INTERNET-BLOCKING

FREQUENTLY ASKED QUESTIONS

In den vergangenen Jahren setzte sowohl auf nationaler als auch auf europäischer und internationaler Ebene eine Diskussion über Technologien zur selektiven Sperre verschiedener Internetinhalte durch Access-Provider auf Empfängerseite ein (z.B. um Urheberrechte durchzusetzen oder den Zugriff auf kinderpornografisches Material, Online-Glücksspiel etc. zu verhindern). Damit wurde eine Reihe von Fragen aufgeworfen, sowohl hinsichtlich Verhältnismäßigkeit solcher Maßnahmen als auch in Bezug auf ihre möglichen unbeabsichtigten Folgen für den Schutz der Grundrechte und der Meinungsäußerungsfreiheit im Internet.

Diese Frequently Asked Questions (FAQ) zielen darauf ab, einen – wenn auch nicht erschöpfenden – Überblick darüber zu bieten, was Internet-Blocking ist. Der Schwerpunkt liegt dabei auf den am weitesten verbreiteten Blocking-Technologien, zu welchen Provider zur Beschränkung des Zugriffs auf Webseiten und Inhalte gezwungen werden können: Domain Name Server (DNS)-Blocking und IP-Blocking sowie deren Kombination (sog. Hybrid-Blocking). Auf Internet-Blocking mit Hilfe der so genannten Deep Packet Inspection (DPI), also der maschinellen Analyse von Inhalten, wird im Rahmen dieser FAQ nicht eingegangen.

Q: Was ist Internet-Blocking?

A: Das Internet wurde entwickelt, um eine unterbrechungsfreie Kommunikation zwischen zwei Punkten sicherzustellen. Seine dezentrale Struktur ermöglicht es, über viele verschiedene Wege auf denselben Inhalt zuzugreifen. Daher ist es empfängerseitig nur möglich den Zugriff auf bestimmte Inhalte zu erschweren, nicht jedoch diesen gänzlich zu unterbinden, solange diese Inhalte auf irgend einem Weg im Internet verfügbar sind. Internet-Blocking wird insbesondere als technische Maßnahme angewendet, um für Nutzerinnen und Nutzer den Zugriff auf „illegale" Inhalte oder Ressourcen einzuschränken, deren Quellen sich außerhalb des jeweils anwendbaren Rechtsraumes befinden. Das primäre Ziel von Sperr-Aufforderungen mittels Internet-Blocking besteht darin zu verhindern, dass bestimmte Inhalte das Endgerät der Nutzerinnen oder der Nutzer erreichen, indem sie von dessen Provider blockiert werden müssen. Möglich ist das durch spezielle Hard- oder Software bzw. Konfigurationsmaßnahmen, die den Empfang oder die Darstellung bestimmter Inhalte unterbindet.

ISPA – Internet Service Providers Austria
Währingerstrasse 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675

Q: Wie effizient sind die Blocking-Verfahren?

A: Vom technischen Standpunkt aus betrachtet kann das Blocking – abhängig von der verwendeten Methode – mehr oder weniger leicht umgangen werden. Da das Internet entwickelt wurde, um einen möglichst offenen Informationsfluss zu gewährleisten, kann eine Nutzerin oder ein Nutzer auf Inhalte, die von einem Provider bzw. in einem Land gesperrt werden, auch über andere Wege zugreifen. Dies kann zum Beispiel über ausländische Proxy-Server erfolgen, welche die lokale Sperre umgehen, über sogenannte „Tunneling Software", die Suchanfragen verschlüsselt und Blocking-Software daran hindert aufgerufene Webseiten zu erkennen, oder indem auf einen anderen Nameserver gewechselt wird, um DNS-Blocking zu umgehen. Weiters reagieren Anbieter „illegaler" Inhalte üblicherweise sehr schnell und stellen ihre Inhalte unter neuen Namen und Adressen ins Netz. Abgesehen davon, dass sie technisch leicht zu umgehen sind, bergen Blocking-Technologien auch immer das Risiko des „Overblocking" (das unbeabsichtigte Verhindern der Verbreitung legaler Inhalte) oder des „Underblocking" (die Nichtverhinderung der Verbreitung illegaler Inhalte) und bringen variierende Kosten mit sich.

Zusammenfassend ist entweder die Effektivität der jeweiligen Sperrmaßnahmen oder ihre Verhältnismäßigkeit zu hinterfragen. Der EuGH fordert von Providern, jede ihnen zumutbare Maßnahme zu setzen, schreibt jedoch gleichzeitig vor, dass diese verhältnismäßig sein muss. (EuGH v. 27.03.2014 C 314/12).

Q: Was ist DNS-Blocking?

