Zentrum der folgenden Erörterungen steht allein die Frage, ob die Sperrung einer IP-Adresse ein rechtmäßiges Mittel gegen den rechtswidrigen Inhalt einer Website ist. Ob es sich bei der zu sperrenden Website um ein Angebot mit rechtsradikalem Inhalt handelt oder um einen Anbieter von Sportwetten: Die zugrunde liegenden und im Fall von Sportwettenanbietern zudem höchst umstrittenen Rechtsfragen sollen hier nicht weiter interessieren. Es soll einmal unterstellt werden, dass eine Website rechtswidrige Inhalte enthält.

Eine Sperrungsverfügung, welche 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.

Bereits zweifelhaft: die Geeignetheit

Geeignet ist ein Mittel dann, wenn mit seiner Hilfe der gewünschte Erfolg gefördert werden kann. Dass der Erfolg in jedem Einzelfall auch tatsächlich erreicht wird oder jedenfalls erreichbar ist, ist nicht erforderlich. Es genügt die Möglichkeit der Zweckerreichung.[11] Das VG Düsseldorf, das im Ergebnis die Rechtmäßigkeit einer Sperrungsverfügung bejahte, tat sich schon bei der Feststellung der Geeignetheit schwer.

Die Zweifel an der Wirksamkeit der in dem Verfahren vorgeschlagenen Sperrungsmethoden waren so groß, dass es bereits ausreichen solle, wenn es sich

> *„bei der Sperrung um einen „Schritt in die richtige Richtung“ handelt.*
>
> *Hiernach reicht es für die Geeignetheit der Maßnahme aus, dass sie den Zugriff … für den durchschnittlichen … Nutzer … erschwert. Dabei handelt es sich um einen Personenkreis, der sich mit technischen Details nicht auseinandergesetzt hat und auch die Konfiguration der eigenen Hard- und Software entweder Dritten überlässt oder nach Möglichkeit in dem werksseitig eingestellten Zustand belässt … Für diese Personengruppe wird der Zugriff … mindestens „sperriger“, nicht selten auch nicht unerheblich erschwert.“*[12]

Wenn man davon ausgeht, dass der durchschnittliche Nutzer eine Suchmaschine bedienen kann, kann er auch einen Anonymizer bedienen. Es ist nicht einzusehen, dass in den zwei erforderlichen Mausklicks eine erhebliche Erschwernis liegt. Wenn das VG Düsseldorf schon den durchschnittlich begabten Internetnutzer heranzieht, dann sollte es diesem auch durchschnittliche Fähigkeiten attestieren. Wer E-Mails lesen und versenden, wer bei eBay einkaufen und wer sein Bahnticket online buchen kann, der wird auch an einem Anonymizer nicht

scheitern. Ganz davon zu schweigen, dass bei Online-Glücksspielen Anbieter und Kunde von handfesten finanziellen Interessen getrieben sind. Sie werden sich kaum von einem derart wirkungslosen Schutz abhalten lassen.

Es wird zu Recht darauf hingewiesen, dass allenfalls „ein kleiner Prozentsatz von technisch weit unterdurchschnittlich versierten Nutzern … durch derartige Maßnahmen ausgesperrt werden“ kann.[13]

Die Erforderlichkeit oder das mildere Mittel

Neben der Geeignetheit muss auch die Erforderlichkeit gegeben sein, das heißt, es darf kein milderes Mittel existieren, was ebenso wirksam ist. Dass das der Fall sein dürfte, zeigt das VG Köln anschaulich am Beispiel der oben erörterten DNS-Sperrung:

> *„Insgesamt ist festzustellen, dass die DNS-Sperrung für technisch versierte Nutzer kein Hindernis darstellt und dass es bei den Normal-Nutzern vom Zufall abhängen kann, ob die Sperre greift.“*[14]

Das VG Köln nahm dennoch 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“*. Unabhängig von der Frage, ob in einem solchen Fall überhaupt noch eine Geeignetheit angenommen werden kann, dürfte diese Methode der Sperrung von IP-Adressen auf jeden Fall unterlegen sein, da die Wirksamkeit der letzteren zumindest nicht vom Zufall abhängt. Auch sonst ist ein milderes Mittel nicht ersichtlich, die Erforderlichkeit also zu bejahen.

Die Angemessenheit – wie weit darf der Staat gehen?

