Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Wirtschaft,
Bildung und Forschung WBF

Staatssekretariat für Wirtschaft SECO
Bilaterale Wirtschaftsbeziehungen
Amerika

Bericht

Roundtable zum Urheberrecht im Internet

Bern, 23. Januar 2014

812.13/2005/02178 \ COO.2101.104.5.3951051

Inhaltsverzeichnis

1 Zielsetzung des Roundtable und seiner Arbeitsgruppe

Die Thematik des Urheberrechtsschutzes im Internet ist im Rahmen des Kooperationsforums Schweiz-USA für Handel und Investitionen[1] von der US-Botschaft in Bern im Jahr 2011 ans SECO herangetragen worden. Das Ziel des Roundtable ist es zu prüfen, wie im Rahmen der geltenden Gesetzgebung Urheberrechtsverletzungen im Internet datenschutzkonform ermittelt und strafrechtlich verfolgt werden können. Aufgrund der Diskussionen an den ersten beiden Sitzungen wurde eine Arbeitsgruppe eingesetzt. Das **Ziel** dieser Arbeitsgruppe wurde auf die **Prüfung der folgenden Schritte ausgedehnt**:

- Eine **Anpassung des Fernmeldegesetzes** (**FMG**) oder des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (**BÜPF**)
- Das Führen eines **Musterstrafverfahrens** gegen mutmassliche Urheberrechtsverletzer
- Weitere ergänzende Massnahmen

Im Unterschied zur Arbeitsgruppe zur Optimierung der kollektiven Verwertung von Urheberrechten und verwandten Schutzrechten (**AGUR12**), welche im September 2012 ihre Arbeit aufnahm und von Roland Grossenbacher, dem Direktor des Eidgenössischen Instituts für Geistiges Eigentum (IGE), präsidiert wurde, ist das **Mandat** des Roundtable damit enger gefasst und konzentriert sich auf die Frage der Rechtsdurchsetzung. Die AGUR12 hat neben der Anpassung des Urheberrechts an die technische Entwicklung auch Möglichkeiten zur Effizienzsteigerung und Kostensenkung bei der kollektiven Verwertung von Urheberrechten geprüft.[2] Der Roundtable und die AGUR12 arbeiteten weitgehend unabhängig voneinander und waren inhaltlich komplementär.

Die Arbeiten wurden seit März 2012 im Rahmen von zwei Sitzungen des gesamten Roundtable und von fünf Sitzungen seiner **Arbeitsgruppe** ausgeführt. Zudem fanden verschiedene Expertengespräche zwischen einzelnen Teilnehmern des Roundtable statt. Der vorliegende Bericht fasst die Ergebnisse des Roundtable zusammen und bietet einen Ausblick auf relevante Entwicklungen zum Thema. Das Musterstrafverfahren wurde am 7. Januar 2013 durch Einreichen einer Strafanzeige eingeleitet. Nach einer Erstermittlung durch die Staatsanwaltschaft wurde das Verfahren eingestellt, wogegen die Anzeigeerstatterin Beschwerde an das Obergericht des Kantons Zürich erhoben hat. Das Verfahren ist daselbst noch hängig.

2 Problematik

Mit seinem Urteil vom 8. September 2010[3] entschied das **Bundesgericht**, dass die Firma **Logistep**, die gewerbsmässig IP-Adressen[4] mutmasslicher Urheberrechtsverletzer gesammelt und an die Rechteinhaber verkauft hatte, mit ihrem Vorgehen gegen das Datenschutzgesetz verstossen hat.

Angaben bezüglich IP-Adressen des Routers des Up- beziehungsweise Downloaders sind häufig notwendig, um Urheberrechtsverletzungen im Internet zu dokumentieren und strafrechtlich ahnden zu können. Wird nun das Bundesgerichtsurteil im Fall Logistep so ausgelegt, dass die **Beschaffung von IP-Adressen** zur Ermittlung des Tatbestands der Urheberrechtsverletzung im Internet **grundsätzlich nicht mit dem Datenschutzgesetz** vereinbar ist, so erschwert dies die strafrechtliche Verfolgung von solchen Urheberrechtsverletzungen erheblich. Denn erst mittels der gesammelten IP-Adressen gelangen die Ermittlungsbehör-

[1] Das Kooperationsforum wurde am 28. Januar 2006 anlässlich des Weltwirtschaftsforums in Davos geschaffen und dient als Rahmen für Gespräche zwischen der Schweiz und den USA über Handels- und Investitionsthemen.

[2] Vgl. https://www.ige.ch/urheberrecht/agur12.html

[3] Bundesgerichtsentscheid 136 II 508.

[4] Eine IP(Internet Protocol)-Adresse ist eine Adresse in Computernetzwerken, die auf dem Internetprotokoll basiert. Eine IP-Adresse wird Geräten zugewiesen, welche an das Netz angebunden sind und macht diese Geräte auf diese Weise adressier- und erreichbar.

den zum Inhaber des Anschlusses, über welchen die Urheberrechtsverletzungen vorgenommen wurden. Die Behörden können dann allenfalls eine Hausdurchsuchung und bei Bedarf die Beschlagnahmung von Beweismitteln veranlassen. Dass die kantonalen **Strafverfolgungsbehörden Anzeigen** der Rechteinhaber mit Verweis auf den Bundesgerichtsentscheid gegen Logistep **nicht mehr nachgehen**, hat deshalb zu Schwierigkeiten bei der Ahndung von Urheberrechtsverletzungen im Internet geführt.