A: Domain Namen werden verwendet, um Internet-Ressourcen wie Webseiten oder Services zu identifizieren. Wenn eine Nutzerin oder ein Nutzer nach einer bestimmten Webseite sucht und deren Namen in seinen Browser eintippt (z.B. www.ispa.at) wird dieser über das Domain Name System (DNS) in seine numerische IP-Adresse (86.59.23.150) übersetzt, über die Computer miteinander kommunizieren. Um den Zugang zu einer bestimmten Website auf Basis ihres DNS-Namens zu blockieren, muss der Provider in die reguläre Namensauflösung, also in die o.g. Übersetzung eingreifen und entweder keine oder eine „falsche" IP-Adresse als Antwort an die Nutzerin oder den Nutzer liefern. Damit kann er diese davon abhalten, die von ihm angeforderte Webseite aufzurufen. DNS-Blocking ist eine sehr drakonische Maßnahme, die nur sehr vorsichtig verwendet werden sollte, da es sämtliche Informationen und Services der betroffenen Domain beeinträchtigt. Alle Webseiten der Domain – sowohl legale als auch illegale – werden „unsichtbar", es kann unmöglich werden E-Mails zu versenden oder zu empfangen und auch alle Subdomains werden davon erfasst. Andererseits können Nutzerinnen und Nutzer unter Verwendung anderer DNS Server solche Sperren sehr leicht umgehen.

DNS-Blocking ist eine jener Sperrmaßnahmen, die von den Rechteinhabern im *kino.to* Verfahren (EuGH v. 27.03.2014 C 314/12) den zur Zugriffssperre aufgeforderten Providern vorgeschlagen wurde.

Q: Was ist IP-Adressen-Blocking?

A: IP-Adressen-Blocking verhindert den Aufbau einer Verbindung zwischen dem Endgerät der Nutzerin oder des Nutzers und typischer Weise einer Webseite.

IP-Blocking zielt in der Regel auf die IP-Adressen umstrittener Inhalte ab, um den Zugriff darauf zu unterbinden (der typischerweise über einen Provider läuft). Für Nutzerinnen oder Nutzer, die sich eines Providers bedienen, der eine derartige Sperre nicht implementiert hat, bleiben diese Inhalte weiterhin frei zugänglich.

IP-Blocking birgt ein hohes „Overblocking" Risiko, da sich in Web-Hosting Umgebungen vielfach hunderte „Services" die gleiche IP-Adresse „teilen". Andererseits kann IP-Blocking sehr leicht unter Verwendung von Proxy-Servern und/oder Tunnel-Systemen umgangen werden.

Auch IP-Adressen-Blocking gehört zu jenen Sperrmaßnahmen, die im *kino.to* Verfahren (EuGH v. 27.03.2014 C 314/12) vorgeschlagen wurden.

Q: Was ist der Unterschied zwischen DNS- und IP-Blocking?

A: DNS- und IP-Blocking sind zwei verschiedene Methoden, um den Zugriff auf Internetinhalte zu unterbinden. Wie bereits zuvor aufgezeigt wurde, ist DNS-Blocking zum Beispiel durch Verschlüsselung oder das Ändern des eigenen DNS-Servers relativ leicht zu umgehen. Das Umgehen des IP-Blocking gestaltet sich schwieriger. Ermöglicht wird es vor allem durch das sogenannte „Tunneling" beziehungsweise „Virtual Private Network (VPN)"-Tunneling-Technologien. Das Tunneling erlaubt den Nutzerinnen und Nutzern die Herstellung eines verschlüsselten „Tunnels" zu einem anderen Computer im Internet, der nicht dem angeordneten IP-Blocking durch den Provider unterliegt, also die Blocking-Software daran hindert, die Webabfragen der Nutzerin oder des Nutzers zu erkennen. VPN-Tunnel werden ausnahmslos verschlüsselt und sind somit schwerer bzw. nicht überwachbar.

Sowohl DNS- als auch IP-Blocking bergen die Gefahr des Overblocking. Overblocking beeinträchtigt ungefährliche Webseiten, hindert Nutzerinnen und Nutzer daran, auf diese zuzugreifen, verursacht Kosten für die Provider aufgrund von Beschwerden über dieses Overblocking und schädigt die Reputation der involvierten Provider. Auf der einen Seite führt IP-Blocking zwangsläufig dazu, dass große Mengen an legalen Inhal-

ten blockiert werden, da viele verschiedene Webseiten sich häufig dieselbe IP-Adresse teilen. Folglich zieht die Blockade einer IP-Adresse beinahe automatisch auch die Blockade einer großen Anzahl anderer (legaler) Webseiten nach sich und nicht nur jene der illegalen Webseite. Auf der anderen Seite impliziert das DNS-Blocking die Sperre einer ganzen Domain (also Website) auf der Ebene eines DNS-Servers. Das bedeutet, dass, wenn illegale Inhalte auf einer Subdomain einer Domain gehostet werden, auch alle anderen (legalen) Subdomains, welche die gleiche übergeordnete Domain haben, ebenfalls blockiert werden. Das ist besonders problematisch, wenn davon benutzergenerierte Inhalte in großen sozialen Netzwerken oder Media-Sharing-Diensten betroffen sind. Wenn zum Beispiel ein Inhalt, den eine Behörde blockieren will, auf das Profil eines sozialen Netzwerks gestellt wird, führt DNS-Blocking zur Sperre der gesamten Webseite dieses sozialen Netzwerks für alle Kunden des Zugangsproviders.

