universität wien

MASTER-THESIS

Titel der Master-Thesis

„Sperrverfügungen hinsichtlich urheberrechtsverletzender Internetseiten – juristische Notwendigkeit oder technische Unmöglichkeit?“

Verfasser

Mag. Matthias Wach

angestrebter akademischer Grad

Master of Laws (LL.M.)

Wien, 2014

Universitätslehrgang:	Informations- und Medienrecht
Studienkennzahl lt. Studienblatt:	A 992 942
Betreuer:	Ing. Dr. Christof Tschohl

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs	Absatz
Art	Artikel
BVG	Bundesverfassungsgesetz
bzw	beziehungsweise
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DPI	Deep Packet Inspection
DSG	Datenschutzgesetz
ECG	E-Commerce Gesetz
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
EO	Exekutionsordnung
ErwGr	Erwägungsgrund
etc	et cetera
EuGH	Europäischer Gerichtshof
EUV	Vertrag über die Europäische Union
FTP	File Transfer Protocol
GA	Generalanwalt
GmbH	Gesellschaft mit beschränkter Haftung
HTML	Hyper Text Markup Language
IETF	Internet Engineering Task Force
IFPI	Verband der Österreichischen Musikwirtschaft
IP	Internet Protocol
leg.cit.	legis citatae
lit	litera
mE	meines Erachtens
NAT	Network Address Translation
OGH	Oberster Gerichtshof
OLG	Oberlandesgericht
PC	Personal Computer
RL	Richtlinie
SPI	Shallow Packet Inspection
StGG	Staatsgrundgesetz
StPO	Strafprozessordnung
TCP/IP	Transmission Control Protocol/Internet Protocol
TKG	Telekommunikationsgesetz
TOR	The Onion Router
ua	unter anderem
UrhG	Urheberrechtsgesetz
URL	Uniform Resource Locator
uU	unter Umständen
VAP	Verein für Anti-Piraterie der Film- und Videobranche
VfGH	Verfassungsgerichtshof
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
zB	zum Beispiel
ZP-EMRK	Zusatzprotokoll zur Europäischen Menschenrechtskonvention

1. Einleitung

Gegenstand meiner Arbeit ist der Themenkomplex rund um die aktuellen Sperrverfügungen gegen österreichische Access-Provider betreffend Internetseiten, welche rechtswidrig Inhalte anbieten, die urheberrechtlichem Schutz unterliegen. Vorrangig geht es in der aktuellen Diskussion dabei um jene Seiten, welche Filme zum Abruf als Stream anbieten, oft während diese noch im Kino laufen und im Handel noch nicht erhältlich sind.

Ausgangspunkt der Arbeit ist die Entscheidung 4 Ob 71/14s[1] des OGH, welche infolge des Vorlageverfahrens C-314/12[2] vor dem EuGH erging. Eine umfassende Darstellung der Rechtsgrundlagen, des Verfahrensgangs und der Entscheidung dient einerseits der Darstellung der aktuellen Rechtslage, soll andererseits aber auch Ausgangspunkt für eine kritische Betrachtung der keinesfalls idealen rechtlichen Gegebenheiten sein.

Um das Thema umfassend zu beleuchten, beschränkt sich meine Arbeit jedoch nicht ausschließlich auf Streamingseiten, sondern bezieht auch jene Bezugswege für urheberrechtlich geschütztes Material mit ein, welche mE neben Streaming die derzeit größte Relevanz besitzen: Bittorrent, Sharehoster sowie das Usenet.
Die Einbeziehung dieser Dienste erscheint deswegen notwendig, da, sollte sich die derzeitige Praxis von Netzsperren bewähren, als logische Konsequenz Rechteinhaber in Zukunft auch Sperren in Bezug auf weitere Verbreitungswege fordern könnten.

Die Darstellung technischer Grundlagen erscheint notwendig, um die konkreten Sperrmöglichkeiten in Bezug auf deren juristische Tragweite beurteilen zu können. Dies ist nicht trivial, da den Entscheidungen des EuGH und OGH nur Hinweise entnommen werden können, welche Sperrmaßnahmen den Access-Providern in concreto zumutbar sind. Zum Zweck dieser Darstellung wird auf die Literatur und Judikatur aus Deutschland zurückgegriffen, weil dort im Rahmen des geplanten – aber nie in Kraft getretenen – deutschen Zugangserschwernisgesetzes eine intensive Diskussion bezüglich der konkret zu setzenden Sperrmaßnahmen geführt wurde.

[1] OGH 24.06.2014, 4 Ob 71/14s.
[2] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) = RdW 2014/196, 173 = ecolex 2014, 297 (*Wilhelm*) = MR 2014, 82 = ecolex 2014, 576 (*Zankl*) = jusIT 2014/42, 83 (*Beimrohr*) = jusIT 2014/43, 87 = ÖJZ 2014/73, 474 = wbl 2014/109, 329 = ecolex 2014, 488 = ecolex 2014/218, 546 = ÖBl 2014/40, 189.

2. Ausgangslage des Vorabentscheidungsverfahrens

Auf der Webseite „kino.to“ wurden in großem Umfang urheberrechtlich geschützte Filme zum kostenlosen Abruf bereitgestellt, welche entweder als Stream direkt angesehen, also flüchtig vervielfältigt, oder heruntergeladen, also dauerhaft vervielfältigt werden konnten.[3] Darunter befanden sich auch Filme der Klägerinnen, Constantin Film Verleih GmbH und Wega Filmproduktionsgesellschaft GmbH, welche ohne deren Einverständnis zugänglich gemacht wurden[4].

Die Klägerinnen hatten gemäß § 81 Abs 1a UrhG beantragt, UPC mittels einstweiliger Verfügung zu verbieten, „*ihren Kunden im Internet den Zugang zur Website kino.to zu vermitteln, wenn den Kunden der beklagten Partei auf dieser Website* [...] [Filme der Klägerinnen] [...] *ganz oder in Ausschnitten online zur Verfügung gestellt werden*“[5]. Weiters wurde beantragt, die vorzunehmenden Sperrmaßnahmen zu konkretisieren, nämlich eine DNS-Sperre der Domain kino.to zu veranlassen sowie die jeweils aktuellen IP-Adressen von kino.to zu sperren, unbeschadet dessen, dass ein allgemeines Zugangsverbot gefordert wurde.[6]

Es stand mit an Sicherheit grenzender Wahrscheinlichkeit fest, dass einzelne UPC-Kunden das Angebot von kino.to nutzten[7]. Der beklagte Access-Provider, UPC Telekabel Wien GmbH, brachte dagegen vor, in keinerlei Rechtsbeziehung zu kino.to zu stehen und seinen Kunden nur Zugang zum Internet zu vermitteln[8].

UPC führte ins Treffen, IP- und DNS-Sperren seien ineffektiv und mit hohen Kosten verbunden, weswegen der Verhältnismäßigkeitsgrundsatz verletzt sei. Es sei denkbar, dass mit IP-Sperren auch der Zugang zu anderen Webseiten verhindert werde, welche unter derselben IP-Adresse angeboten werden.[9]

Das Erstgericht verfügte die Sperre von kino.to insbesondere durch IP- sowie DNS-Sperren. Diese seien die effektivsten zur Verfügung stehenden Methoden, obwohl sie auch nach Ansicht des Gerichts leicht zu umgehen seien. In Bezug auf IP-Sperren sei nicht erwiesen,

[3] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 9.
[4] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 10.
[5] OGH 11.05.2012, 4 Ob 6/12d = wbl 2012/180, 473 = ecolex 2012/291, 708 = RdW 2012/401, 381 = MR 2012, 190 = RZ 2013/EÜ 13, 22 = ÖBl 2013/10, 43.
[6] OGH 11.05.2012, 4 Ob 6/12d.
[7] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 11.
[8] OGH 11.05.2012, 4 Ob 6/12d.
[9] OGH 11.05.2012, 4 Ob 6/12d.

dass kino.to die IP-Adresse mit anderen Servern teile, eine IP-Sperre möglicherweise also auch rechtmäßige Seiten betreffe.[10]

Das Zweitgericht bestätigte die Sperre. Es sei nach dessen Ansicht unerheblich, ob die UPC-Kunden durch Inanspruchnahme der Dienste von kino.to selbst rechtswidrig handeln, weil die Zurverfügungstellung der Filme auf kino.to an sich rechtswidrig sei und UPC als Access-Provider ihren Kunden den Zugriff ermögliche, weswegen eine Inanspruchnahme auf Unterlassung möglich sei.

Der Einwand UPCs, die auferlegten Maßnahmen seien teuer und ineffektiv und daher nicht verhältnismäßig, sei unbeachtlich, da § 81 Abs 1a UrhG ein absolutes Recht schütze. Nach österreichischem Recht sei anerkannt, dass zum Schutz dieses Rechts nur ein reines Erfolgsverbot zulässig sei. Die Wahl der Mittel zur Erreichung desselben würden im Ermessen der Beklagten liegen. Das Gericht habe die konkreten Maßnahmen deswegen nicht aufzuerlegen. Würden die Klägerinnen in weiterer Folge einen Verstoß einwenden, könne die Beklagte ohnedies Beugestrafen mit dem Einwand abwenden, alle zumutbaren Maßnahmen ergriffen zu haben, weswegen im Verfahren zur Erlassung der einstweiligen Verfügung Möglichkeit und Zumutbarkeit der Maßnahmen nicht zu prüfen sei.[11]

[10] OGH 11.05.2012, 4 Ob 6/12d.
[11] OGH 11.05.2012, 4 Ob 6/12d.

3. Rechtsgrundlagen

3.1. Urheberrecht

Die urheberrechtlichen Ausschlussrechte und die daraus erwachsenden Ansprüche der Rechteinhaber auf Unterlassung von Eingriffen in ihre Rechtsposition sind Ausgangspunkt der Debatte rund um Netzsperren, weswegen ein Überblick über die für diese Arbeit relevanten Aspekte unerlässlich ist.

Gemäß § 38 UrhG stehen die Verwertungsrechte an einem gewerbsmäßig hergestellten Filmwerk dem Filmhersteller zu. Verwertungsrechte dienen den Interessen der Urheber bzw Filmhersteller und gewähren ausschließliche Rechte, um vor allem die materielle Verwertung der Werke sicherzustellen.[12] Im Rahmen der Verwertungsrechte verfügt der Filmhersteller insbesondere über das Zurverfügungsstellungsrecht des § 18a UrhG, worunter sowohl das Zugänglichmachen eines Werks als Download als auch als Stream fällt.

Artikel 8 der Richtlinie 2001/29/EG[13] (Informationsgesellschaftsrichtlinie) verpflichtet die Mitgliedsstaaten, angemessene Sanktionen und Rechtsbehelfe zum Schutz der Rechte der Urheber vorzusehen. Gemäß Abs 3 leg.cit. soll sichergestellt werden, „*dass die Rechtsinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden*“[14].

ErwGr 59 Informationsgesellschaftsrichtlinie führt aus, dass „*insbesondere in der digitalen Technik [...] die Dienste von Vermittlern immer stärker von Dritten für Rechtsverstöße genutzt werden [können]*“, weswegen diese am besten in der Lage seien, derartige Verstöße zu beenden. Aufgrund dessen solle die Möglichkeit gerichtlicher Anordnungen gegen solche Vermittler, deren Netze sich Dritte zur rechtsverletzenden Übertragung geschützter Werke bedienen, vorgesehen werden.[15]

Die österreichische Umsetzung des Artikel 8 Informationsgesellschaftsrichtlinie findet sich in § 81 UrhG. Dessen Abs 1 sieht einen Unterlassungsanspruch gegen den Rechtsverletzer für den Fall von Urheberrechtsverletzungen vor. Abs 1a leg.cit. normiert einen Unterlassungsanspruch gegen einen Vermittler, wenn eine Rechtsverletzung unter

[12] *Anderl* in *Kucsko* (Hrsg), urheber.recht § 14, 2.1 (Stand 1.12.2007).
[13] Richtlinie 2001/29/EG des europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl L 2001/167, 10.
[14] Art 8 Informationsgesellschaftsrichtlinie.
[15] ErwGr 59 Informationsgesellschaftsrichtlinie.

Zuhilfenahme seiner Dienste erfolgt. Im Rahmen der gegenständlichen Entscheidungen stellten der EuGH bzw OGH klar, dass unter Vermittler auch ein Access-Provider zu verstehen ist, welcher mit demjenigen, der eine Rechtsverletzung begeht, in keinem Vertragsverhältnis steht und die Daten somit quasi nur von der rechtsverletzenden Website zu seinen Kunden „durchleitet". Im Falle eines Access Providers hat vor Klagsführung eine Abmahnung zu erfolgen.

3.2. Exekutionsrecht

Da die Erlassung und Durchsetzung von Sperrverfügungen auf Ebene des Exekutionsrechts erfolgt ist im Folgenden auf die dafür relevanten Rechtsgrundlagen einzugehen.

§ 87c Abs 1 UrhG gewährt zur Durchsetzung von Unterlassungsansprüchen nach § 81 UrhG das Mittel der einstweiligen Verfügung. Aktivlegitimiert ist dabei jeder Rechtsinhaber, welcher in seinen Ausschließlichkeitsrechten verletzt wurde.[16]

Einstweilige Verfügungen werden in einem summarischen Erkenntnisverfahren erlassen, welches mit dem Erlass des Exekutionstitels „einstweilige Verfügung" endet. Der Anspruch des Antragstellers und die Gefährdung der Durchsetzung desselben müssen bloß bescheinigt werden, das Bestehen des Anspruchs wird als bloße Vorfrage im Zusammenhang mit der Zulässigkeit der einstweiligen Verfügung geprüft. In seiner ursprünglichen Ausgestaltung ist das Verfahren zur einstweiligen Verfügung also ein Provisorialverfahren; dessen Beschlüsse sollen nur vorübergehend Wirkung erlangen.[17]

Verstößt der Verpflichtete gegen die in der einstweiligen Verfügung auferlegten Verpflichtungen, kann der betreibende Kläger die Exekutionsbewilligung beantragen. Das Bewilligungsverfahren ist ein einseitiges Aktenverfahren ohne Anhörung des Verpflichteten. Dieser soll durch die Exekutionsbewilligung „überrascht" werden. [18]

Die Exekution zur Erwirkung von Unterlassungen ist in § 355 EO geregelt. Im Rahmen einer Exekution nach § 355 EO hängt es ausschließlich vom Willen des Verpflichteten ab, ob die Exekution von Erfolg gekrönt ist. Im Falle des Zuwiderhandelns gegen die im Exekutionstitel festgesetzte Unterlassungsverpflichtung normiert § 355 EO Beugestrafen in Form von Geld- und Haftstrafen.[19]

[16] *Ofner* in *Kucsko* (Hrsg), urheber.recht § 81, 7.1 (Stand 1.12.2007).
[17] *Rechberger/Oberhammer*, Exekutionsrecht[5] (2009) Rz 474.
[18] *Rechberger/Oberhammer*, Exekutionsrecht[5] (2009) Rz 93.
[19] *Rechberger/Oberhammer*, Exekutionsrecht[5] (2009) Rz 146.

Sperrverfügungen gegen urheberrechtsverletzende Webseiten werden in Form von Erfolgsverboten erlassen. Zwar schulden die Access-Provider de facto ein aktives Handeln, nämlich das Einrichten von Sperrmaßnahmen, um den Erfolg, also die Aufrufbarkeit einer zu sperrenden Seite aus ihrem Netz, zu verhindern. Das trotzdem im Rahmen der Unterlassungsexekution vorgegangen wird, ist der unscharfen Abgrenzung zwischen Handlungs- und Unterlassungspflichten im Exekutionsrecht geschuldet[20]. Der OGH zieht in seiner gegenständlichen Entscheidung[21] eine Parallele zur Exekution der Unterlassung von Immissionen im nachbarrechtlichen Verhältnis. Den Nachbar trifft in solchen Verfahren de facto die Pflicht, aktive Verhinderungsmaßnahmen gegen einen Erfolg zu ergreifen, der ansonsten von selbst – ohne aktives Tun – eintritt[22].

Dem durch einen Exekutionstitel Verpflichteten steht es offen, Einwendungen gegen eine Exekution in Form einer Impugnationsklage zu erheben.[23] Damit kann er ua gemäß § 36 Abs 1 Z 1 Fall 1 EO einwenden, dem Exekutionstitel nicht zuwider gehandelt zu haben oder kein Verschulden am Zuwiderhandeln zu haben.[24] Im Zuge der Impugnationsklage ist, im Regelfall auf Antrag, eine Aufschiebung der Exekution nach § 42 Abs 1 Z 5 EO möglich.[25] In der Regel ist Voraussetzung der Aufschiebung, dass der Beginn oder die Fortführung der Exekution mit einem erheblichen Nachteil für den Verpflichteten verbunden wäre und die Klagsführung nicht aussichtslos ist[26] – der OGH hat jedoch ausgesprochen, dass beim Erheben einer Impugnationsklage gegen eine einstweilige Verfügung betreffend Internetsperren diese zwei Voraussetzungen nicht vorliegen müssen, um den Anforderungen gerecht zu werden, die der EuGH im Sinne des Rechtsschutzes des Verpflichteten an das nationale Verfahren stellt[27]. Im Impugnationsprozess gilt die Eventualmaxime, was bedeutet, dass alle Einwendungen, die zur Zeit der Erhebung der Klage bekannt waren, bei sonstigem Ausschluss gleichzeitig mit der Impugnationsklage erhoben werden müssen, nach Klagserhebung also nur „nova producta“ vorgebracht werden können.[28] Diese Beschränkung bedeutet eine erhebliche Schlechterstellung der Access-Provider gegenüber einem regulären Erkenntnisverfahren, da sie vor Erhebung der Impugnationsklage sichergehen müssen, alle Einwände gemeinsam mit der Klage zu erheben.

[20] *Klicka* in *Angst* (Hrsg)[2], § 355, RZ 4 (Stand 1.3.2008)
[21] OGH 24.06.2014, 4 Ob 71/14s.
[22] *Klicka* in *Angst* (Hrsg)[2], § 355, RZ 4a (Stand 1.3.2008).
[23] *Rechberger/Oberhammer*, Exekutionsrecht[5] (2009) Rz 211.
[24] *Rechberger/Oberhammer*, Exekutionsrecht[5] (2009) Rz 214.
[25] *Rechberger/Oberhammer*, Exekutionsrecht[5] (2009) Rz 151.
[26] *Rechberger/Oberhammer*, Exekutionsrecht[5] (2009) Rz 150.
[27] OGH 24.06.2014, 4 Ob 71/14s.
[28] *Rechberger/Oberhammer*, Exekutionsrecht[5] (2009) Rz 204.

Greift eine Exekution in die Rechtssphäre eines Dritten ein, so steht es diesem frei, eine sogenannte Exszindierungsklage nach § 37 EO zu erheben.[29] Die Exszindierungsklage ist eine negative Feststellungsklage, welche darauf gerichtet ist, festzustellen, dass eine bestimmte Exekution unzulässig ist; wird ihr stattgegeben, so ist die Exekution einzustellen.[30]
Im Fall eines Eingriffs in die Informationsfreiheit durch eine Exekution zur Durchsetzung von Internetsperren ist nach Ansicht des OGH jedermann aktivlegitimiert, der von diesem Eingriff betroffen ist.[31]

3.3. E-Commerce-Richtlinie

3.3.1. Die Haftungsfreistellung der Access-Provider

Im Zusammenhang mit Sperraufforderungen gegen Access-Provider darf die Haftungsprivilegierung des § 13 ECG nicht außer Acht gelassen werden. Demnach haften Diensteanbieter nicht für Informationen, so lange sie diese nur übermitteln oder den Zugang zu einem Kommunikationsnetz vermitteln, wenn sie die Übermittlung nicht selbst veranlassen, den Empfänger der Übermittlung nicht auswählen und die übermittelten Informationen weder auswählen noch verändern. Artikel 12 Abs 3 der RL 2000/31/EG [32] (E-Commerce Richtlinie) sieht jedoch ausdrücklich vor, dass die Möglichkeit unberührt bleibt, dass ein Gericht oder eine Verwaltungsbehörde vom Access-Provider verlangen, eine Rechtsverletzung zu verhindern oder abzustellen – Sperrverfügungen sind folglich vom ECG bzw der E-Commerce Richtlinie gedeckt.

3.3.2. Verbot allgemeiner Überwachungspflichten: SABAM und Scarlet Extended

Artikel 15 E-Commerce Richtlinie verbietet, Access-Providern eine allgemeine Verpflichtung aufzuerlegen, die von ihnen übertragenen oder gespeicherten Daten zu überwachen oder aktiv nach rechtswidrigen Tätigkeiten zu forschen. Das daraus folgende Verbot der Verpflichtung

[29] *Rechberger/Oberhammer*, Exekutionsrecht[5] (2009) Rz 221.
[30] *Rechberger/Oberhammer*, Exekutionsrecht[5] (2009) Rz 222.
[31] OGH 24.06.2014, 4 Ob 71/14s.
[32] Richtlinie 2000/31/EG des Europäischen Parlamentes und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), Abl L 2000/178, 1.

zur Einrichtung von Filtersystemen wurde in den Entscheidungen SABAM[33] sowie Scarlet-Extended[34] vom EuGH konkretisiert:

Die Urteile SABAM sowie Scarlet Extended beschäftigen sich beide mit der Problematik, ob es einem Access-Provider (im Falle von Scarlet Extended) bzw einem Host-Provider (im Falle von SABAM) zugemutet werden kann, ein Filtersystem einzurichten, das unterschiedslos auf alle Nutzer anwendbar ist und zeitlich unbegrenzt auf Kosten des Providers einzurichten ist, um präventiv Urheberrechtsverletzungen in Peer-to-Peer Netzwerken (Scarlet Extended) bzw sozialen Netzwerken (SABAM) zu verhindern.

Der EuGH hat die Zulässigkeit eines solchen Filtersystems verneint.

Art 15 Abs 1 der E-Commerce Richtline untersage nämlich ausdrücklich, Diensteanbietern generelle Überwachungspflichten aufzuerlegen.[35] Dies gelte gemäß ständiger Rechtsprechung insbesondere auch dann, wenn Gegenstand der Überwachungspflicht die Verhinderung von Verletzungen geistigen Eigentums sei. Ebenso könne die Verhältnismäßigkeit im Sinne des Art 3 RL 2004/48/EG[36] (Enforcementrichtlinie) im Zusammenhang mit solchen Pflichten nicht gewahrt werden[37], derlei Anordnungen würden darüber hinaus kein angemessenes Gleichgewicht zwischen dem Eigentumsrecht der Rechteinhaber und der unternehmerischen Freiheit der Provider herstellen[38].

In Bezug auf die Kunden der Provider bestehe ein grundrechtliches Ungleichgewicht, da einerseits eine vollständige Überwachung der übermittelten Inhalte in Verbindung mit Sammlung und Identifizierung von IP-Adressen deren Grundrecht auf Schutz personenbezogener Daten übermäßig beeinträchtige und andererseits, da Fehler im Rahmen des Filtersystems nicht auszuschließen seien, die Sperrung von rechtmäßigen Inhalten einen Eingriff in die Informationsfreiheit darstellen würde. Es sei beispielsweise denkbar, dass das System Inhalte filtere, die in einem Mitgliedsstaat geschützt, in einem anderen jedoch gemeinfrei seien.[39]

---

[33] EuGH 16.02.2012, C-360/10 (SABAM) = RdW 2012/163, 153 = wbl 2012/49, 150 = ecolex 2012/147, 333 = jusIT 2012/22, 54 = jusIT 2012/40, 85 (*Beimrohr*) = ZTR 2012, 128.
[34] EuGH 24.11.2011, C-70/10 (Scarlet Extended) = RdW 2011/719, 705 = jusIT 2011/98, 215 = SWI 2011, 14 = lex:itec 2011 H 5, 16 = wbl 2012/50, 153 = jusIT 2012/40, 85 (Beimrohr).
[35] EuGH 24.11.2011, C-70/10 (Scarlet Extended), RN 35.
[36] Richtlinie 2004/48/EG des Europäischen Parlamentes und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums, Abl L 2004/157, 45.
[37] EuGH 24.11.2011, C-70/10 (Scarlet Extended), RN 36 mwN.
[38] EuGH 24.11.2011, C-70/10 (Scarlet Extended), RN 49.
[39] EuGH 24.11.2011, C-70/10 (Scarlet Extended), RN 51 ff.

3.4. Grundrechte

3.4.1. Rechtsquellen und Rechtsgrundlagen

3.4.1.1. National garantierte Grundrechte

Die EMRK als erste verbindliche Menschenrechtskonvention weltweit wurde am 4.11.1950 in Rom unterzeichnet und ebenso wie ihre zahlreichen Zusatzprotokolle, welchen die gleiche Wirkung wie der Konvention selbst zukommen, von allen Mitgliedsstaaten der Europäischen Union ratifiziert, wobei in Bezug auf die Zusatzprotokolle kein einheitlicher Ratifizierungsstand besteht.[40]

Österreich trat der EMRK im Jahr 1958 bei, die EMRK steht in Österreich seit 1964 im Verfassungsrang. [41] Weitere grundrechtliche Rechtsquellen sind vor allem das Staatsgrundgesetz 1867 (StGG) gemeinsam mit dem Gesetz zum Schutze der persönlichen Freiheit, dem Gesetz zum Schutze des Hausrechts, dem Beschluss der Provisorischen Nationalversammlung vom 30.10.1918, Abschnitt V des III. Teils des Staatsvertrags von St. Germain und Artikel 1 § 1 DSG. Ergänzt wurde das StGG durch die Einfügung des Fernmeldegeheimnisses[42], die Einfügung der Kunstfreiheit[43] sowie durch das BVG über den Schutz der persönlichen Freiheit[44].[45]

Art 53 EMRK normiert das sogenannte Günstigkeitsprinzip: Gibt es innerstaatlich günstigere Regelungen als korrespondierende Regelungen der EMRK, so geht das innerstaatliche Recht der EMRK vor.[46]

Bei der Umsetzung von Richtlinien in österreichisches Recht oder beim Erlass von innerstaatlichen Verordnungen auf Grundlage von Unionsrecht unterliegt der Gesetzgeber bzw Verordnungsgeber dem sogenannten „Prinzip der doppelten Bindung“[47]. Wird durch Unionsrecht die innerstaatliche Durchführung nicht vollständig determiniert, sind in Bezug auf den offen bleibenden Spielraum sowohl das Unionsrecht als auch das nationale Verfassungsrecht beachtlich.[48] Das Thema meiner Masterarbeit betreffend ergibt sich daraus,

[40] *Jarass*, Charta der Grundrechte der EU[2], Einleitung Rz 42 (2013).
[41] *Öhlinger*, Verfassungsrecht[10] Rz 681 (2014).
[42] BGBl Nr. 8/1974.
[43] BGBl Nr. 262/1982.
[44] Bundesverfassungsgesetz vom 29. November 1988 über den Schutz der persönlichen Freiheit, BGBl Nr. 684/1988.
[45] *Öhlinger*, Verfassungsrecht[10] Rz 679 (2014).
[46] *Öhlinger*, Verfassungsrecht[10] Rz 681 (2014).
[47] Zitiert nach *Öhlinger*, Verfassungsrecht[10] Rz 200 (2014).
[48] *Öhlinger*, Verfassungsrecht[10] Rz 200 (2014).

dass bezüglich der Erlassung von Sperranordnungen nach Artikel 8 Informationsgesellschaftsrichtlinie bzw § 81 Abs 1 UrhG sowohl die Unionsgrundrechte als auch die österreichischen Grundrechte beachtlich sind, da deren Erlassung nicht abschließend durch die Informationsgesellschaftsrichtlinie determiniert ist.

3.4.1.2. Grundrechte im Unionsrecht

Der EuGH entwickelte bereits frühzeitig autonom für das Gemeinschaftsrecht (später: Unionsrecht) Grundrechte in Form allgemeiner Rechtsgrundsätze. Diese stützte er einerseits auf die gemeinsame Verfassungstradition der Mitgliedsstaaten und andererseits auf völkerrechtliche Verträge zum Schutz der Menschenrechte, welchen die Mitgliedsstaaten beigetreten sind, so insbesondere die Europäische Menschenrechtskonvention (EMRK). [49]

Da der EMRK im Rahmen der Bildung der Rechtsgrundsatz-Grundrechte die größte Bedeutung zukam, überschneiden sich diese in erheblichem Umfang, andererseits reichen die Grundrechte der EuGH-Rechtsprechung teilweise über den Schutzgehalt der EMRK hinaus. [50] Die EMRK fungierte als reine Rechtserkenntnisquelle und nicht als Rechtsquelle, lieferte also keine strikten Vorgaben zum Inhalt der Rechtsgrundsatz-Grundrechte. [51] Artikel 6 des Vertrags von Maastricht[52] nimmt ausdrücklich auf diese Rechtsgrundsatz-Grundrechte Bezug, weswegen diese spätestens seit dessen Inkrafttreten unzweifelhaft Teil des Primärrechts sind.

Die Bestrebungen, die Grundrechte in einem verbindlichen Text festzuhalten, gipfelten im Jahr 2000 in der durch den Grundrechtekonvent erarbeiteten „Charta der Grundrechte der Europäischen Union“.[53] Als Ergebnis eines Kompromisses zwischen den Mitgliedsstaaten erfolgte in Form der Charta vor allem eine Niederschrift bereits bestehender allgemeiner Rechtsgrundsätze; die Charta orientiert sich wiederum stark an der EMRK, was vor allem durch Art 52 Abs 2 und 3 Grundrechtecharta deutlich wird. [54] Die Rechtsgrundsatz-Grundrechte des EuGH gelten, wie in Art 6 Abs 3 EUV festgehalten ist, weiter neben der Grundrechtecharta[55], sie stehen gleichberechtigt nebeneinander[56], was zur Notwendigkeit

[49] *Jarass*, Charta der Grundrechte der EU[2], Einleitung Rz 28 (2013).
[50] *Jarass*, Charta der Grundrechte der EU[2], Einleitung Rz 28 (2013).
[51] *Jarass*, Charta der Grundrechte der EU[2], Einleitung Rz 29 (2013).
[52] Vertrag über die Europäische Union, ABl. C 191/1992.
[53] *Jarass*, Charta der Grundrechte der EU[2], Einleitung Rz 2 (2013).
[54] *Jarass*, Charta der Grundrechte der EU[2], Einleitung Rz 3 (2013).
[55] *Jarass*, Charta der Grundrechte der EU[2], Einleitung Rz 30 (2013).
[56] *Jarass*, Charta der Grundrechte der EU[2], Einleitung Rz 33 (2013).

einer harmonisierenden Auslegung der Chartagrundrechte im Lichte der Rechtsgrundsatz-Grundrechte führt[57].

