sbvv
Schweizer
Buchhändler- und
Verleger-Verband

Eidgenössisches Justiz und Polizeidepartement EJPD
Bundeshaus West
CH-3003 Bern

Per Mail an: Revision_URG@ipi.ch

SBVV

Limmatstrasse 111
Postfach
CH-8031 Zürich

T +41 44 421 36 00
F+ 41 44 421 36 18

info@sbvv.ch
www.sbvv.ch

Zürich, 29. März 2016

Vernehmlassung zur Änderung des Urheberrechtsgesetzes

Allgemeine Einschätzung

Der Schweizer Buchhändler- und Verleger-Verband SBVV **befürwortet die grundsätzliche Stossrichtung der URG-Revision,** namentlich die Absicht, den Rechteinhabern endlich einfache und effiziente Werkzeuge zur Bekämpfung der Internetpiraterie in die Hände zu geben.

Wir begrüssen die Absicht, den AGUR12-Konsens in die Vorlage aufzunehmen. **Die Umsetzung weist jedoch über weite Strecken erhebliche handwerkliche und konzeptionelle Mängel auf,** die es dringend zu beheben gilt. Ansonsten drohen die Bemühungen gegen die gewerbliche Internet-piraterie ein (äusserst kostspieliger und bürokratischer) Papiertiger zu bleiben – oder im schlimmsten Fall sogar kontraproduktive Wirkungen zu zeigen.

Die allgemeinen Anpassungen an die aktuellen Erfordernisse eines modernen Urheberrechts sind mit Blick auf die Interessen von Urhebern, Produzenten und Konsumenten ausgewogen und massvoll ausgestaltet. Im Bereich der vorgeschlagenen Schranken ist dies jedoch nur teilweise gelungen: **Uns überzeugen weder das vorgeschlagene Verleihrecht noch die Ausnahmeregelung für „*text and data mining*" (TDM).**

Schliesslich sind die Regelungen über die Aufsicht über die Verwertungsgesellschaften unseres Erachtens ganz zu streichen. Sie sind unnötig und verletzen zudem die Eigentumsgarantie sowie die Wirtschaftsfreiheit der Urheber und Rechteinhaber.

Stellungnahme zu einzelnen Artikeln

1. Vermieten und Verleihen von Werkexemplaren (Art. 13, Absatz 1 und 2)

Der SBVV lehnt das Verleihrecht in der vorgeschlagenen Form ab.

Begründung: Gegen eine Entschädigung der Urheber ist grundsätzlich nichts einzuwenden. Die vorliegende Lösung jedoch hat einen gravierenden Mangel, der u.a. auch Hauptgrund der Opposition durch die Bibliotheken selbst ist: Der Vorschlag müsste konkret benennen, woher das zusätzliche Geld für die Ausschüttung von Beiträgen für den Verleih genommen wird.

Ist dies wie im vorliegenden Entwurf nicht der Fall, werden die Mittel wohl von den Bibliotheken aufgebracht werden müssen – obwohl das die Initianten des Vorschlags nicht beabsichtigen. In Zeiten, wo deren Anschaffungs-Etats stark unter Druck oder bereits gekürzt worden sind, würde dies zu einem Bumerang-Effekt für das gesamte Buch-Ökosystem führen: Bibliotheken würden weniger Bücher einkaufen, worunter nicht nur weniger bekannte Autorinnen und Autoren, sondern auch die hiesigen Verlage und Buchhandlungen zu leiden hätten.

Bei elektronischen Büchern wäre eine kollektive Entschädigung für den Verleih zudem sachfremd, schliessen doch Bibliotheken mit den Verlagen bereits Lizenzverträge ab, wo der Anteil an Tantiemen für Autoren und Verlage privatrechtlich geregelt ist.

2. Verwendung von verwaisten Werken (Art. 22b)

Die Vorlage erweitert richtigerweise den Verwendungsbegriff für verwaiste Werke. Der SBVV unterstützt diesen Vorschlag.[1]

Allerdings lässt der vorgeschlagene Art. 22b offen, wie festgestellt wird, ob ein Werk als „verwaist" gelten kann. Hier regen wir die Einführung einer „diligent search" nach dem Vorbild der Richtlinie 2012/28/EU (Verwaiste-Werke-Richtlinie) an.

Für die eindeutigen Fälle ist eine zentrale Anlaufstelle für entsprechende Verwendungen vorgesehen. Diese Rechte sollen über eine zugelassene Verwertungsgesellschaft abgegolten werden. Der SBVV unterstützt diesen Vorschlag, meldet allerdings Bedenken hinsichtlich der praktischen Umsetzung, welche kompliziert und aufwändig wird. Wir schlagen vor, ein einfacheres Verfahren für eine zentrale Rechteregelung zu prüfen und im Sinne einer effizienten und mit angemessenen Vergütungen versehenen Lösung einzuführen.

3. Verwendung von Werken zu wissenschaftlichen Zwecken (Art. 24 Abs. 1^{bis})

Der SBVV unterstützt diese Bestimmung mit der unabdingbaren Ergänzung, dass diese Werkexemplare einzig zur Sicherung und Erhaltung ihrer Bestände hergestellt und genutzt werden dürfen und auch nachträglich keine andere Nutzung, insbesondere keine wirtschaftliche oder kommerzielle Nutzung der hergestellten Kopien, stattfinden darf. Diese Bedingungen sind dem Artikel in der bisherigen Form nicht zu entnehmen und sollten ergänzt werden.

4. Verwendung von Werken zu wissenschaftlichen Zwecken (Art. 24d)

Die Bestimmung regelt die systematische Anwendung von technologisch basierten Methoden, die der Suche, Analyse und Vernetzung von Daten zu wissenschaftlichen Forschungszwecken dienen (*text and data mining*, TDM). **Eine derartige Ausnahme scheint aus Sicht des SBVV nicht angezeigt,** denn entweder findet TDM (a) in lizenzierten Werken statt und ist deshalb ohne weiteres vertraglich gestattet, oder es lässt sich (b) eine entsprechende Lizenz erwerben oder (c) die Nutzung fällt unter eine der bereits bestehenden Ausnahmen des Eigengebrauchs.

[1] In den Erläuterungen zum URG-Revisionsentwurf ist vermerkt, der SBVV würde den Vorschlag ablehnen. Dies ist ein Fehler, dessen Ursprung nicht eruiert werden konnte.

Der Bundesrat erklärte zum Ziel, den Austausch von Forschungsergebnissen durch die vorgesehene Ausnahme zu ermöglichen. Mit dem vorgeschlagenen Artikel wird dieses Ziel verfehlt. Denn vom Urheberrechtsschutz ausgenommen sind nur Vervielfältigungen, die durch die Anwendung eines technischen Verfahrens bedingt sind. Das Teilen von Werkexemplaren oder abgeleiteten Werken innerhalb von (internationalen) Forschungsgruppen ist keine technische Bedingung. Solche Werknutzungen fallen unter Art. 19 Abs. 1 lit. c URG oder sind zu lizenzieren.

Der SBVV unterstützt die Möglichkeit von TDM, allerdings auf lizenzierter Basis. Die *International Association of Scientific Technical and Medical Publishers* (STM) hat eine entsprechende Deklaration betreffend TDM mit verbindlichen Verpflichtungen der Wissenschaftsverlage erarbeitet.[2] Diese Deklaration wurde von zahlreichen Verlagen bereits unterzeichnet. Der Ratifikationsprozess ist noch nicht abgeschlossen. Diese Deklaration stellt sicher, dass Abonnenten wissenschaftlicher Zeitschriften, also in der Schweiz sämtliche Mitglieder des Konsortiums der Schweizer Hochschulbibliotheken, ohne Aufpreis von TDM uneingeschränkt profitieren können. Weshalb Nichtabonnenten von einer quasi durch die Bibliotheken finanzierten TDM-Möglichkeit profitieren sollen, erschliesst sich dem SBVV nicht. Vollends unverständlich wird der vorgeschlagene Artikel dann, wenn man sich vor Augen führt, dass die dem Konsortium angeschlossenen Bibliotheken eine Abgabe auf eine Leistung bezahlen müssten, für die sie bereits ein Abonnement gelöst haben.

Zusammenfassend: Wer schon für eine Zeitschrift bezahlt hat, soll uneingeschränkt und ohne zusätzliche Abgaben TDM betreiben dürfen. Alle anderen sollen dafür eine Lizenz lösen, welche die verlegerischen Leistungen gebührend berücksichtigt.

Sollte trotzdem eine Ausnahme für nötig erachtet werden, ist diese enger zu formulieren. Die im Vernehmlassungsentwurf vorgeschlagene Regelung offenbart zahlreiche Lücken: Zunächst ist festzulegen, dass eine Ausnahme nur Anwendung findet, sofern auf dem Markt kein entsprechendes Produkt oder eine entsprechende Lizenz angeboten wird. Sodann müsste eine solche Bestimmung klar definieren, welche Sicherheits- und Zuverlässigkeits-Anforderungen Plattformen mit einem TDM-Angebot erfüllen müssen (ohne entsprechende Sicherheitsvorschriften besteht nämlich die Gefahr, dass Vervielfältigungen, die beim TDM angefertigt werden, frei und für jedermann im Internet zugänglich sind). Und schliesslich ist die Ausnahme auf nicht-kommerzielle Forschung zu beschränken.[3]

5. Bestandesverzeichnisse (Art. 24E)

Der SBVV ist mit diesem Vorschlag grundsätzlich einverstanden, der im Wesentlichen dem Vorschlag im AGUR12-Schlussbericht entspricht. Die verwendeten Texte sollen sich auf die offiziellen *Abstracts* oder eine kurze Zusammenfassung beschränken. Bilddarstellungen sind wenn möglich mit einem Wasserzeichen der sie verwendenden Institutionen zu versehen.

[2] http://www.stm-assoc.org/2015_11_10_Text_and_Data_Mining_Declaration.pdf

[3] Für kommerzielle Nutzer, wie z.B. für die Pharmazeutische Industrie, wird TDM schon seit langem durch den Markt sichergestellt. Auch hier hat STM – zusammen mit dem *Pharma Documentation Ring* (PDR)- ein Modell-Lizenzierungsvorschriften erarbeitet. Darüber hinaus bietet die CCC (*Copyright Clearence Center*) ein *text and data mining*-Modell an, welches es der Pharmaindustrie gestattet, in eine maschinelle Verarbeitung Inhalte einzubeziehen, welche das betreffende Pharma-Unternehmen (noch) nicht abonniert hat (*RightFind™ XML for Mining*). Es besteht demnach kein Grund, hier in einen bestehenden Markt einzugreifen.

6. Rechte des Herstellers oder der Herstellerin von Pressefotografien

Die Einführung eines umfassenden Lichtbildschutzes ist zu begrüssen. Die vorgeschlagene Beschränkung auf Pressefotografien, solange „diese für die aktuelle Berichterstattung von Interesse“ sind, stellt ein unscharfes Abgrenzungskriterium dar. Wie soll das Ende des Interesses an der aktuellen Berichterstattung festgestellt werden?