Dies hat direkte Auswirkungen auf die Freiheit der Kommunikation, weil die Existenz zusätzlicher Subdomains nicht ohne weiteres ersichtlich ist und Bedenken bezüglich der Verhältnismäßigkeit dieser Maßnahme im Vergleich zu weniger restriktiven Alternativen aufwirft.

Zudem existiert zusätzlich die Gefahr des Overblocking, sowohl hinsichtlich des Domain Namens (das Blockieren legaler Seiten von Subdomains) als auch hinsichtlich des geografischen Standorts, nämlich für Betreiber, deren Netzwerke eine gesamteuropäische Abdeckung bieten. Abhängig vom Standort seiner Server kann es einem Provider durchaus passieren, dass er unbeabsichtigt auch Seiten in anderen Ländern blockiert.

Grundsätzlich stellt die Anwendung von Websperren für Access-Provider eine enorme technische und rechtliche Herausforderung dar. In seinem Erkenntnis vom 24.06.2014 (4 Ob 71/14s) ist der OGH der Argumentationslinie des EuGH gefolgt und hat bestätigt, dass eine Sperrverfügung keine konkrete Sperrmaßnahme vorschreiben darf. Somit müssen Access-Provider selbst beurteilen, welche konkrete technische Sperrmaßnahe zur Anwendung kommt.

Access-Provider müssen daher selbst die potentiellen Aus- bzw. Nebenwirkungen einer bestimmten Sperrmaßnahme abschätzen und deren Angemessenheit unter Berücksichtigung des Inhalts der betroffenen Webseite beurteilen, da eine überschießende Sperre (z.B. bei Sperren von Webseiten mit teilweise legalen Inhalten) unter Umständen eine Verletzung des Grundrechts auf Informationsfreiheit ihrer Kunden bedeuten könnte und sie dadurch dem Risiko einer Klage durch diese ausgesetzt sind.

Q: Können Maßnahmen, die eingesetzt werden, um kinderpornografisches Material zu blockieren, auch dazu verwendet werden andere Arten von Inhalten zu blockieren?

A: Kinderpornografie wird allgemein verurteilt und als kriminelle Handlung eingestuft. Trotz Investitionen innerhalb der EU zur Blockade solcher illegalen Inhalte aus Drittstaaten, zeitigten entsprechende Initiativen bisher keinen messbaren Effekt. Vielmehr deuten praktische Erfahrungen darauf hin, dass ihre Sperre den politischen Druck in Bezug auf eine wirksame internationale Kooperation zur Bekämpfung derartiger Inhalte an ihrer Quelle (ob innerhalb oder außerhalb der EU) und zur Verfolgung der Kriminellen hinter diesen Seiten eher vermindert. Anstatt ihrer Sperre würde die Entfernung derartiger Inhalte an ihrer Quelle (z.B. durch Meldung auf www.stopline.at), die Förderung der internationalen Kooperation zur Löschung illegaler Inhalte (z.B. durch INHOPE) und die Stärkung der Polizeizusammenarbeit erheblich dazu beitragen, dieses Phänomen innerhalb als auch außerhalb der EU zu bekämpfen und damit eine abschreckende Wirkung zu erzielen, die derzeit fehlt.

Q: Warum ist die Sperre hetzerischer, xenophober oder terroristischer Inhalte so schwierig?

A: Es gibt zahlreiche Beispiele für Individuen oder sogar Staaten die von namhaften Akteuren als terroristisch[i] oder rassistisch[ii] eingestuft werden. Versuche, hetzerische, xenophobe oder terroristische Inhalte zu sperren, erweisen sich zumeist als schwierig, weil diese nicht zwangsläufig illegal sind. Unterschiedliche Auffassungen existieren diesbezüglich bereits zwischen den Mitgliedsstaaten. Ohne richterliche Anordnung, welche die Rechtswidrigkeit eines bestimmten Inhalts klar definiert, besteht beim Blockieren derartiger Inhalte die Gefahr der Zensur vollkommen legaler Meinungsäußerungen. Damit wird das Recht auf freie Meinungsäußerung im Internet verletzt und die Rechtssicherheit für die Internetwirtschaft verringert.

Q: Sind Maßnahmen zur Blockade von Spam dasselbe wie zur Blockade anderer Inhalte?

