Universität Zürich[UZH]

Rechtswissenschaftliches Institut

Lehrstuhl für Informations- und Kommunikationsrecht
Prof. Dr. Florent Thouvenin
Rämistrasse 74 / 49
CH-8001 Zürich
Telefon +41 44 634 59 97
www.rwi.uzh.ch/thouvenin

Institut für Informatik

Communication Systems Group
Prof. Dr. Burkhard Stiller
Binzmühlestrasse 14
CH-8050 Zürich
Telefon +41 44 635 67 10
www.ifi.uzh.ch

Prof. Dr. Florent Thouvenin
Prof. Dr. Burkhard Stiller

Zürich, 16. September 2016

Gutachten: Netzsperren

A. Vorbemerkungen

Momentan laufen Revisionsprojekte in verschiedenen Rechtsgebieten, in denen die Einführung von Netzsperren in bestimmten Fällen diskutiert wird, so namentlich im Fernmeldegesetz (FMG), im Urheberrechtsgesetz (URG) und im Geldspielgesetz (BGS). In diesem Gutachten wird untersucht, welche technischen Möglichkeiten für Netzsperren zur Verfügung stehen, wie deren Wirksamkeit einzuschätzen ist und ob die Einführung von Netzsperren im Geldspielgesetz aus rechtlicher Sicht als zulässig erscheint.

B. Gegenwärtige Anwendung der Netzsperre

In der Schweiz sind Netzsperren bisher nicht gesetzlich vorgesehen. Es fehlt zudem die Rechtsgrundlage, um Internet Service Provider (ISP) zur Durchsetzung von Netzsperren zu verpflichten[1]. In der Realität werden dem Nutzer jedoch gewisse Inhalte in seinem eigenen Interesse vorenthalten. So werden beispielsweise Spam-Filter eingesetzt, um Nutzer vor unerwünschten oder gefährlichen E-Mails zu schützen. Das einzige koordinierte System von Netzsperren findet sich im Bereich der Kinderpornografie. Die Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) führt eine Liste mit illegalen Angeboten, welche von ISP auf freiwilliger Basis gesperrt werden[2].

C. Verfügbare Arten von Netzsperren

Zur Darstellung der heute bekannten technischen Optionen für Netzsperren werden einleitend die relevanten technischen Grundlagen des Internets skizziert und die aus Sicht der ISP wichtigen Funktionen des Netzwerk-Managements dokumentiert. Basierend auf diesen Grundlagen, zwar vereinfacht, aber auf die entscheidenden Kernfunktionen fokussiert, werden (a) die technischen Realisierungsoptionen von Netzsperren aufgezeigt, (b) deren Gegenmassnahmen beschrieben und (c) eine Bewertung dieses jeweiligen Duopols (expliziter Sperrtyp versus Gegenmassnahme) vorgenommen.

1. Technische Grundlagen

Das Internet operiert auf der Basis von *Paketen* – den *IP-Datagrammen* (Internet Protocol) –, welche eine eindeutige Ziel- und Quelladresse, einige wenige *Steuer- und Kontrollinformationen* und den *Nutzdatenanteil* (Payload) aufweisen. Die Entscheidung, welchen Weg ein IP-Datagramm im Netz vom Sender zum Empfänger nehmen soll, wird durch das *Routing* definiert. Im Prinzip wird dabei auf der Basis der Zieladresse des IP-Datagramms der kürzeste Weg gesucht, auf welchem dieses Datagramm vom Sender zum Empfänger gelangt.

Über Border-Router werden einzelne Netzwerke – technisch-operativ als *Autonome Systeme* (AS) bezeichnet – zusammengeschaltet. Jedes AS unterliegt dabei normalerweise einer eigenständigen

1 Siehe hierzu SCHWARZENEGGER CHRISTIAN, Sperrverfügungen gegen Access-Provider – Über die Zulässigkeit polizeilicher Gefahrenabwehr durch Sperranordnungen im Internet, in: Arter Oliver/Jörg Florian S. (Hrsg.), Internet-Recht und Electronic Commerce Law, 3. Tagungsband, Bern 2003, 249-286, *passim*. Siehe auch RIGAMONTI CYRILL P., Providerhaftung – auf dem Weg zum Urheberverwaltungsrecht?, sic! 2016, 117–134, 128, der auf entsprechende gerichtliche Anordnungen in der EU verweist.

2 WULLSCHLEGER MARC, Die Durchsetzung des Urheberrechts im Internet, Bern 2015, Rz. 449.

administrativen Verwaltung, verwendet aber standardkonforme Protokolle zum Austausch von Routing-Informationen untereinander. Beispielsweise ist ein ISP Inhaber eines AS und mindestens eines Border-Routers.

Vereinfacht kann der Aufbau des Internets – wie in Abb. 1 dargestellt – skizziert werden, indem die drei *Akteure* Endbenutzer, ISP und Anbieter unterschieden werden. Die AS in der skizzierten Wolke repräsentieren ISP, welche für den Transitverkehr verantwortlich sind. Der Endbenutzer ist typischerweise Kunde eines ISP. Der ISP ist an ein oder mehrere alternative AS über Border-Router (vereinfacht als Leitung dargestellt) gekoppelt. Der Anbieter – auch Inhalts- oder Dienstanbieter genannt – ist ebenso an mindestens ein AS angeschlossen.

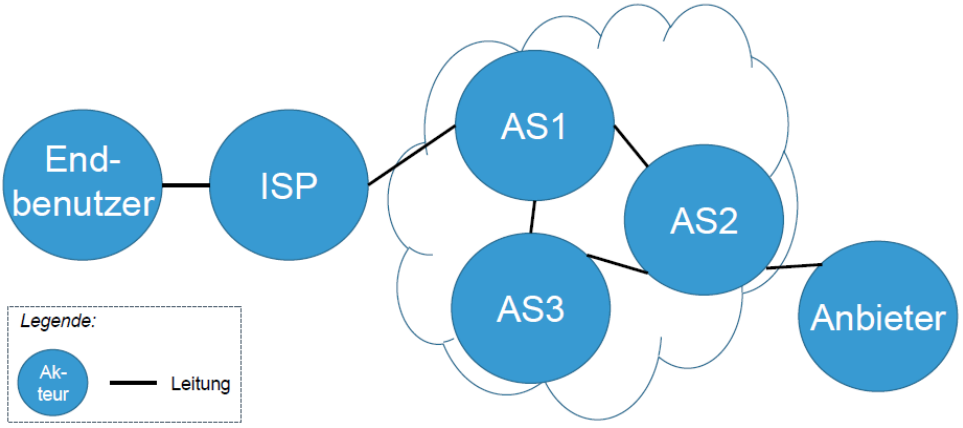

Abb. 1: Vereinfachter Aufbau des Internets anhand der drei wesentlichen Akteure

Aus Sicht einer Anwendung, die zwischen dem Endbenutzer und dem Anbieter eine gewünschte Interaktion herstellt, werden Kommunikationsverbindungen zwischen einem Sender (beispielsweise dem Anbieter) und einem Empfänger (beispielsweise dem Endkunden) durch Protokolle der Transportschicht (unter anderem mittels des Transmission Control Protocols TCP oder des User Datagram Protocols UDP) aufgebaut, um Nutzdaten schnell, zuverlässig oder gesichert zu übertragen. Diese in *Datenströme* zusammengefassten und durch TCP oder UDP transportierten Nutzdaten werden vom Sender in die oben benannten IP-Datagramme als deren Payload integriert und versendet.

Jedes Endsystem, welches am Internet angeschlossen ist (z.B. Laptops, Server oder mobile Geräte), und jedes Zwischensystem im Internet (z.B. Router) verfügen über mindestens eine eindeutige *IP-Adresse*, welche als Ziel- oder Quelladresse in der Kommunikation zwischen den Geräten als eindeutige Kennung verwendet wird. IP-Adressen (z.B. 86.125.22.1) sind eindeutig, aber für den Menschen nicht „einfach“ les- bzw. memorierbar. Aus diesem Grund ist das *Domain Name System* (*DNS*) im Internet definiert worden, um für den Benutzer lesbare Namen (z.B. „www.firmen-name.ch“), als *DNS-Name* bezeichnet, den rein numerischen IP-Adressen zuzuordnen. Dieser Vorgang der Zuordnung des DNS-Namens zu einer IP-Adresse wird als Namensauflösung bezeichnet.