Ohnehin führt die Abgrenzung von urheberrechtlich geschützten Fotografien und nicht geschützten „Schnappschüssen“ bei der gerichtlichen Beurteilung zu nicht immer leicht nachvollziehbaren Resultaten. Es wäre daher sinnvoll, einen umfassenden Lichtbildschutz einzuführen, wie er etwa in Deutschland oder Österreich bereits seit langem besteht.

7. Aufsicht über die Verwertungsgesellschaften (Änderungen in den Art. 40 - 53 URG, Art. 13 IGEG, Art. 83 BGG)

Die Regelungen verletzten die Eigentumsgarantie und die Wirtschaftsfreiheit der Urheber und Rechteinhaber. Am System der Aufsicht über die Verwertungsgesellschaften muss aus Sicht des SBVV nichts geändert werden. Sie funktioniert mehrheitlich zur Zufriedenheit der Betroffenen. Im Fall von ProLitteris, welcher die Debatte erst ausgelöst hat, war es nicht primär die fehlende Aufsicht von aussen, sondern interne Mechanismen, die zu einigen Fehlentwicklungen geführt haben.

Zu den Vorschlägen des Bundesrates im Einzelnen:

- **Aufsicht:** Aufsicht über die Verwertungsgesellschaften ausdehnen auf Bereiche, in welchen es keinen Zwang zur kollektiven Verwertung gibt.

  Der SBVV lehnt den Vorschlag staatlicher Einschränkung privater Rechte ab. Er bevormundet Urheber und Produzenten. Sie sollen selbst entscheiden, wie sie neben gesetzlich vorgeschriebenen Bereichen Rechte wahrnehmen.

- **Geschäftsführung:** Aufsichtsbehörde soll Angemessenheit der Geschäftsführung der Verwertungsgesellschaften prüfen.

  Der SBVV lehnt dies ab: Der Vorschlag bevormundet Urheber und Produzenten. Die Aufsichtsbehörde soll höchstens dann einschreiten, wenn Fälle von Rechtsmissbrauch vorlägen. Eine durch aussenstehende Experten durchgeführte Kostenanalyse hat den Verwertungsgesellschaften Ende 2015 insgesamt kostenbewusstes Wirtschaften attestiert, beim „Klassen-Schlechtesten“ ProLitteris wurden durch die neue Führung Massnahmen zur Verbesserung eingeleitet.

- **Zuweisung der Einnahmen:** Die Aufsichtsbehörde soll über Angemessenheit der Bestimmungen zur Verteilung der Einnahmen der Verwertungsgesellschaften entscheiden.

  Der SBVV lehnt dies ab: Der Vorschlag bevormundet Urheber und Produzenten. Die Verteilung der Gelder regeln die Gesellschaften bisher mehr oder weniger konfliktfrei. Es gibt keinen Anlass zu einem staatlichen Eingriff.

Statt verschärfter Aufsicht ist die Effizienz der Verwertungsgesellschaften mit einfachen Massnahmen zu verbessern, darunter gehören die Beschleunigung des Tarifgenehmigungs-verfahrens (Rückkehr zum alten Rechtsweg: Beurteilung des Tarifs durch paritätische Schieds-

kommission, direkte Beschwerdemöglichkeit ans Bundesgericht) oder der **Zugang zu Registerdaten:** Ergänzung des URG in Art. 51, um den Verwertungsgesellschaften eine kostengünstige Abwicklung für die Ausgestaltung und Durchsetzung der Tarife zu ermöglichen.

8. Pirateriebekämpfung (Änderungen in den Art 62 Abs. 1bis, Art. 62a, Art. 66b-66k URG)

Der Bundesrat hat in der Vorlage die richtigen und unbestrittenen Handlungsfelder definiert. Bezüglich der Ausgestaltung der Massnahmen und den Durchsetzungsprozessen besteht jedoch erheblicher Verbesserungsbedarf. Die vorgeschlagenen Massnahmen sind grösstenteils praxisfremd, kompliziert, schwerfällig, kostentreibend oder teilweise gar kontraproduktiv formuliert.

Der SBVV ist Teil der „Allianz gegen Internetpiraterie" und unterstützt die in der entsprechenden Vernehmlassungsantwort genannten Aussagen integral. Die zentralen Punkte sind zusammengefasst die Folgenden:

- **„Take-down"/„Stay-down":** Die Anforderungen an die Selbstregulierung müssen deutlicher definiert werden (Effizienz, Kooperation und Nachhaltigkeit), um wirksam zu werden. Als Alternative fordert der SBVV eine Branchenvereinbarung unter Einschluss der Rechteinhaber.

- **Zugangssperren:** Die Voraussetzungen für Zugangssperren müssen praxistauglicher werden (insbes. Phase vor/während Lancierung), auch Portalseiten mit massenhafter Vermittlung oder Durchleitung zu Uploads müssen gesperrt werden können und die Provider sind an den Kosten zu beteiligen.

- **Datenschutz:** Die Datenerhebung durch Verletzte zum Zweck des gesetzlichen Rechtsschutzes muss wie in anderen Lebensbereichen zulässig sein und die Massnahme muss technologieneutral ausgestaltet werden (statt beschränkt auf veraltete P2P-Netzwerke). Falls eine Bekanntgabepflicht eingeführt wird, ist sie praktikabler zu definieren.

- **Mitteilung an „Verletzer"/Offenlegung Identität:** Es ist eine (statt 2) sichere Mitteilungen an alle „Verletzer" vorzusehen (nicht nur P2P, sondern technologieneutral, siehe oben) und es sind praxistaugliche, sehr viel kürzere Fristen zu definieren (insbesondere heikelste Phase vor/während Erstveröffentlichung in der Schweiz).

Zu den Vorschlägen des Bundesrates im Einzelnen:

a) "Take-down"/"Stay-down" / Selbstregulierung

I. „Take-down" (Sperren/Entfernen durch Hosting Provider) – Art. 66b Abs. 1-3

Zweck und Ziele

Dass der Hosting-Provider, dessen Server rechtsverletzenden Inhalt beherbergen, diesen bei Kenntnis entfernt oder unzugänglich macht („Take-down"), ist prinzipiell bereits heutige Rechtspflicht, um nicht selber für seine Mitwirkung zur Verantwortung gezogen zu werden (Unterlassung/Beseitigung, Art. 61 Abs. 1 URG); allerdings sind deren Konturen bis heute unklar. Zugleich ist dies, in der Schlüsselposition des Providers, der nächstliegende Schritt zur Beseitigung der Verletzung, v.a. wo nicht auf den „Uploader" selber (Nutzer des Providers) zugegriffen werden kann. **Daher ist die Regelung des „Take-down" einer der Kernpunkte der neuen Bestimmungen** (Art. 66b Abs. 1 und 3).

Wichtig ist, dass dieser Mechanismus einfach, laufend und in grosser Zahl und Frequenz beansprucht werden kann. Musik, Filme oder Bücher werden zu Zehntausenden und immer wieder aufs Neue widerrechtlich zugänglich gemacht, und dabei auf solchen Diensten beherbergt. Ziel einer wirksamen gesetzlichen Regelung ist daher nicht nur, die „Take-down"-Pflicht als solche klarzustellen, sondern damit **Rechtsinhabern einen Rechtsbehelf zu geben, der wirksam, rasch, effizient**[4] **und zu vertretbaren Kosten den Verletzungen abhilft.** D.h., Provider müssen zu einfachen Mechanismen Hand bieten, was in erster Linie die Selbstregulierung (oder besser: Ko-Regulierung durch eine Branchenvereinbarung; siehe dazu Abschnitt 2.1., Rz. 35ff.) bewirken soll. Im Gegenzug werden die Provider von weitergehenden Pflichten freigestellt (Art. 66k), selbst wo sie nach allgemeinen Regeln haften würden, also privilegiert.

Wenn der Gesetzentwurf auf die Definition der „Anbieterinnen abgeleiteter Kommunikationsdienste" gemäss Art. 2 Bst. c des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) verweist, so ist offensichtlich dessen revidierte Fassung gemeint (dort: „Anbieterinnen von Diensten, die sich auf Fernmeldedienste stützen und eine Einweg- oder Mehrwegkommunikation ermöglichen"). Dessen geltende Fassung enthält keine solche Vorschrift. Die Revision befindet sich noch im parlamentarischen Gesetzgebungsprozess, und gegen sie könnte das Referendum ergriffen werden. Für den Fall, dass das revidierte BÜPF nicht oder nicht mit dieser Bestimmung in Kraft tritt, muss der Anwendungsbereich im URG autonom definiert werden.

Angesichts der Unbestimmtheit des Begriffs, der auch noch keine praktische Auslegung erfahren hat, ist es bedeutend, alle solchen Anbieter, deren Dienstleistungen für rechtsverletzende Werknutzungen gebraucht werden, zu erfassen; namentlich auch sogenannte „Social Media" Plattformen, die das Zugänglichmachen geschützter Inhalte vermitteln; dies unbeschadet der Frage, ob und in welchen Fällen das Angebot geschützter Inhalte auf solchen Plattformen diesen als eigenes Zugänglichmachen zuzurechnen ist und daher nicht unter den „sicheren Hafen" für

[4] Bericht, S. 72

solche Dienstanbieter fallen würde. Hierbei wären auch für die Zwecke des URG die Erläuterungen der Botschaft zum revidierten BÜPF (BBl. 2013, 2708) zu Grunde zu legen:

> Buchstabe c erfasst die Anbieterinnen von zwei Arten von Internetdiensten: Die einen ermöglichen eine Einwegkommunikation, die das Hochladen von Dokumenten gestattet (zum Beispiel Google docs oder Microsofts office.live.com), die anderen eine Mehrwegkommunikation, welche die Kommunikation zwischen Nutzerinnen und Nutzern erlaubt (zum Beispiel Facebook). Dabei ist nicht von Belang, ob die Kommunikation synchron oder asynchron erfolgt. Unter diesen Buchstaben fallen zum Beispiel Anbieterinnen von Speicherplatz für E-Mails, die verschiedenen Arten von Webhostern (Hosting-Provider), die z.B. das Hosting von Anwendungen oder E-Mail-Diensten (z.B. gmx), Hosting in Form von «server colocation» oder «server housing» mit Zugriff (z.B. Green.ch und Colt), «facility management»-Hosting ohne Kommunikationsdienste (reine Colocation) oder Cloud-Services anbieten; ebenfalls unter diesen Buchstaben fallen Chat-Plattformen, Plattformen für den Dokumentenaustausch sowie Anbieterinnen von Internettelefoniediensten des Typs Peer-to-Peer (z.B. Skype Peer-to-Peer). […] Es ist […] zu beachten, dass ein Unternehmen, zum Beispiel Swisscom, aufgrund seiner Tätigkeiten zugleich als Fernmeldedienstanbieterin (Buchstabe b) gilt und unter Buchstabe c fallen kann, weil es neben seiner Tätigkeit als Internetzugangsvermittler auch als E-Mail-Provider oder Webhoster (Hosting- Provider) in Erscheinung tritt. […].

