Dokument	**sic! 2017 S. 701**
Autor	**Florent Thouvenin, Burkhard Stiller, Peter Hettich, Thomas Bocek, Kento Reutimann**
Titel	**Keine Netzsperren im Urheberrecht**
Seiten	**701-722**
Publikation	**sic! - Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht**
Herausgeber	**Marc Amstutz, Mathis Berger, Reto M. Hilty, Anne-Virginie La Spada, Eugen Marbach, Cyrill P. Rigamonti, Jacques de Werra, Gregor Wild**
Frühere Herausgeber	**Ivan Cherpillod, Michel Jaccard, Jürg Müller, Michael Ritscher, Werner Stieger, Rolf H. Weber**
ISSN	**1422-2019**
Verlag	**Schulthess Juristische Medien AG**

Keine Netzsperren im Urheberrecht

Florent Thouvenin* | **Burkhard Stiller**** | **Peter Hettich***** | **Thomas Bocek****** | **Kento Reutimann*******

Die Rechtsdurchsetzung im Internet ist aufwendig und bleibt oft erfolglos. Das gilt auch (und gerade) für das Urheberrecht. Es erstaunt deshalb wenig, dass die Rechteinhaber nach Alternativen suchen und sich für die Einführung von Netzsperren starkmachen. Solche Sperren werfen allerdings zentrale technische und rechtliche Fragen auf. Dieser Beitrag untersucht, ob und inwiefern die heute verfügbaren Arten von Netzsperren technisch wirksam sind und ob die Einführung solcher Sperren im URG verhältnismässig und mit den geltenden Konzepten des schweizerischen Urheberrechts vereinbar wäre.

---

* Prof. Dr., ausserordentlicher Professor für Informations- und Kommunikationsrecht, Vorsitzender des Leitungsausschusses des Center for Information Technology, Society, and Law (ITSL) und Direktor der Digital Society Initiative (DSI) der Universität Zürich (UZH).

** Prof. Dr., ordentlicher Professor für Verteilte Systeme und Kommunikation, Leiter der Communication Systems Group CSG, Instituts für Informatik (IfI), Universität Zürich (UZH).

*** Prof. Dr., LL.M., Professor für öffentliches Wirtschaftsrecht mit Berücksichtigung des Bau-, Planungs- und Umweltrechts und Direktor am Institut für Finanzrecht, Finanzwirtschaft und Law and Economics (IFF-HSG) der Universität St. Gallen HSG.

**** Dr., Post Doc, Leiter P2P and Distributed Systems der Communication Systems Group CSG, Institut für Informatik (IfI), Universität Zürich (UZH).

***** MLaw, Assistent am Lehrstuhl für Informations- und Kommunikationsrecht, Universität Zürich (UZH).

La mise en œuvre du droit sur internet demande beaucoup d'effort et reste souvent sans succès. Cela vaut aussi et surtout pour le droit d'auteur. C'est pourquoi, on ne s'étonnera pas du fait que les ayants droit cherchent des alternatives et s'engagent avec détermination pour l'introduction de blocages du réseau. Mais ces blocages soulèvent des questions techniques et juridiques capitales. C'est pourquoi la présente contribution cherche à déterminer si et dans quelle mesure les genres de blocages du réseau disponibles aujourd'hui sont techniquement efficaces et si l'introduction de ces blocages dans la LDA serait proportionnée et compatible avec les concepts en vigueur du droit d'auteur suisse.

I. Einleitung

Die Rechtsdurchsetzung im Internet oder, genauer gesagt, im World Wide Web [1], ist mit massgeblichen Schwierigkeiten verbunden. Der zentrale Grund liegt darin, dass nationale Rechtsordnungen an territoriale Grenzen gebunden sind, die Vorgänge auf dem Web hingegen nicht. Die bestehenden Mittel des internationalen Zivil- und Strafprozessrechts helfen kaum weiter, weil sie für eine effektive Rechtsdurchsetzung in aller Regel zu langsam und zu teuer sind. Dies gilt in ganz besonderem Mass für die Durchsetzung von Urheberrechten, weil hier die einzelne Rechtsverletzung meist lediglich einen marginalen Schaden stiftet, der nur einen Bruchteil der Kosten einer allfälligen Rechtsdurchsetzung ausmacht. Das Problem liegt für die Rechteinhaber denn regelmässig auch nicht in einer einzelnen Rechtsverletzung, sondern in der Summe der Verletzungen, die zu massgeblichen Umsatzeinbussen führen kann.

Vor diesem Hintergrund erstaunt es wenig, dass gewichtige Rechteinhaber und die Gesetzgeber gewisser Länder seit Jahren nach Mitteln suchen, um dieser Situation Herr zu werden. Die teilweise erfolgreichen und teilweise gescheiterten Versuche reichen – um nur die Wesentlichen zu nennen – vom Einsatz und rechtlichen Schutz technischer Schutzmassnahmen (sog. *Digital*

Rights Management Systems [*DRM*]) über das Schaffen besonderer Behörden, etwa die *Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (Hadopi)*[2], bis zu *Netzsperren*, mit denen der Zugang zu Webseiten gesperrt werden soll, auf denen urheberrechtlich geschützte Werke ohne Zustimmung der Rechteinhaber zugänglich gemacht werden.

---

1 Die Begriffe Internet und World Wide Web werden in der Umgangssprache regelmässig als Synonyme verwendet, richtigerweise sind sie aber auseinanderzuhalten. Das Internet ist eine technische Infrastruktur, konkret ein weltweiter Verbund von Computern und Computernetzwerken, auf der bestimmte Dienste angeboten werden, namentlich E-Mail, World Wide Web und Internet-Telefonie. Das World Wide Web ist also nur einer der Dienste, die auf dem Internet angeboten werden. Es handelt sich dabei um ein weltweites System zum Anzeigen von Informationen auf Webseiten.

2 Siehe dazu <www.hadopi.fr> sowie: Schlussbericht AGUR12 vom 28. November 2013, 66 ff.; Schweizerisches Institut für Rechtsvergleichung, Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content, Lausanne 2015, 236 ff.; É. Darmon/S. Dejean/T. Pénard, La réponse graduée de l'Hadopi a-t-elle eu des effets sur le piratage de musique et de films?, Une étude empirique des pratiques de consommation en ligne, Revue économique 2016, Nr. 2, 181 ff., <www.jstor.org/stable/pdf/43746402.pdf>, *passim;* B. Danaher/ M. D. Smith/R. Telang/S. Chen, The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France, 2012, <repository.cmu.edu/cgi/viewcontent.cgi?article=1387&context=heinzworks>, *passim;* C. Jamet, Depuis Ha dopi, le nombre de pirates en France a augmenté, Le Figaro, 9. März 2010, <www.lefigaro.fr/web/2010/03/09/01022-20100309ARTFIG00473-depuis-hadopi-le-nombre-de-pirates-en-france-a-augmente-.php>.

Im Gegensatz zu einigen ausländischen Rechtsordnungen[3] sind Netzsperren in der Schweiz bisher weder im Urheberrecht noch in einer allgemeinen Regelung vorgesehen, die auf das Urheberrecht Anwendung finden würde. Netzsperren werden von schweizerischen *Internet Service Providern (ISP)* allerdings schon seit Jahren «freiwillig» (auf Veranlassung der Behörden) eingesetzt, namentlich um den Zugang zu Kinderpornografie zu unterbinden[4]. Nach durchaus intensiven Debatten im Parlament[5] sollen Netzsperren im neuen *Geldspielgesetz* nun auch in der Schweiz erstmals gesetzlich geregelt werden. Vorgesehen ist, dass Internet-Zugangsprovider (sog. Access-Provider) verpflichtet werden, ihre Kunden mittels Netzsperren am Zugriff auf online durchgeführte Geldspiele zu hindern, wenn diese Spiele von Anbietern mit Sitz oder Wohnsitz im Ausland angeboten werden und die Spiele in der Schweiz nicht bewilligt sind, wenn also die Eidgenössische Spielbankenkommission keine Konzession erteilt hat[6]. Neben dem Geldspielgesetz ist auch im *Fernmeldegesetz (FMG)* die Einführung von Netzsperren vorgesehen. Mit der laufenden Revision soll allerdings lediglich eine gesetzliche Grundlage für die bestehende Praxis nachgeschoben werden, indem die Anbieter von Fernmeldediensten dazu verpflichtet werden, zum Schutz von Kindern und Jugendlichen den Zugriff auf harte Pornografie im Sinn von Art. 197 Abs. 4 f. StGB zu verhindern[7].

---

3 Beispielsweise im Bereich *Urheberrecht:* UK (vgl. dazu A. Lohri-Kerekes, Grenzen der Urheber rechtsdurchsetzung in der Schweiz mittels Filtern und Sperren im Internet, Zürich 2017, N 18, m.w.H), Australien (Urteil vom 15. Dezember 2016, Federal Court of Australia, Roadshow Films Pty Ltd v Telstra Corporation Ltd, FCA 1503, <www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2016/2016fca1503>), Frankreich; im Bereich *Geldspiel:* z. B. Frankreich, Belgien, Dänemark, Italien; im Bereich *Pornografie:* z. B. UK, Finnland, Niederlande, Indien; im Bereich *Terrorismus:* z. B. UK, Australien, Frankreich, Indien; im Bereich *Malware:* z. B. Australien. Vgl. Schwei zerisches Institut für Rechtsvergleichung, Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content, Lausanne 2015, *passim;* N. Cory, How Website Blocking Is Curbing Digital Piracy Without «Breaking the Internet», Infor mation Technology & Innovation Foundation, 2016, <www2.itif.org/2016-website-blocking.pdf>, 12; Botschaft zum Geldspielgesetz vom 21. Oktober 2015, BBl 2015, 8387 ff. (zit. Botschaft BGS), 8473; OSZE, Freedom of Expression on the Internet, 2012, <www.osce.org/fom/105522?download=true>, 220.

4 Für Näheres dazu siehe M. Wullschleger, Die Durchsetzung des Urheberrechts im Internet, Bern 2015, Rz. 449; Botschaft BGS (Fn. 3), 8473. Die gesetzliche Grundlage für dieses informelle Verwal tungshandeln soll nun zumindest in Teilen nachträglich in Art. 46a E-FMG geschaffen werden.

5 Die Netzsperren führten im Nationalrat zu intensiven Diskussionen, vgl. insb. AB NR 2017, 122 ff., sowie: Votum Balthasar Glättli, AB NR 2017, 85; Votum Beat Flach, AB NR 2017, 86; Votum Laurence Fehlmann Rielle, AB NR 2017, 88; Votum Karl Vogler, AB NR 2017, 89; Votum Lukas Reimann, AB NR 2017, 90. Im Ständerat wurden die Netzsperren hingegen ohne Diskussion angenommen, AB SR 2017, 456.

6 Fassung gemäss Referendumsvorlage:
Art. 86 Sperrung des Zugangs zu in der Schweiz nicht bewilligten Online-Spielangeboten
Abs. 1: Der Zugang zu online durchgeführten Geldspielen ist zu sperren, wenn die Spiel angebote in der Schweiz nicht bewilligt sind.
Abs. 2: Gesperrt wird ausschliesslich der Zugang zu Spielen, deren Veranstalterinnen ihren Sitz oder Wohnsitz im Ausland haben oder ihn verschleiern und die von der Schweiz aus zugänglich sind.
Abs. 3: Die ESBK und die interkantonale Behörde führen und aktualisieren jeweils eine Sperrliste betreffend die Angebote in ihrem Zuständigkeitsbereich.
Abs. 4: Die Fernmeldedienstanbieterinnen sperren den Zugang zu den Spielangeboten, die auf einer der Sperrlisten aufgeführt sind.
Abs. 5: Die ESBK und die interkantonale Behörde können einer Benutzerin oder einem Benutzer zu Aufsichts- oder Forschungszwecken Zugang zu den gesperrten Angeboten gewähren.

7 Botschaft und Gesetzesentwurf zum revidierten FMG wurden dabei vom Bundesrat am 6. September 2017 verabschiedet.
Art. 46a E-FMG: Kinder- und Jugendschutz
Abs. 1: […]
Abs. 2: Die Anbieterinnen von Fernmeldediensten unterdrücken die Informationen mit pornografischem Inhalt nach Artikel 197 Absätze 4 und 5 des Strafgesetzbuchs, auf die das Bundesamt für Polizei sie hinweist.

Vorgesehen war die Einführung von Netzsperren auch im Urheberrecht, und zwar im *Vorentwurf für ein teilrevidiertes URG (VE-URG)*, den der Bundesrat gestützt auf die Arbeiten der *Arbeitsgruppe zum Urheberrecht (AGUR 12)* am 11. Dezember 2015 vorgelegt hatte[8].

sic! 2017 S. 701, 703

Nachdem der Vorentwurf in der Vernehmlassung in mancherlei Hinsicht stark kritisiert worden war, hat der Bundesrat die AGUR 12 am 30. August 2016 als AGUR 12 II erneut einberufen, um den Vorentwurf mit Blick auf die Ergebnisse der Vernehmlassung zu überarbeiten und eine breitere Akzeptanz der Vorlage zu erzielen[9]. Tatsächlich konnten in der AGUR 12 II denn auch eine Reihe von Kompromissen gefunden werden. Diese haben unter anderem dazu geführt, dass die Einführung von Netzsperren nun nicht mehr vorgesehen ist, wie aus einer Medienmitteilung des IGE vom 2. März 2017 hervorgeht[10] .

Mit Blick auf den Stand der Entwicklungen mag sich der Leser fragen, weshalb dieser Beitrag die Sinnhaftigkeit und Rechtmässigkeit von Netzsperren im Urheberrecht untersucht. Der Grund ist einfach: Da gewisse *Interessenvertreter die Einführung von Netzsperren dem Vernehmen nach weiterhin fordern* und dieses Instrument – soweit ersichtlich – lediglich als Folge eines politischen Kompromisses aus der Vorlage gestrichen worden ist, besteht die Möglichkeit, dass der Ruf nach der Einführung von Netzsperren im Urheberrecht in den parlamentarischen Beratungen erneut erhoben wird und im Rahmen eines neu verhandelten Kompromisses ein politisch massgebliches Gewicht erhält. Dies umso mehr, als die erstmalige Regelung im Geldspiel- und Fernmeldegesetz nahelegen mag, Netzsperren nun auch in anderen Bereichen einzusetzen[11]. Zwar ist mit derartigen *Dammbruch-Argumenten* stets Vorsicht geboten. Jüngere Untersuchungen haben aber gezeigt, dass die Gefahr eines

---

8 Der Vorentwurf vom 11. Dezember 2015 sah noch die folgende Regelung vor:
Art. 66d VE-URG: Sperrung des Zugangs zu Angeboten
Abs. 1: Wer in seinem Urheber- oder verwandten Schutzrecht verletzt wird, kann vom IGE verlangen, dass es die Anbieterinnen von Fernmeldediensten mit Sitz in der Schweiz verpflichtet, den Zugang zu Angeboten von Werken und anderen Schutzobjekten zu sperren.
Abs. 2: Das IGE verfügt die Sperrung eines Angebots, indem es dieses auf eine Liste der zu sperrenden Angebote setzt (Sperrliste), wenn die verletzte Person glaubhaft macht, dass die folgenden Voraussetzungen erfüllt sind:
a. Das Angebot ist in der Schweiz abrufbar.
b. Das Angebot macht das Werk oder andere Schutzobjekt in nach diesem Gesetz offensichtlich widerrechtlicher Weise zugänglich.
c. Die Anbieterin abgeleiteter Kommunika tionsdienste, auf deren Server sich das Angebot befindet, hat ihren Sitz im Ausland oder verschleiert dessen Ort.
d. Das Werk oder andere Schutzobjekt ist von der Schweiz aus rechtmässig zugänglich oder rechtmässig erhältlich.
Abs. 3: Die in ihrem Urheber- oder verwandten Schutzrecht verletzten Personen haben die Anbieterinnen von Fernmeldediensten für die Kosten der Sperrung angemessen zu entschädigen.