Das **Bundesgericht** hat in seinem im Februar 2011 veröffentlichten Geschäftsbericht den Gesetzgeber darauf hingewiesen, dass die aktuelle Situation hinsichtlich des **Urheberrechtsschutzes unbefriedigend** erscheine**.** Es sei Sache des Gesetzgebers, einen den neuen Technologien angepassten Urheberrechtsschutz zu gewährleisten.[5]

Die Konsequenzen des Entscheids sind auch regelmässig Thema in den **bilateralen Gesprächen** zwischen der Schweiz und den USA, welche den Entwicklungen in der Schweiz kritisch gegenüberstehen. Die USA haben ihre Bedenken auch auf hoher diplomatischer Ebene, so etwa im Rahmen der Joint Economic Commission, zum Ausdruck gebracht. Der US-Handelsbeauftragte (USTR) veröffentlicht zudem einmal jährlich einen **Special 301 Report**, in dem er die Immaterialgütergesetzgebung im Ausland prüft. Werden Mängel erkannt, hat der USTR die Möglichkeit, ein Land auf seine „301 Watch List" zu setzen. Im letzten Bericht wird die **Schweiz** zwar nicht auf dieser Liste geführt, aber **explizit erwähnt**:

> *The United States continues to have serious concerns regarding the inability of rights holders to secure legal redress in Switzerland in cases involving copyright piracy over the Internet. The United States strongly encourages Switzerland to demonstrate its commitment to copyright protection and to combating online piracy vigorously, including by taking steps to ensure that rights holders can protect their rights. The United States will be closely monitoring the results of the current AGUR12 ("Arbeitsgruppe Urheberrecht 2012," or "Working Group on Copyright 2012") process as well as the Swiss Ministry of Economy (SECO)-led roundtable process.*
>
> (301 Report des USTR[6], 2013, S. 21)

3 Sammeln von Beweisen für Urheberrechtsverletzungen im Internet unter Einhaltung der Datenschutzbestimmungen

Die Auffassung der kantonalen **Staatsanwaltschaften,** dass nach dem Bundesgerichtsurteil im Fall Logistep das **Sammeln von IP-Adressen grundsätzlich nicht mehr gestattet** sei und daher auch keine entsprechenden Ermittlungen mehr durchgeführt werden können, steht im **Widerspruch** zur Position des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (**EDÖB**). Dieser hatte in einem **Schreiben** an die Schweizerische Vereinigung zur Bekämpfung der Piraterie (**SAFE**) ein Vorgehen skizziert, das sich seines Erachtens von demjenigen der Firma Logistep klar unterscheidet und mit dem Datenschutzgesetz konform ist. Das vom EDÖB vorgeschlagene Vorgehen unterscheidet sich von den Praktiken der Firma Logistep insbesondere dadurch, dass die Rechteinhaber auf ihrer Website ihre Vorgehensweise (einschliesslich detaillierter Angaben zu Art und Umfang der gesammelten Daten) vollständig offenlegen und deutlich machen sollen, dass sie immer eine rechtskräftige **strafrechtliche Verurteilung abwarten**, bevor sie Urheberrechtsverletzer mit Zivilforderungen konfrontieren.[7]

Bei einem Treffen zwischen der Staatsanwaltschaft Zürich, den Rechteinhabern, dem Institut für Geistiges Eigentum, dem EDÖB und dem SECO im Mai 2012 wurden **Anpassungen** der

---

[5] Vgl. Geschäftsbericht des Bundesgerichts 2010, S. 17, verfügbar unter http://www.bger.ch/gb2010_bger_d.pdf

[6] United States Trade Representative [USTR]. (2013). *2013 Special 301 Report*. Bericht verfügbar unter http://www.ustr.gov/sites/default/files/05012013%202013%20Special%20301%20Report.pdf

[7] Vgl. Tätigkeitsbericht des EDÖB 2011/2012, verfügbar unter http://www.edoeb.admin.ch/dokumentation/00153/00154/00986/index.html?lang=de

datenschutzrechtlichen **Best Practices** diskutiert, da diese nicht den geltenden Strafprozessnormen entsprachen. Die Experten konnten sich dabei auf einen Vorschlag einigen.[8]

Die Gruppe prüfte ausserdem die folgenden alternativen Ermittlungsmethoden:

- Erfassung von nur neun Ziffern der IP-Adresse
- Generierung von Hashcodes[9] der IP-Adressen durch Internet Service Provider (ISP)
- Staatsanwaltschaften ermitteln auf Hinweis „Werk verfügbar"

Die beiden ersten Ansätze wurden als **wenig erfolgversprechend** beurteilt, da sich durch sie wenig an der Datenschutz-Problematik ändert. Die dritte Methode ist aufgrund **der beschränkten Ressourcen der Strafverfolgungsbehörden** und des Erfordernisses eines genügenden initialen Tatverdachtes nicht gangbar.