Art 52 Abs 3 Satz 1 Grundrechtecharta normiert für die Chartagrundrechte die „gleiche Bedeutung und Tragweite" wie die Grundrechte der EMRK, weswegen der EMRK bei überschneidenden Grundrechten eine besondere Bedeutung beizumessen ist.[58] Vielen besonders wichtigen Grundrechten kommt folglich eine vollständige oder zumindest weitreichende Übereinstimmung zu. Finden sich Grundrechte der Charta nicht explizit in der EMRK, so wurden sie dennoch in vielen Fällen vom EGMR aus anderen EMRK-Grundrechten abgeleitet.[59] Die Überschneidung von Chartagrundrechten mit EMRK-Grundrechten bedeutet allerdings nicht, dass Chartagrundrechte nicht einen weitgehenderen Schutz als die EMRK gewähren können. Schutzbereich oder Einschränkungsmöglichkeiten von Chartagrundrechten können zugunsten der Grundrechtsträger folglich über den Schutz der EMRK hinausgehen. In Bereichen, in denen der EGMR zu einer extensiven Auslegung der Grundrechte aufgrund von Lücken in der EMRK greift, entfällt im Bereich der Charta, solange diese spezielle Grundrechte für diese Bereiche vorsieht, die Rechtfertigung für eine extensive Auslegung der Chartagrundrechte. Bei Auslegung jener Chartagrundrechte, welche ihre Entsprechung nur in lückenfüllender EGMR-Rechtsprechung finden, sind dennoch relevante Entscheidungen des EGMR zu berücksichtigen.[60] Es müssen also Charta- und EMRK-Grundrechte nicht immer übereinstimmen, der Schutz der Charta darf aber jedenfalls nicht hinter dem der EMRK zurückbleiben („Gewährleistung des Mindestgehalts").[61] Unbeschadet dieser großen Bedeutung ist es wichtig zu betonen, dass die EMRK kein Bestandteil des Unionsrechts ist, sondern lediglich Rechtserkenntnisquelle, an die die Auslegung der Charta anzupassen ist.[62]

Schon vor der Grundrechtecharta war auf die Rechtsprechung des EGMR Bedacht zu nehmen.[63] Im Zuge der Gewährleistung des Mindestgehalts der Grundrechte durch Art 52 Abs 3 1. Satz Grundrechtecharta ist weiterhin die EGMR-Judikatur einzubeziehen, selbst wenn

[57] *Jarass*, Charta der Grundrechte der EU[2], Einleitung Rz 34 (2013).
[58] *Jarass*, Charta der Grundrechte der EU[2], Art 52 Rz 60 (2013).
[59] *Jarass*, Charta der Grundrechte der EU[2], Art 52 Rz 61 (2013).
[60] *Jarass*, Charta der Grundrechte der EU[2], Art 52 Rz 62 (2013).
[61] *Jarass*, Charta der Grundrechte der EU[2], Art 52 Rz 63 (2013).
[62] *Jarass*, Charta der Grundrechte der EU[2], Art 52 Rz 64 (2013).
[63] EuGH 15.10.2002, C-238/99 (Limburgse Vinyl Maatschappij u.a. / Kommission).

infolge einer dynamischen Auslegung durch den EGMR der Schutzbereich eines Grundrechts erweitert wird.[64]

Mit dem Vertrag von Lissabon[65] wurde die Grundrechtecharta geringfügig ergänzt[66] und erlangte durch Inkrafttreten des Art 6 Abs 1 EUV mit 1.12.2009 ihre Verbindlichkeit.[67] Die Grundrechtecharta ist Teil des Primärrechts, sie ist gleichrangig mit den Verträgen. Aufgrund der Gleichrangigkeit ist beim Aufeinandertreffen im Rahmen der Auslegung ein angemessenes Gleichgewicht herzustellen, die Grundrechte gehen also, im Unterschied zu ihrem Verhältnis zum Sekundärrecht, nicht generell dem sonstigen Primärrecht vor, sondern nur dann, wenn eine Einschränkung des betroffenen Grundrechts im konkreten Fall ausscheidet (siehe dazu sogleich unter 3.4.1.3).[68]

Art 51 Grundrechtecharta normiert, dass die Charta für Organe und Einrichtungen der Union sowie für die Mitgliedsstaaten bei Vollzug von Unionsrecht gilt. Der EuGH legte den Bereich des Vollzugs des Unionsrechts im Zuge der Entscheidung Fransson weit aus: Selbst nationale Vorschriften, die nicht zur Umsetzung einer Richtlinie erlassen wurden, fallen unter den Vollzug des Unionsrechts, wenn sie sicherstellen sollen, dass durch ihre Anwendung Verstöße gegen eine Richtlinie geahndet werden sollen:[69] „*Hat das Gericht eines Mitgliedsstaats zu prüfen, ob mit den Grundrechten eine nationale Vorschrift oder Maßnahme vereinbar ist, die in einer Situation, in der das Handeln eines Mitgliedsstaats nicht vollständig durch das Unionsrecht bestimmt wird, das Unionsrecht im Sinne von Art. 51 Abs. 1 der Charta durchführt, steht es somit den nationalen Behörden und Gerichten weiterhin frei, nationale Schutzstandards für die Grundrechte anzuwenden, sofern durch diese Anwendung weder das Schutzniveau der Charta, wie sie vom Gerichtshof ausgelegt wird, noch der Vorrang, die Einheit und die Wirksamkeit des Unionsrechts beeinträchtigt werden. Dabei haben die nationalen Gerichte, wenn sie Bestimmungen der Charta auslegen sollen, die Möglichkeit und gegebenenfalls die Pflicht, den Gerichtshof um eine Vorabentscheidung nach Art. 267 AEUV zu ersuchen.*“[70]

Daraus folgt, dass im Rahmen des österreichischen Verfahrens zur Erlassung von

[64] *Jarass*, Charta der Grundrechte der EU[2], Art 52 Rz 65 (2013).
[65] Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft, Abl C 306/2007.
[66] *Jarass*, Charta der Grundrechte der EU[2], Einleitung Rz 3 (2013).
[67] *Jarass*, Charta der Grundrechte der EU[2], Einleitung Rz 6 (2013).
[68] *Jarass*, Charta der Grundrechte der EU[2], Einleitung Rz 10 (2013).
[69] EuGH 26.02.2013, C-617/10 (Fransson) = ÖJZ 2013/37, 380 (Posch) = taxlex-EU 2013/47, 147 = ZfRV-LS 2013/14, 71 = RdW 2013/116, 118 = EuGRZ 2013, 124 = UVS-Slg 2013/84, 92 = ÖJZ 2014/81, 494 (*Zeder*) Rz 28.
[70] EuGH 26.02.2013, C-617/10 (Fransson) Rz 29 - 30.

Sperrverfügungen, da es sich dabei um eine Maßnahme zur Ahndung von Verstößen im Rahmen des Art 8 Abs 3 Informationsgesellschaftsrichtlinie handelt, die Rechtsgarantien der Grundrechtecharta neben den national garantierten Grundrechten maßgeblich sind.

3.4.1.3. Rechtfertigung von Grundrechtseingriffen

Art 51 Abs 1 Grundrechtecharta regelt die Voraussetzungen von Grundrechtseingriffen, also wann eine Beschränkung der garantierten Rechte durch Gesetzgebung oder Vollziehung rechtmäßig ist. Die Prüfung der Rechtmäßigkeit eines Eingriffs erfolgt in Form einer Verhältnismäßigkeitsprüfung.[71] Ähnlich prüft auch der VfGH Eingriffe in national garantierte Grundrechte.[72]

Infolge soll nun ein kurzer Überblick über die wichtigsten Eckpunkte einer Grundrechtsprüfung gegeben werden.

Sowohl in Bezug auf die Chartagrundrechte als auch auf die der EMRK sowie die in sonstigen Rechtsakten garantierten nationalen Grundrechte ist generell eine gesetzliche Grundlage, ein legitimes Ziel sowie die Verhältnismäßigkeit der Maßnahme notwendig, um einen Eingriff zu rechtfertigen.[73]

Ein Eingriff in durch die EMRK bzw die Grundrechtecharta garantierte Rechte kann nur dann erlaubt sein, wenn der materielle Gesetzesvorbehalt der EMRK eingehalten wird – de facto ist dies aufgrund des Günstigkeitsprinzips auch zB für Rechte des StGG maßgeblich. Der materielle Gesetzesvorbehalt konkretisiert das öffentliche Interesse, welches einen Eingriff rechtfertigt. So werden bei den meisten Grundrechtsgarantien der EMRK oder der Grundrechtecharta die Rechtsgüter aufgezählt, zu deren Gunsten ein Eingriff erfolgen darf.[74] Findet sich für ein in der Charta und der EMRK garantiertes Grundrecht keine Einschränkung der legitimen Ziele, so ist im Bereich des Unionsrechts Art 52 Abs 1 Grundrechtecharta maßgeblich: Demnach sind Einschränkungen nur dann möglich, wenn sie entweder dem von der Union anerkannten Gemeinwohl oder dem Schutz der Rechte und Freiheiten anderer dienen.[75]

Die Verhältnismäßigkeitsprüfung an sich gliedert sich in drei Teile: Geeignetheit, Erforderlichkeit und Angemessenheit.

---

[71] *Jarass*, Charta der Grundrechte der EU[2], Art 52 Rz 1ff (2013).
[72] *Öhlinger*, Verfassungsrecht[10] Rz 715ff (2014).
[73] *Jarass*, Charta der Grundrechte der EU[2], Art 52 Rz 21 (2013) sowie *Öhlinger*, Verfassungsrecht[10] Rz 716 (2014).
[74] *Öhlinger*, Verfassungsrecht[10] Rz 714 (2014).
[75] *Jarass*, Charta der Grundrechte der EU[2], Art 52 Rz 31 (2013).

Geeignetheit bedeutet, dass die Einschränkung zur Erreichung des angestrebten Ziels geeignet sein muss, also die Einschränkung tatsächlich dem Einschränkungsgrund dient. Ein Beitrag der Maßnahme zur Zielerreichung reicht aus, um die Geeignetheit zu begründen.[76]

Erforderlich ist eine Maßnahme nur dann, wenn sie nicht über das zur Zielerreichung Erforderliche hinausreicht. Die Maßnahme darf also nur so weit gehen, wie es zur Zielerreichung tatsächlich notwendig ist.[77] Außerdem darf es kein anderes, gelinderes Mittel geben, das zur Zielerreichung ebenso gut geeignet ist. Es muss jenes Mittel gewählt werden, welches zwar das Ziel erreicht, die Grundrechtsposition aber am wenigsten einschränkt.[78]

Eine Maßnahme ist angemessen, wenn die Nachteile, die durch sie verursacht werden, in einem angemessenen Verhältnis zum zu erreichenden Ziel stehen. Es ist also eine Güterabwägung zwischen dem Eingriff und dem Ziel vorzunehmen, das gerechte Gleichgewicht muss gewahrt bleiben. Dieser finale Schritt der Abwägung wird auch als Verhältnismäßigkeit im engeren Sinn bezeichnet. [79]

3.4.2. Relevante Grundrechte

3.4.2.1. Einleitung

Die Grundrechtecharta gliedert sich in sieben Titel: Allgemeiner Teil, Rechte betreffend die „Würde des Menschen", „Freiheiten", „Gleichheit", „Solidarität", „Bürgerrechte" sowie „Justizielle Rechte". [80] Meine Master-Thesis betreffend sind jedenfalls Rechte aus dem Bereich der „Freiheiten" tangiert; sie sind im Folgenden näher zu Erörtern.

Relevant sind einerseits das Recht auf freie Meinungsäußerung bzw das daraus resultierende Recht auf Informationsfreiheit: Die Sperre einer Webseite kann nämlich einerseits bedeuten, dass Internetbenutzer auch auf rechtmäßig auf dieser Seite vorhandene Informationen nicht mehr zugreifen können. Andererseits wird natürlich auch die freie Meinungsäußerung der Websitebetreiber beschnitten, wenn deren Website nicht mehr zugänglich ist. Nicht zuletzt ist es auch Aufgabe der Access-Provider, Informationen und Meinungen zu transportieren, weswegen auch diese als indirekte Adressaten des Grundrechts anzusehen sind (siehe dazu 3.4.2.2).

[76] EuGH 05.10.1994, C-280/93 (Deutschland / Rat), Rz 90ff. Siehe dazu weiterführend *Jarass*, Charta der Grundrechte der EU[2], Art 52 Rz 37 (2013).
[77] *Jarass*, Charta der Grundrechte der EU[2], Art 52 Rz 38 (2013).
[78] *Jarass*, Charta der Grundrechte der EU[2], Art 52 Rz 39 (2013).
[79] *Jarass*, Charta der Grundrechte der EU[2], Art 52 Rz 40 (2013).
[80] *Jarass*, Charta der Grundrechte der EU[2], Einleitung Rz 12ff (2013).

Auf der anderen Seite stellt das rechtswidrige Onlinestellen von urheberrechtlich geschütztem Material einen Eingriff in das Recht auf geistiges Eigentum der Rechteinhaber dar (siehe dazu 3.4.2.3).

Die Access-Provider als Adressaten von Sperren sehen sich wiederum einem Eingriff in ihre unternehmerische Freiheit ausgesetzt, da sie wegen der von ihnen zu treffenden Sperrmaßnahmen nicht mehr vollkommen frei über ihre Betriebsmittel verfügen können (siehe dazu 3.4.2.4).

Je nach technischer Umsetzung der Sperre gilt es zudem zu beachten, dass diese in das Recht auf den Schutz personenbezogener Daten (siehe dazu 3.4.2.5) und das Recht auf Schutz des Kommunikationsgeheimnisses (siehe dazu 3.4.2.6) der Internetnutzer eingreifen kann, weswegen auch diese Rechte dargestellt werden.

3.4.2.2. Das Recht auf freie Meinungsäußerung bzw Informationsfreiheit

Art 11 Grundrechtecharta: *„(1) Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben.*

(2) Die Freiheit der Medien und ihre Pluralität werden geachtet."

Mit dem Schutz von Meinungen, Informationen und Ideen bietet Art 11 einen umfassenden Schutz jeglicher Kommunikationsinhalte.[81] Dem Recht des Art 11 Grundrechtecharta korrespondieren die Rechte des Art 13 StGG, Z1 und 2 des Beschlusses der Provisorischen Nationalversammlung 1918 und Art 10 EMRK.[82] Im Rahmen von Einschränkungen des Grundrechts besteht folglich eine Bindung an die Ziele des Art 10 Abs 2 EMRK[83].

Informationen werden laut Satz 2 Art 11 Abs 1 Grundrechtecharta „*ohne Rücksicht auf Staatsgrenzen*" geschützt, der Schutz kommt damit in- wie ausländischen Informationen gleichermaßen zu.[84] Geschützt ist nicht nur die Weitergabe von Informationen oder das

[81] *Jarass*, Charta der Grundrechte der EU[2], Art 11 Rz 7 (2013).
[82] *Öhlinger*, Verfassungsrecht10 Rz 910 (2014).
[83] *Jarass*, Charta der Grundrechte der EU[2], Art 11 Rz 18 (2013).
[84] *Jarass*, Charta der Grundrechte der EU[2], Art 11 Rz 8 (2013).

Äußern von Meinungen, sondern auch deren Empfang, insbesondere der Zugang über das Internet.[85]

Grundrechtsträger ist jede natürliche Person[86], doch kann sich auch ein Access-Provider auf den Grundrechtsschutz berufen, da es seine Aufgabe ist, Meinungen und Informationen seiner Kunden zu übertragen[87]. Diese Ansicht entspricht der des EGMR, welcher im Rahmen der Entscheidung Öztürk gegen Türkei[88] erkannte, ein Verleger, welchem die Verbreitung eines bestimmten Buches untersagt werde, könne sich auf die Meinungsfreiheit berufen, auch gerade wenn dieser durch Verlegen des Buches nicht seine eigene Meinung transportiere, sondern den Autoren ein Medium biete. Das Recht der freien Meinungsäußerung erstrecke sich nämlich nicht nur auf den Informationsinhalt, sondern auch auf die Informationsverbreitung.[89]

Der Schutzbereich der Informationsfreiheit wird vom EGMR weit ausgelegt: Im Rahmen der „Pirate Bay" Entscheidung[90] erkannte der EGMR, dass auch Filesharing-Plattformen wie „The Pirate Bay" als Mittel zum Informationsaustausch in den Schutzbereich des Art 10 EMRK fallen. Eingriffe in Form von Gefängnisstrafen und Schadenersatzzahlungen gegen Betreiber solcher Seiten – sowie mE wohl auch analog dazu Sperrverfügungen – müssten die Schranken des Art 10 Abs 2 EMRK einhalten, wobei die Verbreitung von urheberrechtlich geschütztem Material im Rahmen der Meinungsfreiheit aber nicht dasselbe Schutzniveau erreichen könne wie zB politische Äußerungen und Debatten. Dem Staat komme jedenfalls in diesem Zusammenhang bei Abwägung der gegenläufigen Interessen, in diesem Fall der Meinungsfreiheit und dem Schutz geistigen Eigentums, ein weiter Ermessensspielraum zu. Im konkreten Fall sei dieser Ermessensspielraum nicht überschritten worden, da einerseits die verhängten Strafen verhältnismäßig gewesen seien und darüber hinaus die Betreiber von „the Pirate Bay" auch auf Aufforderung hin keinerlei rechtsverletzende „.torrent"-Dateien entfernt hätten, sich also bewusst darüber waren, dass über ihre Seite urheberrechtlich geschütztes Material verbreitet wurde.[91]

[85] *Jarass*, Charta der Grundrechte der EU[2], Art 11 Rz 10f (2013).
[86] *Jarass*, Charta der Grundrechte der EU[2], Art 11 Rz 13 (2013).
[87] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 82 mwN.
[88] EGMR 28.09.1999, 22479/93 (Öztürk gegen Türkei).
[89] EGMR 28.09.1999, 22479/93 (Öztürk gegen Türkei), § 49.
[90] EGMR 19.02.2013, 40397/12 (Fredrik Neij und Peter Sunde Kolmisoppi) = MR-Int 2013, 45.
[91] EGMR 19.02.2013, 40397/12 (Fredrik NEIJ und Peter SUNDE KOLMISOPPI).

Damit räumt der EGMR den nationalen Behörden in Bezug auf die Meinungsfreiheit einen besonders weiten Ermessensspielraum ein und betont, dass es ganz wesentlich auf die Art der vermittelten Information ankommt.[92]

3.4.2.3. Das Recht auf geistiges Eigentum

Art 17 Grundrechtecharta: *„(1) Jede Person hat das Recht, ihr rechtmäßig erworbenes Eigentum zu besitzen, zu nutzen, darüber zu verfügen und es zu vererben. Niemandem darf sein Eigentum entzogen werden, es sei denn aus Gründen des öffentlichen Interesses in den Fällen und unter den Bedingungen, die in einem Gesetz vorgesehen sind, sowie gegen eine rechtzeitige angemessene Entschädigung für den Verlust des Eigentums. Die Nutzung des Eigentums kann gesetzlich geregelt werden, soweit dies für das Wohl der Allgemeinheit erforderlich ist.*

(2) Geistiges Eigentum wird geschützt."

Das Eigentumsrecht gemäß Art 17 schützt jedes vermögenswerte Recht, wenn dieses von substantieller Bedeutung ist. Es sind also auch Ansprüche erfasst, die dem Einzelnen so zugeordnet sind, dass er erwarten kann, sie eigenverantwortlich nutzen zu können.[93] Voraussetzung für den Schutz ist, dass das Eigentum rechtmäßig erworben wurde.[94]

Art 2 leg.cit. nimmt ausdrücklich auf das geistige Eigentum Bezug und unterstreicht damit unter anderem die Bedeutung der immaterialgüterrechtlichen Ausschließlichkeitsrechte.

Mit dem Recht des Art 17 Grundrechtecharta korrespondieren die Rechte des Art 5 StGG sowie Art 1 1. ZP-EMRK, wobei diese nicht ausdrücklich auf geistiges Eigentum Bezug nehmen, sondern der Schutz desselben Folge von Rechtsfortentwicklung im Rahmen der Rechtsprechung[95] ist.[96]

Grundrechtsadressaten sind in- wie ausländische juristische und natürliche Personen.[97]

---

[92] *Lehofer*, EGMR zur Abwägung zwischen Urheberrecht und freier Meinungsäußerung (Neij und Sunde, The Pirate Bay).
[93] *Jarass*, Charta der Grundrechte der EU[2], Art 17 Rz 6 (2013).
[94] *Jarass*, Charta der Grundrechte der EU[2], Art 17 Rz 7 (2013).
[95] So beispielsweise EGMR 11.01.2007, 73049/01 (Anheuser-Busch Inc. gegen Portugal).
[96] *Öhlinger*, Verfassungsrecht[10] Rz 868 mwN (2014).
[97] *Jarass*, Charta der Grundrechte der EU[2], Art 17 Rz 17 (2013).

3.4.2.4. Das Recht auf unternehmerische Freiheit

Art 16 Grundrechtecharta: *„Die unternehmerische Freiheit wird nach dem Gemeinschaftsrecht und den einzelstaatlichen Rechtsvorschriften und Gepflogenheiten anerkannt."*

Art 16 schützt die freie Berufsausübung der Unternehmer und garantiert dadurch die Wahrung ihrer Interessen und einen freien Wettbewerb.[98] Vom Schutz des Rechts auf unternehmerische Freiheit sind die Aufnahme, Beendigung sowie alle Aspekte der Durchführung einer unternehmerischen Tätigkeit umfasst, ebenso die Art und Weise der Unternehmensführung.[99] Zum Schutzbereich zählt also zweifellos auch die freie Verfügung über technische Ressourcen des Unternehmers.[100]

Grundrechtsadressaten sind in- wie ausländische juristische und natürliche Personen.[101]

3.4.2.5. Des Recht auf Schutz personenbezogener Daten

Art 8 Grundrechtecharta: *„(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.*

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht."

Das Recht auf den Schutz personenbezogener Daten korrespondiert im Wesentlichen dem Grundrecht auf Datenschutz des § 1 DSG. Auch die EMRK schützt personenbezogene Daten, wobei dieser Schutz auf das in Art 8 EMRK normierte Recht auf Privatleben zurückgeht. Die Rechtsfortbildung des Art 8 EMRK stellt den Ausgangspunkt des grundrechtlichen Datenschutzes in Europa dar. [102]

Personenbezogene Daten im Sinne der Grundrechtecharta sind alle Informationen über eine bestimmte oder indirekt bestimmbare natürliche Person[103], der Schutz des § 1 DSG steht auch

[98] *Jarass*, Charta der Grundrechte der EU[2], Art 16 Rz 2 (2013).
[99] *Jarass*, Charta der Grundrechte der EU[2], Art 16 Rz 9 (2013).
[100] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 49.
[101] *Jarass*, Charta der Grundrechte der EU[2], Art 16 Rz 10f (2013).
[102] *Öhlinger*, Verfassungsrecht[10] Rz 827 (2014).
[103] *Jarass*, Charta der Grundrechte der EU[2], Art 8 Rz 5 (2013).

juristischen Personen zu[104]. Im Sinne des Günstigkeitsprinzips (siehe dazu 3.4.1.1) können sich in Österreich juristische Personen also jedenfalls auf das Grundrecht des Schutzes personenbezogener Daten berufen.

Vom Grundrecht der Grundrechtecharta sind alle Informationen erfasst, die die Privat- und Intimsphäre betreffen. Voraussetzung für den Schutz ist ein ausreichend personaler Bezug, eine etwaige Einstufung von Daten als „sensibel" ist unerheblich.[105] Verpflichtete des Grundrechts sind einerseits die Union und ihre Organe, andererseits sind auch Sekundärrechtsakte im Lichte des Grundrechts auszulegen. Privatpersonen werden nur erfasst, wenn sie durch Regelungen in Umsetzung der Schutzpflicht dazu angehalten sind.[106] Vom Grundrecht Verpflichtete sind aber angehalten, im Rahmen ihrer Tätigkeitsbereiche für den Schutz personenbezogener Daten gegenüber Privaten zu sorgen.[107] Insbesondere sind auch privatrechtliche Verträge grundrechtskonform auszulegen.[108]

Unabhängig davon, ob jemandem, der den Schutz des Art 8 Grundrechtecharta genießt, daraus ein Nachteil erwächst, liegt ein Eingriff immer dann vor, wenn Daten verarbeitet, also erhoben, gespeichert, verwendet, gesperrt oder gelöscht werden.[109] Kein Eingriff liegt vor, wenn der Betroffene in Kenntnis der Sachlage der Verarbeitung zustimmt.[110]

Der Schutz des § 1 DSG kommt, wie bereits erwähnt, natürlichen wie juristischen Personen zugute. Verpflichtete des Grundrechts sind einerseits öffentliche Stellen, andererseits auch Private (Drittwirkung des Grundrechts nach § 5 Abs 4 DSG, wonach das Grundrecht auch Wirkung zwischen Privaten entfaltet)[111]. Im Rahmen des § 1 DSG stehen Grundrechtsträgern das Recht auf Geheimhaltung, sowie zu dessen Durchsetzung die Rechte auf Richtigstellung, Löschung sowie Auskunft (sogenannte „Begleitgrundrechte") zu.[112]

In Bezug auf die dieser Masterarbeit zu Grunde liegende Problematik erscheint vor allem das Recht auf Geheimhaltung, insbesondere der dadurch gewährte Ermittlungsschutz[113] von Relevanz; daher steht es im Folgenden im Zentrum meiner Betrachtung. Das Recht auf Geheimhaltung des § 1 DSG schützt die Grundrechtsträger vor Ermittlung und Weitergabe

[104] *Dohr/Pollirer/Weiss/Knyrim*, DSG^2 § 1 Rz 5 (Stand 2.7.2014).
[105] *Jarass*, Charta der Grundrechte der EU^2, Art 8 Rz 6 (2013).
[106] *Jarass*, Charta der Grundrechte der EU^2, Art 8 Rz 2 (2013).
[107] *Jarass*, Charta der Grundrechte der EU^2, Art 8 Rz 10 (2013).
[108] *Jarass*, Charta der Grundrechte der EU^2, Art 8 Rz 3 (2013).
[109] *Jarass*, Charta der Grundrechte der EU^2, Art 8 Rz 8 (2013).
[110] *Jarass*, Charta der Grundrechte der EU^2, Art 8 Rz 9 (2013).
[111] *Dohr/Pollirer/Weiss/Knyrim,* DSG^2 § 5 Rz 13 (Stand 2.7.2014).
[112] *Dohr/Pollirer/Weiss/Knyrim*, DSG^2 § 1 Rz 2ff (Stand 2.7.2014).
[113] *Dohr/Pollirer/Weiss/Knyrim*, DSG^2 § 1 Rz 6 (Stand 2.7.2014).

ihrer Daten. Das Grundrecht erfasst sämtliche personenbezogenen Daten, unabhängig von deren Verwendung. Voraussetzung des Grundrechtsschutzes ist das Vorliegen eines schutzwürdigen Geheimhaltungsinteresses, in Bezug auf allgemein verfügbare Daten und nicht auf Personen rückführbare Daten besteht dieses Interesse wohl nicht.[114]

Eine Beschränkung dieses Grundrechts ist aus drei Gründen zulässig. Erstens: wenn die Verwendung der personenbezogenen Daten im lebenswichtigen Interesse des Betroffenen liegt, zweitens: wenn die Verwendung mit seiner Zustimmung erfolgt oder drittens: wenn die Beschränkung zur Wahrung überwiegender berechtigter Interessen eines anderen notwendig ist. In Bezug auf letztere Möglichkeit ist im privaten Bereich eine Interessenabwägung zwischen Eingreifendem und Betroffenen vorzunehmen, im öffentlichen Bereich bedarf es einer gesetzlichen Ermächtigung, wobei die Interessenabwägung hier auf der generell-abstrakten Ebene durch den Gesetzgeber nach dem Grundsatz der Verhältnismäßigkeit vorzunehmen ist. Sensible Daten im Sinne des § 4 Z 2 DSG, also Daten über ethnische Herkunft, politische Gesinnung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit und Sexualleben, dürfen nur zur Wahrung wichtiger öffentlicher Interessen verarbeitet werden.[115]

Zur Klarstellung soll hier zudem auf den Personenbezug von IP-Adressen eingegangen werden. Einerseits können diese in gewissen Konstellationen unzweifelhaft direkten Personenbezug aufweisen (zB interne IP-Adressen von einem PC am Arbeitsplatz, welcher nur von einer Person genutzt wird), andererseits kann deren direkter Personenbezug auch aufgrund eines Gesetzes gegeben sein (zB sind IP-Adressen aus Perspektive der Polizei aufgrund der Befugnis des § 53 Abs 3a SPG in der Regel ein personenbezogenes Datum). Sie können jedoch auch nur indirekten Personenbezug aufweisen (zB wenn, abgesehen von § 53 Abs 3a SPG, eine Zuordnung nur durch den Provider erfolgen kann) oder aber anonym sein (zB wenn es sich um die IP eines öffentlichen WLANs handelt, welches ohne Registrierung genutzt werden kann).[116] Gemäß der Legaldefinition des § 92 Abs 3 Z 16 TKG sind „öffentliche IP-Adressen" ein Zugangsdatum im Sinne des § 92 Abs 3 Z 4a TKG und unterliegen grundsätzlich dem Kommunikationsgeheimnis [117] (zum Kommunikationsgeheimnis siehe sogleich unter 3.4.3).