Kritik und Verbesserungsbedarf

II. „Take-down“ auch für Portalseiten (Art. 66b Abs. 1)

Im Entwurf geht es um den „Take-down“ bestimmter, auf Servern des Providers beherbergter Werkdaten (Art. 66b Abs. 1 am Ende). Die Dienste solcher Provider werden aber auch zur Beherbergung von so genannten Portalseiten und anderen Vermittler-Diensten genutzt, die (ebenfalls und in besonderem Masse schädigend) den Zugang zu solchen Werken in hoher Zahl vermitteln, während diese selber dezentral oder unauffindbar beherbergt werden. **Falls eine solche Portalseite bei einem Schweizer Provider beherbergt wird, ist „Take-down“ das geeignetere Mittel, diese zu beseitigen, als Zugangssperren (vgl. Art. 66d Abs. 1),** und sollte deshalb ebenfalls möglich sein. Das bedarf einer Klarstellung.

> [1] Anbieterinnen abgeleiteter Kommunikationsdienste […] haben […] den Zugang zu widerrechtlich öffentlich zugänglich gemachten Werken oder anderen Schutzobjekten <u>oder Angeboten, die den widerrechtlichen Zugang zu solchen Werken vermitteln</u> […] zu sperren oder diese von ihren Servern zu entfernen.
>
> [2] Sie leiten dem Kunden oder der Kundin, der oder die das betreffende Werk oder andere Schutzobjekt widerrechtlich öffentlich zugänglich gemacht <u>oder vermittelt</u> hat (Inhaltsanbieter oder Inhaltsanbieterin), die Mitteilung nach Absatz 1 weiter und informieren ihn oder sie über die Möglichkeit des Widerspruchs und dessen Folgen nach Absatz 3.
>
> [3] […] den Zugang zum betreffenden Werk, ~~oder~~ anderen Schutzobjekt <u>oder Vermittlungsangebot</u> zu entsperren […]
>
> [4] […] oder wenn das betreffende Werk, ~~oder~~ andere Schutzobjekt <u>oder Vermittlungsangebot</u> aufgrund eines Gerichtsentscheids oder einer Einigung wieder gesperrt oder von den Servern entfernt wird, […]

III. „Take-down“ auch bei Kenntnis (Art. 66b Abs. 1)

Nach Art. 66b Abs. 1 soll „Take-down“ stets eine Mitteilung von aussen erfordern. Es ist nicht ersichtlich, warum der Provider – entgegen allgemeinen Grundsätzen und anders als in der EU[5] –

[5] Art. 14 Abs. 1 E-Commerce-Richtlinie (2000/31)

nicht auch tätig werden müsste, wenn er selber (ohne nachforschen zu müssen) Kenntnis von offensichtlichen und schwerwiegenden Verletzungen erlangt (z.B. bei Portalen, die massenhaft Piraterie anbieten). Zudem ist es für den Rechtsschutz zentral, dass die Sperrung umgehend erfolgt.

> [1] Anbieterinnen abgeleiteter Kommunikationsdienste […] haben auf Mitteilung der in ihrem Urheber- oder verwandten Schutzrecht verletzten Person oder einer zuständigen Behörde oder bei Kenntnis einer Verletzung den Zugang […] umgehend zu sperren […]

Weiteres

Zentral ist die Angabe der Identität des mutmasslichen Verletzers, der vom Widerspruch (Art. 66b Abs. 3) Gebrauch macht, samt einer Zustelladresse in der Schweiz sowie einer kurzen Begründung des Widerspruches. Nur so kann gegen ihn vorgegangen werden; andernfalls lädt das Widerspruchsrecht zum Missbrauch ein, und der „Take-down" geht ins Leere. Das Zustellungsdomizil ist der mitteilenden (geschädigten) Person daher mit bekanntzugeben (Art. 66b Abs. 3 S. 2).

> „…werden die Identität und das Zustellungsdomizil … bekanntgegeben …"

Nach Art. 66b Abs. 3 zwingt der blosse Widerspruch eines Nutzers den Provider ausnahmslos, den Inhalt wieder freizuschalten - selbst wenn dieser offensichtlich rechtsverletzend sein sollte, also z.B. ein Film während dessen Kinoauswertung oder ein Tonträger vor dessen offiziellem Release. In diesem Fall sollte der Provider aber nicht gezwungen werden können, an der Rechtsverletzung mitzuwirken.

> [3] Auf begründeten Widerspruch des Inhaltsanbieters oder der Inhaltsanbieterin […] haben Anbieterinnen abgeleiteter Kommunikationsdienste umgehend den Zugang zum betreffenden Werk oder anderen Schutzobjekt zu entsperren […], wenn es sich nicht um ein offensichtlich widerrechtliches Angebot handelt.

IV. „Stay-down" (Wieder-Upload verhindern) – Art. 66b Abs. 4/66c Abs. 2, Satz 2

Zweck und Ziele

Art. 66b Abs. 4 sieht Massnahmen vor, die verhindern sollen, dass vom Provider entfernte Inhalte sogleich wieder hochgeladen werden („Stay-down"). Darunter werden zum Teil aktive Massnahmen verstanden (wie z.B. aktive Suche nach Links des Providers, die in Filesharing-Portalen publiziert wurden, und mittels Suchmaschinen und Webcrawlern nach verletzenden Angeboten, die vom eigenen Dienst ausgehen). Auf der anderen Seite sind die Grenzen zu einem wirksamen „Take-down" („sperren oder entfernen" gem. Art. 66b Abs. 1), wenn dieses nicht von vornherein ins Leere gehen soll, fliessend. Es geht demnach um ein sehr breites Spektrum an möglichen Massnahmen, die nicht undifferenziert geregelt werden sollten.

Richtig ist es, Anbieter, deren Geschäftsmodell auf der Förderung von Rechtsverletzungen beruht (bzw. die sich der Selbstregulierung verweigern), strengeren Pflichten – namentlich weiter gehenden „Stay-down"-Pflichten – zu unterwerfen (Art. 66b Abs. 4); wobei das „technisch und wirtschaftlich (!) Zumutbare" auch nach solchen Geschäftsmodellen zu bemessen ist. **Rücksichtnahme auf die Profitabilität rechtsgefährdender Geschäftspraktiken wäre fehl am Platz.**

Ebenso sinnvoll ist es, rechtskonformen Anbietern unter Selbstregulierung (einen hohen Standard sowie die Einhaltung ihrer Pflichten vorausgesetzt) einen „sicheren Hafen" zu bieten.

Kritik und Verbesserungsbedarf

Nachhaltigkeit des „Take-down“ auch bei regulierten Anbietern

Dieser „sichere Hafen“ darf nicht zur Folge haben, dass diese Anbieter gänzlich jeder Verantwortung für die Nachhaltigkeit ihres „Take-down“ entledigt wären, wie dies Art. 66c Abs. 2, Satz 2 in seiner Absolutheit nahelegt (so auch die lapidare Anmerkung im Bericht, S. 74). **Die Pflicht, rechtsverletzende Uploads zu sperren oder zu entfernen, impliziert stets schon eine gewisse Vorsorge, diese Entfernung aufrecht zu erhalten; sonst ist sie von vornherein nicht wirksam.** Das Reglement sollte regeln, welche – angemessenen – Massnahmen auch regulierte Anbieter treffen müssen, um Rechtsverletzungen nachhaltig und nicht bloss symbolisch zu beseitigen. Erprobte und praktikable Lösungen wie „Content-ID“-Software, die geschützte Werkdaten erkennt (und damit unerlaubten Wieder-Upload verhindern helfen kann), werden heute bereits von den grössten Internet-Dienstanbietern routinemässig eingesetzt und Rechtsinhabern angeboten. Die Selbstregulierung darf nicht dazu führen, dass ein Schweizer Provider, der es in die SRO schafft, hinter dem „State of the art“ des Rechtsschutzes zurückbleiben darf und per se nur noch im Minimum für „Take-down“-Massnahmen verantwortlich wäre. Es bedarf daher geeigneter gesetzlicher Vorgaben für das SRO-Reglement (siehe unten).

Weitere Einzelheiten

Auch ein regulierter Provider muss jedenfalls weitergehend (u.a. auf „Stay-down“; Art. 66c Abs. 2, Satz 2) in die Verantwortung genommen werden können, wenn er seinen gesetzlichen und reglementarischen Pflichten nicht nachkommt (entsprechend Art. 66k Abs. 1); es kann nicht schon der blosse Anschluss zur Entlastung genügen.

> „…gilt nicht für angeschlossene Anbieterinnen …, welche ihren Pflichten nach Gesetz und Branchenvereinbarung nachkommen“

Wenn Art. 66b Abs. 4 die „Stay-down“-Pflichten daran knüpft, dass gegen den „Take-down“ kein Widerspruch erhoben (oder dann das Verfahren abgeschlossen) wurde, ist zu beachten, dass für den Widerspruch keine Frist vorgesehen, also nicht absehbar ist, ob und wann er erhoben wird. Richtigerweise ist der „Stay-down“ daher zu gewährleisten, solange das nicht der Fall ist.

> [4] ~~Wird~~ Solange kein Widerspruch erhoben oder wenn ~~wird~~ das betreffende Werk, ~~oder~~ andere Schutzobjekt […] nach Abschluss des Verfahrens nach Absatz 3 wieder gesperrt oder von den Servern entfernt wird, ~~so~~ haben die Anbieterinnen abgeleiteter Kommunikationsdienste im Rahmen des technisch und wirtschaftlich Zumutbaren zu verhindern, dass das Werk oder andere Schutzobjekt Dritten erneut über ihre Server angeboten wird.

Weder für den „Take-down“ nach Abs. 3, noch für den „Stay-down“ nach Abs. 4 kann es auf Endentscheide („Klärung der Angelegenheit“ durch die Gerichte?; Abschluss des Verfahrens?) ankommen; eine vorsorgliche Massnahme (oder eine Einigung) genügt:

> Abs. 3 […] haben Anbieterinnen abgeleiteter Kommunikationsdienste […] zu entsperren oder […] wieder auf den Server zu laden, ~~bis die Angelegenheit zwischen den betroffenen Personen oder durch die Gerichte geklärt ist~~. vorbehältlich des Entscheids eines Gerichts oder einer Einigung…
>
> Abs. 4 […] oder wird das betreffende Werk oder andere Schutzobjekt ~~nach Abschluss des Verfahrens nach Absatz 3~~ aufgrund eines Gerichtsentscheids oder einer Einigung wieder gesperrt oder von den Servern entfernt […]“

V. Selbstregulierung – Art. 66c

Zweck und Ziele

Der Entwurf bietet den Providern im Rahmen eines Selbstregulierungs-Modells sehr weitgehenden „sicheren Hafen" vor jeglicher Verantwortung, die über die reglementarischen Pflichten hinaus geht. Ob dies in der Praxis tatsächlich zu verantwortungsbewusster Geschäftspraxis und wirksamem Rechtsschutz führt, oder lediglich ein Schlupfloch bietet, sich dieser Verantwortung zu entziehen, wird entscheidend von den Anforderungen an die Teilnahme an einer solchen Selbstregulierungs-/Branchenlösung sowie von den Standards für die reglementarischen Pflichten abhängen. Dafür bietet der Entwurf keine Gewähr.