Da die Namensauflösung nicht statisch realisiert werden kann, sondern sich dynamisch ändernden Anforderungen stellen muss, sind die DNS-Server darauf spezialisiert, Anfragen der Art „Welche IP-Adresse muss verwendet werden, um den Server der Firma „firmen-name“ zu finden?“ zu beantworten. Dabei sucht der angefragte DNS-Server in seiner lokalen Datenbank nach einer Namensauflösung bzw. leitet diese Anfrage an andere DNS-Server weiter, wenn der lokale DNS-Server die

Daten nicht in seiner Datenbank hat. Im erfolgreichen Fall meldet der DNS-Server die ermittelte IP-Adresse zurück. Dieser Prozess wird beispielsweise durch einen Web-Browser angestossen, wenn der Uniform Resource Locator (URL) – umgangssprachlich als Web-Adresse bezeichnet – „www.firmen-name.ch“ im Browser angegeben wird, um den Inhalt dieser Web-Seite vom Web-Server der Firma an den Anfragenden zu transportieren und in dessen Web-Browser anzuzeigen.

Die Abb. 2 skizziert vereinfacht einen Server mit IP-Adresse im Internet, die von physikalischen Maschinen (z.B. Servern, Web-Servern oder Dienste-Servern) verwendet wird. Der Server ist über die DNS-Namen „subdomain1.domain1.ch“, domain1.ch“ sowie „domain2.ch“ erreichbar. Diese sind dann explizit mit beispielhaften Ressourcen (gekennzeichnet durch deren DNS-Namen in den Rechtecken: „subdomain1.domain.ch/about“) versehen.

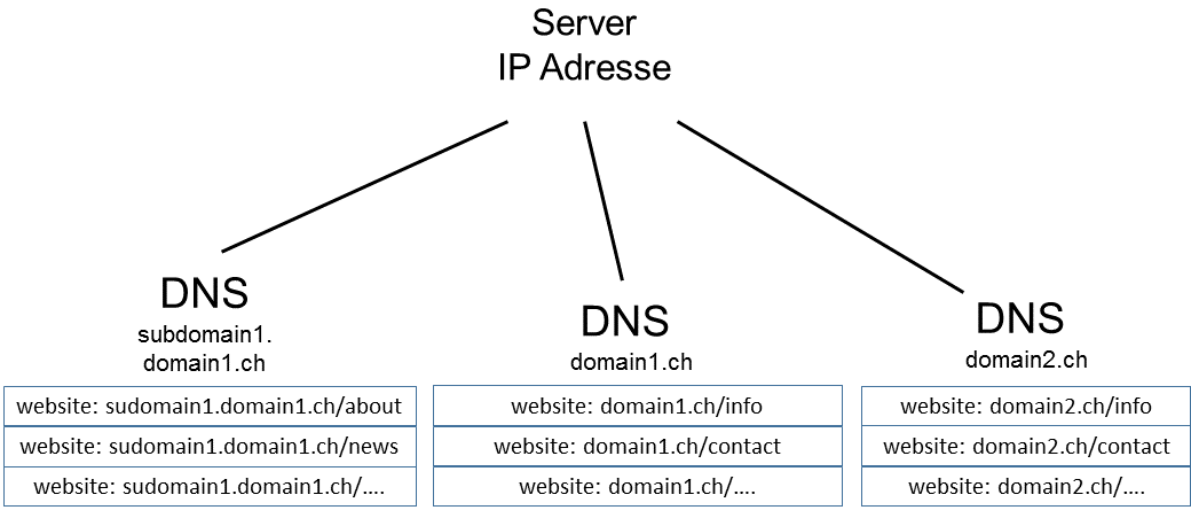

Abb. 2: Vereinfachte Darstellung einer IP-Adresse im Internet und der mit dieser über DNS verknüpften DNS-Namen

2. Netzwerk-Management und Diensterbringung des ISP und durch Dritte

Neben diesen sehr grundlegenden Operationen zur Weiterleitung von IP-Datagrammen innerhalb und zwischen Autonomen Systemen spielt das *Netzwerk-Management* für einen ISP eine wichtige Rolle, um den zuverlässigen Betrieb eines Netzes sicherzustellen. Hierzu sind *Mess- und Monitor-funktionen* im Netzwerk integriert, welche durch nachfolgende (automatisierte) Analyse- und Entscheidungswerkzeuge den Zustand eines Netzwerkes überwachen und interpretieren können. Damit erhält der ISP u.a. einen detaillierten Einblick in den Verkehr, welcher über Border-Router von aussen in das eigene Netz gelangt oder von innen nach aussen weitergeleitet wird.

Neben dieser *Überwachungsmöglichkeit* des Netzverkehrs zum Erreichen eines zuverlässigen Betriebs kann das Netzwerk-Management auch eingesetzt werden, um gewisse Datenströme zu priorisieren. Dies ist aus operativer Sicht im Hochlastfall bedeutend, da damit sichergestellt werden kann, dass die essentiellen Informationen vor den „normalen“ Nutzdatenströmen priorisiert werden können. Andererseits können verschiedene Applikationen Vorrang vor anderen erhalten, um mit notwendigen Dienstgüten (*Quality-of-Service*) die Sicherstellung von essentiellen Anwendungseigenschaften zu erreichen.

Einen weiteren Bereich zur Diensterbringung stellen *Content Distribution Networks* (*CDN*) dar, welche als ein Netz mit typischerweise regional verteilter und über das Internet verbundener Server realisiert ist, mit welchem Inhalte – im Normalfall grosse Daten mit Software- oder Medieninhalten – an registrierte Benutzer oder an definierte Benutzergruppen ausgeliefert werden. Eine dezidierte Art des Überlastschutzes kann CDNs verwenden, indem sie insbesondere in der heutzutage sehr dynamischen Welt von Web-Seiten den Inhalt einer Web-Seite zwischenspeichert. Im gleichen Atemzug können CDNs auch Inhalte an Benutzer ausliefern, deren originärer Bereitstellungsort (definiert über deren DNS-Namen) weder dem ISP, über welche diese Daten transportiert werden, noch dem Benutzer selber bekannt ist oder bekannt sein sollen. Caching-Dienste im Auftrag von diversen Drittdienstanbietern erbringen diese Funktion heutzutage kommerziell.

ISP und Diensteanbieter haben die technische Möglichkeit, *Filter* auf den auszutauschenden Internet-Verkehr anzuwenden. Filter arbeiten beispielsweise auf der Basis der Kontrolldaten der IP-Datagramme, der Protokoll-Identifikatoren von TCP-Kontrolldaten oder auch von Applikationsdaten. Diese im Allgemeinen als *Applikationsfilter* bezeichneten technischen Hilfsmittel erlauben es unter anderem auch, technisch gesehen schädliche Inhalte (wie beispielsweise Würmer, Viren oder Schadsoftware) in transportierten IP-Datagrammen zu erkennen.

Eine Form dieser Filter kann durch Deep Packet Inspection (DPI) realisiert werden, welches im Besonderen die Möglichkeit von detaillierten Paketfiltern bereitstellt, die nach einer Analyse der Nutzdaten eines IP-Datagrammes und beispielsweise dem Prüfen des Inhalts auf gewisse Stichworte eine für diese Interaktion relevante Aktion vornehmen können, beispielsweise das Terminieren einer TCP-Verbindung. DPI kann nur auf unverschlüsselt übertragene Protokolldaten (u.a. TCP, HTTP oder IMAP) und damit auch auf Anfragen an Suchmaschinen angewendet werden.

