economiesuisse
DOSSIER POLITIK

7 / 2018

Nein zu Netzsperren und digitaler Abschottung

02.05.2018

Das Wichtigste in Kürze

Am 10. Juni 2018 stimmt die Schweizer Bevölkerung über das neue Geldspielgesetz ab. Zum Schutz der hiesigen Casinos enthält das Gesetz – dies ein Novum in der Schweiz – Netzsperren, mit denen der Zugriff auf ausländische Geldspielangebote im Internet künftig unterbunden werden soll. Bereits heute ist das Angebot solcher Spiele in der Schweiz zwar verboten, doch das Spielen ist erlaubt.

Bei diesen Netzsperren handelt es sich um staatlich verfügte Sperren, welche den Zugriff auf bestimmte Seiten im Internet für alle blockieren. Dabei werden in der Regel die Internetanbieter in die Pflicht genommen, spezifische Seiten im Internet zu sperren.

Was mit der Sperrung von Online-Glücksspielen beginnt, kann schnell zu weiterer Zensur in anderen Bereichen führen. Denn sind die entsprechenden Instrumente einmal vorhanden, finden weitere Interessengruppen schnell Gründe für zusätzliche Netzsperren.

Netzsperren sind ein Sündenfall für eine offene, moderne Volkswirtschaft wie die Schweiz. Sie sind ein Instrument der Abschottung, lassen sich mit wenigen Klicks selbst von Laien umgehen und richten gleichzeitig grossen Schaden an der Netzinfrastruktur an: zum Schaden von Wirtschaft und Gesellschaft.

Position economiesuisse

Die Schweiz verdankt ihren Wohlstand ihrer wirtschaftlichen Offenheit und den Freiheiten. Beide Werte sind gerade auch im digitalen Zeitalter von herausragender Bedeutung für unsere Gesellschaft und Wirtschaft.

Die uneingeschränkte Verfügbarkeit von Informationen und der freie Datenverkehr spielen eine Schlüsselrolle in der jüngeren Entwicklung. Heute ist das Internet das Rückgrat der digitalen Wirtschaft und Gesellschaft. Es darf darum nicht zum Spielball von Interessensvertretern jeglicher Art werden.

Netzsperren sind ein untauglicher und gefährlicher Versuch, die Grenzen der staatlichen Eingriffsmöglichkeiten auszudehnen. Netzsperren schaden unserer

Kontakt und Fragen

Erich Herzog
Mitglied der Geschäftsleitung, Leiter Wettbewerb & Regulatorisches
Christa Hofmann
Head Legal & Public Affairs, Swico

www.dossierpolitik.ch

freien Gesellschaft, dem Rechtsstaat und der (Internet-)Wirtschaft in der Schweiz. Ausnahmen sind ausschliesslich zum Schutz der öffentlichen Sicherheit zuzulassen (Schutz vor Terrorismus, Schutz vor Kinderpornografie usw.).

Die Einführung von Netzsperren könnte zu einem Dammbruch im Bereich Internetzensur führen. Die Signalwirkung auf andere Bereiche und auf unsere internationale Wahrnehmung als Standort für zukunftsgerichtete Technologieunternehmen wäre verheerend.

Netzsperren beschädigen die Netzinfrastruktur und sind dennoch leicht zu umgehen. Besonders gefährlich ist, wenn ineffiziente Sperren dann im Rahmen künftiger Gesetzesanpassungen noch weiter ausgebaut werden.

Das Internet als Treiber des Fortschritts

Das Internet ist das Rückgrat unserer modernen Gesellschaft und ist aus dem Alltag nicht wegzudenken.

Kein Alltag ohne Internet

Heute stehen wir an der Schwelle zur «digitalen Wirtschaft» beziehungsweise zur «digitalen Gesellschaft». Daten und Informationen sind die neuen Rohstoffe. Das Internet ist eine der Schlüsseltechnologien, die die digitale Transformation antreiben. Es ist das Rückgrat unserer modernen Gesellschaft und aus dem Alltag nicht mehr wegzudenken.

Technologien wie Smartphones, E-Mails, Cloud-Computing und vieles mehr sind ohne das Internet unmöglich. Alle, vom KMU über die Privatperson bis hin zur Hochschule, sind – je länger je mehr – auf einen freien und funktionierenden Austausch von Informationen angewiesen. Angesichts der Entwicklungen und der damit verbundenen neuen Möglichkeiten wird ein uneingeschränkter Datenverkehr aus wirtschaftlicher wie gesellschaftlicher Perspektive stets wichtiger.

Als Nervensystem der Vernetzung schafft das Internet grossen Mehrwert für Zivilgesellschaft wie auch Unternehmen.

Wirtschaftlicher und kultureller Mehrwert

Der durch das Internet ausgelöste Modernisierungsschub trägt nicht nur zur Entstehung neuer Wirtschaftszweige bei, sondern bewirkt auch einen grundlegenden Wandel des Kommunikationsverhaltens und der Mediennutzung im beruflichen und privaten Bereich. Die kulturelle Bedeutung dieser digitalen Vernetzung wird manchmal mit der Erfindung des Buchdrucks gleichgesetzt. Mit Fug und Recht kann heute festgestellt werden, dass das Internet als Nervensystem für Zivilgesellschaft wie Unternehmen von unschätzbarem Wert ist.

Staatliche Eingriffe in die Netzinfrastruktur gefährden die Funktionsfähigkeit von Wirtschaft und Gesellschaft.