9 Siehe dazu: <www.ige.ch/de/recht-und-politik/immaterialgueterrecht-national/urheberrecht/archiv/agur12.html>.

10 Die Begriffe *Internet* und *World Wide Web* werden in der Umgangssprache regelmässig als Synonyme verwendet, richtigerweise sind sie aber auseinanderzuhalten. Das *Internet* ist eine technische Infrastruktur, konkret ein weltweiter Verbund von Computern und Computernetzwerken, auf der bestimmte Dienste angeboten werden, namentlich E-Mail, World Wide Web und Internet-Telefonie. Das *World Wide Web* ist also nur einer der Dienste, die auf dem Internet angeboten werden. Es handelt sich dabei um ein weltweites System zum Anzeigen von Informationen auf Webseiten.

Y. Benhamou, Blocage de sites web en droit suisse, Expert Focus 2017, 524 ff., scheint grundsätzlich eine rechtsgebietsübergreifende Regelung von Netzsperren gegenüber einem sektor spezifischen Ansatz zu bevorzugen, favorisiert dabei aber die Selbstregulierung der Access-Provider.

11 Y. Benhamou, Blocage de sites web en droit suisse, Expert Focus 2017, 524 ff., scheint grundsätzlich eine rechtsgebietsübergreifende Regelung von Netzsperren gegenüber einem sektor spezifischen Ansatz zu bevorzugen, favorisiert dabei aber die Selbstregulierung der Access-Provider.

solchen Dammbruchs bei der Einführung von Netzsperren tatsächlich besteht[12]. Da eine eingehende Analyse der Sinnhaftigkeit und Rechtmässigkeit von Netzsperren im Urheberrecht für die Schweiz bisher fehlt und die Beratungen im Parlament kaum geeignet erscheinen, diese nachzuholen, sollen mit diesem Beitrag die technischen und rechtswissenschaftlichen Grundlagen gelegt werden, auf denen eine politische Debatte aufbauen kann – wenn diese denn tatsächlich geführt werden sollte.

Zu diesem Zweck sind zunächst die verfügbaren Arten von Netzsperren aus technischer Sicht zu untersuchen und es ist der Frage nachzugehen, ob und gegebenenfalls wie solche Sperren umgangen werden können und inwiefern die Gefahr besteht, dass sie nicht nur unrechtmässig, sondern auch rechtmässig zugänglich gemachte Inhalte erfassen (sog. *Overblocking*). Dabei wird sich zeigen, dass der Zugang zu den infrage stehenden Inhalten technisch weder umfassend noch garantierbar gesperrt werden kann. Auf dieser Grundlage ist anschliessend eine rechtliche Analyse vorzunehmen. Wie diese zeigen wird, ist die Einführung von Netzsperren sowohl aus verfassungs- wie aus urheberrechtlicher Sicht problematisch. Die verfassungsrechtlichen Bedenken hängen dabei massgeblich von der Ausgestaltung der Regelung ab. Da derzeit unklar ist, wie eine allfällige Regelung aussehen könnte, und weil eine Analyse aller denkbaren Varianten weder möglich noch sinnvoll wäre, wird nachfolgend ein Regelungsansatz untersucht, der den gegen Netzsperren erhobenen Bedenken möglichst weitgehend Rechnung trägt. Dabei wird sich zeigen, dass selbst eine solche Regelung grundrechtlich problematisch wäre und sich kaum ins dogmatische Grundkonzept des Urheberrechts und in die bestehende Regelung der Verbotsrechte und Schranken einfügen liesse.

II. 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 es wird (c) eine Bewertung dieses Spannungsverhältnisses (Sperrtyp versus Gegenmassnahme) vorgenommen.

1. Technische Grundlagen

Das Internet operiert auf der Basis von *Paketen* – den *IP-Datagrammen* (Internet Protocol) –, welche eine eindeutige Ziel-

12 J. L. Zittrain/R. Faris/H. Noman/ J. Clark/ C. Tilton/R. Morrison-Westphal, The Shifting Landscape of Global Internet Censorship, Berkman Klein Center Research Publication No. 2017-4, Cambridge MA 2017, <ssrn.com/abstract=2993485>, 10.

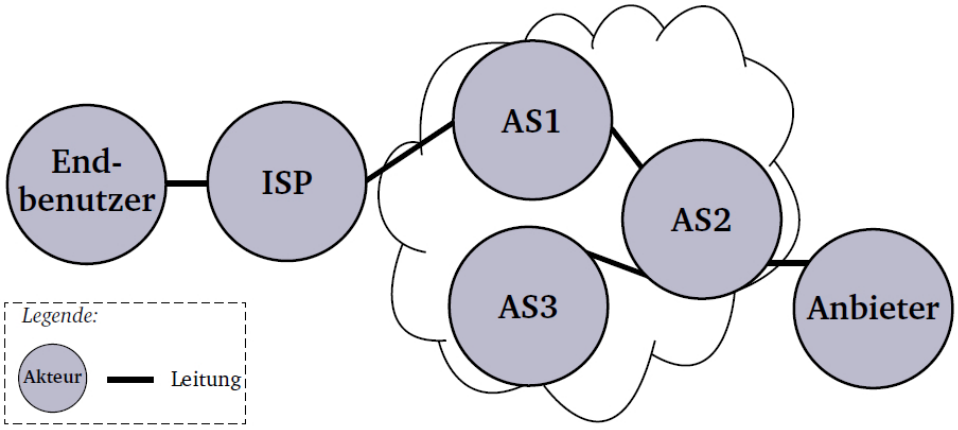

Abb. 1: Vereinfachter Aufbau des Internets anhand drei wesentlicher Akteure.

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

Aus Sicht einer Anwendung, die zwischen dem Endnutzer und dem Anbieter eine gewünschte Interaktion herstellt, werden Kommunikationsverbindungen zwischen einem Sender (bspw. dem Anbieter) und einem Empfänger (bspw. 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 vorne 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) verfügt 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 Endnutzer lesbare Namen (z. B. «www.anbieter-name.ch»), als *Domainname* bezeichnet, den rein numerischen IP-Adressen zuzuordnen. Dieser Vorgang der Zuordnung des Domainnamens 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 des Anbieters ‹anbieter-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 entsprechenden Daten nicht in seiner Datenbank hat. Im erfolgreichen Fall meldet der DNS-Server die ermittelte IP-Adresse zurück. Dieser Prozess wird beispielsweise durch einen Webbrowser angestossen, wenn der Uniform Resource Locator (URL) – umgangssprachlich als Webadresse bezeichnet

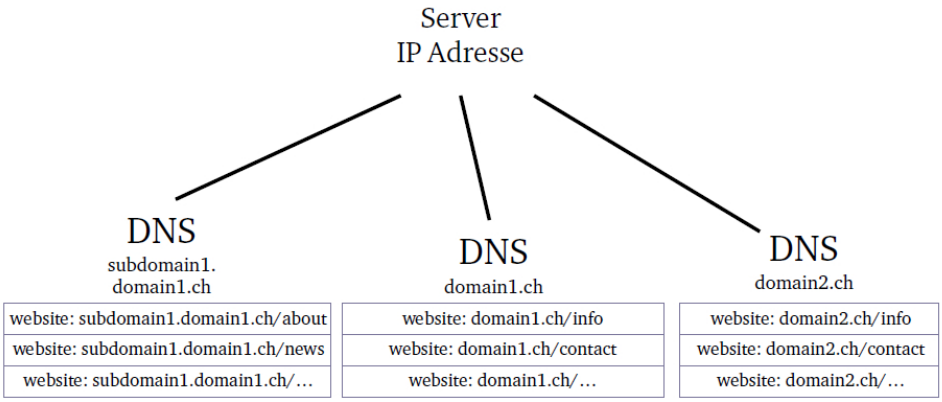

Abb. 2: Vereinfachte Darstellung einer IP-Adresse im Internet und der mit dieser über DNS verknüpften Domainnamen.

sic! 2017 S. 701, 705

- «www.anbieter-name.ch» im Browser angegeben wird, um den Inhalt dieser Webseite vom Webserver des Anbieters an den Anfragenden zu transportieren und in dessen Webbrowser anzuzeigen.

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

2. Netzwerk-Management und Diensterbringung durch ISP und Dritte

Neben diesen sehr grundlegenden Operationen zur Weiterleitung von IP-Datagrammen innerhalb und zwischen Autonomen Systemen spielt das Netzwerk-Management für einen ISP eine zentrale Rolle, um den zuverlässigen Betrieb eines Netzes sicherzustellen. Hierzu sind *Mess- und Monitorfunktionen* 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, der 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 essenziellen Informationen vor «normalen» Nutzdatenströmen priorisiert werden können. Zudem können verschiedene (Management-)Applikationen Vorrang vor anderen erhalten, um einerseits mit notwendigen Dienstgütern (Quality-of-Service) die Sicherstellung von essenziellen

Anwendungseigenschaften zu erreichen und andererseits die gewünschte Betriebssicherheit zu gewährleisten.

Einen weiteren Bereich zur Diensterbringung stellen *Content Distribution Networks (CDN)* dar, die als ein Netz mit typischerweise regional verteilten und über das Internet verbundenen Server realisiert werden. Als eine Möglichkeit des Überlastschutzes im Internet werden CDN häufig eingesetzt, weil Nutzdaten nahe beim Endnutzer zwischengespeichert werden können. Eine Konsequenz davon ist, dass auch Inhalte von Webseiten zwischengespeichert und zur Verfügung gestellt werden. CDN liefern dann auch diese Inhalte an Endnutzer aus, deren originärer Bereitstellungsort (definiert über deren Domainnamen) weder dem ISP, über den diese Daten transportiert werden, noch dem Endnutzer selber bekannt ist oder bekannt sein soll. 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 bspw. 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, beispielsweise das Terminieren einer TCP-Verbindung. DPI kann nur auf unverschlüsselt übertragene Protokolldaten (u. a. TCP, HTTP Hypertext Transfer Protocol oder IMAP Internet Message Access Protocol) und damit auch auf Anfragen an Suchmaschinen angewendet werden.

3. Netzsperren

Netzsperren sollen dazu dienen, unerwünschte Inhalte oder Angebote zu sperren, wie etwa harte Pornografie, terroristische oder extremistische Inhalte, gewaltverherrlichende Inhalte, nicht lizenzierte Angebote urheberrechtlich geschützter Werke und Geldspiele ausländischer Anbieter. Im Folgenden werden ausschliesslich die technischen Optionen für Netzsperren aus Sicht der ISP und die rechtlich erlaubten technischen Gegenmassnahmen der Endnutzer 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 Webseiten beziehen sollen, welche entweder über deren Domainnamen oder über IP-Adressen direkt erreichbar sind und welche durch einen ISP potenziell erbracht werden können, ergeben sich die nachfolgend dargestellten technischen Optionen aus Sicht der ISP, diesen Zugriff zu unterbinden. Nicht berücksichtigt werden dabei neuere Technologien, die es beispielsweise ermöglichen, Inhalte dezentral anzubieten, da der Zugriff auf die dadurch generierten Datenströme durch DPI-Verfahren von einem ISP ohne Verletzung

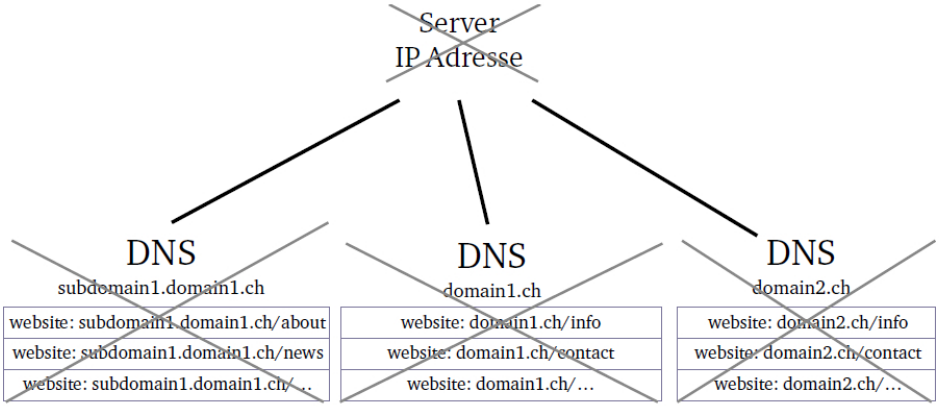

Abb. 3: Vereinfachte Darstellung der nicht mehr erreichbaren Maschinen und Inhalte bei einer IP-Adresssperre. Die Kreuze zeigen, dass in diesem Beispiel alle Maschinen und Inhalte, die durch diese Maschinen verwaltet werden, nach dem Sperren der IP-Adresse nicht mehr erreichbar sein werden.

des Fernmeldegeheimnisses (Art. 13 Abs. 1 BV und Art. 43 FMG) nicht möglich ist. Ausgenommen werden aber auch Suchmaschinen und das (gerichtlich) angeordnete Verbergen gewisser Suchresultate, weil durch das endnutzerseitige Verwenden einer anderen Suchmaschine, die nicht den anordnenden Behörden im gleichen Rechtsraum unterworfen ist, diese Einträge auch gefunden und damit verwendet werden können. Schliesslich sind auch Software und Programme ausgenommen, welche beim Endnutzer zu installieren wären («Staatstrojaner»).

aa) 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, die unerwünschte Inhalte aufweisen (vgl. Abb. 3). Meist wird zunächst bekannt sein, dass unter einem bestimmten Domainnamen mit entsprechender IP-Adresse unerwünschte Inhalte abrufbar sind; für die technische Einrichtung der IP-Adresssperre 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 als Antwort auf seine Anfrage zugestellt. Eine Weiterleitung der gesperrten Anfrage wäre technisch möglich, sodass unter gewissen Voraussetzungen per «Stopp-Schild» auf einer spezifischen Webseite der Endnutzer darauf aufmerksam gemacht werden könnte, dass die aufgerufene IP-Adresse gesperrt ist.

bb) 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.nicht-lizenzierte-inhalte.ch», auf eine spezielle Seite umgeleitet werden, welche (a) von einer staatlichen Behörde oder (b) dem ISP des Endnutzers bereitgestellt oder verwaltet wird (vgl. Abb. 4). Damit kann der Endnutzer per «Stop-Schild» darauf aufmerksam gemacht werden, dass die aufgerufene Seite gesperrt ist. Diese Sperre betrifft damit genau diese explizit genannte Seite, also exakt den gesamten Inhalt, der unter diesem Domainnamen, hier also «www.nicht-lizenzierte-inhalte.ch», abgelegt ist. Es muss damit vorab bekannt sein, dass unter einem bestimmten Domainnamen unerwünschte Inhalte abrufbar sind, da andernfalls DNS-Sperren nicht definiert werden können. Sollte der Anbieter dieser

unerwünschten Inhalte in der Schweiz registriert sein und eine «.ch»-Top-Level-Domain verwenden, kann dieser direkt beim schweizerischen DNS-Registrator beanstandet und nachfolgend gelöscht werden.

cc) Applikationsfilter oder Proxy-Server beim ISP

Wesentlich genauer als DNS-Sperren oder IP-Adresssperren sind Applikationsfilter oder Proxy-Server. Applikationsfilter suchen und erkennen auf der Basis der in den IP-Steuer- und Kontrolldaten sowie der in der Payload untergebrachten Daten der Applikation Datenelemente und Identifikatoren für die Verwendung von unerwünschten

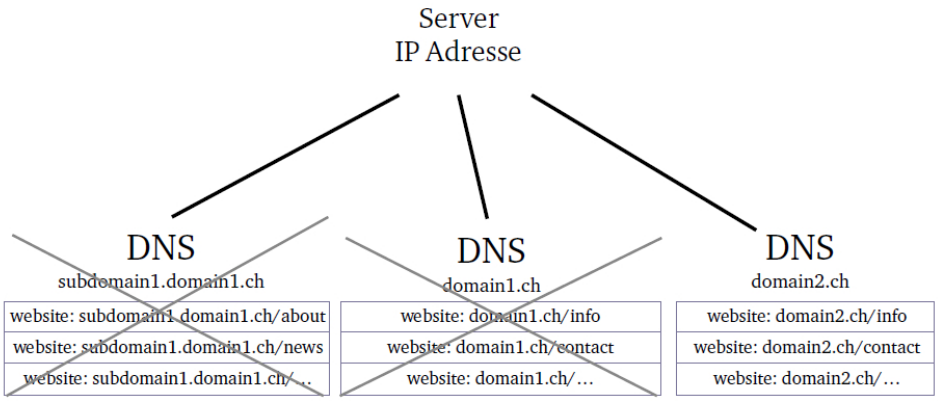

Abb. 4: Vereinfachte Darstellung der nicht mehr erreichbaren Maschinen und Inhalte bei einer DNS-Sperre. Die Kreuze zeigen, dass in diesem Beispiele nur bestimmte Maschinen und Inhalte nach dem Sperren eines Domainnamens (hier «domain1.ch») nicht mehr erreichbar sind.

sic! 2017 S. 701, 707

Inhalten. Proxy-Server liefern 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 Quellinformationen ebenso geschehen wie mit den Originaldaten.