Weiter wurde auch die Vereinbarkeit eines zivilen Auskunftsverfahrens gegen Internet Service Provider (ISP) und eines Strafverfahrens gegen Uploader mit den Bestimmungen des Datenschutzes geprüft. Da die Speicherung von **Randdaten**[10] für ein **Zivilverfahren** nicht erlaubt ist, wurden auch die Best Practices des EDÖB nicht auf Zivilverfahren ausgedehnt. Dies bedeutet, dass der **Weg eines zivilen Auskunftsverfahrens** gegen ISP innerhalb des derzeitigen rechtlichen Rahmens **nicht möglich** ist.

In **Strafverfahren** können Beweise seit dem Logistep-Urteil nach Ansicht der kantonalen Staatsanwaltschaften nur unter erschwerten Bedingungen datenschutzkonform beschafft werden. Mittels einer Strafanzeige und eines Rekurses gegen die Einstellungsverfügung könnte aber allenfalls ein **neuer Leitentscheid des Bundesgerichts** erwirkt werden, welcher die gängige Praxis der Staatsanwaltschaften ändern würde.

4 Musterstrafverfahren

Als erstes Ergebnis dieser Diskussionen haben die Rechteinhaber am 7. Januar 2013 bei der Staatsanwaltschaft Zürich **Strafanzeige** gegen einen **unbekannten Internetnutzer** eingereicht, der über ein Peer-to-peer Netzwerk[11] rund 1'500 urheberrechtlich geschützte Werke verfügbar gemacht hatte. Sie beabsichtigen, mit dem Führen eines **Musterstrafverfahrens** die Tragweite des Logistep-Entscheids des Bundesgerichts zu klären. Die Rechteinhaber berücksichtigten bei ihrer Klage die **Best Practices des EDÖB**. So macht SAFE auf ihrer **Webseite** unter anderem darauf aufmerksam, dass der Verband in Peer-to-peer Netzwerken die **IP-Adressen von Nutzern sammelt**, welche in strafbarer Weise Urheber- und andere Immaterialgüterrechte verletzen.[12]

Die **Staatsanwaltschaft** Zürich veranlasste am 10. Januar 2013 beim Dienst Überwachung Post- und Fernmeldeverkehr auf Basis der von den Rechteinhabern in ihrer Anzeige genannten IP-Adresse eine **Teilnehmeridentifikation**. Diese Massnahme wurde laut Staatsanwaltschaft vorsorglich vorgenommen, weil die Ablehnung des Beweisantrags einen materiellen

---

[8] Die Best Practices wurden modifiziert, da das neue Strafprozessrecht explizit vorsieht, dass der Staatsanwalt die Parteien zu einem zivilrechtlichen Vergleich / einer Schadenstilgung anregen kann und, sollte dies gelingen, das Verfahren einstellen kann. Dahingehend waren die Best Practices etwas zu rigide, da sie den Rechteinhabern jeden Kontakt mit dem Verletzer untersagte, bis der Verletzer strafrechtlich verurteilt wurde.

[9] Eine Hashfunktion ist eine Abbildung, die zu jeder Eingabe aus einer oft sehr grossen Quellmenge eine Ausgabe aus einer kleineren Zielmenge erzeugt, den sogenannten Hashcode.

[10] Randdaten enthalten Informationen über die Nutzung von elektronischer Infrastruktur. Sie dokumentieren beispielsweise, welcher Telefonanschluss, welcher E-Mail-Absender oder welche IP-Adresse wann, wie lange und mit wem kommuniziert oder wie und wann elektronische Geräte genutzt wurden. Diese Daten werden gespeichert und so kann die Identität eines Urheberrechtsverletzer via die IP Adresse eruiert werden.

[11] In einem Peer-to-Peer-Netzwerk sind alle Computer gleichberechtigt und können sowohl Dienste in Anspruch nehmen als auch zur Verfügung stellen.

[12] Vgl. http://www.safe.ch/154.html?&L=nmmfzvhzfukxuz

Rechtsnachteil dargestellt hätte und in einem allfälligen späteren Prozessstadium nicht mehr hätte wiederholt werden können. In ihrer am 4. März 2013 erlassenen **Einstellungsverfügung** hielt die Staatsanwaltschaft jedoch fest, dass die erhobenen **Daten** in einem Zivil- oder Strafverfahren aufgrund einer Datenschutzverletzung **nicht verwertbar** seien. Denn die Erhebung von IP-Adressen durch Private, welche die Identifikation des Anschlussinhabers durch die Untersuchungsbehörde ermöglichen, ist nach Ansicht der Staatsanwaltschaft geeignet, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen. Sie verweist in ihrer Argumentation ausdrücklich auf den **Logistep-Entscheid** des Bundesgerichts.

Der Vertreter der Rechteinhaber **rekurrierte** gegen die Einstellungsverfügung der Staatsanwaltschaft beim **Zürcher Obergericht**. Es wird erwartet, dass dieses in nächster Zeit über die Rechtmässigkeit der Einstellungsverfügung entscheidet. Falls das Obergericht den Entscheid der Staatsanwaltschaft stützt, werden die Rechteinhaber einen **Weiterzug des Entscheids ans Bundesgericht** in Erwägung ziehen. Es kann damit gerechnet werden, dass dieses den Fall im Verlauf des Jahres 2014 beurteilen würde.