3. Netzsperren

Netzsperren sollen dazu dienen, „inakzeptable“ Inhalte, wie unter anderem harte Pornografie, Kinderpornografie, terroristische oder extremistische Inhalte, gewaltverherrlichende Inhalte, urheberrechtlich geschützte Inhalte oder illegale Glücksspiele, zu sperren. Im Folgenden werden ausschliesslich die technischen Optionen für Netzsperren aus Sicht der ISP und die rechtlich erlaubten technischen Gegenmassnahmen der Nutzer unabhängig vom konkreten Inhalt oder Inhaltsanbieter dargestellt.

a) Technische Optionen für Netzsperren aus Sicht der ISP

Unter der Annahme, dass sich Netzsperren auf die möglichen Inhalte von Web-Seiten beziehen sollen, welche entweder über deren DNS-Namen oder über IP-Adressen direkt erreichbar sind und welche durch einen ISP potentiell erbracht werden können, ergeben sich die nachfolgend dargestellten technischen Optionen aus Sicht der ISP, diesen Zugriff zu unterbinden. Nicht berücksichtigt werden dabei (a) sehr neue Technologien, die es beispielsweise ermöglichen, elektronische und verteilte Glücksspiele dezentral über sogenannte Blockchains zu realisieren und zu betreiben, da der Zugriff auf die dadurch generierten Datenströme durch einen ISP ohne Verletzung des Fernmeldegeheimnisses (Art. 13 BV und Art. 43 FMG) nicht möglich ist. Ferner werden an dieser Stelle (b) dezidierte Apps nicht berücksichtigt, über die Glücksspiele betrieben werden, da die beiden aktuell grössten Anbieter Google und Apple diese nicht erlauben und ein ISP auch keinen Zugriff auf die in seinem Netz transportierten Daten hat, die durch die Benutzung dieser Apps entstehen. Zusätzlich werden an dieser Stelle (c) auch Suchmaschinen und das (gerichtlich) angeordnete Ver-

bergen gewisser Suchresultate ausgenommen, da durch das benutzerseitige Verwenden einer anderen Suchmaschine, die nicht den anordnenden Behörden im gleichen Rechtsraum unterworfen sind, eben diese Einträge auch gefunden und damit verwendet werden können. Schliesslich sind an dieser Stelle (d) Software und Programme ausgenommen, welche beim Endbenutzer zu installieren wären („Staatstrojaner“).

i) IP-Adresssperren beim ISP

Die IP-Adresssperren erlauben es ISP, nach IP-Adressen in IP-Datagrammen zu filtern, welche als Ziel- oder Quelladresse auf entsprechende Maschinen verweisen, welche illegale Inhalte aufweisen. Meist wird zunächst bekannt sein, dass unter einem bestimmten DNS-Namen mit entsprechender IP-Adresse illegale Inhalte abrufbar sind, für die technische Einrichtung der IP-Sperre ist die Kenntnis der IP-Adresse jedoch ausreichend.

Im Gegensatz zu den DNS-Sperren werden die gesperrten IP-Datagramme durch einen IP-Adressfilter in den Border-Routern typischerweise nicht mehr vom ISP weitergeleitet. Es wird dem ursprünglichen Sender damit keine dezidierte Information über eine Sperrung oder eine illegale Aktivität als Antwort auf seine Anfrage zugestellt. Eine Weiterleitung wäre technisch möglich, sodass unter gewissen Voraussetzungen per „Stop-Schild“ der Benutzer darauf aufmerksam gemacht werden kann, dass er im Begriff ist, eine gesperrte IP-Adresse aufzurufen.

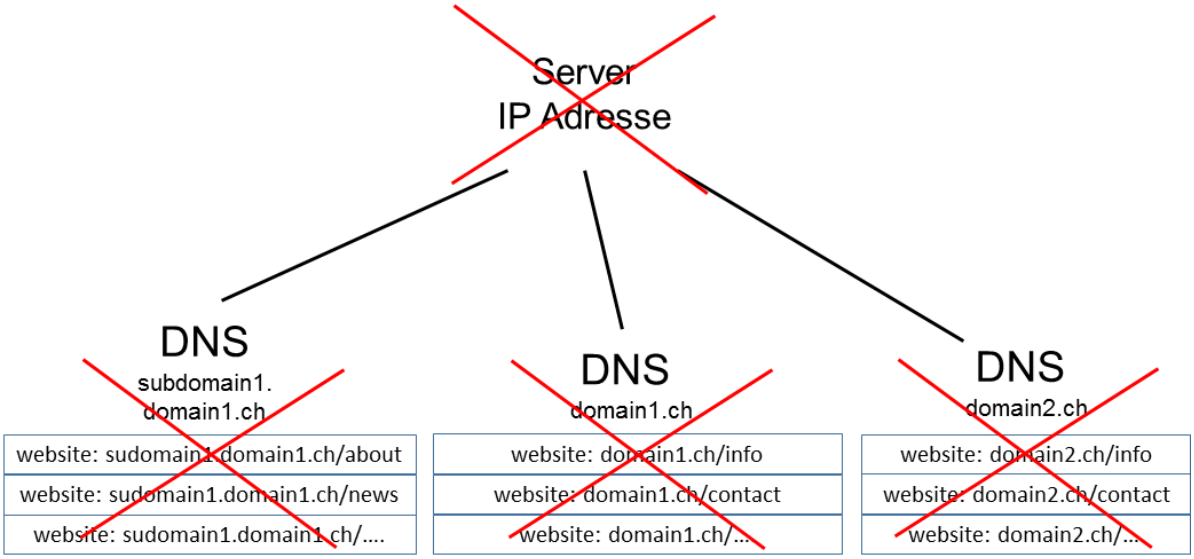

Abb. 3: Vereinfachte Darstellung der nicht mehr erreichbaren Maschinen und Inhalte bei einer IP-Adresssperre. Die roten Kreuze zeigen, welche Maschinen und Inhalte, die durch diese Maschinen verwaltet werden, nach dem Sperren der IP-Adresse nicht mehr erreichbar sein werden.

ii) DNS-Sperren beim ISP

Diese Art der Netzsperren (auch als DNS-Hijacking bezeichnet) greift in den Prozess der Namensauflösung zwischen Anfragendem und DNS-Server des ISP ein, indem alle Anfragen zu einer Seite, beispielsweise „www.illegale-inhalte.ch“, auf eine spezielle Seite umgeleitet werden, welche (a) von einer staatlichen Behörde oder (b) dem ISP, aus dem die Anfrage kam, bereitgestellt oder verwaltet wird, um per „Stop-Schild“ den Benutzer darauf aufmerksam zu machen, dass er im Begriff ist, eine

gesperrte Seite aufzurufen. Diese Sperre betrifft damit genau diese explizit genannte Seite, also exakt den gesamten Inhalt, der unter diesem DNS-Namen, hier also „www.illegale-inhalte.ch“, abgelegt ist. Es ist also und muss damit vorab bekannt sein, dass unter einem bestimmten DNS-Namen illegale Inhalte abrufbar sind, da andernfalls DNS-Sperren nicht definiert werden können. Sollte der Anbieter dieser illegalen Inhalte in der Schweiz registriert sein und eine „.ch“ Top Level Domain verwenden, kann dieser direkt beim schweizerischen DNS-Registrator gelöscht werden.

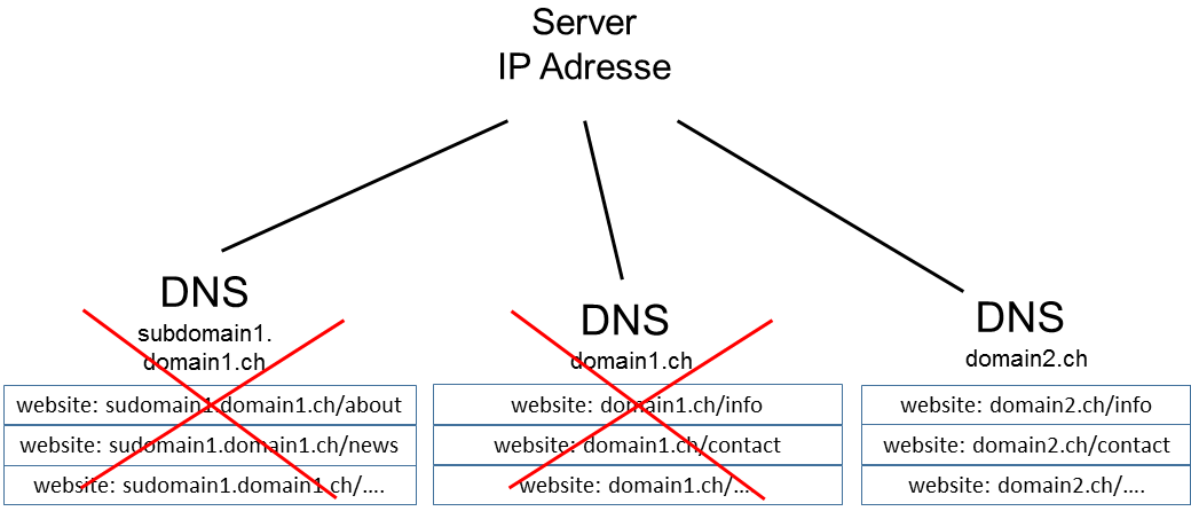

Abb. 4: Vereinfachte Darstellung der nicht mehr erreichbaren Maschinen und Inhalte bei einer DNS-Sperre. Die roten Kreuze zeigen, welche Maschinen und Inhalte, die durch diese Maschinen verwaltet werden, nach dem Sperren eines DNS-Namens (hier „domain1.ch“) nicht mehr erreichbar sind.