Die Funktionalität dieser Proxy-Server ist auch dazu geeignet, anderweitig technisch schädliche Inhalte (z. B. Malware oder Viren) zu filtern und die Inhalte der Webseite bereinigt an den Aufrufenden weiterzugeben, was ein typischer Ansatz zur Erhöhung der Sicherheit in Kommunikationsnetzen ist. Ein Beispiel ist das Cleanfeed-Verfahren[13], das IP-Adresssperren mit den Proxy-Servern kombiniert.

Schliesslich können durch Applikationsfilter diejenigen IP-Datagramme, welche zu einer spezifischen TCP-Verbindung gehören, identifiziert werden. Sollten diese IP-Datagramme durch ein im Filter gesetztes Kriterium den Filter aktivieren, wird diese TCP-Verbindung zurückgesetzt und terminiert. Ein erneuter Aufbau- und Verbindungsversuch vom gleichen Quellknoten durch den Endnutzer 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 *Deep Packet Inspection (DPI)* möglich. Eine weitere spezifische Art des Filterns mit DPI stellen URL-Filter dar. Dabei wird die seitens des Endnutzers gewünschte URL auf das Vorhandensein von Stichwörtern untersucht, unabhängig von der verwendeten Domain.

---

13 A. Schneider, Netzsperren und das Cleanfeed-Verfahren, 2011, <www.telemedicus.info/article/2055-Netzsperren-und-das-Cleanfeed-Verfahren.html>.

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 (bspw. 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 Endnutzer oder Anbieter verschiedene Massnahmen ergreifen, um derartige Netzsperren zu umgehen. Die folgende Liste der Umgehungsmassnahmen fokussiert auf den Endnutzer und auf die Umgehungsmassnahmen der Anbieter, wie zum Beispiel der Wechsel der IP-Adresse oder des Domainnamens.

Auf ein Anbieten der Inhalte über beispielsweise *Tor Hidden Services*, bei welchen IP-Adressen ständig gewechselt werden können, um die IP-Adresssperre bereits inhaltsanbieterseitig zu umgehen, wird hier nicht näher eingegangen. Derartige Umgehungsmassnahmen der Anbieter müssen von diesen initiiert werden (im Gegensatz zur weiter hinten folgenden Anwendung von Tor durch Endnutzer) und können mit heutigen technischen Mitteln problemlos realisiert werden.

aa) Umgehung von IP-Adresssperren

IP-Adresssperren können technisch umgangen werden, indem

(1) Werkzeuge und Systeme zur Anonymisierung des Verkehrs eingesetzt werden. Möglich ist beispielsweise die Anwendung von Tor[14] durch den Endnutzer. Dadurch wird die Originalanfrage zur gewünschten Ziel-IP-Adresse verschlüsselt über verschiedene, zufällig gewählte Netzwerkteilnehmer irgendwo in der Welt geleitet, die sich nicht im Kontrollbereich der staatlichen Behörde oder des ISP befinden. Die erhaltene Antwort wird samt Inhalt ohne Berücksichtigung (und Kenntnis) des aktuellen und tatsächlichen Standorts des Endnutzers (also dessen Zugehörigkeit zu einem bestimmten AS) ausgeliefert;

(2) Virtuelle Private Netzwerke (VPN) genutzt werden, die dem Endnutzer durch private oder berufliche Verbindungen zur Verfügung stehen und die ebenfalls einen Zugriff auf beliebige IP-Adressen von einem Standort aus erlauben, der sich ausserhalb des Kontrollbereiches der staatlichen Behörde oder des ISP befindet; und indem

(3) weitere Massnahmen eingeleitet werden, wie beispielsweise (1) die Verteilung der Inhalte des Anbieters durch CDN oder (2) indem mehrere Server des Anbieters in verschiedenen Ländern mit unterschiedlichen IP-Adressen konfiguriert, eingesetzt und publiziert werden.

bb) Umgehung von DNS-Sperren

DNS-Sperren können technisch umgangen werden, indem

(1) für die Domainnamensauflösung 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 Endnutzers 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 Webservers zur Kommunikation verwendet wird; die IP-Adresse kann entweder gemäss (1) ermittelt werden oder wird durch einschlägige Foren oder persönliche Kommunikation weitergegeben;

---

14 Anonymity on-line, Tor, <www.torproject.org>.

(3) Werkzeuge und Systeme zur Anonymisierung des Verkehrs eingesetzt werden. Möglich ist beispielsweise die Anwendung von Tor[15] durch den Endnutzer. Dadurch wird die Originalanfrage zur Domainnamensauflösung verschlüsselt über verschiedene, zufällig gewählte Netzwerkteilnehmer irgendwo in der Welt geleitet, die sich nicht im Kontrollbereich der staatlichen Behörde oder des ISP befinden. Das Ergebnis der Namensauflösung wird ohne Berücksichtigung (und Kenntnis) des aktuellen und tatsächlichen Standorts des Endnutzers (also dessen Zugehörigkeit zu einem bestimmten AS) ausgeliefert;

(4) Einwahlmöglichkeiten in Virtuelle Private Netzwerke (VPN) eingesetzt werden, welche dem Endnutzer durch private oder berufliche Verbindungen zur Verfügung stehen und die ebenfalls den Zugriff auf DNS-Server erlauben, die sich ausserhalb des Kontrollbereiches der staatlichen Behörde oder des ISP befinden; und indem

(5) ein vom Endnutzer selber betriebener DNS-Server verwendet wird.

cc) Umgehung von Applikationsfiltern oder Proxy-Servern

Applikationsfilter und Proxy-Server können unter anderem umgangen werden, indem

(1) eine verschlüsselte Übertragung eingesetzt wird, etwa in Form von VPN, SSL/TLS (Secure Socket Layer/Transport Layer Security) oder HTTPS (HTTP Secure);

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

(3) Werkzeuge und Systeme zur Anonymisierung des Quellverkehrs aus Sicht des Aufrufenden eingesetzt werden, beispielsweise Tor[16]; und indem

(4) 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 oder 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.

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 Endnutzer gelegt, für den das Umgehen der Netzsperren grundsätzlich kaum ein technisches Problem darstellt, sondern es wird die Wirksamkeit dieser Sperren speziell für den Fall eines technisch nicht versierten Endnutzers untersucht. Dabei wird sich zeigen, dass Netzsperren im Allgemeinen nicht zum gewünschten Ergebnis führen, wobei dieser Effekt durch die zukünftige Zunahme von eingesetzten Sicherheitsmechanismen und damit von verschlüsseltem Verkehr eher verstärkt als vermindert wird.

aa) Wirksamkeit von IP-Adresssperren

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

---

15 Anonymity on-line, Tor, <www.torproject.org>.

16 Anonymity on-line, Tor, <www.torproject.org>.

IP-Adresssperren haben zudem den Nachteil, dass sie Kollateralschäden verursachen können: Da unter einer IP-Adresse sehr viele Webseiten 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 Webseiten betroffen. Mit IPv6-Adressen (Internet Protocol Version 6), welche stark an Bedeutung gewonnen haben[17], kann das Problem des Overblocking zwar entschärft werden, wenn je Webseite eine einzelne IPv6-Adresse verwendet wird. Ob dies allerdings in Zukunft in dieser

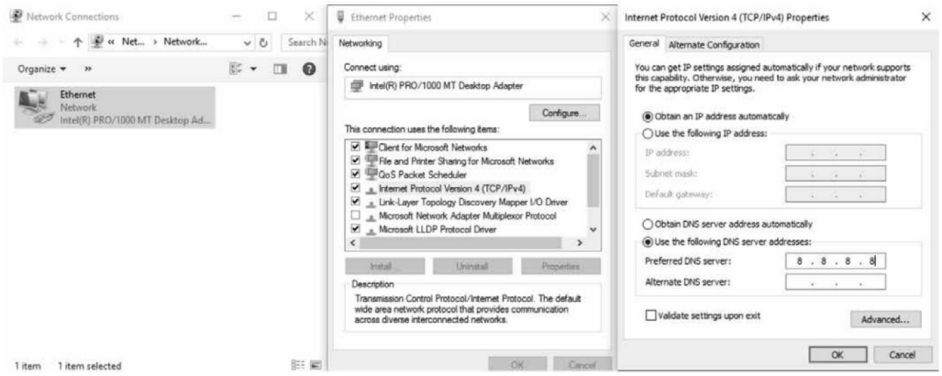

Abb. 5: Beispiel, wie unter Windows 10 eine DNS-Sperre umgangen werden kann.

Form realisiert werden wird, ist nach heutigem Kenntnisstand als ungewiss einzustufen.

bb) Wirksamkeit von DNS-Sperren

DNS-Sperren können mit minimalen technischen Kenntnissen mittels der vorne genannten Methoden umgangen werden. So können manuell DNS-Server aus Sicht eines Anwenders angewählt werden (z. B. 8.8.8.8), um die Domainnamensauflösung 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.

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

Durch geeignete Massnahmen kann man DNS-Anfragen derart umleiten, dass die angefragte Webseite auf eine andere als die ursprüngliche Webseite verweist. Allerdings funktionieren derartige Massnahmen mit dem eher neueren Einsatz bekannter Sicherheitsfunktionen immer schlechter[18].

---

17 <www.google.com/intl/en/ipv6/statistics.html>.

18 Diese Umleitungen funktionieren insbesondere nicht, wenn *Public Key Pinning Exten sions for HTTP* (*HPKP*) eingesetzt werden und die Webseite mindestens einmal zuvor besucht worden ist. Dieses Vorgehen wird ebenso durch die *HTTP Strict Transport Security* (*HSTS*) erschwert, weil die gängigen Webbrowser eine Warnung ob dieser Umleitung anzeigen. Zudem kann mit allfällig eingesetzten *DNS Security Extensions (DNSSEC)* eine Umleitung explizit festgestellt werden, die bei den in Zukunft verwendeten und DNSSEC unterstützenden Webbrowsern zu keiner funktionierenden Umleitung mehr führt.

cc) Wirksamkeit von Applikationsfiltern oder Proxy-Servern

Da die Zahl der Webseiten, auf die nur per HTTPS und damit verschlüsselt zugegriffen werden kann, steigt, sind Applikationsfilter und Proxy-Server bereits heutzutage praktisch wirkungslos. Eine Statistik eines Browser-Herstellers zeigt, dass schon heute mehr als die Hälfte der aufgerufenen Seiten per HTTPS verschlüsselt erfolgt[19].

Zudem ist jede Filtertechnik 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.

III. Rechtliche Beurteilung

1. Ausgangslage

Die vorstehenden Ausführungen haben gezeigt, dass für Netzsperren verschie-

sic! 2017 S. 701, 710

dene technische Möglichkeiten zur Verfügung stehen, dass jedoch alle heute verfügbaren Arten von Netzsperren entweder von Anfang an weitgehend wirkungslos sind (Applikationsfilter und Proxy-Server) oder mehr oder minder einfach umgangen werden können (IP-Adresssperren und DNS-Sperren). Hinzu kommt, dass bei allen verfügbaren Arten von Netzsperren die Gefahr von Overblocking besteht. Diesen Bedenken hat der Gesetzgeber bei der Ausarbeitung des Vorentwurfs für ein teilrevidiertes URG möglichst Rechnung zu tragen versucht, indem er den Anwendungsbereich von Netzsperren vergleichsweise eng gefasst hat. Namentlich sollen nur Angebote erfasst werden, die «ausschliesslich aus widerrechtlich zugänglich gemachten Werken»[20] bestehen, sowie solche, bei denen «vereinzelt rechtmässige Angebote lediglich als ‹Feigenblatt› dienen»[21]. Diese massgebliche Einschränkung des Anwendungsbereichs ergibt sich allerdings nicht aus dem vorgeschlagenen Gesetzestext (Art. 66d ff. VE-URG), sondern nur aus dem Erläuternden Bericht. Damit erscheint nicht gesichert, dass Netzsperren nach Erlass einer solchen Regelung nicht doch auch auf weitere Konstellationen angewendet werden, etwa auf Webseiten, auf denen nur ein gewisser Anteil der Werke ohne Zustimmung der Rechteinhaber zugänglich gemacht wird. Sollte eine Regelung von Netzsperren vom Parlament in Betracht gezogen werden, müsste sich die Einschränkung des Anwendungsbereichs deshalb auf jeden Fall unzweideutig aus dem Gesetzeswortlaut selbst ergeben.

Mit Blick auf die gegenüber Netzsperren erhobenen Bedenken erscheint es zudem angezeigt, eine Regelungsvariante zu wählen, welche diesen Bedenken noch weiter gehend Rechnung trägt als der im Vorentwurf vorgesehene Ansatz. Mit Blick auf die nachfolgend nur kursorisch diskutierten Verfahrensgarantien sollte namentlich sichergestellt werden, dass das *rechtliche Gehör* der Inhaltsanbieter und der ISP (hier der Hosting- und Access-Provider) schon *vor Erlass der Sperrverfügung* gewahrt wird und nicht erst im Rahmen eines Einspracheverfahrens, wie im Vorentwurf vorgesehen (Art. 66e VE-URG). Ausnahmen hiervon sollten, ähnlich wie bei superprovisorischen Verfügungen[22], nur bei besonderer Dringlichkeit gemacht werden. Zudem sollte auch

---

19 <transparencyreport.google.com/https/overview?hl=en>.

20 Erläuternder Bericht zu zwei Abkommen der Weltorganisation für Geistiges Eigentum und zu Änderun gen des Urheberrechtsgesetzes vom 11. Dezember 2015 (zit. Erläuternder Bericht URG 2015), <www.ejpd.admin.ch/dam/data/ejpd/aktuell/news/2015/2015-12-11/vn-ber-d.pdf>, 78.

21 Ebenda.

22 Art. 265 Abs. 1 ZPO setzt eine qualifizierte Dringlichkeit voraus. Es muss ein nicht leicht wieder gutzumachender Nachteil drohen, der nicht im gewöhnlichen Massnahmeverfahren beseitigt werden kann (T. Sprecher, in: K. Spühler/L. Tenchio/D.

den *Endnutzern eine Möglichkeit zur Einsprache* gewährt werden, zumal Netzsperren auch in deren Grundrechte eingreifen[23]. Da kaum mit Einsprachen einzelner Endnutzer zu rechnen ist, sollte die Möglichkeit zur Erhebung einer Einsprache auch *Organisationen mit ideeller Zwecksetzung, bspw. Konsumentenorganisationen*, eingeräumt werden – auch wenn diese in anderen Bereichen von diesem Mittel bisher kaum Gebrauch gemacht haben[24]. Sinnvoll wäre überdies, von den Rechteinhabern zu verlangen, dass sie mit angemessenen Mitteln versucht haben, die Entfernung der ohne ihre Zustimmung zugänglich gemachten Werke von der infrage stehenden Webseite zu erwirken, bevor sie bei der zuständigen Behörde den Erlass von Netzsperren verlangen. Eine blosse Abmahnung *(notice)* wird dabei genügen müssen. Auch hier wird man in Fällen besonderer Dringlichkeit auf eine vorgängige Abmahnung verzichten und direkt den Erlass einer Sperre verlangen dürfen. Unabdingbar ist schliesslich, dass die für den Erlass von Netzsperren zuständige *Behörde* über einen *ausreichenden Ermessensspielraum* verfügt, der es ihr erlaubt, den Nutzen von Sperren in jedem Einzelfall gegenüber den Kollateralschäden abzuwägen und auf den Erlass von Netzsperren zu verzichten, vor allem in Fällen von *Overblocking*[25]. Auch dieser zentrale Aspekt kommt in der Regelung des Vorentwurfs nicht zum Ausdruck. Man mag einwenden, dass die meisten dieser Massnahmen den Aufwand für den Erlass von Netzsperren erhöhen und die Zeitspanne verlängern, die zwischen dem Antrag auf und dem Erlass von Netzsperren vergeht. Diese Nachteile sind allerdings in Kauf zu nehmen, zumal diese Massnahmen der Gewährung des rechtlichen Gehörs und der Sicherstellung angemessener Entscheide dienen.

sic! 2017 S. 701, 711

Mit Blick auf die einleitend skizzierte Ausgangslage, nach der unklar ist, ob im Parlament die Forderung nach der Einführung von Netzsperren im Urheberrecht erhoben wird und wie ein allfälliger Regelungsvorschlag aussehen könnte[26], konzentriert sich die nachfolgende rechtliche Analyse auf *grundsätzliche Überlegungen*. Soweit auf eine konkrete Regelungsvariante Bezug genommen wird, orientieren sich die Ausführungen an der Regelung des Vorentwurfes unter Hinzufügung der gerade vorstehenden skizzierten Massnahmen. Grundlage der Analyse ist damit eine *möglichst milde Regelungsvariante*, die den gegen Netzsperren erhobenen Bedenken so weit wie möglich Rechnung trägt.