Falls das Bundesgericht zum Schluss kommen würde, dass das Vorgehen der Rechteinhaber mit dem Datenschutzgesetz vereinbar ist, würden die kantonalen Strafverfolgungsbehörden ihre im Anschluss an den Logistep-Entscheid entstandene **Praxis**, privat ermittelte IP-Adressen nicht als Beweismittel zuzulassen, voraussichtlich **anpassen** müssen. Damit würde der **Weg für eine strafrechtliche Verfolgung** von Urheberrechtsverletzungen im Internet wieder **frei**. Die Rechteinhaber wünschen sich jedoch aus den nachfolgend erläuterten Gründen neben dem strafrechtlichen Instrumentarium auch eine **zivilrechtliche Handhabe**. Diese würde mit einem Leitentscheid des Bundesgerichts nicht geschaffen.

5 Geprüfte Gesetzesanpassungen

Eine Gesetzesänderung zur Schaffung der Möglichkeit eines **zivilrechtlichen Vorgehens** gegen Urheberrechtsverletzungen im Internet würde den Rechteinhabern neben der Strafklage ein weiteres Instrument in die Hand geben. Die Rechteinhaber argumentierten, dieses Mittel sei mit Blick auf die Schwere des Delikts angemessener, für die Betroffenen weniger traumatisierend und schone überdies die Ressourcen der Strafverfolgungsbehörden.

5.1 Revision des Artikels 45 des Fernmeldegesetzes (FMG)

Zu einer **Anpassung des FMG** äusserten sich an den ersten Sitzungen des Roundtable und seiner Arbeitsgruppe auch Vertreter der Bundesverwaltung **wohlwollend**. Am 27. Februar 2013 unterbreitete der Vertreter der Rechteinhaber dem BAKOM deshalb einen **Vorschlag** zur Verankerung eines **Auskunftsanspruchs** gegen Access Provider im FMG. Laut Art. 45 Abs. 2 FMG haben Nutzer von Fernmeldediensten Anspruch darauf, dass die Anbieter dieser Dienste ihnen eine Reihe von Daten herausgeben, die es gestatten, andere Nutzer, welche den Dienst in bestimmter Weise missbrauchen, zu identifizieren. Die Rechteinhaber schlugen vor, dass die Anbieter von Fernmeldedienstleistungen im Internet (sogenannte **Internet Service Provider, ISP**) nicht nur nach "missbräuchlich hergestellten Verbindungen" und Massenwerbung, sondern auch nach einer mutmasslichen **Verletzung von Urheberrechten** gesetzlich verpflichtet werden sollen, die **Daten des Anschlussinhabers**, von dessen Anschluss der Missbrauch ausging, an die Geschädigten **herauszugeben**.

Die Rechteinhaber argumentierten, dass das **Interesse am Schutz des geistigen Eigentums** eine Aufnahme des Tatbestands der Verletzung von Urheber- und Leistungsschutzrechten in Art. 45 Abs. 2 FMG rechtfertigen würde. Mit der Aufnahme würde der Schweizer Gesetzgeber seine **Rechtsordnung** derjenigen in der **Europäischen Union annähern**, welche in Art. 8 Abs. 1 Bst. c der Richtlinie 2004/48 (**Durchsetzungsrichtlinie**) einen vergleichbaren Auskunftsanspruch kennt.

Das Bundesamt für Kommunikation (**BAKOM**) äusserte in seiner Stellungnahme starke **Bedenken** gegen den Vorschlag der Rechteinhaber. Der Sinn des im Art. 45 Abs. 2 FMG festgeschriebenen Auskunftsrechts sei es, die **Informationsasymmetrie** zwischen den direkt am fernmeldedienstlichen Vorgang **Beteiligten** auszugleichen. Für das BAKOM ist dies das

zentrale Argument, um das Fernmeldegeheimnis ohne gerichtliches oder behördliches Zutun zu durchbrechen. Die **Auskunftspflicht auf Dritte** auszudehnen könne zu einem **Dammbruch** führen, nach dem analoge Begehren auch für andere Rechtsverletzungen, bei denen Fernmeldedienste zum Einsatz kamen, laut würden. Sowieso seien die Anbieter von Fernmeldediensten schon heute kaum in der Lage, den Tatbestand der unlauteren Massenwerbung oder des missbräuchlichen Anrufs festzustellen. Aus Sicht des BAKOM brauche es eine **neutrale** behördliche oder behördenähnliche **Instanz**, die entsprechende Auskunftsbegehren auch dann prüft, wenn es darum geht, Urheberrechtsverletzungen auf zivilrechtlichem Weg zu verfolgen.

Vorprozessuale Informationsbeschaffungsmöglichkeiten könnten demnach unter Umständen im **Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)** festgeschrieben werden, welches bereits heute nicht mehr ausschliesslich auf Tatbestände aus dem Strafrecht beschränkt sei.

5.2 Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

Eine Anpassung des BÜPF zur Verfolgung von Urheberrechtsverletzungen wurde nicht gleichermassen eingehend geprüft wie eine Anpassung des FMG. Das Büro des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (**EDÖB**) sprach sich wiederholt kategorisch **gegen eine solche Revision** aus. Das Gesetz sei zur Ahndung von **Straftatbeständen** wie Terrorismus geschaffen worden und eigne sich nicht für die Durchsetzung zivilrechtlicher Ansprüche. Auch **politisch** sei hier mit besonders viel **Widerstand** zu rechnen.