iii) Applikationsfilter oder Proxy-Server beim ISP

Wesentlich genauer als DNS-Sperren oder IP-Adresssperren sind Applikationsfilter oder Proxy-Server. Während Applikationsfilter dezidiert auf der Basis der in den IP-Steuer- und Kontrolldaten sowie den in der Payload untergebrachten Daten der Applikation selber (und höherer Protokolle) Datenelemente und Identifikatoren für die illegale Verwendung von Inhalten suchen und erkennen, liefern Proxy-Server direkt keine Daten auf eine Anfrage hin aus, sondern fungieren nur als „weiterleitende Zwischensysteme“, welche quasi im Auftrag des ursprünglich Aufrufenden die ursprüngliche Anfrage weitergeben. Dies kann mit geänderten oder angepassten Quellinformation ebenso geschehen, wie mit den Originaldaten.

Die Funktionalität dieser Proxy-Server ist auch dazu geeignet, anderweitig technisch schädliche Inhalte, wie Malware oder Viren, zu filtern und die Inhalte der Web-Seite bereinigt an den Aufrufer weiterzugeben, was einem typischen Ansatz zur Erhöhung der Sicherheit in Kommunikationsnetzen dient. Ein Beispiel ist das Cleanfeed-Verfahren[3], das die genannten IP-Adresssperren mit den Proxy-Servern kombiniert.

[3] SCHNEIDER ADRIAN, Netzsperren und das Cleanfeed-Verfahren, 2011, <https://www.telemedicus.info/article/2055-Netzsperren-und-das-Cleanfeed-Verfahren.html>.

Schliesslich können durch Applikationsfilter diejenigen IP-Datagramme, welche zu einem bestimmten Datenstrom gehören und mit dem TCP-Protokoll die Anwendung unterstützen, identifiziert werden, welche zu einer spezifischen TCP-Verbindung gehören. Sollte diese durch ein im Filter gesetztes Kriterium den Filter aktivieren, wird diese TCP-Verbindung zurückgesetzt und terminiert (Connection Reset). Ein erneuter Aufbau- und Verbindungsversuch vom gleichen Quellknoten durch den Endbenutzer wird durch einen Zeitgeber für eine bestimmte Zeit auf dem Border-Router unterbunden und damit auf dem Weg ins Internet blockiert.

Eine technische Form der Realisierung dieser Applikationsfilter ist durch das Deep Packet Inspection (DPI) möglich. Eine weitere spezifische Art des Filterns mit DPI stellen URL-Filter dar. Dabei wird die seitens des Endbenutzers gewünschte URL auf das Vorhandensein von Stichwörtern untersucht, unabhängig von der verwendeten Domain.

b) Technische Möglichkeiten zur Umgehung dieser Netzsperren

Bei einer Umsetzung der drei genannten technischen Alternativen zur Sperrung von Inhalten ergeben sich die im Folgenden dargestellten Möglichkeiten, diese Netzsperren technisch oder organisatorisch zu umgehen, ohne dass ein Dritter (beispielsweise Strafverfolgungsbehörden) in der Lage wäre, dies (a) zu erkennen, (b) zu protokollieren und damit nachweisbar zu machen oder (c) gar zu verhindern. Da die drei genannten technischen Alternativen beim ISP eingerichtet werden, können grundsätzlich Endbenutzer oder Anbieter verschiedene Massnahmen ergreifen, um diese Netzsperren zu umgehen.

i) Umgehung von IP-Adresssperren

IP-Adresssperren können technisch umgangen werden, indem

(1) Werkzeuge und Systeme zur Anonymisierung des Quellverkehrs aus Sicht des Aufrufenden eingesetzt werden, beispielsweise Tor[4], welche die Originalanfrage zur gewünschten Ziel-IP-Adresse zufällig auf Netzwerkteilnehmer im verteilten Internet irgendwo in der Welt versenden und ohne Berücksichtigung (und Kenntnis) der aktuellen und tatsächlichen physikalischen Lokation des Benutzers (also deren Zugehörigkeit zu einem speziellen Autonomen System) die erhaltene Antwort samt Inhalt, welche sich nicht im Kontrollbereich der staatlichen Behörde oder des ISP befinden, zurückliefern;

(2) Virtuelle Private Netzwerke (VPN) genutzt werden, typischerweise durch Verschlüsselungstechnologien wie Secure Socket Layer (SSL) oder Secure Shell (SSH) unterstützt, welche dem Benutzer durch private oder berufliche Verbindungen zur Verfügung stehen, die ebenfalls einen Zugriff auf beliebige IP-Adressen aus Sicht einer anderen logischen Lokation heraus erlauben, die sich ausserhalb des Kontrollbereiches der staatlichen Behörde oder des ISP befinden; und indem

(3) weitere Massnahmen eingeleitet werden, wie beispielsweise (1) die Verteilung der Inhalte des Anbieters durch CDNs oder WebRTC (die „Web Real-Time Communication“ oder Web-basierte Echtzeitkommunikation, die als eine Sammlung von Kommunikationsprotokollen und Programmierschnittstellen diese Echtzeitkommunikation über eine direkte Rechner-zu-

[4] Anonymity on-line, Tor, <https://www.torproject.org>.

Rechner-Verbindung für eine Implementierung in Webbrowsern bereitstellt) oder (2) indem mehrere Server des Anbieters – durch verschiedene Virtuelle Maschinen in verschiedenen Ländern realisiert – mit unterschiedlichen IP-Adressen konfiguriert, eingesetzt und publiziert werden.

ii) Umgehung von DNS-Sperren

DNS-Sperren können technisch umgangen werden, indem

(1) für die DNS-Namensauflösung ein DNS-Server verwendet wird, der nicht von einer Organisation betrieben wird, die von der Sperre betroffen ist. Die Wahl eines entsprechenden DNS-Servers aus Sicht eines Endbenutzers erfolgt beispielsweise über den DNS-Server 8.8.8.8, welcher von Google faktisch als „unzensierter" DNS-Server nur Sperren realisiert, die innerhalb derjenigen Jurisdiktion gelten, der Google unterliegt;

(2) der Aufruf des DNS-Servers vollständig vermieden wird und direkt die IP-Adresse des Web-Servers zur Kommunikation verwendet wird; die IP-Adresse kann entweder gemäss (1) ermittelt werden oder wird durch einschlägige Foren oder persönliche Kommunikation weitergegeben;

(3) Werkzeuge und Systeme zur Anonymisierung des Quellverkehrs aus Sicht des Aufrufenden eingesetzt werden, beispielsweise Tor[5], welche die Originalanfrage zur DNS-Namensauflösung zufällig auf Netzwerkteilnehmer im verteilten Internet irgendwo in der Welt versenden und ohne Berücksichtigung (und Kenntnis) der aktuellen und tatsächlichen physikalischen Lokation des Benutzers (also deren Zugehörigkeit zu einem speziellen Autonomen System) eine Namensauflösung durchführt, welche sich nicht im Kontrollbereich der staatlichen Behörde oder des ISP befindet;

(4) Einwahlmöglichkeiten in Virtuelle Private Netzwerke (VPN) eingesetzt werden, typischerweise durch Verschlüsselungstechnologien wie Secure Socket Layer (SSL) oder Secure Shell (SSH) unterstützt, welche dem Benutzer durch private oder berufliche Verbindungen zur Verfügung stehen, die ebenfalls den Zugriff auf DNS-Server erlauben, die sich ausserhalb des Kontrollbereiches der staatlichen Behörde oder des ISP befinden;