2. Verfassungsrechtliche Analyse

a) Vorbemerkungen

Die Abhängigkeit der effektiven Ausübung der Kommunikationsgrundrechte von der Kommunikationsinfrastruktur wurde schon früh erkannt. Ebenso erscheint völlig unbestritten, dass vor allem die Fernmeldeordnung unter Beachtung der

---

Infanger (Hg.), Schweizerische Zivilprozessordnung, Basler Kommentar, 3. Aufl., Basel 2017, ZPO 265 N 6; für das Urheberrecht: B. K. Müller, in: B. K. Müller/R. Oertli (Hg.), Urheberrechtsgesetz (URG), Bern 2012, URG 65 N 15). Es handelt sich dabei jedoch um eine *vorläufige* Anordnung und es bestehen verschiedene Schutzmechanismen, die einen Missbrauch verhin dern sollen (möglichst rasche Ge währung des rechtlichen Gehörs gem. Art. 265 Abs. 2 ZPO; Sicherheits leistung gem. Art. 265 Abs. 3 ZPO; Schadenersatz gem. Art. 264 Abs. 2 ZPO).

23 Ebenso: EuGH vom 27. März 2014, Rs C-314/12, N 57; zu den betroffenen Grundrechten siehe hinten, III.2.b.

24 Art. 10 Abs. 2 lit. b UWG. Zur geringen praktischen Bedeutung siehe P. Jung/P. Spitz, in: P. Jung/P. Spitz (Hg.), Bundesgesetz gegen den unlauteren Wettbewerb (UWG), 2. Aufl., Bern 2016, UWG 10 N 33. Als Grund wird auch die mangelnde Finanzkraft von Konsumentenorganisationen angeführt, vgl. Botschaft zur Änderung des Bundesgesetzes gegen den unlauteren Wettbewerb (UWG) vom 2. September 2009, 6151 f., 6160. Erfolgreicher erscheinen die ideellen Verbandsbeschwerden nach Art. 55 ff. USG und Art. 12 ff. NHG.

25 Vgl. Benhamou (Fn. 11), 527, der im Rahmen der Verhältnismässigkeitsprüfung ein generelles Verbot von Overblocking statuiert.

26 Siehe dazu vorn, I.

Kommunikationsgrundrechte auszugestalten ist[27]. Als eher neuere Entwicklung ist festzustellen, dass die Bereitstellung qualitativ hochstehender Fernmeldedienste ganz allgemein eine zentrale Voraussetzung für die Teilnahme am gesellschaftlichen und wirtschaftlichen Leben ist[28]. Entsprechend gewährleistet auch die Verfassung ein zeitgemässes, immer wieder an die gesellschaftlichen und wirtschaftlichen Entwicklungen sowie den Stand der Technik anzupassendes Portfolio von Grundversorgungsdiensten; dieses umfasst auch den Datenverkehr[29].

Die fortschreitende Digitalisierung von gesellschaftlichen und wirtschaftlichen Prozessen schafft eine zunehmende Abhängigkeit dieser Prozesse von der Kommunikationsinfrastruktur, die weit über eigentliche Kommunikationsvorgänge hinausreicht. Entsprechend gewährleistet nur ein angemessener Zugang zu dieser Infrastruktur die Funktionsfähigkeit solcher Prozesse. Die am 27. Juni 2017 ergangene Entscheidung der EU-Kommission betreffend den angeblichen Missbrauch der marktbeherrschenden Stellung von Google als Suchmaschinenbetreiber[30] illustriert eindrücklich, dass unternehmerischer Erfolg heute in fast allen Bereichen auf fortgeschrittene IT-Dienstleistungen angewiesen ist. Entsprechend sind staatliche Beschränkungen des Zugangs zur IT-Infrastruktur in hohem Masse grundrechtsrelevant, selbst wenn diese die freie Kommunikation im engeren Sinn unangetastet lassen und «nur» den Datenverkehr in anderen Zusammenhängen betreffen[31]. Dennoch werden Netzsperren in verschiedenen europäischen Ländern aus unterschiedlichen Gründen eingesetzt und es kann nicht davon ausgegangen werden, dass diese Sperren *per se* gegen die Grundrechte verstossen würden[32].

b) Betroffene Grundrechte

Netzsperren können je nach dem verfolgten Zweck verschiedene Grundrechte verschiedener Grundrechtsträger in jeweils unterschiedlichem Ausmass tangieren. Dabei ist es irrelevant, ob Netzsperren von privaten – und damit nicht grundrechtsgebundenen – ISP umgesetzt werden[33]. In einer losgelöst vom konkreten Einzelfall erfolgenden Untersuchung wie der vorliegenden müssen Netzsperren in jeder vorstellbaren Konstellation einer Rechtfertigung zugänglich sein; es handelt sich ja bei den infrage stehenden Individualrechten definitionsgemäss um individuell

---

27 P. Hettich/T. Steiner, in: B. Ehrenzeller/ B. Schindler/R. Schweizer/K. A. Vallender (Hg.), Die Schwei zerische Bundesverfassung, St. Galler Kommentar, 3. Aufl., Zürich 2014, BV 92 N 6 m.w.H.

28 Art. 1 Abs. 1 FMG; Bundesrat, Fernmelde bericht 2014, 15. So auch EGMR 3111/2010 vom 18. Dezem ber 2012, «Ahmet Yildirim c. Türkei», N 54: «the Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest».

29 Art. 92 Abs. 2 BV; Art. 16 Abs. 3 FMG; Bundesrat, Fernmeldebericht 2014, 15; so auch SGK-Hettich/Steiner (Fn. 27), BV 92 N 16. Die Grundversorgung umfasst ab 1. Januar 2018 einen multifunktionalen Anschluss, der eine minimale Datenübertragungsrate für den Internetzugang von 3000/300 kbits/s aufweist. Die am 27. April 2016 eingereichte und am 30. Mai 2017 vom Nationalrat angenommene Motion 16.3336 von Martin Candinas verlangt nun gar eine Erhöhung der Internet-Mindest geschwindig keit in der Grundversorgung auf 10 Mbit/s.

30 European Commission, Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service – Factsheet, MEMO/17/1785, 27. Juni 2017, <europa.eu/rapid/press-release_MEMO-17-1785 en.htm>.

31 Nicht thematisiert wird vorliegend die Vereinbarkeit der «Sperrung» von teilweise sicherlich legalen Angeboten im Ausland unter Aspekten des GATT/GATS und des FHA mit der EU. Dazu etwa WTO, «United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services», DS285, AB vom 30. März 2007.

32 Siehe für einen Überblick EGMR vom 18. Dezember 2012, 3111/2010, «Ahmet Yildirim c. Türkei», N 31 ff.

33 So auch im Zusammenhang mit der Vorratsdatenspeicherung das deutsche BVerfGE vom 2. März 2010, 125, 260 ff., N 190 und 193, Entscheid vom 2. März 2010. Ferner EuGH vom 8. April 2014, Rs C-293/12 und C-594/12.

durchsetzbare und damit auch individuell zu gewährleistende Grundrechte. Aufgrund des mit Netzsperren fast unweigerlich vorhandenen Risikos des Overblocking, aber auch wegen der Zulässigkeit von Streaming und Download zum Privatgebrauch[34], müssen Netzsperren auch für diejenigen Betroffenen rechtfertigbar sein, die als rechtmässig handelnde Drittpersonen

sic! 2017 S. 701, 712

von der Sperre tangiert sind. Losgelöst vom konkreten Einzelfall erscheint es hier jedoch ausreichend, wenn die Regelung der Netzsperren verfassungskonform interpretiert werden kann[35].

Betroffen ist zunächst offensichtlich die *Informationsfreiheit*, weil Netzsperren auf die Verhinderung des Zugangs zu urheberrechtlich geschützten Werken zielen, die ohne Zustimmung der Rechteinhaber auf dem Web zugänglich gemacht werden[36]. Korrespondierend betroffen sind die *Meinungsäusserungs- und die Medienfreiheit*, wenn Netzsperren den Zugriff auf Informationen verhindern (oder zumindest erschweren), die von Individuen oder Medien auf der gesperrten Webseite zugänglich gemacht wurden, vor allem als Folge eines Overblocking[37]. Betroffen ist zudem die *Wirtschaftsfreiheit*, weil Netzsperren die zu deren Einsatz verpflichteten ISP direkt in ihren rechtlichen Befugnissen zur Ausübung ihrer Tätigkeit einschränken. Ebenso können privatwirtschaftliche Anbieter von – rechtmässig angebotenen – medialen und (anderen) audiovisuellen Inhalten[38] je nach Ausgestaltung der Netzsperren zwar nicht in ihren rechtlichen Befugnissen, aber zumindest faktisch in ihrem Geschäftsgebaren in einem relevanten Ausmass eingeschränkt sein, weil eine Vertriebsmöglichkeit beeinträchtigt wird[39].

Soweit Netzsperren mit der Untersuchung von Datenpaketen verbunden sind, ist auch die *persönliche Freiheit* in verschiedener Intensität betroffen, hier im Besonderen das Recht auf Privatsphäre und auf informationelle Selbstbestimmung (Art. 13 BV)[40]. Dabei ist unbestritten, dass das Fernmeldegeheimnis (siehe den in Konkretisierung von Art. 13 BV ergangenen Art. 43 FMG) technologieneutral ausgestaltet ist und damit auch zeitgemässe Kommunikationsmittel erfasst[41]. Wie im Bereich der Strafverfolgung

---

34 Siehe dazu hinten, III.3.b.

35 So in Anlehnung an das Bundesgericht in ständiger Rechtsprechung, etwa BGer vom 27. März 2014, 2C-1076/2012, E. 2.4 (nicht aufgenommen in BGE 140 I 176).

36 Wobei hier der Verlust des Zugangs zu einer wichtigen Informationsquelle ausreichend sei; EGMR vom 11. März 2014, 20877/10 vom 11. März 2014, «Yaman Akdeniz c. Türkei», Medialex 2014, 209 ff. (mit Anmerkungen von F. Zeller). Vor allem auf die Gewährleistung des Zugangs zu Informationen abstellend auch der EuGH vom 27. März 2014, Rs C-314/12, N 62 ff.

37 Dazu EGMR vom 18. Dezember 2012, 3111/2010, «Ahmet Yildirim c. Türkei», Medialex 2013, 87 f. (mit Anmerkungen von P. Gilliéron). Das Overblocking betraf hier konkret wissenschaftliche und damit von Art. 10 EMRK geschützte Arbeiten. Auf die dogmatische Frage, ob in der Einschränkung der Zugänglichmachung fremder, urheberrechtlich geschützter Werke ein Eingriff in den Schutzbereich einer als umfassend verstandenen Meinungsäusserungsfreiheit zu erblicken ist, wird hier mangels Relevanz für das Ergebnis nicht eingegangen; siehe dazu aber etwa S. Macciacchini, Urheberrecht und Meinungsfreiheit, Bern 2000, 57 ff.

38 Dazu P. Hettich, Regulierung von audiovisuellen Abrufdiensten (Video On Demand) – Nur eine Frage des Nachvollzugs der neuen europäischen Richtlinie 2007/65/EG?, ZBl 2009, 349 ff., 358 f. m.w.H.

39 Zur Einschränkung des Vertriebs BGE 52 I 293 ff. (Verbot der Benutzung von Motorfahrzeugen beim Hausieren). Zu faktischen Einschränkungen in Bezug auf die Wirtschaftsfreiheit BGE 130 I 26 f. E. 4.4. In Bezug auf die Eigentumsgarantie BGE 126 I 213 E. 1b/bb; bestätigt in BGer vom 29. September 2000, 1P.134/2000, E. 2d.

40 So auch im Zusammenhang mit der Vorratsdatenspeicherung das deutsche BVerfGE, Entscheid vom 2. März 2010, 125, 260 ff., N 192.

41 S. Breitenmoser/R. J. Schweizer, in: B. Ehren zeller/B. Schindler/R. Schweizer/K. A. Vallender (Hg.), Die Schweizerische Bundesverfassung, St. Galler Kommentar, 3. Aufl., Zürich 2014, BV 13 N 64; O. Diggelmann, in: B. Waldmann/E. A. Belser/A. Epiney (Hg.), Basler Kommentar, Bundes ver fassung, Basel 2015, BV 13 N 29; J. P. Müller/M. Schefer , Grundrechte in der Schweiz, 4. Aufl., Bern 2008, 202 f.

handelt es sich bei solchen Überwachungsmassnahmen um schwere Eingriffe in die Privatsphäre, die nur unter strengen Voraussetzungen zulässig sein können[42].

Ob die *persönliche Freiheit* auch das Surfen im Web als solches schützt, ist heute unklar. Zwar verlangt die persönliche Freiheit nach der Gewährung eines Freiraums für die Entfaltung der Persönlichkeit. Allerdings schützen Art. 10 Abs. 2 BV und Art. 8 EMRK nur «wesentliche» Ausdrucksmöglichkeiten der Persönlichkeit[43]. Mit Blick auf die Regelung von Netzsperren im Geldspielgesetz[44] ist dabei bemerkenswert, dass nach der Lehre und Rechtsprechung das Recht des Spiels am Geldspielautomaten (auch virtuell) nicht unter die persönliche Freiheit fällt, wohl aber das generelle Recht auf Spielen[45]. Das Bundesgericht konkretisiert den Schutzbereich der persönlichen Freiheit im Einzelfall, abhängig von der Intensität des Eingriffs und der Schutzwürdigkeit des Betroffenen[46]. Dabei weist es auch gerne auf die Fürsorgepflicht des Staates hin, wobei die Grenze zwischen Selbstbestimmung und staatlicher Fürsorge nur vor dem Hintergrund einer umfassenden Interessenabwägung gezogen werden könne[47]. Eine allgemeine Handlungsfreiheit, welche den Einzelnen gegen jegliche staatlichen Eingriffe in seine Lebensgestaltung schützt, gewährleistet der Anspruch auf persönliche Freiheit allerdings weder nach der Bundesverfassung noch nach dem Konventionsrecht[48]. Diese geringe Reichweite der persönlichen Freiheit wurde vor

dem Hintergrund eines um sich greifenden Präventionsrechts auch schon kritisiert, da mit dem Ausgreifen des Schutzes die Förderung der Risikomündigkeit des Bürgers auf der Strecke bleiben muss[49].

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)[50]. Dabei ist das Verfahren keineswegs «grundrechtsneutral»; es hat vielmehr erhebliche Auswirkungen auf das materielle Recht und ist entsprechend mit Blick auf die bestmögliche Verwirklichung der Grundrechte auszugestalten[51]. Bedenken weckt hier die Wahrung des rechtlichen Gehörs, zumal die Eröffnung der Verfügung von Netzsperren regelmässig nicht durch direkte Mitteilung an alle Betroffenen, sondern im Bundesblatt unter Verweis auf sog. *Sperrlisten* erfolgt, 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. Hinsichtlich dieser Rechteinhaber ist bei Erlass von Netzsperren unklar, ob sie für das Zugänglichmachen ihrer Werke auf der betreffenden Webseite eine Lizenz erteilt haben

---

42 BSK-Diggelmann (Fn. 41), BV 13 N 29.

43 C. Grabenwarter/K. Pabel, Europäische Menschenrechtskonvention, Juristische Kurz-Lehrbücher, 6. Aufl., München 2016, § 22 N 13.