[114] Der EuGH bejaht neuerdings ein solches Geheimhaltungsinteresse, wenn er im Zuge der Google-Spain-Entscheidung unter gewissen Voraussetzungen ein „Recht auf Vergessen" einräumt. EuGH 13.04.2014, C-131/12 (Google Spain und Google).
[115] *Jahnel/Mader/Staudegger (Hrsg)*, IT-Recht[3], S 430f (2012).
[116] *Jahnel/Mader/Staudegger (Hrsg)*, IT-Recht[3], S 429 (2012).
[117] Erläuterungen zur Regierungsvorlage zur TKG-Novelle 2011, XXIV. GP, 1074.

3.4.2.6. Das Recht auf Schutz des Kommunikationsgeheimnisses

Art 7 Grundrechtecharta: *„Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation."*

Art 7 Grundrechtecharta schützt die Kommunikation unter Abwesenden, insbesondere wenn sie der technischen Einrichtung eines Dritten zur Übermittlung überlassen wird, welche an bestimmte Adressaten, also nicht an die Öffentlichkeit, gerichtet ist[118]. Ein Recht auf den Schutz von Kommunikation findet sich auch im Fernmeldegeheimnis des Art 10a StGG[119], ebenso schützt Art 8 EMRK Korrespondenz, was inhaltlich dem Schutz des Art 7 Grundrechtecharta entspricht[120]. Verpflichtete dieser Grundrechte sind jeweils der Staat, die Mitgliedsstaaten bzw die Union, nicht jedoch Private.[121] Allerdings haben im Rahmen der Grundrechtecharta bzw EMRK die Grundrechtsverpflichteten dafür zu sorgen, dass im Rahmen ihrer Zuständigkeit dafür Sorge getragen wird, dass das Kommunikationsgeheimnis auch von Privaten geachtet wird.[122] Eine solche Verpflichtung findet sich in den §§ 93ff TKG (siehe dazu gleich unter 3.4.3), § 119 StGB unterwirft das Kommunikationsgeheimnis überdies strafrechtlichem Schutz.

Vom Schutzbereich des Art 10a StGG ist die Vertraulichkeit übermittelter Information erfasst, beispielsweise auch E-Mail-Verkehr und Internettelefonie. Eingriffe in Form der Kenntniserlangung des Inhalts sind nur auf Grundlage eines richterlichen Befehls erlaubt.[123] Strittig ist, ob unter diese Kenntniserlangung nur Inhaltsdaten oder aber auch Verkehrsdaten, also zB IP-Adressen, fallen: Der VwGH bejaht dies[124], seitens des VfGH ist noch keine Klarstellung erfolgt.

Der Schutzbereich des Art 8 EMRK bzw Art 7 Grundrechtecharta umfasst ebenfalls Kommunikationsinhalte, welche nicht an die Öffentlichkeit gerichtet sind, unabhängig von der verwendeten Technologie.[125] Als Eingriff können Handlungen gewertet werden, welche zur Kenntnis der Kommunikationsinhalte oder der Metadaten (Zeitpunkt, Teilnehmer) führen. Ein typisches Beispiel stellt die Beobachtung der Internetnutzung dar.[126]

---

[118] *Jarass*, Charta der Grundrechte der EU[2], Art 7 Rz 47 (2013).
[119] *Öhlinger*, Verfassungsrecht[10] Rz 824 (2014).
[120] *Jarass*, Charta der Grundrechte der EU[2], Art 7 Rz 43 (2013).
[121] *Jarass*, Charta der Grundrechte der EU[2], Art 7 Rz 45 (2013).
[122] *Jarass*, Charta der Grundrechte der EU[2], Art 7 Rz 51 (2013).
[123] *Öhlinger*, Verfassungsrecht[10] Rz 826 (2014).
[124] VwGH 24.04.2013, 2011/17/0293.
[125] *Jarass*, Charta der Grundrechte der EU[2], Art 7 Rz 43ff (2013).
[126] *Jarass*, Charta der Grundrechte der EU[2], Art 7 Rz 49 (2013).

3.4.3. Kommunikationsgeheimnis im TKG

Um die Frage nach der Zulässigkeit einer Deep Packet Inspection (siehe dazu unter 7.5) zu beantworten, sollen die relevanten einfachgesetzlichen Regelungen des TKG kurz dargestellt werden.

Das in § 93 TKG normierte Kommunikationsgeheimnis gilt gemäß § 92 Abs 1 TKG „*für die Verarbeitung und Übermittlung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlicher Kommunikationsdienste in öffentlichen Kommunikationsnetzen*“, wobei § 93 Abs 2 TKG explizit auf „*Betreiber eines öffentlichen Kommunikationsnetzes oder -dienstes*“ Bezug nimmt, worunter zweifelsohne Access-Provider zu subsumieren sind.

§ 93 Abs 1 TKG unterwirft dem Kommunikationsgeheimnis „*die Inhaltsdaten, die Verkehrsdaten und die Standortdaten*“ sowie „*Daten erfolgloser Verbindungsversuche*“. Damit geht der Schutz des § 93 Abs 1 TKG über den Schutzbereich des Art 10a StGG hinaus, da jedenfalls Verkehrsdaten und zusätzlich Standortdaten erfasst sind. Gemäß Abs 3 leg. cit. ist „*[d]as Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer [...] unzulässig*“.

Die §§ 97, 99 und 101 TKG normieren, unter welchen Bedingungen Stammdaten, Verkehrsdaten und Inhaltsdaten vom Diensteanbieter verwendet werden dürfen. *Kassai* führt aus, dass aus diesen Gesetzesstellen folge, „*dass Stammdaten, Verkehrsdaten und Inhaltsdaten ohne Zustimmung verwendet werden dürfen, soweit dies zur Erbringung des Kommunikationsdienstes und damit zur Erfüllung des auf die Erbringung des Dienstes gerichteten Vertrages [...] notwendig ist.*“[127]

[127] *Kassai*, "Location Based Services" im Gefüge des Datenschutzrechts, MR 2004, 443.

4. Verfahren vor dem OGH bzw EuGH

Im Anschluss an das unter 2 dargestellte Verfahren erhob UPC Revisionsrekurs an den OGH mit dem Begehren, den Antrag der Klägerinnen auf Erlass der Sperrverfügung betreffend kino.to abzuweisen. Da nach Ansicht des OGHs im Bezug auf die unter 4.1 dargestellten Vorlagefragen Zweifel an der Auslegung des Unionsrechts bestanden, entschied er sich, obwohl dies im Verfahren zum einstweiligen Rechtsschutz nicht zwingen ist, den EuGH gemäß Art 267 AEUV anzurufen. Die Tatsache, dass zum Zeitpunkt der Erhebung des Revisionsrekurses kino.to längst offline war, war für den OGH unerheblich, da spätere Sachverhaltsänderungen im Revisionsrekursverfahren nicht zu berücksichtigen sind.[128] Diese Tatsache sprach auch nicht gegen eine Zulässigkeit der Anrufung des EuGH, da es alleine Sache des nationalen Gerichts ist, die Erforderlichkeit und Erheblichkeit der dem EuGH vorzulegenden Fragen für das nationale Verfahren zu beurteilen.[129]

4.1. Vorlagefragen

Mit Beschluss vom 11.05.2012[130] legte der OGH dem EuGH vier Vorlagefragen vor:

1. *Ist Art 8 Abs 3 RL 2001/29/EG (Info-RL) dahin auszulegen, dass eine Person, die ohne Zustimmung des Rechteinhabers Schutzgegenstände im Internet zugänglich macht (Art 3 Abs 2 Info-RL), die Dienste der Access-Provider jener Personen nutzt, die auf diese Schutzgegenstände zugreifen?*

2. *Wenn Frage 1 verneint wird:*
   Sind eine Vervielfältigung zum privaten Gebrauch (Art 5 Abs 2 lit b Info-RL) und eine flüchtige und begleitende Vervielfältigung (Art 5 Abs 1 Info-RL) nur dann zulässig, wenn die Vorlage der Vervielfältigung rechtmäßig vervielfältigt, verbreitet oder öffentlich zugänglich gemacht wurde?

3. *Wenn Frage 1 oder Frage 2 bejaht wird und daher gegen den Access-Provider des Nutzers gerichtliche Anordnungen nach Art 8 Abs 3 Info-RL zu erlassen sind:*
   Ist es mit dem Unionsrecht, insbesondere mit der danach erforderlichen Abwägung zwischen den Grundrechten der Beteiligten, vereinbar, einem Access-Provider ganz allgemein (also ohne Anordnung konkreter Maßnahmen) zu verbieten, seinen Kunden

[128] OGH 11.05.2012, 4 Ob 6/12d.
[129] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien), Rz 19.
[130] OGH 11.05.2012, 4 Ob 6/12d.

den Zugang zu einer bestimmten Website zu ermöglichen, solange dort ausschließlich oder doch weit überwiegend Inhalte ohne Zustimmung der Rechteinhaber zugänglich gemacht werden, wenn der Access-Provider Beugestrafen wegen Verletzung dieses Verbots durch den Nachweis abwenden kann, dass er ohnehin alle zumutbaren Maßnahmen gesetzt hat?

4. *Wenn Frage 3 verneint wird:*
   Ist es mit dem Unionsrecht, insbesondere mit der danach erforderlichen Abwägung zwischen den Grundrechten der Beteiligten, vereinbar, einem Access-Provider bestimmte Maßnahmen aufzutragen, um seinen Kunden den Zugang zu einer Website mit einem rechtswidrig zugänglich gemachten Inhalt zu erschweren, wenn diese Maßnahmen einen nicht unbeträchtlichen Aufwand erfordern, aber auch ohne besondere technische Kenntnisse leicht umgangen werden können?

4.2. EuGH Entscheidung

Im Folgenden soll das EuGH-Urteil C-314/12 [131] einschließlich der Anträge des Generalanwalts dargestellt werden. Einleitend ist anzumerken, dass sich die Beantwortung der Vorlagefragen grundsätzlich in zwei Themenkomplexe[132] gliedern lässt:

Einerseits die Problematik, ob ein Access-Provider als Vermittler im Sinne Art 8 Abs 3 Informationsgesellschaftsrichtlinie anzusehen ist und ein Rechtsverletzer dessen Dienste nutzt, wenn die Kunden des Access-Providers die Möglichkeit haben, über das Netz des Access-Providers auf die rechtsverletzenden Inhalte zuzugreifen.

Andererseits die Frage, ob es zulässig ist, allgemeine Sperranordnungen ohne das Vorschreiben konkreter Maßnahmen zu erlassen bzw wenn dies nicht der Fall ist, ob zumindest Sperranordnungen, welche die vorzunehmenden Maßnahmen spezifizieren, mit dem Unionsrecht vereinbar sind.

[131] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien).

[132] Der Themenkomplex der zweiten Frage nach der Rechtmäßigkeit der Vervielfältigung zum privaten Gebrauch und flüchtiger bzw beiläufiger Vervielfältigungen aus rechtswidriger Quelle im Zuge von Internetvideostreaming blieb in der gegenständlichen Entscheidung aufgrund der positiven Beantwortung der ersten Frage unbeantwortet. Im Rahmen der Entscheidung ACI Adam u.a. stellte der EuGH klar, dass eine Vervielfältigung zum privaten Gebrauch nur von einer rechtmäßige Quelle vorgenommen werden kann, auf die Problematik in Bezug auf Internetstreaming ging der EuGH bisher nicht näher ein.

4.2.1. Access-Provider als Vermittler

„Frage 1: Ist Art 8 Abs 3 RL 2001/29/EG (Info-RL) dahin auszulegen, dass eine Person, die ohne Zustimmung des Rechteinhabers Schutzgegenstände im Internet zugänglich macht (Art 3 Abs 2 Info-RL), die Dienste der Access-Provider jener Personen nutzt, die auf diese Schutzgegenstände zugreifen?“

4.2.1.1. Erwägungen des Generalanwalts

Nach Ansicht des GA ergebe sich aus Wortlaut, Zusammenhang und Sinn und Zweck des Art 8 Informationsgesellschaftsrichtlinie, „*dass der Provider des Nutzers als Vermittler, dessen Dienste von einem Dritten zur Verletzung des Urheberrechts genutzt werden, anzusehen ist*“[133].

Es entspreche der ständigen Rechtsprechung des EuGH, „*dass ein Access-Provider, der den Nutzern nur den Zugang zum Internet verschafft, ohne weitere Dienste [...] anzubieten oder eine rechtliche oder faktische Kontrolle über den genutzten Dienst auszuüben, ‚Vermittler‘ im Sinne des Art. 8 Abs. 3 der Richtlinie 2001/29 ist*“[134].

Bereits im Rahmen der RS Scarlet Extended (siehe dazu 3.3.2) sei festgestellt worden, dass Inhaber geistiger Eigentumsrechte auch vorbeugend gerichtliche Anordnungen gegen Vermittler wie Access-Provider beantragen können[135].

In Bezug auf den Vorlagefall sei festzuhalten, dass Art 8 Abs 3 Informationsgesellschaftsrichtlinie nicht explizit nach einer vertraglichen Beziehung zwischen Vermittler und Rechtsverletzer verlange[136]. Von einer Nutzung der Dienste des Access-Providers durch den Rechtsverletzer könne immer dann die Rede sein, wenn dessen Kunden der Zugang zum Internet vermittelt werde. Schließlich seien die Dienste der Access-Provider essentiell, um von einer öffentlichen Zugänglichmachung iSd Art 3 Abs 2 Informationsgesellschaftsrichtlinie an die Mitglieder der Öffentlichkeit sprechen zu können, die Zugänglichmachung durch den Host-Provider des Rechtsverletzers sei nur notwendige Grundvoraussetzung[137].

ErwG 59 der Informationsgesellschaftsrichtlinie verdeutliche zudem, dass Vermittler „*bestmögliche Adressaten von Maßnahmen zum Abstellen von Urheberrechtsverletzungen*“

[133] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 36.
[134] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 38 mwN.
[135] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 40 mwN.
[136] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 44.
[137] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 47.

seien, da sie die Daten in ihrem Netzwerk weiterleiten[138]. Oft seien Betreiber außereuropäischer Websites nicht belangbar, weswegen nur eine Anordnung an den Vermittler als Option verbleibe[139]. Ziel des Gesetzgebers sei es schließlich, eine „*rigorose und wirksame Regelung zum Schutz des Urheberrechts*" zu schaffen[140]. Dem würden auch die Haftungserleichterung der E-Commerce Richtlinie nicht entgegenstehen, da Art 12 Abs 3 leg.cit. die Möglichkeit gerichtlicher Anordnungen unberührt lasse[141].

Freilich sei es offensichtlich, dass der mit dem Rechtsverletzer in keiner vertraglichen Beziehung stehende Access-Provider nicht bedingungslos für die Abstellung der Rechtsverletzung verantwortlich gemacht werden könne, worauf jedoch mit den in den Beantwortungen der Fragen drei und vier aufgestellten Bedingungen Rücksicht genommen werde[142].

Der Generalanwalt schlug somit vor, auf Frage 1 zu antworten, „*dass eine Person, die ohne Zustimmung des Rechteinhabers Schutzgegenstände im Internet zugänglich macht und damit [Urheber-]Rechte [...] verletzt, die Dienste der Provider jener Personen nutzt, die auf diese Schutzgegenstände zugreifen*"[143].

4.2.1.2. Erkenntnis des EuGH

Der EuGH schließt sich mit seiner Beantwortung der ersten Frage vollinhaltlich den Ansichten des GA an:

„Art. 8 Abs. 3 der Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft ist dahin auszulegen, dass eine Person, die ohne Zustimmung des Rechtsinhabers Schutzgegenstände im Sinne von Art. 3 Abs. 2 dieser Richtlinie auf einer Website öffentlich zugänglich macht, die Dienste des als Vermittler im Sinne von Art. 8 Abs. 3 der Richtlinie anzusehenden Anbieters von Internetzugangsdiensten der auf diese Schutzgegenstände zugreifenden Personen nutzt." [144]

[138] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 50f.
[139] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 57.
[140] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 56.
[141] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 52.
[142] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 58.
[143] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 59.
[144] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien).

4.2.2. Sperren ohne Anordnung konkreter Maßnahmen

„Frage 3: Wenn Frage 1 oder Frage 2 bejaht wird und daher gegen den Access-Provider des Nutzers gerichtliche Anordnungen nach Art 8 Abs 3 Info-RL zu erlassen sind: Ist es mit dem Unionsrecht, insbesondere mit der danach erforderlichen Abwägung zwischen den Grundrechten der Beteiligten, vereinbar, einem Access-Provider ganz allgemein (also ohne Anordnung konkreter Maßnahmen) zu verbieten, seinen Kunden den Zugang zu einer bestimmten Website zu ermöglichen, solange dort ausschließlich oder doch weit überwiegend Inhalte ohne Zustimmung der Rechteinhaber zugänglich gemacht werden, wenn der Access-Provider Beugestrafen wegen Verletzung dieses Verbots durch den Nachweis abwenden kann, dass er ohnehin alle zumutbaren Maßnahmen gesetzt hat?“

4.2.2.1. Erwägungen des Generalanwalts

Der GA stellt gleich zu Anfang seiner rechtlichen Beurteilung klar, dass er ein allgemeines Erfolgsverbot ohne die Anordnung konkreter Maßnahmen für unionsrechtswidrig hält, auch wenn der Verpflichtete die Unzumutbarkeit der zur Erfüllung des Erfolgsverbots notwendigen Maßnahmen in einem späteren Vollstreckungsverfahren einwenden kann.[145]

Es stehe den Mitgliedsstaaten zwar frei, Bedingungen und Modalitäten des Erfolgsverbots nach ihrem nationalen Recht auszugestalten[146], sie seien dabei jedoch, wie sich u.a. aus den Urteilen Scarlet Extended[147] sowie SABAM[148] ergebe, den sich aus dem Unionsrecht, insbesondere der Charta der Grundrechte, der Informationsgesellschaftsrichtlinie und der Enforcementrichtlinie ergebenden Einschränkungen unterworfen[149].

In weiterer Folge prüft der GA diese Beschränkung des mitgliedsstaatlichen Ermessens anhand dreier Kriterien: die Auslegung der RL im Sinne einer effektiven Verfolgung ihrer Ziele, Art 15 Abs 1 der E-Commerce Richtlinie und der Grundrechte:

1) Effektiver Schutz des Urheberrechts

   Bei Auslegung der Informationsgesellschaftsrichtlinie müsse stets das Ziel eines effektiven Schutzes der Urheber beachtet werden. Außerdem sei Art 3 Enforcementrichtlinie maßgeblich.[150]

[145] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 71.
[146] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 72.
[147] EuGH 24.11.2011, C-70/10 (Scarlet Extended).
[148] EuGH 16.02.2012, C-360/10 (SABAM).
[149] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 73.
[150] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 75.

„(1) Die Mitgliedsstaaten sehen die Maßnahmen, Verfahren und Rechtsbehelfe vor, die zur Durchsetzung der Rechte des geistigen Eigentums, auf die diese Richtlinie abstellt, erforderlich sind. Diese Maßnahmen, Verfahren und Rechtsbehelfe müssen fair und gerecht sein, außerdem dürfen sie nicht unnötig kompliziert oder kostspielig sein und keine unangemessenen Fristen oder ungerechtfertigten Verzögerungen mit sich bringen.

(2) Diese Maßnahmen, Verfahren und Rechtsbehelfe müssen darüber hinaus wirksam, verhältnismäßig und abschreckend sein und so angewendet werden, dass die Einrichtung von Schranken für den rechtmäßigen Handel vermieden wird und die Gewähr gegen ihren Missbrauch gegeben ist.“[151]

Daraus folge nach Rechtsprechung des EuGH, dass es nicht nur Pflicht der Mitgliedsstaaten sei, Maßnahmen zur Beendigung begangener Verletzungen vorzusehen, sondern auch zu deren Prävention.[152] Dabei hätten Mitgliedsstaaten jedoch auch darauf zu achten, durch die Maßnahmen ein angemessenes Gleichgewicht zwischen den Interessen und Rechten der Beteiligen herzustellen.[153]

2) Allgemeine Überwachungsverpflichtungen

Art 15 Abs 1 der E-Commerce Richtlinie untersage es den Mitgliedsstaaten, Diensteanbietern allgemeine Überwachungsverpflichtungen aufzuerlegen oder aktive Forschung nach rechtswidrigen Tätigkeiten zu fordern. In diesem Sinne wäre es unzulässig, einem Access-Provider aufzutragen, nach Kopien der zu sperrenden Seite unter anderen Domainnamen zu suchen oder Daten im Hinblick darauf zu filtern, ob geschützte Filmwerke übertragen werden.[154]
Da eine solche Maßnahme im konkreten Anlassfall jedoch nicht gegenständlich ist, liege kein Verstoß gegen Art 15 Abs 1 E-Commerce Richtlinie vor.[155]

[151] Art 3 Enforcementrichtlinie
[152] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 75 mwN.
[153] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 76.
[154] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 77.
[155] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 78.

3) Grundrechte

Es liege jedoch ein Verstoß gegen die grundrechtlichen Anforderungen der Informationsgesellschaftsrichtlinie vor, die gegenständliche Maßnahme sei weder „fair und gerecht" noch „verhältnismäßig" iSd Art 3 Enforcementrichtlinie.[156]
Infolge der Bindung der Mitgliedsstaaten an die in Art 6 Abs 1 EUV garantierten Grundrechte der Grundrechtecharta [157] bei Vollzug des Unionsrechts seien die grundrechtlichen Schranken auch im Zusammenhang mit Art 8 Abs 3 Informationsgesellschaftsrichtlinie zu beachten.[158]

Laut Rechtsprechung des EuGH sei der von Art 17 Abs 2 Grundrechtecharta garantierte Schutz geistigen Eigentums beschränkt und an Bedingungen gebunden, er sei gegen den Schutz anderer Grundrechte abzuwägen, um ein angemessenes Gleichgewicht zwischen Rechteinhabern und von Sperren betroffenen Personen herzustellen.[159]

Vor allem in Hinblick auf die Informations- und Meinungsäußerungsfreiheit der Provider nach Art 11 Grundrechtecharta, welche sich dank ihrer Funktion, Meinungen und Informationen an ihre Kunden zu übermitteln, auf diese berufen könnten, sowie auf ihre unternehmerische Freiheit nach Art 16 Grundrechtecharta sei ein Erfolgsverbot ohne konkrete Angabe der zu treffenden Maßnahmen unverhältnismäßig.[160] Dies ergebe sich vor allem aus dem Umstand, dass die Eingriffsintensität der zur Verfügung stehenden Sperrmöglichkeiten, beispielsweise IP- und DNS-Sperren und auf der anderen Seite die Möglichkeit des Umleitens des gesamten Internetverkehrs über einen Proxy, aufgrund deren unterschiedlicher Komplexität divergiere, sowie überhaupt nicht feststehe, ob die vollständige Erfüllung des Erfolgsverbots überhaupt machbar sei.[161] Auch sei den Access-Providern nicht zuzumuten, die Abwägung der betroffenen Grundrechte selbst vorzunehmen. Würden sich diese nämlich im Sinne der Informationsfreiheit ihrer Kunden entscheiden, so würden sie sich der Gefahr von Beugestrafen ausgesetzt sehen. Würden sie

[156] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 79.
[157] Charta der Grundrechte der Europäischen Union, Abl C 326/12, 391.
[158] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 80.
[159] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 81.
[160] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 82 – Rz 85.
[161] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 86.

andererseits dem Schutzinteresse der Rechtsinhaber höheres Gewicht beimessen, so hätten sie eine Auseinandersetzung mit ihren Kunden zu fürchten.[162]

Die Möglichkeit nach österreichischem Recht im Rahmen der Exekution des Erfolgsverbots mittels Impugnationsklage geltend zu machen, alle zumutbaren Maßnahmen ergriffen zu haben, könne das Gleichgewicht der abzuwiegenden Grundrechte nachträglich nicht wiederherstellen. Dieses Gleichgewicht sei infolge Art 8 Abs 3 Informationsgesellschaftsrichtlinie bereits im Zeitpunkt der Verfügungserlassung zu gewährleisten. Schließlich müsse ansonsten der Access-Provider den Erlass einer Anordnung gegen sich erdulden, aus der nicht hervorgehe, welche konkreten Maßnahmen er zu ergreifen habe, was, wie soeben dargestellt, Abwägungsprobleme auf den Access-Provider überwälze.[163]

Es sei also auf die dritte Vorlagefrage zu antworten, dass es mit der erforderlichen Grundrechtsabwägung nicht vereinbar sei, Providern zu verbieten, ihren Kunden Zugang zu urheberrechtsverletzenden Websites zu gewähren, ohne die konkreten Sperrmaßnahmen zu spezifizieren.[164]

4.2.2.2. Erkenntnis des EuGH

Der EuGH weicht bei Beantwortung der dritten Frage vom Vorschlag des GA ab und entscheidet, dass die Anordnung von Maßnahmen ohne die Nennung konkreter Sperrmaßnahmen mit dem Unionsrecht vereinbar ist.

Eine Sperranordnung lege ihrem Adressaten einen Zwang auf, der die freie Nutzung seiner Ressourcen einschränke, da sie ihn verpflichte, eventuell mit hohen Kosten verbundene oder schwierige technische Lösungen erfordernde Sperrmaßnahmen umzusetzen. Dies stelle einen Eingriff in die in Art 16 Grundrechtecharta garantierte unternehmerische Freiheit dar.[165] Allerdings bleibe der Wesensgehalt des Rechts auf unternehmerische Freiheit unangetastet, die Anordnung überlasse es schließlich dem Verpflichteten, die konkrete Maßnahme zu bestimmen, die zur Zielerreichung notwendig ist. Der Verpflichtete könne sich somit für jene Maßnahmen entscheiden, die seinen Möglichkeiten und Ressourcen entsprechen und mit seinen übrigen Pflichten und Anforderungen vereinbar seien.[166] Auch sei es dem Adressaten

[162] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 89.
[163] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 87f.
[164] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 90.
[165] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien Rz 47ff.
[166] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 51f.

einer Sperranordnung möglich, sich durch Nachweis, alle notwendigen Maßnahmen ergriffen zu haben, von seiner Haftung zu befreien, er sei also, auch als Folge, dass nicht er derjenige sei, der die zur Anordnung führende Rechtsverletzung begangen habe, nicht verpflichtet, für ihn untragbare Opfer zu erbringen.[167] Es müsse dem Adressaten jedenfalls möglich sein, dies im Exekutionsverfahen vor Sanktionsverhängung einzuwenden.[168]

Unzweifelhaft habe der Verpflichtete bei Wahl der Maßnahme die Informationsfreiheit der Internetnutzer zu berücksichtigen. [169] Ein Eingriff in den Zugang zu rechtmäßigen Informationen habe zu unterbleiben.[170] Es sei notwendig, dass den nationalen Gerichten die Möglichkeit offenstehe, dies zu prüfen, auch wenn im Vollstreckungsverfahren keine derartige Einwendung erhoben werde. Die nationalen Verfahrensvorschriften müssten folglich vorsehen, dass Internetnutzer ihre Ansprüche geltend machen könnten, sobald die vom Verpflichteten vorgenommen Sperrmaßnahmen bekannt seien.[171]

Es bestünde die Möglichkeit, dass eine Sperrverfügung nicht zu einer vollständigen Beendigung der Rechtsverletzung führe.[172] Es sei nämlich nicht ausgeschlossen, dass schlicht keine technische Maßnahme zur vollständigen Beendigung der Rechtsverletzung existieren würde.[173] Dies sei jedoch nicht unvereinbar mit dem Erfordernis, gemäß Art 52 Abs 1 Grundrechtecharta ein angemessenes Gleichgewicht zwischen allen anwendbaren Grundrechten herzustellen.[174]

Der Verpflichtete habe bestimmte, möglicherweise durchführbare Maßnahmen nicht zu ergreifen, sofern sie als nicht zumutbar eingestuft werden könnten, er könne sich schließlich im Rahmen der Verhängung von Ordnungsstrafen freibeweisen, wenn alle zumutbaren Maßnahmen ergriffen worden seien.[175] Für diesen Aspekt spreche, dass sich aus Art 17 Abs 1 der Grundrechtecharta nicht ergebe, dass der Schutz geistigen Eigentums schrankenlos sei und daher bedingungslos zu gewähren sei.[176]

Jedenfalls müssten die Maßnahmen, die vom Verpflichteten ergriffen werden, hinreichend wirksam sein, um einen wirkungsvollen Schutz des geistigen Eigentums zu gewährleisten.

[167] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 53.
[168] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 54.
[169] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 55.
[170] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 56.
[171] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 57.
[172] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 58.
[173] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 60.
[174] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 63.
[175] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 59.
[176] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 61.

Unerlaubte Zugriffe auf Schutzgegenstände müssten folglich verhindert oder zumindest erschwert werden. Es müssten „*Internetnutzer, die die Dienste des Adressaten der Anordnung in Anspruch nehmen, zuverlässig davon abgehalten werden, auf die ihnen unter Verletzung des Rechts des geistigen Eigentums zugänglich gemachten Schutzgegenstände zuzugreifen*“[177].

4.2.3. Sperren mit Anordnung konkreter Maßnahmen

„Frage 4: Wenn Frage 3 verneint wird:
Ist es mit dem Unionsrecht, insbesondere mit der danach erforderlichen Abwägung zwischen den Grundrechten der Beteiligten, vereinbar, einem Access-Provider bestimmte Maßnahmen aufzutragen, um seinen Kunden den Zugang zu einer Website mit einem rechtswidrig zugänglich gemachten Inhalt zu erschweren, wenn diese Maßnahmen einen nicht unbeträchtlichen Aufwand erfordern, aber auch ohne besondere technische Kenntnisse leicht umgangen werden können?“

4.2.3.1. Erwägungen des Generalanwalts

Auch zur Beantwortung der vierten Vorlagefrage sei wiederum eine Grundrechtsabwägung zwischen dem Recht auf Eigentum der Urheberrechtsinhaber sowie der unternehmerischen Freiheit und Informations- und Meinungsfreiheit der Provider notwendig. Letztere würden insbesondere die Sperre von nicht rechtsverletzenden Informationen ausschließen.