Kritik und Verbesserungsbedarf

Branchenvereinbarung statt einseitigem Reglement

Der Entwurf sieht eine einseitige Selbstregulierung der Provider unter sich vor. Das setzt deren Wirksamkeit und Effizienz bedauerliche Grenzen. **Ein wirksamer Schutz wäre besser zu gewährleisten, wenn die Massnahmen in Koordination und Kooperation mit den Rechtsinhabern getroffen würden;** also in einer Branchenvereinbarung zwischen Rechteinhabern und Providern zu regeln wären (Ko-Regulierung). So sind am besten allseits akzeptable, effiziente Vorkehrungen zu finden, die erforderlichen Kommunikationswege einzurichten, Aufwand und Kosten der rechtlich gebotenen Massnahmen tief zu halten und angemessen zuzuweisen. In den USA, Grossbritannien und den Niederlanden etwa haben sich solche Branchenvereinbarungen etabliert. „Massgebende Verbände" können analog Art. 46 Abs. 2 URG bestimmt werden. Eine solche – effiziente! – Regelung ist zweifellos auch im Interesse der Provider. Nicht effizient ist es, Provider solche Massnahmen einseitig ohne Abstimmung mit den betroffenen Rechtsinhabern regeln zu lassen; ebenso wenig, deren Rechtsschutzbedürfnis nur auf dem Umweg der staatlichen Aufsicht durch das IGE zur Geltung zu bringen.

> [2] Die Selbstregulierungsorganisationen ~~erlassen ein Reglement~~ verhandeln mit betroffenen Inhabern von Urheber- und verwandten Schutzrechten bzw. deren massgebenden Verbänden eine Branchenvereinbarung und überwachen die Einhaltung der ~~reglementarischen~~ darin geregelten Pflichten durch die angeschlossenen Anbieterinnen abgeleiteter Kommunikationsdienste. Die Pflicht nach Artikel *66b* Absatz 4 gilt nicht für angeschlossene Anbieterinnen abgeleiteter Kommunikationsdienste.

Ungenügende Standards der Selbstregulierung

Die Regelung ist an das Vorbild der SRO der Finanzintermediäre nach GWG angelehnt. Dort hat sich die Selbstregulierung bewährt - allerdings vor dem Hintergrund klarer, anspruchsvoller und umfassender gesetzlicher Vorgaben. Selbstregulierung muss hohen gesetzlichen Standards unterworfen sein, soll sie nicht zum blossen Alibi werden und Providern dazu dienen, sich wirksamer Massnahmen gerade zu entziehen.

Es konterkariert geradezu das Konzept einer Selbstregulierung, wenn die Anforderungen an das Reglement bzw. die Vereinbarung (Art. 66c Abs. 3 Bst. a-c) praktisch wortgleich (ein Verweis hätte es hier getan) dieselben sind, denen das Gesetz die Provider ohnehin unterwirft (Art. 66b Abs. 1^{bis} 3); noch nicht einmal alle (Art. 66c Abs. 4, Freistellung von „Stay-down"-Bemühungen), und nichts

darüber hinaus; allein dafür aber im Gegenzug den Providern das Privileg der Haftungsbefreiung nach Art. 66k gewährt wird.

Umso weniger ist mit wirksamen Massnahmen zu rechnen, wenn der bestehende „simsa Code of Conduct“ zum Massstab der gesetzlich geforderten Regulierung erklärt wird.[6] Dessen - ohne gesetzliche Vorgaben aufgestellten - Minimal-Regeln waren einzig an der Selbst-Absicherung der Provider, bei ungesicherter Rechtslage, nicht aber an dem nunmehr vom Gesetz bezweckten wirksamen Rechtsschutz orientiert, bleiben hinter internationalen Standards zurück und taugen nicht als gesetzlicher Standard.

Für das Anforderungsprofil der SRO hat demnach das Gesetz (oder eine Verordnung) den Standard für Effizienz, Kooperation und Nachhaltigkeit zu setzen (die Details sollten dann autonom geregelt werden). Es genügt, sich vergleichsweise vor Augen zu führen, welche gesetzlichen und Verordnungs-Standards von Unternehmen etwa im Bereich des Datenschutzes (Kontakt, Auskunftsrechte, Sicherheitsvorkehrungen und dergleichen) oder anderen Bereichen verlangt werden. Für die Provider-Selbstregulierung wären das namentlich:

- **Vorgaben betreffend solcher Geschäftsmodelle, die nicht anschlusstauglich sind** (Art. 66c Abs. 1, Satz 2) (etwa Nutzer-Anonymität, fehlende Kontaktmöglichkeit zu Kunden, fehlende Reaktionsbereitschaft von Kunden; Rechtsdurchsetzung hindernde AGB, Anreize zur Werkverbreitung, Werkverbreitung als Umsatztreiber)
- **Massnahmen zur Nachhaltigkeit der „Take-down“-Massnahmen** (wie „State-of-the-art“-Lösungen zur Erkennung und Identifizierung geschützter Werke/ Schutzgegenstände, insbesondere illegal wieder hochgeladener Werke, wie Content-ID)
- **Praktikable Formen der Verletzungsanzeigen;** namentlich auch elektronische Kommunikation (Datentransfers) und eine Möglichkeit, massenhaft rechtsverletzende Dienste zu (z.B. Schnittstellen für Datentransfers) und Portalseiten (mittels repräsentativer Auswahl anstatt vollständiger Dokumentation tausender einzelner Werke) anzuzeigen
- **Zusammenarbeit mit Rechteinhabern** zwecks Vereinfachung der Verletzungsanzeigen und Verfahren
- **Kontaktmöglichkeit für Geschädigte** (usw.)

[1] […] Einer Selbstregulierungsorganisation nicht anschliessen dürfen sich Anbieterinnen abgeleiteter Kommunikationsdienste, deren Geschäftsmodell auf der Förderung systematischer Urheberrechtsverletzungen aufbaut, insbesondere indem Nutzern des Dienstes Anonymität gewährt wird, die Anbieterin auf Kontaktmöglichkeiten zu Nutzern verzichtet, Vertragsbedingungen anwendet, die der Erfüllung ihrer Pflichten entgegenstehen, oder Anreize für rechtsverletzende Nutzungen des Dienstes setzt oder durch wiederholte rechtsverletzende Nutzungen aufgefallen ist.

[3] Die Branchenvereinbarung regelt die Voraussetzungen für den Anschluss und Ausschluss von Anbieterinnen abgeleiteter Kommunikationsdienste sowie die Pflichten der angeschlossenen Anbieterinnen abgeleiteter Kommunikationsdienste und soll einen wirksamen und effizienten Rechtsschutz gewährleisten. Insbesondere folgende Pflichten müssen den Anbieterinnen abgeleiteter Kommunikationsdienste auferlegt werden:

> a. die Pflicht, dem Inhaltsanbieter oder der Inhaltsanbieterin die Mitteilung der in ihrem Urheber- oder verwandten Schutzrecht verletzten Person, wonach dieser oder diese ein Werk oder anderes Schutzobjekt widerrechtlich öffentlich zugänglich gemacht habe, weiterzuleiten und ihn oder sie auf die Möglichkeit des Widerspruchs und dessen Folgen hinzuweisen;

[6] Bericht S. 74, 1. Abs.

b. die Pflicht, auf Mitteilung der in ihrem Urheber- oder verwandten Schutzrecht verletzten Person den Zugang zum betreffenden Werk oder anderen Schutzobjekt nach Buchstabe a umgehend zu sperren oder dieses vom Server zu entfernen;

c. die Pflicht, auf Widerspruch eines Inhaltsanbieters oder einer Inhaltsanbieterin, der oder die ein Zustellungsdomizil in der Schweiz bezeichnet, umgehend den Zugang zum betreffenden Werk oder anderen Schutzobjekt zu entsperren oder das betreffende Werk oder andere Schutzobjekt wieder auf den Server zu laden, bis die Angelegenheit zwischen den betroffenen Personen oder durch die Gerichte geklärt ist; hierfür wird die Identität des Inhaltsanbieters der mitteilenden Person bekanntgegeben;

d. die Pflicht, dem Stand der Technik gemässe Verfahren anzuwenden, um ihren Pflichten nach Art. 66b Abs. 1 wirksam nachkommen zu können;

e. die Pflicht, Rechteinhabern einfach zugängliche Kontaktmöglichkeiten und effiziente Kommunikationswege für Verletzungsanzeigen zur Verfügung zu stellen und sich mit diesen darüber abzustimmen.

[4] Die mit der Kontrolle der Einhaltung der ~~reglementarischen~~ Pflichten nach Gesetz und Branchenvereinbarung betrauten Personen und Organe müssen von der Geschäftsleitung und der Verwaltung der kontrollierten Anbieterinnen abgeleiteter Kommunikationsdienste unabhängig sein.

[5] Das IGE beaufsichtigt die Selbstregulierungsorganisationen. Es genehmigt die von den Selbstregulierungsorganisationen ~~erlassenen Reglemente~~ abgeschlossenen Branchenvereinbarungen nach Absatz 2 sowie deren Änderungen.

Weiteres

In jedem Falle bedarf es einer Regelung für den Fall, dass die vorgesehene Selbstregulierung (bzw. Ko-Regulierung) nicht innert nützlicher Frist zustande kommt. Dann sollten entsprechende Regelungen per Verordnung erlassen werden. Dessen ungeachtet, wäre dann Art. 66b uneingeschränkt anwendbar.

Sofern die vorgesehene Branchenvereinbarung nicht in angemessener Frist zustande kommt, trifft der Bundesrat geeignete Regelungen.

b) Zugangssperren – Art. 66d und 66e

Zweck und Ziele

Wo besonders schwer schädigende Plattformen massenhaft und für grosse Nutzerzahlen unrechtmässig Werke anbieten bzw. vermitteln, aber weder die Betreiber der Plattform, noch die zahllosen „Uploader", noch die Provider, die die Plattform beherbergen, in der Schweiz rechtlich greifbar sind (Ausland, Verschleierung), **kommt den Internet-Anschlussanbietern in der Schweiz eine Schlüsselstellung für den Rechtsschutz zu.** Der Schaden, den solche Plattformen in der Schweiz anrichten, kann und muss eingedämmt werden, indem die Access-Provider verpflichtet werden, im Netz (d.h. den Internet-Abonnenten in der Schweiz) den Zugang dazu zu sperren (oder erheblich zu erschweren, was bereits den Schaden signifikant eingrenzt). **Dies ist das zweite Kernstück der Vorlage.** Die Grundzüge eines rechtsstaatlichen Vorgehens hierbei hat der EuGH[7] exemplarisch festgestellt, was eine Orientierungshilfe bietet.