(5) ein vom Benutzer selber betriebener DNS-Server verwendet wird; und

iii) Umgehung von Applikationsfiltern oder Proxy-Servern

Applikationsfilter können technisch umgangen werden, indem

(1) die typischerweise bekannten Kriterien der Filter durch Anpassungen des Sendeverhaltens bzw. der regelmässigen Veränderung der Dateinamen, Inhalte und Adressen durch den Inhaltsanbieter zu keinem Anschlagen des Filters mehr führt;

5 Anonymity on-line, Tor, <https://www.torproject.org>.

(2) das Erlernen der aktuellen Kriterien durch vorab (kurz- oder mittelfristig) gestartete Test- und Versuchsdatensendungen bzw. Anfragen zu einer Anpassung der Konfiguration auf der Inhaltsanbieterseite führt;

(3) aus Inhaltsanbietersicht der DNS-Name samt der verwendeten IP-Adresse(n) wiederkehrend und in unregelmässigen Zeitabständen gewechselt werden;

(4) verschlüsselte Übertragungen eingesetzt werden, unter anderem in Form von VPNs, SSL oder TLS; und indem

(5) in den speziellen URL-Filteransätzen einzelne oder Gruppen von Buchstaben, welche die URL trägt, „kodiert" werden. Dieses Kodieren (Escapen) stellt beispielsweise jedem zweiten Buchstaben ein Zeichen voran, welches auf der Empfängerseite per Grundregel immer herausgenommen wird. Selbstverständlich erlaubt der Einsatz von Verschlüsselungstechnologien auch, URL-Filter zu umgehen, da diese gar nicht erkannt werden.

Proxy-Server können technisch umgangen werden, indem

(1) eigene Proxy-Server aufgesetzt oder im Internet gefunden werden, welche das Laden und Zurückgeben der ursprünglich angefragten Inhalte über unverfängliche Verbindungen erlauben;

(2) Transport Layer Security (TLS) oder Secure Socket Layer (SSL) Verschlüsselung verwendet wird;

(3) Werkzeuge und Systeme zur Anonymisierung des Quellverkehrs aus Sicht des Aufrufenden eingesetzt werden, beispielsweise Tor[6];

(4) Einwahlmöglichkeiten in Virtuelle Private Netzwerke (VPN) eingesetzt werden;

(5) im Falle des Blockierens von TCP-Verbindungen beide Kommunikationsteilnehmer – also der Endbenutzer und der Anbieter – im Speziellen das im TCP-Protokoll definierte TCP-RESET-Paket ignorieren, welches typischerweise unter Anwendung von Spoofing-Methoden durch den ISP von dem Applikationsfelder auf einen Border-Router versandt wird, um die Blockierung seitens des ISP initial zu erreichen; und indem

(6) in weiteren Fällen ein Proxy-Server einen Web-Server simuliert und damit keine eigenen Daten ausliefert, sondern die entsprechende Web-Seite selbst ausliest und weitergibt. Die Anfrage an den Proxy-Server, der die Anfrage in der sehr dynamischen Welt von Web-Seiten entgegennimmt, kann den Inhalt einer Web-Seite zwischenspeichern, um ihn im Nachgang an eine andere, den IP-Adressfilter oder die DNS-Sperre umgehende Lokation – hier den ursprünglichen Anfrageort – weiterzugeben. Die genannten CDNs sowie die kommerziell angebotenen Caching-Dienste können damit durch einen Proxy-Server als auch einen Applikationsfilter eines ISP nicht erkannt werden, weil diese IP-Adressen in den IP-Datagrammen verwenden, die nicht gesperrt werden können.

6 Anonymity on-line, Tor, <https://www.torproject.org>.

c) Bewertung der Wirksamkeit dieser Netzsperren

Unter Berücksichtigung der heute technisch realisierbaren Ansätze für Netzsperren und der Alternativen zu deren Umgehung wird die Wirksamkeit von Netzsperren wie nachfolgend ausgeführt bewertet. Dabei wird der Fokus nicht auf den technisch versierten Endbenutzer, für den das Umgehen der Netzsperren kaum ein technisches Problem darstellt, gelegt, sondern es wird die Wirksamkeit dieser Sperren speziell für den Fall eines technisch nicht versierten Endbenutzers untersucht. Dabei wird sich zeigen, dass Netzsperren im Allgemeinen nicht zum gewünschten Ergebnis führen.

i) Wirksamkeit von IP-Adresssperren

IP-Adresssperren können mit minimalen technischen Kenntnissen umgangen werden, da die oben beschriebenen Umgehungsmethoden heutzutage standardmässig in Form von Werkzeugen auf faktisch allen Rechnern verfügbar sind. IP-Sperren sind zwar etwas schwieriger zu umgehen als DNS-Sperren, da im Gegensatz zu DNS-Sperren ein anderer DNS-Server nicht weiterhilft. Jedoch können ohne detaillierte technische Kenntnisse VPN oder Tor verwendet werden. IP-Adresssperren erscheinen damit als faktisch unwirksam, da sie mit minimalem Aufwand und mit kleinstem technischem Wissen umgangen werden können.

IP-Adresssperren haben zudem den Nachteil, dass sie Kollateralschäden verursachen können: Da unter einer IP-Adresse sehr viele Web-Seiten abrufbar sein können (beispielsweise bei einem kommerziellen Web-Hoster, der verschiedene Kunden bedient), wäre mit der Sperrung einer IP-Adresse unter Umständen auch eine gewisse Anzahl rechtlich unbedenklicher Web-Seiten von einer Sperrung betroffen.

ii) Wirksamkeit von DNS-Sperren

DNS-Sperren können mit minimalen technischen Kenntnissen mittels der oben genannten Methoden umgangen werden. So können manuell DNS-Server aus Sicht eines Anwenders angewählt werden (z.B. 8.8.8.8), um die DNS-Namensauflösung auszuführen (wie in Abb. 5 dargestellt). Auch lassen sich über Skript-Files oder Registry-Editoren (semi-)automatisiert vordefinierte Einträge von DNS-Servern ändern. Anleitungen, wie der DNS-Server in die lokale Rechnerkonfiguration eingetragen und definiert werden kann oder wie Proxy-Server aufzusetzen sind, sind im Internet öffentlich und leicht verständlich verfügbar. Damit sind auch DNS-Sperren faktisch unwirksam, weil sie mit sehr geringem Aufwand und fast ohne technisches Wissen umgangen werden können.

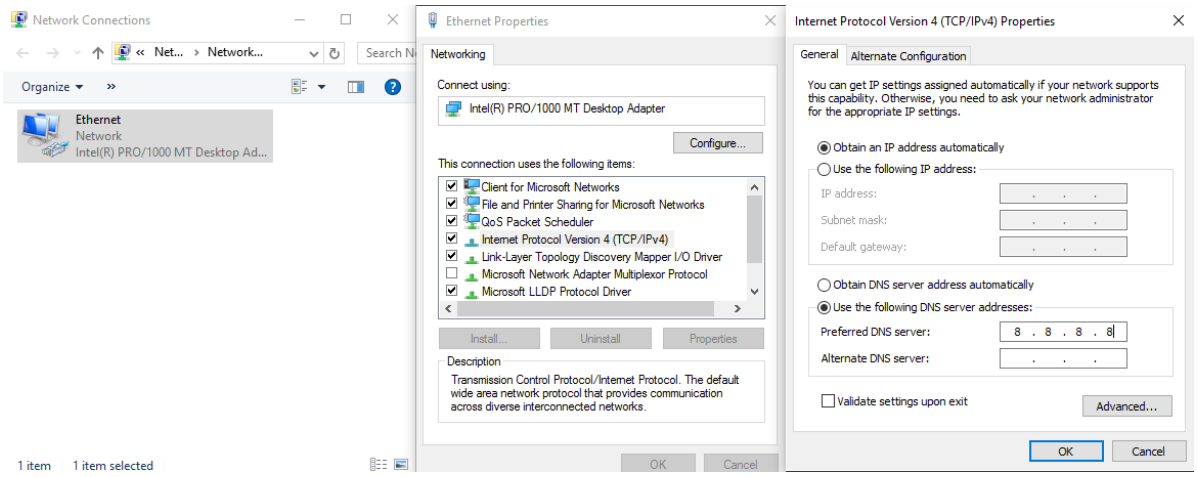

Abb. 5: Beispiel, wie man unter Windows 10 eine DNS-Sperre umgehen kann.