Im Zuge der vorzunehmenden Verhältnismäßigkeitsprüfung seien insbesondere die den Providern durch Sperren entstehenden Kosten sowie die Möglichkeit, Sperren zu umgehen, miteinzubeziehen.[178] Es sei jedenfalls davon auszugehen, dass konkrete Sperrmaßnahmen einen Eingriff in den Schutzbereich der unternehmerischen Freiheit darstellen würden,[179] welcher jedoch angesichts des Wortlauts des Art 16 Grundrechtecharta nach Rechtsprechung des EuGH im allgemeinen Interesse Schranken unterworfen sei.[180]

Art 52 Abs 1 Grundrechtecharta erlege auf, bei Prüfung des Eingriffs unter anderem den Gesetzesvorbehalt und die Wahrung des Verhältnismäßigkeitsgrundsatzes zu beachten. Im gegenständlichen Fall sei es jedoch, vor allem auch aufgrund der Formulierung der Vorlagefrage, zweckdienlich, sich ausschließlich auf die Prüfung der Verhältnismäßigkeit zu beschränken.[181]

[177] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 62.
[178] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 94.
[179] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 95.
[180] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 96.
[181] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 97.

Nach ständiger Rechtsprechung des EuGH müsse ein Grundrechtseingriff geeignet und erforderlich sein, um das angestrebte Ziel zu erreichen. Von mehreren möglichen Maßnahmen sei stets das gelindeste zur Verfügung stehende Mittel zu wählen, verursachte Nachteile müssten in einem angemessenen Verhätnis zu den zu erreichenden Zielen stehen. Diese Voraussetzungen würden ihrem Wesen nach den Anforderungen entsprechen, welche in Art 52 Abs 1 Grundrechtecharta normiert seien.[182]

1) Geeignetheit

Sei auch das Ziel der in Frage stehenden Sperranordnungen ohne Zweifel zulässig, da damit „Rechte anderer" iSd Art 52 Abs 1 Grundrechtecharta, nämlich das Eigentumsrecht der Urheber, geschützt werden sollen, so stelle sich doch die Frage, ob Sperrmaßnahmen zur Zeilerreichung geeignet seien. Diese Zweifel würden sich darauf gründen, dass, wie auch der vorlegende OGH festgestellt habe, Sperrmaßnahmen ohne Fachwissen leicht umgangen werden könnten. Einerseits sei eine unkomplizierte Umgehung seitens der Internetbenutzer möglich, andererseits würden auch die Seitenbetreiber infolge der Änderung von IP-Adresse und/oder Domainname die Möglichkeit haben, die Sperren auszuhebeln.[183]

Aus der bloßen Umgehungsmöglichkeit der Internetnutzer folge jedoch nicht, dass diese Möglichkeit auch von jedem wahrgenommen werden würde. Es wäre schließlich möglich, dass Nutzer wegen der Sperre von der Rechtswidrigkeit einer Seite erfahren und somit auf deren Nutzung verzichten würden. Es könne schließlich nicht davon ausgegangen werden, dass bei jedem Nutzer der Wille zur Förderung eines Rechtsbruchs vorliege.[184]

Auch die Änderung der IP-Adresse bzw des Domainnamens durch den Betreiber einer urheberrechtsverletzenden Seite würde dem angesprochenen Effekt der Publizität des Rechtsbruchs nicht schaden. Es wäre schließlich für den neuerlichen Aufruf der Seite notwendig, eine Suchmaschine zu benutzen um den neuen Domainnamen überhaupt zu finden. Wiederholte Sperrmaßnahmen hätten außerdem den Effekt, eine Suche über Suchmaschinen zu erschweren.[185]

[182] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 98.
[183] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 99.
[184] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 100.
[185] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 101.

Eine Sperrverfügung unter Nennung konkreter Maßnahmen sei folglich nicht generell ungeeignet, das Schutzziel zu erreichen.[186]

2) Erforderlichkeit und Angemessenheit

Aufgrund der Natur des Zusammenwirkens nationaler Rechtsprechung und EuGH-Judikatur und weil der Sachverhalt der vorgelegten Rechtssache nicht vollumfänglich geklärt sei sowie Angaben hinsichtlich konkreter Maßnahmen fehlen würden, sei nicht eine vollständige Prüfung der Angemessenheit und Erforderlichkeit durchzuführen, sondern seien lediglich Gesichtspunkte zu erörtern, die das nationale Gericht bei seiner Entscheidung zu berücksichtigen habe.[187]

Maßstab bei der Beurteilung einer Maßnahme seien nach Rechtsprechung des EuGH Komplexität, Kosten und Dauer. Es sei zu berücksichtigen, dass in weiterer Folge erneut Sperranforderungen an die Beklagte herangetragen werden würden, der gegenständliche Fall also gleichsam als Präzedenzfall herangezogen werden würde. Sollte sich daraus ergeben, dass eine Maßnahme nach den soeben genannten Kriterien unverhältnismäßig sei, sei zu prüfen ob eine teilweise oder vollständige Kostenübernahme durch die Rechteinhaber zur Herstellung der Verhältnismäßigkeit geeignet sei.[188]

Unzweifelhaft sei, dass Rechteinhaber gegenüber rechtsverletzenden Websites nicht schutzlos gestellt sein dürften, jedoch sei abzuwägen, dass die Access-Provider als Adressaten der Sperraufforderung keinerlei Rechtsbeziehung zum Rechtsverletzer hätten. Die Inanspruchnahme der Access-Provider sei also nicht gänzlich ausgeschlossen, vorrangig sollten Rechteinhaber jedoch Betreiber und Provider rechtsverletzender Seiten in Anspruch nehmen.[189]

Aus Art 16 der Grundrechtecharta resultiere jedenfalls, dass durch Sperrmaßnahmen die unternehmerische Tätigkeit der Access-Provider an sich nicht in Frage gestellt

[186] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 102.
[187] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 104.
[188] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 106.
[189] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 107.

werden dürfe. Schließlich käme den Access-Providern erhebliche gesellschaftliche Bedeutung zu, da diese den Zugang zu Information als wesentlichen Bestandteil einer demokratischen Gesellschaft erst ermöglichen würden. Der EGMR habe insoweit festgestellt, dass im Rahmen einer rechtsvergleichenden Studie in 20 Mitgliedsstaaten des Europarats[190] offensichtlich wurde, dass das Recht auf einen Internetzugang theoretisch von der verfassungsrechtlichen Garantie der Meinungs- und Informationsfreiheit umfasst sei.[191]

Folglich sei auf die vierte Vorlagefrage zu antworten, dass eine konkrete Sperrmaßnahme nicht deswegen prinzipiell unverhältnismäßig sei, weil sie einen beträchtlichen Aufwand erfordere, aber leicht zu umgehen sei. Die nationalen Gerichte hätten im jeweils konkreten Fall eine Abwägung zwischen den Grundrechten der Beteiligten vorzunehmen um ein angemessenes Gleichgewicht zwischen diesen Grundrechten herzustellen.[192]

4.2.3.2. Erkenntnis des EuGH

Angesichts der Antwort des Gerichtshofs auf die dritte Frage unterblieb die Beantwortung der vierten Frage.

[190] OSCE, Freedom of Expression on the Internet.
[191] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 108 mwN.
[192] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 109.

4.3. OGH Beschluss[193]

4.3.1. Vorbemerkungen

Im Zuge der Vorabentscheidung entschied der OGH im Verfahren 4 Ob 71/14s, dass der Revisionsrekurs nicht berechtigt sei, die Sperrverfügung gegen die Beklagte also aufrecht bleibt.

Im Rahmen des Verfahrens äußerten sich sowohl die Klägerinnen als auch die Beklagte zur Entscheidung des EuGH:

Die Beklagte brachte vor, aufgrund der Vorabentscheidung stehe fest, dass die österreichische Rechtslage ein Erfolgsverbot ausschließe. Dies folge daraus, dass die Unzumutbarkeit weiterer Maßnahmen erst nach Verhängung von Beugestrafen in einem Impugnationsprozess geltend gemacht werden könne. Außerdem hätten die Kunden UPCs keine realistische Möglichkeit, gerichtlich gegen bekannt gewordene Sperrmaßnahmen vorzugehen.

Die Klägerinnen entgegneten, eine Impugnationsklage gemeinsam mit einem Aufschiebungsantrag garantiere ausreichenden Rechtsschutz. Auch eine Erhebung von Einwänden im Exekutionsbewilligungsverfahren analog § 358 Abs 2 EO sei denkbar. Den Kunden stehe die Geltendmachung ihrer Ansprüche auf vertraglicher Grundlage offen.

Der OGH erörterte, dass es auf die Frage, ob eine flüchtige Vervielfältigung der rechtsverletzenden Inhalte durch die Kunden des Access-Providers rechtswidrig sei, nicht ankomme. Gemäß der Beantwortung des EuGH nutze der Rechtsverletzer die Dienste der Access-Provider jener Personen, welche das rechtswidrige Angebot aufrufen (siehe dazu 4.2.1). Es bestünde auch keine Problematik hinsichtlich des Grundrechts auf Informationsfreiheit, da bescheinigt worden sei, dass auf kino.to ausschließlich rechtswidrige Inhalte online seien – rechtmäßige Inhalte seien somit nicht von einer Sperre betroffen. Folglich stehe den Klägerinnen der Unterlassungsanspruch nach § 81 Abs 1 a UrhG vollumfänglich zu.

4.3.2. Sperrverfügung als reines Erfolgsverbot

Da der Unterlassungsanspruch auf Unterlassung der Mitwirkung an einem Eingriff in ein absolut geschütztes Recht gerichtet sei, seien nach geltendem Recht keine konkreten Maßnahmen vorzuschreiben, es genüge ein reines Erfüllungsverbot.

[193] OGH 24.06.2014, 4 Ob 71/14s. Da das OGH Urteil keine Randzahlen enthält, unterbleibt im folgenden Abschnitt die Setzung von Fußnoten. Der gesamte Inhalt des folgenden Abschnitts ist dem Urteil 4 Ob 71/14s entnommen.

Dies folge einerseits aus einer Analogie zu nachbarrechtlichen Ansprüchen. Im Nachbarrecht sei es unstrittig, dass der Kläger nur das Abwehrrecht habe, dem Beklagten den Eingriff an sich zu untersagen, die Wahl der Mittel obliege jedoch dem Beklagten. Diesem sei es dadurch möglich, die für ihn günstigste noch zum Ziel führende Maßnahme zu ergreifen. Freilich handle der Beklagte dabei auf sein eigenes Risiko, da er sich bei ungeeigneten Maßnahmen dem Risiko von Beugestrafen gem § 355 EO ausgesetzt sehe. Jedoch könne er so auf veränderte Umstände flexibel reagieren, was gerade bei zeitlich unbefristeten Anordnungen vorteilhaft sei.
Andererseits ließe sich auch aus § 81 Abs 1a UrhG kein Anspruch auf bestimmte Maßnahmen ableiten. Auch die unternehmerische Freiheit des Access-Providers spreche dafür, ihn selbst die zu ergreifenden Maßnahmen bestimmen zu lassen.

4.3.3. Unionsrechtskonforme Ausgestaltung des Exekutionsverfahrens

Im Hinblick auf eine unionsrechtskonforme Auslegung des österreichischen Exekutionsverfahrens referiert der OGH mehrere alternative Möglichkeiten und entscheidet sich schließlich für die Option, „*die Behauptung des Titelverstoßes im Verfahren über den Exekutions- oder Strafantrag ausreichen zu lassen und das dem Antrag zugrunde liegende Verhalten erst im Impugnationsprozess zu prüfen*“.

Dabei sei eine unionsrechtskonforme Auslegung der Regelung über die Aufschiebung der Exekution notwendig. Auch eine Unterlassungsexekution kenne die Aufschiebung der Exekution aufgrund einer Impugnationsklage gemäß § 42 Abs 1 Z 5 EO. Allerdings erfordere diese nach § 44 Abs 1 EO, dass einerseits das Festhalten an der Exekution trotz der Möglichkeit der Rückzahlung von Geldstrafen mit erheblichen Nachteilen verbunden sei und andererseits die Klagsführung nicht mit hoher Wahrscheinlichkeit aussichtslos sei.

Um dem Erfordernis einer Prüfung der vom Verpflichteten getroffenen Maßnahmen vor der Entscheidung über eine Geldstrafe, worunter auch bloß eine Entscheidung vor dem exekutiven Einbringen einer Forderung verstanden werden könne, beizukommen, könne infolge unionsrechtskonformer Auslegung auf diese beide Voraussetzungen verzichtet werden. Die Verhängung der Geldstrafe werde damit nämlich nur zu einem Zwischenschritt im Zuge der Durchsetzung der materiell-rechtlichen Sperrverpflichtung. Damit würde die mit einer zwingenden Aufschiebung verbundene Impugnationsklage zu der vom EuGH geforderten Möglichkeit des Providers, vor Sanktionsverhängung geltend zu machen, alle zumutbaren Maßnahmen ergriffen zu haben.

Als Folge dieser Lösung stünde der Provider nicht schlechter dar, als wenn dies bereits im Exekutionsverfahren selbst geprüft würde – in beiden Fällen könne er schließlich eine inhaltliche Prüfung vor Wirksamkeit der Sanktion anstoßen. Der konkrete Zeitpunkt der Verhängung der Strafe sei unter diesen Voraussetzungen eine schlichte Formalität. Die Notwendigkeit der Erhebung einer Impugnationsklage sei unionsrechtlich unbedenklich, da der EuGH keine amtswegige Prüfung der vorgenommenen Sperrmaßnahmen verlangt habe. Schließlich spreche für die Impugnationsklage mit zwingend aufschiebender Wirkung auch, dass diese weit weniger als eine Prüfung im Exekutionsverfahren in das österreichische System der Zwangsvollstreckung eingreife, da die Trennung zwischen Exekutions- und Impugnationsverfahren erhalten bleibe.

4.3.4. Klagemöglichkeit der Kunden

Die Möglichkeit der Kunden des Access-Providers, ihr Recht auf Zugang zu Informationen gerichtlich geltend zu machen, sobald die infolge eines Erfolgsverbots getroffenen Maßnahmen bekannt seien, sei in Österreich bereits gegeben. Es bestünde die Möglichkeit der Kunden, ihren Provider auf vertraglicher Grundlage zu klagen, wenn sie von ihrer Meinung nach überschießenden oder unrechtmäßigen Sperrmaßnahmen betroffen seien. Denn der Vertrag zwischen Providern und Kunden sei dahingehend auszulegen, dass nur vom EuGH-Entscheid gedeckte Sperrmaßnahmen zulässig seien. Diese Klagsmöglichkeit genüge den Vorgaben des EuGH.

Um widersprechende Entscheidungen zu vermeiden, habe der Provider im Falle einer Klage dem die Sperre veranlassenden Rechteinhaber den Streit zu verkünden.

Außerdem stehe es den Kunden zu, auch direkt den die Sperre veranlassenden Rechteinhaber nach Einleitung des Exekutionsverfahrens mittels Exszindierungsklage in Anspruch zu nehmen, wenn dieser durch die erwirkte Sperre mittelbar ihr Recht auf freien Informationszugang verletze. Denn es genüge, wenn der Rechteinhaber ein Verhalten des Providers erzwingen wolle, welches mittelbar in ein absolut geschütztes Rechtsgut eines Dritten eingreife, wenn dieser den Eingriff nicht aufgrund besonderer Rechtsbeziehung zum Rechteinhaber dulden müsse, was bei einem Eingriff in den freien Informationszugang erfüllt sei.

Es sei zwar als gegeben anzusehen, dass faktisch nur wenige Nutzer Klage erheben würden, um eine Sperre zu bekämpfen, allerdings seien die Vorgaben des EuGH durch die bloße Möglichkeit einer Rechtsdurchsetzung bereits erfüllt. In Fällen wie dem gegenständlichen

könne ohnehin davon ausgegangen werden, dass Nutzer keine gerichtliche Auseinandersetzung anstreben würden, weil bereits beim Download, außer eventuell im Falle des Streamings, jedenfalls eine rechtswidrige Handlung des Nutzers vorliege. Bei unklaren Sachverhalten hingegen habe alleine schon die Möglichkeit einer gerichtlichen Auseinandersetzung den Effekt, dass Rechteinhaber wie Provider bei Sperrforderungen eine bedachte Handlungsweise an den Tag legen würden.

4.4. Auswirkungen: Sperren bei A1, UPC, Drei und Tele2

Infolge der soeben behandelten OGH-Entscheidung erging Anfang Oktober 2013 auf Antrag des VAP eine einstweilige Verfügung des Handelsgerichts Wien gegen die Access-Provider A1, UPC, Drei und Tele2 zur Sperre der Seiten kinox.to und movie4k.to, welcher die genannten Provider in Form einer DNS-Sperre entsprachen.[194]

Als Reaktion auf die Sperre richteten die Betreiber beider betroffener Seiten alternative Domains und IP-Adressen ein, über welche die Seiten weiterhin zugänglich sind. Das vom Verband der österreichischen Musikwirtschaft (IFPI) angestrengte Verfahren zur Sperre der Seiten isohunt.to, 1337x.to und h33t.to ist im Moment gerade anhängig.[195]

Obwohl eine Sperre von piratebay.se in der außergerichtlichen Aufforderung des VAP an die genannten Provider noch enthalten war, nahm der VAP von einer gerichtlichen Durchsetzung dieser Sperre Abstand.[196] Es liegt die Vermutung nahe, dass dies aus den unter 5.4.3 erörterten Gründen geschehen ist.

4.5. Kritische Betrachtung

4.5.1. Access-Provider als Adressaten der Sperrverfügungen

Die Entscheidung, dass Access-Provider als Vermittler iSd Art 8 Informationsgesellschaftsrichtlinie anzusehen sind, führt dazu, dass entgegen der bisherigen österreichischen Judikatur[197] eine bloß adäquate Verursachung einer Rechtsverletzung in Form der Zugangsvermittlung ausreicht, um Access-Provider auf Unterlassung nach § 81 Abs 1a UrhG in Anspruch nehmen zu können.[198]

[194] http://derstandard.at/2000006347840/Provider-muessen-unverzueglich-Piratenseiten-kinoxto-und-movie4-sperren.
[195] http://derstandard.at/2000006365884/Netzsperren-Ab-sofort-im-Einsatz-aber-leicht-zu-umgehen.
[196] http://derstandard.at/2000006365884/Netzsperren-Ab-sofort-im-Einsatz-aber-leicht-zu-umgehen.
[197] RIS-Justiz RS0026577.
[198] *Beimrohr*, Internetsperren zur Durchsetzung des Urheberrechts – Die Entscheidung des EuGH zum Fall UPC Telekabel Wien/kino.to, jusIT 2014, 83.

Die Entscheidung des EuGH geht über den Wortlaut des Art 8 Abs 3 Informationsgesellschaftsrichtlinie hinaus, da der Beweis, dass Kunden der Access-Provider tatsächlich auf die rechtsverletzenden Dienste zugreifen, zugunsten der Gewährung eines hohen Schutzniveaus nicht erbracht werden muss.[199] Es sollen nämlich nicht nur Verstöße abgestellt, sondern auch zukünftigen Verstößen vorgebeugt werden. Infolgedessen sieht sich de facto jeder Access-Provider der Möglichkeit ausgesetzt, zahlreiche Seiten sperren zu müssen, auch wenn dessen Kunden diese gar nicht nutzen.

Den Rechteinhabern wird es ermöglicht, den einfachen Weg der Zensur über die Access-Provider zu gehen.[200] Dies ist zwar sicherlich im Sinne eines effektiven Rechtsschutzes zu rechtfertigen[201], schließlich sind sowohl Betreiber und Hoster rechtsverletzender Seiten meist in Drittländern und deswegen nur schwer greifbar, jedoch stellt sich die Frage, ob ein effektiver Rechtsschutz auf Grundlage der technischen Möglichkeiten überhaupt gewährleistet werden kann (siehe dazu weiterführend unter 7).

4.5.2. Ausschließlich rechtsverletzende Seiten als Gegenstand von Sperren?

Sehr zu begrüßen ist mE die Rechtsansicht des OGH, dass zum Erlass einer Sperrverfügung zu bescheinigen ist, dass die Inhalte der zu sperrenden Seite ausschließlich oder weit überwiegend rechtsverletzend sind. Problematisch in diesem Zusammenhang erscheint jedoch, dass dieses Erfordernis im Rahmen des Vorabentscheidungsverfahrens vom EuGH nicht ausdrücklich betont wurde, wie *Zankl*[202] vor Augen führt. *Zankl* führt darüber hinaus aus, dass sich, auch wenn das Kriterium der ausschließlich oder weit überwiegend rechtsverletzenden Inhalte vorausgesetzt werde, erhebliche Abgrenzungsprobleme ergeben könnten, da nicht feststehe, wie zu überprüfen sei, ob die Inhalte diesem Kriterium entsprechen oder nicht. Auch ich schließe mich dieser Ansicht an. Gerade in Bezug auf Seiten wie Pirate Bay (siehe dazu unter 5.4.3) oder Foren wie boerse.bz (siehe dazu unter 5.3.3) wird eine Analyse des gesamten Inhalts ohne vollständigen Zugriff auf die zugrunde liegenden Datenbanken nicht abschließend vorgenommen werden können.

---

[199] *Beimrohr*, Internetsperren zur Durchsetzung des Urheberrechts – Die Entscheidung des EuGH zum Fall UPC Telekabel Wien/kino.to, jusIT 2014, 83.

[200] zu dieser Tatsache ebenfalls kritisch: *Zankl*, EuGH für Datenzugangssperre und gegen Datenvorratsspeicherung, ecolex 2014, 576; diesen Umstand ausdrücklich befürwortend: *Kraft*, Zugangssperren zu Webseiten als Mittel der Rechtsdurchsetzung, MR 2014, 171.

[201] *Walter*, Umfang der Unterlassungspflichten von Vermittlern – Access-Provider – kino.to, MR 2014, 82 und *Kraft*, Zugangssperren zu Webseiten als Mittel der Rechtsdurchsetzung, MR 2014, 171 vertreten die Ansicht, dass die Inanspruchnahme der Access-Provider notwendig und gerechtfertigt sei, da sie Zwingen an jeder Übertragung einer Rechtsverletzung beteiligt seien.

[202] *Zankl*, EuGH für Datenzugangssperre und gegen Datenvorratsspeicherung, ecolex 2014, 576.

4.5.3. Anordnung eines reinen Erfolgsverbots

Raum für Kritik schafft mE die Entscheidung des EuGH, Sperren ohne die Anordnung konkreter Maßnahmen zuzulassen[203]. Schon der Generalanwalt hat gegen ein solches Vorgehen gewichtige Gründe vorgebracht[204], insbesondere das Argument, dass die zur Verfügung stehenden Sperrmaßnahmen in ihrer Eingriffsintensität derart divergieren, dass es nicht gerechtfertigt ist, die Abwägung, welche Maßnahmen zu ergreifen sind, dem Access-Provider zu überbürden, der dadurch nicht nur die Gefahr trägt, Beugestrafen im Rahmen der Exekution durch die Rechteinhaber hinnehmen zu müssen[205], sondern sich auch dem Risiko ausgesetzt sieht, von seinen Kunden in Anspruch genommen zu werden (siehe dazu näher unter 4.2.2.1).

In diesem Sinne ist auch die Entscheidung des OGH zu kritisieren, wäre es diesem doch freigestanden, dennoch die Anordnung konkreter Maßnahmen vorzusehen, schließlich folgt mE im Größenschluss, dass konkrete Maßnahmen jedenfalls das gelindere Mittel gegenüber einem reinen Erfolgsverbot darstellen. Das Argument des OGH, durch das Auftragen konkreter Maßnahmen würde die unternehmerische Freiheit mehr beschnitten als durch ein Erfolgsverbot mag zwar auf den ersten Blick einleuchten. Aus Perspektive der Access-Provider entsteht jedoch durch Erlassung eines Erfolgsverbots jedenfalls eine erhebliche Rechtsunsicherheit in Bezug auf die zu ergreifenden Maßnahmen, wie auch *Beimrohr* ausführt.[206] Dass der weitere Gestaltungsspielraum im Bezug auf die Sperrmaßnahmen diese Rechtsunsicherheit aus Perspektive der Provider aufwiegt, scheint mE fraglich.

Die Analogie des OGH zu nachbarrechtlichen Unterlassungsansprüchen mag zwar rechtlich vertretbar sein, der OGH zieht diese Analogie jedoch auf der Grundlage, dass genauso wie bei nachbarrechtlichen Ansprüchen der „*Unterlassungsanspruch [nach § 81 Abs 1a UrhG] [...] auf Unterlassung der Mitwirkung an einem Eingriff in ein* ***absolut geschütztes Recht***[207]

[203] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 64.
[204] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 71ff.
[205] Außerdem trägt der Access-Provider im Rahmen eines etwaigen Impugnationsverfahrens das volle Prozesskostenrisiko. Um zu beweisen, dass er alle zumutbaren Maßnahmen ergriffen hat, wird der Access-Provider in der Regel zumindest ein Sachverständigengutachten beibringen müssen.
[206] *Beimrohr*, Internetsperren zur Durchsetzung des Urheberrechts – Die Entscheidung des EuGH zum Fall UPC Telekabel Wien/kino.to, jusIT 2014, 83.
[207] Interessant ist, wie leichtfertig der OGH von einem „absolut geschützten Rechtsgut“ spricht. Absolut geschützt sind lediglich die Menschenwürde (Art 3 EMRK), das Sklavereiverbot (Art 4 EMRK) und Nulla Poena sine lege (Art 7 EMRK). Nur im Bezug auf diese Grundrechte ist eine Gewichtung gegenläufiger Interessen ausgeschlossen. (siehe dazu *Öhlinger*, Verfassungsrecht[10] bei den jeweiligen Grundrechten) In Bezug auf alle anderen Grundrechte erfolgt diese Abwägung, weswegen diese Rechte eben nicht „absolut“ geschützt sind.

[Hervorhebung nicht im ursprünglichen Urteil, Anm.] gerichtet [ist]", weswegen sich kein Anspruch auf konkrete Maßnahmen ergebe.[208]

Nach mE ist jedoch der Schutz geistigen Eigentums weit weniger gewährt, als der Schutz des Eigentums, weswegen der Vergleich mit dem Nachbarrecht verfehlt ist. Im Falle von Immissionen im nachbarschaftlichen Rechtsverhältnis können die in Anspruch genommenen Eigentümer diese in der Regel unzweifelhaft vollständig abstellen. Natürlich erkennt der OGH das Faktum an, dass ein vollständiges Abstellen der Rechtsverletzungen durch Internetsperren womöglich nicht machbar ist, schließlich müssen von Access-Providern nur die für diese zumutbaren Maßnahmen ergriffen werden. Auch der EuGH erkennt dies an, wenn er davon spricht, dass die Möglichkeit einer Umgehung nichts an der Wirksamkeit einer Anordnung ändert[209]. Die Überbürdung der Wahl der Maßnahmen auf den Access-Provider scheint mE aber gerade aufgrund dieser Tatsache nicht sachgerecht: Der Nachbar, welcher die Immissionen abstellt, kann sich sicher sein, keine Beugestrafen erdulden zu müssen – er hat es in der Regel selbst in der Hand, den Eingriff abzustellen. Dem gegenüber ist es für den Access-Provider von vornherein nicht beherrschbar, die Störung vollständig abzustellen. Selbst wenn er die seiner Meinung nach zumutbaren Maßnahmen ergreift, sieht er sich dennoch der Gefahr von Beugestrafen weiterhin ausgesetzt, sollte das Gericht zu einem anderen Abwägungsergebnis kommen. Auch die Formulierung des EuGH, der Access-Provider müsse bei Wahl der zu ergreifenden Maßnahme keine „*untragbaren Opfer*"[210] hinnehmen gemeinsam mit der Tatsache, dass die gerichtliche Grundrechtsabwägung erst im Rahmen der Exekution stattfindet, tragen nicht zur Rechtssicherheit der Access-Provider bei und schieben die äußert komplexe Abwägung der möglichen Maßnahmen, welche eigentlich die Höchstgerichte vorzunehmen hätten, vorerst auf Access-Provider ab.

4.5.4. Rechtsschutzmöglichkeiten der betroffenen Nutzer

Nicht zuletzt scheint auch die Umsetzung des Gebots, Nutzern einen effektiven Weg zu bieten, gegen Sperren vorzugehen, in meinen Augen nur sehr schwach ausgeprägt.

Einerseits ist zu beachten, dass die Inanspruchnahme eines Access-Providers ausschließlich demjenigen zusteht, der eine vertragliche Beziehung zu ihm hat. An dieser Voraussetzung könnten schon viele Betroffene scheitern, sind doch auch zB Nutzer freier WLANs von Sperren betroffen, obwohl diese keinerlei Vertragsbeziehung zum Provider haben. Auch in

[208] OGH 24.06.2014, 4 Ob 71/14s.
[209] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 60f.
[210] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 53.

Wohngemeinschaften, welche sich einen Internetanschluss teilen, der möglicherweise sogar auf den Namen des Vermieters läuft, oder bei der privaten Internetnutzung am Dienstort sind die Nutzer de facto von einer klagsweisen Geltendmachung gegen den Access-Provider ausgeschlossen.

Natürlich besteht neben der Inanspruchnahme aus Vertrag noch das Instrument der Exszindierungsklage gegen den exekutionsführenden Rechteinhaber. Ob viele Betroffene von dieser Möglichkeit (und der Möglichkeit einer Klage gegen den Access-Provider) Gebrauch machen werden, ist jedoch stark zu bezweifeln, da, wie der OGH treffend ausführt, „*ohnehin kaum ein Nutzer an einer gerichtlichen Auseinandersetzung mit seinem Provider oder einem Rechteinhaber interessiert sein [wird]; dies schon deswegen, weil auch er beim Download – abgesehen möglicherweise von einer bloß flüchtigen Vervielfältigung (Streaming) – rechtswidrig handelt*". Der Aspekt, dass sich auch Nutzer einem solchen Vorwurf ausgesetzt sehen, die nur auf legale Inhalte auf einer gesperrten Seite zugreifen wollen, bzw die Rechtsunsicherheit in Bezug auf Streaming (siehe dazu weiterführend unter 5.2.3) wird dazu beitragen, die Arbeitsbelastung der Gerichte in derartigen Angelegenheiten gering zu halten.