Abhängigkeit steigert Verletzlichkeit

Die fortschreitende Digitalisierung führt zu einer zunehmenden Abhängigkeit von der Kommunikationsinfrastruktur und damit vom Internet. In der Folge steigt automatisch die Verletzlichkeit vieler Prozesse. Diese ist umso weitreichender, da diese Abhängigkeit weit über blosse Kommunikationsvorgänge hinausreicht. Es ist die zunehmende Vernetzung der Menschen und Geräte an sich, welche den substanziellen Mehrwert schafft.

Ein freier Internetzugang ist Ausdruck unserer generellen wirtschaftlichen Offenheit und ein bedeutender Standortfaktor.

Offenheit als Standortfaktor im Informationszeitalter

Die Schweiz verfügt dank ihrer traditionellen Offenheit über eine ausgezeichnete Ausgangslage, um von diesem digitalen Umbruch zu profitieren. Beleg dafür sind Unternehmen wie Google, IBM, Microsoft oder Oracle, die sich für die Schweiz als bedeutenden Entwicklungsstandort entschieden haben. Zudem ist die Schweiz attraktiv als Datentresor und steht hoch im Kurs für Unternehmen, die auf die Blockchain-Technologie setzen.

Alles in allem ist die Schweiz wegen ihrer wirtschaftlichen Offenheit, der guten (Netz-)Infrastruktur und dem freien Zugang zum Internet heute Anziehungspunkt für innovative Unternehmer und Investoren.

Offenheit prägt Denken und Handel
Die wirtschaftliche Offenheit ist Kernstück des Schweizer Erfolgsmodells. Unser hoher und breit gefächerter Wohlstand ist ohne offene Märkte und unternehmerische Freiheit undenkbar. Dank dieser Offenheit konnte unser kleiner Binnenstaat von der Globalisierung und dem technologischen Fortschritt der letzten Jahrzehnte stark profitieren. Dank dieser wettbewerbsfördernden Offenheit zeichnet sich unsere Wirtschaft durch eine hohe Anpassungs- und Innovationsfähigkeit aus, durch die wir Krisen und Strukturwandel oft erfolgreicher meistern wie im Ausland. Auch darum braucht sich die Schweiz vor der Digitalisierung nicht zu fürchten.

→ **Auch der Bundesrat hat die Bedeutung des ungestörten Datenverkehrs in der «Strategie Digitale Schweiz» festgehalten.**

Auch der Bundesrat hat dies erkannt und bereits in der «Strategie Digitale Schweiz» 2016 festgehalten, dass die Schweiz

- als sicherer internationaler Standort für Datenspeicher und Informatikdienstleistungen etabliert sein muss und über eine Datenpolitik verfügt, welche die Interessen der Schweiz auch im digitalen Bereich berücksichtigt;
- die Diskussion über die Zukunft des Internets mitprägt;
- ihre Chancen im Hinblick auf den virtuellen internationalen Wirtschaftsraum nutzt, um damit auch das Risiko einer Ausgrenzung abzuwenden.

Daraus ergibt sich, dass die Bedeutung des ungestörten Datenverkehrs für die weitere wirtschaftliche und gesellschaftliche Entwicklung unseres Landes nicht unterschätzt werden kann. Es handelt sich dabei um den Kern unseres künftigen wirtschaftlichen Erfolgs.

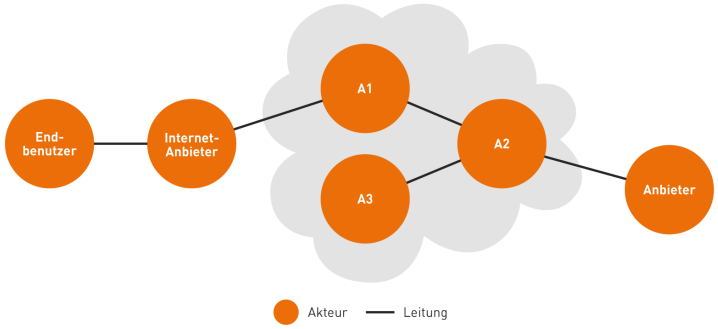
Aufbau und Funktion von Netzsperren

Funktionsweise des Internets

Beim Internet handelt es sich um einen weltweiten Verbund von selbstständigen Rechnernetzwerken beziehungsweise internetfähigen Endgeräten. Das Internet stellt die Vernetzung dieser Netzwerke untereinander sicher und ermöglicht so die Nutzung von Diensten und Applikationen wie World Wide Web, E-Mail, Apps und vielem mehr. Im Prinzip kann sich jedes Endgerät dabei mit jedem anderen verbinden. Der Datenaustausch zwischen den über das Internet verbundenen Endgeräten erfolgt über technisch normierte Internetprotokolle.

→ **Das Internet ist ein Zusammenschluss von unabhängigen Netzwerken. Im Prinzip kann sich jedes internetfähige Gerät mit jedem anderen Gerät verbinden.**

Vereinfachter Aufbau des Internets anhand drei wesentlicher Akteure



Quelle: Thouvenin/Stiller/Hettich/Bocek/Reutimann: Keine Netzsperren im Urheberrecht, sic! 2017, S. 704.
www.economiesuisse.ch

→ **Aufgrund seines Netzwerkaufbaus ist das Internet grundsätzlich ausfallsicher konstruiert.**

Ausfallsichere Konstruktion

Das Internet ist grundsätzlich ausfallsicher konzipiert worden. Darum gibt es im Netzwerk immer mehrere Wege, die zum Ziel führen. Wenn einer dieser Wege ausfällt, kann ein anderer gewählt werden. Netzsperren machen aber das Internet in der Nutzung risikoanfällig und unsicherer.