5.3 Revision des Datenschutzgesetzes

Etwas weniger ablehnend steht das Büro des EDÖB einer Aufnahme einer Bestimmung zur Verbesserung des Urheberrechtsschutzes ins **Datenschutzgesetz** gegenüber. Auch dieses sei dafür aber nur bedingt geeignet, da es sich um ein allgemein formuliertes Regelwerk handle und konkrete **Urheberrechtsbestimmungen** darin ein **Fremdkörper** wären. Grundsätzlich müssten Massnahmen zum Schutz der Urheberrechte so wenig intrusiv wie möglich sein und die **Verhältnismässigkeit** wahren, was beispielsweise bei einer vollständigen Überwachung des Internetverkehrs nicht der Fall wäre.

5.4 Revision des Urheberrechtsgesetzes

Es wurde auch eine **Anpassung des Urheberrechtsgesetzes** (URG) ins Spiel gebracht. Dagegen wendeten die Vertreter der Rechteinhaber, des Bundesamts für Justiz sowie des Instituts für Geistiges Eigentum allerdings ein, dass die Unmöglichkeit, Urheberrechtsverletzungen im Internet zu ahnden, nicht durch eine Änderung im Bereich des Urheberrechts entstanden sei, sondern aufgrund einer **Verschiebung in der Gewichtung** des Datenschutzes gegenüber derjenigen des Urheberrechtsschutzes. Deshalb sei eine Änderung des URG der falsche Ansatz.

6 Ergänzende Massnahmen

Neben der Erörterung von gesetzgeberischen Massnahmen oblag der Arbeitsgruppe auch eine Prüfung von ergänzenden Massnahmen zur Gewährleistung des Urheberrechts. Drei mögliche Wege zu diesem Ziel werden in der Folge kurz vorgestellt.

6.1 Vorgehen gegen Plattformen innerhalb des bestehenden Rechts

Einzelne file-hosting Plattformen sind im Ausland in juristische Verfahren wegen Urheberrechtsverletzungen ihrer Nutzer verwickelt. Im Jahr 2010 wurde die Schweizer Firma **Rapidshare** vom Anti-Piracy Caucus des US-Kongresses gar auf einer Liste von "notorious illegal sites" aufgeführt. In der Folge von zahlreichen einschneidenden Gerichtsentscheiden, welche in Deutschland gegen Rapidshare erlassen wurden, hat Rapidshare sein Business-

modell angepasst und wurde in den folgenden Jahren deshalb auf der Liste nicht mehr erwähnt. Die Firma kennt ein **take-down Verfahren**, im Rahmen dessen sie verschiedenen Rechteinhabern erlaubt, sie direkt auf urheberrechtlich geschützte Inhalte hinzuweisen, die danach umgehend von den Servern entfernt werden. Die **Rechteinhaber spüren** solche **Inhalte** heute mittels Software **automatisch auf** und beantragen täglich die Löschung von mehreren Hunderttausend Links. Die Bemühungen der Firma Rapidshare im Kampf gegen illegale Inhalte auf ihren Servern wurden denn auch verschiedentlich anerkannt.

Es wurde moniert, die **illegalen Aktivitäten** ihrer Nutzer wären jedoch weiterhin ein **integraler Teil des Geschäftsmodells** gewisser Plattformen. Strafrechtliche Verfahren gegen diese **Plattformen** sind jedoch schwierig, da sie juristisch gesehen bloss die **Gehilfen der Haupttäter** sind, also der Uploader von urheberrechtlich geschützten Inhalten auf ihre Server. Verfahren gegen solche Plattformen drohen deshalb durch andere Rechtsfragen **überfrachtet** zu werden, so dass die **Klärung** der den Roundtable interessierenden **Einzelfrage**, nämlich diejenige nach der Abwägung des Datenschutzes gegen den Urheberrechtsschutz, laut den Rechteinhabern höchst **unsicher** sei. Vertreter der Bundesverwaltung äusserten hingegen die Meinung, dass ein zivilrechtliches Verfahren gegen urheberrechtsverletzende Plattformen nicht per se erfolglos scheine. Ein solches Vorgehen wurde an den Roundtable-Sitzungen aber nicht im Detail besprochen.

6.2 DNS-Blockaden

Die **DNS[13]-Blockade** ist ein Mittel, welches auch bei der Pirateriebekämpfung zur Anwendung kommen könnte. Das Instrument wird in der Schweiz bereits heute von der Koordinationsstelle zur Bekämpfung der Internetkriminalität (**KOBIK**) eingesetzt. Die KOBIK wurde 2003 als Ansprechpartnerin für **sämtliche strafrechtlich relevanten Handlungen im Internet** ins Leben gerufen, widmet sich aber vorwiegend der Bekämpfung der Kinderpornographie. Die Koordinationsstelle ist eine Mischform zwischen einer **kantonalen** und einer **nationalen** Organisation und beruht auf einer Verwaltungsvereinbarung zwischen Bund und Kantonen.

DNS-Blockaden werden von der KOBIK seit 2007 eingesetzt. Diese wurden nötig, da die Löschung von ausserhalb der Schweiz gehosteten pädokriminellen Seiten bei den zuständigen ausländischen Behörden zwar beantragt, aber während Wochen nicht vorgenommen wurde. Um dieser unbefriedigenden Situation zu begegnen wurde mit den grössten Schweizer **ISP** eine **Vereinbarung** getroffen: Diese passten ihre Allgemeinen Geschäftsbedingungen (**AGB**) so an, dass sie für ihre Nutzer statt der angeforderten Seite mit widerrechtlichen Inhalten einen Warnhinweis anzeigen können. Zu diesem Zweck stellt die KOBIK den ISP eine mehrmals täglich aktualisierte **Liste der zu blockierenden Domain-Namen** zur Verfügung (mit ca. 200–300 Einträgen).