Ein weiterer Aspekt, der derlei Klagen gering halten könnte, ist, wie *Beimrohr*[211] ausführt, die möglicherweise mangelnde Publizität von Sperren. Zwar kann diese mE in Bezug auf die aktuellen Sperren von kinox.to und movie4k.to aufgrund der ausführlichen Berichterstattung nur schwer argumentiert werden, wenn Sperren in Zukunft jedoch zur Regel werden, könnten diese auch an der öffentlichen Aufmerksamkeit vorbeigehen, in dem Sinne, dass Benutzer bei gesperrten Seiten davon ausgehen, dass diese aufgrund eines technischen Fehlers nicht erreichbar sind bzw nicht mehr existieren. Wie *Beimrohr* ausführt, besteht nämlich keinerlei Rechtsgrundlage, die es den Gerichten ermöglichen würde anzuordnen, im Falle einer Sperre bei Aufruf der gesperrten Adresse einen Hinweis auf die Sperre anzuzeigen.[212]

[211] *Beimrohr*, Internetsperren zur Durchsetzung des Urheberrechts – Die Entscheidung des EuGH zum Fall UPC Telekabel Wien/kino.to, jusIT 2014, 83.

[212] Die derzeit aktiven Sperren gegen kinox.to werden in diesem Hinblick je nach Provider unterschiedlich behandelt: Während UPC schlicht zurückliefert, dass die gesperrte Seite nicht existiert, der Benutzer also nur eine schlichte Fehlermeldung „Seite nicht gefunden" wie im Falle von tatsächlich nicht existierenden Seiten erhält, liefert A1 die Meldung „Webseite gesperrt – Aufgrund einer einstweiligen Verfügung des Handelsgerichts Wien musste der Zugang zu dieser Website gesperrt werden" aus – siehe dazu die Screenshots unter http://derstandard.at/2000006365884/Netzsperren-Ab-sofort-im-Einsatz-aber-leicht-zu-umgehen.

5. Rechtswidrige Verbreitung von urheberrechtlich geschütztem Material: Portalseiten und Verbreitungswege[213]

5.1. Vorbemerkungen

Grundsätzlich lassen sich, unabhängig von der konkreten Verbreitungsart, im Zusammenhang mit der Zurverfügungstellung urheberrechtlich geschützten Materials grob zwei Kategorien von Websites abgrenzen:

- Portalseiten in Form von Linksammlungen, wie es kinox.to oder movie4k.to sind, Suchmaschinen in Form von Bittorrent-Datenbanken oder Usenet-Crawlern oder Foren wie boerse.bz bieten ihren Nutzern die Möglichkeit, sich Kenntnis zu verschaffen, wo geschütztes Material bezogen werden kann. Sie stellen also Links zu Sharehostern, Streaminganbietern, Bittorent-Dateien oder ins Usenet bereit.
- Die Inhalte selbst werden von von diesen Portalen unabhängigen Hostern in Form von Usenet-Providern, Share- bzw Streamhostern oder wie im Fall von Bittorrent von anderen Bittorrent-Nutzern bereitgestellt.

Diese Unterscheidung dient zwar dem besseren Verständnis, ist jedoch, abgesehen von der bei Bittorrent gegebenen Problematik, auf welche unter 5.4.2 Bezug genommen wird, juristisch weitgehend unerheblich. So haften nach ständiger Rechtsprechung des OGH Linksetzer, welche Portalseiten oder spezielle Suchmaschinen unzweifelhaft sind und worunter mE auch Links ins Bittorrent-Netz in Form von „.torrent"-Dateien fallen, als Gehilfe neben dem Verfügungsberechtigten der verlinkten Seite. Sie wollen „*und veranlass[en] demnach zurechenbar, dass der Internet-Nutzer von [der von ihnen betriebenen] Seite auch auf den Inhalt der über den Link erreichbaren fremden Seite zugreifen kann*". [214]

5.2. Streaming-Dienste

5.2.1. Technische Grundlagen

Warum sich die aktuellen Sperraufforderungen des Verein für Anti-Piraterie gegen die Film-Streamingportale kinox.to und movie4k.to richten, ist unschwer erkennbar: Die weite Verbreitung von Breitbandanschlüssen hat nämlich nicht nur legalen Portalen wie youtube zum Durchbruch verholfen, sondern auch die Entwicklung von Diensten ermöglicht, welche

[213] Die Inhalte dieses Abschnitts beruhen, sollten sie nicht durch Zitate belegt sein, auf meinen eigenen Beobachtungen.
[214] RIS-Justiz RS0114467.

ohne die notwendige Zustimmung der Rechteinhaber den teils kostenlosen Konsum urheberrechtlich geschützten Materials ermöglichen.

Waren für die Nutzung von Streaming-Diensten anfangs eigenständige Programme notwendig, ermöglicht Streaming-Technologie heutzutage mittels verschiedener Standards wie Adobe Flash oder HTML5 die unkomplizierte Videowiedergabe innerhalb des Browsers. Im Zuge der Wiedergabe von Streaming-Inhalten werden die Videodaten auf dem Computer des Anwenders zwischengespeichert, ein permanenter Download erfolgt nicht. Wird beispielsweise das Browserfenster geschlossen, ist eine spätere Wiedergabe nicht mehr möglich. Portale wie kinox.to oder movie4k.to bieten in der Regel aber die zusätzliche Möglichkeit, Filme herunterzuladen.

5.2.2. Geschäftsmodell

Der inoffizielle Vorgänger von kinox.to war die im Juni 2011 in Folge von Ermittlungen abgeschaltete[215] Seite kino.to, welche Ausgangsfall für die EuGH Vorlageentscheidung C-314/12 und die infolge ergangene OGH-Entscheidung 4 Ob 71/14s war. Die folgende Darstellung lässt sich auch auf die noch in Betrieb befindlichen Seiten kinox.to und movie4k.to übertragen, da diese das kino.to Geschäftsmodell übernahmen und technisch mit kino.to vergleichbar sind.

Kino.to war eine reine Portalseite, welche eine Sammlung von Links auf von sogenannten Streamhostern gespeicherte Filme bereitstellte. Die Filme an sich waren also auf vom Portal separaten Servern gehosted. Aufgrund des Charakters als Portalseite waren zu einem einzelnen Film meist mehrere Links zu verschiedenen Streamhostern verfügbar. Über entsprechende Verwertungsrechte verfügten weder kino.to noch die Streamhoster.[216]

Die Streamhoster waren von kino.to organisatorisch wie finanziell getrennt, das Bindeglied zwischen diesen stellten die sogenannten Uploader dar. Diese verschafften sich das urheberrechtlich geschützte Filmmaterial aus diversen Quellen und luden es auf einen beliebigen Streamhoster, von welchem sie in Folge entweder einen festgelegten Betrag oder einen Anteil an den Werbeeinnahmen, welche der Streamhoster mit den von ihnen hochgeladenen Filmen erzielte, erhielten. Als zusätzliche Einnahmequelle boten die Streamhoster auch Premium-Zugänge an, welche beispielsweise den Download von Filmen erlaubten. Auch die bei einigen Streamhostern bestehende Minutenbegrenzung von Streams in

[215] http://www.zeit.de/digital/internet/2011-06/kino-stream-ermittlung.
[216] Amtsgericht Leipzig 21.12.2011, 200 Ls 390 Js 184/11.

der Gratisversion war ein Verkaufsargument. Kino.to wiederum erzielte pro Monat Werbeeinnahmen von circa 150.000 Euro durch auf dem Portal eingebundene Werbung, an diesen Einnahmen partizipierten die Uploader nicht.[217]

Um in die Linksammlung von kino.to aufgenommen zu werden, hatten die Filme gewisse Qualitätskriterien zu erfüllen, wie eine Eingangs- und Schlusssequenz, welche auf kino.to hinweist, das gleichzeitige Bereitstellen von schriftlichen Inhaltszusammenfassungen sowie das Hinaufladen auf einen Hoster, welcher den Abruf in angemessener Geschwindigkeit gewährleistete. Nach dem Hinaufladen auf einen Streamhoster mussten die Uploader, welche für diesen Zweck Zugang zu einer eigenen Administrationsoberfläche auf kino.to hatten, die Links an kino.to übermitteln. In weiterer Folge erfolgte eine Überprüfung der Links seitens kino.to auf die genannten Qualitätskriterien, bei positiver Beurteilung wurde der Link danach für die Benutzer von kino.to freigeschaltet.[218]

Obwohl kino.to grundsätzlich jeden beliebigen Streamhoster zuließ, wurden die Meistgenutzten seitens kino.to bevorzugt. Diese erhielten prominentere Schaltflächen in der Übersicht der verfügbaren Streams eines Films, kleinere Hoster waren unter einer gemeinsamen Schaltfläche zusammengefasst. Da zumindest ein Mitarbeiter von kino.to, nämlich der für den Betrieb der Server zuständige Techniker, auch einen eigenen Streamhoster betrieb, ist es naheliegend, dass die Auswahl der prominenten Streamhoster nicht ausschließlich nach dem Kriterium der Beliebtheit bei den Uploadern erfolgte; schließlich lag es im Interesse des genannten Mitarbeiters, neben den Einnahmen an kino.to auch die Einnahmen seines Streamhoster zu maximieren. Dies gelang mit Erfolg, von 2008 bis zur Sperrung von kino.to Anfang Juni 2011 erzielte der kino.to-Mitarbeiter mit seinem Streamhoster einen Gewinn von ungefähr 320.000 Euro.[219]

5.2.3. Rechtswidrigkeit der Nutzung?

Der Konsum von Streaminginhalten ist, da nur eine flüchtige Vervielfältigung zum Zweck der Wiedergabe erfolgt, unter das Recht der flüchtigen und begleitenden Vervielfältigung des § 41a UrhG zu subsumieren. Diese ist zwar nur dann zulässig, wenn der Betreiber der Streamingseite über die notwendigen Rechte zur öffentlichen Wiedergabe verfügt, allerdings kann sich ein Nutzer darauf berufen, keine Kenntnis von der Unrechtmäßigkeit der Quelle zu haben oder haben zu können und sich dadurch von einer etwaigen Haftung gegenüber den

[217] Amtsgericht Leipzig 21.12.2011, 200 Ls 390 Js 184/11.
[218] Amtsgericht Leipzig 21.12.2011, 200 Ls 390 Js 184/11.
[219] Amtsgericht Leipzig 21.12.2011, 200 Ls 390 Js 184/11.

Rechteinhabern befreien.[220] Es erscheint nicht unwahrscheinlich, dass sich Nutzer von Streamingseiten erfolgreich verteidigen, da es für unbedarfte Nutzer aufgrund der professionellen Gestaltung der meisten Streamingseiten argumentierbar ist, sie hätten nicht von deren Rechtswidrigkeit gewusst bzw wissen können.

Für den Fall eines Downloads von einem Streamhoster kann auf die Erwägungen unter 5.3.2 verwiesen werden.

5.2.4. Sperre?

Abgesehen von den konkreten Sperrmaßnahmen, welche näher in Kapitel 7 erörtert werden, stellt sich die Frage, ob eine Sperre von Streaming-Portalseiten oder deren Streamhostern grundsätzlich mit deren grundrechtlich garantierten Rechten vereinbar ist. Im Hinblick auf die gegenständliche EuGH-Judikatur lässt sich diese Frage freilich recht einfach beantworten:

Zwar können sich nach der Pirate Bay-Entscheidung (siehe dazu unter 3.4.2.2) auch Anbieter von Streamingportalen oder Streamhostern auf die Informationsfreiheit berufen, eine Abwägung zugunsten der Schutzinteressen der Rechteinhaber wird jedoch unzweifelhaft Bestand haben (und wurde in diesem Sinne auch vom EuGH und OGH vorgenommen).

Dies resultiert aus der Tatsache, dass eine Bescheinigung, dass sich auf Streamingportalen bzw deren Streamhostern ausschließlich rechtsverletzende Inhalte befinden, relativ leicht möglich ist.

Schon ein Blick auf kinox.to bzw movie4k.to offenbart, dass dort zu einem weit überwiegenden Teil Filme ohne die dazu notwendigen Rechte verlinkt werden. Zwar weisen die Betreiber von kinox.to in einer Meldung auf der Startseite darauf hin, dass auch Filme verfügbar seien, die gemeinfrei sind, führen dazu aber nur ein einziges Beispiel auf[221]. Die Bescheinigung der Rechtverletzung wird aber sicherlich nicht daran scheitern, dass auf der Seite alibihalber ein Film angeboten wird, der nicht in Rechte von Urheberrechtsinhabern eingreift.

Ebenso stellt es kein Problem dar zu bescheinigen, dass ein bestimmter Streamhoster praktisch nur rechtsverletzendes Material anbietet: Am Beispiel des Streamhost „movshare.net“ offenbart schon eine simple Google-Suche nach „film site:movshare.net“, dass zumindest die Suchergebnisse ausschließlich urheberrechtlich geschützte Filme

[220] *Vogel* in *Kucsko* (Hrsg), urheber.recht § 41a, 4.3.2 (Stand 1.12.2007).
[221] Dieses Beispiel ist, nur der Interesse halber angemerkt, eine Dokumentation darüber, dass das Urheberrecht im Sinne von Streamingseiten „reformiert“ werden soll.

betreffen. Im Gegensatz zu Sharehostern besteht auch keinerlei Problem für Rechteinhaber, die angebotenen Inhalte auf deren Rechtmäßigkeit zu prüfen: Ein einfacher Klick auf den Wiedergabeknopf ermöglicht es nachzuvollziehen, welcher Inhalt hinter einem Link zu einem Streamhoster steht.

5.3. Sharehoster

5.3.1. Grundlagen

Sharehoster stellen ihren Kunden einerseits meist kostenlos Speicherplatz zur Verfügung, auf welchem beliebige Dateien gehostet werden können. Andererseits bieten sie im Rahmen sogenannter „Premiumzugänge" Tarife an, welche im Hinblick auf das herunterladbare Dateivolumen unbegrenzt oder nur geringfügig limitiert sind und Downloads zu hohen Geschwindigkeiten ermöglichen. [222] Ohne Premiumzugang sind meist nur langsame Downloads möglich, welche durch Werbeschaltungen auf den Downloadseiten der Sharehoster Einnahmen generieren.

Auch die auf Sharehostern bereitgehaltenen Inhalte sind im Hinblick auf ihre Rechtmäßigkeit unzweifelhaft diversifiziert, es liegt jedoch die Vermutung nahe, dass viele Kunden Premiumzugänge überwiegend dazu nutzen, urheberrechtlich geschütztes Material herunterzuladen.

Das Geschäftsmodell der Sharehoster ist mit jenem der Streaminganbieter vergleichbar: Auch Sharehoster bieten ihren Uploadern die Möglichkeit, über diverse Bonusprogramme an im Rahmen von Werbeeinnahmen oder Premiumzugängen lukrierten Einnahmen beteiligt zu werden. [223]

Sharehoster bieten in der Regel nicht die Möglichkeit, die bei ihnen gehosteten Inhalte gezielt zu durchsuchen. Um Inhalte eines Sharehosters zu beziehen, ist die Kenntnis der exakten Links zu den gespeicherten Dateien notwendig; diese Links erhält der Uploader, nachdem er Dateien hinaufgeladen hat. Diese Links werden wiederum über einschlägige Portale wie zB serienjunkies.org oder Foren wie zB boerse.bz, mygully.com oder boerse.to verbreitet, welche Einnahmen durch Werbeschaltungen generieren.[224]

[222] Siehe dazu etwa http://uploaded.net/register
[223] *Launinger/Kirda/Michiardi*, Paying for Piracy? An Analysis of One-Click Hosters' Controversial Reward Schemes.
[224] Landgericht Hamburg 02.03.2014, 308 O 458/10, RZ 9.

Die Forcierung gewisser Sharehoster auf bestimmten Portalen legt somit die Vermutung nahe, dass zwischen deren Betreibern – ähnlich wie bei den Streamhostern im Fall kino.to – Geschäftsbeziehungen oder Besitzverhältnisse herrschen mit dem Ziel, möglichst viele Einnahmen zu lukrieren. Diese Vermutung bestätigte sich im Rahmen der aktuell in Deutschland laufenden strafrechtlichen Ermittlungen gegen die Hintermänner von kinox.to, wo bekannt wurde, dass diese Personen neben kinox.to auch movie4k.to, die Foren mygully.com und boerse.sx sowie zwei Sharehoster betreiben[225].

5.3.2. Rechtswidrigkeit der Nutzung?

Spätestens seit der Entscheidung ACI-Adam[226] ist endgültig klargestellt, dass sich Nutzer nur dann auf eine Vervielfältigung zum privaten Gebrauch berufen können, wenn diese aus einer rechtmäßigen Quelle erfolgt. Daraus folgt, dass der Download von urheberrechtlich geschütztem Material von Sharehostern, ein dauerhafter Download von einem Streaminganbieter oder das Beziehen aus dem Usenet jedenfalls rechtswidrig ist. Diese rechtliche Bewertung hat jedoch faktisch wenig Auswirkungen, da es in der Regel für Rechteinhaber nicht feststellbar ist, welche Nutzer rechtswidrige Downloads vornehmen. Nutzer können nur dann ausgeforscht werden, wenn Server von Sharehostern, Streamhostern oder Usenet-Providern beschlagnahmt werden und auf diesen Aufzeichnungen (Log-Dateien) vorhanden sind, welche die IP-Adressen der Nutzer enthalten oder Nutzer aufgrund von Zahlungsdaten für Premiumdienste identifiziert werden können. Wie die Erfahrungen aus dem Verfahren rund um kino.to in Deutschland zeigen, bleibt die Verfolgung von Nutzern jedoch meist erfolglos.[227]

Auch ein zivilrechtliches Vorgehen seitens der Rechteinhaber gegen die Nutzer macht, abgesehen von der Problematik der Ermittlung der IP-Adresse (siehe dazu näher unter 5.4.2), nur begrenzt Sinn: Zwar könnten Rechteinhaber Schadenersatz verlangen. Dass dieser jedoch höher anzusetzen ist als der Preis eines Kinotickets oder einer DVD, wird nur schwer zu argumentieren sein, weswegen ein Vorgehen gegen die Nutzer wirtschaftlich wenig sinnvoll erscheint.

[225] http://heise.de/-2432216.
[226] EuGH 10.04.2014, C-435/12 (ACI Adam u.a.) = jusIT 2014/44, 88 (*Staudegger*) = MR-Int 2014, 42 (*Walter*) = ecolex 2014/297, 727 (*Zemann*).
[227] So berichtete der Focus im Februar 2012 von Ermittlungen gegen Permiumnutzer von kino.to, eine Internetrecherche hat jedoch keinerlei Ergebnisse dieser Ermittlungen zu Tage gefördert, was den Schluss zulässt, dass die Verfahren zwischenzeitlich eingestellt wurden. http://www.focus.de/digital/internet/stillgelegte-raubkopie-seite-kino-to-und-kinox-to-nutzern-illegaler-filmportale-droht-strafverfahren_aid_713251.html.

5.3.3. Sperre?

Im Hinblick auf Sharehoster ergibt sich mE das Problem, dass eine generelle Sperre eines Sharehosters nicht mit der Informationsfreiheit vereinbar ist bzw schon die Bescheinigung, dass über einen Sharehoster ausschließlich rechtswidrige Inhalte angeboten werden, fehlschlägt.

Die Unvereinbarkeit mit der Informationsfreiheit resultiert einerseits daraus, dass zumindest einige Sharehoster auch rechtmäßige Inhalte speichern und es Nutzer gibt, welche Sharehoster zB für berufliche Zwecke verwenden.[228]

Die Unvereinbarkeit lässt sich aber auch schlicht damit begründen, dass es oft nicht möglich sein wird, die Rechtswidrigkeit von auf Sharehostern angebotenen Inhalten zweifelsfrei festzustellen und daher auch nicht die im Rahmen des nationalen Verfahrens notwendige Bescheinigung zu führen. Dieses Problem resultiert aus dem Umstand, dass größere Dateien auf Sharehostern aufgrund von Begrenzungen der Dateigrößen seitens der Sharehoster in der Regel nicht im Ganzen, sondern meist mittels spezieller Programme wie „Winrar“ als gestückelte Archive angeboten werden, welche zudem oft mit einem Passwort verschlüsselt sind. Diese Archive werden erst nach dem Download vom Benutzer extrahiert, um wieder die vollständige Datei herzustellen. Das zum Archiv gehörige Passwort wird meistens gemeinsam mit den Links zum Sharehoster veröffentlicht – der Passwortschutz dient nämlich nicht dazu, Benutzer vom Extrahieren der Archive abzuhalten, sondern hat den Zweck, automatische Überprüfungen der hinaufgeladenen Inhalte zu unterbinden. Inhalte werden nämlich meist durch das Erstellen von Dateihashes (zu Dateihashes siehe unter 6.6) abgeglichen, sodass ein erneutes Hinaufladen bereits gelöschter Inhalte unterbunden wird. Der Passwortschutz und die Aufteilung von Dateien in mehrere Archive verhindert derartige Überprüfungen deswegen, weil sich einerseits der Hashwert der einzelnen Archivteile je nach Passwort bzw Einstellungen des Nutzers, der die Archive erstellt, verändert und es Sharehostern nicht möglich ist, passwortgeschützte Archive automatisiert zu entpacken, um deren Inhalt zu überprüfen. Diese Tatsache macht es Rechteinhabern auch unmöglich, Dateien auf Sharehostern auf deren Rechtmäßigkeit zu überprüfen, so lange sie nicht die Seite kennen, auf der die Links zu allen Archivteilen sowie das Passwort zu finden ist.[229]

[228] So nutzte zB ein Sportreporter nachweislich den inzwischen geschlossenen Sharehoster „megaupload.com“ für berufliche Zwecke, siehe http://torrentfreak.com/megaupload-user-asks-court-to-order-return-of-his-data-120525/.

[229] Siehe dazu die Ausführungen des Landgerichts Hamburg 02.03.2014, 308 O 458/10, RZ 34ff.

Auch im Hinblick auf die Portale, welche Links zu Sharehostern anbieten, ergibt sich eine nicht unwesentliche Problematik. Abgesehen von reinen Linkportalen wie serienjunkies.org, welche durchaus mit kinox.to vergleichbar sind, ist in Bezug auf spezielle Linkforen wie zB boerse.bz die Abwägung zwischen der Informations- bzw Meinungsfreiheit und dem Schutz des geistigen Eigentums äußerst schwierig:

Zwar ist ein wesentlicher Teil dieser Foren jener Bereich, in welchem Links getauscht werden, allerdings sind auch Bereiche vorhanden, die – wie in jedem anderen Internetforum auch – der allgemeinen Diskussion gewidmet sind.[230] Die Themenbereiche reichen dabei über Smalltalk und technische Hilfestellungen der Forennutzer untereinander bis zu politischen Diskussionen.

Der EGMR gab den Mitgliedsstaaten im Rahmen der Pirate Bay-Entscheidung einen weiten Ermessensspielraum bei Abwägungen zwischen der Meinungsfreiheit und dem Schutz des geistigen Eigentums in die Hand, sodass im Lichte dieser Entscheidung eine rechtskonforme Argumentation zugunsten beider Grundrechte möglich sein sollte. Vor allem das Vorhandensein politischer Diskussionen in solchen Foren erscheint mE jedoch durchaus als ein gewichtiges Argument, Sperren auf Grundlage der derzeitigen Rechtslage zu verwehren.

5.4. Tauschbörsen am Beispiel von Bittorrent

5.4.1. Grundlagen

Das Bittorrent-Protokoll wurde 2001 vom Programmierer Bram Cohen geschaffen, um die Verteilung großer Dateien mit einem deutlich geringeren Aufwand als per klassischem Download zu ermöglichen. Im Gegensatz zu einem Download von einem einzelnen Server erfolgt das Herunterladen von Daten über Bittorent aus möglichst vielen verschiedenen Quellen, dem sogenannten Schwarm. Jedermann, der Dateien über Bittorrent bezieht, stellt diese gleichzeitig anderen Teilnehmern im Rahmen des Schwarms zur Verfügung. Dateien werden dabei in kleine Datenpakete zerlegt, welche selbst dann schon von einem Nutzer verteilt werden, wenn dieser noch nicht die komplette Datei besitzt.[231]

Um eine Datei aus dem Bittorrent-Netzwerk zu beziehen, muss sich der Nutzer eine „.torrent"-Datei verschaffen. Diese enthält einerseits Informationen zu den Datenpaketen, in welche eine über Torrent verteilte Datei zerlegt ist und andererseits solche über den sogenannten Tracker, welcher die Teilnehmer im Netzwerk zueinander vermittelt, also

[230] Beispielsweise Foren zu diversen Themenbereichen unter https://boerse.to/categories/talk.42/.
[231] http://www.bittorrent.org/introduction.html.

Informationen bereithält, welcher Nutzer welche Datei zur Verfügung stellt.[232] Aufgrund der Notwendigkeit von „.torrent"-Dateien ist es nicht möglich, das Bittorrent-Netzwerk gezielt nach Inhalten zu durchsuchen. Zwar gibt es Entwicklungen, welche eine Suche, wie sie andere Tauschbörsenstandards bieten, implementieren, diese haben sich bisher aber nicht auf breiter Front durchgesetzt.[233]

Der Tracker stellt ein zentrales Element im Bittorrent-Netz dar[234], welches im Rahmen gerichtlicher Entscheidungen gesperrt oder geschlossen werden könnte. Als Reaktion auf derlei Forderungen gibt es jedoch Entwicklungen hin zum „trackerless" Netzwerk – also einer Weiterentwicklung des Bittorrent-Protokolls, welche Übertragungen ohne das zentrale Element des Trackers mittels einer über das Netzwerk verteilten Datenbank ermöglicht.[235]

5.4.2. Rechtswidrigkeit der Nutzung?

Tauschbörsen sind im Hinblick auf die Rechtswidrigkeit, welche aus deren Nutzung erwächst, nicht mit den bereits dargestellten Diensten zu vergleichen: Deren technisch großer Vorteil, von klassischen Downloadservern unabhängig zu sein, da die Daten direkt zwischen den Nutzern getauscht werden, präsentiert sich als rechtlicher Nachteil für die Nutzer:

Das Anbieten von Dateien im Bittorrent-Netz lässt sich nicht unter eine freie Werknutzung des UrhG subsumieren, ist also unzweifelhaft rechtswidrig. Nutzer von Tauschbörsen sehen sich also theoretisch der Gefahr von Schadenersatzansprüchen ausgesetzt, die je nach Sach- und Beweislage durchaus beträchtlich sein können.

Relativiert wird dies jedoch durch die faktische Unmöglichkeit für Rechteinhaber, Inhaber von IP-Adressen zu ermitteln:

Grundsätzlich bestünde zur Ermittlung eines Anschlussinhabers die Ermittlungsbefugnis der Staatsanwaltschaft nach § 76a StPO. Da nach der österreichischen Rechtslage Urheberrechtsdelikte der Privatanklage unterliegen (§ 91 Abs 3 UrhG), also kein Ermittlungsverfahren der Staatsanwaltschaft stattfindet, ist die Ausforschung eines Anschlussinhabers für den Rechteinhaber, da ihm als Privatankläger nicht die Ermittlungsbefugnisse des § 76a StPO zukommen, auf strafrechtlichem Weg faktisch

[232] http://jonas.nitro.dk/bittorrent/bittorrent-rfc.html#anchor13.
[233] http://www.cs.cornell.edu/People/egs/papers/hyperspaces.pdf.
[234] http://jonas.nitro.dk/bittorrent/bittorrent-rfc.html#anchor17.
[235] http://bittorrent.org/beps/bep_0005.html.

unmöglich.[236] Ein zivilrechtlicher Anspruch bestünde nach § 87b Abs 3 UrhG, ist jedoch in seiner derzeitigen Ausgestaltung nicht anwendbar[237].

5.4.3. Sperre?

Über Bittorrent wird einerseits unzweifelhaft urheberrechtlich geschütztes Material unrechtmäßig verbreitet. Seiten wie piratebay.se oder isohunt.to beherbergen große Datenbanken an „.torrent"-Dateien, welche auf geschütztes Material verweisen.

Andererseits darf aber nicht außer Acht gelassen werden, dass Bittorrent viele rechtmäßige Nutzungsmöglichkeiten eröffnet, die in der Praxis eine große Rolle spielen. So benutzt beispielsweise der Spielehersteller Blizzard Bittorrent, um populäre Spiele wie World of Warcraft an seine Kunden zu verteilen[238], zahlreiche Linuxdistributionen werden darüber bereitgestellt[239], der öffentlich-rechtliche norwegische Rundfunk verteilt seine Sendungen teilweise über Bittorrent[240] aber auch independent Lables wie DGM stellen Inhalte über Bittorrent bereit[241], um nur einige der zahlreichen Beispiele zu nennen.

Ein generelles Filtern von Bittorrent-Verkehr ist aufgrund der potentiellen Verletzung der Informationsfreiheit durch das Blockieren der eben genannten legitimen Inhalte jedenfalls nicht rechtmäßig. Ein gezieltes Filtern rechtswidriger Bittorrent-Inhalte wäre andererseits nicht mit dem Urteil Scarlet-Extended in Einklang zu bringen, müsste dafür doch ein auf alle Nutzer unterschiedslos anwendbares und zeitlich unbegrenzt auf Kosten der Access-Provider eingerichtetes System benutzt werden, um präventiv Urheberrechtsverletzungen vorzubeugen, welches noch dazu aufgrund der großen Komplexität mit erheblichen Kosten verbunden wäre.