Das Internet als dezentrales Netzwerk

Das Internet besteht aus Netzwerken unterschiedlicher administrativer Verwaltung, die zusammengeschaltet sind. Dies sind zur Hauptsache Netzwerke der Internetanbieter (Providernetzwerke), an welche die Geräte der Endbenutzer eines Internetserviceproviders (ISP) angeschlossen sind.

An Internet-Knoten werden viele verschiedene Backbone-Netzwerke über leistungsstarke Verbindungen und Geräte (Router und Switches) miteinander verbunden. Darauf wird der Austausch von Erreichbarkeitsinformationen zwischen jeweils zwei Netzen vertraglich und technisch als Peering, also auf der Basis von Gegenseitigkeit organisiert und somit der Datenaustausch ermöglicht.

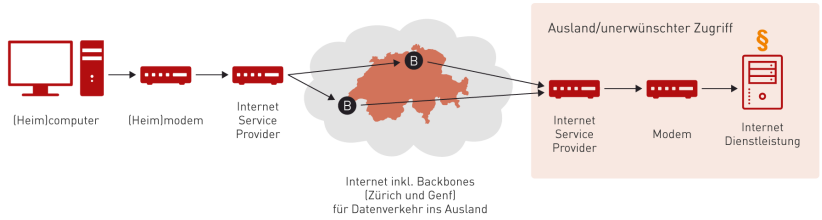
Das Mutternetzwerk des Internets, das Arpanet, war als dezentrales Netzwerk möglichst ausfallsicher konzipiert worden. Entsprechend war bei der Planung

kein Zentralrechner vorgesehen worden, an dem alle Verbindungen zusammenlaufen. Die netzartige Struktur des Internets trägt damit bis heute zu einer hohen Ausfallsicherheit bei. Für die Kommunikation zwischen zwei Nutzern existieren daher immer mehrere mögliche Wege über Router mit verschiedenen Betriebssystemen. Der Ausfall einer physikalischen Verbindung im Kernbereich des Internets hat so in der Regel keine schwerwiegenden Auswirkungen.

Das Protokoll, in dem die weltweit eindeutige Adressierung von angebundenen Rechnern festgelegt und benutzt wird, heisst Internetprotokoll (IP). Um ein bestimmtes Endgerät ansprechen zu können, identifiziert es das Internetprotokoll mit einer eindeutigen IP-Adresse. Diese Adressen funktionieren ähnlich wie Telefonnummern und enthalten auch eine länderspezifische Kennziffer, die Geotargeting ermöglicht. Vereinfacht gesagt kann eine IP-Adresse als Identität eines Endnutzers im Internet gesehen werden.

Das Domain Name System (DNS) waltet als automatisches «Telefonbuch» und stellt einen wichtigen Teil der Internetinfrastruktur dar. Diese internationale Datenbank stellt einen Übersetzungsmechanismus zur Verfügung, der eine IP-Adresse (z.B. 86.125.22.1) in einen für Menschen gut merkbaren Domänennamen (z.B. «economiesuisse.ch») übersetzt. Dies geschieht – vom Nutzer unbemerkt – immer dann, wenn er etwa im Webbrowser auf einen neuen Hyperlink klickt oder direkt eine Webadresse eingibt. Der Browser fragt dann zuerst mittels IP-Paket eines ihm bekannten DNS-Servers nach der IP-Adresse des fremden Namens und tauscht dann IP-Pakete mit dieser Adresse aus, um die Inhalte der dort angebotenen Dienste wie beispielsweise Webseiten abzurufen.

Datenverkehr im Internet



Quelle: Thomas Verasani, digital-liberal.ch
www.economiesuisse.ch

Netzsperren sollen den Zugang zu gewissen Webseiten verhindern. Möglich ist das über drei Wege mit unterschiedlichen Folgen..

Arten und Funktionsweisen von Netzsperren

Mit Netzsperren soll der Zugang von Endnutzern zu bestimmten Webseiten und deren Inhalten gesperrt werden. Im Zentrum stehen dabei unerwünschte Inhalte, die den öffentlichen Frieden gefährden. So können Netzsperren genutzt werden, um klar illegale Angebote wie z.B. harte Pornografie, terroristische oder extremistische Inhalte von den Endnutzern fernzuhalten.

Jedes Gerät, das am Internet angeschlossen ist, verfügt über (mindestens) eine eindeutige IP-Adresse (z.B. 86.125.22.1). Da diese Adressen für Menschen nicht einfach zu lesen und zu merken sind, wird den rein numerischen IP-Adressen auf Grundlage des sogenannten Domain Name System (DNS) ein Domain Name zugeordnet (z.B. www.swico.ch). Dieser Domainname wird standardmässig durch die DNS-Server der Internetanbieter in IP-Adressen übersetzt (sogenannte Namensauflösung). Unter einer IP-Adresse sind die Webseiten verschiedener Anbieter erreichbar, die unter ihrem jeweiligen Domainnamen unterschiedliche Inhalte anbieten.

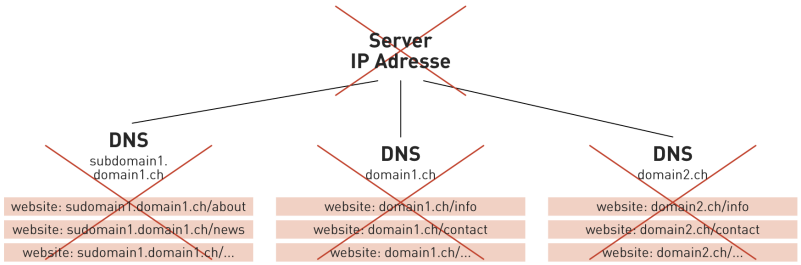
Heute stehen für Netzsperren primär drei Optionen im Vordergrund.