Ein analoges Vorgehen ist auch gegen ausländische **Plattformen[14]** denkbar, welche widerrechtlich Werke anbieten, die urheberrechtlich geschützt sind (oder auf andere Seiten mit solchen Inhalten verweisen). Ein Beispiel ist der Fall der **Offshore-Domain kino.to**, die bis 2011 vor allem im deutschsprachigen Raum zur Verbreitung von urheberrechtlich geschütztem Filmmaterial verwendet wurde. Nach vorwiegend zivilrechtlichen Schritten blockierten die Nachbarstaaten der Schweiz den Zugang zu dieser Seite (ähnlich wurde auch gegen The Pirate Bay vorgegangen), die Schweiz jedoch nicht. Rechtliche Bestimmungen, welche dies erlaubt hätten, fehlen in unserem Land bis heute weitgehend.

---

[13] Domain Name System. Das DNS ist ein weltweit auf Tausenden von Servern verteilter hierarchischer Verzeichnisdienst, der den Namensraum des Internets verwaltet.

[14] Mit Plattformen sind hier insbesondere Internetdienstleister gemeint, die sog. file-hosting Dienste anbieten. Diese erlauben es Internetnutzern, Daten mit anderen Nutzern zu teilen, indem Dateien auf den Server der Firma hochgeladen und über einen *uniform resource locator* (URL) für andere zugänglich gemacht werden. Eine weitere Form von Plattformen sind *streaming websites*, die es den Nutzern ermöglichen, sich Inhalte direkt im Internet anzuschauen.

Die Rechteinhaber argumentierten, die DNS-Blockade sei **technisch einfach, effektiv, günstig** umzusetzen und richte sich **nicht gegen einzelne Benutzer**, sondern gegen die widerrechtlichen Anbieter von urheberrechtlich geschütztem Material. Damit wäre auch ein wichtiges **Anliegen der Bundesbehörden** erfüllt, welche eine **Kriminalisierung des Endverbrauchers verhindern** möchten. Dank der Arbeit der KOBIK verfüge man über grosse Erfahrung mit DNS-Blockaden. Die Massnahme sei auch viel einfacher umzusetzen als etwa das Senden von Warnhinweisen an die Nutzer von Peer-to-peer-Netzwerken. Zwar bieten DNS-Blockaden **keinen umfassenden Schutz** für die Rechteinhaber, es sei jedoch entscheidend, dass sie mit ihnen ein wirkungsvolles rechtliches Instrument in Händen halten würden.

Das **Bundesamt für Justiz und das BAKOM** vertraten die Position, dass bei einer allfälligen Umsetzung des Vorschlags dem **Rechtsschutz** viel Gewicht beigemessen werden müsse. So soll der Rechtsweg zu einer unabhängigen Schlichtungsstelle offenstehen, um irrtümliche Blockaden anfechten zu können. Die Schaffung einer **unabhängigen Stelle**, welche die Liste mit den zu sperrenden Seiten verwaltet, stiess auch bei den Rechteinhabern auf Zustimmung. Die Aufgabe einer solchen Behörde wäre laut ihren Vorstellungen mit derjenigen der Eidgenössischen Zollverwaltung (EZV) bei der Bekämpfung der Produktepiraterie vergleichbar. Die Rechteinhaber können bei der EZV Informationen hinterlegen, welche das Erkennen von gefälschten Produkten erleichtern. Die von Massnahmen der EZV Betroffenen hätten dabei ein **klar festgeschriebenes Rekursrecht**.

Die konkrete Ausgestaltung der gesetzlichen Grundlagen von DNS-Blockaden zum Schutz der Urheberrechte wurde von der Arbeitsgruppe nicht diskutiert. Es wurde jedoch festgehalten, dass die **KOBIK** in ihrer heutigen Form aufgrund von **Ressourcenknappheit** und des **fehlenden Auftrags** hier wohl kaum tätig werden könnte. Es wurden zudem Zweifel geäussert, ob die Kantone einer Ausweitung des Mandats der KOBIK auf die Bekämpfung von Urheberrechtsverletzungen zustimmen würden.

6.3 Voluntary best practices

Von Seiten der US-Botschaft wurde die Idee einer **freiwilligen Vereinbarung** zwischen den Rechteinhabern und den ISP eingebracht. Demnach würden die ISP ihre **AGB anpassen**, um so Massnahmen gegen Urheberrechtsverletzungen ihrer Kunden ergreifen zu können. Nach Auffassung der US-Botschaft könnte so eine (zumindest provisorische) Lösung zur Bekämpfung der Internetpiraterie gefunden werden. In den **USA** hat man mit einem vergleichbaren Arrangement bereits **Erfahrungen** sammeln können.