So verwundert es nicht, dass sich die aktuellen Sperraufforderungen nicht gegen Bittorrent-Traffic an sich richten, sondern Portale wie piratebay.se oder isohunt.com zum Gegenstand haben. Die Problematik in diesem Zusammenhang ist jedoch, dass auch diese Portale „.torrent"-Dateien für legale Inhalte wie Linuxdistributionen bereithalten; es wäre also notwendig, im Rahmen einer Abwägung zwischen der Informationsfreiheit und dem Urheberrecht zu beurteilen, ob rechtswidrige Inhalte auf diesen Portalen tatsächlich derart überwiegen, dass eine Sperre gerechtfertigt werden kann. Das OLG Köln hat eine

[236] Um diesem Problem beizukommen gab es 2009 einen Ministerialentwurf (XXIV. GP, 82/ME) welcher vorsah, Privatanklägern Ermittlungsbefugnisse zukommen zu lassen. Zu einer Umsetzung ist es jedoch bisher nicht gekommen.
[237] siehe dazu weiterführend *Briem*, Ist der Auskunftsanspruch gegenüber Providern nach § 87b Abs 3 UrhG tot?, MR 2011, 55.
[238] http://us.blizzard.com/en-us/company/about/legal-faq.html.
[239] zB die Distribution Ubuntu, siehe http://www.ubuntu.com/download/alternative-downloads.
[240] http://nrkbeta.no/bittorrent/.
[241] http://www.dgmlive.com/help.htm#whyusebittorrent.

Sperrverfügung gegen eine mit piratebay.se vergleichbare Seite kürzlich ua auch deswegen abgelehnt, weil bei einer Gesamtanzahl von 45.000 über diese Seite angebotenen Musiktiteln schon die Anzahl von 1.800 rechtmäßig angebotenen Musiktiteln als nicht vernachlässigenswert gering anzusehen sei[242].

Ein Ergebnis einer solchen Abwägung lässt sich nicht zuletzt aufgrund des großen mitgliedsstaatlichen Ermessensspielraums und der Tatsache, dass sich ohne eine eingehende Analyse der Datenbanken der betroffenen Seiten nicht sagen lässt, ob diese tatsächlich fast ausschließlich rechtswidriges Material bereitstellen, nicht seriös voraussagen.

5.1. Usenet

5.1.1. Grundlagen

Das Usenet besteht schon seit den frühen 80ger Jahren und entwickelte sich damit deutlich vor dem World Wide Web. Das Usenet besteht aus sogenannten Newsgroups, eingeteilt in verschiedenste Kategorien, welche eigentlich, ähnlich den modernen Internetforen, zur Diskussion verschiedenster Themen benutzt werden.[243]

Das Usenet besitzt keinen zentralen Server, sondern wird verteilt auf vielen verschiedenen Servern betrieben, welche die Newsgroups untereinander synchronisieren.[244] Der Zugang zum Usenet erfolgt mittels eines Usenet-Providers, wobei nicht jede Newsgroup über jeden Provider abgerufen werden kann. Usenet-Provider kann zB der Access-Provider sein, es gibt jedoch auch Provider, welche ausschließlich kostenpflichtige Usenet-Dienste anbieten. Im Unterschied zu Internetforen werden Daten in Newsgroups von den meisten Usenet-Providern nicht unbegrenzt gespeichert, sondern nach einem gewissen Zeitablauf gelöscht.

Neben dem Meinungsaustausch wird das Usenet, insbesondere Newsgroups wie „alt.binaries“, auch dazu genutzt, urheberrechtlich geschütztes Material zu verbreiten. Spezielle Suchmaschinen erlauben das gezielte Suchen nach allen Arten urheberrechtlich geschützter Inhalte. Will ein Benutzer eine über eine solche Suchmaschine gefundene Datei beziehen, so lädt er, vergleichbar mit „.torrent“-Dateien für Bittorrent (siehe dazu unter 5.4.1), eine Definitionsdatei herunter, welche die genauen Angaben enthält, um die Datei mittels eines speziellen Programms aus dem Usenet herunterzuladen. [245] Wie bereits erwähnt, sind nicht alle Newsgroups über jeden beliebigen Usenet-Provider zugänglich, viele Provider

[242] OLG Köln 18.07.2014, 6 U 192/11 S 48.
[243] http://today.duke.edu/2010/05/usenet.html
[244] http://tools.ietf.org/html/rfc5537
[245] zB www.usenet-crawler.com

führen zB „alt.binaries“ nicht, da diese Newsgroup fast ausschließlich für die rechtswidrige Verbreitung urheberrechtlich geschützten Materials genutzt wird. Einige Usenet-Provider, zB newsdemon.com, sind jedoch offensichtlich genau auf die Verbreitung solcher Newsgroups spezialisiert und werben zB mit einer besonders langen Archivierungsdauer von Nachrichten, was zur Folge hat, dass über solche Provider besonders viel urheberrechtlich geschütztes Material verfügbar ist.

5.1.2. Rechtswidrigkeit der Nutzung?

Zur Rechtswidrigkeit der Nutzung von Usenet-Diensten, um urheberrechtlich geschütztes Material zu beziehen, sei an dieser Stelle an die Erörterungen unter 5.2.3 verwiesen, welche sich, da aus dem Usenet ein reiner Download ohne gleichzeitigen Upload erfolgt, analog auf Usenet-Dienste übertragen lassen.

5.1.3. Sperre?

In Bezug auf Usenet-Suchmaschinen kann auf die Argumentation zu Portalen wie piratebay.se verwiesen werden (siehe dazu unter 5.4.3), da diese Suchmaschinen, mit Bittorrent-Portalen vergleichbar, Dateien bereitstellen, mit deren Hilfe der eigentlich gewünschte Download initiiert werden kann.

Betrachtet man Usenet-Provider, so ergibt sich eine ähnliche Problemstellung wie in Bezug auf Sharehoster-Foren (siehe dazu unter 5.3.3), mit dem Unterschied, dass im Gegensatz zu Sharehoster-Foren der Download nicht von einem externen Anbieter, sondern direkt vom Usenet-Provider erfolgt. Da, wie bereits erwähnt, die meisten seriösen Usenet-Provider jene Newsgroups, welche Zugang zu urheberrechtlich geschützten Inhalten ermöglichen, nicht führen, sind diese für die Erörterung eventueller Sperren unbeachtlich.
In Bezug auf jene Usenet-Provider, welche de facto auf Downloads aus einschlägigen Newsgroups spezialisiert sind, ist wiederum eine Abwägung zwischen der Informationsfreiheit einerseits und dem Schutz des geistigen Eigentums andererseits vorzunehmen. Trotz des weiten Ermessensspielraums muss eine solche Abwägung mE zwangsläufig zugunsten des Schutzes des geistigen Eigentums erfolgen. Die Sperre eines einzelnen Usenet-Anbieters hat nämlich nicht zur Folge, dass der Zugang zum Usenet insgesamt unmöglich ist, sondern betrifft eben nur einen von vielen Providern. Benutzer, die legitimer Weise Zugang zu Newsgroups wollen, in denen legale Inhalte vorhanden sind, können im Fall einer Sperre gewisser Usenet-Provider auf einen anderen, weniger zwielichtigen Anbieter wechseln, was mE den Eingriff in das Grundrecht der Informationsfreiheit äußert gering erscheinen lässt.

6. Technische Grundlagen

Im folgenden Kapitel sollen die technischen Grundlagen vermittelt werden, die zum Verständnis der im Kapitel 7 behandelten Sperrmethoden notwendig sind.

6.1. Paketvermittelte Netzwerke

In paketvermittelten Netzwerken wie dem Internet werden Daten in Form von Datenpaketen übertragen. Diese Datenpakete lassen sich in zwei Teile gliedern, den sogenannten Header und die Payload.

Der Header enthält, vergleichbar mit einem Briefumschlag, die Adressinformationen, nämlich die des Absender und des Empfänger. Die Payload ist der eigentliche Nachrichtenteil des Pakets und enthält die zu übermittelnden Daten.[246] Wird beispielsweise eine E-Mail im Internet übertragen, so verteilt sie sich je nach Dateigröße über viele verschiedene Pakete, da jedes Datenpaket in seiner Größe begrenzt ist. Die Payload enthält also immer nur ein Bruchstück des zu übertragenden Inhaltes, der Empfänger rekonstruiert diesen durch Zusammenfügen aller Datenpakete.

Die Übertragung dieser Pakete ermöglicht im Internet der sogenannte TCP/IP Standard. Dieser legt fest, wie ein Datenpaket vom Absender zum Empfänger mittels Routing übertragen wird. Dem Absender und dem Empfänger müssen jeweils eine eindeutige, sogenannte IP-Adresse zugeordnet werden, um Kommunikation zu ermöglichen.[247]

Sogenannte Router besorgen innerhalb der zahlreichen Netzwerke, welche in ihrer Gesamtheit das Internet ausmachen, die Weiterleitung von Datenpaketen zwischen dem Absender und dem Empfänger. Router haben die jeweils effektivsten Wege bzw auch alternative Routen von einem Knotenpunkt zum nächsten in sogenannten Routing-Tabellen gespeichert und leiten Datenpakete dementsprechend weiter.[248]

Aufgrund der Knappheit der bis zum heutigen Tag am meisten genutzten Adressen des Standards IPv4, teilen sich in der Regel mehrere Geräte eine einzige Adresse, eine Adresse ist also meistens nicht exklusiv einem Gerät zugeordnet:

[246] https://tools.ietf.org/html/rfc793#section-3.1. Die RFC-Dokumente der Internet Engeneering Taskforce (IETF) legen die im Rahmen des Internets notwendigen technischen und organisatorischen Standards fest. Diese Dokumente werden deshalb als Belegquellen für die darzulegenden technischen Grundlagen herangezogen.
[247] https://tools.ietf.org/html/rfc1180.
[248] https://tools.ietf.org/html/rfc1812#section-2.2.3.

Da Access-Provider normalerweise jedem Kunden nur eine IPv4 Adresse zuordnen, in einem modernen Haushalt jedoch eine Vielzahl von mit dem Internet verbundenen Endgeräten vorhanden ist, wird die Technologie der Network Address Translation (NAT) angewendet, um die gemeinsame Nutzung der IP-Adresse zu ermöglichen. Handelsübliche (WLAN-)Router errichten dazu ein internes Netzwerk. Geräte innerhalb dieses Netzwerks bekommen sogenannte private IP-Adressen, welche aus einem für diesen Zweck vorgesehenen Bereich der IP-Adressspezifikation stammen und frei vergeben werden dürfen. Da diese Adressen in einer Vielzahl von privaten Netzwerken verwendet werden, sind sie innerhalb des Internets nicht einzigartig, erlauben also keine eindeutige Adressierung. Um diese zu ermöglichen, kommunizieren die Geräte über die im Router integrierte NAT quasi wie über einen Mittelsmann. Nach Außen hin, also im Internet, tritt nur der Router unter Benutzung der einzigartigen, vom Access-Provider zugewiesenen IP-Adresse als Absender in Erscheinung.[249]

Viele Host-Provider verwenden ihrerseits oft nur eine einzige IPv4-Adresse, um verschiedene Seiten ihrer Kunden mit dem Internet zu verbinden. Dies hat seine Ursache zB darin, dass sich eine Vielzahl unterschiedlicher Seiten entweder auf dem gleichen Server befindet oder dass eine Mehrzahl an Servern nicht direkt mit dem Internet verbunden ist. In diesem Fall wir dann deren Datenverkehr über ein gemeinsames Gateway abgewickelt wird. So teilen sich oft dutzende, wenn nicht hunderte, Internetseiten ein- und die selbe IP-Adresse.[250]

Die Notation von IPv4 erfolgt durch vier jeweils bis zu dreistellige Zahlengruppen, welche durch einen Punkt voneinander getrennt werden (z.B. 80.101.102.103).[251]

Aufgrund der Knappheit der zur Verfügung stehenden IPv4 Adressen ist bereits seit Jahren die – schleppende – Umstellung auf IPv6 im Gange.[252] IPv6 ermöglicht theoretisch die individuelle Adressierung jedes mit dem Internet verbundenen Gerätes bzw jeder gehosteten Internetseite. Die Darstellung von IPv6 Adressen erfolgt hexadezimal, wobei die Notation in acht durch Doppelpunkt getrennten Zeichenfolgen zu jeweils bis zu vier Zeichen erfolgt (z.B. 2001:470:1f0a:78a:0000:0000:0000:0002).[253] Nur ca 4,5% des weltweiten Internetverkehrs werden derzeit mittels IPv6 abgewickelt.[254]

[249] http://tools.ietf.org/html/rfc2663.
[250] http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/.
[251] http://technet.microsoft.com/en-us/library/dd469716(v=ws.10).aspx.
[252] http://heise.de/-1698607.
[253] http://technet.microsoft.com/en-us/library/dd458966(v=ws.10).aspx.
[254] https://www.google.com/intl/en/ipv6/statistics.html.

6.2. Domain Name System

Das Domain Name System (DNS) ermöglicht mittels einer verteilten Datenbank die Umsetzung von für Menschen gut lesbaren Internetadressen, beispielsweise www.univie.ac.at, in die zugehörige IP-Adresse, beispielsweise 131.130.70.8 für www.univie.ac.at. Erst durch Umsetzung eines Domainnamens in eine IP-Adresse kann ein Verbindungsaufbau zur unter einer Domain angebotenen Website erfolgen. DNS ermöglicht sowohl die Übersetzung in Adressen des IPv4 wie des IPv6 Standards.[255]

Das DNS System ist hierarchisch aufgebaut, Domainnamen werden stets von rechts nach links aufgelöst. An der Spitze dieser Hierarchie steht folglich die sogenannte Top-Level-Domain wie „.at", „.com" oder „.net". Diese Top-Level-Domains werden jeweils von verschiedenen Organisationen verwaltet, Individuen können unter Einhaltung der Regeln dieser Organisationen Domainnamen unter einer Top-Level-Domain registrieren.[256]

Access-Provider betreiben DNS-Server, um ihren Kunden Namensauflösung zu ermöglichen. Diese Server erhalten ihrerseits die Informationen zu individuellen Adressen von den für einen konkreten Domainnamen zuständigen sogenannten Nameservern. Ist ein Domainname nicht beim Access-Provider zwischengespeichert, so wendet sich der DNS-Server des Access-Providers an diesen Nameserver, um die vom Kunden gewünschte Information bereitstellen zu können.[257]

DNS-Server von Access-Providern speichern die zum Domainnamen gehörigen IP-Adressen in der Regel nur zwischen. Wie lange diese Zwischenspeicherung erfolgt, also wie lange es dauert, bis Änderungen an einem DNS-Eintrag übernommen werden, hängt von der sogenannten „Time to Live" ab. Diese wird vom Domaininhaber in Sekunden definiert und kann im Fall, dass IP-Sperren befürchtet werden, dementsprechend kurz angesetzt werden.[258]

Der sogenannte DNSSEC-Standard ermöglicht mittels einer „chain of trust" die Validierung von DNS-Abfragen. Dies bedeutet, dass DNSSEC-fähige Clients nachvollziehen können, ob im Zuge einer DNS-Abfrage Manipulationen vorgenommen wurden, also ob die Antwort der Abfrage beispielsweise infolge krimineller Aktivitäten oder auch Netzsperren verändert wurde.[259] DNSSEC befindet sich derzeit in der Einführung und ist mit Stand November 2014

[255] https://tools.ietf.org/html/rfc1035 sowie http://tools.ietf.org/html/rfc2874.
[256] *Ofcom*, „Site Blocking" to reduce online copyright infringement, S 19ff.
[257] https://tools.ietf.org/html/rfc1035.
[258] *Ofcom*, „Site Blocking" to reduce online copyright infringement, S 29.
[259] https://tools.ietf.org/html/rfc4033.

weder auf den im Netz der Universität Wien noch im Netz von UPC verwendeten DNS Servern aktiv[260], auch die „.at“ Top-Level-Domain unterstützt derzeit kein DNSSEC[261].

6.3. Paketfilter

Die Technologie der Packet Inspection ermöglicht es, den Datenverkehr in IP-Netzen zu überwachen und zu beeinflussen. Grundsätzlich kann zwischen drei Arten der Paket Inspection, welche sich durch ihre abgestufte Intensität auszeichnen, unterschieden werden. Nach mE sind im Zusammenhang mit Internetsperren vor allem zwei Arten dieser Filter relevant, nämlich der einfache Paketfilter und die Deep Packet Inspection.

Ein simpler Paketfilter erlaubt auf Grundlage der Header-Informationen eines Datenpakets das Zulassen bzw das Unterbinden von Verbindungen zwischen zwei Kommunikationspartnern. Ein solcher Paketfilter kann beispielsweise nur bestimmte Arten von Datenverkehr, wie etwa das Aufrufen von Websites mittels http, zulassen oder die Kommunikation zu gewissen IP-Adressen, beispielsweise im Zusammenhang mit Sperrverfügungen, unterbinden.[262]

Stateful Paket Inspection (SPI) wird vor allem in Firewalls eingesetzt. Zusätzlich zu den Funktionen eines simplen Paketfilters erlaubt Stateful Paket Inspection die Überwachung des Zustands verschiedener Verbindungen. Somit ist es beispielsweise möglich, Kommunikation mit einem Gerät hinter einer SPI-Firewall nur dann zuzulassen, wenn diese gerade von von diesem Gerät ausgehend initiiert wurde. [263]

Die Technik der Deep Paket Inspection (DPI) erlaubt zwecks Filterung und Überwachung nicht nur den Rückgriff auf Header-Informationen, sondern auch die Analyse der Payload, also der zu übertragenden Daten. Diese Analyse kann durchaus legitimen Zwecken dienen: So filtern einige Anbieter, etwa Mobilfunkbetreiber, gewisse Verkehrsarten wie zB die Internettelefonie in ihren Netzen, weil sie zur Nutzung solcher Dienste zusätzliche Gebühren verlangen. Andererseits nutzen aber auch diktatorische Regime rund um den Globus, allen voran China, diese Technik um das Internet zu zensieren.[264]

Was den unverschlüsselten Datenverkehr betrifft, so findet DPI vom Nutzer weitgehend unbemerkt statt. Eigens vorgesehene, äußerst leistungsfähige Hardware ermöglicht es, die

[260] getestet mittels http://dnssec.vs.uni-due.de/.
[261] getestet mittels http://dnssec-debugger.verisignlabs.com/.
[262] http://tools.ietf.org/html/rfc2647#section-3.22.
[263] http://tools.ietf.org/html/rfc2647#section-3.29.
[264] https://netzpolitik.org/2012/deep-packet-inspection-der-unterschied-zwischen-internet-in-diktaturen-und-deutschland-ist-nur-eine-konfigurationsdatei/.

Datenpakete während der Übertragung zusammenzusetzen und deren Inhalt beispielsweise nach verschiedenen Kriterien automatisch zu durchsuchen. Taucht dabei ein zu filternder Inhalt auf, kann die Verbindung unterbrochen und die Kommunikation somit unterbunden werden.[265]

Verschlüsselte Verbindungen lassen sich infolge von DPI einerseits gänzlich unterbinden[266], andererseits stehen auch Methoden zu deren Überwachung zur Verfügung[267]. Der Inhalt lässt sich jedoch nur dann überwachen, wenn im Rahmen der DPI eine Entschlüsselung erfolgen kann. Dies ist im Regelfall nur im Zusammenhang mit SSL-verschlüsselten Verbindungen, wie sie zB für Websiteaufrufe oder E-Mailversand genutzt werden, möglich, nicht jedoch bei VPN-Verbindungen (siehe dazu 6.4). Je nach konkreter Umsetzung kann die Entschlüsselung vom Nutzer mit verschiedenen Mitteln erkannt werden. Die Verschlüsselung der Übertragung von Websites erfolgt unter Heranziehung von Zertifikaten, deren Authentizität durch eine Zertifikatskette vom Browser automatisch überprüft wird. Als Folge der DPI kann es vorkommen, dass aufgrund ungültiger Zertifikate infolge der Entschlüsselung Warnmeldungen im Browser erzeugt werden. Werden hingegen im Rahmen der DPI gültige Zertifikate verwendet, lässt sich mittels Browsererweiterungen oft zumindest feststellen, dass das Zertifikat zwar gültig ist, aber nicht dem Original des Websitebetreibers entspricht. Infolge verschiedener sicherheitsrelevanter Vorfälle bei Zertifizierungsstellen liegt die Vermutung nahe, dass der Grund dieser Vorfälle auch darin liegt, scheinbar ordnungsgemäße Zertifikate zu erlangen, die das Erkennen von Entschlüsselung infolge von DPI erschweren.[268]

6.4. Virtual Private Network, Netzwerktunnel

Ein Virtual Private Network (VPN) ermöglicht es, über das Internet Zugang zu einem entfernten Netzwerk zu erlangen, mit der Wirkung, als wäre man physisch (per Netzwerkkabel) mit diesem Netzwerk verbunden. Je nach Konfiguration kann lediglich Zugang zum VPN vermittelt werden oder aber der gesamte Netzwerkverkehr über das VPN

[265] https://netzpolitik.org/2012/deep-packet-inspection-der-unterschied-zwischen-internet-in-diktaturen-und-deutschland-ist-nur-eine-konfigurationsdatei/.

[266] https://www.techdirt.com/articles/20121217/10222821404/china-tries-to-block-encrypted-traffic.shtml; Es gibt jedoch auch Methoden, um verschlüsselte Kommunikation vor DPI zu verstecken. Das komplette Blockieren von verschlüsselten Verbindungen ist also nicht möglich. http://www.forbes.com/sites/andygreenberg/2012/02/10/as-iran-cracks-down-online-tor-tests-undetectable-encrypted-connections/.

[267] Verschiedene namhafte Hersteller bieten solche Lösungen an, siehe beispielsweise http://software.dell.com/documents/sonicwall-ssl-inspection-datasheet-29063.pdf.

[268] http://heise.de/-1741726.

abgewickelt werden. Das Netzwerk, über das der Nutzer die Verbindung ins VPN herstellt, dient in diesem Fall nur noch der Übertragung der Daten ins VPN.[269]

VPNs lassen sich über verschiedene Standards realisieren, alle modernen VPN-Standards erlauben die Verschlüsselung des Verkehrs zum bzw vom VPN. Diese Verschlüsselung lässt sich zwar per DPI erkennen, jedoch im Normalfall nicht, wie im Fall von verschlüsselten Websiteaufrufen, entschlüsseln, da die zur Verschlüsselung verwendeten Zertifikate dem Betreiber der DPI im Normalfall nicht zur Verfügung stehen. Es ist also nur möglich, verschlüsselte VPN-Verbindungen gänzlich zu unterbinden, wobei auch Gegenmaßnahmen zu VPN-Sperren zur Verfügung stehen.[270]

Im Zusammenhang mit Netzsperren ermöglichen VPN Verbindungen die Umgehung aller Sperrarten, so lange nicht VPN-Verbindungen an sich unterbunden werden. Dies resultiert aus der Tatsache, dass alle Daten vom und zum Internet, inklusive der Namensauflösung über DNS, über das VPN abgewickelt werden und deren Kontrolle dem Access-Provider somit nicht möglich ist.[271]

Viele kommerzielle Anbieter bieten VPN-Services zum Zweck an, Internetverkehr gegenüber dem Access-Provider zu anonymisieren und Sperren zu umgehen. Dies dient einerseits dazu, Zugriff auf Dienste zu erhalten, die vom Anbieter nur in bestimmten Regionen angeboten werden (zB bis vor kurzem Netzflix für Nutzer außerhalb der USA), also Dienste, die vom sogenannten Geoblocking betroffen sind, oder den Zugang zu Diensten sicherzustellen, welche vom Access Provider zB mittels kombinierter IP- und DNS-Sperren blockiert werden.[272]

Neben VPNs existieren verschiedene Protokolltunnelverfahren, welche in Bezug auf die Umgehung von Sperren mit der Funktion eines VPNs vergleichbar sind. Diese seien der Vollständigkeit halber an dieser Stelle erwähnt, im Zuge der weiteren Betrachtung wird jedoch im Rahmen der Umgehungsmaßnahmen nur auf VPNs Bezug genommen.

6.5. Proxy-Server

Ähnlich einem VPN-Netzwerk können auch diverse Proxy-Server zur Umgehung von Netzsperren genutzt werden. Der ursprüngliche Zweck von Proxy-Servern lag darin, in den langsamen Netzen des Modem-Zeitalters Inhalte zwischenzuspeichern und somit deren

[269] http://tools.ietf.org/html/rfc2764.
[270] http://www.greycoder.com/how-hide-vpn-connections/.
[271] http://tools.ietf.org/html/rfc2764.
[272] Beispielsweise bietet hidemyass.com einen solchen VPN-Dienst ab 6,55 US-Dollar an.

schnelleren Abruf zu ermöglichen. Auch wurden und werden Proxys zB häufig in lokalen Netzen (zB Schulen) eingesetzt, um unerwünschte Inhalte zu filtern.[273]

Erfolgt Kommunikation mittels eines Proxy-Servers, wird die Verbindung zwischen Absender und Empfänger nicht direkt hergestellt, sondern der Proxy-Server wird zwischengeschaltet. Dieser übernimmt die Kommunikation quasi im eigenen Namen und leitet die Daten an das Gerät weiter, welches die Dienste des Proxys in Anspruch nimmt. Somit ist es mittels eines außerhalb des Netzes eines Access-Provider liegenden Proxys möglich, Webseiten aufzurufen, welche vom Access-Provider blockiert werden.[274]

Es besteht die Möglichkeit, einen Proxyserver in den Browsereinstellungen einzutragen, wodurch die gesamte Kommunikation über den Proxy geleitet wird. Es gibt jedoch auch Dienste, welche die Proxybenutzung über eine spezielle Website ermöglichen: Der Nutzer ruft dabei diese Website auf, gibt in einem Adressfeld auf dieser Website die gewünschte Adresse ein und bekommt den gewünschten Inhalt dann auf dieser Website angezeigt, ohne etwas an der Konfiguration seines PCs ändern zu müssen[275].

Umgekehrt können Access-Provider auch den Verkehr zu bestimmten Websites über einen Proxy abwickeln, um bestimmte Inhalte zu filtern oder zu verändern (siehe dazu unter 7.4).

Proxys können neben der Umgehung oder Realisierung von Sperren auch der Anonymisierung dienen. So nutzen vor allem in nichtdemokratischen Regimen Dissidenten beispielsweise das TOR Netzwerk, um ihre Spuren zu verschleiern.[276] Auch Proxy-Dienste können mittels DPI geblockt oder, vorausgesetzt sie sind unverschlüsselt, überwacht werden.

Der Unterschied zwischen VPN-Diensten und Proxy-Diensten liegt darin, dass VPN-Dienste auf einer niedrigeren Schicht im OSI-Modell[277] arbeiten. Während VPN protokollunabhängig IP-Pakete transportiert, sind Proxys meist anwendungs- bzw protokollspezifisch.[278]

---

[273] https://kb.iu.edu/d/ahoo.

[274] *Ofcom*, „Site Blocking" to reduce online copyright infringement, S 36ff. (http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf

[275] Diese Dienste werben meistens damit, die Kommunikation zu anonymisieren. Ein Beispiel für einen solchen Dienst ist www.vtunnel.com.

[276] https://www.torproject.org/about/overview.html.en.

[277] Das OSI Modell beschreibt, wie Daten von Host zu Host weitergeleitet werden. Das OSI-Modell beschreibt 7 Netzwerkschichten, wobei jede spezifische Aufgaben erfüllt. *Castelli*, Network Consultants Handbook, S 3 (2001).

[278] *Castelli*, Network Consultants Handbook, S 631 (2001).

6.6. Datei-Hashwert

Ein Datei-Hashwert ermöglicht die eindeutige Identifizierung einer Datei, ähnlich wie ein Fingerabdruck. Ein Hashwert kann mittels verschiedener mathematischer Formeln berechnet werden. Die meisten Berechnungsmethoden liefern als Ergebnis unabhängig von der Dateigröße eine immer gleich lange Zeichenkette (zB 160 Bit lang). Die Eigenheit einer mathematischen Hashberechnung ist, dass diese, so lange die zugrunde liegende Datei nicht verändert wurde, immer zum selben Ergebnis führt. Wird jedoch nur ein einzelnes Bit der Datei manipuliert, führt dies zu einem vollkommen anderen Ergebnis der Hashwertberechnung.[279]

7. Sperrmöglichkeiten

7.1. Vorbemerkungen

Im folgenden Kapitel werden die technisch möglichen Sperrmaßnahmen vorgestellt. Da eine Umgehung von Sperren aus noch auszuführenden technischen Gründen fast immer möglich ist, kann unter dem Terminus „Sperrmaßnahme“ aber keine vollständige Verhinderung des Zugangs zu einer Seite verstanden werden, sondern nur eine möglichst weitgehende Behinderung im Sinne einer Erschwerung der Erreichbarkeit.[280] Im Rahmen der Diskussion rund um das Zugangserschwernisgesetz[281] in Deutschland fand bereits eine ausführliche öffentliche Debatte zu technischen Sperrmaßnahmen und deren juristischer Zulässigkeit statt, welche hier als Grundlage der Erörterungen dient.

Maßnahmen zur Blockierung einer Internetseite sollen gemäß der Rechtsprechung des EuGH als ultima ratio nur dann ergriffen werden, wenn das Löschen der beanstandeten Inhalte nicht möglich ist, also sowohl Aufforderungen an den Content-Anbieter als auch den Host-Provider folgenlos geblieben sind.

So bieten Portale wie Youtube, welche nicht wie kinox.to auf rechtsverletzende Zurverfügungstellung von Inhalten „spezialisiert“ sind, für Einzelfälle Formulare an, um

[279] https://cseweb.ucsd.edu/~mihir/cse207/w-hash.pdf.
[280] *Frey/Rudolph*, Rechtsgutachten zur Evaluierung des „Haftungsregimes für Host und Access-Provider im Bereich der Telemedien“, Rz 140.
[281] Ziel des Zugangserschwernisgesetzes war es, auf Grundlage von IP-, DNS- und eventuell auch Proxy-basierten Filtern den Zugang zu Kinderpornographie im Internet einzuschränken. Das Zugangserschwernisgesetz wurde als Folge der Ablehnung von Sperrmaßnahmen durch die Öffentlichkeit zugunsten des Grundsatzes „Löschen statt Sperren“ und aufgrund der Inneffektivität von Sperren noch vor dessen Inkrafttreten wieder aufgehoben.