Variante 1: «IP-Sperren»

Bei IP-Adresssperren filtern die Internetanbieter die Anfragen ihrer Kunden nach spezifischen, auf einer Sperrliste hinterlegten IP-Adressen. Entweder blockieren sie diese oder leiten sie auf eine Webseite um, welche die Kunden informiert, dass eine gesperrte IP angefragt wurde. Die Sperre erfasst dabei alle Inhalte – legale wie illegale –, die unter der gesperrten IP-Adresse abrufbar sind (siehe hierzu auch unten, Overblocking).

→ **Bei IP-Sperren werden die Adressen von Computern im Internet blockiert. Anfragen auf solche Adressen werden in der Regel auf eine Warnseite umgeleitet.**

IP-Adresssperren: blockieren Adressen von Computern



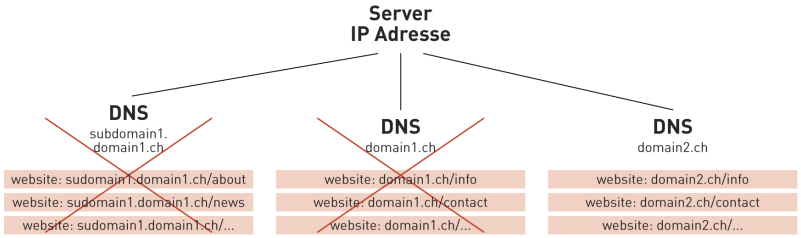
Quelle: Thouvenin/Stiller/Hettich/Bocek/Reutimann: Keine Netzsperren im Urheberrecht, sic! 2017, S. 704.
www.economiesuisse.ch

Variante 2: «DNS-Sperren»

Bei DNS-Sperren wird entweder die Namensauflösung durch den DNS-Server verhindert oder die Anfragen durch den Internetanbieter werden auf eine Webseite umgeleitet, welche die Kunden informiert, dass sie eine gesperrte Webseite aufzurufen versuchen. Die DNS-Sperre erfasst dabei alle Inhalte, die unter der gesperrten Domain abrufbar sind. Nicht erfasst werden hingegen andere Inhalte, die unter derselben IP-Adresse (aber unter einer anderen Domain) abrufbar sind.

Bei DNS-Sperren wird das «Telefonbuch» für gewisse IP-Adressen gesperrt. Damit können Seiten nur noch erreicht werden, wenn man die genaue IP-Adresse kennt.

DNS-Sperren blockieren die Aufschlüsselung der Adressen von Computern



Quelle: Thouvenin/Stiller/Hettich/Bocek/Reutimann: Keine Netzsperren im Urheberrecht, sic! 2017, S. 704.
www.economiesuisse.ch

Applikationsfilter analysieren die Datenpakete auf ihren Zweck und verhindern so beispielsweise bestimmte Dienstleistungen (IP-Telefonie, Messaging).

Variante 3: «Applikationsfilter»

Bei Applikationsfiltern wenden Internetanbieter und Diensteanbieter Filter auf den auszutauschenden Internetverkehr an. Solche im Allgemeinen als Applikationsfilter bezeichneten technischen Hilfsmittel erlauben es unter anderem auch, technisch gesehen schädliche Inhalte (wie z.B. Würmer, Viren oder Schadsoftware) in transportierten IP-Datagrammen zu erkennen. Eine Form dieser Filter kann durch Deep Packet Inspection (DPI) realisiert werden. DPI stellt namentlich die Möglichkeit detaillierter Paketfilter bereit, 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. DPI kann nur auf unverschlüsselt übertragene Protokolldaten angewendet werden, umfasst damit aber auch Anfragen an Suchmaschinen.

Probleme aus technischer Sicht

→ **Netzsperren schaffen unnötige Sicherheitsrisiken.**

Zusätzliche Sicherheitsrisiken

Netzsperren gefährden die Sicherheit des Internets, da Internetanbieter gezwungen werden, Datenpakete zu fälschen. Diese Interventionen schwächen die Technologien zur Erkennung von (kriminellen) Fälschungen und Manipulationen im Internet. Mit Netzsperren ist es auch nicht mehr möglich festzustellen, ob hinter einem Angebot tatsächlich der behauptete Anbieter steckt. Wenn aufgrund von Netzsperren mehr und mehr Nutzer gezwungen werden, sich anonymisiert im Netz zu bewegen, wird auch dadurch die Sicherheit gefährdet und der Kampf gegen Internetkriminalität erschwert. Das alles sind falsche Entwicklungen in einer Zeit, in der die Cyber-Kriminalität international auf dem Vormarsch ist.

Overblocking-Effekte

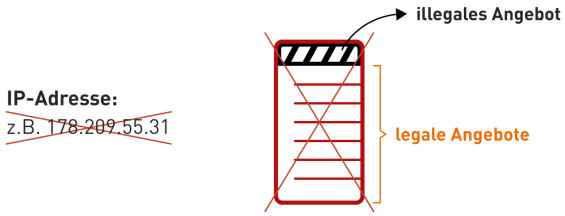
Aufgrund ihrer Funktionsweise besteht bei Netzsperren die Gefahr, dass auch der Zugang zu legalen Inhalten gesperrt wird. Man spricht dabei von einem sogenannten Overblocking. Diese Gefahr ist bei IP-Adresssperren besonders gross, weil unter einer IP-Adresse Webseiten verschiedener Anbieter mit unterschiedlichen Inhalten abrufbar sein können. Bei DNS-Sperren ist diese Gefahr geringer; allerdings lassen sich DNS-Sperren noch einfacher umgehen als IP-Adresssperren.