Für die Umsetzung dieses Vorschlages in der Schweiz sah insbesondere der Vertreter der **Rechteinhaber grundsätzliche Probleme**. Er berichtete, dass sich die Access Provider in der Schweiz auf den Standpunkt stellen würden, dass es neue gesetzliche Grundlagen für ein Tätigwerden ihrerseits brauche. Trotz jahrelangen Gesprächen mit den Access Providern hätten diese bisher keinen Schritt in Richtung einer freiwilligen Zusammenarbeit getan. Dies sei der Fall, weil sie **Wettbewerbsnachteile** befürchten, wenn sie einseitig gegen die Urheberrechtsverletzungen ihrer Kunden vorgehen würden, obwohl ein solches Vorgehen nach einer Änderung der AGB bereits heute ohne Weiteres jedem Access Provider möglich wäre.

7 Fazit und Ausblick

An ihrer Sitzung im Juni kamen die Mitglieder der Arbeitsgruppe zum Schluss, dass es an der Zeit sei, ein **Fazit** ihrer Arbeit zu ziehen. Als erstes **Ergebnis** der Gespräche lancierten die Rechteinhaber zu Beginn des Jahres 2013 ein **Musterstrafverfahren**. Weitere konkrete Massnahmen zur Gewährleistung der Urheberrechte im Internet wurden vorgestellt und diskutiert. Dabei wurden neben Massnahmen, welche innerhalb des geltenden Rechts gangbar sind, auftragsgemäss auch mögliche Vorschläge für Gesetzesänderungen geprüft. Die **Schaffung eines zivilrechtlichen Instruments**, welches die strafrechtliche Klagemöglichkeit ergänzt, erscheint mit Blick auf die Verhältnismässigkeit und die Kapazitäten der Strafverfolgungsbehörden **angezeigt**.

In einem **nächsten Schritt** würde es nun darum gehen, ein **Gesetzesvorhaben** auszuarbeiten. Mit den beschränkten Ressourcen des Roundtable einen substantiellen Beitrag zu solchen Arbeiten zu leisten, wäre allerdings nur schwer möglich. Es muss ebenfalls festgehalten werden, dass es nicht gelang, die **Vorbehalte verschiedener Bundesstellen** gegen Gesetzesänderungen in ihrem Zuständigkeitsbereich auszuräumen. Es kommt hinzu, dass der **Bundesrat** der Bundesverwaltung bisher **keinen Auftrag** für den Erlass neuen Rechts erteilt hat. Er stellte sich in der Vergangenheit auf den Standpunkt, dass ein solcher nicht angezeigt ist, solange die **Ergebnisse der AGUR12** sowie eines 2011 in Auftrag gegebenen Berichts zu den Sozialen Medien nicht vorliegen. Diese Position vertrat der Bundesrat zuletzt in seiner Antwort auf eine Motion von Nationalrätin Riklin, welche die Regelung der rechtlichen Verantwortung von Internetprovidern zum Ziel hatte.[15] Aus diesen Gründen kommt die Arbeitsgruppe zum Schluss, dass sie ihre **explorativen Arbeiten de lege ferenda bis auf Weiteres einstellt** und die weiteren Entwicklungen im Themengebiet abwartet. Weiterhin wird der Roundtable das Musterverfahren begleiten, wobei hier insbesondere der Entscheid des Obergerichtes des Kantons Zürich abzuwarten ist.

Der **Social Media Bericht des Bundesrates** in Erfüllung des Postulats Amherd wurde in der Zwischenzeit publiziert. Dieser **enthält** auch einen **Auftrag an das EJPD**, die zivilrechtliche Verantwortlichkeit von Plattformbetreibern und ISP zu untersuchen:

> *Zu prüfen ist, ob im **Zivilrecht** gesetzgeberischer Handlungsbedarf besteht, um die Zuordnung der Verantwortlichkeit von Plattformbetreibern sowie technischen Dienstleistern (Access- und Hostingprovider) zu regeln. Diese Abklärungen beschränken sich nicht auf das Phänomen der sozialen Netzwerke, sondern betreffen ganz allgemein die rechtliche Verantwortlichkeit von Online-Dienstleistern (Providern). Das EJPD wird sich dieser Frage annehmen und dem Bundesrat bei Bejahung eines Gesetzesänderungsbedarfs eine Vernehmlassungsvorlage unterbreiten.*
>
> (Social Media Bericht des Bundesrates[16], 2013, S. 80)

Man darf demnach davon ausgehen, dass viele der zentralen **zivilrechtlichen Fragen**, welche am Runden Tisch diskutiert worden sind, auch vom EJPD aufgenommen werden. Gleichzeitig könnte im Verlauf des nächsten Jahres eine **Klärung der Situation im Strafrecht** erfolgen, falls sich das Bundesgericht zum von den Rechteinhabern lancierten Musterstrafverfahren äussert.