Auch die Anwendung von DNS-Filtern, welche sehr generisch sein können, kann zu unerwünschten Kollateralschäden führen. Beispielsweise führt die Blockierung derjenigen DNS-Namen, welche die Zeichenfolge „sex“ beinhalten, auch zur Blockierung eines DNS-Namens, welcher das Wort „betriebsextern“ aufweist.

iii) Wirksamkeit von Applikationsfiltern oder Proxy-Servern

Jedwede Filtertechnik ist nur so gut, wie sie sich in der Definition der gewünschten Kriterien darstellt. Da sowohl die Kriterien als auch das Erlernen neuer Werte dieser Kriterien (semi-)automatisiert erkannt bzw. extern beeinflusst werden kann, sowohl vom Anbieter als auch vom ISP, wird es keinen länger andauernden „stabilen“ Zustand zwischen diesen beiden Akteuren geben. Zudem muss bei einem Filter die gesamte Payload in einem IP-Datagramm überprüft werden, was mit heutiger Technik ohne geeignete Methoden zum Ermitteln gültiger Stichproben praktisch nicht möglich ist.

Damit sind Applikationsfilter oder Proxy-Server nur kurzfristig wirksam, da sich die Anbieter illegaler Inhalte kontinuierlich „bewegen“ und ISP ohne Garantie einer Dienstleistung immer nur nach dem Anwenden von Monitoring-Techniken des Netzwerk-Managements „nachziehen“ können. Im Sinne eines Katz-und-Maus-Spiels wird es in einer nach oben offenen Spirale der Anpassungen enden.

Beim Blockieren von TCP-Verbindungen kann es zu Kollateralschäden kommen, da auch Web-Seiten, die nicht blockiert werden sollen, jedoch auf demselben Zielrechner des Anbieters zur Verfügung gestellt werden, durch dieses Vorgehen nicht mehr erreichbar sind.

Da zusätzlich die Zahl von verschlüsselten Web-Seiten, auf welche nur über „https“ zugegriffen werden kann, steigt, sind Applikationsfilter und Proxy-Server ebenfalls praktisch wirkungslos.

D. Das Revisionsvorhaben

Die Geldspiele sind heute im Spielbankengesetz (SBG) und im Bundesgesetz betreffend die Lotterien und die gewerbsmässigen Wetten (LG) geregelt. Das neue Geldspielgesetz führt diese beiden Erlasse in einem Bundesgesetz zusammen und soll eine kohärente sowie zweck- und zeitgemässe Regelung des Geldspiels in der Schweiz schaffen.

Gemäss der Botschaft besteht der primäre Gesetzeszweck im Schutz der Spieler vor exzessivem Geldspiel[7]. Daneben soll das Gesetz der Bekämpfung der illegalen Spielangebote und der Kriminalität im Zusammenhang mit Geldspielen dienen[8]. Ferner bezweckt das Geldspielgesetz die Generierung von Erträgen für das Gemeinwesen[9].

Wie bis anhin benötigen die Spielbanken für ihren Betrieb eine Konzession und unterstehen der Bundesaufsicht. Dieses System soll die Einhaltung der gesetzlichen Anforderungen sicherstellen. Das Problem ist, dass heute ein grosser Teil der illegalen Spiele in der Schweiz auf Websites stattfindet, die von ausländischen Betreibern auf Servern im Ausland betrieben werden. Damit stehen der Anwendung des schweizerischen Rechts oft rechtliche und praktische Hindernisse entgegen. Diese Probleme bestehen nicht bei Websites, die in der Schweiz betrieben werden.

Netzsperren im Bereich von Geldspielen werden teilweise mit dem Argument abgelehnt, dass den Schweizer Anbietern damit ein Heimatschutz gewährt werde. Ein gewisser Schutz ist nicht abzustreiten, da lediglich schweizerische Aktiengesellschaften überhaupt eine Konzession erhalten können. Allerdings ist dieser Argumentation entgegenzuhalten, dass Schweizer Anbieter für die Erteilung einer Konzession verschiedene Voraussetzungen erfüllen müssen, welche den Schutz der Kunden sicherstellen sollen. Zu beachten ist, dass Geldspielanbieter im Online-Markt weltweiter Konkurrenz ausgesetzt sind, welche die Konzessionsvoraussetzungen nicht erfüllen müssen. Die Überlegung, ausländische Anbieter vom Schweizer Markt auszuschliessen, erscheint deshalb grundsätzlich sinnvoll, um sicherzustellen, dass der Konzessionszweck erfüllt werden kann. Es stellt sich aber die Frage, mit welchem Mittel dies erreicht werden kann und soll.

Der Gesetzesentwurf sieht in Art. 84 E-BGS im Wesentlichen vor, schwarze Listen nicht bewilligter Angebote einzuführen, die in der Folge von Fernmeldedienstanbietern (in ihrer Rolle als Internetzugangsprovider) gesperrt werden müssen. Die Listen sollen von den Aufsichtsbehörden regelmässig auf den neuesten Stand gebracht werden und möglichst genaue Angaben zu den betreffenden Angeboten enthalten, damit die Fernmeldedienstanbieterinnen diese ohne weitere Nachforschungen sperren können. Es ist momentan vorgesehen, dass die Liste vor allem Domain-Namen enthält. Es wurde aber nicht ausgeschlossen, dass sich dies abhängig vom technischen Fortschritt ändern kann.

E. Verhältnismässigkeit der vorgesehenen Netzsperren

Der Grundsatz der Verhältnismässigkeit ist ein allgemeiner Rechtsgrundsatz[10], der sowohl für die Rechtsetzung als auch für die Rechtsanwendung gilt[11]. Auch das Parlament als rechtsetzendes

7 Botschaft zum Geldspielgesetz vom 21. Oktober 2015, BBl 2015 8387 ff., 8406; vgl. Art. 2 lit. a E-BGS.

8 Botschaft BGS (Fn. 7), 8406; vgl. Art. 2 lit. b E-BGS

9 Botschaft BGS (Fn. 7), 8406; vgl. Art. 2 lit. c & d E-BGS.

10 KIENER REGINA/KÄLIN WALTER, Grundrechte, 2. Aufl., Bern 2013, 119.

Organ ist an diesen Grundsatz gebunden[12]. Dieses Prinzip setzt dem staatlichen Handeln (selbst bei Verfolgung legitimer öffentlicher Interessen) Grenzen, wenn eine unverhältnismässig starke Beeinträchtigung des Einzelnen bewirkt wird[13].

Eine Massnahme ist verhältnismässig, wenn sie zur Erreichung des verfolgten Zwecks geeignet, erforderlich und zumutbar (Verhältnismässigkeit im engeren Sinn) ist[14]. Diese drei Kriterien müssen kumulativ erfüllt sein[15]. Nachfolgend ist zu prüfen, ob Netzsperren diese Kriterien erfüllen.

1. Eignung

Eine Massnahme muss zunächst geeignet sein, einen Beitrag zur Erreichung des verfolgten Ziels zu leisten[16]. Es reicht bereits aus, wenn die Massnahme in Bezug auf das verfolgte Ziel nicht wirkungslos oder gar kontraproduktiv ist[17].

Wie aufgezeigt, lassen sich die zurzeit verfügbaren technischen Möglichkeiten der Netzsperren relativ einfach ohne vertieftes technisches Wissen umgehen (siehe dazu vorne, S. 8 ff.). Zur Beurteilung der Wirksamkeit stellt sich jedoch die Frage, ob solche Umgehungsmöglichkeiten in der Realität tatsächlich genutzt werden. Für einen Nutzer stellt sich im Einzelfall die Frage, ob sich der Umgehungsaufwand im Verhältnis zum erwarteten subjektiven Nutzen lohnt. Diese Frage lässt sich nicht pauschal beantworten. Auf der Aufwandseite ist zu beachten, wie gross der Umgehungsaufwand für einen Nutzer ist, wobei insbesondere dessen technisches Wissen entscheidend sein dürfte. Auf der Nutzenseite können verschiedene Faktoren eine Rolle spielen, entscheidend ist aber das subjektive Bedürfnis des Nutzers nach dem betreffenden Inhalt.