Das Perfide beim Overblocking ist, dass die legalen Webinhalte einfach aus unserer Wahrnehmung verschwinden. In der Regel merken es die Endnutzer nicht, wenn ein solches Angebot plötzlich aus dem Internet verschwindet oder ein Angebot nicht mehr erreichbar ist.

Unbeabsichtigte Sperren infolge Overblocking können auch gravierende wirtschaftliche Auswirkungen für einzelne Unternehmen nach sich ziehen. Sie rücken vollkommen legale Webinhalte ins Umfeld krimineller Angebote und verursachen einen Imageschaden oder einen geschäftsschädigenden Vertrauensverlust. Im Extremfall kann Overblocking existenzbedrohend sein, da (Schweizer) Kunden beispielsweise einen Onlineshop einfach nicht mehr finden.

→ **Netzsperren können auch Webinhalte blockieren, die rechtlich völlig unproblematisch sind.**

Sperren führen leicht zu Overblocking und sperren damit mehr, als vorgesehen



Quelle: eigene Darstellung
www.economiesuisse.ch

Folgen der Verschlüsselung

Immer mehr Webseiten sind nur noch per HTTPS und somit verschlüsselt erreichbar. Diese Verschlüsselung wirkt sich auch auf Netzsperren aus. So verhindert die Verschlüsselung Netzsperren, die auf Applikationsfilter und Proxy-Server setzen. Oftmals verhindert eine Verschlüsselung auch die Weiterleitung des Endnutzers auf eine Informationsseite die erklärt, warum die aufgerufene Webseite nicht erreichbar ist.

→ **Netzsperren verursachen einen enormen Aufwand bei Internetanbietern und benachteiligen so gerade KMU im Markt.**

Nachteile für KMU

Staatliche Netzsperren bedeuten massive Eingriffe in die Netzinfrastruktur. Denn die Internetanbieter werden durch Netzsperren gezwungen, gegen die Logik und Konstruktion des Internets zu agieren. Sie müssen in einem dezentralen Netzwerk, das darauf ausgerichtet ist, solche Störungen zu ignorieren bzw. über das Netzwerk zu umgehen, einzelne Webseiten blockieren. Sie müssen in einem dezentralen Netzwerk einzelne Webseiten blockieren, das darauf ausgerichtet ist, solche Störungen zu ignorieren bzw. über das Netzwerk zu umgehen. Darum verursachen Netzsperren für Internetanbieter einen enormen Aufwand. Dieser Sperraufwand führt zu einem Wettbewerbsnachteil gerade für kleinere Anbieter. Durch Netzsperren steigt das Risiko einer Marktkonzentration, weil KMU aus dem Markt verdrängt werden.

Umgehungsmöglichkeiten

Jede Netzsperre kann umgangen werden

IP-Adresssperren und DNS-Sperren können durch einfache technische oder organisatorische Massnahmen umgangen werden. Es gibt sogar Möglichkeiten, ohne dass Dritte (z.B. Strafverfolgungsbehörden) in der Lage wären, die Umgehung zu erkennen, nachzuweisen oder gar zu verhindern.

Umgehung von IP-Adresssperren

IP-Adresssperren und DNS-Sperren können durch Einwahl in Virtuelle Private Netzwerke (VPN) umgangen werden. Dadurch können Endnutzer über einen VPN-Server im Ausland auf die gesperrten IP-Adressen zugreifen. Die Namensauflösung erfolgt über einen DNS-Server, der nicht von der Sperre betroffen ist. Beide Arten von Sperren können auch durch Werkzeuge und Systeme zur Anonymisierung des Internetverkehrs technisch umgangen werden, z.B. durch Tor (siehe unten).

Umgehung von DNS-Sperren

DNS-Sperren können technisch umgangen werden, beispielsweise indem ausländische DNS-Server angefragt werden, die nicht von der Sperre betroffen sind, oder ein eigener lokaler DNS betrieben wird. In vielen Fällen braucht es auch überhaupt keinen DNS-Server. Dabei wird direkt die IP-Adresse des Web-Servers verwendet, die z.B. über einschlägige Internetforen oder persönliche Kommunikation in Erfahrung gebracht wird. Seit Kurzem steht auch ein neuer Standard DoH (DNS over HTTPS) zur Verfügung. Die zur Wahrung der Privatsphäre entwickelte Technologie ist neu fester Bestandteil von Browsern (z.B. Firefox) und umgeht alle DNS-Sperren automatisch.