[7] 27.3.2014 (C-314/62)

Kritik und Verbesserungsbedarf

Der Entwurf sieht ein auf den ersten Blick einfaches und rechtsstaatlich abgesichertes Behördenverfahren vor, dessen Voraussetzungen sich aber im Einzelnen als völlig untauglich, ja kontraproduktiv erweisen.

Portalseiten nicht erfasst

Im Wortlaut richtet sich die Regelung gegen „Angebote von Werken und anderen Schutzobjekten" (Art. 66d Abs. 1) unter der Voraussetzung (u.a.), dass das Angebot „das Werk […] zugänglich macht" (Abs. 2 Bst. b).

Wörtlich verstanden wären das nur Dienste, die selber „uploaden"; somit würde sich der Anspruch allein auf den Zugang zu den konkreten Werken richten, an denen der Gesuchsteller berechtigt ist („Wer in seinem […] Recht verletzt wird", Abs. 1).

Die Vorstellung, es könne eine Adresse oder Seite gesperrt werden, auf der nur gerade ein Werk zugänglich ist, ist abwegig. In der Realität werden Sperren vor allem gegen sogenannte Portalseiten, Linksammlungen und dergleichen benötigt (und im Ausland angewendet), die als „Schaltstelle" das Zugänglichmachen und Auffinden von Piraterie-Angeboten zu Tausenden ermöglichen, auch ohne selber „Uploader" zu sein.

Solche Angebote müssen gesamthaft gesperrt werden, wenn feststeht, dass sie offensichtlich (und in grosser Zahl) Piraterie-Angebote vermitteln, ohne dass im Einzelfall die Aktivlegitimation an den (typischerweise tausenden) zugänglichen Filmen oder Musikproduktionen nachzuweisen wäre – was schlicht nicht möglich ist.

Unter diesen Umständen sollte – wie auch sonst im Urheberrecht – **nicht nur die akute Verletzung, sondern auch die Gefährdung des Rechts Schutzansprüche gewähren:**

> [1] Wer in seinem Urheber- oder verwandten Schutzrecht verletzt oder gefährdet wird, kann vom IGE verlangen, dass es die Anbieterinnen von Fernmeldediensten mit Sitz in der Schweiz verpflichtet, den Zugang zu Angeboten von Werken und anderen Schutzobjekten respektive zu Seiten, welche solche Angebote ~~enthalten~~vermitteln, zu sperren.
>
> [2] Das IGE verfügt die Sperrung eines Angebots […], wenn die verletzte oder gefährdete Person glaubhaft macht, dass die folgenden Voraussetzungen erfüllt sind: […]
>
> Mittels des ~~Das~~ Angebots ~~macht~~ werden ~~das~~ Werke oder andere Schutzobjekte in grosser Zahl in nach diesem Gesetz offensichtlich widerrechtlicher Weise zugänglich gemacht.

Rechtmässiger Zugang

Weiter setzt der Entwurf voraus, dass das Werk von der Schweiz aus rechtmässig zugänglich oder rechtmässig erhältlich ist (Abs. 2 Bst. d).

Diese Voraussetzung ist illegitim, denn sie respektiert nicht das Recht des Urhebers zu bestimmen, ob, wann und wie das Werk verwendet wird (Art. 10 Abs. 1).

Sie ist kontraproduktiv, weil sie den Rechtsinhaber gerade in der kritischen Phase, bevor sein Werk in legalen Vertriebswegen oder Onlineangeboten erhältlich ist (Lizenzverhandlungen, Vermarktung, Lancierung, vorgelagerte Verwertungshandlungen wie Kino oder Konzert) schutzlos lässt.

Sie ist unbrauchbar, weil kein Rechteinhaber sie je beanspruchen könnte: Kein Einzelner wäre in der Lage, zu gewährleisten oder auch nur glaubhaft zu machen, alle Tausende Filme oder Musikproduktionen einer solchen Plattform seien legal erhältlich.

Im Ergebnis hätte eine solche Vorschrift gerade gegenteilige Wirkung und würde Massen-Piraterie-Angebote entgegen allen urheberrechtlichen Grundsätzen geradezu legitimieren: Weil der Nachweis legaler Angebote nicht möglich ist, würden die illegalen Plattformen letztlich toleriert.

> **Art. 66d Abs. 2 Bst. d ist ersatzlos zu streichen.**

Kosten

Es ist nicht gerechtfertigt, sämtliche Kosten dem (ohnehin) Geschädigten anzulasten (Art. 66d Abs. 3). Rechtsverletzungen durch Nutzer sind auch bei anerkannten Fernmeldedienstanbietern unvermeidbarer (und umsatzrelevanter) Teil ihres eigenen Geschäfts.[8] Diese sind bereits nach Art. 1 Abs. 2 Bst. a (i.V.m. Art. 58 Abs. 1 Bst. a) FMG verpflichtet, einen die Immaterialgüterrechte achtenden Fernmeldeverkehr sicherzustellen. **Kosten der Vorkehrungen, die ein rechtskonformer Geschäftsbetrieb erfordert, sind grundsätzlich Teil des Geschäftsaufwands.** Die Allianz hatte bereits, als vermittelnde Lösung, eine angemessene Teilung der Kosten zwischen Provider und Rechtsinhaber vorgeschlagen. Der Entwurf begünstigt nunmehr einseitig die Provider, die ihre eigene Compliance vom Geschädigten finanziert bekommen, ja als „Service" vermarkten könnten.

Noch weitergehend führt der Erläuternde Bericht (S. 71) aus, es sei voller Ersatz ausgewiesener Kosten geschuldet, und diese seien per se ein klagbarer Anspruch des Providers. Mit anderen Worten: Auf dieser Basis könnte ein Geschädigter Rechtsschutz nur gegen das Risiko erlangen, nachher einer beliebigen, nicht absehbaren Kostenforderung ausgesetzt zu sein. **Ein solches Kostenrisiko ist für Geschädigte schlicht nicht tragbar; schon gar nicht im Zuge eines behördlich angeordneten Verfahrens zur Beseitigung schwerwiegender, massenhafter Rechtsverletzung und -gefährdung.**

> [3] Die Anbieterin von Fernmeldediensten kann von der in ihrem Urheber- oder verwandten Schutzrecht verletzten Person~~en~~ einen angemessenen Beitrag an die Abgeltung ihrer ~~haben die Anbieterinnen von Fernmeldediensten für die~~ Kosten ~~der~~ für die Sperrung verlangen ~~angemessen zu entschädigen~~.

Ungeachtet der Kostenteilung zwischen Geschädigtem und Provider, darf die gesetzliche Regelung nicht dazu führen, dass dem Geschädigten (Regress-) Schadenersatzansprüche gegen den Verletzer abgeschnitten werden. Das könnte sich aber daraus ergeben, dass dem Geschädigten eine gesetzliche Zahlungspflicht auferlegt wird, die er womöglich nicht als Schaden geltend machen könnte.

> […] Im Verhältnis der in ihren Rechten verletzten oder gefährdeten zur rechtsverletzenden Person gilt Art. 62 Abs. 2 entsprechend.

[8] Vgl. nur die damalige PTT in BGE 121 IV 109, Telekiosk.

c) Offenlegung – Art. 62a

Zweck und Ziele

Ein drittes Kernstück des mit dem Entwurf verfolgten Konzepts soll es sein, **wenigstens in Fällen schwerer Rechtsverletzungen durch Internet-Nutzer (hinter denen sich sowohl Privatpersonen als auch kriminelle Organisationen verbergen könnten) die Anschlussinhaber offenzulegen, damit auf dem Zivilrechtsweg gegen sie vorgegangen werden kann.** Das soll namentlich auch die übermässige Beanspruchung von Strafverfahren – heute der einzige gegebene Rechtsbehelf in solchen Fällen – eindämmen.

Dieses Ziel verfehlt der Entwurf (Art. 62a, 66g), der eine in mehrfacher Hinsicht nicht praxistaugliche Regelung vorsieht:

Kritik und Verbesserungsbedarf

Unverständliche Beschränkung auf „Peer-to-Peer"-Technologie

Der Eingriff ist nur für „Peer-to-Peer"-Netzwerke vorgesehen (Art. 62a Abs. 2 Bst. a Ziff. 2; Art. 66g Abs. 1; per Verweis auch Art. 66j). Offenbar folgt dies der Vorstellung, nur in solchen Netzwerken finde die Verbreitung dezentral statt, fehle es an einem „zentralen Serverbetreiber", und sei ein „Blocking" nicht statthaft (Bericht, 68 f.).

Was unter einem „Peer-to-peer-Netzwerk" zu verstehen ist, ist nicht hinreichend bestimmt, um als abschliessendes gesetzliches Tatbestandsmerkmal zu dienen. **Die Festlegung auf eine „Filesharing"-Technologie widerspricht grundlegend der Technologieneutralität des Urheberrechts.** Diese Organisationsform der Internet-Piraterie ist bereits heute nicht die einzige: Bereits sind andere „dezentrale" Filesharing-Technologien mit gleichen Problemen gebräuchlich (z.B. das „Share-Hosting" mit einer Vielzahl wechselnder und rechtlichem Zugriff entzogener „Share-Hoster"). In der Zukunft könnten weitere Organisationsformen und Technologien hinzukommen. Das Gesetz muss eine technologisch neutrale Regelung vorsehen.

Gerade in solchen Netzwerken tun sich einzelne Internet-Nutzer (oder Organisationen) auch in der Schweiz als „Feeder" und „Heavy Uploader" mit dem Zugänglichmachen neu veröffentlichter Werke oder grosser Mengen geschützter Werke hervor. Diese direkt zur Verantwortung zu ziehen, ist sowohl gerechtfertigt (auch im Interesse der übrigen Internet-Nutzer), als auch zur Abhilfe notwendig. Das Warnhinweis-/Offenlegungsverfahren sollte daher immer anwendbar sein, wo weder „Take-down" (beim Hosting-Provider) noch Sperre (beim Fernmeldedienstanbieter) in Betracht kommen; mindestens aber bei allen Formen „dezentralisierter Datenaustauschsysteme" (Bericht S. 79).