44 Siehe dazu vorn, I.

45 R. J. Schweizer, in: B. Ehrenzeller/B. Schindler/R. Schweizer/K. A. Vallender (Hg.), Die Schweizerische Bundesverfassung, St. Galler Kommentar, 3. Aufl., Zürich 2014, BV 10 N 41 m.H.a. BGE 101 Ia 336, 347 E. 7b.

46 BGE 133 I 58, 66.

47 BGE 130 I 16, 20.

48 BGE 130 I 369, 373; BGer vom 27. April 2006, 6P.25/2006, EuGRZ 2006, 682, E. 3.1. Siehe auch SGK-Schweizer (Fn. 45), BV 10 N 25.

49 Zu diesem Abschnitt P. Hettich, Kooperative Risikovorsorge, Zürich 2014, N 136 ff., N 143.

50 Wobei eine Popularbeschwerde nicht vorgesehen werden muss; EGMR vom 11. März 2014, 20877/10, «Yaman Akdeniz c. Türkei», Medialex 2014, 209 ff. (mit Anmerkungen von F. Zeller).

51 P. Hettich, in: B. Ehrenzeller/B. Schindler/ R. Schweizer/K. A. Vallender (Hg.), Die Schweizerische Bundes verfassung, St. Galler Kommentar, 3. Aufl., Zürich/St. Gallen 2014, BV 97 N 8. Solche Bezüge zwischen Verfahren und Verhältnismässigkeit sind auch in F. Uhlmann, Gutachten zuhanden IFPI Schweiz betreffend Verhältnismässigkeit von Zugangssperren (unveröffent licht), 6, skizziert.

oder – auch bei fehlender Lizenzerteilung – eine Sperre ablehnen, weil sie den Zugang zu ihren Werken nicht unterbinden wollen. Gerade in den besonders relevanten Fällen, in denen der Zugriff auf Webseiten gesperrt werden soll, auf denen sich eine Vielzahl von Werken befindet, ist nicht ersichtlich, wie das rechtliche Gehör aller Rechteinhaber gewahrt werden kann. Dies nicht nur wegen der Menge der betroffenen Werke, sondern auch, weil oft nicht ohne Weiteres erkennbar ist, wer die Rechteinhaber sind und wie diese über die Netzsperren informiert werden können. Fraglich erscheint auch, ob der *Begründungspflicht* als Teil des rechtlichen Gehörs durch den Erlass von Sperrlisten Genüge getan werden kann[52]. Ferner ist zu beachten, dass Endnutzer kaum geneigt sein dürften, für die Durchsetzung ideeller Interessen, hier also für den ungehinderten Zugang zu ungerechtfertigt gesperrten Inhalten, grössere Kosten auf sich zu nehmen. Schliesslich sind allenfalls auch direkt in ihren Rechten betroffene ISP nicht geneigt, im Interesse ihrer Kunden und eines «freien» Internets Rechtsmittel gegen die Sperrlisten zu ergreifen, zumal Netzsperren auch die Interessen der ISP als Inhaltsanbieter befördern dürften[53].

Schliesslich ist der Staat auch ausserhalb der Grundrechte an bestimmte *Grundsätze rechtsstaatlichen Handelns* gebunden[54]. Sein Handeln muss also stets auf einem Rechtssatz beruhen, im öffentlichen Interesse liegen und verhältnismässig sein. Bei der Prüfung dieser allgemeinen Grundsätze legt das Bundesgericht allerdings keinen strengen Massstab an[55].

c) Gesetzliche Grundlage

Der Erlass von Netzsperren stellt einen schweren Eingriff in die grundrechtlich geschützte freie Kommunikation dar[56]. Für eine entsprechende Regelung ist deshalb eine Grundlage im formellen Gesetz zu fordern (Art. 36 Abs. 1 BV), an deren Präzision hohe Anforderungen zu stellen sind[57]. Da vorliegend auch Konventionsrechte betroffen sind, die das Bundesgericht selbst bei Bundesgesetzen durchsetzt, kann sich der Gesetzgeber bei der Formulierung einer

---

52 Allerdings ist es bei der Eröffnung von Verfügungen durch amtliche Publikation üblich, dass die Begrün dung wegen Platzproblemen und zur Wahrung der Vertraulichkeit nicht veröffentlicht wird. Es ist deshalb eine Nachfrage bei der verfügenden Behörde er forderlich; siehe dazu F. Uhlmann/ A. Schilling-Schwank, in: B. Waldmann/P. Weis sen berger (Hg.), Praxiskommentar zum Bundesgesetz über das Verwaltungsverfahren, 2. Aufl., Zürich 2016, VwVG 36 N 4 und N 8 ff. Für die hier infrage stehenden Netzsperren ist die Veröffentlichung im Bundesblatt aber unbehelflich, weil sich die be troffenen Webseiten-Betreiber im Ausland befinden und eine amtliche Publikation in der Schweiz deshalb kaum zur Kenntnis nehmen werden. Ohnehin ist die Sperrung ihrer Webseite für sie kaum erkennbar. Beides gilt erst recht für die Rechteinhaber, die von Overblocking betroffen sind.

53 Siehe illustrativ BGE 137 II 199 zu überhöhten Terminierungspreisen im Mobilfunk, wo an sich kein Telekommunikationsunternehmen Interesse an der Durchsetzung einer Senkung haben konnte. Hierzu nun UVEK, Erläuterungsbericht zur Änderung des Fernmeldegesetzes vom 11. Dezember 2015, 16.

54 Art. 5 BV.

55 BGE 138 I 378, 393, 397 f., wo das Bundesgericht im Zusammenhang mit einem öffentlichen Unterneh men von materiellrecht lichen und prozessualen Konsequenzen für den Prüfmassstab spricht. Art. 5 BV könne «ausserhalb von Grundrechtseingriffen bzw. der Eingriffsverwaltung nicht die gleiche Tragweite haben wie im Rahmen von Art. 36 BV».

56 Zu den betroffenen Grundrechten siehe vorn, III.2.b.

57 So im Zusammenhang mit Strafverfolgungshandlungen BSK-Diggelmann (Fn. 41), BV 13 N 30. All gemein dazu R. J. Schweizer, in: B. Ehrenzeller/B. Schindler/R. Schweizer/ K. A. Vallender (Hg.), Die Schwei zeri sche Bundesverfassung, St. Galler Kommentar, 3. Aufl., Zürich 2014, BV 36 N 16 ff.

Regelung nicht zu sehr auf sein in Art. 190 BV statuiertes Massgeblichkeitsprivileg verlassen[58].

d) Öffentliches Interesse

Mit Netzsperren im Urheberrecht soll in erster Linie der Schutz von Eigentumsrechten Dritter (Immaterialgüterrechte)[59] sichergestellt werden (Art. 36 Abs. 2 BV). Mit Blick auf die Strafbarkeit des Zugänglichmachens urheberrechtlich geschützter Werke (Art. 67 Abs. 1 lit. g[bis] URG) dienen Netzsperren aber auch der Bekämpfung von Kriminalität (polizeiliche Interessen, Schutz der Rechtsordnung)[60]. Netzsperren liegen somit grundsätzlich im öffentlichen Interesse bzw. dienen dem Schutz von Grundrechten Dritter.

e) Verhältnismässigkeit

aa) Eignung

Eine Massnahme muss zunächst geeignet sein, einen Beitrag zur Erreichung des verfolgten Ziels zu leisten. Dabei reicht es bereits aus, wenn die Massnahme in Bezug auf das verfolgte Ziel nicht wirkungslos oder gar kontraproduktiv ist[61]. Die Geeignetheit müsste vorliegend allerdings näher hinterfragt werden, wenn von informiert und rational handelnden Menschen ausgegangen wird, die – wie vorstehend ausgeführt[62] – Netzsperren leicht umgehen können. Zumindest für einen Teil der Endnutzer dürften jedoch verschiedene verhaltenspsychologische Phänomene ausreichend stark wirken, um von einem Besuch der «gesperrten» Seiten abzuhalten[63]. Auf Basis dieser Annahme wären Netzsperren zumindest für einen Teil der Endnutzer als geeignet

---

58 Zu partiellen Verfassungsgerichtsbarkeit aufgrund des Primats des Völkerrechts ausführlich M. E. Looser, Verfassungsgerichtliche Rechtskontrolle gegenüber schweizerischen Bundesgesetzen, Eine Be standesaufnahme unter Berücksichtigung der amerikanischen und deutschen Verfassungsgerichtsbarkeit, der Geschichte der schweizerischen Ver fassungsgerichtsbarkeit sowie der heutigen bundesgerichtlichen Praxis, St. Galler Schriften zur Rechtswissenschaft, Bd. 21, Zürich 2011, 937 ff.

59 BGer vom 11. Februar 1993, 1P.465/1991 und 1P.183/1992 zu Zwangsräumungen (= BGE 119 Ia 28 = ZBl 1993, 378 ff.). Dazu allgemein K. A. Vallender/P. Hettich/ J. Lehne, Wirtschafts freiheit und begrenzte Staatsverantwortung, Grundzüge des Wirtschaftsverfassungs- und Wirtschaftsver waltungsrechts, 4. Aufl., Bern 2006, § 6 N 18. Als Grund für Einschränkungen der Meinungsäusserungs freiheit erwähnt ist der Schutz der Rechte anderer auch in Art. 10 Abs. 2 EMRK.

60 SGK-Schweizer (Fn. 57), BV 36 N 32.

61 Zu dieser geringen Hürde etwa Hettich (Fn. 49), N 483 m.w.H.

62 Siehe dazu vorn, II.3.b.

63 Zur Effektivität der Sperren etwa Cory (Fn. 3), 18 f.; Incopro, Site blocking efficacy in Portugal, September 2015 to February 2016 (zit. Incopro, Site blocking Por tugal), Mai 2016, <www.incoproip.com/wp-content/uploads/2016/10/Site-Blocking-and-Piracy-Landscape-in-Portugal-NPM.pdf>, 3; Incopro, Site blocking efficacy study, United Kingdom (zit. Incopro, Site blocking UK), 13. November 2014, überarbeitete Version vom 19. März 2015, <www.incoproip.com/wp-content/uploads/2016/11/Site-Blocking-Efficacy-UK-revised-19-03-2015.pdf>, 4. Dieselben verhaltenspsycholo gischen Phänomene, welche einen Teil der Endnutzer von der Umgehung der Sperre abhalten, dürften jedoch auch Wirkung über den intendierten Zweck hinaus zeigen (z. B. das Gefühl, dauernd beobachtet und kontrolliert zu werden). Abschreckende Effekte dieser Art sind bei der rechtlichen Ausgestaltung der kommunikativen Infrastruktur zu berücksichtigen (SGK-Hettich/Steiner [Fn. 27], BV 92 N 6). So führt das deutsche Bundesverfassungsgericht (BVerfGE Entscheid vom 2. März 2010, 125, 260 ff., N 241) im Zusammenhang mit der Vorratsdatenspeicherung aus, diese sei «deshalb ein so schwerwiegender Eingriff, weil sie ein Gefühl des ständigen Überwachtwerdens hervor rufen kann; sie erlaubt in unvorhersehbarer Weise tiefe Einblicke in das Privatleben, ohne dass der Rück griff auf die Daten für den Bürger unmittel bar spürbar oder ersichtlich ist. Der Einzelne weiß nicht, was welche staatliche Behörde über ihn weiß, weiß aber, dass die Behörden vieles, auch Höchstpersönliches über ihn wissen können.».

anzusehen, auch wenn sich vermutlich gerade die Vielnutzer, die mit Netzsperren in erster Linie erfasst werden sollen, kaum von diesen beeindrucken lassen[64].

Ausländische Studien zeigen, dass Netzsperren bei einem Grossteil der Endnutzer wirken und nur in geringem Ausmass umgangen werden[65]. Zu beachten ist allerdings, dass in den untersuchten Ländern die Nutzung von nicht lizenzierten Angeboten zum Privatgebrauch – anders als in der Schweiz[66] – nicht von einer Schranke freigestellt ist. Entsprechend wäre zu klären, ob die abschreckende Wirkung von Netzsperren in diesen Ländern – zumindest auch und möglicherweise sogar primär – darauf zurückzuführen ist, dass die Endnutzer die gesperrten

sic! 2017 S. 701, 715

Angebote nicht nutzen dürfen und mit zivil- oder gar strafrechtlichen Sanktionen rechnen müssen[67], wenn sie es trotzdem tun. Eine allfällige *Informationsseite*, auf welche die Endnutzer mittels Netzsperren weitergeleitet werden, müsste die in der Schweiz geltende Rechtslage jedenfalls korrekt wiedergeben, den Endnutzern also mitteilen, dass das Anbieten der fraglichen Werke zwar unzulässig, die Nutzung dieses Angebots durch die Endnutzer aber zulässig ist. Die abschreckende Wirkung einer solchen Mitteilung dürfte gering sein. Vielmehr müssten die Behörden damit den Widerspruch offenlegen, den die Einführung von Netzsperren im Urheberrecht schaffen würde, indem mittels Sperren zu verhindern versucht würde, was rechtlich erlaubt ist[68]. Netzsperren könnten in der Schweiz bei den Endnutzern deshalb eine deutlich geringere Wirkung entfalten als im Ausland.

bb) Erforderlichkeit

Die Massnahmen müssen für das Erreichen des angestrebten Ziels erforderlich sein. Daran fehlt es, wenn das Ziel mit einem gleichermassen geeigneten, aber milderen Mittel ebenso gut erreicht werden kann[69]. 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 führen würden. Sicherzustellen ist somit,

---

64 So führt BVerfGE vom 2. März 2010, 125, 260 ff., N 207, im Zusammenhang mit der anlass losen Vorratsdatenspeicherung aus: «Auch wenn eine solche Datenspeicherung nicht sicherstellen kann, dass alle Telekommunikationsverbindungen verlässlich bestimmten Anschlussnehmern zugeordnet wer den können, und etwa Kriminelle die Speicherung durch die Nutzung von Hotspots, Internetcafés, ausländischen Internettelefondiensten oder unter falschen Namen angemeldeten Prepaid-Handys unter laufen können, kann dies der Geeignetheit einer solchen Regelung nicht entgegenhalten werden. Diese erfordert nicht, dass das Regelungsziel in jedem Einzelfall tatsächlich erreicht wird, sondern verlangt lediglich, dass die Zweckerreichung gefördert wird.» Ein materieller Entscheid zum parallel ge lagerten deutschen Gesetz zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen (Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen) vom 17. Feb ruar 2010 fehlt, da auf eine Beschwerde nicht eingetreten wurde (BVerfG vom 29. März 2011, 1 BvR 508/11, N 1 ff.). Das Zugangserschwerungsgesetz wurde dennoch faktisch nicht angewendet und vorzeitig aufgehoben. Die Geeignetheit bejahend auch Uhlmann (Fn. 51), 7 ff.

65 Cory (Fn. 3), 19 ff.; Incopro, Site blocking UK (Fn. 63), 7 ff.; Incopro, Site blocking Portugal (Fn. 63), 10 ff. A.A. Schweizerisches Institut für Rechtsvergleichung, Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content, Lausanne 2015, 789, wonach Netzsperren im Allgemeinen nicht sehr effektiv seien.

66 Siehe dazu hinten, III.3.b.

67 EuGH vom 10. April 2014, Rs C-435/12, N 58 und Dispositiv Ziff. 1. Bestätigt in EuGH vom 5. März 2015, Rs C-463/12, N 74 ff. Siehe auch O. Jani, Reformbedarf der privaten Vervielfältigung aus Sicht der Praxis, Zeitschrift für geistiges Eigentum 2015, 196 ff., 200. Die ausländischen Studien zur Effekti vität von Netzsperren untersuchten den Effekt nur für Zeiträume nach der Klarstellung durch den EuGH.

68 Siehe dazu hinten, III.3.b.

69 BGE 140 I 353, 373 f. E. 8.7; BGE 137 I 31, 53 ff. E. 7.5.2; BGE 136 I 87, 92 ff. E. 3.2; BGE 133 I 77, 81 ff. E. 4.1; R. Kiener/W. Kälin, Grundrechte, 2. Aufl., Bern 2013, 121; U. Häfelin/G. Müller/F. Uhlmann, Allgemeines Verwaltungsrecht, 7. Aufl., Zürich 2016, N 527.

dass Massnahmen in sachlicher, räumlicher, zeitlicher und personeller Hinsicht nicht über das Notwendige hinausgehen[70].