Die Angemessenheit ist gegeben, so drückt es das

Bundesverfassungsgericht aus, *„wenn die Maßnahme nicht außer Verhältnis zu dem verfolgten Zweck steht. 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.“*[15]

Im Rahmen der Angemessenheit sind folgende Argumente in die Waagschale zu werfen:

Zunächst ist in Betracht zu ziehen, dass die Sperrungen erhebliche Kosten bei den Internet-Providern verursachen. Sollen mehrere hundert Websites blockiert werden – wie es beim Glücksspielmonopol in Deutschland derzeit diskutiert wird – muss ein Weg gefunden werden, wie dies automatisiert geschehen kann. Die Automatisierung kann jedenfalls nicht darin liegen, dass, wie in Italien geschehen, die Behörde ein selbst erstelltes PDF-Dokument auf einer Webseite zum Download anbietet, welches für die automatische Auswertung schon aufgrund des Dokumentenformates völlig ungeeignet ist. Die Einrichtung eines solchen Verfahrens ist mit erheblichen Kosten verbunden. Auch das VG Köln hat diese Problematik gesehen, die Kammer hält es daher für denkbar, dass *„irgendwann ein Punkt erreicht sein könnte, an dem die Maßnahme dem Provider nicht mehr zugemutet werden kann*“.

Weiter ist zu berücksichtigen, dass die Sperrung einer IP-Adresse oftmals hunderte von Angeboten trifft, die auf demselben Webserver unter einer anderen Domain liegen. Das VG Düsseldorf stellt dazu lakonisch fest:

> *„Dass mit der Sperrung einer IP-Adresse wegen Rechtswidrigkeit eines Angebots auch (u.U. viele) 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.“[16]

Das Gericht hat insoweit recht, als dass nicht die Geeignetheit, sondern die Angemessenheit dadurch entfällt. Ansonsten zeigt diese Äußerung eine erschreckende Selbstüberschätzung. Um eines klarzustellen: Die Sperrungsverfügung richtet sich an deutsche Internet-Zugangsprovider. Das VG Düsseldorf geht allerdings davon aus, dass hier Webseiten-Betreiber in aller Welt freiwillig und auf eigene Kosten tätig werden, um nordrhein-westfälischen Sperrungsverfügungen zu entgehen. Glauben die Richter tatsächlich, ein amerikanischer Webseiten-Betreiber wird einem Rechner mit Tausenden von Websites eine neue IP-Adresse verpassen, weil irgendein Gericht in Düsseldorf den Internetnutzern in Nordrhein-Westfalen den Zugang dazu verweigern will? Die Realität dürfte anders aussehen: zahlreiche willkürlich gesperrte Websites, veraltete Listen mit längst aufgegebenen Domainnamen und überholten IP-Adressen – und frustrierte Nutzer. Diese werden vermehrt Anonymizer und andere Techniken nutzen, um die mit der Streuschussmethode gesperrten harmlosen Angebote ansehen zu können. Die IP-Sperre wird damit lediglich Unkosten bei allen Beteiligten verursachen, und ihre Wirksamkeit wird in wenigen Monaten nach der Einführung endgültig verpufft sein.

Schließlich ist im Rahmen der Angemessenheit vor allem zu berücksichtigen, dass die gewählte Sperrmethode keine ernsthafte Hürde darstellt, wie auch vom VG Köln bestätigt wurde.[17] Wie oben demonstriert, sind weder technische Spezialkenntnisse, noch besondere Hard- oder Software erforderlich. Lediglich das Eingeben einer Internetadresse in ein Texteingabefeld muss beherrscht werden. Mit anderen Worten: Wer eine Internetadresse in die Adresszeile eines Browsers eingeben kann, kann diese auch in das Eingabefeld eines Anonymizers eingeben. Wer diese Fähigkeiten einem

Internetnutzer abspricht, geht nicht mehr vom Durchschnitt aus.

Um es zusammenzufassen: Die hohen Kosten für die Einrichtung und Administration einer IP-Sperre, die Notwendigkeit täglicher Updates der gesperrten Adressen, die Gefahr von Kollateralschäden in Form von Sperrungen zahlreicher harmloser Websites vermögen nicht eine „Sperre“ zu rechtfertigen, welche mit zwei Mausklicks außer Kraft gesetzt werden kann. Eine derartige Sperrungsverfügung ist daher unverhältnismäßig und rechtswidrig.[18]

Ähnlich hat auch das OVG Sachsen-Anhalt geurteilt, als es die Verpflichtung eines Sportwettenanbieters kassierte, keine Verträge mit Nutzern aus Sachsen-Anhalt zu schließen. Eine derartige Maßnahme sei technisch kaum umsetzbar, Urteilten die Richter.[19] Der Vollständigkeit halber sei noch darauf hingewiesen, dass durch die billigend in Kauf genommene Sperrung von harmlosen Websites die in Art. 5 Abs. 1 S. 1 GG geschützte Informationsfreiheit der Internetnutzer verletzt wird.[20] Soweit zudem die Anbieter der gesperrten Websites betroffen sind, stellt diese Maßnahme auch eine Verletzung der Meinungsfreiheit dar.