A: Der Begriff „Spam" beschreibt die Zirkulation von unerwünschten Nachrichten (daher auch Spam-E-Mail). Etwa 85 bis 90 Prozent aller weltweit versendeten E-Mails sind Spam. Spam ist nicht nur ein Hindernis für das reibungslose Funktionieren der Online-Kommunikation und für die Freiheit der Korrespondenz der Nutzerinnen und Nutzer sowie des Dienstes, sondern auch eine Sicherheitsbedrohung, weil er oft dazu verwendet wird, Schadsoftware zu verbreiten. Bei Spam handelt es sich nicht notwendigerweise um illegale Inhalte, allerdings kann er zu illegalen Aktionen führen, wie zum Beispiel der Installation eines Trojaners auf dem Endgerät einer Nutzerin oder eines Nutzers, um diesen zu hacken. Weitere Unterschiede bestehen darin, dass Spam-E-Mails auf den Servern des Providers gespeichert werden, bis sie durch die Nutzerin oder den Nutzer heruntergeladen werden, während andere Arten vermeint-

lich illegaler Inhalte direkt zwischen den Nutzerinnen und Nutzern ausgetauscht werden. Darüber hinaus tragen Konsumenten durch Beschwerden über Spam zur Entwicklung entsprechender Filter bei, die auf den Ursprung des Spams abzielen, welcher nicht immer mit anderen Formen vermeintlich illegaler Inhalte auftritt. Auch können E-Mails von einer IP-Adresse, die nicht die IP-Adresse eines bekannten E-Mail-Servers ist, unter Spam-Verdacht geraten. Schließlich existiert mit dem „Spam-Blocking" eine Sicherheitsmaßnahme, die für den Kunden die sichere und effiziente Nutzung der Internet-Infrastruktur gewährleistet. Im Gegensatz dazu bezieht sich das Blockieren von Inhalten auf Methoden, die wesentlich geringere Auswirkungen auf die Netzwerke von Providern haben.

Q: Stellt die Selbstregulierung ein probates Mittel im Umgang mit illegalen Online-Inhalten dar?

A: Selbstregulierung ist ein flexibles Instrument, das von der Industrie zur Bewältigung von Sicherheitsproblemen herangezogen wird. Im Umgang mit Sicherheitsbedrohungen hat der Provider die vollständige technische Kontrolle über schädliche Inhalte, die es ihm erlaubt interne Standards und Prozesse auf selbstregulatorischer Basis zu etablieren. Wenn es sich allerdings um andere, vermeintlich illegale Inhalte ohne Sicherheitsbezug handelt, hat der Provider keine Kontrolle darüber, weil er naturgemäß keine Kenntnis über den Inhalt der über seine Leitungen laufenden Kommunikation hat. Für einige spezifische Inhalte (z.B. Kinderpornografie) ist die Selbstregulierung ein probates Mittel, um das Problem in Zusammenarbeit mit Hotlines oder Strafverfolgungsbehörden anzugehen, die über eine entsprechende Ausbildung und Know-how zur Bewertung der Inhalte verfügen, und falls erforderlich die Entfernung des illegalen Materials empfehlen. Für andere Kategorien vermeintlich rechtswidriger Inhalte (wie z.B. die unerlaubte Verbreitung urheberrechtlich geschützten Materials, Online-Glücksspiel, Diffamierung, Terrorismus etc.) stellt die Selbstregulierung nicht die ideale Lösung dar. Ein Provider ist nämlich nicht dazu in der Lage sich ein Urteil über die Rechtmäßigkeit oder Unrechtmäßigkeit derartiger Inhalte zu bilden. Selbstregulatorische Maßnahmen müssen zudem darauf achten, nicht eine Reihe von Grundrechten zu verletzen, wie sie in der Grundrechtecharta der Europäischen Union verankert sind (z.B. die Meinungsäußerungsfreiheit und die Informationsfreiheit). Wie auch im interinstitutionellen Abkommen zwischen Europäischer Kommission, Europäischem Parlament und Europäischem Rat aus dem Jahr 2003 festgehalten wurde, hat *„Selbstregulierung immer im Einklang mit Gemeinschaftsrecht"* zu sein und *„sind diese Mechanismen nicht anwendbar, wenn Grundrechte auf dem Spiel stehen"*. Gerade deswegen fordert die ISPA eine richterliche Prüfung, bevor ein Anbieter dazu verpflichtet werden darf, den Zugang zu einer Webseite zu blockieren, einen Internetzugang zu sperren oder persönliche Daten über einen vermeintlichen Rechtsbrecher herauszugeben.

[i] Mandelas African National Congress wurde von Margaret Thatcher als klassische Terrororganisation eingestuft.
[ii] UN-Resolution 3379 bezeichnet Israel als „rassistischen" Staat.

ISPA – Internet Service Providers Austria
Währingerstrasse 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675