Als Alternative zu Netzsperren drängt es sich auf, die ohne Zustimmung der Rechteinhaber zugänglich gemachten Werke von den Servern der Anbieter löschen zu lassen *(Löschen statt Sperren).* Während dieser Ansatz in einem rein nationalen Kontext sicherlich vorzuziehen, wenn nicht gar geboten ist, vermag er die Probleme bei der (internationalen) Rechtsdurchsetzung kaum zu lösen, weil Anbieter ihren Sitz verschleiern, ständig wechseln oder in einem Land operieren, in welchem die Durchsetzung von Löschungsansprüchen von vornherein aussichtslos ist. Will der Gesetzgeber den Rechteinhabern hier effektive Rechtsbehelfe verschaffen, sind für diese Fälle kaum Alternativen zu Netzsperren ersichtlich. Allerdings könnten Massnahmen mit Overblocking leicht als überschiessend und damit als nicht erforderlich angesehen werden. Mit anderen Worten ist nicht zu verkennen, dass Netzsperren relativ breit sowohl auf lizenzierte wie auch auf nicht lizenzierte Angebote einwirken, und zwar nur indirekt, da sich an der Verfügbarkeit der nicht lizenzierten Angebote auf dem Web durch das blosse Sperren des Zugriffs nichts ändert. Aufgrund der geringen Wirkung von Netzsperren – die Angebote sind weiter verfügbar und die Sperren können umgangen werden – ist die Erforderlichkeit dieses breit wirkenden und institutionell schwach abgesicherten Instruments ganz grundsätzlich infrage gestellt. Oder mit den Worten von F. Fleiner: «Die Polizei soll nicht mit Kanonen auf Spatzen schiessen.»[71]

Hinzu kommt, dass gezieltere und mildere Massnahmen, namentlich die blosse Information der Endnutzer *(Informieren statt Sperren)*, gar nicht erst versucht wurden, sodass generell wenig empirische Evidenz zum Nutzen der verschiedenen Instrumente bestehen[72]. Ein auf blosser Information beruhender Ansatz scheint gerade in der Schweiz naheliegend, weil Netzsperren im Kommunikationsvorgang aufseiten der Endnutzer eingreifen, deren Handlungen urheberrechtlich zulässig sind. Allerdings lässt sich die Information, bspw. durch Umleitung der Endnutzer auf eine Informationsseite des Bundes, angesichts der technischen Entwicklung nur beschränkt und immer schlechter umsetzen, und zwar unabhängig davon, ob sie mit einer Netzsperre verbunden wird oder nicht. Der zunehmende Einsatz von Sicherheitsmechanismen (z. B. HPKP und DNSSEC) verhindert nämlich derartige Umleitungen und führt dazu, dass dem Endnutzer anstelle der Informationsseite eine generische Fehlermeldung angezeigt wird[73]. Die Informationsfunktion der Netzsperre wird damit weitgehend vereitelt.

cc) Zumutbarkeit

Die anvisierte Massnahme muss den einzelnen Betroffenen schliesslich auch zumutbar sein. Dabei ist eine Abwägung vorzunehmen zwischen den öffentlichen Interessen an der Massnahme einerseits und den privaten Interessen der Betroffenen andererseits[74]. Wie auf-

gezeigt, reichen die involvierten Interessen vom Schutz der Eigentumsrechte von Dritten (Immaterialgüterrechte) bis zur Bekämpfung der damit verbundenen Kriminalität (polizeiliche Interessen, Schutz der Rechtsordnung)[75]. Bei den privaten Interessen fallen v.a. die Interessen der ISP an einer uneingeschränkten Ausübung ihrer Tätigkeit

---

70 BGE 142 I 49, 69 E. 9.1 m.w.H.; Kiener/ Kälin (Fn. 69), 121; Häfelin/Müller/ Uhlmann (Fn. 69), N 530.

71 F. Fleiner, Institutionen des Deutschen Verwaltungsrechts, 1. Aufl., Tübingen 1911, 323.

72 Zur Wichtigkeit interdisziplinärer Ansätze bei der Prüfung der Verhältnismässigkeit M. Müller, Verhältnismässigkeit, Gedanken zu einem Zauberwürfel, Kleine Schriften zum Recht (KSR), Bern 2013, 35 ff.

73 Siehe dazu vorn, II.3.c.ii, insb. Fn. 18.

74 Häfelin/Müller/Uhlmann (Fn. 69), N 556 f.; Kiener/Kälin (Fn. 69), 123; U. Häfe lin/ W. Haller/H. Keller/ D. Thurn herr, Schweizerisches Bundesstaatsrecht, 9. Aufl., Zürich 2016, N 323.

75 Siehe dazu vorn, III.2.b.

und die Interessen der Endnutzer am ungefilterten Zugang zu den Inhalten des Web ins Gewicht.

Für die *ISP* scheint die Durchführung von Netzsperren nicht unzumutbar, solange ihr Aufwand überschaubar bleibt und sie von den Rechteinhabern hierfür auch entschädigt werden[76]. Ins Gewicht fällt dagegen, dass den *Endnutzern* die Nutzung der gesperrten Webseite nach der geltenden Rechtslage erlaubt ist und sie für diese Nutzung, sofern sie dabei Werke auf im Handel erhältlichen Datenträgern speichern, grundsätzlich sogar bezahlen[77]. Hier besteht denn auch ein zentraler Unterschied zur Regelung von Netzsperren im Fernmeldegesetz[78]. Denn Netzsperren können weit eher als zumutbar qualifiziert werden, wenn kein schutzwürdiges Interesse am Zugang zu den Inhalten der gesperrten Webseiten besteht, weil die Inhalte selbst mit den Vorgaben der Rechtsordnung kollidieren, wie namentlich bei harter Pornografie. Als unzumutbar erscheint eine Sperre hingegen dann, wenn die Nutzung der gesperrten Webseite rechtlich erlaubt ist.

Hinzu kommt die Gefahr des *Overblocking*. Dabei ist auf Basis der heutigen technischen Gegebenheiten davon auszugehen, dass wirksamere Sperren generell mit einem höheren Risiko von Overblocking einhergehen. Kann die Sperre von Inhalten Dritter nicht vermieden werden, so treffen die – mit dem Schutz der Rechtsordnung vor allem auch polizeilich motivierten – Massnahmen auch unbeteiligte Dritte. Als Folge des Verhältnismässigkeitsgebots sind polizeiliche Massnahmen jedoch ganz grundsätzlich gegen den Störer zu richten, also gegen diejenigen Personen, die in einem relevanten Zusammenhang zur Störung oder Gefährdung von Polizeigütern stehen[79]. Die Lehre ist sich uneinig, ob gegen unbeteiligte Dritte nur in Fällen der polizeilichen Generalklausel oder gar nur bei Vorliegen eines Polizeinotstandes vorgegangen werden kann[80]. Dazu muss hier allerdings nicht Stellung genommen werden, denn solche Fälle liegen hier nicht vor: Ein Vorgehen gegen unbeteiligte Dritte kann ohnehin kaum zulässig sein, wenn diese Dritten – hier die Endnutzer – nicht zur Behebung des polizeiwidrigen Zustands beitragen können. Ebendies gilt aber eigentlich auch für die ISP, weil die Netzsperren nichts daran ändern, dass das rechtswidrige Angebot im Web weiterhin bestehen bleibt[81].

Verfassungskonforme polizeiliche Massnahmen können solche «Kollateralopfer» auch zum Schutz hoher Rechtsgüter kaum in Kauf nehmen, sodass Netzsperren jedenfalls bei unvermeidbarem Overblocking meist als unzumutbar erscheinen müssen[82]. Auch

---

76 So jedenfalls Art. 66d Abs. 3 VE-URG.

77 Die Leerträgerabgabe wird gem. Art. 20 Abs. 3 URG von Herstellern und Importeuren von Leerträgern entrichtet und auf die Endnutzer überwälzt. Voraussetzung ist jedoch, dass eine Nutzung von einem Tarif erfasst ist. Zur Wahrung der Privatsphäre richtet sich die Abgabe nicht nach der tatsächlichen Nutzung, sondern nach dem Nutzungspotenzial. Die heute geltenden Tarife sehen u. a. Ver gütungen für Speicher von Mobiltelefonen und Tablets vor, nicht erfasst werden aber in PCs verbaute Festplatten. Diese Nutzungen sind damit faktisch vergütungsfrei.

78 Siehe dazu vorn, I.

79 Unterschieden werden Verhaltens- und Zustandsstörer sowie Zweckveranlasser; dazu Häfelin/Müller/Uhlmann (Fn. 69), N 2612 ff.

80 Dazu P. Tschannen/U. Zimmerli/M. Müller, Allgemeines Verwaltungsrecht, 4. Aufl., Bern 2014, § 56 N 13; Häfelin/Müller/Uhlmann (Fn. 69), N 2627 m.w.H.

81 Uhlmann (Fn. 51), 10 f., sieht die ISP unter Hinweis auf ein Urteil des deutschen Bun desgerichtshofs vom 26. November 2015, I ZR 174/14, als Störer an. Dieser Entscheid hält jedoch einschränkend fest: «Eine Störerhaftung des Vermittlers von Internetzugängen kommt nur in Betracht, wenn der Rechte inhaber zunächst zumutbare Anstrengungen unternommen hat, gegen diejenigen Be teiligten vorzugehen, die – wie der Betreiber der Internetseite – die Rechtsverletzung selbst begangen haben oder – wie der Hosting Provider – zur Rechtsverletzung durch die Erbringung von Dienstleistungen beigetragen haben. Nur wenn die Inanspruchnahme dieser Beteiligten scheitert oder ihr jede Erfolgsaussicht fehlt und deshalb andern falls eine Rechtsschutzlücke entstünde, ist die Inanspruchnahme des Zugangsvermittlers als Störer zumutbar. Bei der Ermittlung der vorrangig in Anspruch zu nehmenden Be teiligten hat der Rechteinhaber in zumut barem Umfang Nachforschungen anzu stellen.».

82 Im Ergebnis gleich auch EuGH vom 27. März 2014, Rs C-314/12, N 62 ff. Ebenso: F. La

Erwägungen der Verwaltungsökonomie und der Praktikabilität können Beschränkungen einer prinzipiell zulässigen Freiheitsausübung höchstens in engen Grenzen rechtfertigen[83]. Durch Overblocking betroffen ist ferner auch die *Rechtsgleichheit*, weil notwendige Differenzierungen zwischen dem Sperren des Zugangs zu Werken, die mit, und solchen, die ohne Zustimmung der Rechteinhaber zugänglich gemacht

sic! 2017 S. 701, 717

worden sind, bei der Ausgestaltung und Durchführung der Netzsperren unterlassen werden[84]. Ob sich an dieser kritischen Beurteilung etwas ändern müsste, wenn Netzsperren gezielter durchgeführt, die Gefahr von Overblocking also massgeblich verringert werden könnte, erscheint äusserst fraglich, weil mit Netzsperren Nutzungen von Webseiten verhindert werden sollen, die urheberrechtlich ohne Einschränkung zulässig sind.

f) Zwischenfazit

Aus verfassungsrechtlicher Sicht kann festgehalten werden, dass Netzsperren im Lichte des heutigen Stands der Technik (Umgehungsmöglichkeiten), wegen ihrer indirekten Wirkung (Adressierung von ISP), aufgrund der potenziell bedrohten, teilweise überragenden Rechtsgüter (Grundrechte) und als Folge des kaum rechtsstaatlich einwandfrei ausgestaltbaren Rechtsschutzes (rechtliches Gehör) regelmässig als unzumutbar und damit als unverhältnismässig erscheinen. Insbesondere sind die im VE-URG vorgesehenen, nachträglichen Rechtsbehelfe als Kompensation des Overblocking wohl als unzureichend anzusehen[85].

Die Analyse nach schweizerischem Recht weicht damit bei oberflächlicher Betrachtung von der Beurteilung ab, welche der EuGH aus Sicht des *europäischen Rechts* vorgenommen hat. In seinem Urteil vom 27. März 2014 in Sachen UPC Telekabel kommt der EuGH bekanntlich zum Schluss, dass die durch das Unionsrecht anerkannten Grundrechte einer gerichtlichen Anordnung von Netzsperren nicht grundsätzlich entgegenstehen. Voraussetzung ist allerdings, dass diese Massnahmen den Endnutzern nicht unnötig die Möglichkeit vorenthalten, in rechtmässiger Weise Zugang zu den verfügbaren Informationen zu erlangen und dass sie unerlaubte Zugriffe auf geschützte Werke oder Leistungen verhindern oder zumindest erschweren, sodass die Endnutzer zuverlässig davon abgehalten werden, auf diese Schutzgegenstände zuzugreifen[86]. Der EuGH nimmt seine Beurteilung also mit Blick auf eine urheberrechtliche Rechtslage vor, die von der schweizerischen entscheidend abweicht. Die Analyse basiert nämlich auf der Annahme, dass der Zugriff der Endnutzer auf die geschützten Werke und Leistungen unerlaubt ist, was im schweizerischen Recht nicht der Fall ist[87]. In seinen Erwägungen hält der EuGH denn auch ausdrücklich fest, dass die Massnahmen der Access-Provider «streng zielorientiert» sein, also «dazu dienen

---

Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Human Rights Council, 2011, <www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>, Rz. 31; Benhamou (Fn. 11), 527. Zur grossen «Streubreite» im Zu sammenhang mit der anlass losen Vorratsdatenspeicherung auch BVerfGE vom 2. März 2010, 125, 260 ff., N 210, 213 ff. Siehe aber Urteil des deutschen Bundes gerichtshofs vom 26. November 2015, I ZR 174/14, N 54 ff., das Overblocking in geringem Umfang toleriert; verlangt sei gemäss EuGH vom 27. März 2014, Rs C-314/12, N 56, aber eine «strenge Zielorientierung».

83 B. Weber-Dürler, Verwaltungsökonomie und Praktikabilität im Rechtsstaat, ZBl 87 (1986), 193 ff., 204 ff. m.w.H.

84 BGE 125 I 173, 178; BGE 122 I 18, 25; BGE 119 Ia 123, 128. Siehe weiter B. Weber-Dürler, Die Rechtsgleichheit, in: D. Thürer/ J.-F. Aubert/J. P. Müller (Hg.), Verfassungsrecht der Schweiz, Zürich 2001, 657 ff., 661; A. Auer/G. Malinverni/M. Hottelier, Droit constitutionnel suisse, vol. II: Les droits fondamentaux, 3. Aufl., Bern 2013, 488; Kiener/Kälin (Fn. 69), 347.

85 Diesbezüglich a.M. Uhlmann (Fn. 51), 15.

86 EuGH vom 27. März 2014, Rs C-314/12, Dispositiv Ziff. 2.

87 Seihe dazu hinten, III.3.c.

müssen, der Verletzung des Urheberrechts oder eines verwandten Schutzrechts durch einen Dritten ein Ende zu setzen, ohne dass Internetnutzer, die die Dienste dieses Anbieters [sc. des Access-Providers] in Anspruch nehmen, um rechtmässig Zugang zu Informationen zu erlangen, dadurch beeinträchtigt werden. Andernfalls wäre der Eingriff des Anbieters in die Informationsfreiheit dieser Nutzer gemessen am verfolgten Ziel nicht gerechtfertigt.»[88] Die Anordnung von Netzsperren erscheint also auch nach europäischem Recht nur dann mit den Grundrechten vereinbar, wenn diese dazu dienen, einen *unrechtmässigen Zugriff auf Werke und Leistungen zu verhindern*. Grundrechtlich betrachtet stimmt die vorliegende Analyse mit derjenigen des EuGH somit überein.

3. Urheberrechtliche Analyse

a) Vorbemerkungen

Neben den zentralen verfassungsrechtlichen Überlegungen stellt sich zusätzlich die Frage, ob und gegebenenfalls inwiefern sich eine Regelung von Netzsperren ins dogmatische Konzept des schweizerischen Urheberrechts und in die bestehende Regelung der Verbotsrechte und Schranken einfügen liesse.