Urheberrechtsverstöße zu melden[282]. Auch eine Vorabprüfung von auf Youtube hinaufgeladenen Inhalten ist mittels des Systems „Content ID" möglich, welches die Inhalte vor ihrer Veröffentlichung automatisiert mit einer Datenbank abgleicht, um urheberrechtlich geschütztes Material zu erkennen. Rechteinhaber haben im Vorfeld die Möglichkeit zu bestimmen, wie im Fall einer Verletzung ihrer Rechte vorgegangen werden soll:
So kann die Hintergrundmusik eines Videos stummgeschaltet werden, es kann eine komplette Sperre desselben veranlasst werden, das Video kann durch Schaltung von Anzeigen monetarisiert werden oder der Rechteinhaber kann sich auf eine Beobachtung der Zugriffszahlen beschränken. Alle diese Möglichkeiten können auch länderspezifisch konfiguriert werden, sodass das Sperren in einem Land und das Monetarisieren in einem anderen möglich wäre.[283]

Sollte der Content-Anbieter auf Löschanforderungen nicht reagieren, besteht die Möglichkeit, stattdessen den Host-Provider um Löschen der Inhalte bzw der kompletten Seite zu ersuchen. Diesem steht nämlich zwar nach dem E-Commerce-Gesetz, ähnlich einem Access-Provider, eine Haftungsfreistellung zu. Erlangt der Host-Provider jedoch Kenntnis von rechtswidrigen Inhalten, muss er im Sinne einer Löschung oder Sperrung tätig werden, um sich weiterhin auf seine Haftungsfreistellung berufen zu können (§ 17 Abs 1 Z 2 E-Commerce-Gesetz).

Bleibt die Inanspruchnahme von Content-Anbieter und Host-Provider ohne Erfolg und wird zum Mittel von Internetsperren gegriffen, können als Sperrkriterium einerseits die Kommunikationsinhalte sowie andererseits die Kommunikationsumstände dienen.[284] Erstere können durch eine Deep Packet Inspection untersucht werden, für letztere sind IP-, DNS- und Proxy-Sperren maßgeblich. Eine Filterung nach Kommunikationsinhalten erfolgt mittels DPI auf Grundlage diverser Filterkriterien, wodurch die übertragenen Daten auf zu sperrende Inhalte überwacht werden, eine Filterung nach den Kommunikationsumständen kann an der Domain, an der IP-Adresse, aber auch an einer konkreten URL[285] anknüpfen.

[282] siehe https://www.youtube.com/copyright_complaint_form.
[283] Siehe näher zu Content ID unter https://support.google.com/youtube/answer/2797370.
[284] *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access Provider – Technisches Gutachten, S42.
[285] Der Uniform Resource Locator (URL) dient der Lokalisierung einer bestimmten Ressource auf einem Server. Im WWW setzt sich dieser aus der Domain (zB www.univie.ac.at) sowie der konkreten Pfadangabe (zB /dokumente/info.pdf) zusammen (im Beispiel wäre die komplette URL also www.univie.ac.at/dokumente/info.pdf).

Generell kann auch noch danach unterschieden werden, dass IP- oder Proxy-Sperren eine Kommunikation vollständig verhindern, wohingegen DNS-Sperren und Deep Packet Inspection die Kommunikation stören.[286]

7.2. DNS-Sperren

7.2.1. Grundlagen

Im Rahmen von DNS-Sperren werden die DNS-Server derart manipuliert, dass sie nicht mehr jene Datensätze als Antwort liefern, die sie von dem für den zu sperrenden Domainnamen zuständigen Nameserver erhalten. Stattdessen antwortet der DNS-Server auf Anfragen nach der gesperrten Domain, dass diese nicht existiert oder liefert eine falsche oder verfälschte IP-Adresse[287] als Antwort. [288]

DNS-Sperren lassen sich für Provider relativ kostenschonend umsetzen. Auch wenn die vom Provider benutzte Infrastruktur keine dezidierte, benutzerfreundliche Möglichkeit zur Sperre bietet, ist die Umsetzung durch Eingriff in Konfigurationsdateien relativ einfach vorzunehmen. [289] Ein kurzer Neustart der Systeme um eine neue Konfiguration zu übernehmen kann uU notwendig sein, der Erwerb neuer Hardware ist in der Regel nicht erforderlich, außer es handelt sich um einen kleinen Access-Provider, welcher keinen eigenen DNS-Server betreibt.[290]

Sobald DNSSEC (siehe dazu näher unter 6.2) weitflächig etabliert sein wird, ist die Implementierung von DNS-Sperren nicht mehr möglich.[291]

7.2.2. Umgehung

Reine DNS-Sperren lassen sich mit geringem Aufwand umgehen. Der IT-Sicherheitsforscher *Hannes Federrath* bezeichnete diese im Rahmen eines Expertenhearings vor dem deutschen Bundestag als „völlig wirkungslos“.[292] Es reicht aus, statt der DNS-Server des Providers alternative DNS-Server zu benutzen. Zahlreiche Anbieter wie Google oder OpenDNS bieten eine kostenlose DNS-Infrastruktur an, welche derzeit nicht von Sperrverfügungen betroffen ist. Selbst technisch unbedarfte Nutzer können durch eine kurze Google-Recherche im Stande

[286] *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access Provider – Technisches Gutachten, S46.
[287] Die UPC-DNS-Server Antworten aufgrund der vom VAP durchgesetzten Sperren auf Anfragen nach kinox.to mit der nicht existenten IP-Adresse „0.0.0.0“.
[288] *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access Provider – Technisches Gutachten, S52.
[289] *Ofcom*, „Site Blocking“ to reduce online copyright infringement, S 31ff.
[290] *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access Provider – Technisches Gutachten, S52.
[291] *Ofcom*, „Site Blocking“ to reduce online copyright infringement, S 43.
[292] http://www.zeit.de/online/2009/08/internetsperren-leyen.

sein, die verwendeten DNS-Server innerhalb weniger Minuten zu ändern. Eine Sperre alternativer DNS-Dienste seitens des Access-Providers wäre technisch möglich[293], wurde in der aktuellen Diskussion aber nicht angedacht. Nach mE wäre sie im Hinblick auf die dazu fehlende Rechtsgrundlage und die daraus resultierende Verletzung der Informationsfreiheit jedenfalls ausgeschlossen.

Die Nutzung eines VPN-Dienstes oder Proxyservers ist bei reinen DNS-Sperren zwar auch zur Umgehung geeignet, jedoch oft mit zusätzlichen Kosten verbunden. Solange keine weiteren Maßnahmen wie IP-Sperren implementiert sind, hat die Benutzung alternativer DNS-Server keine Nachteile gegenüber der Umgehung per VPN oder Proxy.

Seitens des Content-Anbieters besteht im Fall von DNS-Sperren die Möglichkeit, alternative Domainnamen zu registrieren.[294] Je nach Formulierung der Sperrverfügung kann es notwendig werden, in Bezug auf diese alternativen Adressen eine neuerliche einstweilige Verfügung zu erwirken.
Wie auch der GA in seinen Schlussanträgen ausgeführt hat[295], können in einem solchen Fall Nutzer zwar über Suchmaschinen von der neuen Adresse Kenntnis erlangen, je mehr alternative Adressen jedoch ebenfalls einer Sperre unterliegen, umso schwieriger wird die Recherche nach noch nicht gesperrten Adressen.

7.2.3. Rechtliche Beurteilung

Die deutsche Rechtsprechung erachtet einen Arbeitsaufwand von zwei Stunden für die Sperre von zwei Webseiten mit Blick auf das Grundrecht der unternehmerischen Freiheit als zumutbar, ebenso müssten der Aufwand für einen Entscheidungsfindungsprozess bzw die Erstellung einer Hinweisseite, genauso wie der Neustart der Systeme sowie die Beantwortung von etwaigen Kundenanfragen wegen Sperren hingenommen werden, soweit damit keine erhebliche Belastung verbunden sei.[296]

Nach mE stellen diese DNS-Sperren im Hinblick auf das Grundrecht der Informationsfreiheit das gelindeste zur Verfügung stehende Mittel dar, um Sperren umzusetzen. Allerdings sind sie aufgrund der simplen Umgehungsmöglichkeiten relativ wirkungslos. Die Differenzierung

[293] *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access Provider – Technisches Gutachten, S53.
[294] In Bezug auf Seiten wie Pirate Bay oder Wikileaks erfolgt die Zugänglichmachung oft auch in Form einer Spiegelung der Seite. Diese wird von Personen, welche jeglichen Eingriff in den Zugang zu Websites als Zensur betrachten, oft ohne Zutun des Content-Anbieters vorgenommen. Zahlreiche solcher Spiegelungen von Pirate Bay finden sich unter http://proxybay.info/. Zur Spiegelung durch die Community siehe weiterführend *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access Provider – Technisches Gutachten, S53.
[295] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 101.
[296] *Frey/Rudolph*, Rechtsgutachten zur Evaluierung des „Haftungsregimes für Host und Access-Provider im Bereich der Telemedien“, Rz 167.

nach Domainnamen erlaubt es im Gegensatz zu IP-Sperren, gezielt ausschließlich rechtsverletzende Seiten einer Sperre zu unterwerfen, weswegen die Gefahr eines „Over-Blockings“[297] deutlich geringer erscheint. Davon abgesehen bleibt das Problem aufrecht, ob eine DNS-Sperre aufgrund teils legaler Inhalte überhaupt zulässig sein kann (siehe dazu unter 5).

Zwar fordert der EuGH, dass eine Sperrmaßnahme zur Folge haben muss, dass „*die Internetnutzer, die die Dienste des Adressaten der Anordnung in Anspruch nehmen, zuverlässig davon abgehalten werden, auf die ihnen unter Verletzung des Rechts des geistigen Eigentums zugänglich gemachten Schutzgegenstände zuzugreifen*“ [298] . Ob diese „Zuverlässigkeit“ im erforderlichen Ausmaß tatsächlich gegeben ist, könnte, wie dargestellt, freilich bezweifelt werden. Aufgrund der Tatsache, dass der Eingriff in das Grundrecht der unternehmerischen Freiheit aber dem Grundsatz der Verhältnismäßigkeit entspricht, die Gefahr eines unverhältnismäßigen Eingriffs in die Informationsfreiheit äußerst gering ist und dass trotz der Inneffektivität von DNS-Sperren der Zugang zu gesperrten Informationen, wie vom EuGH gefordert, „zumindest erschwert“[299] wird, sind diese mE dem Access-Provider zumutbar.

7.3. IP-Sperren

7.3.1. Grundlagen

Ist eine IP-Adresse von einer Sperre betroffen, so werden Anfragen an diese schlicht nicht mehr geroutet. Anfragen landen in einer sogenannten NULL-Route, werden also vom Access-Provider verworfen.[300] Im Zusammenhang mit IP-Sperren besteht immer das Problem von „Kollateralschäden“: Dies resultiert aus dem Umstand, dass, wie bereits erörtert, oft mehrere Seiten unter derselben IP-Adresse angeboten werden. Wird die IP gesperrt, weil eine dieser Seiten rechtsverletzend ist, können alle Seiten nicht mehr aufgerufen werden.[301] ZB kam es im Zuge einer Sperre von drei Pornoseiten durch einen deutschen Access-Provider zur ungewollten Sperre von fast 3,5 Millionen Internetseiten, darunter Seiten von Forschungskongressen und Industrieunternehmen.[302]

[297] Unter Over-Blocking ist zu verstehen, dass infolge einer Sperre auch rechtmäßige Inhalte nicht mehr zugänglich sind.
[298] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 63.
[299] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 63.
[300] *Ofcom*, „Site Blocking“ to reduce online copyright infringement, S 28.
[301] *Heidinger*, Die zivilrechtliche Inanspruchnahme von Access-Providern auf Sperre urheberrechtsverletzender Webseiten, ÖBl 2011, 37.
[302] Siehe dazu weiterführend http://www.spiegel.de/netzwelt/web/0,1518,506143,00.html.

Die Frage nach den Kosten der Implementierung von IP-Sperren lässt sich nicht generell beantworten. Wichtiger Kostenfaktor ist einerseits die Netzwerktopologie des Access-Providers, andererseits auch die Anzahl der zu sperrenden Adressen. Lässt sich die Sperre von wenigen Adressen meist mit bestehender Hardware relativ einfach umsetzen, so erfordern lange Sperrlisten mit hoher Wahrscheinlichkeit Neuanschaffungen, um keine Geschwindigkeitsverluste im Netzwerk zu verursachen.[303]

Die Umsetzung von IP-Sperren kann meist nicht sofort, sondern erst in einem vom Access-Provider regelmäßig angesetzten Wartungsfenster erfolgen, da erstens mögliche negative Auswirkungen der Sperre analysiert werden müssen und zweitens Eingriffe in Routing-Tabellen mit einem Neustart der betroffenen Hardware verbunden sein können, was kurze Ausfälle für die Nutzer nach sich zieht und deswegen nur Nachts vorgenommen wird.[304]

Im Rahmen von IP-Sperren sollte möglichst eine Eingrenzung der Sperre auf jenen Port, also jenen Dienst, erfolgen, über welchen die zu sperrende Webseite angeboten wird, da es sonst zB zu Störungen des E-Mailverkehrs kommen kann, wenn auf dem gleichen Server auch ein Mailserver betrieben wird.[305]

7.3.2. Umgehung

Die Umgehung von IP-Sperren von Seiten des Content-Anbieters ist simpel. Vorausgesetzt, die IP-Sperre ist nicht mit einer DNS-Sperre gekoppelt, kann der Content-Anbieter schlicht die IP-Adresse wechseln und die geänderte IP im DNS eintragen. Dies hat zur Folge, dass Endnutzer, abhängig davon wie lange DNS-Einträge von den DNS-Servern zwischengespeichert werden (siehe dazu 6.2), meist schon nach kurzer Zeit die von der Sperre betroffene Seite wieder aufrufen können, ohne zB einen geänderten Domainnamen recherchieren zu müssen. Weiters besteht die Möglichkeit, mit einem Domainnamen mehrere IP-Adressen zu assoziieren, sodass die Sperre einer einzelnen IP keine negativen Auswirkungen auf die Erreichbarkeit der Seite hat.[306]

Für Endnutzer besteht die Möglichkeit, die Sperren mittels Proxy-Servern oder VPN-Diensten zu umgehen.

[303] *Ofcom*, „Site Blocking“ to reduce online copyright infringement, S 28ff.
[304] *Ofcom*, „Site Blocking“ to reduce online copyright infringement, S 28ff.
[305] *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access Provider – Technisches Gutachten, S55.
[306] *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access Provider – Technisches Gutachten, S55 sowie *Ofcom*, „Site Blocking“ to reduce online copyright infringement, S29.

Gegen die Umgehung der Sperren durch die Content-Anbieter können sich Rechtsinhaber im Rahmen der Sperrverfügung vorbehalten, dem Access-Provider geänderte IP-Adressen mitzuteilen, um diese ebenfalls zu sperren.

7.3.3. Rechtliche Beurteilung

Zwar stellen IP-Sperren aufgrund der höheren Hürden in Bezug auf deren Umgehung mE ein geeigneteres Mittel als DNS-Sperren dar, um Sperrverpflichtungen umzusetzen. Verglichen mit DNS-Sperren ist die Gefahr des „Over-Blockings" jedoch, wie unter 7.3.1 ausgeführt, deutlich höher. Infolgedessen muss bei IP-Sperren bei einer Abwägung zwischen dem Urheberrechtsschutz und der Informationsfreiheit beachtet werden, dass die potentielle Begleiterscheinung des Sperrens von unbeteiligten, rechtmäßigen Seiten zu einem Ungleichgewicht führen kann, die das Sperren nach der derzeitigen Rechtslage als unverhältnismäßig erscheinen lässt.

Im Hinblick auf den Schutz der unternehmerischen Freiheit der Access-Provider hängt die Verhältnismäßigkeit davon ab, ob aus technischen Gründen Neuanschaffungen zur Implementierung der IP-Sperren notwendig sind. Ist das nicht der Fall, so sieht die deutsche Rechtsprechung einen Zeitaufwand von 1,5 bis 2 Stunden zur Implementierung als angemessen an.[307] Sollte diese Abwägung allerdings unverhältnismäßig erscheinen, kann dieses Ergebnis allenfalls noch durch eine zusätzliche Überlegung relativiert werden: So könnte eine Übernahme der anfallenden Kosten durch die Rechteinhaber, wie auch der Generalanwalt argumentiert[308], doch noch dazu führen, die Verhältnismäßigkeit von IP-Sperren zu gewährleisten.

Nicht außer Acht gelassen werden sollte der Umstand, dass es in Bezug auf IP-Sperren notwendig ist, neben einer im Verfügungsantrag vorbehaltenen Sperre weiterer IP-Adressen auch regelmäßig zu überprüfen, ob bereits gesperrte IP-Adressen noch immer von der zu sperrenden Seite genutzt werden und ob zwischenzeitlich weitere, eventuell nicht rechtsverletzende Seiten unter dieser IP angeboten werden. Das OLG Köln führt dazu aus, dass dies jedenfalls zu einer Bindung von personellen Kapazitäten des Access-Providers führen würde.[309]

[307] *Frey/Rudolph*, Rechtsgutachten zur Evaluierung des „Haftungsregimes für Host und Access-Provider im Bereich der Telemedien", Rz 156.
[308] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 106.
[309] OLG Köln 18.07.2014, 6 U 192/11 S 51.

Obwohl IP-Sperren mehr als DNS-Sperren dazu geeignet erscheinen, „zuverlässig“[310] den Zugang zu rechtsverletzenden Seiten zu verhindern, bin ich der Meinung, dass diese in Folge einer Abwägung zwischen Urheberrechtsschutz und unternehmerischer Freiheit sowie Informationsfreiheit nur in jenen Fällen dem Access-Provider zumutbar sind, in denen bewiesen ist, dass eine IP-Adresse ausschließlich von der zu sperrenden Seite verwendet wird. Darüber hinaus müsste der Access-Provider vom Rechteinhaber für seine Aufwendungen, insbesondere das regelmäßige Überprüfen bereits gesperrter IPs, entschädigt werden.

7.4. Proxy-Sperren

7.4.1. Grundlagen

Wie bereits erörtert, können Proxy-Server einerseits der Umgehung von Sperren dienen, andererseits können sie von Access-Providern auch zur Implementierung von Sperren genutzt werden. Die technischen Gegebenheiten von Proxy-Servern ermöglichen dabei vorrangig das Filtern von Webtraffic, zur Filterung von beispielsweise Bittorrent sind sie technisch nicht geeignet. Ebenso können in der Regel keine verschlüsselten Verbindungen mittels Proxy gefiltert werden bzw würde die dazu notwendige Entschlüsselung unzweifelhaft einen unverhältnismäßigen Eingriff in das Kommunikationsgeheimnis und den Schutz personenbezogener Daten darstellen. In Bezug auf die Nutzung zu Sperrzwecken ist dabei grundsätzlich an zwei Szenarien zu denken[311]:

- Einerseits kann die gesamte Abwicklung des Netzwerkverkehrs über einen Proxy erfolgen. Resultat dessen ist, dass die gesamte Kommunikation der Nutzer überwacht und gefiltert werden kann. Die Einrichtung eines solchen Proxys kann nicht unerhebliche Kosten verursachen, da entsprechend leistungsfähige Hardware notwendig ist, um Geschwindigkeitsverluste zu vermeiden. Das Filtern des gesamten Netzwerkverkehrs birgt die Gefahr extensiven „Over-Blockings“.
- Andererseits kann nur die Kommunikation zu bestimmten IP-Adressen über einen Proxy umgeleitet werden. Als Alternative zu einer kompletten IP-Sperre ermöglicht

[310] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) Rz 63.
[311] Die technischen Grundlagen in Bezug auf Proxy basierte Filter wurden der Präsentation von Prof. Dr. Hannes Federrath, abrufbar unter http://svs.informatik.uni-hamburg.de/publications/2009/2009-04-23KoelnFederrath.pdf, entnommen.

eine solche Lösung das gezielte Blockieren rechtswidriger Inhalte, ohne dass von dieser Maßnahme auch rechtmäßige Inhalte betroffen sind.[312]

Zur Identifizierung rechtswidriger Inhalte stehen, unabhängig davon, ob ein Proxy nur für bestimmte IPs oder den gesamten Netzwerkverkehr eingerichtet wird, verschiedene Möglichkeiten zur Verfügung:

- In Form eines Blacklist/Whitelist-Verfahrens könnte, wenn mehrere Seiten unter derselben IP-Adresse betrieben werden, eine dieser Seiten komplett blockiert und der Zugang zu allen anderen Seiten ungehindert gewährleistet werden.
- Mithilfe einer Sperrliste könnten gewisse Unterseiten gezielt blockiert werden (zB http://zusperren.at/rechtsverletzend.html). Wird die Unterseite in der Struktur der Website jedoch verschoben (im genannten Beispiel zB nach http://zusperren.at/rechtsverletzend2.html), wäre ein Adaptieren der Liste notwendig.
- Ebenso könnte eine Filterung mithilfe einer Stichwortliste erfolgen. Diese könnte eine Filterung auf Grundlage des Pfads einer Unterseite (http://zusperren.at/stichwort/rechtsverletzend.html) vornehmen oder zur Filterung den Inhalt der Seiten nach Stichwörtern durchsuchen[313]. Nachteil an dieser Möglichkeit ist freilich, dass es infolge der Filterung zu Fehltreffern und somit zum „Over-Blocking" legaler Inhalte kommen könnte.
- Geht es um den Zugriff auf Dateien, so können diese auch mit Hilfe von Hash-Werten identifiziert und blockiert werden.

  Im Zusammenhang mit Streaming wäre diese Möglichkeit mE technisch nur schwer umzusetzen, sie kann aber eine effektive Möglichkeit bieten um zB Bilder oder Musikdateien zu blockieren. Die Nachteile einer Identifizierung mittels Hashwert, nämlich dass sich dieser verändert, wenn nur ein Bit der Datei geändert wird, wurden unter 6.6 schon näher erörtert.

Im Unterschied zu IP- bzw DNS-Sperren müssen Access-Provider die Infrastruktur zur Realisierung von Proxy-basierten Sperren in der Regel erst zukaufen. Zwar betreiben Access-Provider meist auch Proxy-Server, diese sind aber technisch nicht für die Implementierung

[312] In der deutschen Literatur wird diese Sperrmöglichkeit auch oft als „Hybride Sperre" bezeichnet, da zwecks Umleitung des Verkehrs zur zu sperrenden Seite über den Proxy eine IP-Umleitung, ähnlich einer IP-Sperre, eingerichtet wird.

[313] Zu beachten ist dabei, dass eine solche Filterung des Inhalts im Gegensatz zur DPI nicht anhand der übertragenen Daten erfolgt, sondern der Proxy-Server die Seite schlicht „für sich selbst" abruft und danach analysiert und als Folge dieser Analyse die Entscheidung trifft, ob er die Seite für den Nutzer ebenfalls aufruft.

von Sperren ausgelegt.[314] Je nach Umfang der Filterung können hohe Kosten entstehen, die umfangreiche Filterung zahlreicher Seiten könnte die Kapazität eines ganzen Rechenzentrums erfordern.[315] Je nach konkreter Netzwerktopologie könnte es auch notwendig sein, diese zu ändern, um eine Umleitung über einen Proxy zu ermöglichen. Außerdem ist es naheliegend, dass Access-Provider zur Verwaltung umfangreicher Sperrlisten Personal einstellen müssten.[316]

7.4.2. Umgehung

Proxy-basierte Filter können seitens der Benutzer einerseits durch die Verwendung eines VPNs, andererseits durch Verwendung eines Proxys umgangen werden.

Ob Content-Anbieter ihrerseits Schritte setzen können, die die Filtermaßnahmen des Proxys umgehen, hängt von der Filtermethode ab. Proxys, die nur bestimmte IPs filtern, können durch Änderung der IP-Adresse relativ einfach ausgehebelt werden.
Filtermethoden, die auf Sperrlisten oder Stichwortlisten beruhen, können durch Verändern der Struktur der betroffenen Website bzw durch das Vermeiden der gefilterten Stichwörter umgangen werden. Hash-basierte Filter lassen sich aushebeln, indem eine Datei nur geringfügig geändert wird, uU reicht dazu ein neuerliches Abspeichern aus.

7.4.3. Rechtliche Beurteilung

Im Hinblick auf die rechtliche Beurteilung muss mE wieder nach Proxys zur generellen Filterung des gesamten Netzwerkverkehrs und solchen, welche nur den Verkehr zu bestimmten IP-Adressen filtern, unterschieden werden:

- Proxys, welche den gesamten Netzwerkverkehr filtern, sind meiner Meinung nach aufgrund des Urteils Scarlet Extended[317] von vornherein unzulässig und somit auch nicht den Access-Providern zumutbar. Ein solcher Proxy stellt nämlich im Sinne dieses Urteile ein Filtersystem dar, welches unterschiedslos auf alle Nutzer anwendbar ist und zeitlich unbegrenzt auf Kosten des Access-Providers zu betreiben wäre, um präventiv Urheberrechtsverletzungen zu verhindern. Die zwangsweise Einrichtung eines solchen Proxys würde Diensteanbietern generelle Überwachungspflichten in Bezug auf den gesamten Verkehr mit Websites auferlegen, was aber von Art 15 Abs 1 E-Commerce Richtlinie verboten ist.

[314] Pursch/Bär, Sperrverfügung gegen Internet-Provider, S18f.
[315] OLG Köln 18.07.2014, 6 U 192/11 S 53.
[316] *Frey/Rudolph*, Rechtsgutachten zur Evaluierung des „Haftungsregimes für Host und Access-Provider im Bereich der Telemedien“, Rz 177.
[317] EuGH 24.11.2011, C-70/10 (Scarlet Extended).

Auch die Gefahr eins Eingriffs in das Grundrecht der unternehmerischen Freiheit wäre mE gegeben. Es scheint nämlich fraglich, ob eine Abwägung zwischen dem Urheberrechtsschutz und der unternehmerischen Freiheit die Einrichtung eines solchen Systems gestatten würde, da die erheblichen Kosten den Eingriff für Access-Provider als unverhältnismäßig erscheinen lassen könnte.

Weiters besteht die Möglichkeit, dass infolge ungenauer Filterung ein unverhältnismäßiger Eingriff in die Informationsfreiheit erfolgen könnte. Zudem wäre – je nach Konfiguration des Systems – auch das Recht auf Schutz personenbezogener Daten beeinträchtigt, falls unberechtigte Zugriffsversuche samt IP-Adressen gespeichert würden. Auch erscheint fraglich, ob die Verarbeitung der IP-Adresse und weiterer Verkehrsdaten, insbesondere der URL, mit dem Kommunikationsgeheimnis des TKG vereinbar sind. Diese Daten dürfen ja nur verarbeitet werden, wenn dies zur Erbringung des Kommunikationsdienstes notwendig ist[318] (siehe dazu auch 3.4.3).

- Auch der Einsatz von Proxys zur gezielten Filterung des Zugriffs auf einzelne IP-Adressen ist nach meiner Auffassung einem Access-Provider nicht zumutbar. Zwar liegt kein Filtersystem im Sinne des Urteils Scarlet Extended[319] vor, da nicht der gesamte Netzwerkverkehr des Providers gefiltert wird, sondern nur die Kommunikation zu spezifischen IP-Adressen einer Filterung unterliegt.

  Problematisch könnte aber der Eingriff in das Recht auf den Schutz personenbezogener Daten der Internetnutzer sein, da im Zuge einer Filterung durch den Proxy zwangsläufig die IP-Adressen der Internetnutzer verarbeitet werden müssen, welche einen Rückschluss auf den individuellen Nutzer zulassen. Ebenso ist es fraglich, ob die Verarbeitung von Verkehrsdaten mit dem Kommunikationsgeheimnis des TKG vereinbar ist. Die etwaig hohen Einrichtungskosten sprechen ebenfalls gegen die Zumutbarkeit dieser Maßnahme, die deutsche Rechtsprechung sieht insbesondere die Anschaffung von Hardware, das Einstellen von zusätzlichem Personals und notwendige Änderungen an der Netzwerktopologie als Grenzen der Zumutbarkeit.[320] Ein finanzieller Ausgleich der

[318] *Kassai*, "Location Based Services" im Gefüge des Datenschutzrechts, MR 2004, 443.
[319] EuGH 24.11.2011, C-70/10 (Scarlet Extended).
[320] *Frey/Rudolph*, Rechtsgutachten zur Evaluierung des „Haftungsregimes für Host und Access-Provider im Bereich der Telemedien“, Rz 177.

Rechteinhaber[321] könnte mE allenfalls das Kostenargument entkräften, aber nicht dazu führen, die Zumutbarkeit der Maßnahme zu bejahen.

7.5. Deep Packet Inspection

7.5.1. Vorbemerkungen

Der Bereich der Deep Packet Inspection wurde im Zuge der Diskussion des Zugangserschwernisgesetztes nicht behandelt. Auch im Rahmen der aktuellen Sperrverfügungen ist DPI ein bislang wenig diskutiertes Thema. Da jedoch vermutet wird, dass zumindest einige Access-Provider DPI zum Netzwerkmanagement einsetzen und diese Infrastruktur theoretisch auch für Sperren eingesetzt werden kann[322], soll DPI der Vollständigkeit halber kurz dargestellt werden.