Am 6. Dezember 2013 hat die **AGUR12** ihren **Schlussbericht** vorgelegt.[17] Darin enthalten sind auch Vorschläge für eine Reihe von Massnahmen zur besseren Durchsetzung von Urheberrechten. Diese Empfehlungen nehmen eine Reihe der Themen auf, welche auch am Roundtable besprochen wurden. So schlägt die AGUR12 vor, dass Plattformbetreiber künftig für die Verhinderung der Verteilung von urheberrechtlich geschütztem Material über ihre Server verantwortlich sein sollen, dass ISP auf behördliche Anweisung durch DNS- oder IP-

---

[15] Auszug aus der Antwort des Bundesrats auf die Motion Riklin (13.3215): „Zurzeit sind bereits verschiedene Arbeiten zu den entsprechenden Fragen im Gang, deren Ergebnisse nicht vorweggenommen werden sollten: Zum einen ist die Arbeitsgruppe zur Optimierung der kollektiven Verwertung von Urheberrechten und verwandten Schutzrechten ("Agur 12"; https://www.ige.ch/urheberrecht/agur12.html) zu nennen. Zum andern ist ein Bericht des Bundesrates in Erfüllung des Postulates Amherd 11.3912, "Rechtliche Basis für Social Media", in Arbeit, in welchem die Rechtslage in Bezug auf Social Media dargestellt und analysiert wird. Es ist geplant, dass der Bundesrat diesen Bericht noch in diesem Jahr dem Parlament vorlegen wird. Der Bundesrat wird auf der Grundlage dieser Arbeiten und der laufenden Entwicklungen im In- und Ausland prüfen, ob im Zivilrecht tatsächlich ein gesetzgeberischer Handlungsbedarf besteht. Die Motion hingegen würde den Ergebnissen der laufenden Arbeiten vorgreifen."

[16] *Rechtliche Basis für Social Media – Bericht des Bundesrates in Erfüllung des Postulats Amherd 11.3912 vom 29. September 2011*. Bericht verfügbar unter http://www.bakom.admin.ch/themen/infosociety/03932/03943/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDfH59fWym162epYbg2c_JjKbNoKSn6A

[17] Vgl. https://www.ige.ch/fileadmin/user_upload/Urheberrecht/d/Schlussbericht_der_AGUR12_vom_28_11_2013.pdf

Blocking den Zugang zu Internetseiten mit illegalen Inhalten sperren sollen und Rechteinhaber Internetverbindungsdaten für die Ermittlung von Urheberrechtsverletzungen bearbeiten dürfen. Weiter sollen wo nötig **gesetzliche Grundlagen** geschaffen werden, damit schwerwiegende Urheberrechtsverletzungen **sowohl zivil- als auch strafrechtlich verfolgt** werden können. Dazu schlägt die AGUR12 vor, die Randdaten von Anschlüssen, welche für Urheberrechtsverletzungen verwendet wurden, zu speichern, und sie auf behördliche Anordnung den Rechteinhabern bekannt zu geben. Der Bericht der AGUR12 geht nun an die **Vorsteherin des EJPD**, welche über die weitere Umsetzung seiner Empfehlungen befinden wird.

Vor diesem Hintergrund findet ein **weiteres Treffen** des Roundtable und seiner Arbeitsgruppe einstweilen erst wieder statt, wenn der Entscheid des Obergerichtes des Kantons Zürich vorliegt oder wenn die Situation dies aus anderen Gründen angezeigt scheinen lässt.

Anhang 1 – Roundtable zum Urheberrechtsschutz im Internet: Teilnehmerkreis

Bundesamt für Justiz, Fachbereich Zivilrecht und Zivilprozessrecht
Bundesrain 20, 3003 Bern

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
Feldeggweg 1, 3003 Bern

Embassy of the United States of America
Sulgeneckstrasse 19, 3007 Bern

Institut für Geistiges Eigentum
Stauffacherstrasse 65, 3014 Bern

Staatsanwaltschaft II des Kantons Zürich
Selnaustrasse 28, Postfach, 8001 Zürich

Staatssekretariat für Wirtschaft, Ressort Amerika
Holzikofenweg 36, 3003 Bern

Staatssekretariat für Wirtschaft, Ressort Internationales Wirtschaftsrecht
Holzikofenweg 36, 3003 Bern

Universal Music GmbH
Hardturmstrasse 130, 8005 Zürich

Walt Disney GmbH
Höschgasse 45, 8034 Zürich

Werder Viganò Anwälte, Rechtsberater der Swiss Anti-Piracy Federation
Genferstrasse 2, 8002 Zürich

Anhang 2 – Arbeitsgruppe des Roundtable: Teilnehmerkreis

Bundesamt für Justiz, Fachbereich Internationales Strafrecht
Bundesrain 20, 3003 Bern

Bundesamt für Justiz, Fachbereich Zivilrecht und Zivilprozessrecht
Bundesrain 20, 3003 Bern

Bundesamt für Kommunikation - BAKOM
Zukunftstrasse 44, 2501 Biel

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
Feldeggweg 1, 3003 Bern

Institut für Geistiges Eigentum, Rechtsdienst Urheberrecht
Stauffacherstrasse 65, 3014 Bern

Staatssekretariat für Wirtschaft, Ressort Amerika
Holzikofenweg 36, 3003 Bern

Staatssekretariat für Wirtschaft, Ressort Internationales Wirtschaftsrecht
Holzikofenweg 36, 3003 Bern

Werder Viganò Anwälte, Rechtsberater der Swiss Anti-Piracy Federation
Genferstrasse 2, 8002 Zürich

Weitere Stellen, welche punktuell an Sitzungen der Arbeitsgruppe teilgenommen haben:

Embassy of the United States of America[18]
Sulgeneckstrasse 19, 3007 Bern

Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK)[19]
Nussbaumstrasse 29, 3003 Bern

[18] Sitzung vom 25. März 2013

[19] Sitzungen vom 28. Januar und 25. März 2013