Für die erste Frage ist entscheidend, dass das schweizerische Urheberrecht auf der Erteilung von Ausschliesslichkeitsrechten beruht, gegen deren Verletzung der Rechteinhaber vorgehen kann. Die vom Gesetz vorgesehenen Mittel des Zivil- und Strafrechts greifen dabei immer nur gegenüber Personen, die als Verletzer zu qualifizieren sind. Unbeteiligte Dritte können dagegen weder für eine Verletzung belangt noch kann von ihnen die Vornahme von Handlungen verlangt werden, die geeignet wären, eine Verletzung zu verhindern. Wie nachfolgend aufgezeigt wird[89], wäre aber gerade dies der Fall, wenn Access-Provider zum Einsatz von Netzsperren verpflichtet würden. Bei der zweiten Frage liegt das Problem darin, dass Netzsperren Handlungen erfassen können – und durchaus auch sollen –, die von den Rechteinhabern nicht verboten werden können, weil sie entweder als blosser Werkkonsum zu qualifizieren oder von einer Schranke, insb. derjenigen des Privatgebrauchs, freigestellt sind[90]. Damit zeigt sich, dass die Einführung von Netzsperren im schweizerischen Urheberrecht *zwei grundlegende Widersprüche* begründen würde: einen Widerspruch zum dogmatischen Konzept des URG und einen Widerspruch zur geltenden Rechtslage,

sic! 2017 S. 701, 718

namentlich zu derjenigen beim Privatgebrauch.

b) Widerspruch zum dogmatischen Konzept des Urheberrechts

Das dogmatische Konzept des schweizerischen Urheberrechts ist einfach. Sind die Schutzvoraussetzungen erfüllt, steht den Urheberinnen und Urhebern von Werken der Literatur und Kunst ein Bündel *eigentumsähnlicher Ausschliesslichkeitsrechte* an ihren Werken zu. Im Vordergrund stehen dabei die *Nutzungsrechte*, die es dem jeweiligen Rechteinhaber erlauben, darüber zu bestimmen, ob, wann und wie das Werk verwendet wird (Art. 10 URG). Diese Rechte werden zwar durch eine Reihe von Schranken beschränkt (Art. 19 ff. URG). Soweit aber keine Schranke greift, kann der Rechteinhaber gegen jeden Verletzer vorgehen und namentlich Unterlassung oder Beseitigung der Verletzung sowie Schadenersatz und Gewinnherausgabe verlangen (Art. 62 URG). Verletzer ist dabei, wer allein oder im Zusammenwirken mit einer (oder mehreren) anderen Person(en) ohne Zustimmung des Rechteinhabers eine Handlung vornimmt, die von einem (oder mehreren) Nutzungsrecht(en) erfasst ist. Unbeteiligte Dritte können dagegen weder für die Verletzung von Urheberrechten belangt werden noch können die Rechteinhaber von ihnen die Vornahme von Handlungen verlangen, die geeignet wären, eine Verletzung zu verhindern. Dieses *klassische zivilrechtliche*

---

88 EuGH vom 27. März 2014, Rs C-314/12, N 56.

89 Siehe dazu gerade nachfolgend, III.3.b.

90 Siehe dazu hinten, III.3.c.

Konzept wird zwar durch strafrechtliche Sanktionen verschärft (Art. 67 ff. URG), strafrechtlich kann aber immer nur zur Verantwortung gezogen werden, wer auch zivilrechtlich haftet[91]. Die Einführung von Netzsperren würde mit diesem Konzept des Urheberrechts in Widerspruch stehen, weil mit den Access-Providern erstmals Unternehmen zur Vornahme von Handlungen verpflichtet würden, obwohl ihre Tätigkeit, wie sogleich zu zeigen ist, nicht als Verletzung von Urheberrechten qualifiziert werden kann[92].

Die Frage der sog. *Provider-Haftung* ist in der Schweiz – anders als in den Mitgliedstaaten der EU[93] – bekanntlich nicht geregelt und entsprechend umstritten[94]. Unbestritten ist allerdings, dass es bei der Provider-Haftung um eine Haftung von ISP für die Mitwirkung an Rechtsverletzungen geht, die von Dritten unter Inanspruchnahme der Dienste dieser ISP begangen werden. Es geht damit stets um die Frage der *Teilnehmerhaftung*. Diese ist im Urheberrecht nicht gesetzlich geregelt. Die wohl überwiegende Lehre will diese Frage deshalb durch eine Anwendung der allgemeinen Regelung von Art. 50 OR lösen[95], andere sprechen sich für eine analoge Anwendung der Regelung im Design- und Patentrecht aus[96]. Beide Ansätze gelangen dabei zu ähnlichen Ergebnissen. Unbestritten ist zudem der Grundsatz: Eine Haftung von Teilnehmern besteht nur, wenn diese an einer Rechtsverletzung mitwirken.

Die Tätigkeit von Access-Providern besteht darin, ihren Kunden Zugang zum Internet zu verschaffen, typischerweise gegen Bezahlung eines Entgelts. Nur dank diesem Zugang sind die Endnutzer in der Lage, die verschiedenen Dienste des Internets zu nutzen und namentlich auf die Angebote im Web oder die Inhalte von sog. Peer-to-Peer-Netzwerken zuzugreifen und allenfalls auch selbst Inhalte online zugänglich zu machen. Access-Provider machen aber selbst keine urheberrechtlich geschützten Werke oder Leistungen zugänglich, sofern sie sich, wovon für die nachfolgende Analyse ausgegangen wird, auf ihre Rolle als Zugangsvermittler beschränken und nicht zugleich auch als Content- oder Hosting-Provider tätig sind. Da Access-Provider Urheberrechte damit nicht durch selbständige Handlungen verletzen, stellt sich die Frage, ob ihre Tätigkeit als rechtlich relevante Mitwirkung zu qualifizieren ist.

---

91 In diesem Sinn etwa: L. David, in: B. K. Müller/ R. Oertli (Hg.), Urheberrechtsgesetz (URG), Bundesgesetz über das Urheberrecht und Leistungsschutzrechte, 2. Aufl., Bern 2012, Vor URG 67–73 N 15; M. Reh binder/A. Viganò, Urheberrecht, Kommentar, 3. Aufl., Zürich 2008, URG 67 N 3 ff.; D. F. Barrelet/W. Egloff, Das neue Ur heberrecht, Kommentar zum Bundesgesetz über das Urheber recht und verwandte Schutzrechte, 3. Aufl., Bern 2008, URG 67 N 4.

92 Als ein gewisser Einbruch in das klassische Konzept des schweizerischen Urheberrechts kann zwar die Regelung über die *Hilfeleistung der Zollverwaltung* (Art. 75 ff. URG) verstanden werden, die verwal tungsrechtliche Mittel einsetzt, um die Ein-, Aus- und Durchfuhr urheberrechtsverletzender Waren zu verhindern. Zur Vornahme von Handlungen verpflichtet werden hier aber allein die Zollbehörden. Auch hier müssen Privatpersonen und Unternehmen also weder für Verletzungen einstehen noch werden sie zur Vornahme von Handlungen verpflichtet, wenn sie nicht als Verletzer zu qualifizieren sind.

93 Siehe dazu: Art. 12 ff. Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Infor mationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, («Richtlinie über den elektronischen Geschäfts verkehr»), sog. E-Commerce-RL.

94 Für Näheres zur Provider-Haftung in jüngerer Zeit siehe: F. Thouvenin, Vergleichs- und Bewertungsdienste: eine Analyse aus Sicht des Wettbewerbsrechts (UWG), in: F. Thouvenin/R. H. Weber (Hg.), Werbung online, Zürich 2017, 131 ff., 145 ff., m.w.H.

95 Barrelet/Egloff (Fn. 91), URG 62 N 5; Rehbinder/Viganò (Fn. 91), URG 62 N 1; N. Schoch/M. Schüepp, Provider-Haftung «de près ou de loin»?, Jusletter vom 13. Mai 2013, N 28 Fn. 66; I. Cherpillod, Violation des droits de propriété intellectuelle: complicité et instigation, in: Tissot (Hg.), Quelques facettes du droit de l'internet, Bd. 6, Neuenburg 2005, 55 ff., 67 f.; A. Hess-Blumer, Teilnahmehandlungen im Immaterialgüterrecht unter zivilrechtlichen Aspekten, sic! 2003, 95 ff., *passim;* P. Fehlbaum, Lutte contre l'échange illicite de musique sur Internet: une autre approche?, sic! 2007, 855 ff. Siehe auch BGE 107 II 82 ff. E. 9a.

96 C. P. Rigamonti, Providerhaftung – Auf dem Weg zum Urheberverwaltungsrecht?, sic! 2016, 117 ff., 122.

Naheliegend wäre es, die schweizerischen Access-Provider als Teilnehmer an Urheberrechtsverletzungen ihrer Kunden einstehen zu lassen. Die Handlungen dieser Kunden – also der Zugriff auf und der Konsum von urheberrechtlich geschützten Werken oder Leistungen[97] – sind in der Schweiz aber urheberrechtlich zulässig, weil sie entweder *reinen Werkgenuss* darstellen, der urheberrechtlich frei ist[98], oder von einer Schranke freigestellt sind. Das *Streamen* urheberrechtlich geschützter Werke fällt

97 Nicht infrage steht hier die Konstellation, in der Kunden von schweizerischen Access-Providern urheber rechtlich geschützte Werke und Leistungen auf dem Internet zugänglich machen. Denn gegen diese Urheberrechtsverletzungen kann in der Schweiz mit den bestehenden rechtlichen Mitteln vorgegangen werden.

98 H. Pfortmüller, in: B. K. Müller/R. Oertli (Hg.), Urheberrechtsgesetz (URG), Bundesgesetz über das Urheberrecht und Leistungsschutzrechte, 2. Aufl., Bern 2012, URG 10 N 2; R. M. Hilty, Urheber recht, Bern 2011, N 150; Barrelet/Egloff (Fn. 91), URG 10 N 6a; W. Egloff, Revisionsbedarf beim urheberrechtlichen Eigengebrauch?, Medialex 2006, 35 ff., 36.

dabei unter die Schranke der vorübergehenden Vervielfältigung (Art. 24a URG)[99], der *Download* unter diejenige des *Privatgebrauchs* (Art. 19 Abs. 1 lit. a URG)

---

99 Wie Streaming urheberrechtlich zu qualifizieren ist, wurde im schweizerischen Recht zwar kaum diskutiert und ist bisher nicht abschliessend geklärt (siehe dazu etwa: S. Brändli/A. Tamò, Mainstream – Streaming als Nutzungsform der Gegenwart und der Zukunft, sic! 2013, 651 ff.; V. Salvadé, Du streaming au cloud computing: quel avenir pour la copie privée en Suisse?, sic! 2016, 434 ff.). Wie sogleich zu zeigen sein wird, sind die Handlungen der Endnutzer, namentlich das Erstellen von vorübergehenden (Teil-)Vervielfältigungen von Werken, aber freigestellt. Unzweifelhaft ist dabei zunächst, dass das Bereitstellen eines Werks zum Streamen, bspw. auf einer Webseite, als Zugänglichmachen im Sinn von Art. 10 Abs. 2 lit. c URG zu qualifizieren ist (siehe dazu statt vieler: Rehbinder/Viganò [Fn. 91], URG 10 N 6). Etwas komplexer ist die Frage nach der Qualifikation der vorübergehenden (Teil-)Vervielfältigungen der Werke, die beim Streaming auf dem Rechner der Endnutzer anfallen, aber lediglich der Wiedergabe des Werkes dienen und nach dieser in aller Regel sogleich gelöscht oder überschrieben werden. Entscheidend ist dabei, dass die beim Streamen anfallenden (Teil-)Vervielfältigungen allein dem unterbruchslosen Abspielen der Inhalte und der Vermeidung wiederholter Zugriffe auf den Server dienen. Das Erstellen der (Teil-)Vervielfältigungen ist damit ein blosses *Buffering* oder *Caching* (für Näheres zum technischen Vorgang siehe etwa: J. G. Apostolopoulos/W. Tan/S. J. Wee, Video Streaming: Concepts, Algorithms, and Systems, Palo Alto 2002, <www.hpl.hp.com/techreports/2002/HPL-2002-260.pdf>, 10; Brändli/Tamò (Fn. 99), sic! 2013, 652 f.; A.-A. Wandtke/F.-T. von Gerlach, Die urheberrechtliche Rechtmässigkeit der Nutzung von Audio-Video Streaminginhalten im Internet, GRUR 2013, 676 ff.). Richtigerweise sind diese (Teil-)Vervielfältigungen deshalb als vorübergehende Vervielfältigungen im Sinn von Art. 24a URG zu qualifizieren und damit freigestellt. Denn sie sind flüchtig und begleitend (Art. 24a lit. a URG), stellen einen integralen und wesentlichen Teil eines technischen Verfahrens dar (Art. 24a lit. b URG) und haben keine eigenständige wirtschaftliche Bedeutung (Art. 24a lit. d URG), weil sie keine «neue, eigenständige Nutzungsmöglichkeit» eröffnen (Rehbinder/Viganò [Fn. 91], URG 24a N 9; terminologisch anders, in der Sache aber ebenso: R. Oertli, in: B. K. Müller/R. Oertli [Hg.], Urheberrechtsgesetz [URG], Bundesgesetz über das Urheberrecht und Leistungsschutzrechte, 2. Aufl., Bern 2012, URG 24a N 12; Barrelet/Egloff [Fn. 91], URG 24a N 7; anders für das Streaming allerdings Brändli/Tamò [Fn. 99], sic! 2013, 658, die bei der Nutzung nicht lizenzierter Angebote eine eigenständige wirtschaftliche Bedeutung bejahen, weil der Rechteinhaber für den Konsum der Werke keine Vergütung erhält; dabei verkennen die Autorinnen allerdings, dass sich die Frage der eigenständigen wirtschaftlichen Bedeutung allein danach bestimmt, ob die Nutzungsmöglichkeiten erweitert werden; liegt eine solche Erweiterung vor, greift die Schranke nicht und der Rechteinhaber kann allenfalls eine Vergütung fordern – nicht aber umgekehrt). Zudem ist auch das dritte (und meist entscheidende) Kriterium erfüllt. Die (Teil-)Vervielfältigungen dienen zwar nicht ausschliesslich der Übertragung in einem Netz zwischen Dritten durch einen Vermittler, wohl aber einer rechtmässigen Nutzung (Art. 24a lit. c URG). Denn eine solche muss immer dann vorliegen, wenn der Rechteinhaber die fragliche Handlung nicht verbieten kann. Dies ist hier der Fall, weil das *Streamen* durch den Endnutzer allein dem Werkgenuss dient, der urheberrechtlich frei ist (siehe dazu gerade vorstehend, Fn. 98). Zu Recht verstehen denn schon die Botschaft und mit ihr die Lehre das *Caching* als einen der zentralen Anwendungsfälle der Schranke von Art. 24a URG (Botschaft zum Bundesbeschluss über die Genehmigung von zwei Abkommen der Weltorganisation für geistiges Eigentum und zur Änderung des Urheberrechtsgesetzes vom 10. März 2006, BBl 2006, 3389 ff.; ebenso: Barrelet/Egloff [Fn. 91], URG 24a N 4; Oertli [Fn. 99], URG 24a N 6; Rehbinder/Viganò [Fn. 91], URG 24a N 4). Und ein solches *Caching* liegt seitens der Endnutzer beim *Streaming* vor. Bestätigt wird dieses Ergebnis auch dadurch, dass es bei der urheberrechtlichen Qualifikation auf die Art der Nutzung und nicht auf die dabei verwendete Technik ankommen sollte, dass es also keinen Unterschied machen darf, ob der Endnutzer eine Fernsehsendung (oder ein beliebiges anderes Werk) über Satellit oder Kabel empfängt und auf einem klassischen Fernsehgerät schaut, über einen Internetanschluss *streamt* und am PC oder auf dem Mobile ansieht oder per IP-TV auf seinem Smart-TV konsumiert. Nichts anderes ergibt sich im Übrigen auch aus der Rechtsprechung des EuGH vom 4. Oktober 2011, Rs C-403/08 und C-429/08, N 160 ff., wonach der blosse Empfang einer Sendung eine rechtmässige Nutzung darstellt. Im Ergebnis anders nun zwar EuGH, vom 26. April 2017, Rs C-527/15, N 54 ff., nach welchem das *Streaming* nicht unter die Schranke der vorübergehenden Vervielfältigung fällt; für das Fehlen einer rechtmässigen Nutzung war hier allerdings entscheidend, dass die urheberrechtlich geschützten Werke nicht (alle) aus einer rechtmässigen Quelle stammen – ein Kriterium, das dem schweizerischen Recht gerade fremd ist.