Die grundsätzliche Frage, ob die Installation von DPI-Equipment in Österreich überhaupt zulässig ist, kann aufgrund deren Komplexität im Rahmen dieser Arbeit nicht abschließend gekärt werden. Zu dieser Problemstellung soll hier auf die Master Thesis des Absolventen des Jahrgangs 2012/13 *Phillipp König* verwiesen werden, welcher schlussfolgerte, dass die „*Frage, ob DPI eine Verletzung des verfassungsmäßig gewährleisteten Fernmeldegeheimnisses gem Art 10a StGG bzw dessen einfachgesetzlicher Ausgestaltung in § 93 TKG ist, [...] für den Fall, dass der Benutzer seine Zustimmung nicht erteilt hat, mit ja beantwortet werden [kann] [...]*". Die Einrichtung einer DPI sie also nur dann zulässig, wenn die betroffenen Nutzer zustimmen.[323]

7.5.2. Grundlagen

Die Technologie der Deep Packet Inspection ermöglicht das Untersuchen aller Netzwerkpakete im Hinblick auf deren Header- und deren Payload-Informationen, umfasst sind also sowohl Adressinformationen (Verkehrsdaten) als auch der Inhalt des Netzwerkpakets. Ist ein Paket Teil einer E-Mail-Nachricht oder eines privaten Chats, sind von einer solchen Analyse folglich Inhaltsdaten betroffen.[324]

Wird Deep Packet Inspection zur Filterung von Inhalten eingesetzt (so wäre zB das generelle Filtern von Filmstreams denkbar, aber auch nur das gezielte Blocken bestimmter Inhalte von

[321] GA 26.11.2013, C-314/12 (UPC Telekabel Wien) Rz 106.
[322] So forderten zB Rechteinhaber im Rahmen eines Verfahrens vor dem OLG Köln die Heranziehung von DPI zu Filterzwecken. OLG Köln 18.07.2014, 6 U 192/11 S 44. Auch *Stadler/Strass* sprechen DPI in ihrem Aufsatz zumindest als eine der zur Verfügung stehenden Optionen kurz an. *Stadler/Strass*, Website-Blockaden gegen Online-Piraterie?, ecolex 2013,292.
[323] *König*, Deep Packet Inspection und das Kommunikationsgeheimnis, S 64.
[324] *Ofcom*, „Site Blocking" to reduce online copyright infringement, S 39.

einer Website wäre möglich) und wird ein zu filternder Inhalt entdeckt, kann ein Reset-Befehl in die Verbindung eingeschleust werden, welcher zu deren Abbruch führt.[325]

Da DPI den gesamten Netzwerkverkehr nach den vorgegebenen Filterkriterien durchsucht, ist es notwendig, eine genaue Konfiguration der Filterkriterien vorzunehmen um „Over-Blocking" zu verhindern. Ob jedoch eine derart genaue Konfiguration überhaupt möglich ist, sodass keinerlei Daten fälschlicherweise blockiert werden, ist mE äußerst fraglich.

Verschlüsselte Verbindungen müssen entschlüsselt werden, um mittels DPI analysiert werden zu können. Siehe dazu näher oben unter 6.3.

7.5.3. Umgehung

Die Frage nach der Umgehung von DPI seitens der Content-Anbieter kann nicht generell beantwortet werden. Ob dies möglich ist, hängt immer von der konkreten Konfiguration der DPI ab. Ist sie zB nur darauf ausgelegt, Verkehr mit spezifischen IP-Adressen zu filtern, kann sie durch Änderung der IP seitens des Content-Anbieters genauso leicht umgangen werden wie eine klassische IP-Sperre. Werden jedoch alle Netzwerkpakete nach gewissen Kriterien gefiltert, kann es, je nachdem, wie strikt die Konfiguration ausgelegt ist, zu einer Situation kommen, in der eine Umgehung durch den Content-Anbieter unmöglich wird. [326]

Von Seiten der Benutzer kann DPI wiederum durch das Nutzen von VPN- oder Proxydiensten umgangen werden. In diesem Zusammenhang ist jedoch darauf hinzuweisen, dass es theoretisch möglich ist, durch die DPI auch VPN- und Proxyverbindungen zu unterbinden.

7.5.4. Rechtliche Beurteilung

Nach mE sprechen schwerwiegende Argumente gegen die Verhältnismäßigkeit des DPI-Einsatzes zu Sperrzwecken, weswegen DPI jedenfalls nicht als Sperrmaßnahme angeordnet werden darf. Eine umfassende Darstellung und Erörterung der Verhältnismäßigkeit, wie ich sie im Rahmen dieser Arbeit bei den anderen Sperrmethoden vorgenommen habe, erübrigt sich angesichts der folgenden, gewichtigen, negativen Argumente:

- Ein DPI-Filtersystem stellt ein unzulässiges Filtersystem iS der Entscheidung Scarlet-Extended[327] dar.

[325] *Ofcom*, „Site Blocking" to reduce online copyright infringement, S 39f.
[326] *Ofcom*, „Site Blocking" to reduce online copyright infringement, S 40f.
[327] EuGH 24.11.2011, C-70/10 (Scarlet Extended).

- Die Installation und Wartung von DPI-Filter-Infrastruktur wäre mit erheblichen Kosten für den Access-Provider verbunden. Es läge somit jedenfalls ein unverhältnismäßiger Eingriff in das Grundrecht der unternehmerische Freiheit vor.
- Eine umfassende Überwachung von Verkehrs- und Inhaltsdaten stellt einen schwerwiegenden Eingriff in das Recht auf den Schutz personenbezogener Daten dar.
- Ebenso ist eine umfassende Überwachung von Verkehrs- und Inhaltsdaten als schwerwiegender Eingriff in das Kommunikationsgeheimnis bewerten.
- Die Möglichkeit des DPI-Einsatzes zur Erfüllung eines Erfolgsverbots wird außerdem durch den Umstand relativiert, dass eine Zustimmung der Nutzer zur DPI notwendig ist (siehe dazu unter 7.5.1). Nach mE müsste sich diese Zustimmung aufgrund des Wortlauts und Schutzzwecks des § 93 Abs 3 TKG auch explizit auf den Einsatz zu Sperrzwecken beziehen. Es scheint äußert zweifelhaft, dass Nutzer eine solche Einwilligung erteilen würden, gerade auch aufgrund der Tatsache, dass eine solche Zustimmungsaufforderung wohl ein großes Medienecho erzeugen würde.

8. Schlusswort

Im Hinblick auf die weitere Rechtsentwicklung bleibt es spannend, ob die Rechteinhaber gewillt sind, die Frage nach der Zumutbarkeit der konkreten Sperrmaßnahmen einer Klärung zuzuführen, indem sie Zwangsstrafen gegen die betroffenen Access-Provider beantragen oder ob sich die Erkenntnis durchsetzt, dass aufgrund der mannigfaltigen Umgehungsmöglichkeiten aller Sperrmaßnahmen ein Umdenken stattfinden sollte.

Die Erfahrungen im Zusammenhang mit der Schließung von kino.to haben gezeigt, dass selbst strafrechtliches Vorgehen gegen Betreiber rechtsverletzender Seiten bestenfalls einen Kurzzeiteffekt nach sich zieht. Die enormen Einnahmemöglichkeiten im Rahmen der Piraterie lassen den Abschreckungseffekt schnell verblassen, Nachfolgeseiten schließen entstandene Lücken im Angebot urheberrechtlich geschützten Materials schneller als erwartet.

Nach mE würde das Unterbinden von Finanzflüssen an Betreiber rechtsverletzender Seiten ein weitaus effektiveres Mittel zur Bekämpfung von Piraterie darstellen als zu versuchen, kosmetische Zensur auf Ebene und Kosten der Access-Provider zu betreiben. Es stellt sich die Frage, warum im deutschsprachigen Raum nicht ähnliche Initiativen wie in Großbritannien[328] oder Australien[329] forciert werden, Werbeschaltungen auf rechtsverletzenden Seiten zu unterbinden. Eine weitere Möglichkeit wäre, Zahlungsdiensteanbieter wie Visa, Mastercard, Sofortüberweisung oder Paypal dazu zu verpflichten, keine Zahlungen an Streamhoster, Sharehoster etc entgegenzunehmen, wie dies in der Vergangenheit bereits der Fall war[330], offensichtlich aber nicht mehr oder nicht in der nötigen Intensität durchgesetzt wird[331].

Abgesehen davon werfen sogar einige Rechtsinhaber selbst die Frage auf, ob die Piraterie ihrer Werke ihnen vielleicht mehr Nutzen als Schaden bringt, womit sie auch die Sinnhaftigkeit und Rechtfertigung von Sperren in Frage stellen. Der Chef des Konzerns Time Warner bezeichnete den Umstand, dass die vom Konzernunternehmen HBO produzierte Serie „Game of Thrones“ die am meisten heruntergeladene TV-Serie weltweit ist, als eine Auszeichnung, die wertvoller als der Gewinn eines Emmys sei. Piraterie sei den

[328] Siehe dazu http://www.theguardian.com/technology/2014/apr/02/infringing-websites-list-anti-piracy.
[329] Siehe dazu http://www.theaustralian.com.au/technology/ads-ban-on-music-movie-piracy-sites/story-e6frgakx-1227051863944.
[330] Siehe dazu https://torrentfreak.com/paypal-bans-major-file-hosting-services-over-piracy-concerns-120710/
[331] So werben zB die auf kinox.to verlinkten Streamhoster „xvidstage.com“ und „bitshare.com“ mit Zahlung per Kreditkarte und Paypal. Der populäre Sharehoster „uploaded.net“ bietet darüber hinaus sogar Sofortüberweisung als Zahlungsmethode an.

Untersuchungen des Konzerns zufolge kein ernsthaftes Problem, sondern bringe dem Sender HBO langfristig gesehen sogar mehr Abonnenten.[332]

Vielleicht sollten Rechteinhaber besser auf neue Geschäftsmodelle setzen, welche die Chance hätten, rechtswidrige Angebote zu verdrängen, anstatt Ressourcen in Prozesse zur Durchsetzung von ineffektiven Sperren zu investieren:

Die Entwicklungen in der Musikindustrie hin zu Streamingdiensten, die entweder werbefinanziert sind oder gegen monatliche Gebühr werbefrei genutzt werden können, hat gezeigt, dass viele Nutzer bereit sind, zugunsten solcher Dienste von illegalen Musikdownloads abzusehen.[333]

Auch in der Filmbranche sprechen die Zahlen für sich: Während im ersten Halbjahr 2014 in Nordamerika Netflix am Internetverkehr zu Spitzenzeiten einen Anteil von ca 31% und Bittorrent einen Anteil von ca 6% hatte, betrug der Bittorrent-Verkehr in Europa ca 15% und Netflix, da es im ersten Halbjahr 2014 nur im Vereinigten Königreich und Irland verfügbar war, war nur für ca 3% des europaweiten Internetverkehrs zu Spitzenzeiten verantwortlich.[334] Zwar lassen sich daraus, da Bittorrent, wie unter 5.4.1 erwähnt, nicht ausschließlich zum Herunterladen urheberrechtlich geschützter Filme benutzt wird, nur begrenzt Schlüsse ziehen – ein genereller Trend ist jedoch unzweifelhaft erkennbar.

Ein Grund für viele Nutzer, überhaupt Material raubzukopieren könnte darin zu finden sein, dass im europäischen Raum viele Serien und Filme erst zu einem viel späteren Zeitpunkt verfügbar sind als in den Vereinigten Staaten. Zudem sind zahlreiche Filme und Serien nur über den „klassischen" Vertrieb als DVDs, nicht jedoch als Downloads, erhältlich. Dies steht mE im Widerspruch zum Konsumverhalten junger Verbraucher, denn die Entscheidung, welchen Film man an einem Filmabend sehen will, fällt nicht mehr ein paar Tage vorher, sondern wird spontan getroffen. Eine DVD anzuschaffen ist daher nicht möglich.
Konsumenten, die aus diversen Gründen von einem Kinobesuch abstand nehmen, die neuesten Filme aber gerne über das Internet konsumieren würden, müssen entweder monatelang auf die Veröffentlichung der DVD warten oder sind darauf angewiesen, Raubkopien in schlechter Qualität über dubiose Seiten zu beziehen.

---

[332] http://derstandard.at/1375626103185/Time-Warner-Boss-Game-of-Thrones-Piraterie-besser-als-ein-Emmy.
[333] siehe dazu zB http://wirtschaftsblatt.at/blogs/stefan_mey/1336673/Raubkopien-sind-out oder http://www.tagesschau.de/wirtschaft/interview-musiklizenzen100.html.
[334] Siehe dazu den Sandvine Global Internet Phenomena Report 1H 2014, abrufbar unter https://www.sandvine.com/trends/global-internet-phenomena/.

Das Problem von Raubkopien lässt sich unter diesen Gesichtspunkten wahrscheinlich am effektivsten bekämpfen, indem Inhalte weltweit gleichzeitig über das Internet zu fairen Konditionen verfügbar gemacht werden. Würde die Filmindustrie die Trends der Zeit erkennen, anstatt zu versuchen, Althergebrachtes durch Internetsperren zu verteidigen, könnte sie ihren Umsatz im Internet beträchtlich steigern und als Nebeneffekt die Geschäftsmodelle rechtsverletzender Seiten untergraben. In diesem Sinn argumentiert auch die ehemalige EU-Kommissarin für die Digitale Agenda, *Neelie Kroes*:

„*The digital age isn't a threat to the film industry, neither to cinemas nor broadcasters. It's not something to be ignored; still less something to be fought, tackled, legislated against. But it's an opportunity: something to be welcomed, supported, embraced.*

Online channels offer a new way to reach out to a different audience—an audience who, for one reason or another, wouldn't go to the cinema. “[335]

[335] http://europa.eu/rapid/press-release_SPEECH-12-704_en.htm.

9. Literatur- und Quellenverzeichnis

Kommentare, Bücher, Monographien und Beiträge

- *Kucsko* (Hrsg), Urheberrecht online - MANZ Kommentar zum Urheberrechtsgesetz (Stand 1.12.2007) via rdb-online
- *Angst* (Hrsg)^2, Kommentar zur Exekutionsordnung (Stand 1.3.2008) via rdb-online
- *Beimrohr*, Internetsperren zur Durchsetzung des Urheberrechts – Die Entscheidung des EuGH zum Fall UPC Telekabel Wien/kino.to, jusIT 2014, 83
- *Briem*, Ist der Auskunftsanspruch gegenüber Providern nach § 87b Abs 3 UrhG tot?, MR 2011, 55
- *Castelli*, Network Consultants Handbook (2001) via Google Books
- *Dohr/Pollirer/Weiss/Knyrim*, DSG^2 (Stand 2.7.2014) via rdb-online
- *Frey/Rudolph*, Rechtsgutachten zur Evaluierung des „Haftungsregimes für Host und Access-Provider im Bereich der Telemedien“ via http://www.bvdw.org/mybvdw/media/download/rechtsgutachten-klein.pdf?file=169
- *Heidinger*, Die zivilrechtliche Inanspruchnahme von Access-Providern auf Sperre urheberrechtsverletzender Webseiten, ÖBl 2011, 37
- *Jahnel/Mader/Staudegger (Hrsg)*, IT-Recht^3 (2012)
- *Jarass*, Charta der Grundrechte der EU (2013)
- *Kassai*, "Location Based Services" im Gefüge des Datenschutzrechts, MR 2004, 443
- *König*, Deep Packet Inspection und das Kommunikationsgeheimnis
- *Kraft*, Zugangssperren zu Webseiten als Mittel der Rechtsdurchsetzung, MR 2014, 171
- *Launinger/Kirda/Michiardi*, Paying for Piracy? An Analysis of One-Click Hosters' Controversial Reward Schemes via http://www.iseclab.org/papers/uploader-income.pdf
- *Lehofer*, EGMR zur Abwägung zwischen Urheberrecht und freier Meinungsäußerung (Neij und Sunde, The Pirate Bay) via http://blog.lehofer.at/2013/03/egmr-zur-abwagung-zwischen-urheberrecht.html
- *Ofcom*, „Site Blocking“ to reduce online copyright infringement via http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf
- *Öhlinger*, Verfassungsrecht^{10} (2014)
- *OSCE*, Freedom of Expression on the Internet via http://www.osce.org/fom/80723
- *Pfitzmann/Köpsell/Kriegelstein*, Sperrverfügungen gegen Access Provider – Technisches Gutachten via https://glueckksspiel.uni-hohenheim.de/fileadmin/einrichtungen/glueckksspiel/Regulierung/20080428_technisches_Gutachten_Sperrvervuegungen.pdf
- *Pursch/Bär*, Sperrverfügung gegen Internet-Provider via https://netzpolitik.org/wp-upload/bundestag_filter-gutachten.pdf
- *Rechberger/Oberhammer*, Exekutionsrecht^5 (2009)
- Sandvine Global Internet Phenomena Report 1H 2014 via https://www.sandvine.com/trends/global-internet-phenomena/
- *Stadler/Strass*, Website-Blockaden gegen Online-Piraterie?, ecolex 2013,292.
- *Walter*, Umfang der Unterlassungspflichten von Vermittlern – Access-Provider – kino.to, MR 2014, 82
- *Zankl*, EuGH für Datenzugangssperre und gegen Datenvorratsspeicherung, ecolex 2014, 576

Judikate und Rechtssätze

- Amtsgericht Leipzig 21.12.2011, 200 Ls 390 Js 184/11
- EGMR 28.09.1999, 22479/93 (Öztürk gegen Türkei)
- EGMR 11.01.2007, 73049/01 (Anheuser-Busch Inc. gegen Portugal)
- EuGH 05.10.1994, C-280/93 (Deutschland / Rat)
- EuGH 15.10.2002, C-238/99 (Limburgse Vinyl Maatschappij u.a. / Kommission)
- EuGH 24.11.2011, C-70/10 (Scarlet Extended) = RdW 2011/719, 705 = jusIT 2011/98, 215 = SWI 2011, 14 = lex:itec 2011 H 5, 16 = wbl 2012/50, 153 = jusIT 2012/40, 85 (*Beimrohr*)
- EuGH 16.02.2012, C-360/10 (SABAM) = RdW 2012/163, 153 = wbl 2012/49, 150 = ecolex 2012/147, 333 = jusIT 2012/22, 54 = jusIT 2012/40, 85 (*Beimrohr*) = ZTR 2012, 128
- EGMR 19.02.2013, 40397/12 (Fredrik Neij und Peter Sunde Kolmisoppi) = MR-Int 2013, 45
- EuGH 26.02.2013, C-617/10 (Fransson) = ÖJZ 2013/37, 380 (*Posch*) = taxlex-EU 2013/47, 147 = ZfRV-LS 2013/14, 71 = RdW 2013/116, 118 = EuGRZ 2013, 124 = UVS-Slg 2013/84, 92 = ÖJZ 2014/81, 494 (*Zeder*)
- EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien) = RdW 2014/196, 173 = ecolex 2014, 297 (*Wilhelm*) = MR 2014, 82 = ecolex 2014, 576 (*Zankl*) = jusIT 2014/42, 83 (*Beimrohr*) = jusIT 2014/43, 87 = ÖJZ 2014/73, 474 = wbl 2014/109, 329 = ecolex 2014, 488 = ecolex 2014/218, 546 = ÖBl 2014/40, 189
- EuGH 10.04.2014, C-435/12 (ACI Adam u.a.) = jusIT 2014/44, 88 (*Staudegger*) = MR-Int 2014, 42 (*Walter*) = ecolex 2014/297, 727 (*Zemann*)
- EuGH 13.04.2014, C-131/12 (Google Spain und Google)
- Landgericht Hamburg 02.03.2014, 308 O 458/10
- OGH 11.05.2012, 4 Ob 6/12d = wbl 2012/180, 473 = ecolex 2012/291, 708 = RdW 2012/401, 381 = MR 2012, 190 = RZ 2013/EÜ 13, 22 = ÖBl 2013/10, 43
- OGH 24.06.2014, 4 Ob 71/14s
- OLG Köln 18.07.2014, 6 U 192/11
- RIS-Justiz RS0026577
- RIS-Justiz RS0114467
- VwGH 24.04.2013, 2011/17/0293

Rechtsquellen

- Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz)in der Fassung BGBl I Nr 150/2013 (UrhG)
- Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000) in der Fassung BGBl I Nr 83/2013 (DSG)
- Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz - SPG) in der Fassung BGBl I Nr 73/2014 (SPG)
- Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch - StGB) in der Fassung BGBl I Nr 134/2013 (StGB)
- Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz - ECG) in der Fassung BGBl I Nr 152/2001 (ECG)

- Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 - TKG 2003) in der Fassung BGBl I Nr 44/2014 (TKG)
- Bundesverfassungsgesetz vom 29. November 1988 über den Schutz der persönlichen Freiheit, BGBl Nr. 684/1988
- Erläuterungen zur Regierungsvorlage zur TKG-Novelle 2011, XXIV. GP, 1074
- Gesetz vom 27. Mai 1896, über das Exekutions- und Sicherungsverfahren (Exekutionsordnung – EO) in der Fassung BGBl I Nr 69/2014 (EO)
- Konvention zum Schutze der Menschenrechte und Grundfreiheiten in der Fassung BGBl III Nr 47/2010 (EMRK)
- Ministerialentwurf XXIV. GP, 82/ME
- Richtlinie 2000/31/EG des Europäischen Parlamentes und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), Abl L 2000/178, 1
- Richtlinie 2001/29/EG des europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl L 2001/167, 10
- Richtlinie 2004/48/EG des Europäischen Parlamentes und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums, Abl L 2004/157, 45
- Staatsgrundgesetz vom 21. December 1867, über die allgemeinen Rechte der Staatsbürger für die im Reichsrathe vertretenen Königreiche und Länder in der Fassung BGBl I Nr 684/1988 (StGG)
- Vertrag über die Arbeitsweise der Europäischen Union, Abl C 83/2010, 47
- Vertrag über die Europäische Union, Abl C 83/2010, 13

Internetquellen*

- http://bittorrent.org/beps/bep_0005.html
- http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/
- http://derstandard.at/1375626103185/Time-Warner-Boss-Game-of-Thrones-Piraterie-besser-als-ein-Emmy
- http://derstandard.at/2000006347840/Provider-muessen-unverzueglich-Piratenseiten-kinoxto-und-movie4-sperren
- http://derstandard.at/2000006365884/Netzsperren-Ab-sofort-im-Einsatz-aber-leicht-zu-umgehen
- http://europa.eu/rapid/press-release_SPEECH-12-704_en.htm
- http://heise.de/-1698607
- http://heise.de/-1741726
- http://heise.de/-2432216
- http://jonas.nitro.dk/bittorrent/bittorrent-rfc.html
- http://nrkbeta.no/bittorrent/
- http://software.dell.com/documents/sonicwall-ssl-inspection-datasheet-29063.pdf.
- http://svs.informatik.uni-hamburg.de/publications/2009/2009-04-23KoelnFederrath.pdf
- http://technet.microsoft.com/en-us/library/dd458966(v=ws.10).aspx
- http://technet.microsoft.com/en-us/library/dd469716(v=ws.10).aspx
- http://today.duke.edu/2010/05/usenet.html
- http://tools.ietf.org/html/rfc1180
- http://tools.ietf.org/html/rfc2647

- http://tools.ietf.org/html/rfc2663
- http://tools.ietf.org/html/rfc2764
- http://tools.ietf.org/html/rfc2874
- http://tools.ietf.org/html/rfc5537
- http://torrentfreak.com/megaupload-user-asks-court-to-order-return-of-his-data-120525/
- http://us.blizzard.com/en-us/company/about/legal-faq.html
- http://wirtschaftsblatt.at/blogs/stefan_mey/1336673/Raubkopien-sind-out
- http://www.bittorrent.org/introduction.html
- http://www.cs.cornell.edu/People/egs/papers/hyperspaces.pdf
- http://www.dgmlive.com/help.htm#whyusebittorrent
- http://www.focus.de/digital/internet/stillgelegte-raubkopie-seite-kino-to-und-kinox-to-nutzern-illegaler-filmportale-droht-strafverfahren_aid_713251.html
- http://www.forbes.com/sites/andygreenberg/2012/02/10/as-iran-cracks-down-online-tor-tests-undetectable-encrypted-connections/
- http://www.greycoder.com/how-hide-vpn-connections/
- http://www.spiegel.de/netzwelt/web/0,1518,506143,00.html.
- http://www.tagesschau.de/wirtschaft/interview-musiklizenzen100.html
- http://www.theaustralian.com.au/technology/ads-ban-on-music-movie-piracy-sites/story-e6frgakx-1227051863944
- http://www.theguardian.com/technology/2014/apr/02/infringing-websites-list-anti-piracy
- http://www.zeit.de/digital/internet/2011-06/kino-stream-ermittlung
- http://www.zeit.de/online/2009/08/internetsperren-leyen
- https://cseweb.ucsd.edu/~mihir/cse207/w-hash.pdf
- https://kb.iu.edu/d/ahoo
- https://netzpolitik.org/2012/deep-packet-inspection-der-unterschied-zwischen-internet-in-diktaturen-und-deutschland-ist-nur-eine-konfigurationsdatei/
- https://support.google.com/youtube/answer/2797370.
- https://tools.ietf.org/html/rfc1035
- https://tools.ietf.org/html/rfc1812
- https://tools.ietf.org/html/rfc4033
- https://tools.ietf.org/html/rfc79
- https://torrentfreak.com/paypal-bans-major-file-hosting-services-over-piracy-concerns-120710/
- https://www.google.com/intl/en/ipv6/statistics.html
- https://www.techdirt.com/articles/20121217/10222821404/china-tries-to-block-encrypted-traffic.shtml
- https://www.torproject.org/about/overview.html.en
- https://www.youtube.com/copyright_complaint_form

* Alle Internetquellen wurden zuletzt am 03. November 2014 abgerufen.

Zitate nach *Jahnel/Sramek*, NZR, 2012
Times New Roman 12pt, Zeilenabstand 1,5
Fußnoten Times New Roman 10pt, Zeilenabstand 1,0

10. Anhang

10.1. Abstract

Diese Masterarbeit widmet sich dem Themenkomplex rund um die Sperrverfügungen zur Sperre rechtsverletzender Internetseiten gegenüber Access-Providern, welche aktuell von Rechteinhabern aus Film- und Musikindustrie angestrengt werden. Im Zuge aktueller Entscheidungen des EuGH[336] und OGH[337] wurde die Rechtmäßigkeit derartiger Verfügungen bejaht, allerdings ist der Beitrag dieser Erkenntnisse hinsichtlich einer Klärung der Rechtslage jedoch gering: Es wir nämlich in diesen Entscheidungen die rechtliche Bewertung, welche konkrete technische Sperrmaßnahme vorgenommen werden muss, den Access-Providern überbürdet.

Obwohl sich die aktuellen Sperren vor allem gegen jene Internetseiten richten, welche rechtswidrig Filme zum Abruf mittels sogenannten Streamings anbieten, ist der Fokus dieser Masterthesis weiter gefasst: Neben Streamingseiten werden nämlich jene Verbreitungsmöglichkeiten urheberrechtlich geschützten Materials aus juristischer wie technischer Sicht beleuchtet, welche in näherer Zukunft Gegenstand von Sperrforderungen sein könnten.

Das Hauptaugenmerkt dieser Arbeit liegt auf der Erörterung der juristischen und technischen Grundlagen der zur Verfügung stehenden Sperrmethoden. Einerseits stellt sich nämlich die grundsätzliche Frage, ob überhaupt taugliche Mittel zur Implementierung von Sperren zur Verfügung stehen; andererseits stehen die Access-Provider vor dem Problem, welche technischen Lösungen sie zur Umsetzung gerichtlicher Anordnungen zur Sperre von Internetseiten ergreifen müssen.

Abschließend werden Alternativen zur Lösung der faktischen Probleme im Zusammenhang mit der Rechtsdurchsetzung der Rechteinhaber dargelegt. Diese Überlegungen ermöglichen es, die Problematik auch ohne den Rückgriff auf Sperren zu lösen.

[336] EuGH 27.03.2014, C-314/12 (UPC Telekabel Wien).
[337] OGH 24.06.2014, 4 Ob 71/14s.

10.2. Lebenslauf

Bildungsweg

Oktober 2013 – Dezember 2014	LL.M. Informations- und Medienrecht an der Universität Wien • Schwerpunkte: Telekommunikationsrecht, Datenschutzrecht • Masterarbeit zum Thema „Sperrverfügungen hinsichtlich urheberrechtsverletzender Internetseiten – juristische Notwendigkeit oder technische Unmöglichkeit?“
Oktober 2006 – November 2012	Studium der Rechtswissenschaften an der Universität Wien • Schwerpunkte: Unternehmensrecht, Immaterialgüterrecht • Diplomandenseminararbeiten zu den Themen „Leerkassettenvergütung im grenzüberschreitenden Versandhandel“ und „Zur Beugehaft gegen den Geschäftsführer der verpflichteten GmbH“
1998 - 2006	Erzbischöfliches Privatgymnasium Borromäum Salzburg • Humanistischer Schwerpunkt • Matura mit gutem Erfolg

Berufliche Tätigkeit

November 2014 – Jänner 2015	Royal Bank of Canada (London) • Juristische Begleitung und Programmiertätigkeit zur Automatisierung von Derivat-Produktprospekten • Automatisierung von Workflow-Abläufen
März 2013 – Juni 2013 bzw Oktober 2014 – November 2014	Gerichtspraxis (Wien) • Bestandsrecht und allgemeine streitige Zivilrechtssachen am BG Hernals • Jugendstrafsachen am LGSt Wien
Juni 2011 – Juni 2014	Wallstreetdocs Ltd. (Wien/London) • Selbstständige Betreuung folgender Klienten: Bank of America/Merrill Lynch New York, Citibank New York, Erste Bank Wien, Raiffeisen Centrobank Wien • Juristische Begleitung und Programmiertätigkeit zur Automatisierung von Derivat-Produktprospekten • Automatisierung von Workflow-Abläufen
Jänner 2009 – Mai 2011	Baurechts- und Bauwirtschafts GmbH (Wien/Salzburg) • Administrative Tätigkeiten • Recherchetätigkeiten • Vorbereitung von Schriftsätzen • Vorbereitung von Verträgen

Praktika

August 2010	Praktikum bei Berger & Partner Rechtsanwälte (Salzburg) • Vorbereitung von Schriftsätzen • Unterstützung im Rahmen von Publikationen • Kontakt mit Klienten
August 2006, August 2007, August 2008	Praktika bei Firma HaBau • Bürotätigkeiten am Standort Wien Dresdnerstraße sowie in diversen Baubüros (Bhf St. Pölten, U1 Verlängerung Leopoldau, AS IZ Niederösterreich-Süd) • Unterstützung in baurechtlichen Fragen • Unterstützungsarbeiten im Rahmen der Rechnungslegung an den Bauherren • Bestandsaufnahmen auf den Baustellen

Publikationen

- *Agnes Balthasar/Matthias Wach/Alexander Balthasar*, Sind Sicherheitslücken wirklich unvermeidlich? Technische, rechtsdogmatische und rechtspolitische Überlegungen, Jusletter IT 15. Mai 2014

Sprachkenntnisse

Muttersprache: Deutsch
Englisch: C1
(Latein, Altgriechisch)