Art. 62a Abs. 2 Bst. a Ziff. 2 ist ersatzlos zu streichen

Voraussetzung der erfolgten aufklärenden Hinweise (Warnhinweise) ist untauglich

Die in ihren Rechten verletzte Person kann unmöglich glaubhaft machen, dass der Teilnehmer oder die Teilnehmerin in den letzten 12 Monaten zwei „aufklärende Hinweise" (hier vereinfacht als „Warnhinweise" bezeichnet) erhalten habe. Woher soll die in ihren Rechten verletzte Person das wissen? Die IP-Adressen werden im Internet dynamisch vergeben, also immer wieder neu vergeben. Deshalb ist es auch für einen eifrigen Ermittler im Internet nur möglich fest zu stellen,

dass es viele Rechtsverletzungen gibt (also eine schwerwiegende Verletzung vorliegt). Ob diese jedoch durch immer wieder die gleiche Person oder durch mehrere unterschiedliche Personen begangen wurden, kann so nicht festgestellt werden.

Art. 62a Abs. 2 Bst. a Ziff. 3 ist ersatzlos zu streichen

Die Voraussetzungen in Art. 62a Abs. 2 sind auf Buchstabe a Ziff. 1, also auf "schwerwiegende Verletzung" zu beschränken. Allerdings ist die Definition anzupassen:

Definition „schwerwiegende Verletzung"

Die Beschränkung auf „schwerwiegende" Rechtsverletzungen hätte zur Folge, dass grosse Teile der Rechtsverletzungen de facto nicht verfolgt werden können. Dies, während es gegenüber den Anschlussinhabern zunächst nicht um (schwerwiegende) Sanktionen geht, sondern um blosse Warnhinweise; und höchstens im Renitenzfall darum, die mutmasslichen Rechtsverletzungen gerichtlich überprüfbar zu machen. Selbst das könnte hinzunehmen sein im Gegenzug für schnelle und effiziente Rechtsbehelfe bei wirklich schwerwiegende Verletzungen, bei denen es für die Auswertung darauf ankommt. (Allemal besser wäre, in Umkehr geeignet definierte Bagatellfälle freizustellen.) Genau das leistet der Entwurf nicht:

Was eine „schwerwiegende Verletzung" (Art. 62a Abs. 2 Bst. a Ziff. 1, 66g Abs. 1) ist, sollte grundsätzlich nach den Umständen des Einzelfalls und in der Kompetenz der Gerichte zu beurteilen sein. Eine eingrenzende und abschliessende (!) Definition wie in Art. 62a Abs. 4 genügt bereits rechtsstaatlichen Grundsätzen nicht: Davon nicht erfasste, wenngleich tatsächlich schwerwiegende Verletzungen müssten schutzlos hingenommen werden.

Dies umso weniger, als die vorgeschlagene Definition am Schutzbedarf völlig vorbeizielt, weil sie nur zwei Fallgruppen erfasst (bis zur Veröffentlichung und wieder ab der physischen oder Online-Verbreitung), zwischen denen das Werk, in einer besonders kritischen Phase seiner Auswertung, ungeschützt über solche Netzwerke zugänglich gemacht werden könnte.

Die erste Fallgruppe greift zu kurz, weil sie mit der (Erst-)Veröffentlichung (Art. 9 Abs. 3 URG; ggf. irgendwo auf der Welt) endet, während es ab dann längere Zeit brauchen kann, Auswertungsverträge (z.B. Lizenzen für die Schweiz) für das Werk zu verhandeln, Marketing und Öffentlichkeitsarbeit zu betreiben, je nach Medium auch zuerst exklusivere, primäre Auswertungsformen (Kino, Konzerte) zu bedienen. Gerade in dieser Phase ist Piraterie besonders schädlich (z.B. für laufende Lizenzverhandlungen).

Für die zweite Fallgruppe kann es hingegen nicht darauf ankommen, dass die widerrechtlich zugänglich gemachten Werke tatsächlich verfügbar sind. Das widerspricht dem Recht der Urheber zu bestimmen, ob, wann und wie das Werk verwendet wird (Art. 10 Abs. 1), also Schutz auch für aktuell nicht verfügbare Werke zu beanspruchen (etwa um eine optimale Auswertung vorbereiten und steuern zu können).

Es wäre auch bei der hierfür vorausgesetzten grossen Zahl betroffener Werke schlicht gar nicht möglich, diese Voraussetzung auch nur glaubhaft zu machen; zumal kein Rechtsinhaber je die Rechte an allen (oft tausenden) Titeln eines solchen Angebots für sich beanspruchen kann. In solchen Fällen ist ja gerade eine grosse Zahl von Werken und von Rechtsinhabern betroffen.

Zur blossen Abgrenzung von der ersten Fallgruppe ist dies völlig entbehrlich: Es genügt entweder die Störung der vorgängigen Auswertung (Bst. a) oder die grosse Zahl (Bst. b).

Auch dieser Rechtsbehelf ist nicht auf eigentliche „Uploader“ zu beschränken, sondern muss die Betreiber von Plattformen des Filesharing einschliessen, sofern diese sich eines schweizerischen Internet-Zugangs bedienen und über diesen ermittelbar sind.

> [4] Eine schwerwiegende Verletzung liegt insbesondere vor, wenn:
>
> ein Werk oder anderes Schutzobjekt ~~vor seiner Veröffentlichung~~ widerrechtlich zugänglich gemacht wurde, bevor es mit Einwilligung der Rechtsinhaber für unbeschränkte Nutzerkreise verbreitet oder auf Abruf zugänglich gemacht wurde; oder
>
> eine grosse Anzahl von Werken oder anderen Schutzobjekten, ~~die rechtmässig zugänglich oder erhältlich sind~~, widerrechtlich zugänglich gemacht wurden oder dies wesentlich gefördert wird.

Verfügbarkeit der Daten

Ungeachtet der Aufbewahrungsfristen etwa nach Art. 15 Abs. 3 BÜPF (6 Monate) gilt es zu vermeiden, dass der Fernmeldedienstanbieter während des laufenden Warnungs-Prozesses (je nach dessen Dauer, s.u.) die notwendigen Daten zur Teilnehmeridentifikation aufgibt und das laufende Verfahren folglich ins Leere geht. Daher sollte das Gesetz (als Rechtfertigung wie als Pflicht) deren Aufbewahrung während der Verfahrensdauer (gem. Entwurf 12 Monate, Art. 62a Abs. 2 Bst. a Ziff. 3) vorsehen. Das ist gerechtfertigt, weil es nur die Daten des einzelnen Falls betrifft, in dem ausreichende Anhaltspunkte für eine schwerwiegende Rechtsverletzung vorliegen, und die Daten zur Bearbeitung des gesetzlich vorgesehenen Verfahrens nötig sind (keine Vorratsdatenspeicherung).

> Art. 62a Abs. 2 Bst. b: Die Anbieterin von Fernmeldediensten verfügt im Zeitpunkt des Begehrens (Abs. 1) über Daten, die eine Identifikation der Teilnehmer oder Teilnehmerinnen noch erlauben. Diese Daten sind bis zum Abschluss des Verfahrens durch die Anbieterin von Fernmeldediensten aufzubewahren.

Offenlegung

Der Entscheid einer (zentralen und routinierten) Behörde über die Offenlegung wäre bedeutend effizienter als die Belastung der Gerichte mit diesem Verfahren. Geschädigte, die ohnehin ihren Rechtsschutz vor Gericht geltend machen müssen, hätten nicht Kosten und Risiko zweier gerichtlicher Verfahren in jedem einzelnen „Verletzer“-Fall zu tragen. Alternativ könnten der Offenlegungsentscheid (als Vorfrage) und Klage bzw. Massnahmengesuch in einem einheitlichen Verfahren behandelt werden.

Kosten

Auch bei den Massnahmen für Warnhinweise und Offenlegung ist es nicht gerechtfertigt, sämtliche Kosten dem (ohnehin) Geschädigten anzulasten (Art. 62a Abs. 3). Rechtsverletzungen durch Nutzer sind auch bei anerkannten Fernmeldedienstanbietern unvermeidbarer (und umsatzrelevanter) Teil ihres eigenen Geschäfts[9]. Auf die Erläuterungen zu Art. 66b Abs. 3 wird verwiesen.

> [3] Die Anbieterin von Fernmeldediensten kann von der in ihrem Urheber- oder verwandten Schutzrecht verletzten Person~~en~~ vorschussweise einen angemessenen Beitrag an die Abgeltung ihrer ~~haben die Anbieterinnen von Fernmeldediensten für die~~ Kosten ~~der~~ für die Identifizierung verlangen ~~angemessen zu entschädigen~~, sofern diese Kosten nicht direkt dem Verletzer auferlegt werden können.

Ungeachtet der Kostenteilung zwischen Geschädigtem und Provider, darf die gesetzliche Regelung nicht dazu führen, dass dem Geschädigten (Regress-) Schadenersatzansprüche gegen den

[9] Vgl. nur die damalige PTT in BGE 121 IV 109, Telekiosk.

Verletzer abgeschnitten werden. Das könnte sich aber daraus ergeben, dass dem Geschädigten eine gesetzliche Zahlungspflicht auferlegt wird, die er womöglich nicht als Schaden geltend machen könnte.

> […] Im Verhältnis der in ihren Rechten verletzten oder gefährdeten zur rechtsverletzenden Person gilt Art. 62 Abs. 2 entsprechend.

d) Warnhinweis – Art. 66g

Kritik und Verbesserungsbedarf

Der Entwurf zu Art. 66g verkennt die Abläufe im Internet: Unter anderem wird bei der Verwendung dynamischer IP-Adressen (die also pro Anschluss mit jeder Session wechseln) ohne die Identifikation des Anschlusses gar nicht feststellbar sein, ob dieser „für eine schwerwiegende Verletzung der Urheber- oder verwandten Schutzrechte ... verwendet" wurde. Dies kann sich ja gerade daraus ergeben, dass der Anschluss laufend (unter jeweils neuer IP-Adresse) für Rechtsverletzungen benutzt wird. **Mehr als der Verdacht einer schwerwiegenden Rechtsverletzung kann – jedenfalls für die Mitteilung an den Dienstanbieter – nicht verlangt werden; sonst, wird niemand in der Lage sein, in solchen schwerwiegenden Fällen das Versenden von Warnhinweisen zu fordern.**

Weiter geht der Entwurf an der Praxis und den Marktumständen bei der Auswertung von Urheberrechten vorbei: Sämtliche digital verfügbaren Werke wie Filme, Musikalben, Bücher, Games etc. erzielen ihre weitaus grössten Einnahmen in den ersten paar Wochen/Monaten ab ihrer Veröffentlichung. **Das vorgesehene Verfahren betreffend Warnhinweise dauert derart lange, dass es per se immer viel zu spät kommt und folglich nicht benutzt werden wird.**

Das Verfahren bis zur Offenlegung eines (renitenten) Rechtsverletzers ist mit wiederholtem Warnhinweis zu aufwendig und kompliziert, und mit den implizierten Fristen viel zu lang, um gegen einen Täter in der Schweiz wirksam Schutz zu bieten. Namentlich in den „schwerwiegenden Fällen" nach Art. 62a Abs. 4 Bst. a (Schutz vor und während der Primärauswertung) ist es offensichtlich, dass während einem Verfahren von mindestens vier Monaten Wartefristen (zuzüglich der Dauer zweier gerichtlicher Verfahren – Offenlegung und Massnahmen – und Bearbeitungsfristen) der grösste Schaden längst angerichtet sein wird.