Fazit

So wie es nach Terroranschlägen zum guten Ton gehört, den Einsatz von Interkontinentalraketen zur Terroristenjagd zu fordern,[21] so werden bei aktuellen Ereignissen mit Internetbezug zunehmend Forderungen laut, rechtswidrige, wirtschaftlich nachteilige oder einfach nur missliebige Inhalte im Internet zu unterdrücken. Die dahinter stehenden Interessen mögen in einigen Fällen noch verständlich sein, „machbarer“ wird eine Sperrung dadurch jedoch nicht. Wer dennoch daran festhält, hat die grundlegende Struktur des Internet nicht verstanden und gibt sich mit einer teuer erkauften Placebo-Wirkung zufrieden. Im Fall der Sperrung von

EU-ausländischen Online-Spielanbietern kommt noch hinzu, dass dies auf einer mit Europarecht unvereinbaren Grundlage geschähe. Es gibt dennoch gute Gründe zu hoffen, dass die Bundesländer letztlich doch nicht das zensurfreie Internet missbrauchen und damit finanziellen Interessen opfern. Es wäre nämlich der absurde Versuch mit den Rezepten von gestern die Probleme von morgen lösen zu wollen.

(1) Karl-Heinz Hage von der Berliner Senatskanzlei, zitiert nach dem Protokoll der 16. Sitzung des Sportausschusses vom 20.09.2006, S. 27.

(2) Siehe die Erläuterungen zum Entwurf des Staatsvertrages zum Glücksspielwesen vom 25.10.2006, S. 5.

(3) Spiegel Online vom 22.11.2006, http://www.spiegel.de/politik/deutschland/0,1518,449970,00.html.

(4) So etwa in einer Sperrungsverfügung der Bezirksregierung Düsseldorf vom 06.02.2002, siehe http://odem.org/material/verfuegung/sperrungsverfuegung.pdf.

(5) Eine solche Sperrung kann im übrigen leicht selbst simuliert werden. Unter Windows XP ist dazu eine Zeile in der Datei C:\WINDOWS\system32\drivers\etc\hosts hinzuzufügen.

(6) Die Liste kann auf der Website der Amministrazione Autonoma dei Monopoli di Stato unter http://www.aams.it/site.php?page=20060213093814964&on=download heruntergeladen werden.

(7) Siehe Telepolis-Meldung vom 5.04.2002, http://www.heise.de/tp/r4/artikel/12/12249/1.html.

(8) Abrufbar unter http://www.datenschutzzentrum.de/material/tb/tb26/kap15.htm.

(9) Wer sich die URL nicht selbst zusammensetzen möchte, rufe einfach die deutsche Startseite unter http://anonymouse.org/anonwww_de.html auf, dort lässt sich die

aufzurufende Adresse auch bequem in ein Eingabefeld eintippen.

(10) Schneider, Sperren und Filtern im Internet, MMR 2004, 18 (22).

(11) BVerfG, Beschluss vom 18.07.2005, 2 BvF 2/01, BVerfGE 113, 167 ff.

(12) VG Düsseldorf, Urteil vom 10.05.2005, 27 K 5968/02, MMR 2005, 794. Vgl. auch OVG NRW, Beschluss vom 19.03.2003, 8 B 2567/02, MMR 2003, 348.

(13) Stadler, MMR 2003, 209, Anm. zu VG Düsseldorf.

(14) VG Köln, Urteil vom 3.03.2005, 6 K 7603/02.

(15) BVerfG, Beschluss vom 18.07.2005, 2 BvF 2/01, BVerfGE 113, 167 ff.

(16) VG Düsseldorf, Urteil vom 10.05.2005, 27 K 5968/02, MMR 2005, 794.

(17) VG Köln, Urteil vom 3.03.2005, 6 K 7603/02, Rn. 73.

(18) Ebenso Schmittmann in: Hoeren/Sieber, Rechtsfragen des elektronischen Geschäftsverkehrs, 9., Rn. 144; Stadler, Sperrungsverfügung gegen Access-Provider, MMR 2002, 343; Rosenkranz, JurPC Web-Dok. 16/2003, Rn. 28. Ebenso zur Sperrungsverfügung gegen einen Host-Provider OVG Sachsen-Anhalt, Beschluss vom 27.07.2005, 1 M 320/05.

(19) OVG Sachsen-Anhalt, Beschluss vom 27.07.2005, 1 M 320/05.

(20) Ebenso Rosenkranz, JurPC Web-Dok. 16/2003, Rn. 28.

(21) „Rumsfeld: Mit Raketen gegen Terroristen“, Focus Online vom 28.06.2006, http://www.focus.de/politik/ausland/rumsfeld_nid_34375.html.