Netzsperren im Bereich von nichtkonzessionierten Geldspielangeboten bezwecken den Schutz des Schweizer Konsumenten, einerseits vor der eigenen Sucht und andererseits vor unsicheren Spielangeboten (Betrug, Illiquidität des Anbieters). Im Falle einer Geldspielsucht ist das Verlangen nach Geldspielen als hoch einzuschätzen und es erscheint deshalb wahrscheinlich, dass Betroffene die kleinen Hürden zur Umgehung von Netzsperren überwinden werden. Die Wirksamkeit von Netzsperren ist bei Süchtigen deshalb wohl beschränkt.

Bei Spielern mit unauffälligem Spielverhalten ist zu differenzieren. Gewisse Nutzer (insb. die bestehenden Kunden) wählen das nicht konzessionierte Geldspielangebot bewusst. Gründe dafür können u.a. sein, dass das Angebot grösser ist, die Gewinnmöglichkeiten höher sind, die Möglichkeit, sich mit der internationalen Konkurrenz zu messen, oder ein Restguthaben bei einem Anbieter be-

---

11 HÄFELIN ULRICH/MÜLLER GEORG/UHLMANN FELIX, Allgemeines Verwaltungsrecht, 7. Aufl., Zürich/St.Gallen 2016, N 520; KIENER/KÄLIN (Fn. 10), 119.

12 So explizit HOFSTETTER DAVID, Das Verhältnismässigkeitsprinzip als Grundsatz rechtsstaatlichen Handelns (Art. 5 Abs. 2 BV), Zürich 2014, Rz. 218.

13 KIENER/KÄLIN (Fn. 10), 119.

14 BGE 141 I 20, 32, E. 6.2.1; BGE 140 I 353, 373 f., E. 8.7; BGE 140 I 168, 173, E. 4.2.1; BGE 136 IV 97, 104, E. 5.2.2; HÄFELIN/MÜLLER/UHLMANN (Fn. 11), N 514; MÜLLER MARKUS, Verhältnismässigkeit: Gedanken zu einem Zauberwürfel, Bern 2013, 29; HÄFELIN ULRICH/HALLER WALTER/KELLER HELEN, Schweizerisches Bundesstaatsrecht, 8. Aufl., Zürich/Basel/Genf 2012, 320.

15 HÄFELIN/HALLER/KELLER (Fn. 14), 320; HÄFELIN/MÜLLER/UHLMANN (Fn. 11), N 521.

16 HÄFELIN/MÜLLER/UHLMANN (Fn. 11), N 522; MÜLLER (Fn. 14), 29; HOFSTETTER (Fn. 12), Rz. 235.

17 KIENER/KÄLIN (Fn. 10), 120; MÜLLER (Fn. 14), 29.

steht. Bei solchen Spielern ist die Wahrscheinlichkeit ebenfalls gross, dass sie die Möglichkeiten zur Umgehung der Netzsperren nutzen werden. Allerdings ist bei solchen Spielern wohl grundsätzlich von besseren Kenntnissen über die verschiedenen Anbieter auszugehen, weshalb sie einem kleineren Betrugsrisiko ausgesetzt sind als weniger erfahrene Spieler oder Neueinsteiger.

Anders gestaltet sich die Situation u.U. bei Neueinsteigern oder wenig erfahrenen Nutzern von Geldspielangeboten, welche nicht ein bestimmtes Angebot nutzen wollen und für die eine Substituierbarkeit durch in der Schweiz konzessionierte Anbieter angenommen werden kann. Bei diesen Spielern besteht die Möglichkeit, dass sie durch Empfehlung, Werbung oder Websuche möglicherweise zufällig auf ausländischen Portalen landen, welche keine Gewähr für eine einwandfreie und unabhängige Führung der Geschäfte der Spielbank bieten. In diesem Bereich kann eine (gewisse) positive Wirkung der Netzsperren angenommen werden.

Zudem werden Geldspielanbieter mit betrügerischen Absichten ihren Domainnamen und ihre IP-Adresse häufiger wechseln als die etablierten vertrauenswürdigen ausländischen Anbieter, weshalb die Effektivität der Sperren gerade für die besonders problematischen Angebote tiefer ausfallen dürfte. Insbesondere für unerfahrene Spieler könnte sich die Wahrscheinlichkeit erhöhen, dass sie auf betrügerischen Geldspielseiten landen.

Netzsperren können somit für den Schutz der Konsumenten sowie die Generierung von Erträgen für das Gemeinwesen geeignet sein, indem sie unerfahrene Nutzer, welche den Geldspielanbieter nicht gezielt auswählen, davon abhalten können, ausländische Geldspielangebote zu nutzen. Nicht geeignet scheinen Netzsperren hingegen für sämtliche (auch unerfahrene) Nutzer, welche ein ganz bestimmtes ausländisches Geldspielangebot nutzen wollen (beispielsweise aufgrund einer Spielsperre in der Schweiz, des grösseren Angebots, höherer Jackpots oder eines bestehenden Restguthabens). Die Massnahme dürfte also gerade bei denjenigen Nutzern kaum Wirkung zeigen, bei denen das grösste Verlangen nach Geldspielen und entsprechend das höchste Gefährdungspotential besteht.

2. Erforderlichkeit

Die Massnahmen müssen für das Erreichen des angestrebten Ziels erforderlich sein. Massnahmen erfüllen die Voraussetzung der Erforderlichkeit nicht, wenn das Ziel mit einem gleichermassen geeigneten aber milderen Mittel ebenso gut erreicht werden kann[18]. Es ist somit zu prüfen, ob überhaupt weitere gleichermassen geeignete Massnahmen zur Verfügung stehen und, falls ja, ob diese zu einem geringeren Eingriff für die Betroffenen führt. Sicherzustellen ist somit, dass die Massnahme in sachlicher, räumlicher, zeitlicher und personeller Hinsicht nicht über das Notwendige hinausgeht[19].

Unerfahrene Nutzer, bei denen die Netzsperren eine gewisse Wirkung erzielen dürften, sind primär deshalb gefährdet, weil sie sich der Gefahren gewisser Geldspielangebote nicht bewusst sind. Der Gesetzesentwurf sieht denn auch vor, dass Nutzer, welche eine gesperrte Seite aufzurufen versuchen, auf eine Informationsseite der ESBK weitergeleitet werden (Art. 87 E-BGS). Sollte sich ein Nutzer dennoch entscheiden, auf die gesperrte Seite zuzugreifen, wäre eine allfällige Sperre, wie aufgezeigt, leicht zu umgehen. Eine Sperre erscheint somit für das Erreichen des Gesetzeszwecks nicht erforderlich.

18 BGE 140 I 353, 373 f., E. 8.7; BGE 137 I 31, 53, E. 7.5.2; BGE 136 I 87, 92, E. 3.2; BGE 133 I 77, 81, E. 4.1; KIENER/KÄLIN (Fn. 10), 121; HÄFELIN/MÜLLER/UHLMANN (Fn. 11), N 527; HOFSTETTER (Fn. 12), Rz. 251.

19 BGE 142 I 49, 69, E. 9.1 m.w.H.; HÄFELIN/MÜLLER/UHLMANN (Fn. 11), N 530; KIENER/KÄLIN (Fn. 10), 121.

Einige alternative Massnahmen scheitern daran, dass das Gesetz nur das Anbieten von Geldspielen, jedoch nicht deren Nutzung durch die Spieler sanktioniert oder dass die Geldspiele aus Ländern angeboten werden, in denen diese legal und teilweise gar konzessioniert sind, weshalb Rechtshilfeersuchen regelmässig scheitern dürften. Weitere technische Massnahmen, wie z.B. das Sperren von Suchtreffern in den Resultaten von Suchmaschinen, wären zudem wirkungslos (siehe dazu vorne, S. 5 f.).

Als weitere Alternative könnte geprüft werden, ob anstelle des Datenflusses nicht eher die Finanzströme zu unterbinden wären, wie dies der Unlawful Internet Gambling Enforcement Act (UIGEA) in den USA vorsieht. Finanzintermediäre könnten verpflichtet werden, keine Zahlungen an ausländische Geldspielanbieter auszuführen. Zahlungen über Schweizer Kreditkarten könnten zwar auf diese Weise grösstenteils verhindert werden, Zahlungen über e-Wallets (bspw. Paypal) wären allerdings weiterhin nicht kontrollierbar. Eine solche Massnahme ist deshalb ebenfalls nur punktuell wirksam und leicht zu umgehen.