Ein einziger Warnhinweis, ggf. in doppelter (elektronischer und schriftlicher) Form; und eine Frist zur Abklärung und Anpassung von zwei Wochen genügen völlig. Dies erlaubt ein zügiges Vorgehen zur Beseitigung der (schwerwiegenden!) Verletzung, und wahrt die Interessen eines allenfalls unbelasteten Anschlussinhabers ausreichend. Das Verfahren führt ja nicht (wie HADOPI o.ä.) direkt zu Sanktionen, sondern nur zur Offenlegung seiner Identität, worauf ihm die Möglichkeit, seine Nicht-Beteiligung etwa unter Verweis auf den Missbrauch durch andere Anschlussbenutzer einzuwenden, gewahrt bleibt. Unter diesen Umständen ist es nicht erforderlich, den Anschlussinhaber – falls er nicht ohnehin der Verletzer ist – bis in den Vorsatz zu treiben (so der Bericht, S. 70), um der Verletzung abzuhelfen. In anderen Lebensbereichen sind auch Privatpersonen sogar verschuldensunabhängiger Haftung ausgesetzt (Werkeigentümerhaftung, Art. 58 f. OR); und gewisse Sorgfaltsanforderungen zur Missbrauchsvorkehr beim Betrieb eines Internetanschlusses, der Dritten zugänglich ist, sollten sich von selbst verstehen.

Pflicht zur Abhilfe

Auch nach der Vorstellung des Bundesrats müsste der Anschlussinhaber, der sich keiner eigenen Verletzung gewahr ist, die Frist nach dem Warnhinweis gebrauchen, um dem mutmasslichen Missbrauch seines Anschlusses nachzugehen und diesem abzuhelfen (Bericht, S. 79). Das muss im Gesetz aber auch so vorgesehen sein. Andernfalls böte sich jedem Anschlussinhaber die Möglichkeit, sich der Verantwortlichkeit mit der blossen Behauptung zu entziehen, andere (Mitnutzer) seien für die Verletzungen verantwortlich, es sei aber nicht bekannt, wer und wie den Anschluss bei den Verletzungen benutzt habe. Den Rechtsinhabern wäre damit das Vorgehen verwehrt, denn zivilrechtlicher Schutz „gegen unbekannt" ist nicht zu erlangen.

Art. 66g Zustellung der aufklärenden Hinweise

[1] Auf Mitteilung der in ihrem Urheber- oder verwandten Schutzrecht verletzten Person oder einer zuständigen Behörde stellen die Anbieterinnen von Fernmeldediensten den Teilnehmern und Teilnehmerinnen, sofern begründeter Verdacht besteht, dass deren Anschluss für eine schwerwiegen- de Verletzung der Urheber- oder verwandten Schutzrechte ~~über Peer-to-Peer- Netzwerke~~ verwendet werden, einen ~~ersten~~ aufklärenden Hinweis zu. Dieser kann elektronisch und/oder in Papierform übermittelt werden.

[2] [Ersatzlos streichen und ersetzen durch:] Will der Anschlussinhaber geltend machen, für über seinen Anschluss begangene schwerwiegende Verletzungen nicht verantwortlich zu sein, so hat er umgehend Massnahmen zu ergreifen, um die missbräuchliche Verwendung seines Anschlusses zu unterbinden.

[3] Erfolgt frühestens nach zwei ~~Monaten~~ Wochen ~~seit der Zustellung des zweiten aufklärenden Hinweises~~ und spätestens nach zwölf Monaten seit der Zustellung des ~~ersten~~ aufklärenden Hinweises eine ~~dritte~~ weitere Mitteilung einer in ihrem Urheber- oder verwandten Schutzrecht verletzten Person oder einer zuständigen Behörde, so informieren die Anbieterinnen von Fernmeldediensten die Person oder Behörde über den oder die bereits erfolgten Hinweise und die Möglichkeit, die Identität der Teilnehmer und Teilnehmerinnen, deren Anschluss für die Verletzung verwendet wurde, zu erfahren (Art. 62a).

[4] Wenn innerhalb der Frist nach Absatz 3:

a. keine ~~dritte~~ zweite Mitteilung erfolgt, […];

b. eine ~~dritte~~ zweite Mitteilung erfolgt, […].

Kosten

Es ist (einmal mehr) nicht gerechtfertigt, sämtliche Kosten dem ohnehin Geschädigten anzulasten (Art. 66d Abs. 3). Dies ist auch eine ungerechtfertigte Abweichung vom Prinzip, dass schlussendlich der Verletzer resp. Mittäter und Gehilfe die Kosten tragen muss, auch wenn sie der Rechteinhaber allenfalls teilweise bevorschusst.

Rechtsverletzungen durch Nutzer sind auch bei anerkannten Fernmeldedienstanbietern unvermeidbarer (und umsatzrelevanter) Teil ihres eigenen Geschäfts.[10] Diese sind nach Art. 1 Abs. 2 Bst. a (i. V.m. Art. 58 Abs. 1 Bst. a) FMG ohnehin verpflichtet, einen die Immaterialgüterrechte achtenden Fernmeldeverkehr sicherzustellen. **Kosten der Vorkehrungen, die ein rechtskonformer Geschäftsbetrieb erfordert (Compliance), sind grundsätzlich Teil des Geschäftsaufwands.** Die „Allianz gegen Internetpiraterie" hatte bereits, als vermittelnde Lösung, eine angemessene Teilung der Kosten zwischen Provider und Rechtsinhaber vorgeschlagen. Der Entwurf begünstigt nunmehr einseitig die Provider, die ihre eigene Compliance vom Geschädigten finanziert bekommen, ja als „Service" vermarkten könnten.

[10] Vgl. nur die damalige PTT in BGE 121 IV 109, Telekiosk.

Noch weitergehend, führt der Erläuternde Bericht (S. 71) aus, es sei voller Ersatz ausgewiesener Kosten geschuldet, und diese seien per se ein klagbarer Anspruch des Providers. Mit anderen Worten: Auf dieser Basis könnte ein Geschädigter Rechtsschutz nur gegen das Risiko erlangen, nachher einer beliebigen, nicht absehbaren Kostenforderung ausgesetzt zu sein. Ein solches Kostenrisiko ist für Geschädigte schlicht nicht tragbar; schon gar nicht im Zuge eines behördlich angeordneten Verfahrens zur Beseitigung schwerwiegender, massenhafter Rechtsverletzung und Rechtsgefährdung.

> [5] Die Anbieterin von Fernmeldediensten kann von der in ihrem Urheber- oder verwandten Schutzrecht verletzten Person~~en~~ vorschussweise einen angemessenen Beitrag an die Abgeltung ihrer ~~haben die Anbieterinnen von Fernmeldediensten für die~~ Kosten ~~der~~ für die Zustellung der aufklärenden Hinweise und der damit verbundenen Kosten verlangen ~~angemessen zu entschädigen~~, sofern diese Kosten nicht direkt dem Verletzer auferlegt werden können.

Ungeachtet der Kostenteilung zwischen Geschädigtem und Provider, darf die gesetzliche Regelung nicht dazu führen, dass dem Geschädigten (Regress-) Schadenersatzansprüche gegen den Verletzer abgeschnitten werden. Das könnte sich aber daraus ergeben, dass dem Geschädigten eine gesetzliche Zahlungspflicht auferlegt wird, die er womöglich nicht als Schaden geltend machen könnte.

> […] Im Verhältnis der in ihren Rechten verletzten oder gefährdeten zur rechtsverletzenden Person gilt Art. 62 Abs. 2 entsprechend.

e) Provider-Privileg – Art. 66k

Zweck und Ziele

Wenn Art. 66k Provider, die ihren jeweiligen speziellen gesetzlichen Pflichten nachkommen, im Übrigen vollständig von der Verantwortlichkeit für Urheberrechtsverletzungen freistellt („sicherer Hafen“ bzw. „Providerprivileg“ nach dem Vorbild der E-Commerce-Richtlinie 2000/31 der EU), so setzt das voraus, dass diese Pflichten (v.a. in der Selbstregulierung) ihrerseits der tatsächlichen Verantwortung der Provider gerecht werden.

Das muss auch solche Umstände betreffen, die in den Art. 66b und 66c sowie 62a Abs. 2, 66d und 66g nicht ausdrücklich geregelt, aber vorausgesetzt sind; namentlich Kenntnis der eigenen Kunden, zugängliche Kontakte für Anzeigen der Rechteinhaber, die zur Pflichterfüllung benötigten vertraglichen Regelungen der Kundenbeziehungen inklusive griffiger AGB und adäquate technischen Mittel. Andernfalls wäre die Freistellung nicht gerechtfertigt.

Kritik und Verbesserungsbedarf

Die Formulierung scheint nicht sehr geglückt. Sie sollte klarstellen, dass nur die tatsächliche Erfüllung der Pflichten (im jeweiligen Fall) die Freistellung bewirkt.

Die vergleichbaren Bestimmungen des EU-Rechts[11] stellen zudem klar, dass Access-Provider nur privilegiert sind, sofern sie nicht selber auf den Datenverkehr Einfluss nehmen, und Hosting-Provider, wenn die Verletzung nicht aus ihrer eigenen Sphäre stammt. Dies muss auch in der Schweiz gelten.

[11] Art. 14 Abs. 2 E-Commerce-Richtlinie 2000/31 der EU

Art. 66k Ausschluss der Verantwortlichkeit

[1] Sofern Anbieterinnen abgeleiteter Kommunikationsdienste, ~~die~~ ihren Pflichten nach den Artikeln 66b und 66c Absätze 2 und 3 nachkommen ~~wahrnehmen~~, können sie nicht verantwortlich gemacht werden für:

Urheberrechtsverletzungen durch ~~ihre~~ dritte Inhaltsanbieter und Inhaltsanbieterinnen, die sich ihres Dienstes bedienen; […]

[2] Sofern Anbieterinnen von Fernmeldediensten~~,~~ ~~die~~ die Datenübermittlung weder veranlassen noch deren Adressaten oder Inhalt bestimmen oder ändern und ihren Pflichten nach den Artikeln 62a Absatz 2, 66d Absatz 2 und 66g nachkommen ~~wahrnehmen~~, können nicht verantwortlich gemacht werden für: […]

f) Leistungsklagen

Zweck und Ziele

Art. 62 Abs. 1bis gewährt Rechtsinhabern klagbare Ansprüche gegen einen Hosting Provider, der seine gesetzlichen bzw. reglementarischen Provider-Pflichten verletzt. Gemäss Erläuterndem Bericht (S. 68) soll es dabei um die Durchsetzung dieser neuen Pflichten selber gehen (also „Take-down", „Notice", Offenlegung, ggf. „Stay-down"). Kommt er diesen Pflichten nach, ist er nach Art. 66k Abs. 1 (im Übrigen) von der Verantwortung für Rechtsverletzungen seiner Nutzer freigestellt.