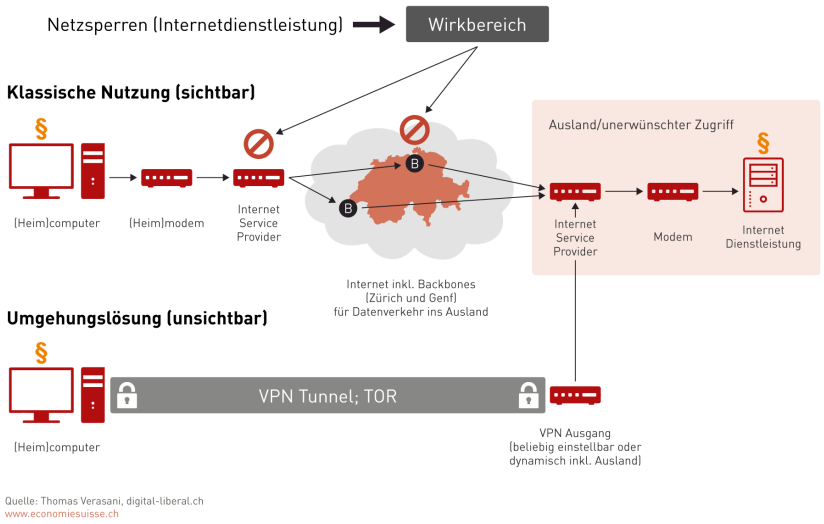
Umgehung von Applikationsfiltern oder Proxy-Servern

Selbst die aufwendigen Applikationsfilter und Proxy-Server können technisch umgangen werden. So kann der Endnutzer eine verschlüsselte Übertragung einsetzen, beispielsweise in Form eines VPN. Andere Möglichkeiten sind die Verwendung von SSL/TLS (Secure Socket Layer/Transport Layer Security) oder HTTPS (HTTP Secure). Der Endnutzer kann auch eigene Proxy-Server aufsetzen oder solche nutzen, die ihm im Internet angeboten werden.

Schliesslich gibt es eine Vielzahl von Werkzeugen und Systemen zur Anonymisierung des Quellverkehrs aus Sicht des Aufrufenden, beispielsweise Tor.

Jede Art von Netzsperre kann durch einfache technische oder organisatorische Massnahmen umgangen werden.

Wirkungsbereich und Umgehungsmöglichkeit von Netzsperren



Quelle: Thomas Verasani, digital-liberal.ch
www.economiesuisse.ch

Selbst in Ländern mit autokratischen Regierungen werden Umgehungsmöglichkeiten rege genutzt.

Die Realität in autokratischen Ländern

Es gibt Länder, welche die Internetzensur sehr weit treiben. Aber auch sie stossen mit Netzsperren an ihre Grenzen. So sind beispielsweise im Iran alle Seiten gesperrt, die mit der religiösen Ideologie des streng islamischen Landes kontrastieren oder Kritik an der Führung üben. Gerade städtische, moderne Iraner nutzen daher VPNs und andere technische Mittel, um beispielsweise westliche Filme oder TV zu schauen sowie internationale Zeitungen zu lesen.
In Russland wurde unlängst der dort beliebte Messaging-Dienst «Telegram» vom Staat gesperrt, da er die Verschlüsselung von Mitteilungen zuliess und der Geheimdienst diese Verschlüsselung nicht knacken konnte. Die vom russischen Staat gegen Telegram ausgelösten Sperrmassnahmen haben zwar Google und Amazon lahmgelegt, der eigentlich anvisierte Messaging-Dienst war aber weiterhin problemlos nutzbar. Dies zeigt, dass selbst in autokratischen Staaten nicht mit chirurgischer Präzision unliebsame Angebote abgestellt werden können, obwohl in solchen Ländern regelmässig die Nutzung von VPNs mit schweren Strafen geahndet wird.

Lediglich Länder wie Nordkorea, welche ihrer Bevölkerung die Nutzung des Internets faktisch verbieten, können die Kontrolle sicherstellen. Die Nachteile liegen auf der Hand: Die digitale Wirtschaft ist in solchen Ländern inexistent und die persönliche Freiheit der Bürger massiv eingeschränkt. Und auch hier findet der Mensch Lösungen: Die Antwort ist beispielsweise ein Schwarzmarkthandel mit USB-Sticks und anderen Datenträgern.

VPN (Virtual Private Network)

Ein VPN-Zugang lässt sich mit in der Schweiz völlig legal erhältlicher Software nutzen. Er ist auch für Laien ohne Schwierigkeiten einzurichten. Es reicht dazu,

ein entsprechendes App auf sein Gerät zu laden oder eine Browser-Erweiterung zu aktivieren. VPN verschlüsselt anschliessend die Internetverbindung, beginnend bei der Netzwerkkarte bis hin zu einem VPN-Server. Das lässt sich mit einem Tunnel vergleichen, mit dem man aus dem persönlichen Gerät bis zu einem vertrauenswürdigen Haus im Ausland gelangt. Bewegt man sich im Internet, so wird die Adresse dieses Hauses als Absender der Bewegungen wahrgenommen. Es gibt zahlreiche Anbieter solcher VPNs, die in der Regel kostenpflichtig sind. Eine Übersicht über die aktuell empfohlenen VPNs gibt es beispielsweise unter https://vpncreative.net/vpn-providers/.

Tor (The Onion Routing)
Das Tor-Netzwerk ermöglicht allen Endnutzern anonymes Surfen im Internet. Tor nutzt das Prinzip des sogenannten Onion-Routings, um die Verbindungs- und Transferdaten von Nutzern im Internet zu verschlüsseln. So erlaubt es das anonyme, abgesicherte Surfen im Internet. Für eine Nutzung von Tor muss der Nutzer anfänglich erst einmal einen Client (Software) herunterladen, welcher im Fachjargon als «Proxy»bezeichnet wird. Diese Software stellt nun eine Verbindung zum Tor-Netzwerk her und liefert eine Aufstellung aller verfügbaren Server, mit denen sich der Nutzer verbinden kann. Die Server weisen einen öffentlichen Schlüssel auf, um deren authentische Zugehörigkeit zum Netzwerk zu untermauern. Sobald der Nutzer die Liste auf seinem Gerät empfangen hat, findet schliesslich eine zufällig gewählte Route durch diese Tor-Server statt. Das Netzwerk selbst nutzt aus Gründen der Anonymisierung dabei nicht nur einen Server, sondern verbindet sich im Regelfall mit mindestens drei Servern. Details sowie auch ein Link zum Download des Proxy finden sich auf der Internetseite des Tor-Projekts: https://www.torproject.org/projects/torbrowser.html.en

Bedenken aus rechtlicher Perspektive

Netzsperren sind nicht zu unterschätzende Eingriffe in unsere Rechte und damit aus rechtsstaatlicher Sicht ein bedenkliches Instrument.