Auch wenn heute wohl eine Rechtsgrundlage fehlt, damit Netzsperren gerichtlich verfügt werden können[20], steht einer freiwilligen Umsetzung nichts entgegen. Dies insbesondere auch, da das Prinzip der Netzneutralität in der Schweiz (bisher) nicht gesetzlich verankert ist. Den ISP steht es somit offen, ihre Kunden vor gefährlichen betrügerischen Angeboten zu schützen, wovon sie bereits heute Gebrauch machen. Es wäre somit möglich, den ISP eine Liste mit betrügerischen Geldspielangeboten im Sinne einer Empfehlung bereitzustellen, welche auf freiwilliger Basis gesperrt werden könnten. Auch insofern erscheint eine gesetzliche Regelung von Netzsperren nicht erforderlich.

3. Zumutbarkeit

Die dritte Voraussetzung des Verhältnismässigkeitsprinzips bedingt, dass die Massnahme dem Einzelnen zumutbar ist[21]. Es ist eine Abwägung vorzunehmen zwischen den öffentlichen Interessen an der Massnahme einerseits und den privaten Interessen der dadurch Betroffenen andererseits. Die Zumutbarkeit ist nur zu bejahen, wenn ein die privaten Interessen überwiegendes öffentliches Interesse besteht[22].

Netzsperren können je nach Anwendungsbereich zu einem Eingriff in die persönliche Freiheit, in die Meinungs- und Informationsfreiheit, in die Medien-, Wissenschafts- und Kunstfreiheit und in die Wirtschaftsfreiheit führen. Bei der Regelung von Netzsperren im Geldspielgesetz stehen besonders die persönliche Freiheit der Internet-Nutzer und die Wirtschaftsfreiheit der Website-Betreiber und der ISP im Vordergrund.

Sollten Dienstanbieter tatsächlich zur Einführung von Netzsperren verpflichtet werden, so müssten diese wohl für die entstehenden Kosten, insbesondere für technische Einrichtungen und Personalaufwand, angemessen entschädigt werden.

Die meisten Geldspielangebote dürften über einen separaten Domainnamen verfügen, weshalb die Risiken für ein Overblocking im Falle einer korrekten Eintragung der DNS-Sperre in diesem Anwen-

20 SCHWARZENEGGER (Fn. 1), 281. Siehe auch RIGAMONTI (Fn. 1), 128, der auf entsprechende gerichtliche Anordnungen in der EU verweist.

21 KIENER/KÄLIN (Fn. 10), 121; MÜLLER (Fn. 14), 30 f.

22 HÄFELIN/MÜLLER/UHLMANN (Fn. 11), N 556 f.; KIENER/KÄLIN (Fn. 10), 123 HÄFELIN/HALLER/KELLER (Fn. 14), 323.

dungsbereich relativ klein sein dürften. Wie aufgezeigt, lässt sich eine DNS-Sperre aber bereits durch die Eingabe der IP-Adresse oder eine einzige Browsereinstellung umgehen (siehe dazu vorne, S. 9 & 11 f.).

Im Vergleich zu DNS-Sperren ist die Umgehung von IP-Sperren zwar mit etwas mehr Aufwand verbunden, derartige Sperren führen jedoch zu einem stark erhöhten Overblocking-Risiko[23]. Rechtmässige Inhalte von anderen unbeteiligten Anbietern, welche über die gleiche IP-Adresse abrufbar sind, werden dabei ebenfalls gesperrt. Nicht ausgeschlossen sind zudem auch Eintragungsfehler bei der Einrichtung von Netzsperren durch menschliches Versagen. Die mit Netzsperren verfolgten Ziele vermögen die Verletzung der Wirtschaftsfreiheit von Unbeteiligten nicht zu rechtfertigen.

Weiter ist auch nicht vorgesehen, dass die von der Sperre betroffenen Website-Betreiber über die Sperre informiert werden, womit diese kaum eine Möglichkeit haben, die Sperre selbst zu entdecken und dagegen vorzugehen. Derartige Beschränkungen können innert kurzer Zeit zu erheblichen Ertragsausfällen bei den Betroffenen führen und die Wirtschaftsfreiheit der Betroffenen einschränken.

Unter illegalen Geldspielen werden nicht nur Angebote mit betrügerischen Absichten erfasst, sondern sämtliche Geldspielangebote im Internet ohne schweizerische Konzession. Gesperrt werden also auch sämtliche Anbieter, welche im Ausland die nötigen Voraussetzungen erfüllen. Nicht konzessionierte Anbieter sind nicht per se unsicher. Aus Konsumentensicht erscheint es im Hinblick auf die persönliche Freiheit entsprechend unnötig, das Angebot übermässig einzuschränken, sofern im Einzelfall keine Gefährdung vorliegt.

Letztlich darf nicht ausser Acht gelassen werden, dass die Nutzung nicht konzessionierter Geldspielangebote durch die Spieler erlaubt ist. Hier besteht ein durchaus relevanter Unterschied zu anderen Bereichen, in denen die Einführung von Netzsperren ebenfalls in Betracht gezogen wird. Netzsperren könnten möglicherweise als zumutbar qualifiziert werden, wenn kein schutzwürdiges Interesse am Zugang zu den gesperrten Inhalten besteht, weil die Inhalte selbst mit den Vorgaben der Rechtsordnung kollidieren, wie beispielsweise bei harter Pornografie. Im Bereich des Geldspiels kann dies bei Spielern mit problematischem Spielverhalten der Fall sein, wenn man diese Spieler vor sich selbst schützen will. Umgekehrt erscheinen Netzsperren unter dem Gesichtspunkt der persönlichen Freiheit aber insgesamt dennoch als unzumutbar, weil Nutzer ohne auffälliges Spielverhalten ebenfalls von der Sperre betroffen sind.

4. Ergebnis der Verhältnismässigkeitsprüfung

Die Verhältnismässigkeitsprüfung zeigt, dass Netzsperren wohl nicht das richtige Mittel zur Erreichung der damit verfolgten Ziele sind. Netzsperren können mit kleinstem technischem Wissen umgangen werden und in jenen Bereichen, in denen kaum mit einer Umgehung zu rechnen ist, stehen mit der Weiterleitung auf Informationsseiten mildere Mittel zur Verfügung, welche die gleiche Wirkung erzielen dürften. Dies gilt grundsätzlich für IP- ebenso wie für DNS-Sperren. Im Bereich des Geldspiels sind DNS-Sperren angesichts der Overblocking-Risiken letztlich zwar das weit weniger problematische Mittel, sie sind aber noch weniger wirksam als die ebenfalls relativ leicht zu umgehenden IP-Sperren.

[23] So auch die ESBK, Überprüfung der Lockerung des Verbots der telekommunikationsgestützten Durchführung von Glücksspielen, Bericht vom 31. März 2009, 21.

F. Fazit

Die heute verfügbaren technischen Möglichkeiten der Netzsperren lassen sich ohne grossen Aufwand und mit bescheidenem technischem Wissen umgehen, da die dazu erforderlichen „Werkzeuge“ für jedes Endgerät verfügbar sind und ohne weiteres im Internet gefunden werden können. Netzsperren sind damit auch für technisch wenig versierte Nutzer faktisch unwirksam. Aus rechtlicher Sicht ist die Eignung von Netzsperren zur Erreichung der vom Gesetzgeber verfolgten Ziele deshalb äusserst fraglich. Problematisch sind Netzsperren vor allem auch, weil ein Overblocking in der Regel nicht ausgeschlossen werden kann.

Mit Blick auf den geringen Nutzen und die mit Netzsperren verbundenen Eingriffe in Grundrechte erscheint die Einführung von Netzsperren als problematisch. Hinzu kommt, dass die Glaubwürdigkeit der Rechtsordnung Schaden nehmen kann, wenn sie sich zur Rechtsdurchsetzung weitgehend untauglicher Mittel bedient. Letztlich muss es aber dem Gesetzgeber überlassen werden, ob er Netzsperren einführen will, weil ihm die Schaffung eines weitgehend untauglichen Mittels besser erscheint als ein Nichtstun.

* * * * *

Prof. Dr. Burkhard Stiller

Prof. Dr. Florent Thouvenin