Festzuhalten ist, dass gegenüber fehlbaren Providern, die nicht durch Art. 66k Abs. 1 privilegiert sein können, auch nicht nur die darin genannten neuen Pflichten (nach Art. 62a Abs. 2, 66b, 66c Abs. 2 und 3, 66g) durchsetzbar sind, sondern prinzipiell alle Ansprüche (insbesondere Unterlassungs- und Beseitigungsansprüche), die sich unter den Umständen des jeweiligen Falles aus Art. 62 ergeben; und dass zudem Schadenersatzansprüche vorbehalten bleiben (Art. 62 Abs. 2). Art. 66k soll Rechtssicherheit und einen „sicheren Hafen" für rechtstreue Anbieter schaffen, nicht aber auch fehlbare Provider privilegieren.

Massnahmen in allfälligen Strafverfahren müssen ohnehin unberührt bleiben. Auch wenn mit der Revision beabsichtigt ist (und im Erfolgsfall auch erreicht werden kann), dass Abhilfe gegen Urheberrechtsverletzungen in erster Linie in den vorgesehenen Verfahren und, soweit erforderlich, über zivilprozessuale Massnahmen erwirkt werden kann, schränkt das die Strafbarkeit vorsätzlich begangener Verletzungen nicht ein, und muss die Strafverfolgung vor allem schwerer Täter gewährleistet bleiben. Wünschenswert beim strafrechtlichen Schutz wäre, dass Anbieter von dezentral organisierten Internetdienstleistungen, insbesondere „Sharehoster", Linkressourcen etc., als Täter strafbar sind, wenn ihr Dienst Urheberrechtsverletzungen Dritter fördert, etwa durch finanzielle Anreize, oder ihr Dienst für eine Vielzahl von Urheberrechtsverletzungen missbraucht wird, ohne dass der Anbieter wirksame Gegenmassnahmen implementiert.

Eine entsprechende Regelung klagbarer Ansprüche gegen Access Provider (Fernmeldedienstanbieter) fehlt in Art. 62 Abs. 1bis. Daraus könnte e contrario zu schliessen sein, dass der Gesetzgeber hier kein zivilrechtliches Vorgehen vorsehen wollte. Das stiftet Unklarheit, denn Art. 66k Abs. 2 behält gerade vor, dass diese bei Verletzung ihrer Provider-Pflichten für Urheberrechtsverletzungen durch ihre Teilnehmer verantwortlich gemacht werden können; und auch der Bericht hält fest, die Eröffnung eines Sperr-Verwaltungsverfahrens bedeute nicht, „dass e contrario eine entsprechende gerichtliche Anordnung als Folge zivilrechtlicher Beseitigungs- und Unterlassungsklagen unzulässig wäre". Hier scheint eine Klarstellung geboten (komplementär zu Art. 66k Abs. 2).

„…und bei Verletzung der Pflichten nach den Artikeln 66b und 66c sowie 62a Absatz 2, 66d Absatz 2, 66e und 66g."

g) Datenschutzrechtliche Freistellung / Rechtfertigungsgrund – Art. 66j

Zweck und Ziele

Eines der Kernanliegen der Revision (seit dem Logistep-Entscheid des Bundesgerichts BGE 136 II 508 von 2009, der den gesetzgeberischen Handlungsbedarf festgehalten hatte) **war es, die zum Rechtsschutz erforderliche Datenerhebung und -bearbeitung auf eine gesetzliche Grundlage zu stellen, um sie überhaupt wieder zu ermöglichen.** Massstab dafür kann es nur sein, dass und wie Opfer von deliktischen Handlungen in praktisch allen anderen Lebensbereichen selbstverständlich berechtigt sind, die Informationen zu erheben und Rechtsverfolgungsbehörden vorzulegen, deren es zur Verfolgung der Täter und zur Geltendmachung der Ansprüche bedarf (Art. 2 Abs. 2, 13 Abs. 1 i. V. m. 6 Abs. 2 DSG[12]). Bei Internet-Urheberrechtsverletzungen sind das in der Regel (aber nicht zwingend) die IP-Adresse des benutzten Anschlusses und (v.a. bei dynamischen, also laufend neu zugewiesenen IP-Adressen) die Zeit, zu der der Anschluss missbraucht wurde, sowie die Evidenz für die Verletzungen.

Ziel muss also eine einfache und umfassende Rechtfertigung solcher Datenbearbeitung sein, wie sie andere Deliktsopfer auch beanspruchen könnten. Stattdessen macht es der Entwurf in Art. 66j so schwer wie möglich.

Kritik und Verbesserungsbedarf

Voraussetzungen

Datenerhebung wäre überhaupt nur in „Peer-to-Peer"-Netzwerken möglich - für alle anderen, vielfältigen Organisationsformen der Internet-Piraterie wäre es Geschädigten e contrario dann endgültig verboten, zu ihrem Schutz die nötigen Informationen zu erfassen. Auch diese Bestimmung muss technologieneutral formuliert werden.

Sie wäre zudem nur möglich, wenn von vornherein feststeht, dass es sich um eine schwerwiegende Verletzung nach dem Massstab des Hinweis-/ Offenlegungsverfahrens handelt. Damit würde das Gesetz die strengen Anforderungen, die es für eine (unterstellt) „fernmelderechtliche Teilnehmeridentifikation" bei Offenlegung der Anschlussinhaber aufstellt (Art. 62a Abs. 4), auch schon auf die blosse Erhebung der IP-Adressen und Zeitangaben anwenden, die (a) jedermann im Internet frei zugänglich sind und (b) den Geschädigten ohne das nachfolgende, aufwendige, gerichtliche Hinweis-/ Offenlegungsverfahren die Identifikation ja gerade noch nicht ermöglichen. Das ist offensichtlich der falsche Massstab.

In vielen Fällen wird erst anhand solcher Daten und nach der gerichtlichen Offenlegung der Identität überhaupt erkennbar sein, ob es sich um eine schwerwiegende Verletzung handelt – d.h., der Verletzte wird nicht einmal feststellen können, ob er die Daten erheben dürfte, ohne potentiell das Recht bereits gebrochen zu haben. (Die Erfahrung der Vergangenheit hat gelehrt, dass besonders schwere Rechtsverletzungen häufig erst in einem Strafverfahren durch die Strafverfolgungsbehörden ermittelt werden, was bei einem entsprechenden Tatverdacht selbstverständlich ebenfalls möglich bleiben muss.)

[12] Vgl. dazu Rosenthal/Jöhri, DSG, Art. 13 N 18.

Abschliessende Aufzählung

Die abschliessende Aufzählung der „erlaubten" Daten (IP-Adressen, „Time Codes", Werkdaten-„Hashcode"), widerspricht der Technologieneutralität des Urheberrechts; die Erhebung anderer benötigter Daten wäre e contrario nicht erlaubt; die Bestimmung wäre mit dem technologischen Wandel bald überholt.

Bekanntgabepflicht

Zu guter Letzt will der Entwurf den Verletzten verpflichten, Zweck, Art und Umfang der Datenerhebung „bekannt zu geben" (Art. 66j Abs. 3), z.B. auf seiner Website (Bericht S. 82). Auch hier wird der falsche Massstab angelegt, nämlich der einer Empfehlung des EDÖB für die Übergangszeit ohne gesetzliche Grundlage der Datenerhebung, während hier gerade diese Grundlage ja geschaffen werden soll. Zwar gilt dennoch das Transparenzprinzip, aber gerade keine Informationspflicht[13]; das Gesetz kann und sollte auch ohne explizite „Bekanntgabe" eine Rechtfertigung für die Datenerhebung (Art. 13 DSG) bieten – wie es ja auch in anderen Fällen möglich ist, aufgrund einer Interessenabwägung Informationen über Rechtsverletzer und Rechtsverletzung zu bearbeiten, um diese zu verfolgen bzw. Ansprüche geltend zu machen. Dies ganz abgesehen davon, dass keineswegs jeder verletzte Urheber oder Kleinproduzent über ausreichend prominente Kommunikationskanäle verfügt, um eine (sinnvolle) „Bekanntgabe" zu publizieren. Absatz 3 ist ersatzlos zu streichen. Die allgemeinen Grundsätze des DSG sind anwendbar und genügen.

Auch Abs. 2 und 4 sind redundant, weil sie ohnehin geltende Datenbearbeitungsgrundsätze wiederholen.

> **Art. 66j Datenbearbeitung durch die in ihrem Urheber- oder verwandten Schutzrecht verletzte Person**
>
> [1] Werden Urheber- oder verwandte Schutzrechte ~~über Peer-to-Peer-Netzwerke schwerwiegend~~ verletzt, so darf die verletzte Person ~~zur Bekämpfung dieser Verletzung~~ die zur Wahrung ihrer Rechte erforderlichen ~~folgenden~~ Daten erheben und speichern; bei Verletzungen mittels Fernmeldediensten insbesondere:
>
> die IP-Adresse des Teilnehmers oder der Teilnehmerin, dessen oder deren Anschluss für die Verletzung verwendet wurde;
>
> das Datum und die Uhrzeit der Zugänglichmachung der Werke und anderer Schutzobjekte sowie die Dauer, während der das Werk oder andere Schutzobjekt zugänglich war;
>
> den elektronischen Fingerabdruck des Werks oder des anderen Schutzobjekts.
>
> ~~[2] Die in ihrem Urheber- oder verwandten Schutzrecht verletzte Person darf nicht mehr Daten erheben und speichern, als für die Verfolgung der Rechtsverletzungen unabdingbar ist.~~
>
> ~~[3] Sie hat den Zweck, die Art und den Umfang der Datenerhebung und -speicherung bekannt zu geben.~~
>
> ~~[4] Sie hat die Daten durch angemessene technische und organisatorische Massnah- men gegen unbefugte Bearbeitung zu schützen.~~

Entsprechend genügt beim Verweis auf die Datenbearbeitung in Art. 62a der Hinweis auf die Rechtmässigkeit der Datenschutzbearbeitung, die nicht allein Art. 66j folgt:

> **Art. 62a Absatz 1** Wer in seinem Urheber- oder verwandten Schutzrecht schwerwiegend verletzt wird, kann gestützt auf Daten, die er oder sie ~~nach Artikel 66j~~ rechtmässig bearbeitet hat, vom Gericht verlangen, dass dieses die Anbieterin von Fernmeldediensten verpflichtet, die Teilnehmer oder Teilnehmerinnen zu identifizieren, deren Anschlüsse für die Verletzung verwendet wurden.

[13] Vgl. Rosenthal/Jöhri, DSG Art. 4 N 51