Staatlicher Eingriff

Netzsperren sind aus juristischer Perspektive in vielen Fällen als unverhältnismässiger rechtsstaatlicher Eingriff zu klassifizieren, weil sie ungeeignet und unzumutbar sind. Folgende Punkte spielen in der Beurteilung eine Rolle:

- die technischen Möglichkeiten und die damit verbundenen Umgehungsmöglichkeiten; - die indirekte Wirkung von Netzsperren auf Endnutzer und Internetanbieter statt auf die -verletzer (Webseiten-Betreiber);
- die potenzielle Bedrohung oder teilweise Verletzung von bedeutend wichtigeren Rechtsgütern (Grundrechte);
- der kaum rechtsstaatlich einwandfrei ausgestaltbare Rechtsschutz (rechtliches Gehör).

Gewisse Experten [1] sehen in Netzsperren einen schweren Eingriff in die grundrechtlich geschützte freie Kommunikation. Folglich brauchen Netzsperren in jedem Fall eine gesetzliche Grundlage. Für eine entsprechende Regelung ist deshalb eine Grundlage im formellen Gesetz zwingend (Art. 36 Abs. 1 Bundesverfassung).

Netzsperren können auch verschiedene Grundrechte betreffen.

Grundrechte tangiert

Aufgrund des Overblocking-Risikos und der Zulässigkeit von beispielsweise Geldspiel auf ausländischen Plattformen müssen Netzsperren auch für diejenigen Betroffenen rechtfertigbar sein, die als rechtmässig handelnde Drittpersonen von der Sperre tangiert sind.

Je nachdem können die Informationsfreiheit, die Wirtschaftsfreiheit oder – soweit Netzsperren mit der Untersuchung von Datenpaketen verbunden sind – auch die persönliche Freiheit in verschiedener Intensität betroffen sein. Im Vordergrund steht dabei das Recht auf Privatsphäre und auf informationelle Selbstbestimmung (Art. 13 BV).

Zu beachten sind zudem verschiedene Verfahrensgarantien, so die allgemeine Verfahrensgarantie einschliesslich des rechtlichen Gehörs (Art. 29 BV), die Möglichkeit der Anrufung einer richterlichen Behörde (Art. 29a BV) sowie minimale Standards eines gerichtlichen Verfahrens (Art. 30 BV): Namentlich beim Einsatz von Sperrlisten, die von den Internetanbietern umgesetzt werden müssen, steht die Wahrung des rechtlichen Gehörs zur Debatte. Denn die Eröffnung der Verfügung von Netzsperren erfolgt oft im Bundesblatt und nicht durch direkte Mitteilung an alle Betroffenen. Die Internetanbieter müssen demnach selbstständig die Sperrlisten überprüfen, auf welchen die zu sperrenden Webseiten aufgeführt sind. Werden solche Sperrlisten ohne Anhörung der Betreiber der zu sperrenden Webseiten erlassen, ist deren Anspruch auf rechtliches Gehör betroffen. Dasselbe gilt für diejenigen Rechteinhaber, die den Erlass einer Netzsperre nicht selbst verlangt haben.

Noch ungeklärt ist auch die Vereinbarkeit von schweizerischen Netzsperren für legale Angebote im Ausland unter dem Aspekt von internationalen Handelsabkommen.

→ **Netzsperren sind besonders in jenen Fällen fragwürdig, wo sie legales Verhalten von Endnutzern zu verhindern versuchen.**

Widersprüchliche Gesetzgebung

Eine besondere Problematik weisen Netzsperren auf, die grundsätzlich legales Verhalten von Endnutzern erschweren wollen. Steht das mit Netzsperren zu blockierende Verhalten nicht unter Strafe, so sind Sperren widersprüchlich. Ein an sich für die Bürger zulässiges Verhalten darf nicht unterbunden oder erschwert werden. Der Gesetzgeber darf nicht an der (rechtlichen) Zulässigkeit eines Verhaltens festhalten (so z.B. das Spielen von ausländischen Geldspielen im Internet) und gleichzeitig eine Regelung einführen, um den Zugriff auf solche Seiten im Internet (tatsächlich) zu verhindern. Eine geeignete Analogie wäre es, dass der Staat das Befahren einer Strasse nicht verbieten will, dafür aber aktiv darauf hinwirkt, dass die Strasse vereist oder Nägel auf der Strasse ausschüttet. Will sich der Gesetzgeber nicht dem Vorwurf des widersprüchlichen Verhaltens aussetzen, bleiben nur zwei Möglichkeiten: Er kann entweder an der heutigen Rechtslage festhalten und auf die Einführung von Netzsperren verzichten, oder er muss Farbe bekennen und mit der Einführung von Netzsperren auch gleichzeitig das Spielen auf ausländischen Geldspielplattformen verbieten. Ein Mittelweg zwischen diesen beiden Positionen ist in sich widersprüchlich.