100 . Mangels Urheberrechtsverletzung ihrer Kunden entfällt damit eine Teilnehmerhaftung der schweizerischen Access-Provider – und damit zugleich eine potenzielle Anknüpfung für deren Verpflichtung zum Erlass von Netzsperren.

Denkbar – wenn auch etwas entlegen – ist ferner die Argumentation, dass die schweizerischen Access-Provider als Teilnehmer für Urheberrechtsverletzungen haften, die durch das Zugänglichmachen von Werken durch beliebige Dritte entstehen, die weder Kunden der Access-Provider sind noch sonst in einer

Beziehung zu diesen stehen. Ein solcher Ansatz würde allerdings dazu führen, dass Access-Provider ganz allgemein für alle Arten von Urheberrechtsverletzungen auf dem Internet einstehen müssten, weil sie «Teil des Kommunikationsvorgangs» und schon allein deshalb an der Verwertung von Urheberrechten beteiligt sind[101]. Ein derart offener Begriff, der eine Art *«Systemhaftung»* der Access-Provider begründen würde, liesse sich allerdings mit dem Konzept der Teilnehmerhaftung kaum vereinbaren. Auch wenn die Kriterien der Zurechnung im Einzelnen umstritten sind, so sollen diese doch stets eine angemessene Grenze zwischen erlaubtem und unerlaubtem Handeln ziehen, indem namentlich ein bewusstes Zusammenwirken des Verletzers und des Teilnehmers[102] und ein *adäquater Kausalzusammenhang* zwischen der Verletzung und dem Zusammenwirken der Beteiligten[103] vorausgesetzt wird. Bei einem blossen Dulden oder Unterlassen, wie es bei den Access-Providern infrage steht, haftet ein Teilnehmer denn nach allgemeiner Auffassung auch nur, wenn er zum Handeln verpflichtet gewesen wäre[104]. All dies ist hier jedoch nicht der Fall. Vielmehr fehlt es schon an einem natürlich kausalen Beitrag der schweizerischen Access-Provider zu den hier infrage stehenden Urheberrechtsverletzungen. Denn diese bestehen allein darin, Werke oder Leistungen auf dem Web oder in Peer-to-Peer-Netzwerken zugänglich zu machen. Eine darüber hinausgehende Nutzung der zugänglich gemachten Werke durch Dritte, etwa durch die Kunden der schweizerischen Access-Provider, ist für das Vorliegen einer Verletzung nicht erforderlich. An diesen Handlungen, also am Zugänglichmachen der Werke auf ausländischen Servern, wirken die schweizerischen Access Provider aber in keiner Weise mit.

Fehlt es damit an einer rechtlich relevanten Teilnahme der Access-Provider, so ist klar, dass deren allfällige Verpflichtung zum Erlass von Netzsperren mit dem dogmatischen Konzept des schweizerischen Urheberrechts brechen müsste. Ein derart grundlegender Widerspruch zum bestehenden Konzept sollte angesichts der verfassungsrechtlichen Bedenken[105] und der beschränkten Wirksamkeit von Netzsperren[106] nicht in Kauf genommen werden.

---

100 < www.ige.ch/fileadmin/user_upload/recht/national/d/urheberrecht/AGUR12_II_Medienmitteilung_20170302_DE.pdf>.

101 In diesem Sinn K.-P. Uhlig, in: N. Kuzniar, 16. Urheberrechtstagung des Schweizer Forums für Kommunikationsrecht (SF-FS), URG-Revision: Experten aus Wissenschaft und Praxis im Gespräch, sic! 2017, 510 ff., 514, nach welchem Access-Provider Teil der Verwertungskette im Internet sind und (schon allein) deshalb einen adäquat kau salen Beitrag zu den Urheberrechtsverletzungen leisten sollen, die Dritte auf dem Internet begehen.

102 BGE 104 II 225, 230; W. Fellmann/A. Kottmann, Schweizerisches Haftpflichtrecht, Bd. I, Bern 2012, N 2773, m.w.H.; W. Fischer/ M. A. Iten, in: W. Fischer/T. Luter bacher (Hg.), Haftpflichtkommentar, Kommentar zu den schweizerischen Haftpflichtbestimmungen, Zürich 2016, OR 50 N 16; F. Werro, La responsabilité civile, 2. Aufl., Bern 2011, N 1607, m.w.H.; H. Rey, Ausservertragliches Haftpflichtrecht, 4. Aufl., Zürich 2008, N 1436.

103 Fellmann/Kottmann (Fn. 102), N 2779, m.w.H.; R. Brehm, Die Entstehung durch unerlaubte Handlung, Art. 41–61 OR, Berner Kommentar, 4. Aufl., Bern 2013, OR 50 N 16; Rey (Fn. 102), N 1436.

104 BGE 71 II 107, 113 f.; Fellmann/Kottmann (Fn. 102), N 2765, m.w.H.; BK-Brehm (Fn. 103), OR 50 N 22.

105 Siehe dazu vorn, III.2.

106 Siehe dazu vorn, II.3.

c) Widerspruch zur Rechtslage beim Privatgebrauch

Das schweizerische Urheberrecht kennt eine Reihe von Eigenheiten. Eine besonders bemerkenswerte ist, dass der sog. *«Download aus illegaler Quelle»* nach fast einhelliger und damit zweifellos herrschender Auffassung zulässig ist, sofern er zum Privatgebrauch im Sinn von Art. 19 Abs. 1 lit. a URG erfolgt[107]. Diese Rechtsauffassung ist international auf Widerspruch gestossen. Namentlich die USA haben mehrfach deutlich gemacht, dass sie die schweizerische Haltung für problematisch erachten[108]. An der bestehenden Rechtslage will der schweizerische Gesetzgeber aber anscheinend festhalten[109]. Jedenfalls wird die Frage im Bericht zum VE-URG nicht als solche thematisiert, sondern die Zulässigkeit des «Downloads aus illegaler Quelle» vielmehr faktisch vorausgesetzt[110]. Anstelle einer Änderung der materiellen Rechtslage, die zumindest einer klaren Aussage in der noch ausstehenden Botschaft bedürfte, wurde im VE-URG

sic! 2017 S. 701, 721

vorgeschlagen, mittels Netzsperren den Zugriff auf ausländische, in der Schweiz abrufbare Angebote zu verhindern, die Werke oder andere Schutzobjekte «in nach diesem Gesetz offensichtlich widerrechtlicher Weise zugänglich» machen (Art. 66d Abs. 2 lit. b VE-URG).

Dieser Ansatz ist allerdings höchst widersprüchlich und deshalb verfehlt. Der Gesetzgeber kann nicht an der (rechtlichen) Zulässigkeit des «Downloads aus illegaler Quelle» festhalten und gleichzeitig eine Regelung einführen, um ebendiesen Download (tatsächlich) zu verhindern. 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 den Anwendungsbereich der Privatgebrauchsschranke einschränken und klarstellen, dass der «Download aus illegaler Quelle» von dieser nicht mehr erfasst ist. Einen «dritten Weg» kann es nicht geben.

Die Wirkungen eines solchen Paradigmenwechsels wären allerdings gering. Denn wie vorstehend ausgeführt[111], sind die beim *Streaming* seitens der Endnutzer entstehenden (Teil-)Vervielfältigungen als vorübergehende Vervielfältigungen im Sinn von Art. 24a URG zu qualifizieren und damit freigestellt. Selbst wenn der «Download aus illegaler Quelle» künftig als unzulässig angesehen werden sollte, würde sich an der Zulässigkeit des Streamings durch die Endnutzer deshalb nichts ändern. Ein Blick auf

---

107 Barrelet/Egloff (Fn. 91), URG 19 N 7b; C. Gasser, in: B. K. Müller/R. Oertli (Hg.), Urheberrechtsgesetz (URG), Bundesgesetz über das Urheberrecht und Leistungsschutzrechte, 2. Aufl., Bern 2012, URG 19 N 10 ff.; Hilty (Fn. 98), N 220 und 223; C. P. Rigamonti, Eigengebrauch oder Hehlerei? Zum Herunterladen von Musik- und Filmdateien aus dem Internet, GRUR Int. 2004, 281 und 286; Salvadé, (Fn. 99), sic! 2016, 435; I. Cherpillod, La révision sur la loi du droit d'auteur, Jusletter 11. Februar 2008, N 10; J. de Werra, Téléchargements d'œuvres protégés, l'imputé mainte nue, Medialex 2006, 171 f., 171; T. Baumgartner, Privatvervielfältigung im digitalen Umfeld, Zürich 2006, 200; M. Häuptli, Vorübergehende Vervielfältigungen im schweizerischen, europäischen und amerikanischen Urheberrecht, Basel 2004, 114; a. M. Rehbinder/Viganò (Fn. 91), URG 19 N 19, unter Verweis auf die Rechtslage im Ausland.

108 Office of the United States Trade Representative, 2016 Special 301 Report, Washington DC 2016, <ustr.gov/sites/default/files/USTR-2016-Special-301-Report.pdf>, 55 f.; US Congress International Creativity and Theft-Prevention Caucus, 2014 Watch List, Washington DC 2014, <www.scribd.com/doc/231134282/International-Creativty-and-Theft-Prevention-Caucus-2014-Watch-List>, 3 f.

109 Siehe dazu explizit: Schlussbericht AGUR12 vom 28. November 2013, 9.3.1. Eine allfällige gegenteilige Auffassung der AGUR und/oder der Bundesverwaltung wurden seither nicht kommuniziert.

110 Erläuternder Bericht URG 2015 (Fn. 20), 91, wo lediglich davon die Rede ist, dass der Download ab offen sichtlich illegaler Quelle künftig nicht mehr *möglich* sein wird.

111 Siehe dazu vorn, III.3.b.

die rasch wachsenden Märkte für Streaming[112] und die schwindenden Zahlen der Downloads[113] macht klar, dass den Rechteinhabern mit einer solchen Regelung kaum geholfen wäre. Auch deshalb erscheint es richtig, auf die Regelung von Netzsperren im Urheberrecht zu verzichten.

IV. Fazit

Die eingehende Analyse von Netzsperren aus technischer sowie verfassungs- und urheberrechtlicher Sicht hat gezeigt, dass Netzsperren im Urheberrecht technisch weitgehend unwirksam und rechtlich problematisch wären.

Aus technischer Sicht fällt ins Gewicht, dass die heute verfügbaren Arten von Netzsperren entweder von Anfang an weitgehend wirkungslos sind (Applikationsfilter und Proxy-Server) oder mit minimalem Aufwand und bescheidenen technischen Kenntnissen umgangen werden können (IP-Adresssperren und DNS-Sperren). Hinzu kommt, dass ein Overblocking, also das ungewollte (Mit-)Sperren lizenzierter Inhalte, oft kaum vermieden werden könnte. Aus verfassungsrechtlicher Sicht erscheinen die indirekte Wirkung von Netzsperren (Adressierung von ISP), die potenzielle Bedrohung teilweise überragender Rechtsgüter (Grundrechte) sowie der Umstand als problematisch, dass ein Rechtsschutz (rechtliches Gehör) kaum einwandfrei ausgestaltet werden kann. Verfassungsrechtlich erscheinen Netzsperren deshalb insgesamt als unzumutbar und unverhältnismässig. Aus urheberrechtlicher Sicht ist sodann zentral, dass die Einführung von Netzsperren einen doppelten Widerspruch zur bestehenden Rechtslage begründen würde: zum einen zum dogmatischen Konzept des Urheberrechts, indem mit den Access-Providern erstmals Unternehmen in die Pflicht genommen würden, deren Tätigkeit nicht als Verletzung von Urheberrechten qualifiziert werden kann. Zum andern zur geltenden Rechtslage beim Privatgebrauch, indem der Gesetzgeber versuchen würde, die Endnutzer mittels Netzsperren (tatsächlich) an der Vornahme von Handlungen (Download und Streaming) zu hindern, die diese (rechtlich) gerade vornehmen dürfen.

Insgesamt erscheint damit klar, dass auf die Einführung von Netzsperren im schweizerischen Urheberrecht verzichtet werden sollte.

Zusammenfassung

Die eingehende Analyse von Netzsperren aus technischer und rechtlicher Perspektive zeigt, dass solche Sperren technisch wirkungslos und rechtlich problematisch sind.

Aus technischer Sicht fällt ins Gewicht, dass die heute verfügbaren Arten von Netzsperren entweder von Anfang an weitgehend wirkungslos sind oder mit minimalem Aufwand und bescheidenen technischen Kenntnissen umgangen werden können. Hinzu kommt, dass sich ein Overblocking oft kaum vermeiden lässt. Aus verfassungsrechtlicher Sicht erscheint problematisch, dass Netzsperren eine Reihe von Grundrechten bedrohen, dass sie nicht gegen die Verletzer selbst, sondern nur gegenüber Dritten und damit indirekt wirken und dass der Rechts-schutz kaum einwandfrei ausgestaltet werden kann. Verfassungsrechtlich erscheint die Einführung von Netzsperren im Urheberrecht deshalb als unzumutbar und unverhältnismässig. Aus urheberrechtlicher Sicht besteht das Problem, dass die Einführung von Netzsperren mit

sic! 2017 S. 701, 722

---

112 M. Borghi, Chasing Copyright Infringement in the Streaming Landscape, International Review of Intellectual Property and Com petition Law, Vol. 42, No. 3, 2011, <ssrn.com/abstract=2358915>, 2 f.; G. Sinclair/ T. Green, Download or stream? Steal or buy? Developing a Typology of today's music consumer, Journal of Consumer Behaviour 2016, 3 ff.; H. Ellis-Petersen, Streaming growth helps digital music revenues surpass physical sales, The Guardian, 12. April 2016, <www.theguardian.com/music/2016/apr/12/strea ming-revenues-bring-big-boost-to-global-music-industry>; ferner: Brändli/Tamò (Fn. 99), sic! 2013, 651; Wandtke/von Gerlach (Fn. 99), GRUR 2013, 676.

113 In Bezug auf Musik-Downloads Salvadé, (Fn. 99), sic! 2016, 434.

Grundprinzipien des immaterialgüterrechtlichen Rechtsschutzes brechen müsste, weil mit den Access-Providern erstmals Unternehmen in die Pflicht genommen würden, deren Tätigkeit nicht als Verletzung von Urheberrechten qualifiziert werden kann. Zudem – und dies vor allem – stünden Netzsperren im Widerspruch zur geltenden Rechtslage beim Privatgebrauch, weil der Gesetzgeber versuchen würde, die Endnutzer mittels Netzsperren an der Vornahme von Handlungen zu hindern, die diese durchaus vornehmen dürfen.

Aus diesen Gründen erscheint klar, dass auf die Einführung von Netzsperren im schweizerischen Urheberrecht verzichtet werden sollte.

Résumé

Dans une perspective technique et juridique, l'analyse approfondie des blocages du réseau montre que de tels blocages sont techniquement sans effet et juridiquement problématiques.

D'un point de vue technique, les genres de blocages du réseau disponibles aujourd'hui sont soit la plupart du temps inefficaces soit facilement contournables avec des connaissances techniques modestes. On peut ajouter qu'il est presque impossible d'éviter un surblocage. Du point de vue du droit constitutionnel, le fait que les blocages du réseau menacent une série de droits fondamentaux, qu'ils produisent leur effet à l'encontre de tiers et non contre les auteurs eux-mêmes et, partant, indirectement, et qu'il soit presque impossible de concevoir une protection juridique parfaite, paraît problématique. C'est pourquoi, en matière de droit constitutionnel, l'introduction de tels blocages du réseau dans le droit d'auteur paraît inacceptable et disproportionnée. Du point de vue du droit d'auteur, il reste que l'introduction de ces blocages du réseau rompt avec des principes fondamentaux de la protection juridique du droit de la propriété intellectuelle, car, en visant les fournisseurs d'accès, des entreprises dont l'activité ne peut pas être qualifiée de violation de droits d'auteur se verraient pour la première fois rendues responsables. En outre et surtout, les blocages du réseau seraient en contradiction avec le droit en vigueur en matière d'usage privé car le législateur tenterait d'empêcher via les blocages du réseau les utilisateurs finaux d'accomplir des actes qu'ils ont parfaitement le droit d'accomplir.

Pour ces raisons, il paraît évident qu'il faudrait renoncer à l'introduction de blocages du réseau dans le droit d'auteur suisse.