→ **In Bereichen, in denen es um strafbare Handlungen geht, sind bereits heute – dies zumeist auf freiwilliger Basis – Netzsperren möglich.**

Freiwillige Zusammenarbeit als effizientes Instrument

Es gibt Bereiche des Alltags, in denen wir aus guten Gründen keine absolute Freiheit im Internet zulassen können. So z.B. wenn es um die Bekämpfung von Terrorismus oder der Kinderpornografie geht. Die Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) arbeitet beispielsweise eng mit den Internetanbietern zusammen. Seit 2007 besteht zwischen der KOBIK und den grössten Schweizer Internetanbietern ein Abkommen über die Blockade von Internetseiten mit verbotenen kinderpornografischen Inhalten. Die Sperre richtet sich dabei ausschliesslich gegen ausländische Internetseiten, die verbotene Pornografie mit Kindern gemäss Art. 197 Abs. 4 und 5 StGB zum Download anbieten. Die Internetanbieter blockieren aufgrund ihrer allgemeinen Geschäftsbedingungen und ethischen Grundsätzen den Zugang zu strafrelevanten Seiten und leiten den Benutzer auf eine «Stopp Seite» weiter. KOBIK erstellt und unterhält diesbezüglich eine laufend aktualisierte Liste, die zwischen 700 bis 1000 Webseiten enthält. Im Rahmen dieses Projekts arbeitet KOBIK eng mit Interpol zusammen. Die in der Schweiz erstellte Liste alimentiert zu einem grossen Teil die Interpol-«Worst of»-Liste von Webseiten, die kinderpornografische Inhalte anbieten. KOBIK sucht täglich proaktiv neue Internetseiten mit kinderpornografischen Inhalten und ergänzt laufend die Interpol-Liste, die in Zusammenarbeit mit mehreren Ländern unterhalten wird. Es ist fragwürdig, ob man mit der gesetzlichen Verankerung dieser Zusammenarbeit einen Mehrwert schaffen würde. Die Liste müsste – da sie dann eine staatliche Zwangsmassnahme auslösen würde – einer rechtsstaatlichen Kontrolle durch eine Behörde oder ein Gericht unterstehen. Es ist aber nicht im Interesse der Allgemeinheit, dass solche Listen der breiten Öffentlichkeit zugänglich gemacht werden.

Auf Netzsperren ist zu verzichten

Wirtschaftliche, gesellschaftliche, technische und juristische Gründe sprechen gegen die Einführung von Netzsperren.

Zahlreiche Nachteile

Eine eingehende Analyse von Netzsperren aus wirtschaftlicher, gesellschaftlicher, technischer und rechtlicher Perspektive zeigt, dass Netzsperren ein untauglicher und gefährlicher Versuch darstellen, die Grenzen der staatlichen Eingriffsmöglichkeiten auszudehnen. Netzsperren schaden unserer freien Gesellschaft, dem Rechtsstaat und der (Internet-)Wirtschaft in der Schweiz.

Besonders störend ist, dass Netzsperren die Netzinfrastruktur beschädigen und dennoch leicht zu umgehen sind. Zudem lässt sich ein Overblocking von legalen Webinhalten oft kaum vermeiden. Widersprüchlich sind Netzsperren in den Bereichen, wo sie grundsätzlich legales Verhalten von Bürgern einschränken (so der Fall im Geldspielgesetz).

Das Internet und der freie Datenverkehr sind das Rückgrat unserer Gesellschaft und sind aus dem Alltag kaum wegzudenken. Es darf nicht zum Spielball von Interessensvertretern jeglicher Art werden. Vielmehr muss es grundsätzlich überall frei zugänglich sein. Namhafte Experten erachten die Einführung von Netzsperren im Urheberrecht als unzumutbar und unverhältnismässig. Ausnahmen sind ausschliesslich zum Schutz der öffentlichen Sicherheit zuzulassen (Schutz vor Terrorismus, Schutz vor Kinderpornografie usw.).

Aus diesen Gründen wird klar, dass auf die Einführung von Netzsperren aus grundsätzlichen Überlegungen zu verzichten ist.

Netzsperren im Geldspielgesetz bergen die Gefahr eines Dominoeffekts.

Geldspielgesetz: Dammbruch droht

Am 10. Juni 2018 stimmt die Schweizer Bevölkerung über das neue Geldspielgesetz ab. Zum Schutz der hiesigen Casinos enthält das Gesetz – dies ein Novum in der Schweiz – Netzsperren, mit denen der Zugriff auf ausländische Geldspielangebote im Internet künftig unterbunden werden soll. Bereits heute ist das Angebot solcher Spiele in der Schweiz zwar verboten, doch das Spielen ist erlaubt.

economiesuisse lehnt das Geldspielgesetz wegen der Einführung von Netzsperren ab und warnt gleichzeitig vor einem Paradigmenwechsel. Den freien Internetzugang aufzugeben könnte zu einem Dammbruch im Bereich Internetzensur führen. Denn sind die entsprechenden Instrumente einmal vorhanden, finden weitere Interessengruppen schnell Gründe für zusätzliche Netzsperren. Die Signalwirkung auf andere Bereiche und auf unsere internationale Wahrnehmung als Standort für zukunftsgerichtete Technologieunternehmen wäre verheerend.

1. Florent Thouvenin, Burkhard Stiller, Peter Hettich, Thomas Bocek, Kento Reutimann in sic! 2017 S. 701 ff.